Decodificação de máxima verossimilhança para códigos de bloco lineares: probabilidades de erro do código de repetição e do código de Hamming

Maximum likelihood decoding for linear block codes: error probabilities of the repetition code and of the Hamming code

Jorge Kysnney Santos Kamassury
Universidade Federal de Santa Catarina (UFSC)
Programa de Pós-Graduação em Engenharia Elétrica (PPGEEL), Florianópolis, SC, Brasil
http://orcid.org/0000-0001-8335-9796, jorge.kamassury@posgrad.ufsc.br

Israel Félix de Moura Tôrres
Universidade Federal de Santa Catarina (UFSC)
Programa de Pós-Graduação em Engenharia Elétrica (PPGEEL), Florianópolis, SC, Brasil
http://orcid.org/0000-0003-0673-3259, israel.felix@posgrad.ufsc.br

Wandesson Gomes Duarte
Universidade Federal de Santa Catarina (UFSC)
Programa de Pós-Graduação em Engenharia de Automação e Sistemas (PPGEAS)
Florianópolis, SC, Brasil
http://orcid.org/0000-0001-7651-1462, wandesson.duarte@posgrad.ufsc.br

Informações do Artigo

Histórico do Artigo
Submissão: 27 de março de 2019.
Aceite: 28 de maio de 2019.

Palavras-chave
Máxima Verossimilhança
Códigos Corretores de Erros
Códigos de Bloco Lineares
Código de Hamming
Probabilidade de Erro

Resumo
No presente artigo, apresentamos os resultados de simulações dos desempenhos dos códigos de bloco lineares para três diferentes taxas de transmissão. Empregado o critério de máxima verossimilhança, computamos e comparamos os desempenhos (teóricos e simulados) dos casos codificados com os casos não codificados. Para fins de simulação do canal de transmissão, utilizamos a modelagem do canal BSC. Os resultados apresentados evidenciam os benefícios da codificação de canal para reduzir as taxas de erros de símbolos e/ou bits nos sistemas de comunicação. Todas as rotinas usadas para as simulações foram implementadas por meio da plataforma computacional MATLAB e estão disponíveis no endereço virtual indicado.

Keywords
Maximum Likelihood
Error Correcting Codes
Linear Block Codes
Hamming Code
Probability of Error

Abstract
In this paper, we present the performance simulation results of linear block codes for three different transmission rates. Using the maximum likelihood criterion, we compute and compare the cases coded performances (theoretical and simulated) with the non-coded cases. For the transmission channel simulating purpose, we used the BSC channel modeling. The results presented highlight the benefits of channel coding to reduce the error rates of symbols and/or bits in communication systems. All simulations routines were implemented through the MATLAB computer platform and are available at the indicated virtual address.

1 Introdução

Os sistemas digitais de comunicação - transmissão e armazenamento de dados - estão sujeitos a várias fontes de erros (ruídos aleatórios, interferências e falhas) que corrompem a informação emitida. Nesse contexto de interesse, os códigos corretores de erros (ECCs) podem ser empregados para detectar e corrigir erros; em outras palavras, os ECCs são aplicados com o objetivo de reduzir a probabilidade de erro de bit ou de bloco de informação transmitida.

Com efeito, os ECCs têm como principal vantagem a otimização dos desempenhos dos sistemas em relação a uma transmissão não codificada. De fato, hoje, praticamente todos os sistemas de comunicação (telefonia digital, internet, TV digital, transmissão via satélite etc.) fazem uso de algum tipo de ECC.

De modo geral, esses códigos incorporam bits redundantes na informação a ser transmitida, de tal forma que, na etapa de decodificação, esses bits adicionais permitem a detecção e correção de erros nos bits recebidos. Em detalhe, a codificação de canal pode ser compreendida como o mapeamento da constelação do sinal a ser interpretada em um espaço do sinal com dimensão maior do que aquela necessária para a transmissão do sinal desejado. Esse mapeamento permite elevar a distância entre os pontos da constelação e reduzir o efeito do ruído.

Os ECCs podem ser agrupados em duas grandes categorias, a saber: os códigos de bloco e os códigos convolucionais[1]. No caso dos códigos de bloco, os dados são codificados/decodificados bloco por bloco que, por sua vez, são considerados independentes. Dessa forma, a codificação em bloco é considerada uma operação sem memória e pode ser modelada/implementada via lógica combinatória.

No presente artigo, são apresentados os resultados das probabilidades de erro de palavra-código de códigos de bloco lineares para três diferentes taxas de transmissão[2] - código de repetição (7,1), código de Hamming (7,4) e caso não codificado (7,7) - bem como discute-se as características e vantagens da codificação. Para a etapa de decodificação, utiliza-se o critério de máxima verossimilhança.

[1] Realizados recorrendo a codificadores com memória.

[2] As notações "(7,1), (7,4) e (7,7)" correspondem, respectivamente, aos códigos de bloco lineares com taxas de transmissão $R = \frac{1}{7}$, $R = \frac{4}{7}$ e $R = \frac{7}{7} = 1$ abordados na seção 6.

2 Aspectos gerais sobre códigos de blocos

No contexto dos códigos de blocos, uma sequência de informação gerada, por exemplo, por uma fonte binária é subdividida em blocos de k bits cada, denotadas pelo vetor $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$. Nesse caso, para cada $u_i \in \{0, 1\}$, $0 \leq i \leq k-1$, há 2^k possíveis vetores de informação.

A codificação de bloco, em específico, associa um vetor $\mathbf{v} = (v_0, v_1, v_2, \cdots, v_{n-1})$, denominado de palavra-código, com n bits ($n > k$) a cada um dos vetores de informação. Conforme conceituam Lathi e Ding (2009), a palavra-código é a unidade de bits que pode ser decodificada de modo independente. Com efeito, o conjunto das 2^k palavras-código é chamado de código de bloco. Enfatiza-se que um código de bloco é essencialmente um subconjunto $\mathcal{C}$ de todos os 2^n vetores binários.

Para um canal BSC (*Binary Symmetric Channel*), por exemplo, sabe-se que o canal transmite um dígito binário por vez; por consequência, um canal BSC deverá ser usado n vezes para a devida transmissão de uma palavra-código (UCHÔA FILHO, 2005). Como o vetor de informação é formado por k dígitos binários, então a taxa de transmissão é dada por:

$$R = \frac{k}{n}, \qquad \text{bits por uso do canal} \tag{1}$$

Objetivando a modelagem da transmissão de informação no canal ruidoso (nesse caso, o BSC), pode-se adicionar um vetor $\mathbf{e} = (e_0, e_1, e_2, \cdots, e_{n-1})$ à palavra-código transmitida (pós codificação) conforme ilustra a Figura 1. Logo, $\mathbf{r}$ é uma versão ruidosa de $\mathbf{v}$, ou seja[3]:

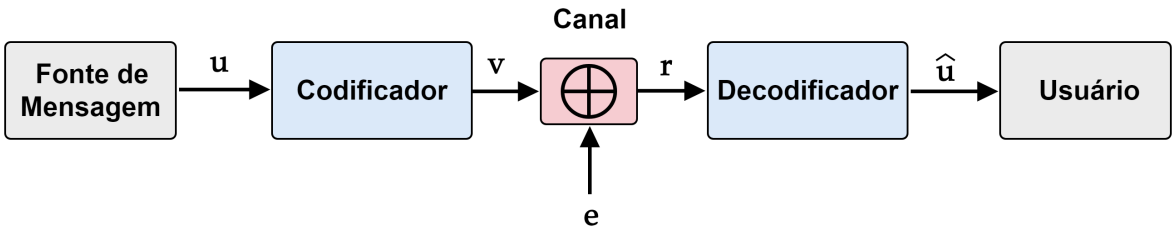
$$\begin{aligned} \mathbf{r} &= \mathbf{v} \oplus \mathbf{e} \\ &= (v_0, v_1, v_2, \cdots, v_{n-1}) \oplus (e_0, e_1, e_2, \cdots, e_{n-1}) \\ &= (v_0 \oplus e_0, v_1 \oplus e_1, v_2 \oplus e_2, \cdots, v_{n-1} \oplus e_{n-1}) \\ &= (r_0, r_1, r_2, \cdots, r_{n-1}) \end{aligned} \tag{2}$$

Nesse sentido, a função do decodificador do canal ilustrado na Figura 1 será obter uma estimativa $\widehat{\mathbf{v}}$ para $\mathbf{v}$ transmitido, ou equivalentemente, uma estimativa $\widehat{\mathbf{u}}$ para o vetor de informação $\mathbf{u}$.

Ainda, vale observar, conforme menciona Uchôa Filho (2005), que, para especificarmos um código de taxa definida pela Equação 1, precisamos escolher 2^k palavras-código dentre os 2^n pos-

[3] O símbolo $\oplus$ denota que a operação de adição é dada pela operação módulo-2.

Figura 1 – Diagrama simplificado de um sistema de comunicação binária com código de bloco.



Fonte: Elaboração dos autores.

síveis vetores de comprimento n. Não é difícil perceber que isso implica em uma exaustiva tarefa, haja vista que há $\binom{2^n}{2^k}$ modos de se escolher 2^k palavras-código!

Nesse contexto, manifesta-se a necessidade de estabelecer alguns critérios para essa árdua escolha. Dentre esses critérios, acentua-se o de máxima verossimilhança (*Maximum Likelihood*-ML) que atua minimizando a probabilidade de erro de palavra-código quando os bits da fonte são equiprováveis (SKLAR, 2001).

3 Decodificação de máxima verossimilhança e a distância de Hamming

De início, considere **u** o bit de informação e **v** a palavra transmitida conforme ilustrado na Figura 1. Com efeito, o processo de decodificação atuará para estimar $\widehat{\mathbf{u}}$ (ou $\widehat{\mathbf{v}}$) a partir de **r** (os bits recebidos). De fato, o erro de palavra-código ocorre se $\widehat{\mathbf{u}} \neq \mathbf{u}$ (ou $\widehat{\mathbf{v}} \neq \mathbf{v}$). Nesse caso, a probabilidade de ocorrência do evento erro (E) de palavra-código dado que **r** foi recebido é definida por

$$\Pr\{\mathsf{E}|\mathbf{r}\} \triangleq \Pr\left\{\widehat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r}\right\} \tag{3}$$

enquanto a probabilidade de erro de palavra-código média é expressa por:

$$\Pr\{\mathsf{E}\} = \sum_{\mathbf{r}} \Pr\{\mathsf{E}|\mathbf{r}\} \times \Pr(\mathbf{r}) \tag{4}$$

Nesse contexto, o objetivo fundamental do processo de decodificação incorre em otimizar a estimativa de $\widehat{\mathbf{v}}$, isto é, minimizar a probabilidade condicionada $\Pr\left\{\widehat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r}\right\}$ ou, alternativamente, maximizar $\Pr\left\{\widehat{\mathbf{v}} = \mathbf{v}|\mathbf{r}\right\}$. Para tanto, podemos fazer uso da *regra de Bayes*, cuja aplicação nos retorna:

$$\Pr(\mathbf{v}|\mathbf{r}) = \frac{\Pr(\mathbf{r}|\mathbf{v}) \times \Pr(\widehat{\mathbf{v}})}{\Pr(\mathbf{r})} \tag{5}$$

Admitindo que os 2^k vetores de informação **u** sejam *equiprováveis*, infere-se facilmente que $\Pr(\mathbf{v})$ não depende de **v**. Da mesma forma, $\Pr(\mathbf{r})$ não depende de **v**. Por fim, a otimização da Equação 5 resulta na maximização de $\Pr(\mathbf{r}|\mathbf{v})$ que, por sua vez, recebe o nome de *função de verossimilhança*.

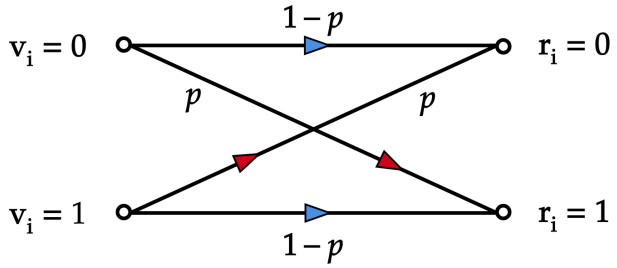
Para um canal *sem memória*, r_i não depende estatisticamente do dígito transmitido v_j (para $i \neq j$); naturalmente, em razão do ruído e_i, r_i também pode ser diferente de v_i. Isto posto, conforme discutido anteriormente, a decodificação se empenhará na maximização da expressão:

$$\begin{aligned} \mathsf{P}(\mathbf{r}|\mathbf{v}) &= P\left[(r_0, r_1, r_2, \cdots, r_{n-1}) \,|\, (v_0, v_1, v_2, \cdots, v_{n-1})\right] \\ &= \prod_{i=0}^{n-1} P\left(r_i|v_i\right) \end{aligned} \tag{6}$$

Para o canal BSC representado na Figura 2, as probabilidades condicionadas serão dadas por:

$$\mathsf{P}(r_i|v_i) = \begin{cases} 1-p, & \text{para} \quad r_i = v_i \\ p, & \text{para} \quad r_i \neq v_i \end{cases}$$

Figura 2 – Canal binário simétrico com probabilidade de transição p.



Fonte: Elaboração dos autores.

Nesse ínterim, para dois vetores **v** e **v**′ quaisquer, define-se a *distância de Hamming* entre **v** e **v**′ como:

$$d_H(\mathbf{v}, \mathbf{v}') = \text{número de posições em que os dois vetores diferem} \tag{7}$$

3.1 Algoritmo simplificado da decodificação de máxima verossimilhança para códigos de blocos

As etapas para a decodificação usando o critério de máxima verossimilhança podem ser elencadas da seguinte forma:

- Registrar a saída do canal, isto é, **r** (palavra-código + ruído);
- Calcular a distância de Hamming $d_H(\mathbf{v}, \mathbf{r})$ para as 2^k palavras-código do código $\mathcal{C}$;
- Selecionar a palavra $\hat{\mathbf{v}}$ mais próxima de **v** tal que:

$$d_H(\widehat{\mathbf{v}}, \mathbf{r}) \leq d_H(\mathbf{v}, \mathbf{r}) \, , \, \forall \, \mathbf{v} \neq \widehat{\mathbf{v}} \in \mathcal{C} \tag{8}$$

4 Códigos de bloco lineares

Um código em bloco (n, k) é dito linear se e somente se as 2^k palavras-código formam um subespaço de dimensão k de um espaço vetorial composto por todos os vetores binários de comprimento n (CAVALCANTI *et al.*, 2018). Nesse sentido, os códigos de bloco lineares têm como principais características:

- A soma de duas palavras-código quaisquer em $\mathcal{C}$ também pertence a $\mathcal{C}$, isto é:

$$\mathbf{v} \oplus \mathbf{v}^{'} = \mathbf{v}^{''} \in \mathrm{C} \tag{9}$$

- Há k palavras-código linearmente independentes tais que qualquer palavra em $\mathcal{C}$ pode ser expressa como uma combinação linear de k palavras-código.

4.1 Matriz Geradora

Conforme já mencionado, em virtude da linearidade do código, é possível selecionar k palavras-código linearmente independentes formando uma base de um espaço linear k-dimensional de modo que qualquer palavra-código possa ser obtida por uma combinação linear das k palavras-código da base. Essas k palavras-código podem ser obtidas fazendo uso da *matriz geradora*[4] denotada por **G**. Em geral, para k e n quaisquer, temos:

$$\mathbf{v} = \mathbf{u}\,\mathbf{G} \tag{10}$$

na qual,

$$\mathbf{u} = (u_0, u_1, \cdots, u_{k-1}) \tag{11}$$

$$\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \tag{12}$$

[4] Apenas os códigos de bloco lineares possuem matriz geradora.

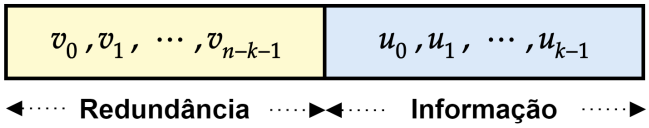
e

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & g_{0,3} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{1,n-1} \\ g_{2,0} & g_{2,1} & g_{2,2} & g_{2,3} & \cdots & g_{2,n-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k=1,0} & g_{k-1,1} & g_{k-1,2} & g_{k-1,3} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

Pode-se ainda incluir os bits de informação inalterados na palavra-código. Um código de bloco linear com essa característica é chamado de *sistemático* (ver Figura 3). Nesse caso, a palavra-código é denotada por

$$\mathbf{v} = (v_0, v_1, \cdots, v_{n-k-1}, u_0, u_1, \cdots, u_{k-1}) \tag{13}$$

Figura 3 – Representação sistemática de uma palavra-código.



Fonte: Elaboração dos autores.

enquanto a matriz geradora é

$$\mathbf{G} = \left[\mathbf{P}_{k\times(n-k)} : \mathbf{I}_k\right] \tag{14}$$

onde $\mathbf{I}_k$ é a matriz identidade de ordem k e **P** é a matriz que determina os bits de paridade que são utilizados para detecção e/ou correção de erro.

4.2 Matriz de verificação de paridade

Considere o conjunto formado por todas as palavras-código de um código linear de taxa R com matriz geradora **G**. Da Teoria de Espaços Lineares, existe uma matriz $\mathbf{H}_{(n-k)\times n}$ cujas linhas são linearmente independentes tal que qualquer vetor em $\mathcal{C}$ é ortogonal às linhas de **H**, assim como qualquer vetor de comprimento n ortogonal às linhas de **H** pertence a $\mathcal{C}$.

Dessa última observação, pode-se argumentar que uma $n-$upla **v** é uma palavra-código (do código $\mathcal{C}$) se e somente se

$$\mathbf{v} \cdot \mathbf{H}^T = 0 \tag{15}$$

onde **H** é a matriz de verificação de paridade do código.

4.3 **Distância de Hamming, capacidade de detecção e capacidade de correção**

Pode-se estender a definição da distância de Hamming apresentada na seção (3.1) para um bloco linear $\mathcal{C}$. Nesse contexto, $\mathsf{d}_{\min}(\mathcal{C})$ será expressa por

$$\mathsf{d}_{\min} \stackrel{\triangle}{=} \min\left\{d_H(\mathbf{v},\mathbf{v}')|\mathbf{v}\in\mathcal{C},\,\mathbf{v}'\in\mathcal{C},\,\mathbf{v}\neq\mathbf{v}'\right\} \tag{16}$$

ou, alternativamente

$$\mathsf{d}_{\min} \stackrel{\triangle}{=} \min\left\{w_H(\mathbf{v}'')|\mathbf{v}''\in\mathcal{C},\mathbf{v}''\neq 0\right\} \tag{17}$$

onde w_H refere-se ao peso de Hamming e indica o número de elementos diferentes de zero no vetor de código. Isto posto, pode-se enunciar que, para um código linear, a distância mínima é igual ao peso mínimo de suas palavras-código não-nulas! Essas novas definições são bastante úteis para se determinar as capacidades de detecção e correção de um código.

Compreende-se que um código tem capacidade de detecção de N_d erros de bit se o mesmo for capaz de detectar qualquer padrão de erro **e**, em que $w_H(\mathbf{e}) \leq N_d$, e se existir pelo menos um padrão de erro **e**, isto é $w_H(\mathbf{e}) = N_d + 1$, que o código não seja capaz de detectar (LIN; COSTELLO, 2004). Nesse sentido, a capacidade de detecção (C_d) será[5]:

$$C_d = \mathsf{d}_{\min} - 1 \tag{18}$$

Por sua vez, um código tem capacidade de correção de N_c erros de bit se ele for capaz de corrigir qualquer padrão de erro **e**, onde $w_H(\mathbf{e}) \leq N_c$, e se existir ao menos um padrão de erro **e** que o código não seja capaz de corrigir [6]. Por consequência, a capacidade de correção do código t é obtida por:

$$t = \left\lfloor \frac{\mathsf{d}_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{C_d}{2} \right\rfloor \tag{19}$$

5 Códigos de Hamming

Os códigos de Hamming são aqueles definidos como uma família de códigos lineares em bloco (n, k) que possuem as seguintes características:

[5]Enfatiza-se que a detecção de erro ocorre quando o vetor recebido **r** não é uma palavra-código, visto que apenas palavras-código são transmitidas pelo canal.

[6]Vale observar que o decodificador tentará corrigir erros quando **r** não for uma palavra-código.

- Comprimento do bloco: $n = 2^m - 1$;
- Quantidade de bits de mensagem: $k = 2^m - m - 1$;
- Quantidade de bits de paridade $m = n - k$, com $m \leq 3$;
- Distância mínima: $d_{min} = 3$.

6 Resultados das simulações e discussões

Nessa seção, são apresentados os resultados das simulações das probabilidades de erro de palavra-código (P_{wer_s}) para os seguintes casos: código de repetição (7,1), código de Hamming (7,4) e o caso não codificado (7,7). Todas as simulações[7] foram realizadas através da plataforma computacional MATLAB (Matrix Laboratory).

A expressão geral para a probabilidade de erro médio teórico da palavra-código (P_{wer_t})[8] será dada pela Equação 20, na qual t corresponde à capacidade de correção do código de bloco.

$$P_{wer_t} = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i \, (1-p)^{n-i} \tag{20}$$

Para fins de análise, as curvas simuladas são comparadas com as curvas das probabilidades teóricas e àquelas referentes aos casos não codificados (P_{wer_u}). Enfatiza-se que P_{wer_t} e P_{wer_u} são diferentes, visto que P_{wer_t} denota a probabilidade de erro médio téorico da palavra-código usando o critério ML para decodificação, enquanto P_{wer_u} refere-se à probabilidade de erro médio da palavra-código não decodificada usando o referido critério. Assim, para obtenção de P_{wer_u}, a palavra-código recebida é considerada igual à palavra-código transmitida.

Em todas as simulações, utiliza-se $L = 5000$ blocos[9] e probabilidade $p \in [0,\, 0.5]$ para o canal BSC. O Quadro 1 mostra uma versão simplificada do algoritmo implementado.

[7] Os códigos utilizados podem ser consultados em: `https://github.com/Kamassury/Decodificacao-ML`.
[8] WER - Word Error Rate.
[9] Os códigos se diferenciam pelos comprimentos de k e n.

Quadro 1: Algoritmo simplificado que retorna a probabilidade de erro das palavras-código.

Entrada: k, n, G, L

Saída: $P_{wer_t}, P_{wer_s}, P_{wer_u}$

início
- Gerar as palavras-código iniciais
- Gerar aleatoriamente os bits de informação e palavras-código para transmissão
- **para** *cada* p **faça**
  - Gerar ruido aleatório e adicioná-lo aos bits de informação transmitidos
  - Definir as palavras recebidas como resultado da adição de ruido às palavras-código transmitidas
  - Promover a decodificação usando o critério ML
  - Calcular P_{wer_s} e P_{wer_u}
- **fim**
- Calcular P_{wer_t}

fim

retorna $P_{wer_t}, P_{wer_s}, P_{wer_u}$

Fonte: Elaboração dos autores.

Para simular o canal BSC, utiliza-se a expressão `round(rand(bits,n)-0.5+p)` para gerar o ruído binário do canal. Nesse caso, são gerados valores aleatórios entre 0 e 1 que, por sua vez, são arredondados para 0 ou 1 (para baixos valores de p, obtém-se bit 0 e para p próximo de 0.5, obtém-se bit 1).

Na etapa de decodificação, aplica-se o critério ML para o código de repetição[10] e o código de Hamming. Conforme é discutido posteriormente, o código (7,7) não tem decodificação.

6.1 Código de repetição (7,1)

Para o referido código de repetição, temos $k = 1$ e $n = 7$, ou seja, esse código tem 1 bit de informação para cada bloco (sendo a palavra-código composta por 7 bits). Nesse caso, a matriz geradora é:

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

[10] Pode-se também promover decodificação via lógica majoritária.

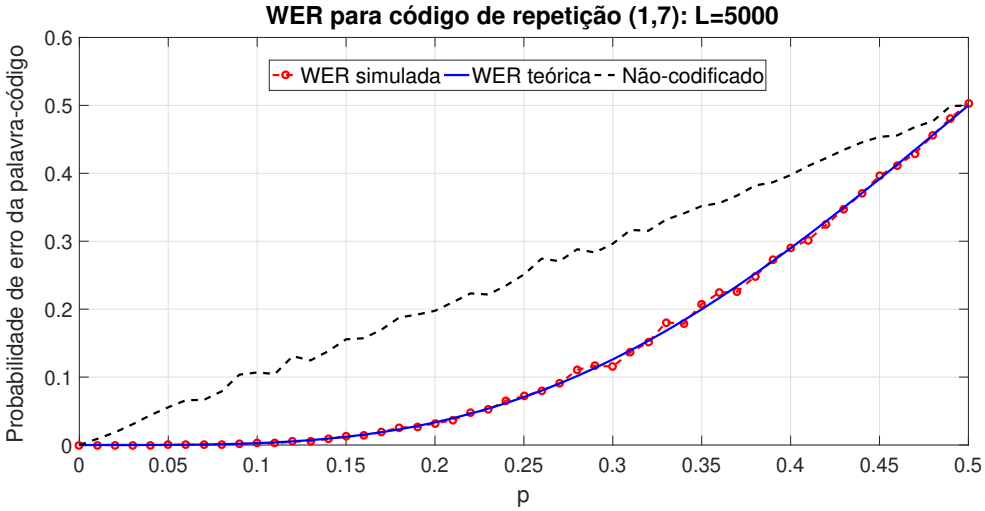
A expressão da probabilidade teórica do erro médio da palavra-código para o código (7,1) é dada por:

$$\begin{aligned} P_{wer_t} &= 1 - \sum_{i=0}^{t=3} \binom{7}{i} p^i (1-p)^{7-i} \\ &= 1 - \left[\binom{7}{0} p^0 (1-p)^7 + \binom{7}{1} p (1-p)^6 + \binom{7}{2} p^2 (1-p)^5 + \binom{7}{3} p^3 (1-p)^4 \right] \\ &= 1 - \left[35p^3(1-p)^4 + 21p^2(1-p)^5 + 7p(1-p)^6 + (1-p)^7 \right] \end{aligned} \tag{21}$$

A Figura 4 apresenta os resultados da simulação do código de repetição (7,1). De fato, verifica-se que a probabilidade de erro médio da palavra-código obtida via simulação (P_{wer_s}) é bastante próxima do valor teórico (P_{wer_t}) dado pela Equação 21.

A curva do caso não codificado (P_{wer_u}) permite-nos avaliar o quão importante é a estratégia de codificação para reduzir a probabilidade de erro médio da palavra-código. Enfatiza-se que, para o intervalo de probabilidade do canal em questão, a diferença entre P_{wer_s} e P_{wer_u} tem comportamento crescente para baixas probabilidades, atingindo seu valor máximo em torno de $p = \frac{1}{4}$.

Figura 4 – Curvas das probabilidades dos erros médios das palavras-código (simulada e teórica) referentes ao código de repetição (7,1) e ao caso não codificado (7,1).



Fonte: Dados da pesquisa.

6.2 **Código de Hamming (7,4)**

No caso do código de Hamming (7,4), tem-se uma taxa de transferência de $R = \frac{4}{7}$. Para o processo de codificação, utilizou-se a seguinte matriz geradora:

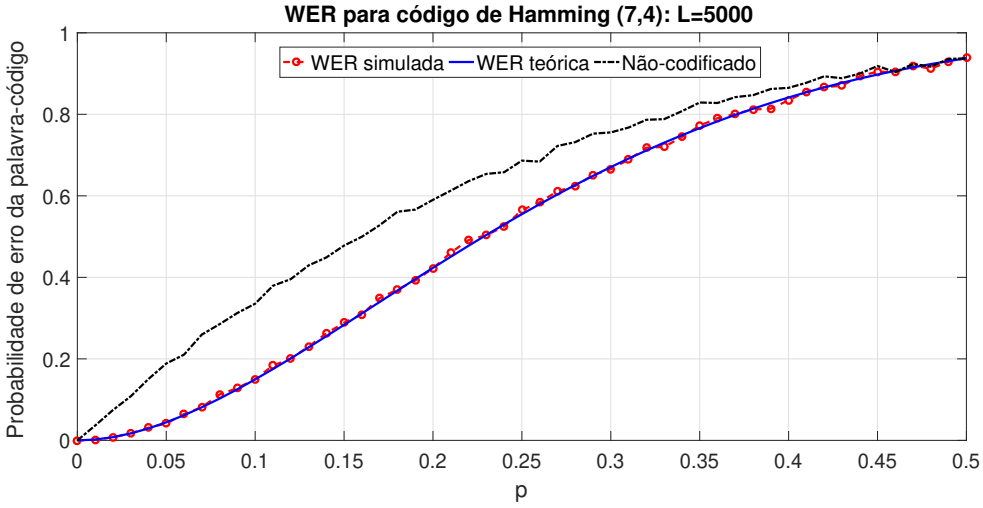
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Esse código tem capacidade de detecção de $t = 1$ e sua probabilidade teórica do erro médio é dada por:

$$\begin{aligned} P_{wer_t} &= 1 - \sum_{i=0}^{t=1} \binom{7}{i} p^i (1-p)^{7-i} \\ &= 1 - \left[\binom{7}{0} p^0 (1-p)^7 + \binom{7}{1} p (1-p)^6 \right] \\ &= 1 - \left[7p(1-p)^6 + (1-p)^7 \right] \end{aligned} \tag{22}$$

Os resultados da simulação para esse código de Hamming estão ilustrados na Figura 5.

Figura 5 – Curvas das probabilidades dos erros médios das palavras-código (simulada e teórica) referentes ao código de Hamming (7,4) e ao caso não codificado (7,4).



Fonte: Dados da pesquisa.

De fato, as curvas das probabilidades simulada e teórica são bastante próximas, endossando a validade da equação (22). Novamente, observa-se que a estratégia de codificação apresenta uma probabilidade de erro médio de palavra-código menor que o caso não codificado. Assim como no código de repetição, o desempenho da codificação apresenta melhores resultados para valores baixos de p do canal BSC.

6.3 **Código (7,7)**

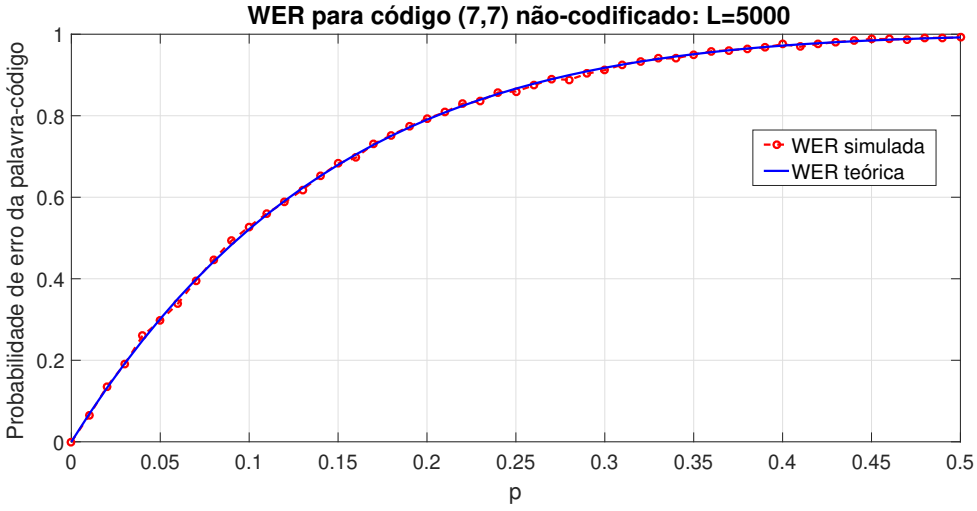
De imediato, verifica-se que esse código corresponde à transmissão de blocos de 7 bits não codificados ($R = 1$). Naturalmente, a matriz geradora nesse caso é a matriz identidade $\mathbf{I}_{7\times 7}$. Vale enfatizar que nesse caso não há decodificação, ou seja, a palavra-código decodificada é o próprio vetor recebido **r**.

Por razões óbvias, o código (7,7) não tem capacidade de correção e, portanto, a probabilidade teórica do erro médio é dada por:

$$\begin{aligned} P_{wer_t} &= 1 - \sum_{i=0}^{t=0} \binom{7}{i} p^i (1-p)^{7-i} \\ &= 1 - \left[\binom{7}{0} p^0 (1-p)^7 \right] \\ &= 1 - (1-p)^7 \end{aligned} \tag{23}$$

A Figura 6 apresenta os resultados da simulação para o código (7,7). Nesse caso estão plotadas as curvas da probabilidade de erro médio (simulada e teórica) da palavra-código em questão.

Figura 6 – Curvas das probabilidades dos erros médios das palavras-código (simulada e teórica) referentes ao código (7,7).

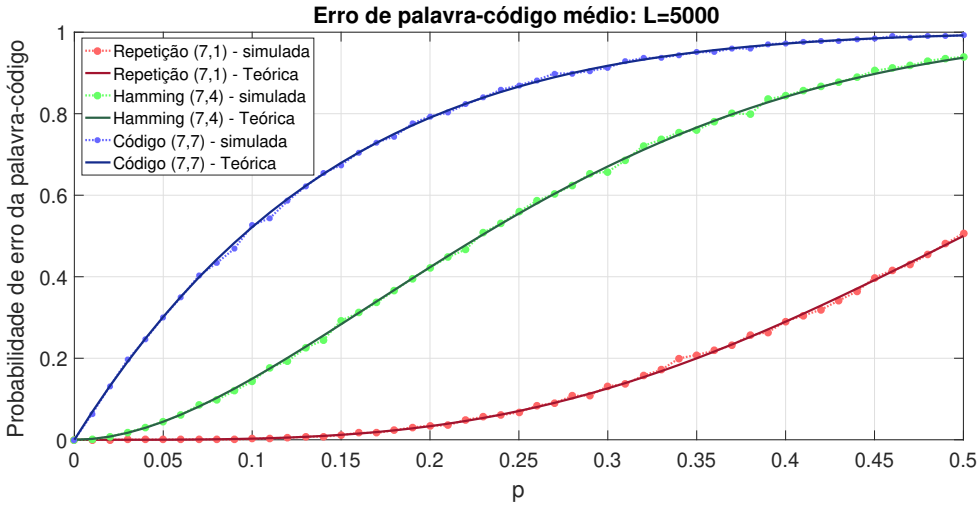


Fonte: Dados da pesquisa.

Com efeito, não ocorre melhoria da probabilidade de erro médio, fato esse já esperado, haja vista que não há codificação e, por consequência, incapacidade de correção de erros.

Para efeitos de comparação, a Figura 7 apresenta as probabilidades de erro para todos os três códigos abordados.

Figura 7 – Curvas das probabilidades dos erros médios das palavras-código (simulada e teórica) para o código de repetição (7,1), o código de Hamming (7,4) e o código (7,7).



Fonte: Dados da pesquisa.

Facilmente se verifica que a redução da taxa de transmissão promove a redução da probabilidade de erro médio da palavra-código, ou seja, o código (7,1) tem desempenho melhor que o código de Hamming (7,4) e ambos são melhores que o caso não codificado.

Apesar do código (7,1) apresentar desempenho superior ao código de Hamming (7,4), vale ressaltar que a redundância incorpora uma sobrecarga e, por conseguinte, consome recursos adicionais como potência e banda. Por esse motivo, na prática, é essencial manter o nível de repetição o menor possível sem comprometer severamente a performance do código.

7 Considerações finais

No discorrer desse artigo, discutiu-se a importância da codificação e elencamos aspectos fundamentais da teoria de códigos de bloco lineares, além de abordar a modelagem do canal BSC e a decodificação ML. Em foco, foram apresentados os resultados das simulações do desempenho dos códigos de bloco lineares para três diferentes taxas de transmissão em um canal BSC (com $p \in [0, 0.5]$).

Verificou-se que os códigos com $R < 1$ têm desempenhos bem melhores que a transmissão sem codificação ($R = 1$), justificando assim a relevância do uso de ECCs.

Ademais, vale salientar que, embora o desempenho do código de repetição (7,1) seja superior ao do código de Hamming (7,4), fato este diretamente relacionado às capacidades de detecção e correção de erros, na prática, sua implementação demanda mais banda e potência; isso evidencia, portanto, que o *trade-off* entre desempenho e recursos para implementação é outro aspecto a ser considerado em um projeto de codificação!

Referências

CAVALCANTI, F. R. P.; MACIEL, T. F.; FREITAS JÚNIOR, W. C.; SILVA, Y. C. B. **Comunicação Móvel Celular**. 1. ed. Rio de Janeiro: Elsevier, 2018.

LATHI, B. P.; DING, Z. **Modern Digital and Analog Communication Systems**. 4. ed. New York: Oxford University Press, 2009.

LIN, S.; COSTELLO, D. **Error Control Coding**: Fundamentals and Applications. 2. ed. Upper Saddle River, NJ: Prentice-Hall, 2004.

SKLAR, B. **Digital Communication**: Fundamentals and Applications. 2. ed. Upper Saddle River, NJ: Prentice-Hall, 2001.

UCHÔA FILHO, B. F. **Probabilidade e Teoria da Informação**. Florianópolis: UFSC, 2005. 124 p. Apostila.