

## O Código de Hamming e suas Aplicações

Rafaela C. Queiroz<sup>1</sup>

Bacharelado em Engenharia Química - UTFPR, Campo Mourão, PR

Belatrice R. Bolzani<sup>2</sup>

Bacharelado em Engenharia Ambiental - UTFPR, Campo Mourão, PR

Erika P. D. O. Guazzi<sup>3</sup>

DAMAT - UTFPR, Campo Mourão, PR

Na atualidade, os meios de comunicação transmitem milhares de informações a cada fração de segundo devido aos avanços tecnológicos e utilização da internet. Contudo, com tantas informações enviadas e recebidas, os canais de transmissão podem sofrer interferências e provocarem erros nessas transmissões de dados. Para corrigir esses erros, os canais de transmissão utilizam os Códigos Corretores de Erros com o objetivo de detectar e corrigir os erros que possam ocorrer. Recorda-se que essa área de pesquisa, dentro da Teoria da Informação, foi iniciada em 1948 por Shannon com o trabalho “A Mathematical Theory of Communications”, [1].

O presente trabalho aborda o código de Hamming e algumas aplicações. Esse é um código simples capaz de detectar e corrigir erros no processamento de sinais e nas telecomunicações. O matemático Richard Hamming foi um dos pioneiros na pesquisa e desenvolvimento de Códigos Corretores de Erros. Trabalhou no laboratório da Bell Telephone colaborando com Shannon.

Hamming observou que as máquinas utilizadas detectavam erros em sua programação, mas não eram capazes de corrigi-los. Assim, a motivação de Hamming foi criar um código que fosse capaz de detectar e corrigir erros. Em outras palavras, uma vez que fosse detectado um erro, a máquina não poderia realizar nenhum outro cálculo até que o erro detectado fosse localizado e corrigido. Diante disso, foi desenvolvido o código de Hamming, que é um código de bloco linear, baseado na adição de bits de paridade sobre um bloco de dados de comprimento fixo, para diminuir a influência de ruídos nas transmissões. Ressalta-se que o código de Hamming é capaz de detectar dois bits e corrigir um bit único, [2].

Os passos para construir um código de Hamming são: (i) determinar o número de bits de paridade  $b$  necessários, que satisfaça  $2^b \geq k + b + 1$ , onde  $k$  é o número de dígitos da informação a ser codificada,  $b$  é o primeiro número natural que satisfaz esta relação; (ii) arranjar os bits de paridade na informação colocando-os da esquerda para a direita na posição onde se encontram as potências de 2; (iii) atribuir adequadamente o valor 0 ou 1 para cada bit de paridade; e (iv) determinar a palavra-código resultante, [3].

Assim, em geral, um código de Hamming de ordem  $m \geq 2$  é um código linear  $C(n, k)$ , onde  $n = 2^m - 1$ ,  $k = 2^m - m - 1$  e  $m = n - k$  é o número de bits de paridade. E mais, a distância de Hamming é importante no processo de decodificação de mensagens e é dada por  $d(x, y) = |\{i \in \{1, 2, \dots, n\} / x_i \neq y_i\}|$ , onde  $x, y \in C$  e a capacidade de correção de erro é dada por  $t = \lfloor \frac{d_{min}-1}{2} \rfloor$ , onde  $\lfloor x \rfloor$  denota o maior inteiro menor ou igual a  $x$  e  $d_{min} = \min\{d(x, y) / x, y \in C \text{ e } x \neq y\}$ .

Além disso, as palavras-códigos podem ser obtidas a partir da matriz geradora  $G$ , cujas linhas são formadas pelos vetores que formam uma base do código. Sempre que possível, a matriz  $G$  é dada na forma padrão  $G = (I_k | P)$ , onde  $P$  é a submatriz de paridade de ordem  $(n - k) \times k$ .

---

<sup>1</sup>rafaelacorreaqueiroz@hotmail.com

<sup>2</sup>bolzanibelatrice24@gmail.com

<sup>3</sup>erikapatricia@utfpr.edu.br

Para verificar se uma mensagem recebida  $y$  é ou não uma palavra-código, utiliza-se a matriz de verificação de paridade  $H = (P^t | I_{n-k})$ , a saber, se  $H \cdot y^t = 0$  então  $y$  é uma palavra-código.

O código de Hamming é amplamente utilizado para controle de erros em comunicação digital e armazenamento de dados e apresenta muitas aplicações nas telecomunicações. Diante disso, destacamos alguns trabalhos desenvolvidos, os quais permitem vislumbrar esse amplo leque de utilização do código de Hamming nas mais diversas áreas. Iniciamos com destaque do trabalho desenvolvido em [4], que apresenta uma implementação alternativa de Códigos Corretores de Erros para Sistemas de Comunicações Ópticas de 400 Gbps no qual utiliza o código de Hamming duplamente estendido com algoritmo DEPT (Direct Error-Pattern Testing) para decodificação.

Como os circuitos eletrônicos estão cada vez mais suscetíveis ao ruído, em [5] foram combinados os usos de dois códigos, a saber, o código Reed-Solomon e o código de Hamming, com o objetivo de proteger as memórias SRAM, Static Random Access Memory contra falhas múltiplas.

Além disso, destacamos o estudo realizado por Robson Bonetti em [6] onde código de Hamming foi empregado para reproduzir o modelo de crescimento de um tumor cancerígeno através de um autômato celular, mais especificamente, foi estudado a evolução temporal da distância de Hamming para o caso de células tumorais. Em seguida, foram apresentadas as características em relação à evolução temporal, e assim, a avaliação da supressão de células cancerígenas.

Por fim, neste trabalho foi apresentado o código de Hamming, que apesar de ser um código simples, possui uma vasta gama de aplicações nas mais diversas áreas. Richard Hamming tornou possível a criação de um código que fosse capaz de detectar e corrigir de forma simples, e a partir das aplicações destacadas, vislumbramos como a evolução tecnológica e com um mundo cada vez mais conectado, a busca por códigos corretores de erros mais eficientes continua atual.

## Agradecimentos

Agradecemos a UTFPR-PR e à Fundação Araucária, pelo apoio financeiro.

## Referências

- [1] C. E. Shannon. “A mathematical theory of communication”. Em: **The Bell system technical journal** 27.3 (1948), pp. 379–423.
- [2] S. Lin e D. J. Costello. **Error control coding: Fundamentals and Applications**. Prentice hall Lebanon, IN, 1983.
- [3] E. R. Nicoletti. “Aplicações de álgebra linear aos códigos corretos de erros e ao ensino médio”. Dissertação de mestrado. UNESP, 2015.
- [4] L. A. Borges Junior. **Implementação Alternativa de Códigos Corretores de Erros para Sistemas de Comunicações Ópticas de 400 Gbps : Código de Hamming Duplamente Estendido com Algoritmo DEPT para Decodificação**. Trabalho de Graduação em Engenharia Eletrônica e de Telecomunicações. UNESP. 2022.
- [5] Reis.R Neuberger.G Lima.F. **Projeto de uma Memória SRAM Tolerante a Múltiplas Falhas**. Online. Acessado em 11/03/2023, [https://www.researchgate.net/profile/Ricardo-Reis-5/publication/228579386\\_Projeto\\_de\\_uma\\_Memoria\\_SRAM\\_Tolerante\\_a\\_Multiplas\\_Falhas/links/0046351740aee46224000000/Projeto-d](https://www.researchgate.net/profile/Ricardo-Reis-5/publication/228579386_Projeto_de_uma_Memoria_SRAM_Tolerante_a_Multiplas_Falhas/links/0046351740aee46224000000/Projeto-d).
- [6] R. C. Bonetti et al. “Evolução Temporal da Distância de Hamming para o Caso de Células Tumorais”. Em: **Conferência Brasileira de Dinâmica, Controle e Aplicações**. Vol. 1. único. SBMAC. 2011, pp. 767–769.