Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 7, n. 1, 2020.

Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Codificação e Decodificação de Códigos Lineares[1]

Fabiana Aucco Egidio[2]
Departamento de Matemática, UNESP, Ilha Solteira, SP
Bruna Neves Machado[3]
Departamento de Matemática, UNESP, Ilha Solteira, SP
Edson Donizete de Carvalho[4]
Departamento de Matemática, UNESP, Ilha Solteira, SP

1 Resumo

Uma das principais preocupações em projetos de transmissão de dados de grande porte é garantir o controle de erros, de tal forma que a mensagem possa ser recuperada. Se na transmissão tiver m erros, como detectar e corrigir estes padrões de erros para recuperar a mensagem original enviada? É neste enfoque que consideramos a Teoria de Códigos [1].

Neste trabalho, focaremos nos códigos lineares binários C, isto é, quando C é dado por um subespaço vetorial de $\mathbb{F}_2^n$, onde $\mathbb{F}_2$ é um corpo binário.

Neste sentido, consideremos $\{v_1, \cdots, v_k\}$ de $\mathbb{F}_2^k$ um conjunto linearmente independente de vetores e a transformação linear $T : \mathbb{F}_2^k \to \mathbb{F}_2^n$, com $n < k$ dada por $T(x) = x_1v_1 + \cdots + x_kv_k$. Tomando $Im(T) = C$, temos $T(\mathbb{F}_2^k) = C$, e, obtendo assim, um código de dimensão k. Podemos ver $\mathbb{F}_2^k$ como o código de fonte, C como o código de canal, já a codificação é dada via a transformação linear T.

Quando um receptor recebe um elemento $v \in \mathbb{F}_2^n$, para sabermos se v é uma palavra código de C, precisa resolver o sistema de n equações nas k incógnitas $x_1, \cdots, x_k$ dado por: $x_1v_1 + x_2v_2 + \cdots + x_kv_k = v$.

Caso a cardinalidade de k e n seja alta, teremos um custo computacional elevado. Para contornarmos essa dificuldade, faremos uma abordagem matricial.

Consideremos o subespaço vetorial $C^\perp$ complementar de C em $\mathbb{F}_2^n$. Podemos escrever $\mathbb{F}_2^n = C \otimes C^\perp$. A partir da base $\{v_1, \cdots, v_n\}$ de C, consideremos a mesma transformação linear anterior $T : \mathbb{F}_2^k \to \mathbb{F}_2^n$ dada por $T(x) = xG$, onde

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}$$

[1] versão 1.2.

[2] fabiana.egidio30@hotmail.com
[3] bruna.neves28.bn@gmail.com
[4] edson.donizete@unesp.br

e é chamada de matriz geradora do código C.

Se a matriz G do código C for da forma $G = (Id_k|A)$, onde Id_k é a matriz identidade $k \times k$ e A, uma matriz $k \times (n-k)$, diremos que G está na forma padrão. Caso contrário, através de operações elementares sobre as linhas de G, obtem-se uma matriz equivalente a uma na forma padrão.

Agora, seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos, então que $v \in C \Leftrightarrow Hv^t = 0$.

Isso nos permite caracterizar os elementos de um código C por uma condição de anulamento. A matriz geradora H de $C^{\perp}$ é chamada *matriz teste de paridade* de C. Isto é, basta verificar se o vetor Hv^t é nulo [2].

Exemplo: Seja dado o código C sobre $\mathbb{F}_2$ com matriz geradora

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

Como G está na forma padrão, é fácil calcular uma matriz teste de paridade H, pois $H = (-A^t|Id_{n-k})$, então

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

Dados $v = (100111)$ e $v' = (010101)$, como

$$Hv^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

e

$$H(v')^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \neq 0,$$

temos que $v \in C$ e $v' \notin C$.

2 Agradecimentos

À FAPESP, pelo apoio financeiro, nº 2018/18433-4.

Referências

[1] A. Hefez e M. L. T. Vilela. *Códigos Corretores de Erros*. Rio de Janeiro: Ed. IMPA, 2002.

[2] C. C. Lavor. *Uma introdução à teoria de códigos*. Notas em Matemática Aplicada. São Carlos, SP: Ed. SBMAC, 2006.

