A PERSPECTIVA DOS BINÁRIOS NA TEORIA DE CÓDIGOS LINEARES

Lucas Machado Fernandes[1], *Maria José Sousa Vital Amaral*[2] & *Paulo César Cavalcante de Oliveira*[3]

Resumo

Não é segredo que a matemática é essencial para o nosso cotidiano e que fazemos uso de instrumentos que necessitam desta ciência mesmo sem estarmos utilizando-a diretamente. Em especial, quando uma mensagem é transmitida através de um canal, no whatsapp, como por exemplo, ela está propensa a sofrer alguma interferência, isto é, ser recebida com algum erro. Neste aspecto, a detecção e correção desses erros é um dos principais objetivos da Teoria de Códigos. Portanto, direcionaremos nossa produção científica, com embasamento teórico da álgebra, para a aplicação dos códigos binários no estudo dos códigos lineares.

Palavras-Chave: *Códigos, Interferência, Correção e Detecção.*

THE BINARY PERSPECTIVE IN THE LINEAR CODE THEORY

Abstract

It is no secret that mathematics is essential to our daily lives and that we make use of instruments that need this science even without using it directly. In particular, when a message is transmitted through a channel, in whatsapp, for example, it is prone to interference, that is, to be received with some error. In this aspect, the detection and correction of these errors is one of the main objectives of the Code Theory. Therefore, we will direct our scientific production, based on theoretical algebra, for the application of binary codes in the study of linear codes.

Keyword: *Codes, Interference, Correction and Detection.*

[1]Matemática/URCA - Bolsista PIBIC/URCA, e-mail: lucasmachadofernandes2@gmail.com
[2]Matemática/URCA - Bolsista PIBIC/URCA, e-mail: mariasousavitalamaral@gmail.com
[3]Matemática/URCA, e-mail: paulocesar.oliveira@urca.br

1 Introdução

A comunicação é um dos grandes pilares que move o mundo contemporâneo de tal forma que, o problema no envio de dados pode acarretar catástrofes para o desenvolvimento das atividades humanas, desde a falta de energia elétrica na sua casa, até o envio de uma mensagem no seu whatsapp. Refletir sobre o que há por trás desses envios de dados é um estímulo para estudarmos os códigos corretores de erros.

A teoria dos códigos corretores de erros nasceu em 1948 com a publicação de um trabalho elaborado por C. E. Shannon, e assim passou a ser estudada e desenvolvida por matemáticos da época.

A partir da década de 70, houve um grande interesse por parte de engenheiros em auxiliar no aperfeiçoamento da teoria de códigos. Devido ao avanço das pesquisas espaciais e a difusão dos computadores. É importante ressaltar que os primeiros computadores eram restritos às grandes instituições, além dos operadores não terem total liberdade de acesso a essas máquinas. Podemos citar o Laboratório Bell de Tecnologia, onde Richard W. Hamming e C. E. Shannon trabalhavam. Atualmente, os códigos corretores são utilizados sempre que se deseja transmitir dados com confiabilidade.

A teoria estudada tem, por finalidade, acrescentar novas informações que serão transmitidas fazendo com que estas possam ser corrigidas quando ocorrem erros de transmissão de dados. Precisamente ao transmitir uma mensagem por um dispotivo, ela será codificada através de dois processos. Inicialmente, a mensagem será transformada em um sinal no codificador da fonte e depois recodificada no codificador de canal para amenizar as redundâncias introduzidas. Após feito isso, o código será transmitido por um canal, seja ele digital ou não, tal que será decodificado e remodelado para chegar até o usuário. Esquematizaremos o processo abaixo.

$$\boxed{\text{Fonte}} \rightarrow \boxed{\text{Codificador da Fonte}} \rightarrow \boxed{\text{Codificador de Canal}}$$

$$\downarrow \text{Canal}$$

$$\boxed{\text{Decodificador de Canal}} \rightarrow \boxed{\text{Decodificador da Fonte}} \rightarrow \boxed{\text{Usuário}}$$

Neste trabalho, estudaremos os códigos lineares, enfatizando os códigos binários, sendo estes um dos tipos de códigos corretores de erros mais simples. A princípio, abordaremos a distância de Hamming, assunto de fundamental importância para o desenvolvimento desta teoria, que por sua vez determinarão os parâmetros dos códigos lineares, as matrizes geradoras, os códigos duais e os algoritmos de correções de erros. Por fim, apresentamos uma aplicação sobre a teoria estudada.

2 Objetivos

Em linhas gerais, apresentaremos os aspectos primordiais para a construção dos códigos lineares, mesclando as definições da Álgebra Linear com as aplicações da vida real da nossa socidade.

Especificamente, apresentamos um pouco da teoria que envolve os códigos, aos quais possibilitarão a compreensão dos algoritmos necessários para detecção e correção de erros na transmissão de mensagens.

3 Preliminares

3.1 Distância de Hamming

O primeiro passo para construir um código corretor de erros, é definir um conjunto finito A denominado alfabeto e sua respectiva cardinalidade $|A| = q$.

O código corretor de erros é um subconjunto próprio de A^n, para algum $n \in \mathbb{N}$, de tal forma que esse espaço é formado pelas n-uplas com entradas em A^n, ou seja,

$$A^n = (x_1\ x_2\ ...\ x_n)$$

tal que $x_i \in A$, com $i = 1, 2, ..., n$.

Sendo A um alfabeto, definimos C um código de comprimento n quando ele é um subconjunto próprio de A^n. Os elementos de um código são chamados de *palavras-código*.

Veremos abaixo uma aplicação cotidiana que reflete as definições anteriores:

Exemplo 1. *Dado o "alfabeto" A formado pelas 23 letras do alfabeto da língua portuguesa, bem como o espaço em branco como uma letra, o c cedilha e as vogais acentuadas, uma palavra da língua portuguesa pode ser considerada como um elemento de A^{27}, onde 27 é o comprimento da palavra mais longa do idioma.*

Definição 1. *Sejam $u = (u_1\ u_2\ ...\ u_n)$ e $v = (v_1\ v_2\ ...\ v_n)$ pertencentes a A^n. A distância de Hamming entre u e v é definida por*

$$d(u, v) = |\{i;\ u_i \neq v_i,\ com\ 1 \leq i \leq n\}|.$$

Teorema 1. *A distância de Hamming é uma métrica no espaço A^n, isto é, dados $u, v, w \in A^n$ valem as propriedades:*

1. *$d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$;*
2. *$d(u, v) = d(v, u)$;*
3. *$d(u, v) \leq d(u, w) + d(w, v)$.*

Agora, apresentaremos os conceitos de Disco e Esfera, além de um resultado importantíssimo para o estudo de códigos:

Definição 2. *Dados $a \in A^n$ e $t > 0$ um número real, define-se Disco e Esfera de centro a e raio t como*

$$D[a, t] = \{c \in A^n; d(c, a) \leq t\} \quad e \quad S(a, t) = \{c \in A^n; d(c, a) = t\},$$

respectivamente.

Lema 2. *Para todo $a \in A^n$ e todo número natural $r > 0$, temos que*

$$|D[a, r]| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Demonstração: Ver [3, Lema 11.21]. ∎

Inicialmente, definiremos a distância mínima d.

Definição 3. *Seja C um código. A distância mínima de C é o número*

$$d = min\{d(u, v);\ u, v \in C\ e\ u \neq v\}.$$

Dado um código C com distância mínima d, definiremos o raio dos discos como

$$\kappa = \left[\frac{d-1}{2}\right],$$

onde $[t]$ representa a parte inteira de um número real t. É importante salientar que um código C pode corrigir κ erros e detectar $d-1$ erros.

Definição 4. *Seja $C \subset A^n$ um código com distância mínima d, e seja $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se $\bigcup_{a \in C} D[a, \kappa] = A^n$.*

Repare que quanto maior a distância mínima, melhor é o código. De fato, a distância mínima é diretamente proporcional ao tamanho do raio κ. Logo, quanto maior o raio, maior a probabilidade da palavra pertencer à algum disco em torno de uma palavra c e ser decodificada com boa margem de segurança.

3.2 Códigos Lineares

Seja K um corpo finito com q elementos tomado como alfabeto. Temos, para cada número $n \in \mathbb{N}$ um K-espaço vetorial K^n de dimensão n. Assim, temos que

Definição 5. *Um código $C \subset K^n$ será chamado de código linear se for um subespaço vetorial de K^n.*

Dessa forma, sendo C um código que admite uma base finita $B = \{v_1, v_2, ..., v_k\}$, então sua dimensão é igual ao número de elementos de tal base. Em outras palavras, $dim_K C = k$.

Tendo em vista que cada elemento de C se escreve de maneira única como combinação linear de elementos de B, isto é,

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_k v_k,$$

ao qual $\lambda_i \in K$, com $i = 1, 2, ..., k$, segue-se que $|C| = q^k$.

Definição 6. *O peso de um código linear C é o inteiro $\omega(C) := \min\{\omega(x); x \in C \setminus \{0\}\}$, onde $\omega(x) = d(x, 0)$.*

Proposição 3. *Seja $C \subset K^n$ um código linear com distância mínima d. Temos que:*

1. *Para todo $x, y \in K^n$, $d(x, y) = \omega(x - y)$;*
2. *$d = \omega(C)$.*

Demonstração:

1. Dados $x, y \in K^n$, temos que $d(x, y) = |\{i; x_i \neq y_i, 1 \leq i \leq n\}| = |\{i; x_i - y_i \neq 0, 1 \leq i \leq n\}| = \omega(x - y)$.
2. Dados $x, y \in C$, com $x \neq y$, tem-se $z = x - y \in C \setminus \{0\}$ de modo que $d(x, y) = \omega(x - y) = \omega(z)$. Assim, $d = min\{d(x, y); x, y \in C \ \ e \ \ x \neq y\} = min\{\omega(z); z \in C \setminus \{0\}\} = \omega(C)$.

■

3.3 Matriz Geradora de um Código

Considere K o corpo finito com q elementos e $C \subset K^n$ um código linear. Chamaremos a terna (n, k, d) de parâmetros do código linear C, onde n é a dimensão do espaço K^n, k é a dimensão de C sobre K e d é a distância mínima do código.

Definição 7. *A matriz G é dita geradora de um código C associada à uma base β, quando cada linha dessa matriz representa um vetor dessa base. Em outras palavras, sendo $\beta = \{v_1, v_2, ..., v_k\}$ uma base de C e $v_i = \{v_{i1}, v_{i2}, ..., v_{in}\}$, com $i = 1, 2, ..., k$, tem-se*

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

Sendo a transformação linear,

$$\begin{array}{rccc} T: & K^k & \to & K^n \\ & x & \mapsto & xG \end{array}$$

e tomando $x = (x_1, x_2, ..., x_k)$, temos

$$T(x) = xG = (x_1\ x_2\ ...\ x_k) \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix} = x_1v_1 + ... + x_kv_k.$$

Logo, $T(K^k) = C$. Podemos então considerar K^k sendo o código da fonte, C o código do canal e T uma codificação.

É importante destacar que a matriz geradora não é unicamente determinada por C, pois ela depende da base β escolhida. Sendo assim, podemos encontrar várias matrizes geradoras atráves de uma outra com o uso de uma sequência de operações com suas linhas. Além disso, para construir códigos a partir de G basta tomar uma matriz com linhas linearmente independentes e definir um código C sendo imagem da transformação linear T acima.

Definição 8. *Diremos que uma matriz geradora G de um código C está na forma padrão se tivermos $G = (Id_k|A)$, onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n - k)$.*

3.4 Códigos Duais

Sendo $C \subset K^n$ um código linear, chamaremos de ortogonal a C ao conjunto

$$C^\perp = \{v \in K^n; \langle v, u\rangle = 0, \forall \in C\}.$$

com as operações usuais de produto interno.

Lema 4. *Se $C \subset K^n$ é um código linear, com matriz geradora G, então*

1. *$C^\perp$ é um subespaço vetorial de K^n;*
2. *$x \in C^\perp \iff Gx^t = 0$.*

Demonstração: Ver [1, Lema 1 - Seção 5.3]. ∎

Dessa forma, definimos o principal o conceito desta seção:

Definição 9. *O subespaço vetorial $C^{\perp}$ de K^n, ortogonal a C, é chamado código dual de C.*

Proposição 5. *Seja $C \subset K^n$ um código com dimensão k, com matriz geradora $G = (Id_k|A)$, na forma padrão. Então,*

1. *dim $C^{\perp} = n - k$;*
2. *$H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.*

Demonstração:

1. Pelo Lema 4, $x = (x_1 \ ... \ x_n)$ pertence a $C^{\perp}$ se, e somente se, $Gx^t = 0$. Como G está na forma padrão, isto equivale a termos

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}.$$

   Portanto, $C^{\perp}$ possui q^{n-k} elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1}, ..., x_n$. Logo, $C^{\perp}$ tem dimensão $n - k$.

2. É evidente que as linhas de H são linearmente independentes por causa do bloco Id_{n-k}, portanto, geram um subespaço de dimensão $n - k$. Como as linhas de H são ortogonais às linhas de G, temos que o espaço gerado pelas linhas de H está contido em $C^{\perp}$; E como esses dois subespaços têm mesma dimensão, eles coincidem, provando assim que $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

■

Definição 10. *A matriz geradora H de $C^{\perp}$ é chamada matriz teste de paridade de C.*

Proposição 6. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é maior do que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração: Ver [1, Proposição 5 - Seção 5.3]. ■

Teorema 7. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: De fato, suponhamos que $w(C) = s$, logo, todo o conjunto de $s - 1$ colunas de H é linearmente independente. Por outro lado, existem s colunas de H linearmente dependentes, pois caso contrário, pela Proposição 6, teríamos $w(C) \geq s + 1$. Reciprocamente, suponhamos que todo conjunto de $s-1$ vetores colunas de H é linearmente independente e existem s colunas linearmente dependentes. Logo, da Proposição 6, temos que $w(C) \geq s$. Mas, $w(C)$ não pode ser maior que s, pois, neste caso, novamente a proposição anterior nos diria que todo conjunto com s colunas de H é linearmente independente, o que é um absurdo. ■

Corolário 8. *Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

$$d \leq n - k + 1.$$

Demonstração: Se H é uma matriz teste de paridade, ela tem posto $n - k$. Como, pelo Teorema 7, $d - 1$ é menor ou igual ao posto de H, segue a desigualdade. ■

3.5 Decodificação

Sabendo que processo de detecção e correção de erros num determinado código chama-se decodificação, iniciaremos com a definição de vetor erro e como sendo a diferença entre o vetor recebido r e o vetor transmitido c, isto é,

$$e = r - c,$$

onde o peso $\omega(e)$ corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.

Definição 11. *Dados um código C com matriz teste de paridade H e um vetor $v \in K^n$, chamamos o vetor Hv^t de síndrome de v.*

Seja H a matriz teste de paridade de C, isto é, H é a matriz geradora de $C^{\perp}$. Como $c \in C$ segue-se que $Hc^t = 0$. Com efeito, temos

$$He^t = H(r^t - c^t) = Hr^t - Hc^t = Hr^t,$$

afirmando que a palavra recebida e o vetor erro e tem mesma síndrome.

Agora, denotaremos por h^i a i-ésima coluna de H. Se $e = (\alpha_1, ..., \alpha_n)$, então é fácil ver que

$$\sum_{i=0}^{n} \alpha_i h^i = \alpha_1 h^1 + \cdots + \alpha_n h^n = (h^1 \ \cdots \ h^n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = He^t = Hr^t.$$

Lema 9. *Seja C um código linear em K^n com capacidade de correção κ. Se $r \in K^n$ e $c \in C$ são tais que $d(c, r) \leq \kappa$, então existe um único vetor e com $w(e) \leq \kappa$, cuja síndrome é igual à síndrome de r e tal que $c = r - e$.*

Demonstração: Dados $r, c \in C$, com $r \neq c$, tem-se

$$e = r - c \in C \setminus \{0\}$$

e $d(r, c) = d(c, r) = w(e) \leq \kappa$. Para provar a unicidade, suponhamos

$$e = (\alpha_1 \cdots \alpha_n) \ \ e \ \ e' = (\alpha'_1 \cdots \alpha'_n)$$

tais que $w(e), w(e') \leq \kappa$, além de terem a mesma síndrome que r. Então, se H é uma matriz teste de paridade de C, temos

$$He^t = He'^t \Rightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha'_i h^i,$$

o que nos dá uma relação linear entre 2κ colunas ($\leq d - 1$) colunas de H são linearmente independentes, temos que $\alpha_i = \alpha'_i$ para todo i, logo $e = e'$. ∎

Exemplificaremos abaixo, um problema essencial para a determinação do algoritmo de decodificação para códigos corretores de um erro.

Seja C um código com matriz teste de paridade H com distância mínima $d \geq 3$ e peso $w(C) \leq 1$. Daí, sendo r e c as palavras recebidas e transmitidas, respectivamente, temos:
Se $He^t = 0$, então $Hr^t = 0$. Logo, $r \in C$ e se toma $c = r$;
Se $He^t \neq 0$, então $Hr^t \neq 0$. Logo, $r \notin C$. Daí, $w(e) = 1$ e, consequentemente,

$$e = (0 \ \cdots \ \alpha \ \cdots \ 0),$$

com $\alpha \neq 0$ na i-ésima coordenada. Assim,

$$He^t = (h^1 \ \cdots \ h^i \ \cdots \ h^n) \cdot \begin{pmatrix} 0 \\ \vdots \\ \alpha \\ \vdots \\ 0 \end{pmatrix} = \alpha h^i,$$

podemos determinar e como sendo o vetor com todas as componentes nulas exceto a i-ésima componente que é α. Note que i é bem determinado, pois $d \geq 3$.

Estabelecemos então, o algoritmo de decodificação em códigos corretores de um erro:

Algoritmo

Seja H a matriz teste de paridade do código C, e seja r um vetor recebido. Supondo $d \geq 3$, façamos:

(a) - Calcule Hr^t;
(b) - Se $Hr^t = 0$, aceite r como sendo a palavra transmitida;
(c) - Se $Hr^t = s^t \neq 0$, compare s^t com as colunas de H;
(d) - Se existirem i e α tais que $s^t = \alpha h^i$, para $\alpha \in K$, então e é a n-upla com α na posição i e zeros nas outras posições. Corrija r pondo $c = r - e$;
(e) - Se o contrário de (d) ocorrer, então mais de um erro foi cometido.

Cada conjunto $v + C$ é chamado de classe lateral de v segundo C, definido por

$$v + C = \{v + c; \ c \in C\}.$$

Definição 12. *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

Proposição 10. *Seja C um código linear em K^n com distância mínima d. Se $u \in K^n$ é tal que*

$$w(u) \leq \left[\frac{d-1}{2}\right] = \kappa,$$

então u é o único elemento líder de sua classe.

Demonstração: Suponhamos $u, v \in K^n$ tais que $w(u), w(v) \leq \left[\frac{d-1}{2}\right]$. Se $u - v \in C$, então

$$w(u-v) = d(u,v) \leq d(u,0) + d(v,0) = w(u) + w(v) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] \leq d - 1.$$

Como $w(u - v) \geq d$, então $u - v = 0$ e assim $u = v$. ∎

Dessa forma, sejam as palavras r, c e e. Como $He^t = Hr^t$, então a classe lateral onde e encontra-se é determinada pela síndrome de r. Supondo $w(e) \leq \kappa$, temos e sendo o único líder de sua classe e, consequentemente, pelo Lema 9, $c = r - e = r - l$ é determinado.

Algoritmo

(i) - Determine todos os elementos $u \in K^n$ que satisfaçam $w(u) \leq \kappa$;
(ii) - Calcule a síndrome $Hr^t = s^t$;
(iii) - Se s está na tabela, seja l o elemento líder da classe determinada por s e troque r por $r - l$;
(iv) - Se s não está na tabela, então na mensagem recebida foram cometidos mais do que κ erros.

4 Resultados

Após a exposição da teoria de códigos lineares, apresentaremos uma aplicação que contemple todos os resultados descritos anteriormente. Basicamente, utilizaremos o código binário sobre o corpo de Galois, $\mathbb{F}_2$, munido das operações:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Seja a matriz abaixo geradora de um código binário C dada por

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

A partir das informações anteriores, temos que a dimensão de K sobre C é $k = 4$, o comprimento é $n = 7$ e a cardinalidade $|C| = 2^4 = 16$, já que $q = 2$.

Desse modo, apresentaremos abaixo todos os elementos do código C utilizando a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^4 & \to & \mathbb{F}_2^7 \\ & (x_1, x_2, x_3, x_4) & \mapsto & x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4 \end{array}$$

onde $\{v_1, v_2, v_3, v_4\}$ é uma base de C com $i = 1, ..., 4$ sendo as linhas da matriz geradora. Assim,

x	xH	$d(xH, 0)$
0000	0000000	00
1000	1110000	03
0100	1001100	03
0010	1000011	03
0001	0101010	03
1100	0111100	04
0110	0001111	04
0011	1101001	04
1001	1011010	04
1010	0110011	04
0101	1100110	04
1110	1111111	07
0111	0100101	03
1101	0010110	03
1011	0011001	03
1111	0010101	03

Como temos $w(C) = 3$, segue-se

$$k = \left[\frac{3-1}{2}\right] = 1$$

e, consequentemente, para $c \in C$, a cardinalidade do disco é

$$|D[c,1]| = \sum_{i=0}^{1} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i = 1 + n.$$

O comprimento do corpo é 7. Daí,

$$\left| \bigcup_{c \in C} D[c,1] \right| = [1+7] \cdot 2^4 = 9 \cdot 2^4 = 2^3 \cdot 2^4 = |\mathbb{F}_2^7|.$$

Portanto, o código é perfeito.

Inicialmente, transformaremos G na forma padrão $(Id_4|A)$. Fazendo o escalonamento nas linhas de G encontramos a matriz,

$$\left(\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right).$$

Pela Proposição 5, a matriz teste paridade é da forma $H = (-A^t|Id_3)$. Assim,

$$H = \left(\begin{array}{ccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right).$$

É perceptível que o comprimento de C é 7. Logo, é de fácil análise que

$$dim\ C^{\perp} = n - k = 7 - 4 = 3.$$

Acharemos o vetor erro da mensagem $r = (1101101)$, admitindo que apenas um erro foi cometido. Pelo algoritmo, calculemos

$$Hr^t = \left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right) = 1 \cdot h^5.$$

Assim, $e = (0000100)$, e assim, $c = (1101001)$.

Por último, considerando $(7,4)-$código linear definido sobre $\mathbb{F}_2$. Pelo Lema 9, consideremos os vetores de peso ≤ 1, pois $\kappa = \left[\dfrac{3-1}{2} \right] = 1$.

Dessa forma, relacionaremos os vetores com as suas respectivas síndromes na tabela abaixo

Líder	Síndrome
0000000	000
1000000	011
0100000	101
0010000	110
0001000	111
0000100	100
0000010	010
0000001	001

Supondo que as palavras recebidas sejam $r_1 = (1110111)$ e $r_2 = (0001110)$. Logo,

$$Hr_1^t = (1\ 1\ 1)^t \quad e \quad Hr_2^t = (0\ 0\ 1)^t.$$

Portanto, $e_1 = (0001000)$ e $e_2 = (0000001)$ e, consequentemente, $c_1 = (1111111)$ e $c_2 = (0001111)$, respectivamente.

Referências

[1] Hefez, A. e Villela, M.L.V., Códigos Corretores de Erros, IMPA, 2008.

[2] Nogueira, J. A. P., Códigos Corretores de Erro, Monografia de Graduação - URCA, Juazeiro do Norte, 2017.

[3] Shokranian, S., Exemplos de Álgebra Linear sobre Corpos: Corpos Finitos, vol. 1, Ed. Ciência Moderna, Rio de Janeiro, 2015.