PRINCÍPIOS TEÓRICOS DOS CÓDIGOS CORRETORES DE ERROS: CÓDIGOS LINEARES E CÍCLICOS*

TAUAN DE SOUSA BARBOSA, **ALINE MOTA DE MESQUITA ASSIS**

Resumo: *este artigo é resultado de uma pesquisa bibliográfica e tem por objetivo apresentar os fundamentos matemáticos de caráter algébrico que envolve a Teoria dos Códigos Corretores de Erros, especificamente, os Códigos Lineares e os Códigos Cíclicos. Este assunto, além de ser bastante interessante, constitui-se uma junção dos conceitos e técnicas importantes da Álgebra Abstrata com aplicações imediatas na vida real.*

Palavras-chave: *Códigos Lineares. Códigos Cíclicos. Codificação. Decodificação.*

Atualmente, os Códigos Corretores de Erros são utilizados para transmitir ou armazenar informações de modo confiável. O seu uso ocorre quando são identificados erros durante uma transmissão, causados por alguma interferência no canal utilizado, fazendo com que o receptor não consiga identificar a mensagem original que lhe foi enviada, ou então, quando não for possível recuperar uma informação armazenada em fitas, disquetes magnéticos, entre outros meios de armazenamento de dados. Tal ferramenta está presente, também, em comunicações via satélite, comunicações internas de um computador, navegações pela internet e ao assistir um programa de televisão.

Essa teoria teve início com o surgimento dos primeiros computadores. Estes, por sua vez, eram utilizados somente por pesquisadores em instituições de grande porte, como universidades e centros de pesquisas. Uma das instituições que possuía tais computadores era o Laboratório Bell de Tecnologia e Richard Wesley Hamming foi um dos pesquisadores que utilizou esses equipamentos.

No ano de 1947 Hamming, durante suas pesquisas aos finais de semana, utilizava os computadores do laboratório para fazer a leitura de informações gravadas em cartões perfurados. Entretanto, no momento da leitura dos cartões ocorriam erros, os quais atrasavam o seu trabalho. A partir desse problema, Hamming obteve um código corretor de erros capaz de detectar até dois erros e corrigir um. Este trabalho foi publicado no ano de 1950 em um artigo intitulado *"Error Detecting and Error Correcting Codes"*.

Da data de descoberta desse tipo de código até a publicação do artigo, Hamming, em memorandos internos publicados no Laboratório Bell, questionava a obtenção de códigos mais eficientes. Essa questão foi respondida indiretamente no ano de 1948 pelo pesquisador Claude Elwood Shannon num artigo intitulado *"A Mathematical Theory of communication"*, dando início a dois novos campos de pesquisa: a Teoria dos Códigos e a Teoria da Informação.

Nos anos iniciais, a maioria dos interessados na Teoria de Códigos Corretores Erros eram os matemáticos que desenvolveram, nas décadas de 50 e 60, muitos conceitos acerca do assunto. Após os anos 60, ocorreu um grande avanço nos estudos e aplicações dos códigos devido ao desenvolvimento das pesquisas espaciais.

Um exemplo que ilustra a utilização dos códigos corretores de erros e os seus princípios é o chamado *código do robô*. Suponhamos então que um robô foi enviado a Marte e para se deslocar nas direções norte, sul, leste e oeste utiliza-se a seguinte codificação:

$$\begin{array}{ll} \text{Leste} \rightarrow (1,0) & \text{Oeste} \rightarrow (1,1) \\ \text{Norte} \rightarrow (0,0) & \text{Sul} \rightarrow (0,1) \end{array}$$

Cada direção é associada a um único elemento do produto cartesiano $\{0,1\}\times\{0,1\}$, denominado *código da fonte*, que no contexto dos códigos também pode ser chamado de *palavra*. Logo, caso seja necessário que o robô vá para o norte será lhe enviado um comando com o código (0,0). Agora, suponhamos que cada código é transmitido via rádio e por alguma interferência durante a transmissão do comando (0,1) o robô receba o código de fonte (1,0), o que faria com que ele fosse para o leste e não para o sul. Logo, é necessária fazer a correção do erro. Contudo, como cada código da fonte utilizado se assemelha em termos de componentes, fica difícil identificar qual foi a mensagem original enviada ao robô e, assim, não é possível corrigir o erro. Dessa forma, é feito uma recodificação do código da fonte de tal maneira que possa ser identificado o erro, caso ele ocorra. Por exemplo:

$$\begin{array}{ll} (0,0) \rightarrow (0,0,0,0,0) & (0,1) \rightarrow (0,1,0,1,1) \\ (1,0) \rightarrow (1,0,1,1,0) & (1,1) \rightarrow (1,1,1,0,1). \end{array}$$

Cada recodificção é denominada código de canal. Agoa, se for enviado a mensagem (1,0,1,1,0) e por alguma interferência no canal de transmissão for recebida a palavra (1,1,1,1,0), será feito uma comparação entre a palavra erroneamente recebida e todas

as outras palavras do código de canal, de modo a procurar qual seassemelha ao código (1,1,1,1,0) em termos de componentes de cada vetor. Assim, observa-se que a palavra que é mais próxima de (1,1,1,1,0), ou seja, aquela que possui menor número de componentes diferentes é justamente a palavra (1,0,1,1,0), logo a correção do erro é possível.

Com o exemplo exposto acima é possível afirmar que a Teoria de Códigos Corretores de Erros consiste em: transformar o código da fonte em código de canal, detectar e corrigir erros na recepção de uma mensagem e decodificar o código de canal em código da fonte. A Figura 1 descreve o procedimento para a transmissão de uma mensagem de modo seguro.

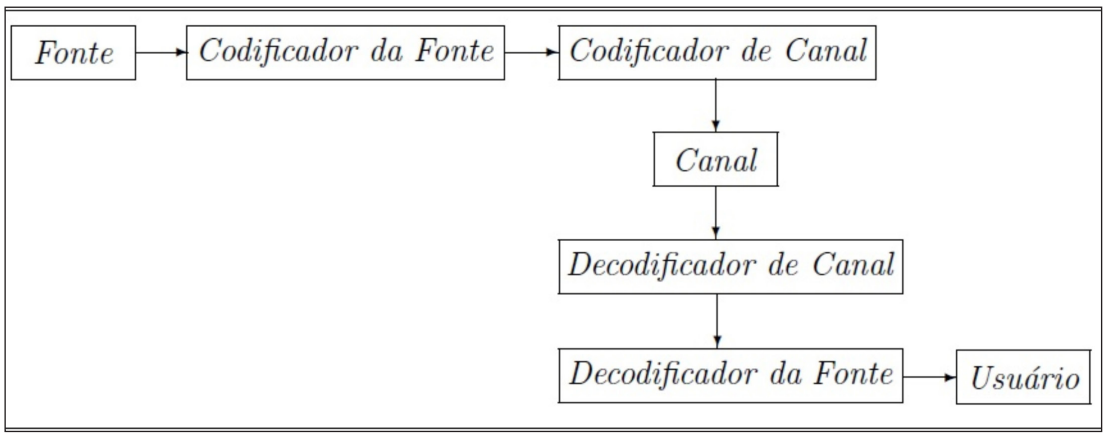

Figura 1: Procedimento para transmissão de uma mensagem

Consideraremos neste artigo canais de transmissão que possuem as seguintes propriedades:

i) Todos os símbolos transmitidos têm a mesma probabilidade (pequena) de serem recebidos errados.

ii) Se um símbolo é recebido errado, a probabilidade de ser qualquer um dos outros é a mesma.

Os canais que satisfazem as duas propriedades acima são chamados de *canais simétricos.*

Apresentaremos neste artigo duas classes de Códigos Corretores de Erros. A primeira é a dos Códigos Lineares e a segunda é a classe dos Códigos Cíclicos. O intuito é mostrar os conceitos de Álgebra Linear e Álgebra Abstrata presentes nesses dois tipos de códigos, bem como exibir o principal problema existente até os dias de hoje: a determinação da *distância mínima.*

CONSTRUÇÃO DE UM CÓDIGO CORRETOR DE ERROS

Para a construção de um código corretor de erros é necessário um conjunto finito A, com q elementos, *chamado de alfabeto*.

Um código corretor de erros é um subconjunto próprio qualquer de A^n, para algum número $n \in \mathbb{N}$. Notemos que o conjunto A^n possui elementos do tipo

$(a_1, a_2, \ldots, a_n)$ que serão substituídos pela notação $a_1 a_2 \ldots a_n$.

Para tornar mais preciso a noção de proximidade entre palavras, definimos a seguir a maneira de medir distâncias entre elementos de A^n chamada de *distância de Hamming*.

Definição 1. Dados dois elementos $u, v \in A^n$, a *distância de Hamming* entre u e v é definida como:

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

Por exemplo, considerando as palavras 100 e 110 do conjunto $\{0,1\}^3$ temos, pela distância de Hamming, que $d(100, 110) = 1$, pois comparando as palavras observa-se que a segunda entrada de cada uma delas se diferem. Da mesma forma, observamos que:

$$d(000, 111) = 3 \quad \text{e} \quad d(001, 111) = 2.$$

UM PROBLEMA SUTIL DA TEORIA DE CÓDIGOS CORRETORES DE ERROS

Dentre as distâncias de Hamming, podemos estabelecer a menor delas denominada de *distância mínima,* e que está descrita na Definição 2.

Definição 2. Seja C um código. A *distância mínima* de C é o número

$$d = min \{ d(u, v) : u, v \quad C \text{ e } u \neq v \}.$$

Observe que a distância mínima no exemplo do código do robô é $d = 3$.

O problema de calcular a distância mínima é a quantidade de vezes que deverá ser feita tal operação. Por exemplo, se q é a quantidade de elementos de um código, seria necessário calcular a combinação simples C_2^q o que teria um grande custo computacional caso a quantidade q fosse suficientemente grande.

Um resultado muito importante que cuja demonstração se encontra em Hefez e Villela (2002, p. 6), é que um código C com distância mínima d pode corrigir até $K = \left[\frac{d-1}{2}\right]$ erros, onde [t] é a parte inteira de um número real t, e detectar até $d - 1$ erros. Esse resultado facilitaria a correção e a detecção de erros, porém, como na maioria das vezes não é possível determinar a distância mínima, ela torna-se de difícil utilização. Note que, a partir dessa afirmação, pode-se concluir que um código terá maior capacidade de correção de erros quanto maior for a distância mínima d, pois se d for suficientemente grande, o número será aumentado consideravelmente. Portanto, é fundamental poder calcular d ou pelo menos determinar uma cota inferior.

Podemos concluir então, que a obtenção da distância mínima é de suma importância para os códigos corretores de erros, se consagrando como um grande desafio para os pesquisadores na atualidade.

CÓDIGOS LINEARES

Para construção dos códigos lineares consideraremos um corpo finito K com q elementos, denominado de alfabeto. Naturalmente, para cada número natural n, temos um K - espaço vetorial K^n de dimensão n. A Definição 3 nos diz quando um código $C \subset K^n$ é um *código linear.*

Definição 3. Um código $C \subset K^n$ será chamado de *código linear* se for um subespaço vetorial de K^n.

Concluímos a partir dessa definição que um código linear é um espaço vetorial de dimensão finita. Então, sendo k a dimensão de um código linear e $v_1, v_2, \ldots, v_k$ uma de suas bases, todo elemento de C se escreve de modo único na forma $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$, onde os λ_i, $i = 1, \ldots, k$, são elementos de K. Além disso, como para cada λ_i existem q possibilidades, segue que o número de elementos de C é q^k.

Definição 4. Dado $x \in K^n$, define-se o *peso* de x como sendo o número inteiro

$$\omega(x) := |\{ i : x_i \neq 0 \}|.$$

Em outras palavras, temos que $\omega(x) = d(x, 0)$, onde d representa a métrica de Hamming.

Definição 5. O *peso de um código* linear C é o inteiro

$$\omega(C) := \min \{ \omega(x) : x \in C - \{0\} \}.$$

Proposição 1. Seja $C \subset K^n$ um código linear com distância mínima d. Temos que:

i) $\forall\, x, y \in K^n$, $d(x, y) = \omega(x - y)$.
ii) $d = \omega(C)$
Demonstração: O item (i) segue imediatamente das definições de métrica de Hamming e de peso de um código. O item (ii) decorre do fato que, para todo par de elementos x, $y \in C$ com $x \neq y$, tem-se $z = x - y \in C - \{0\}$ e $d(x, y) = \omega(z)$.

A Proposição 1 nos mostra que em códigos lineares com q elementos pode-se obter a distância mínima a partir de $q - 1$ cálculos de distâncias, em vez de C_2^q, o que torna a quantidade de cálculos da primeira menor que a da segunda forma. Entretanto, ainda é inviável fazer essa quantidade de cálculos.

Em virtude da Proposição 1(ii), a distância mínima de um código linear C será também chamada de peso do código C.

Em Álgebra Linear existem dois modos de se descrever subespaços vetoriais C

de um espaço vetorial K^n: uma delas é como imagem e outra como núcleo de transformações lineares. Em códigos do tipo linear consideraremos a descrição como imagem de uma transformaçã ¨near injetora. Como um código C para ser linear tem que ser subespaço vetorial de K^n, será suficiente obter C como imagem da transformação linear

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

em que x = $(x_1, x_2,\ldots, x_k)$ e $u = x_1u_1 + x_2u_2 + \ldots + x_ku_k$. Assim, um código C de dimensão k pode ser dado como a imagem da transformação T, isto é, $Im(T) = C$.

Tendo em mente a transformação linear explicitada acima podemos obter uma matriz denominada *matriz geradora* de um código linear. Para isso, seja $\beta = \{v_1, v_2,\ldots, v_k\}$ uma base de C e considere a matriz G de tal modo que cada uma de suas linhas sejam os vetores $v_i = (v_{i1}, v_{i2},\ldots, v_{ik})$, com i = 1,…, k. Ou seja:

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

A matriz G é chamada de *matriz geradora* de C e se $x = (x_1, x_2,\ldots, x_k)$ temos que $T(x) = xG = x_1v_1 + x_2v_2 + \ldots + x_kv_k$. Logo $T(K^k) = C$. Dessa forma, podemos considerar T como sendo a codificação, K^k o código da fonte e C o código de canal.

A cada matriz geradora G de um código linear C podemos associar uma matriz na forma padrão. A matriz G está na forma padrão se $G = (Id_k \mid A)$, em que Id_k é a matriz identidade $k \times k$ e A é uma matriz de ordem $k \times (n - k)$.

Definimos agora o conjunto $C^\perp = \{ v \in K^n : \langle v, u\rangle = 0, \forall u \in C \}$, onde C é um código linear e $\langle v, u\rangle$ é o produto interno de $v, u \in K^n$. Esse conjunto será muito importante na construção de um algoritmo para saber se uma mensagem recebida é ou não uma palavra de C, pois até o momento só exibimos como obter os elementos de um código linear C.

Proposição 2. Se $C \subset K^n$ é um código linear, com matriz geradora G, então $C^\perp$ é um subespaço vetorial de K^n e $x \in C^\perp$ se, e somente se, $Gx^t = 0$.

Demonstração: Para verificar a primeira parte basta aplicar a definição de subespaço vetorial. Agora, provemos a segunda parte: $x \in C^\perp$ se, e somente se, x é ortogonal a todos os elementos de C se, e somente se, x é ortogonal a todos os elementos de uma base de C, o que é equivalente a dizer que $Gx^t = 0$, pois as linhas de G são uma base de C.

O subespaço vetorial $C^\perp$ de K^n, ortogonal a C, é chamado de *código dual* de C. Como $C^\perp$ é também um código linear, podemos obter uma matriz geradora H que é exibida na Proposição 3.

Proposição 3. Seja $C \subset K^n$ um código linear de dimensão k com matriz $G = (Id_k \mid A)$ na forma padrão. Então
i) dim $C^{\perp} = n - k$

ii) $H = (-A^t \mid Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Demonstração: i) Pela Proposição 2, $x = (x_1, x_2, \ldots, x_n)$ pertence a $C^{\perp}$ se, e somente se, $Gx^t = 0$. Como G está na forma padrão, isso equivale a ter

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

Portanto, $C^{\perp}$ possui q^{n-k} elementos, que são justamente as possíveis escolhas arbitrárias de $x_{k+1},\ldots, x_n$. Logo, $C^{\perp}$ tem dimensão $n - k$.
ii) É evidente que as linhas de H são linearmente independentes (devido ao bloco Id_{n-k}), portanto, geram um subespaço vetorial 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 a mesma dimensão, eles coincidem, provando assim que $H = (-A^t \mid Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

A matriz H é dita a *matriz teste paridade* de C. Ela é quem determina se uma dada palavra pertence ou não ao código C. Por exemplo, se uma dada palavra v pertencer ao código C então o produto da matriz H pela transposta de v é igual à zero, isto é, $Hv^t = 0$, em que a vetor Hv^t é denominado de *síndrome* de v.

DECODIFICAÇÃO DE CÓDIGOS LINEARES

Decodificar é um procedimento muito importante no processo de transmissão ou armazenamento de uma informação. Esse processo permite detectar e corrigir erros em um determinado código. Inicialmente, definimos o vetor erro e como sendo a diferença entre o vetor recebido r e o vetor transmitido c, isto é, $e = r - c$. Por exemplo, se a palavra transmitida foi 010011 e a palavra recebida foi 101011 então o vetor erro é $e = 101011 - 010011 = 111000$. Note que, definido o vetor erro temos que seu peso corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção.
Agora, seja H a matriz teste de paridade do código linear C. Como $Hc^t = 0$ temos que $He^t = H(r^t - c^t) = Hr^t - Hc^t = Hr^t$. Portanto, a palavra recebida e o vetor erro tem a mesma síndrome.

O nosso objetivo nesse momento é determinar um algoritmo para decodificação em códigos lineares. No que segue, denotaremos por h^i a i – ésima coluna de H. Logo, se $e = (\alpha_1,\ldots, \alpha_n)$ temos que:

$$\sum_{i=1}^{n} \alpha_i h^i = He^t = Hr^t$$

Essa notação nos ajudará demonstrar a Proposição 4.

Proposição 4. Seja C um código linear em K^n com capacidade de correção k. Se $r \in K^n$ e $c \in C$ são tais que $d(c, r) \leq \kappa$, então existe um único vetor e com $\omega(e) \leq \kappa$, cuja síndrome é igual à síndrome de r e tal que $c = r - e$.

Demonstração: De fato, $e = r - c$ tem a propriedade da proposição, já que $\omega(e) = d(c, r) \leq \kappa$. Para provar a unicidade, suponhamos que $e = (\alpha_1, \ldots, \alpha_n)$ e $e' = (\alpha_1', \ldots, \alpha_n')$ sejam tais que $\omega\omega(e) \leq \kappa$ e $\omega(e') \leq \kappa$ e tenha mesma síndrome de r. Então, se H é a matriz teste de paridade de C, temos $He^t = H(e')^t$, ou seja,

$$\Sigma_{i=1}^{n} \alpha_i h^i = \Sigma_{i=1}^{n} \alpha_i' h^i$$

o que nos dá uma relação de dependência linear entre $2\kappa\ (\leq d - 1)$ colunas de H. Como quaisquer $d - 1$ linhas de H são linearmente independentes, vide Hefez e Villela (2002, p. 92), temos que $\alpha_i = \alpha_i'$, para todo i, logo $e = e'$.

Levando em consideração a Proposição 4, podemos estabelecer um algoritmo de decodificação em códigos corretores de erros. Essa decodificação deve seguir os seguintes passos:

Seja H a matriz teste de paridade do código C e seja r um vetor recebido. (Suponha $d \geq 3$.)
(i) Calcule Hr^t.
(ii) Se $Hr^t = 0$, aceite r como sendo a palavra transmitida.
(iii) Se $Hr^t = s^t \neq 0$, compare s^t com as colunas de H.
(iv) 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 $c = r - e$.
(v) Se o contrário de (iv) ocorrer, então mais de um erro foi cometido.

Esse processo de decodificação só poderá ser utilizado somente quando ocorrer um único erro na transmissão. No caso em que ocorre mais de um erro na mensagem enviada, o processo se difere do citado acima e pode ser encontrado em Hefez e Villela (2002, p. 103).

CÓDIGOS CÍCLICOS

Os códigos cíclicos são uma classe dos códigos lineares que possui bons algoritmos de codificação e decodificação. Toda a teoria dessa classe é desenvolvida sobre um corpo finito K e representaremos as coordenadas de K^n por

$(x_0, x_1,\ldots, x_{n-1})$. No que segue, definimos quando um código linear é um código cíclico.

Definição 6. Um código linear $C \subset K^n$ será chamado de código cíclico se, para $c = (c_0, c_1,\ldots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0,\ldots, c_{n-2})$ pertence a C.

A construção dos códigos cíclicos consiste em enriquecer a estrutura de espaço vetorial de K^n através de novas estruturas matemáticas. Primeiramente, para fazer esse enriquecimento é definido R_n como sendo o anel das classes residuais em $K[x]$ módulo $x^n - 1$.

O anel R_n munido da operação de multiplicação por escalar $\lambda\lambda \in K$ definida por $\lambda\overline{f(x)} = \overline{\lambda f(x)}$ é um K-espaço vetorial de dimensão n com base $\overline{1}$, $\overline{x}$, ..., $\overline{x^{n-1}}$. Além disso, o R_n é isomorfo a K^n através da transformação linear:

$$v : K^n \to R_n$$
$$(a_0, a_1,\ldots,a_{n-1}) \mapsto \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}$$

Temos, então, que todo código linear $C \subset K^n$ pode ser transportado para R_n mediante o isomorfismo *vv*. A vantagem da utilização dessa transformação linear é que sua imagem nos dá uma estrutura adicional de anel, chamada de *ideal*.

O *ideal* de um anel A é um subconjunto $I \subset A$, diferente do vazio, no qual são verificadas as condições:

i)$\forall\ a, b \in I, a + b \in I$
i) $\forall\ a \in I$ e $\forall\ c \in A, ca \in I.$

Definido a estrutura de um ideal, temos que o conjunto $I(a) = \{ ca : c \in A \}$ é um ideal de um anel A chamado de *ideal principal* gerado por $a \in A$. No caso dos códigos cíclicos será considerado o ideal $I(\overline{f(x)})$ gerado pelo resíduo $\overline{f(x)} \in R_n$. O Teorema a seguir mostra quem é a base de um ideal I gerado por um resíduo $\overline{g(x)}$.

Teorema 1. Seja $I = I(\overline{g(x)})$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $\overline{g(x)}$, $\overline{xg(x)}$, $\overline{x^2g(x)}$, ..., $x^{n-s-1}g(x)$ é uma base de I como espaço vetorial sobre K.
Demonstração: Basta provar que os elementos são linearmente independentes e geram I.

É possível encontrar a partir do Teorema 1 um elemento $u \in C$ onde todo elemento de C será obtido a partir de u. Tal resultado é mostrado no Corolário 1.

Corolário 1. Dado um código cíclico C, existe $u \in C$ tal que $C = \langle u \rangle$.

Demonstração: Seja $I = v(C)$. Logo, I é gerado como K – espaço vetorial por $\overline{g(x)}$, $\overline{xg(x)}$, $\overline{x^2g(x)}$,..., $\overline{x^{n-s-1}g(x)}$, onde g(x) é um divisor de $x^n - 1$. Dessa forma, colocando $u = v^{-1}(\overline{g(x)})$, temos que C é gerado por $u, T_\pi u, \ldots, T_\pi^{n-s-1} u$, sendo T_π a função permutação de coordenadas onde, através da bijeção $\pi : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$, definimos $T_\pi(a_1, a_2, \ldots, a_n) = (a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)})$. Portanto, $C = \langle u \rangle$.

Assim como nos códigos lineares, os códigos cíclicos também possuem matrizes geradoras G. A obtenção dessa matriz consiste em uma simples aplicação do Teorema 1:

$$G = \begin{pmatrix} v^{-1}(\overline{g(x)}) \\ v^{-1}(\overline{xg(x)}) \\ \vdots \\ v^{-1}(\overline{x^{n-s-1}g(x)}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_s \end{pmatrix}.$$

Observe que essa matriz geradora é constituída de modo que suas linhas sejam a imagem inversa de vv aplicado a cada elemento da base de $I = I(\overline{g(x)})$.

Podemos determinar nessa classe de códigos uma matriz geradora de C na forma padrão ($R \mid Id$). Para isso, seja

$$\begin{array}{rcl} \mu : K^s & \to & K[x]_{s-1} \subset K[x] \\ (a_0, \ldots, a_{s-1}) & \mapsto & \sum_{i=0}^{s-1} a_i x^i \end{array}.$$

Essa aplicação é um isomorfismo de K – espaços vetoriais, onde $K[x]_{s-1}$ é o espaço vetorial dos polinômios de grau menor ou igual a $s - 1$. Esse isomorfismo será de grande utilidade no que se segue.

Teorema 2. Seja $C \subset K^n$ um código cíclico. Suponhamos que C = $v^{-1}(I)$, onde $I = I(\overline{g(x)})$, com g(x) um divisor de $x^n - 1$. Seja R a matriz $(n - s) \times s$ cuja i – ésima linha é

$$R_i = -\mu^{-1}(r_i(x)), \quad \text{com } 1 \le i \le n - s,$$

onde $r_i(x)$ é o resto da divisão de x^{s-1+i} por g(x). Então, ($R \mid Id_{n-s}$) é a matriz geradora de C na forma padrão.

Demonstração: A demonstração desse resultado se encontra em Hefez e Villela (2002, p. 117).

No próximo parágrafo definimos o polinômio dito recíproco que será de grande utilidade para a obtenção da matriz teste de paridade.

Dado um polinômio $h(x) = h_0 + h_1 x + \cdots + h_t x^t$ que divide $x^n - 1$, o *polinômio recíproco* de h(x) é $h^*(x) = x^t h(1/x) = h_t + h_{t-1} x + \cdots + h_0 x^t$.

Podemos agora obter a matriz teste de paridade e mostrar que $C^{\perp}$ também é cíclico. Esse resultado está explicitado no Teorema 3.

Teorema 3. Seja $C = v^{-1}(I)$ um código cíclico, onde $I = I(\overline{g(x)})$, com g(x) um divisor de $x^n - 1$. Então $C^{\perp}$ é cíclico e $C^{\perp} = v^{-1}(J)$, onde $J = I(h^{*}(x))$.
Demonstração: A demonstração desse resultado se encontra em Hefez e Villela (2002, p. 114).

Corolário 2. A matriz teste de paridade de $C = v^{-1}(I)$, em que $I = I(\overline{g(x)})$, é dada por

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 \end{pmatrix},$$

onde

$$\frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_{n-s} x^{n-s}$$

Demonstração: A demonstração desse resultado se encontra em Hefez e Villela (2002, p. 115).

DECODIFICAÇÃO DE CÓDIGOS CÍCLICOS

Para a decodificação é necessário determinar a síndrome de um elemento v. Para tanto, o Teorema 4 nos mostra como obter esse resultado.

Teorema 4. Seja $C \subset K^n$ um código cíclico gerado por um polinômio mônico g(x) com matriz geradora na forma padrão ($R \mid Id$) e matriz teste de paridade $H = (Id \mid -R^t)$. Se v = $(v_0, \ldots, v_{n-1}) \in K^n$, então a síndrome de v com relação à matriz H é dada por
$\mu^{-1}(r(x))$, $\left(\mu^{-1}(1), \mu^{-1}(x), \ldots, \mu^{-1}\left(x^{s-1}\right), \mu^{-1}(r_1(x)), \ldots, \mu^{-1}\left(r_{n-s}(x)\right)\right)v^t$
onde $r(x)$ é o resto da divisão de $v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$ por g(x).

$$\mu^{-1}(v_0 + v_1 x + \cdots + v_{s-1} x^{s-1} + v_s r_1(x) + \cdots + v_{n-1} r_{n-s}(x))$$

Demonstração: A síndrome de v é o vetor

$$(Id \mid -R^t)v^t = \left(\mu^{-1}(1), \mu^{-1}(x), \ldots, \mu^{-1}\left(x^{s-1}\right), \mu^{-1}(r_1(x)), \ldots, \mu^{-1}\left(r_{n-s}(x)\right)\right)v^t$$

$$(Id \mid -R^t)v^t = , \ \mu^{-1}(v_0 + v_1 x + \cdots + v_{s-1} x^{s-1} + v_s r_1(x) + \cdots + v_{n-1} r_{n-s}(x))$$

o que implica o resultado, visto que

$$r(x) = v_0 + v_1 x + \cdots + v_{s-1} x^{s-1} + v_s r_1(x) + \cdots + v_{n-1} r_{n-s}(x)$$

é o resto da divisão de $v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ por g(x).

CONCLUSÃO

Foi apresentado neste artigo um estudo bibliográfico sobre os princípios teóricos dos códigos corretores de erros, com enfoque nas classes dos códigos lineares, especificando a classe dos códigos cíclicos. É notável que os conceitos de Álgebra Linear e Álgebra Abstrata estão bastante presentes em todos o processos que envolvem essa teoria.

Os conceitos aqui estudados possui intervenção direta na vida real. Assistir um filme em DVD ou escutar uma música em um CD são exemplos de aplicações dos códigos corretores de erros. Esses tipos de aplicações mostram que se torna cada vez mais difusa a fronteira entre a Matemática Pura e a Matemática Aplicada por meio da sofisticação tecnológica. Ficou evidente nesse artigo que a classe dos códigos cíclicos recebe uma estrutura matemática adicional muito importante, o que faz com que ela tenha uma maior utilização, pois possui um bom método de codificação e decodificação.

Podemos concluir que o grande desafio na atualidade é a determinação da distância mínima. Com esse problema resolvido, conseguiríamos um melhor processo de codificação e decodificação, o que melhoraria o processo de transmissão e armazenamento de dados, entretanto, atualmente, as pesquisas feitas só conseguiram estabelecer cotas mínimas para a distância mínima.

Em linhas gerais, é possível verificar que há muito a ser feito na teoria de códigos corretores de erros. Dessa forma, deve-se levar em consideração quais as ferramentas matemáticas que serão utilizadas para a obtenção de códigos mais eficientes e, além disso, saber se tal código é viável para a aplicação na vida real.

THEORETIC PRINCIPLES OF ERROR-CORRECTING CODES: LINEAR AND CYCLIC CODES

Abstract: *this article is the result of a literature review and aims to present the mathematical foundations of algebraic character which involves the Theory of Error-Correcting Codes, specifically, linear codes and cyclic codes. This subject, besides being quite interesting, it constitutes a junction of important concepts and techniques of Abstract Algebra with immediate applications in real life.*

Keywords: *Linear Codes. Cyclic Codes. Codification. Decodification.*

Referências

HEFEZ, Abramo; VILLELA, Maria Lúcia T. *Códigos Corretores de Erros*. Rio de Janeiro: IMPA, 2002.

MACWILLIAMS, Florence J; SLOANE, Neil A. J. *The Theory of Error-correcting Code.* Edição. North Holland: North-Holland Publishing Company, 1977.

LINT, Jacobus H. van. *Introduction to Coding Theory*. Netherlands: Springer, 1992.

LIDL, Rudolf; NIEDERREITER, Harald. *Introduction to finite fields and their applications.* New York: Cambridge University Press, 1988.

LIMA, Elon Lages. *Álgebra Linear.* Rio de Janeiro: IMPA, 2009.

Gonçalves, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1979.

GARCIA, Arnaldo; LEQUAIN, Yves. *Álgebra: um curso de introdução.* Rio de Janeiro: IMPA, 1988.

* Recebido em: 02.02.2014. Aprovado em: 22.02.2014. Agradecemos ao Núcleo de Estudos e Pesquisas em Educação Matemática do IFG (NEPEM/IFG) pelo apoio.

TAUAN DE SOUSA BARBOSA
Graduando em Licenciatura em Matemática no Instituto Federal de Ciência e Tecnologia de Goiás – Câmpus Goiânia. *E-mail*: tauansousa@hotmail.com

ALINE MOTA DE MESQUITA ASSIS
Mestre em Matemática. Professora do Instituto Federal de Ciência e Tecnologia de Goiás – Câmpus Goiânia. *E-mail*: aline.mesquita@ifg.edu.br