Revista de Divulgação Científica em
Ciências Exatas e Tecnológicas
PORANDU
Vol. 3, n. 1, 2019, pg. 9-16

Códigos Corretores de Erros

M. V. P. SPREAFICO[1,*] , W. R. ZUCARELLI[1,†] ,

[1] Universidade Federal de Mato Grosso do Sul, INMA, MS, Brasil,

Submetido em 22/09/2018; Aceito em 13/12/2018; Publicado em 06/09/2019

Resumo. Este artigo tem por principal objetivo apresentar os princípios teóricos de códigos corretores de erros, tema em que *C.E. Shannon* [1] é o pioneiro no estudo e forneceu uma descrição formal de um sistema de comunicação. Neste contexto, mostramos alguns tipos de canais (meio onde passa a informação) e métodos de codificação e decodificação em classes de códigos, além de alguns exemplos de códigos, bem como os fundamentos matemáticos algébricos que envolvem a Teoria da Informação.

Palavras-chave. Códigos Corretores de Erros, Álgebra, Teoria da Informação.

Abstract. The main goal of this work is to provide theoretical principles of the error-correcting codes, the main issue that *C.E. Shannon* [1] is the pioneer of the study and has a formal description of a communication system. In this context, we show some kinds of channels (medium where information is passed) and coding and decoding methods in code classes, besides some code examples, as well as the algebraic mathematical bases that involves the Information Theory.

1 Introdução

A comunicação de uma pessoa à outra é, obviamente, uma atividade tão antiga quanto a própria existência do homem. A Teoria (matemática) dos princípios adjacentes não é tão antiga quanto. Ela teve início em 1948, com a publicação do pioneiro e fundamental trabalho de *C.E. Shannon (1916 - 2001)* [1] intitulado *"A Mathematical Theory of Communication"*, o qual deu uma descrição formal de um sistema de comunicação, e ao mesmo tempo, também introduziu uma bela teoria sobre o conceito de informação, incluindo uma medida para a quantidade de informação em uma mensagem. Pelo feito, *Shannon* acabou ficando conhecido como *"o pai da teoria da informação"*. Em 1949, junto com o matemático *Warren Weaver (1894-1978)*, publicam o livro *"The Mathematical Theory of Communication"* [2], contendo reimpressões do artigo original de Shannon, mas de forma mais acessível, de modo que os conceitos se popularizaram.

*mvspreafico@gmail.com
†willianzuca@hotmail.com

Neste contexto, há sempre duas partes envolvidas na transmissão de informação, o *remetente* (quem transmite a mensagem) e o *destinatário* (quem recebe a mensagem). Em algumas aplicações, o *remetente* "escreve" a informação em um meio (como por exemplo, um "CD" ou dispositivos de memória flash) e o *destinatário* a "lerá" mais tarde. Em outras aplicações, o *destinatário* nem sempre obterá a mesma informação enviada pelo *remetente*, pois o meio nem sempre é perfeito ou está em perfeito estado. Erros em transmissão de informação estão quase sempre presentes, o problema a ser solucionado ocorre então em duas etapas: a detecção da existência do erro e a correção. Neste cenário, para aumentar a confiabilidade da comunicação, os dados a serem enviados podem ser convertidos em outra forma de informação, não necessariamente da mesma natureza, por um processo chamado *codificação* e então após a transmissão da informação, esta é tratada por um processo de *decodificação* para que o *destinatário* receba a mensagem original. A partir da *codificação* obtém-se o que é chamado de *código corretor de erros*, estrutura capaz de detectar e corrigir erros em um sistema de comunicação.

O objetivo neste trabalho é fornecer ao leitor conhecimentos básicos da Teoria de Códigos, área de pesquisa que reside na interseção da Ciência da Computação, Matemática, Física e Engenharia Elétrica, e que, de modo mais abrangente, possibilita a investigação sobre o campo da Teoria Matemática da Informação e áreas correlatas. Ao mesmo tempo, esse texto busca motivar e instigar uma reflexão posterior sobre o tema. Esse tema exige aprofundarnos o estudo de diversas estruturas algébricas, tais como espaços métricos, anéis de polinômios, corpos finitos e espaços vetoriais. Uma introdução básica à construção de códigos corretores de erros pode ser vista em [3]. Existem muitas referências na área, entre muitos textos recomendamos também, por exemplo, [4, 5, 6, 7, 8, 9]. En [10] podemos encontrar um artigo publicado na revista *Plus Magazine* e que explica, em suma, como se usaram os códigos corretores nas viagens espaciais.

2 Sobre a teoria

O meio pelo qual as informações são enviadas é chamada de *canal*, essas características consistem em um alfabeto de entrada X, um alfabeto de saída Y e uma função de probabilidade P. Nesse estudo estamos considerando que toda transmissão tem a mesma função de probabilidade e essas probabilidades serão independentes das transmissões anteriores e posteriores.

Com isso, definimos um *canal* como a terna $(X, Y; P)$, onde X é o alfabeto de entrada, Y é o alfabeto de saída, e para todo $x \in X$, $y \in Y$ a probabilidade condicional $P(y|x)$, de receber o bit y, dado que foi enviado o bit x.

Como exemplo, consideremos o *Canal Simétrico Binário (CBS)*, no qual $X = Y = \{0, 1\}$ e P é dado por $P(1|0) = P(0|1) = p$ e $P(0|0) = P(1|1) = 1 - p$, com $0 \leq p \leq 1$. Dessa forma, cada bit x tem probabilidade $1 - p$ de ser recebido corretamente e probabilidade p de ocorrer um erro durante a transmissão. Por esse motivo consideramos $0 \leq p \leq 1/2$.

Uma generalização direta é o *Canal Simétrico q-Ário*. Definido por $X = Y$,

com cardinalidade q, e probabilidade de transmissão $P(y|x) = 1 - p$, se $x = y$, e $P(y|x) = p/(q-1)$, se $x \neq y$.

Consideramos, por um momento, o *canal simétrico binário*, com probabilidade p de ocorrer um erro durante a transmissão, e definimos a capacidade do canal como sendo

$$C(p) = \log_2 2p^p(1-p)^{1-p}.$$

Com esses conceitos, *Shannon* conseguiu provar que se o tamanho da informação é menor do que a capacidade do canal, então existe um código capaz de transmitir essa informação com uma probabilidade de decodificação incorreta tão pequena quanto se queira. O problema é que a teoria de *Shannon* não nos fornece como conseguir os códigos na prática, com isso, foram, e ainda são criadas, técnicas de codificação.

Dado um conjunto finito A, de cardinalidade q, temos que um *código corretor de erros* é um subconjunto próprio $C \subset A^n$, para algum número natural n. Os elementos de A^n são chamados *palavras* e os elementos que estão em C *palavras-código*. Com objetivo de medir o erro ocorrido durante a transmissão de mensagens é introduzida uma métrica em A^n. A mais comum é a *métrica de Hamming* [11], definida como o número de coordenadas em que as palavras diferem, i.e.,

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

Estabelecida a noção de proximidade entre palavras, é conhecido que num *Canal q-ario simétrico*, a decodificação por máxima verossemelhança coincide com a decodificação por palavra mais próxima, ou seja, o resultado de se decodificar uma palavra recebida como a palavra-código mais provável é o mesmo que se decodificar pela palavra-código mais próxima. Assim, a partir desta consideração, faz-se necessário o estudo de propriedades métricas deste espaço, para se chegar em bons algoritmos de codificação e decodificação.

Dados um elemento $a \in A^n$ e um número real $t \geq 0$, definimos o *disco* e a *esfera* de centro a e raio t como sendo, respectivamente, os conjuntos

$$D(a,t) = \{u \in A^n : d(u,a) \leq t\},$$

$$S(a,t) = \{u \in A^n : d(u,a) = t\}.$$

Chamamos de *distância mínima* d do código, a menor das distâncias entre as palavras do código, isto é,

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

Com isso, conseguimos o resultado de que o decodificador consegue detectar até $d-1$ erros e corrigir até

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor$$

erros, onde $\lfloor h \rfloor$ é o maior inteiro menor do que h.

O código C será dito *perfeito* se

$$\bigcup_{c\in C}^{*} D(c,k) = A^n.$$

Uma das razões dessa nomenclatura, deve-se ao fato de que, se c e c' são palavras distintas de C, então

$$D(c,k) \cap D(c',k) = \emptyset,$$

ou seja, não há ambiguidades em até k erros.

O que não dá a garantia de que a palavra será decodificada corretamente, uma vez que ocorridos mais de k erros, a palavra recebida estará mais próxima de uma palavra-código diferente da enviada, essa classe de códigos apenas nos garante que não terá ambiguidade durante a decodificação das palavras.

O grande problema é que trabalhar com códigos usando apenas esses conceitos fará com que o custo computacional seja alto, e afim de contornar esse problema são introduzidas estruturas algébricas para construir códigos eficientes e com codificações e decodificações mais simples. A classe de códigos mais utilizada na prática é a chamada classe dos códigos lineares.

Assim, trataremos o alfabeto A como um corpo finito com q elementos, e o denotaremos por K. Teremos, portanto, para cada número natural n, um K-espaço vetorial K^n de dimensão n. Definindo, assim, o *código linear* $C \subset K^n$ de parâmetros $[n,k,d]$ como um subespaço vetorial de K^n, de dimensão k e menor distância entre palavras d.

De imediato a utilização de códigos lineares simplificam o custo computacional para obter a distância mínima do código. Com efeito, ao invés de calcular

$$\begin{pmatrix} |C| \\ 2 \end{pmatrix}$$

distâncias, podemos obter a menor das distâncias fazendo $|C|-1$ cálculos de distâncias, uma vez que, dados $x, y \in C$ então $x - y \in C$. Em outras palavras, ao invés de comparar as distâncias de todas as palavras do código, calculamos apenas a distância de cada palavra em C ao zero. Segue então que,

$$d(x,y) = d(x-y,0).$$

Sendo assim, o peso de um código linear é dado por

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

Outra propriedade útil, que segue do fato do código ser um subespaço vetorial de dimensão finita, é que o mesmo pode ser completamente descrito a partir de uma base ordenada finita. Supondo que $\beta = (v_1, v_2, \cdots, v_k)$ é uma base de C, construímos uma *matriz geradora* de C como a matriz cujas linhas são vetores da base β, isto é, se $v_i = (v_{i1}, v_{i2}, \cdots, v_{ik}), i = 1, \cdots, k$, temos

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

Com isso, podemos codificar uma palavra $x = (x_1, x_2, \cdots, x_k)$ a ser transmitida no canal, de maneira simples, por meio da transformação linear T cuja matriz é G, ou seja, $T(x) = xG$.

A fim de diminuir custos computacionais na codificação e decodificação, utilizamos para a construção do mesmo código C, uma matriz $G' = (Id_k|A)$, equivalente a G, obtida por operações elementares nas linhas de G, isto é,

$$G' = (Id_k|A) = \begin{pmatrix} 1 & 0 & \cdots & 0 & v_{1k+1} & \cdots & v_{1n} \\ 0 & 1 & \cdots & 0 & v_{2k+1} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & v_{kk+1} & \cdots & v_{kn} \end{pmatrix}.$$

Outra estrutura bastante útil, é a de subespaço ortogonal, que neste contexto, é chamado *código dual* de C. Seja $C \subset K^n$ um código linear, define-se *código dual* por

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

Dessa forma, temos o resultado de que $x \in C^{\perp}$ se, e somente se, $Gx^t = 0$. Note que, se tivermos a matriz geradora $G = (Id_k|A)$, na forma padrão, então $\dim C^{\perp} = n - k$, e $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Afim de verificar se uma palavra recebida pertence, ou não, ao código definimos *código dual* de C. Dado $C^{\perp} \subset K^n$ um *código dual* de C, a matriz geradora H de $C^{\perp}$ é chamada de *matriz teste de paridade* de C, utilizada para verificar se um determinado vetor v em K^n pertence ou não a um código C com matriz geradora G, é preciso verificar se o sistema de n equações com k incógnitas $x = (x_1, x_2, \cdots, x_k)$, dado por

$$xG = v$$

admite solução. Em geral, esse processo de decodificação requer um custo computacional elevado para ser respondida. No entanto, se decodificar utilizando uma matriz teste de paridade H, a solução pode ser encontrada bem mais rapidamente. Para tanto, é suficiente verificar se o vetor Hv^t é nulo, o que pode ser feito via circuito com baixo grau de complexidade.

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. Inicialmente, define-se o vetor erro e como sendo a diferença entre o vetor recebido r e o vetor transmitido c, isto é,

$$e = r - c.$$

Note que o peso do vetor erro corresponde ao número de erros cometidos numa palavra entre a transmissão e a recepção. Seja H a matriz teste de paridade do código. 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 têm a mesma síndrome.

Denotaremos por h^i a i-ésima coluna de H. Se $e = (\alpha_1 \cdots \alpha_n)$, então

$$\alpha_1 h^1 + \alpha_2 h^2 + \cdots + \alpha_n h^n = He^t = Hr^t.$$

O problema que se coloca então, é como determinar esse único vetor e a partir de Hr^t. Uma decodificação para quando $\omega(e) \leq 1$ e $d \geq 3$, ou seja, o canal introduziu no máximo um erro. Desse modo, se $He^t = 0$ temos que $r \in C$ e se toma $c = r$. Caso contrário, se $He^t \neq 0$, então $\omega(e) = 1$, e portanto, e tem apenas uma coordenada não nula. Nesse caso, consideremos que $e = (0, \cdots, \alpha, \cdots, 0)$ com $\alpha \neq 0$ na i-ésima posição. Logo,

$$He^t = \alpha h^i,$$

onde h^i é a i-ésima coluna de H. Portanto, não conhecendo e, mas conhecendo

$$He^t = Hr^t = \alpha h^i,$$

podemos determinar e como sendo o vetor com todas as coordenadas nulas exceto a i-ésima coordenada que é α.

Podemos sofisticar ainda mais a codificação e decodificação com uma outra classe de códigos lineares. Um código linear $C \subset K^n$ será chamado de *código cíclico* se, para todo $c = (c_0, c_1, \cdots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, \cdots, c_{n-2})$ pertence a C.

Em outras palavras, o código linear C será um *código cíclico* se, dada a permutação π de $\{0, \cdots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1, & \text{se } i > 1 \\ n-1, & \text{se } i = 1 \end{cases}$$

ou ainda,

$$\tau_\pi(c_0, c_1, \cdots, c_{n-1}) = (c_{n-1}, c_0, \cdots, c_{n-2}),$$

temos que $\tau_\pi(c) \in C$ para todo $c \in C$, ou seja, $\tau_\pi(C) \subset C$.

Defina R_n como sendo o anel das classes residuais em $K[X]$ módulo $X^n - 1$, isto é,

$$R_n = K[X]_{X^n - 1}.$$

Temos, então, um isomorfismo

$$\begin{array}{rccc} \upsilon: & K^n & \longrightarrow & R_n \\ & (a_0, \cdots, a_{n-1}) & \mapsto & [a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}]. \end{array}$$

onde nos dá a vantagem de adicionar a estrutura de anel, além de continuar com as estruturas de espaço vetorial. Então, temos que, um subespaço C de K^n é um *código cíclico* se, somente se, $\upsilon(C)$ é um ideal de R_n.

Portanto, $\upsilon(C) = [g(X)]$, onde $g(X) \in K[X]$ é um divisor de $X^n - 1$. Logo, se $\dim C = s$, então possui matriz geradora

$$G = \begin{pmatrix} \upsilon^{-1}([g(X)]) \\ \upsilon^{-1}([Xg(X)]) \\ \vdots \\ \upsilon^{-1}([X^{n-s-1}g(X)]) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & \cdots & \cdots & g_s \end{pmatrix}$$

No que se segue, $g(X)$ denotará sempre um divisor de $X^2 - 1$ e poremos

$$h(X) = \frac{X^n - 1}{g(X)}.$$

Note que, como $\mathrm{gr}(h(X)) = s$, temos que $\mathrm{gr}(h(X)) = n - s$, e portando, C possui matriz *teste de paridade*

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

3 Considerações Finais

Ao longo de mais de meia década da descoberta, inúmeras aplicações práticas foram descobertas usando a teoria de *Shannon*, desde missões interplanetárias como *Voyager*, *Galileo* ou *Cassini* [12], passando pelo entendimento de buracos negros [13], até o entendimento da consciência humana pela linguagem matemática [14].

O pioneiro trabalho de *C.E Shannon* [1] nos garante que é possível codificar e descodificar uma palavra com probabilidade de erro tão pequena quanto se queira, mas não nos fornece como conseguir os códigos na prática, e por isso, são estudadas, aprimoradas e criadas novas técnicas de codificação, buscando um alto nível de confiabilidade e um baixo custo computacional. No presente texto, tentamos elucidar os primeiros conceitos e vimos algumas técnicas que podemos utilizar neste contexto.

Referências

[1] C. E. SHANNON, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 7 1948.

[2] C. E. SHANNON and W. WEAVER, *The Mathematical Theory of Communication.* Urbana: University of Illinois Press IL, 1949.

[3] C. P. MILIES, "Breve Introdução à Teoria dos Códigos Corretores de Erros," *Colóquio de Matemática da Região Centro-Oeste, SBM*, 2009.

[4] A. HEFEZ and M. L. T. VILLELA, *Códigos Corretores de Erros.* IMPA, Rio de Janeiro, 2017.

[5] S. LING and C. XING, *Coding Theory: a First Course.* Cambridge University Press, 2004.

[6] J. BAYLIS, *Error-correcting Codes. A Mathematical Introduction.* Chapman & Hall Mathematics, 1998.

[7] J. H. VAN LINT, *Introduction to Coding Theory*. Springer Verlag, 1992.

[8] R. HILL, *A First Course in Coding Theory*. Oxford University Press, 1986.

[9] C. MUNUERA GOMEZ and J. G. TENA AYUSO, *Codificación de la Información*. Valladolid: Ed. Universidad de Valladolid, 1997.

[10] R. FINCH, "Coding Theory: the firts 50 years." `http://pass.maths.org.uk/issue3/codes`. Accessado em Jul. 2019.

[11] R. W. HAMMING, "Error Detecting and Errors Correcting Codes," *Bell System Tech. J.*, no. 29, 1950.

[12] W. GAPPMAIR, "Claude E. Shannon: the 50th anniversary of information theory," *IEEE Communications Magazine*, vol. 37, no. 4, pp. 379–423, 1999.

[13] S. GHOSH, "Black Hole Entropy: From Shannon to Bekenstein," *International Journal of Theoretical Physics*, vol. 50, no. 11, p. 3515, 2011.

[14] G. TONONI, "Integrated Information Theory of Consciousness: an updated account," *Archives Italiennes de Biologie*, no. 150, pp. 290–326, 2012.