
II W. A.
31 de março a 03 de abril de 2014
$G \times G \to G$
$(g,h) \mapsto g \cdot h$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
$g \cdot e = g = e \cdot g$
$\iota : G \to G$
$g \mapsto g^{-1}$
$g \cdot g^{-1} = e$

Códigos Corretores de Erros

Jorge Alencar
UNICAMP

Grasiele Jorge
UNIFESP

II Workshop de Álgebra da UFG-CAC

Catalão, Brasil 31 de Março até 03 de Abril, 2014

Um Pouco de História

- Teoria dos Códigos Corretores de Erros: matemática, computação, engenharia elétrica e estatistíca entre outras;
- Transmissão de dados e ruídos: interferências eletromagnéticas e erros humanos;
- Década de 40 e a exclusividade dos computadores;
- O Laboratório Bell de Tecnologia possuia tais computadores e Richard W. Hamming trabalhava com estas máquinas em 1947;
- Finais de semana e cartões perfurados.

Um Pouco de História

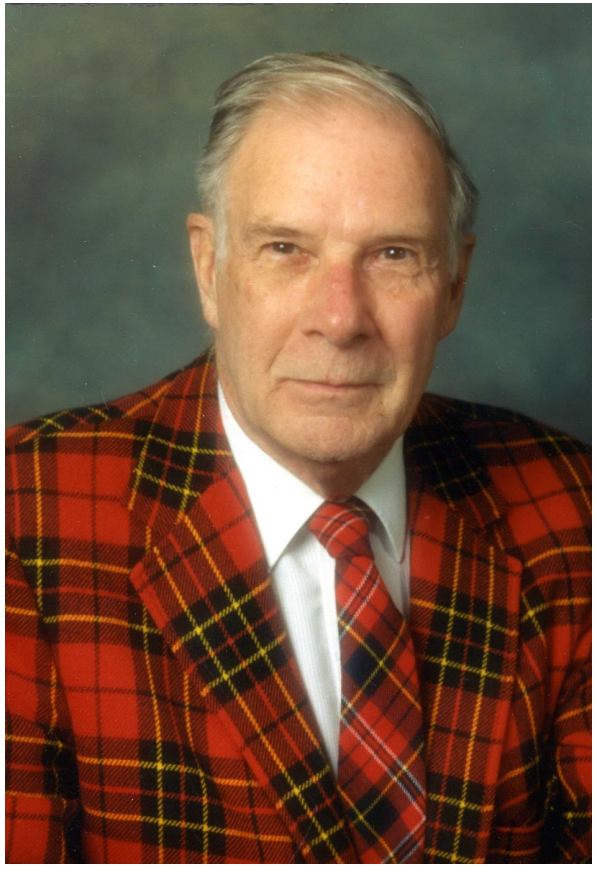


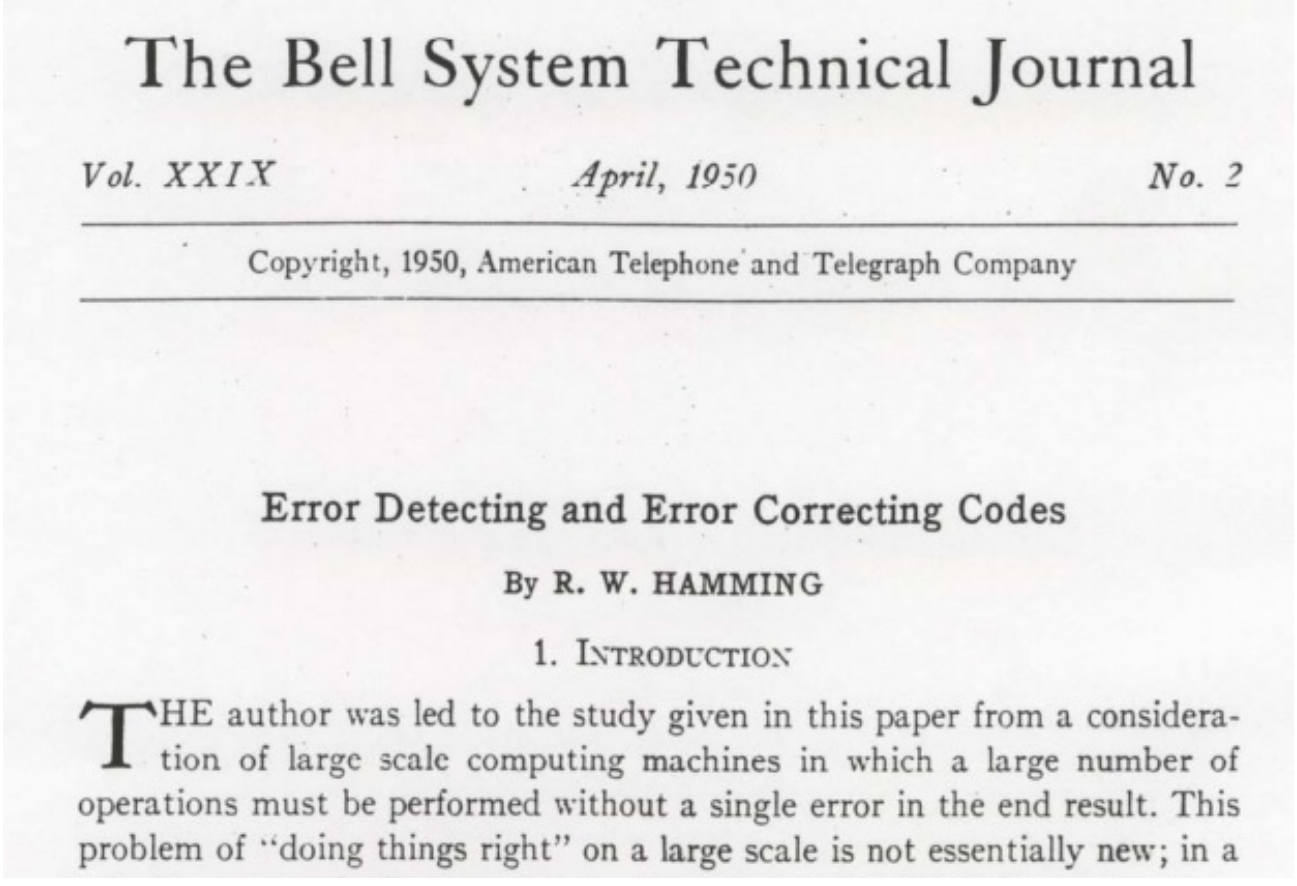
Figura : Richard W. Hamming

Um Pouco de História

Hamming relembra:

> *Em dois finais de semanas consecutivos eu fui e descobri que todas minhas coisas tinham sido descarregadas e nada tinha sido feito. Eu estava realmente aborrecido e irritado porque queria estas respostas e tinha perdido dois finais de semana. E então eu me disse "Maldição", se as máquinas podem detectar um erro, porque não podemos localizar a posição do erro e corrigi-lo.*
>
> *R.W. Hamming, Interview, Fevereiro de 1977*

Um Pouco de História



The Bell System Technical Journal

Vol. XXIX *April, 1950* *No. 2*

Error Detecting and Error Correcting Codes

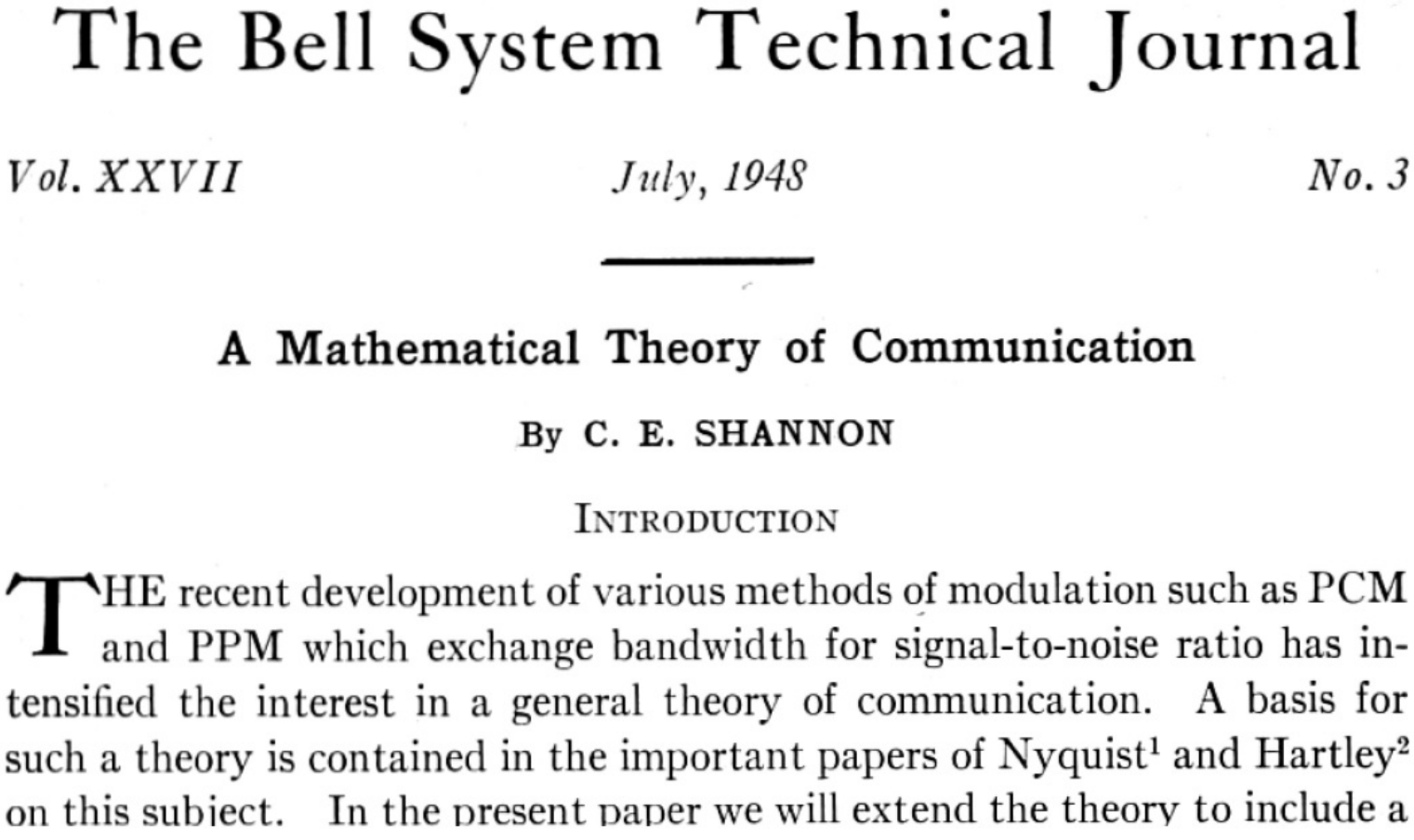
By R. W. HAMMING

1. INTRODUCTION

THE author was led to the study given in this paper from a consideration of large scale computing machines in which a large number of operations must be performed without a single error in the end result. This problem of "doing things right" on a large scale is not essentially new; in a

Figura : The Bell System Technical Journal, 1950.

Um Pouco de História



The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

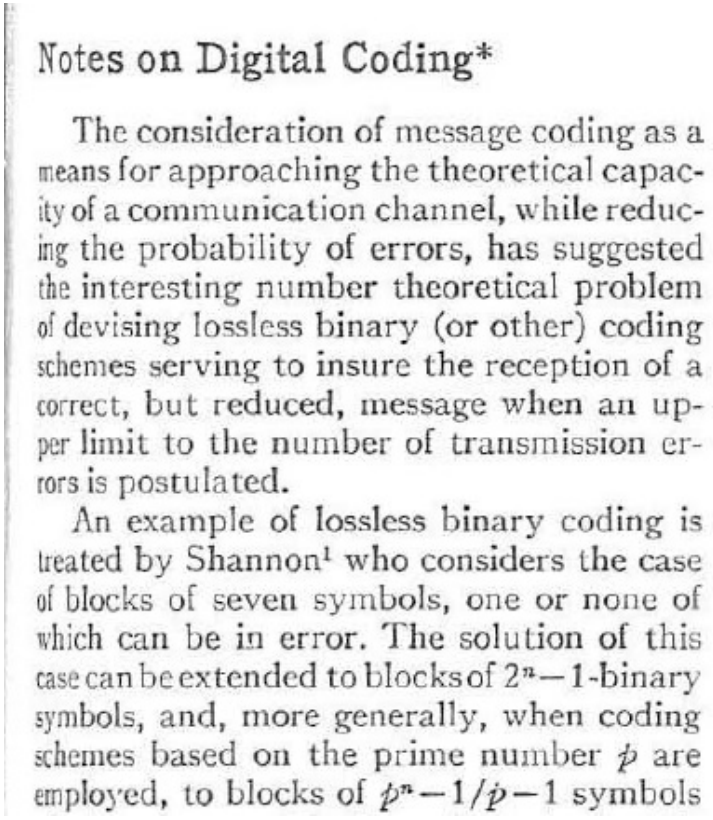
THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a

Figura : The Bell System Technical Journal, 1948.

O artigo de C. E. Shannon deu inicio a dois novos campos de pesquisa em matemática:

- A Teoria de Códigos (em conjunto com o trabalho de Hamming);
- A Teoria da Informação.

Um Pouco de História



Notes on Digital Coding*

The consideration of message coding as a means for approaching the theoretical capacity of a communication channel, while reducing the probability of errors, has suggested the interesting number theoretical problem of devising lossless binary (or other) coding schemes serving to insure the reception of a correct, but reduced, message when an upper limit to the number of transmission errors is postulated.

An example of lossless binary coding is treated by Shannon[1] who considers the case of blocks of seven symbols, one or none of which can be in error. The solution of this case can be extended to blocks of 2^n-1-binary symbols, and, more generally, when coding schemes based on the prime number p are employed, to blocks of $p^n-1/p-1$ symbols

Figura : Proceedings of the IRE (IEEE), 1949.

Um Pouco de História

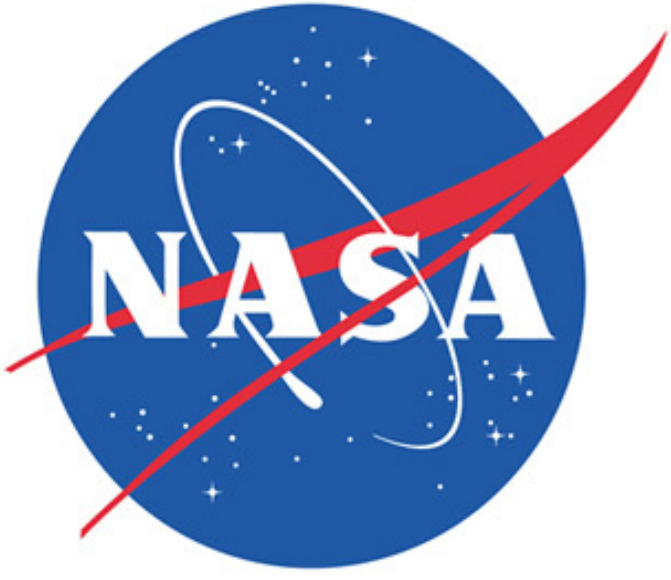
Figura : Espaçonave Voyager que usa um código desenvolvido por Golay para transmitir fotos coloridas de Júpiter e Saturno.

Um Pouco de História

Golay, Hamming e Shannon foram os grandes pioneiros e desenvolvedores de estudos e ideias que são usadas até hoje no nosso dia a dia:

- Comunicação Móvel (telefones celulares);
- Aparelhos de armazenamento de dados;
- Processamento de Imagens Digitais;
- Internet;
- Rádio.

Um Pouco de História



JPL

Jet Propulsion Laboratory

Conceitos Básicos

- Podemos dizer que a construção de códigos inspira-se no mais comum dos códigos utilizados pelos seres humanos: os idiomas;
- Na língua portuguesa temos:
  1. Um alfabeto de 26 letras;
  2. Palavras, que nada mais são que sequências finitas dessas letras.

Conceitos Básicos

Os elementos básicos para construção de um código são:

- Um conjunto finito, $\mathcal{A}$ que chamaremos de **alfabeto**. Se q é a quantidade de elementos de $\mathcal{A}$, dizemos que o código é q-ário;
- Sequências finitas de símbolos do alfabeto são **palavras**. O número de letras numa palavra é o seu **comprimento**.

Conceitos Básicos

Assim, um **código q-ário de comprimento** n será um subconjunto $\mathcal{C}$ de palavras de comprimento n, ou seja,

$$\mathcal{C} \subseteq \mathcal{A}^n.$$

Conceitos Básicos - Exemplo

Quanto o alfabeto utilizado é o conjunto $\mathbb{Z}_2 = \{0, 1\}$ o código diz-se binário. O conjunto

$$\mathcal{C}_1 = \{00000, 01011, 10110, 11101\}.$$

é um código em blocos, binário, de comprimento 5.

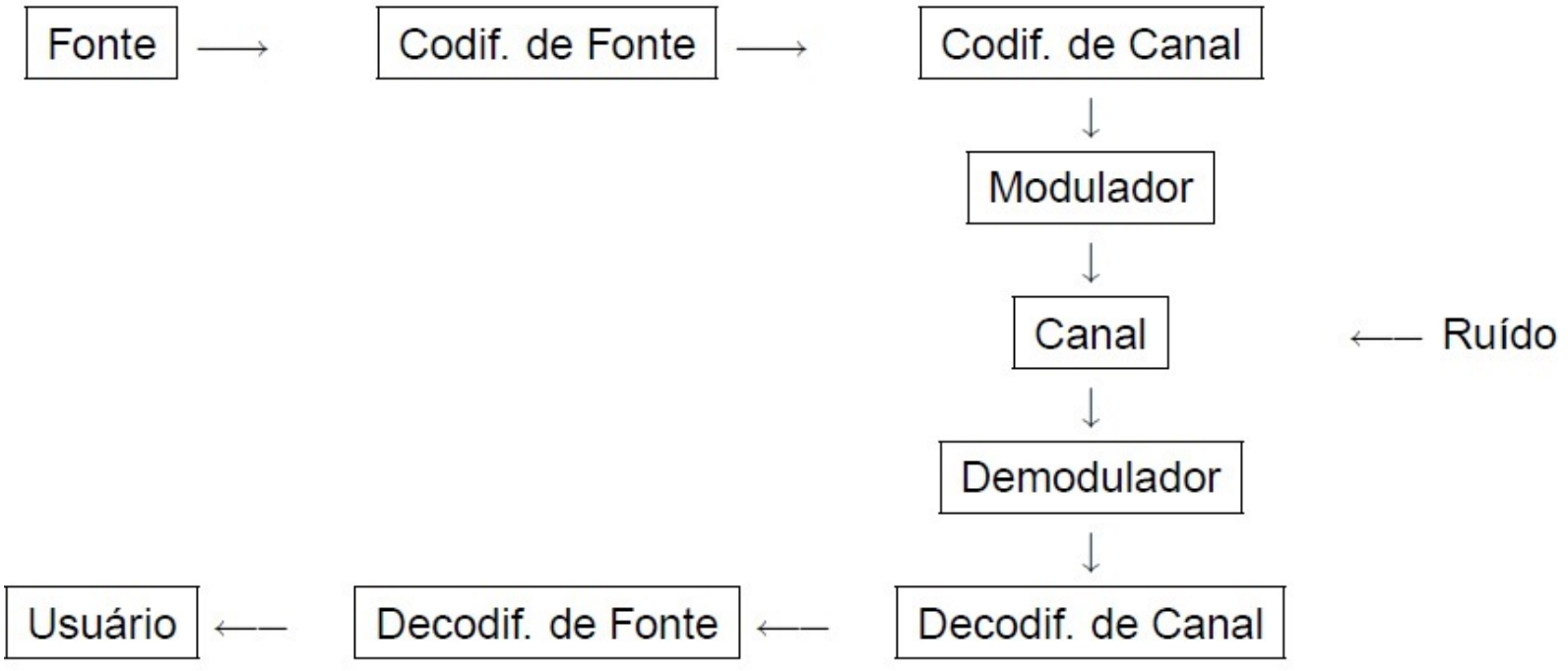
Conceitos Básicos - Exemplo

Se consideramos como alfabeto o conjunto $\mathbb{Z}_3 = \{0, 1, 2\}$. O conjunto

$$\mathcal{C}_2 = \{00012, 11022, 10101, 10201, 20202\},$$

obtemos um código em blocos, ternário, de comprimento 5.

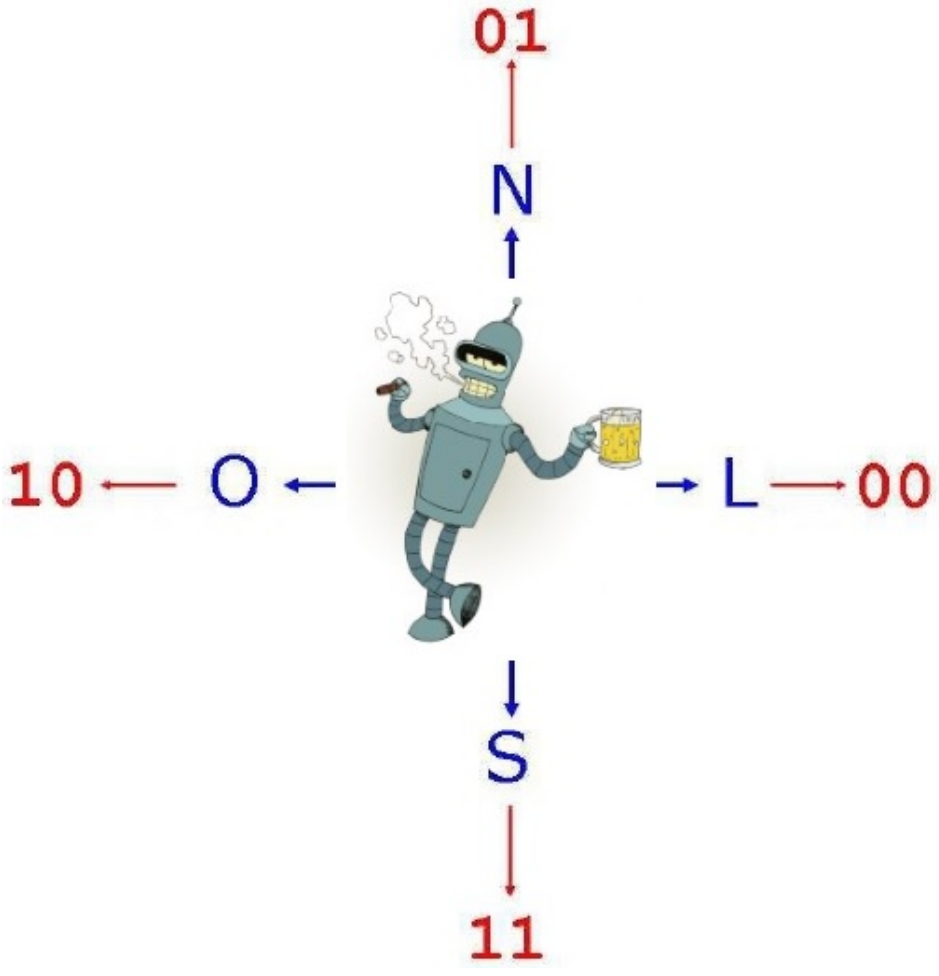
Conceitos Básicos



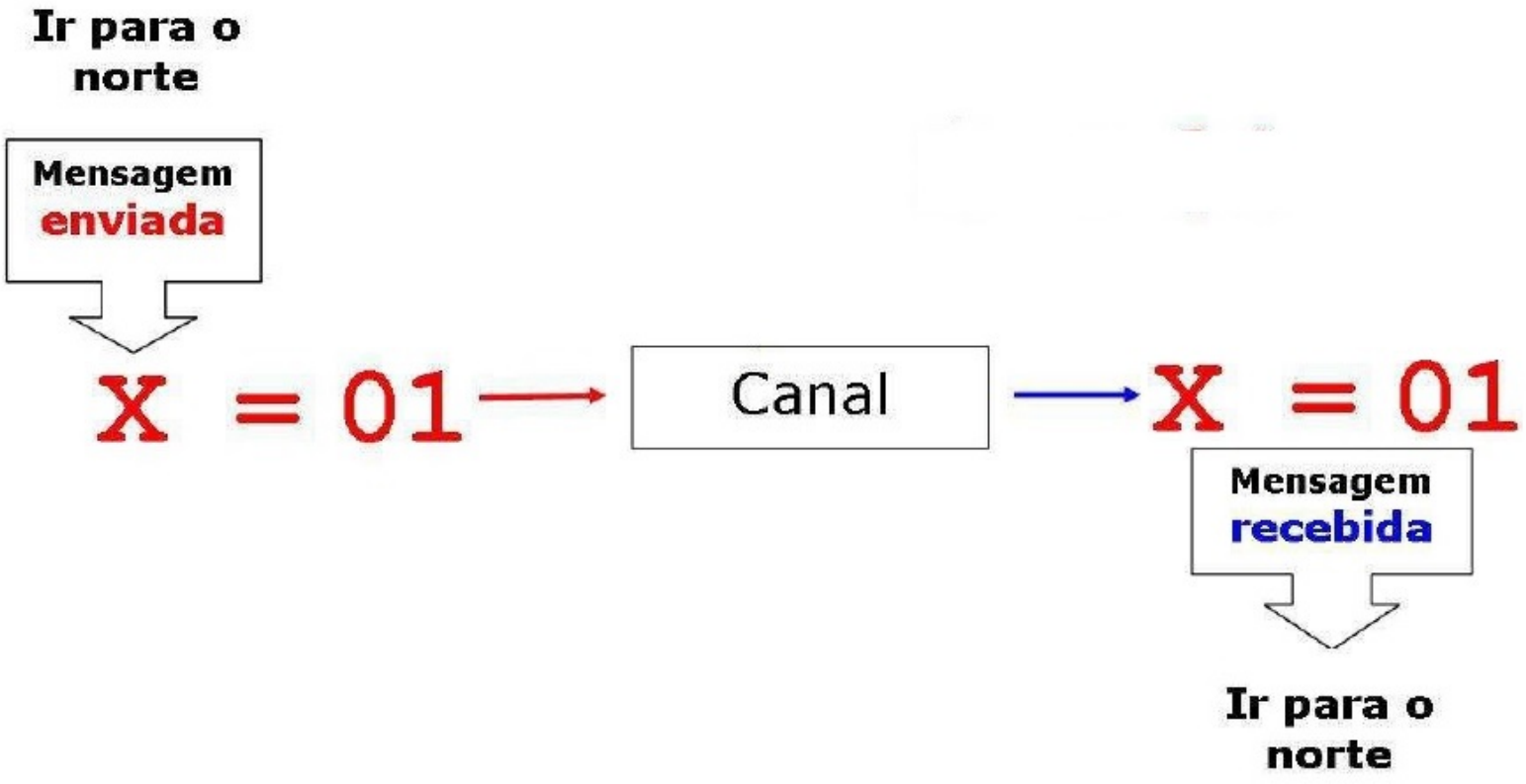
Conceitos Básicos

A ideia de teoria de códigos corretores de erros é codificar a informação inicial, adicionando *informação redundante*, de modo que, ao receber o sinal modificado pelo "ruído" seja possível recuperar a mensagem original.

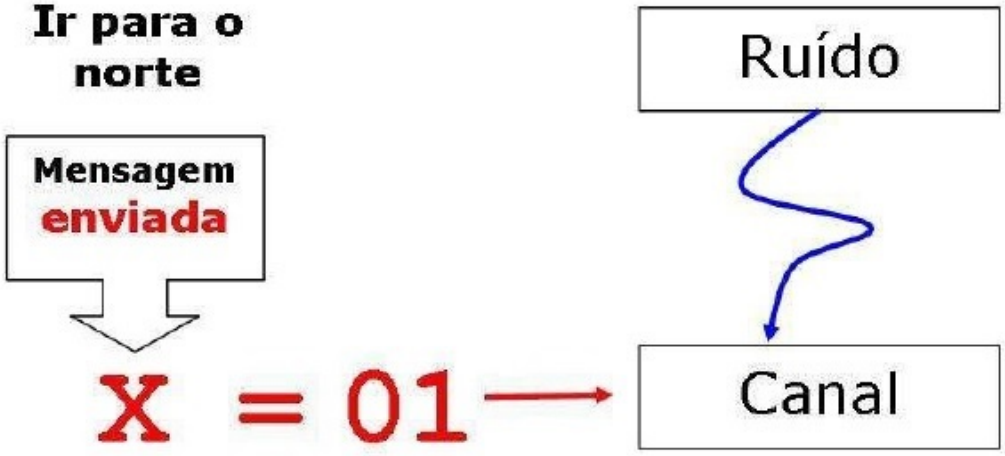
Conceitos Básicos - Exemplo



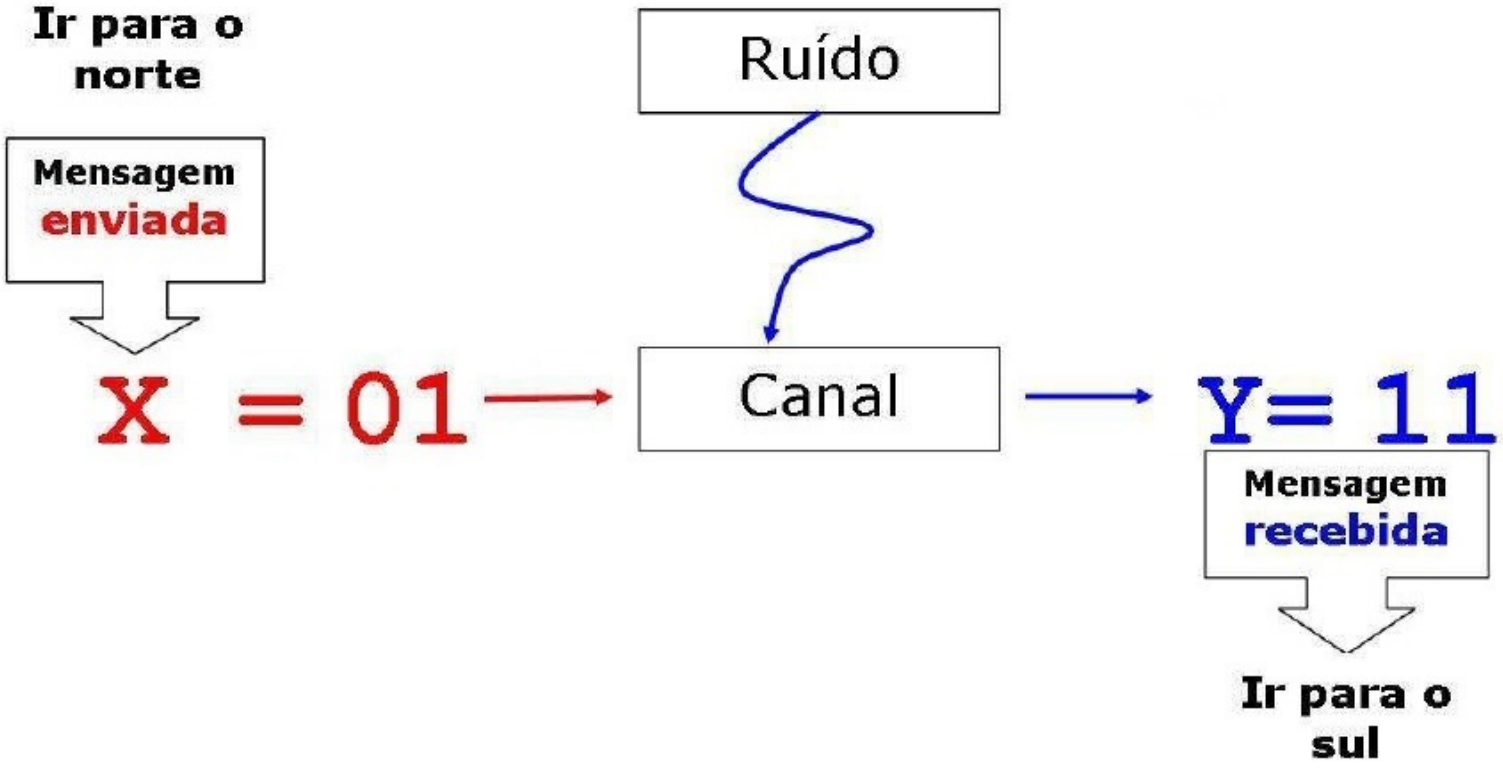
Conceitos Básicos - Exemplo



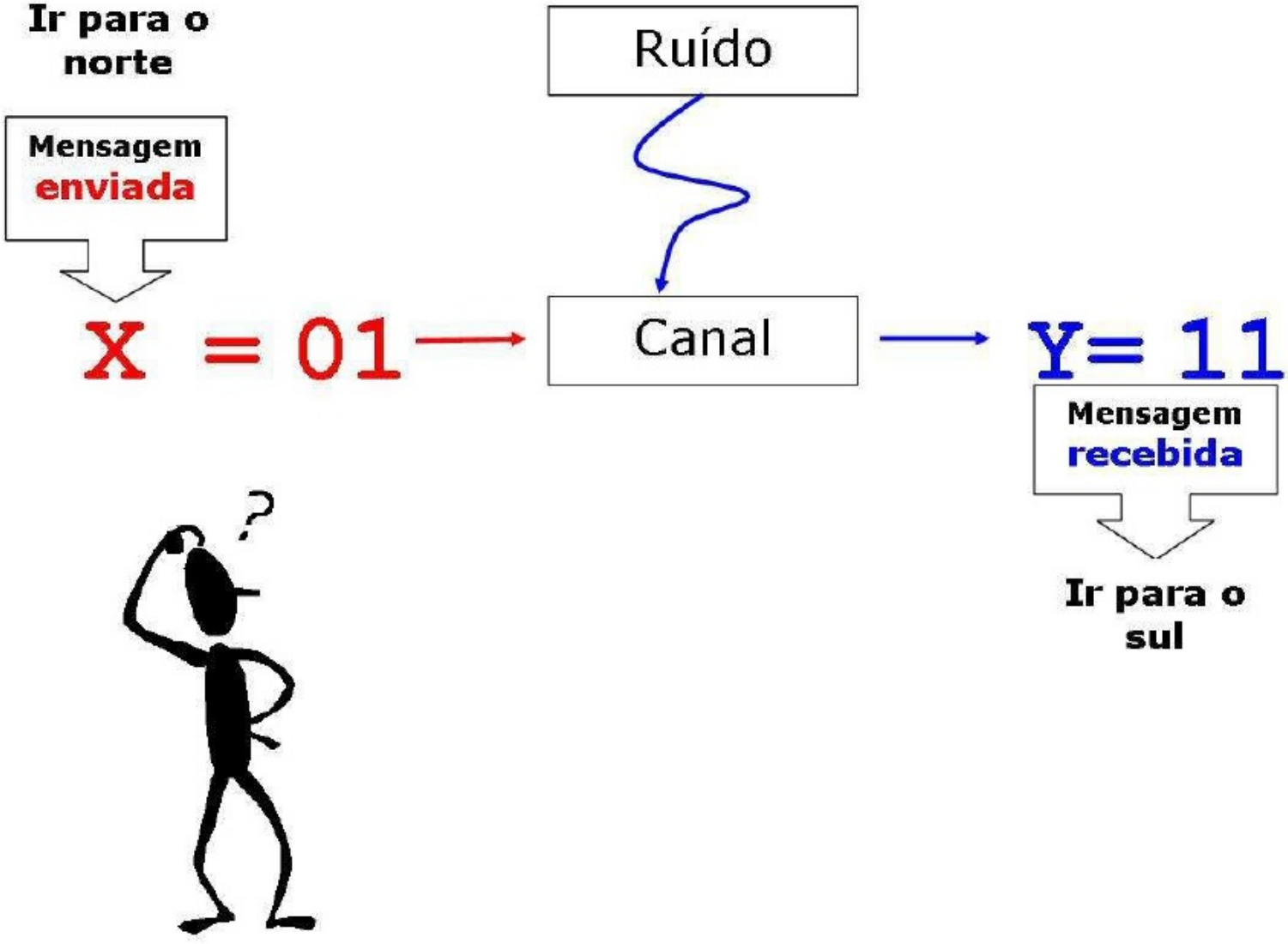
Conceitos Básicos - Exemplo



Conceitos Básicos - Exemplo



Conceitos Básicos - Exemplo



Conceitos Básicos - Exemplo

Mensagem	Código de Fonte	Código de Canal
L	00	000000
N	01	010101
O	10	101010
S	11	111111

Conceitos Básicos - Exemplo

Mensagem	Código de Fonte	Código de Canal
L	00	000000
N	01	010101
O	10	101010
S	11	111111

Conceitos Básicos - Exemplo

Se voltarmos a pensar na língua portuguesa:

> *Na verdade, você nunca entende uma nova teor**x**a.*
> *Você simplesmente a utiliza. (Einstein)*

Conceitos Básicos - Exemplo

Se voltarmos a pensar na língua portuguesa:

Maldito seja aquele ***w****ato!*

Conceitos Básicos

(**Distância de Hamming**). Dados dois elementos $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ de um espaço $\mathcal{A}^n$, chamamos de **distância de Hamming** de x a y ao número de coordenadas em que estes diferem, ou seja,

$$d(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|.$$

Dado um código $\mathcal{C} \subseteq \mathcal{A}^n$ chamamos de **distância mínima** de $\mathcal{C}$ ao número

$$d = \min\{\, d(x, y) : x, y \in \mathcal{C}, x \neq y\}.$$

Conceitos Básicos - Exemplo

Sendo $leste = (0, 0, 0, 0, 0, 0)$, $oeste = (1, 0, 1, 0, 1, 0)$, $norte = (0, 1, 0, 1, 0, 1)$ e $sul = (1, 1, 1, 1, 1, 1)$.

Conceitos Básicos - Exemplo

Sendo $leste = (0,0,0,0,0,0)$, $oeste = (1,0,1,0,1,0)$, $norte = (0,1,0,1,0,1)$ e $sul = (1,1,1,1,1,1)$. Temos que

$$\begin{aligned} d(leste, oeste) &= 3 \\ d(leste, norte) &= 3 \\ d(leste, sul) &= 6 \\ d(oeste, norte) &= 6 \\ d(oeste, sul) &= 3 \\ d(norte, sul) &= 3 \end{aligned}$$

Conceitos Básicos - Exemplo

Sendo $leste = (0,0,0,0,0,0)$, $oeste = (1,0,1,0,1,0)$, $norte = (0,1,0,1,0,1)$ e $sul = (1,1,1,1,1,1)$. Temos que

$$\begin{aligned} d(leste, oeste) &= 3 \\ d(leste, norte) &= 3 \\ d(leste, sul) &= 6 \\ d(oeste, norte) &= 6 \\ d(oeste, sul) &= 3 \\ d(norte, sul) &= 3 \end{aligned}$$

Logo, a distância mínima é $d = 3$.

Conceitos Básicos

(**Métrica**). Dado um conjunto X e uma função

$$d : X \times X \longrightarrow \mathbb{R}_+,$$

dizemos que d é uma **métrica** sobre X (ou uma **função distância** sobre X), se, para quaisquer $x, y, z \in X$, temos:

1. $d(x, y) \geq 0$ e $d(x, y) = \Leftrightarrow x = y$;
2. $d(x, y) = d(y, x)$;
3. $d(x, y) \leq d(x, z) + d(z, y)$.

Conceitos Básicos

Dado um elemento $x \in \mathcal{A}^n$ e um inteiro positivo r chama-se **bola de centro em x e raio r**, ao conjunto

$$B(x, r) = \{u \in \mathcal{A}^n : d(u, x) \leq r\},$$

e **esfera de centro em x e raio r**, ao conjunto

$$S(x, r) = \{u \in \mathcal{A}^n : d(u, x) = r\}.$$

Conceitos Básicos

(**Teorema**) Seja $\mathcal{C}$ um código com distância mínima d e seja

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

então é possível dectar até $d-1$ erros e corrigir até κ erros.

Conceitos Básicos - Exemplo

Sendo nosso código dado por

$$\begin{aligned} leste &= (0,0,0,0,0,0) \\ oeste &= (1,0,1,0,1,0) \\ norte &= (0,1,0,1,0,1) \\ sul &= (1,1,1,1,1,1) \end{aligned}$$

Conceitos Básicos - Exemplo

Sendo nosso código dado por

$$\begin{aligned} leste &= (0,0,0,0,0,0) \\ oeste &= (1,0,1,0,1,0) \\ norte &= (0,1,0,1,0,1) \\ sul &= (1,1,1,1,1,1) \end{aligned}$$

Temos, pelo Teorema,

$$\kappa = \left\lfloor \frac{3-1}{2} \right\rfloor = 1.$$

Conceitos Básicos - Exemplo

Sejam $x = (1, 0, 1, 0, 0, 0)$ e $y = (1, 0, 0, 0, 0, 0)$ palavras recebidas. Logo,

Conceitos Básicos - Exemplo

Sejam $x = (1, 0, 1, 0, 0, 0)$ e $y = (1, 0, 0, 0, 0, 0)$ palavras recebidas. Logo,

$$\begin{array}{cc} d(x, leste) = 2 & d(y, leste) = 1 \\ d(x, oeste) = 1 & d(y, oeste) = 2 \\ d(x, norte) = 5 & d(y, norte) = 3 \\ d(x, sul) = 4 & d(y, sul) = 5 \end{array}$$

Conceitos Básicos - Exemplo

Sejam $x = (1, 0, 1, 0, 0, 0)$ e $y = (1, 0, 0, 0, 0, 0)$ palavras recebidas. Logo,

$$\begin{array}{cc} d(x, leste) = 2 & d(y, leste) = 1 \\ d(x, oeste) = 1 & d(y, oeste) = 2 \\ d(x, norte) = 5 & d(y, norte) = 3 \\ d(x, sul) = 4 & d(y, sul) = 5 \end{array}$$

Logo, x é corrigido para *oeste* e y para *leste*.

(**Corolário**) Um código $\mathcal{C}$ pode corrigir até κ erros se e somente se sua distância mínima $d(\mathcal{C})$ verifica a desigualdade

$$d(\mathcal{C}) \geq 2\kappa + 1.$$

Conceitos Básicos

Dado um código $\mathcal{C}$ com distância mínima d, o número

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

chama-se a **capacidade** de $\mathcal{C}$.

Equivalência de Códigos

Seja M o número de palavras de um código $\mathcal{C}$, ou seja, $M = |\mathcal{C}|$.

Um código q-ário de comprimento n, com M palavras e distância mínima d diz-se um (n, M, d)-código.

Equivalência de Códigos

Sejam $\mathcal{A}$ um conjunto finito e n um inteiro positivo. Uma funçao $\mu : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ diz-se uma **isometria de Hamming** ou, brevemente, uma isometria de $\mathcal{A}^n$ se preserva a distância de Hamming em $\mathcal{A}^n$; i.e., se:

$$d(\mu(x), \mu(y)) = d(x, y) \quad \forall z, y \in \mathcal{A}^n.$$

Equivalência de Códigos

Dois códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ em $\mathcal{A}^n$ são ditos **equivalentes** se existe uma isometria $\mu : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ tal que $\mu(\mathcal{C}_1) = \mathcal{C}_2$.

Equivalência de Códigos - Exemplo

Seja π um permutação dos inteiros positivos $\{1, \ldots, n\}$. Então a função $\mu_\pi : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ dada por

$$\mu_\pi(a_1, \ldots, a_n) = (a_{\pi(1)}, \ldots, a_{\pi(n)})$$

é uma isometria.

Equivalência de Códigos - Exemplo

Seja $f : \mathcal{A} \longrightarrow \mathcal{A}$ uma bijeção $\mathcal{A}$. Fixado um indice i, $1 \leq i \leq n$, definimos a função $\mu_f^{(i)} : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ dada por

$$(a_1, \ldots, a_i, \ldots, a_n) \longrightarrow (a_1, \ldots, f(a_i), \ldots, a_n)$$

é uma isometria. Em particular, se $F = \{f_1, \ldots, f_n\}$ é uma família de bijeções de $\mathcal{A}$, então a função $\mu_F : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ dada por

$$(a_1, \ldots, a_i, \ldots, a_n) \longrightarrow (f_1(a_1), \ldots, f_i(a_i), \ldots, f_n(a_n))$$

é uma isometria.

O problema principal da Teoria de Códigos

- Maior quantidade de palavras M vs. Maior distância mínima d;
- O problema principal da Teoria de Códigos.

O problema principal da Teoria de Códigos

Seja $\mathcal{C}$ um (n, M, d)-código q-ário. Então,

$$B(x, r) = \bigcup_{t=0}^{r} S(x, t)$$

O problema principal da Teoria de Códigos

Seja $x \in \mathcal{A}^n$ e $\mathcal{A}$ um alfabeto com q elementos. Então,

$$y \in S(x,t) \Rightarrow \{i_1, \ldots, i_t\} \in \{1, \ldots, n\} : y(i_j) \neq x(i_j), j \in \{1, \ldots, t\}$$

O problema principal da Teoria de Códigos

Seja $x \in \mathcal{A}^n$ e $\mathcal{A}$ um alfabeto com q elementos. Então,

$$y \in S(x,t) \Rightarrow \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\} : y(i_j) \neq x(i_j), j \in \{1, \ldots, t\}$$
$$\Rightarrow y(i_j) \in \mathcal{A} \setminus \{x(i_j)\}, j \in \{1, \ldots, t\}$$

O problema principal da Teoria de Códigos

Seja $x \in \mathcal{A}^n$ e $\mathcal{A}$ um alfabeto com q elementos. Então,

$$y \in S(x,t) \Rightarrow \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\} : y(i_j) \neq x(i_j), j \in \{1, \ldots, t\}$$
$$\Rightarrow y(i_j) \in \mathcal{A} \setminus \{x(i_j)\}, j \in \{1, \ldots, t\}$$

O problema principal da Teoria de Códigos

- Ou seja, existem $q-1$ possibilidades de letras para colocarmos na posição $y(i_j)$, $j \in \{1, \ldots, t\}$. Logo existem $(q-1)^t$ palavras de $\mathcal{A}^n$ que diferem de x nas t posições $i_1, \ldots, i_t$;
- Como podemos escolher o subconjunto $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ de $\binom{n}{t}$ formas, então:

$$|S(x,t)| = \binom{n}{t} (q-1)^t$$

O problema principal da Teoria de Códigos

Portanto,

$$\begin{aligned} |B(x,r)| &= |\bigcup_{t=0}^{r} S(x,t)| \\ &= \sum_{t=0}^{r} |S(x,t)| \\ &= \sum_{t=0}^{r} \binom{n}{t} (q-1)^t \end{aligned}$$

O problema principal da Teoria de Códigos

Seja $\mathcal{C}$ um (n, M, d)-código q-ário e κ a capacidade de $\mathcal{C}$. Como,

$$B(x, \kappa) \cap B(y, \kappa) = \emptyset \quad \forall x, y \in \mathcal{C} \quad \text{e}$$
$$\bigcup_{x \in \mathcal{C}} B(x, \kappa) \subseteq \mathcal{A}^n.$$

O problema principal da Teoria de Códigos

Seja $\mathcal{C}$ um (n, M, d)-código q-ário e κ a capacidade de $\mathcal{C}$. Como,

$$B(x, \kappa) \cap B(y, \kappa) = \emptyset \quad \forall x, y \in \mathcal{C} \quad \text{e}$$
$$\bigcup_{x \in \mathcal{C}} B(x, \kappa) \subseteq \mathcal{A}^n.$$

Segue que

$$\sum_{x \in \mathcal{C}} |B(x, \kappa)| \leq q^n.$$

O problema principal da Teoria de Códigos

Segue que

$$\sum_{x \in \mathcal{C}} |B(x, \kappa)| \leq q^n.$$

Portanto, como se trata de M esferas contendo o mesmo número de elementos, temos:

$$M \left[\sum_{t=0}^{\kappa} \binom{n}{t} (q-1)^t \right] \leq q^n.$$

O problema principal da Teoria de Códigos

(**Teorema - Cota de Hamming**) Dado um (n, M, d)-código q-ário, tem-se que

$$M \leq \frac{q^n}{\left[\sum_{t=0}^{\kappa} \binom{n}{t} (q-1)^t\right]}.$$

O problema principal da Teoria de Códigos

Um código $\mathcal{C} \subseteq \mathcal{A}^n$ com distância mínima d e capacidade κ diz-se **perfeito** se

$$\bigcup_{x \in \mathcal{C}} B(x, \kappa) = \mathcal{A}^n$$

.

O problema principal da Teoria de Códigos

(**Proposição**) Dado $\mathcal{C}$ um (n, M, d)-código q-ário, $\mathcal{C}$ é perfeito se, e somente se,

$$M = \frac{q^n}{\left[\sum_{t=0}^{\kappa} \binom{n}{t} (q-1)^t\right]}.$$

Referências

- C.C. Lavor, M.M. Alvez, R.M. Siqueira, S.I.R. Costa, *Uma introdução à teoria de códigos*, SBMAC, 2006.
- A. Hefez, M.L.T. Villela, *Códigos Corretores de Erros*, IMPA, Rio De Janeiro, 2002.
- C. P. Milies, *Breve introdução à teoria dos códigos corretores de erros*, Colóquio de Matemática da Região Centro-Oeste, 2009.

Agradecimentos

Gostaria de agradecer:

- UFG - Catalão.

Agradecimentos

Gostaria de agradecer:

- UFG - Catalão.

Obrigado!