Introdução a Teoria dos Códigos

Marcelo Muniz Alves - UFPR

VIII Semana da Matemática UNIFAL

6, 8 e 9 de maio de 2025

VIII Semana da Matemática - UNIFAL

Códigos Corretores de Erros

3a Aula

Códigos de Reed-Muller

Códigos MDS

Códigos de Reed-Solomon

Códigos de Reed-Muller

Códigos de Reed-Muller binários (Muller 1953, Reed 1954)

- $\mathbb{F} = \mathbb{F}_2$

Códigos de Reed-Muller binários (Muller 1953, Reed 1954)

- $\mathbb{F} = \mathbb{F}_2$
- Os códigos de Reed-Muller $RM(1, m)$ são obtidos a partir dos códigos de Hamming.

Códigos de Reed-Muller binários (Muller 1953, Reed 1954)

- $\mathbb{F} = \mathbb{F}_2$
- Os códigos de Reed-Muller $RM(1, m)$ são obtidos a partir dos códigos de Hamming.
- Seus parâmetros são $n = 2^m$, $k = m + 1$, $d = 2^{m-1}$.

Códigos de Reed-Muller binários (Muller 1953, Reed 1954)

- $\mathbb{F} = \mathbb{F}_2$
- Os códigos de Reed-Muller $RM(1, m)$ são obtidos a partir dos códigos de Hamming.
- Seus parâmetros são $n = 2^m$, $k = m + 1$, $d = 2^{m-1}$.
- Neste caso, a taxa k/n é baixa, e tende a zero, e a distância mínima é muito alta (e tende a infinito).

Códigos de Reed-Muller binários (Muller 1953, Reed 1954)

- $\mathbb{F} = \mathbb{F}_2$
- Os códigos de Reed-Muller $RM(1, m)$ são obtidos a partir dos códigos de Hamming.
- Seus parâmetros são $n = 2^m$, $k = m + 1$, $d = 2^{m-1}$.
- Neste caso, a taxa k/n é baixa, e tende a zero, e a distância mínima é muito alta (e tende a infinito).
- O código $RM(1, 6)$ foi utilizado na sonda espacial Mariner de 1969.

Códigos de Reed-Muller

A CLASS OF MULTIPLE-ERROR-CORRECTING CODES
AND THE DECODING SCHEME

Irving S. Reed

Lincoln Laboratory - Massachusetts Institute of Technology
Cambridge, Massachusetts

I. Introduction

A procedure for constructing one-error-correcting and two-error-detecting systematic codes was introduced in a recent study by R. W. Hamming.[1] It is the purpose of this paper to exhibit some examples of n-error-correcting and (n + 1) error-detecting systematic codes for the cases where both the code length and (n + 1) are powers of two. The class of codes to be considered was developed by D. E. Muller in his recent work.[2]

Códigos de Reed-Muller

II. Some Mathematical Preliminaries

A code having n binary digits may be considered the element of a space, consisting of 2^n elements of the form

$$f = (f_0, \ldots f_{n-1})$$

where

$$(f_j = 0, 1) \quad \text{for} \quad (j = 0, 1, 2, \ldots n-1) \ .$$

This space is technically an Abelian group if the sum of any two elements f and g in the space is defined as follows:

$$f \oplus g = (f_0, f_1, \ldots f_{n-1}) \oplus (g_0, g_1, \ldots g_{n-1}) = (f_0 \oplus g_0, f_1 \oplus g_1, \ldots f_{n-1} \oplus g_{n-1}) \ ,$$

Códigos de Reed-Muller

- Seja H_m a matriz de paridade do código de Hamming binário $\mathcal{H}_m$ de parâmetros $[2^m - 1, 2^m - m - 1, 3]$.

Códigos de Reed-Muller

- Seja H_m a matriz de paridade do código de Hamming binário $\mathcal{H}_m$ de parâmetros $[2^m - 1, 2^m - m - 1, 3]$.
- Considere a matriz *geradora* $m + 1 \times 2^m$

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

em que $\mathbf{1} = [1\ 1 \cdots\ 1]$
(m entradas).

Códigos de Reed-Muller

- Seja H_m a matriz de paridade do código de Hamming binário $\mathcal{H}_m$ de parâmetros $[2^m - 1, 2^m - m - 1, 3]$.
- Considere a matriz *geradora* $m + 1 \times 2^m$

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

em que $\mathbf{1} = [1\ 1 \cdots\ 1]$
(m entradas).

- O código definido por G é o código de Reed-Muller de primeira ordem $RM(1, m)$.

Códigos de Reed-Muller

$R(1,3)$ tem matriz geradora

$$G = \left[\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right]$$

Códigos de Reed-Muller

Construção equivalente:

- $A(m) = \{a_0 + a_1 x_1 + \cdots + a_m x_m;\ a_j \in \mathbb{F}_2\}$
  (*funções afins em* $\mathbb{F}_2^m$)

Códigos de Reed-Muller

Construção equivalente:

- $A(m) = \{a_0 + a_1 x_1 + \cdots + a_m x_m;\ a_j \in \mathbb{F}_2\}$
  (*funções afins em* $\mathbb{F}_2^m$)
- temos função linear bijetora

$$S : \mathbb{F}_2^{m+1} \to A(m),\ \ (a_0, \ldots, a_m) \mapsto a_0 + a_1 x_1 + \cdots + a_m x_m$$

Códigos de Reed-Muller

Construção equivalente:

- $A(m) = \{a_0 + a_1 x_1 + \cdots + a_m x_m;\ a_j \in \mathbb{F}_2\}$
  (*funções afins em* $\mathbb{F}_2^m$)
- temos função linear bijetora

$$S : \mathbb{F}_2^{m+1} \to A(m),\ \ (a_0, \ldots, a_m) \mapsto a_0 + a_1 x_1 + \cdots + a_m x_m$$

- $R(1, m)$ é a imagem de

$$T : A(m) \to \mathbb{F}_2^{2^m},\ \ f \mapsto (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^m}))$$

em que $\mathbb{F}_2^m = \{\mathbf{v}_1, \ldots, \mathbf{v}_{2^m-1}, \mathbf{v}_{2^m} = \mathbf{0}\}$.

Códigos de Reed-Muller

Construção equivalente:

- $A(m) = \{a_0 + a_1 x_1 + \cdots + a_m x_m;\ a_j \in \mathbb{F}_2\}$
  (*funções afins em* $\mathbb{F}_2^m$)
- temos função linear bijetora

$$S : \mathbb{F}_2^{m+1} \to A(m),\ \ (a_0, \ldots, a_m) \mapsto a_0 + a_1 x_1 + \cdots + a_m x_m$$

- $R(1, m)$ é a imagem de

$$T : A(m) \to \mathbb{F}_2^{2^m},\ \ f \mapsto (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^m}))$$

  em que $\mathbb{F}_2^m = \{\mathbf{v}_1, \ldots, \mathbf{v}_{2^m-1}, \mathbf{v}_{2^m} = \mathbf{0}\}$.
- Esta função é linear e injetora, logo a dimensão é $m + 1$.

Códigos de Reed-Muller

Construção equivalente:

- $A(m) = \{a_0 + a_1 x_1 + \cdots + a_m x_m;\ a_j \in \mathbb{F}_2\}$
  (*funções afins em* $\mathbb{F}_2^m$)
- temos função linear bijetora

$$S : \mathbb{F}_2^{m+1} \to A(m),\ \ (a_0, \ldots, a_m) \mapsto a_0 + a_1 x_1 + \cdots + a_m x_m$$

- $R(1, m)$ é a imagem de

$$T : A(m) \to \mathbb{F}_2^{2^m},\ \ f \mapsto (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^m}))$$

  em que $\mathbb{F}_2^m = \{\mathbf{v}_1, \ldots, \mathbf{v}_{2^m-1}, \mathbf{v}_{2^m} = \mathbf{0}\}$.
- Esta função é linear e injetora, logo a dimensão é $m + 1$.
- Para conseguir a matriz geradora vamos usar a imagem das funções

$$1, x_1, \ldots, x_m$$

Códigos de Reed-Muller

- A 1a linha vem da função constante igual a 1.

Códigos de Reed-Muller

- A 1a linha vem da função constante igual a 1.
- Nas linhas restantes colocamos as imagens de $x_1, \ldots, x_m$.

Códigos de Reed-Muller

- A 1a linha vem da função constante igual a 1.
- Nas linhas restantes colocamos as imagens de $x_1, \ldots, x_m$.
- Veja que não há duas colunas iguais: a coluna j é

$$(1, x_1(\mathbf{v}_j), x_2(\mathbf{v}_j), \ldots, x_m(\mathbf{v}_j))^T$$

Códigos de Reed-Muller

- A 1a linha vem da função constante igual a 1.
- Nas linhas restantes colocamos as imagens de $x_1, \ldots, x_m$.
- Veja que não há duas colunas iguais: a coluna j é

$$(1, x_1(\mathbf{v}_j), x_2(\mathbf{v}_j), \ldots, x_m(\mathbf{v}_j))^T$$

- Se as colunas i e j são iguais então

$$\begin{aligned} \mathbf{v}_i &= (x_1(\mathbf{v}_i), x_2(\mathbf{v}_i), \ldots, x_m(\mathbf{v}_i)) \\ &= (x_1(\mathbf{v}_j), x_2(\mathbf{v}_j), \ldots, x_m(\mathbf{v}_j)) \\ &= \mathbf{v}_j, \end{aligned}$$

contradição.

Códigos de Reed-Muller

- A 1a linha vem da função constante igual a 1.
- Nas linhas restantes colocamos as imagens de $x_1, \ldots, x_m$.
- Veja que não há duas colunas iguais: a coluna j é

$$(1, x_1(\mathbf{v}_j), x_2(\mathbf{v}_j), \ldots, x_m(\mathbf{v}_j))^T$$

- Se as colunas i e j são iguais então

$$\begin{aligned} \mathbf{v}_i &= (x_1(\mathbf{v}_i), x_2(\mathbf{v}_i), \ldots, x_m(\mathbf{v}_i)) \\ &= (x_1(\mathbf{v}_j), x_2(\mathbf{v}_j), \ldots, x_m(\mathbf{v}_j)) \\ &= \mathbf{v}_j, \end{aligned}$$

  contradição.
- Com isso reobtemos a submatriz H_m (a menos de permutação de colunas).

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

- Sejam $N_0 = \{\mathbf{v} \in \mathbb{F}_2^m; f(\mathbf{v}) = 0\}$ e $N_1 = \{\mathbf{u} \in \mathbb{F}_2^m; f(\mathbf{v}) = 1\}$. Fixe $\mathbf{u} \in N_1$.

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

- Sejam $N_0 = \{\mathbf{v} \in \mathbb{F}_2^m; f(\mathbf{v}) = 0\}$ e $N_1 = \{\mathbf{u} \in \mathbb{F}_2^m; f(\mathbf{v}) = 1\}$. Fixe $\mathbf{u} \in N_1$.
  - Se $\mathbf{v} \in N_0$ então $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = 1 + 0 = 1$.

Logo, temos função $N_0 \to N_1, \quad \mathbf{v} \mapsto \mathbf{u} + \mathbf{v}$.

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

- Sejam $N_0 = \{\mathbf{v} \in \mathbb{F}_2^m; f(\mathbf{v}) = 0\}$ e $N_1 = \{\mathbf{u} \in \mathbb{F}_2^m; f(\mathbf{v}) = 1\}$. Fixe $\mathbf{u} \in N_1$.
  - Se $\mathbf{v} \in N_0$ então $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = 1 + 0 = 1$.

    Logo, temos função $N_0 \to N_1, \quad \mathbf{v} \mapsto \mathbf{u} + \mathbf{v}$.
  - Reciprocamente, se $\mathbf{w} \in N_1$ então $f(\mathbf{u} + \mathbf{w}) = f(\mathbf{u}) + f(\mathbf{w}) = 1 + 1 = 0$.

    Temos outra função $N_1 \to N_0, \quad \mathbf{w} \mapsto \mathbf{u} + \mathbf{w}$.

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

- Sejam $N_0 = \{\mathbf{v} \in \mathbb{F}_2^m; f(\mathbf{v}) = 0\}$ e $N_1 = \{\mathbf{u} \in \mathbb{F}_2^m; f(\mathbf{v}) = 1\}$. Fixe $\mathbf{u} \in N_1$.
  - Se $\mathbf{v} \in N_0$ então $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = 1 + 0 = 1$.

    Logo, temos função $N_0 \to N_1, \quad \mathbf{v} \mapsto \mathbf{u} + \mathbf{v}$.
  - Reciprocamente, se $\mathbf{w} \in N_1$ então $f(\mathbf{u} + \mathbf{w}) = f(\mathbf{u}) + f(\mathbf{w}) = 1 + 1 = 0$.

    Temos outra função $N_1 \to N_0, \quad \mathbf{w} \mapsto \mathbf{u} + \mathbf{w}$.
  - Como $\mathbf{u} + \mathbf{u} = \mathbf{0}$, temos bijeção entre N_0 e N_1.

Códigos de Reed-Muller

- Se $f \in A(m)$ não é constante então metade dos seus valores é 1 e metade é zero, e portanto $\omega(T(f)) = 2^m/2 = 2^{m-1}$.
- Vamos supor que $f = a_1 x_1 + \cdots a_m x_m$. Neste caso,

$$f : \mathbb{F}_2^m \to \mathbb{F}_2 \text{ é linear.}$$

- Sejam $N_0 = \{\mathbf{v} \in \mathbb{F}_2^m; f(\mathbf{v}) = 0\}$ e $N_1 = \{\mathbf{u} \in \mathbb{F}_2^m; f(\mathbf{v}) = 1\}$. Fixe $\mathbf{u} \in N_1$.
  - Se $\mathbf{v} \in N_0$ então $f(\mathbf{u} + \mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v}) = 1 + 0 = 1$.

    Logo, temos função $N_0 \to N_1, \quad \mathbf{v} \mapsto \mathbf{u} + \mathbf{v}$.
  - Reciprocamente, se $\mathbf{w} \in N_1$ então $f(\mathbf{u} + \mathbf{w}) = f(\mathbf{u}) + f(\mathbf{w}) = 1 + 1 = 0$.

    Temos outra função $N_1 \to N_0, \quad \mathbf{w} \mapsto \mathbf{u} + \mathbf{w}$.
  - Como $\mathbf{u} + \mathbf{u} = \mathbf{0}$, temos bijeção entre N_0 e N_1.
- Segue que $\omega(T(f) = 2^{m-1} = d(R(1, m))$.

Códigos de Reed-Muller

- Geometricamente, $R(1, m)$ é análogo a se tomar um "código biortogonal" na esfera unitária em $\mathbb{R}^n$, isto é, um conjunto da forma

$$\pm\mathbf{u}_1, \ldots, \pm\mathbf{u}_n$$

em que $\mathbf{u}_1, \ldots, \mathbf{u}_n$ formam uma base ortogonal.

Códigos de Reed-Muller

- Geometricamente, $R(1,m)$ é análogo a se tomar um "código biortogonal" na esfera unitária em $\mathbb{R}^n$, isto é, um conjunto da forma

$$\pm\mathbf{u}_1, \ldots, \pm\mathbf{u}_n$$

em que $\mathbf{u}_1, \ldots, \mathbf{u}_n$ formam uma base ortogonal.

- A função é

$$(a_1, \ldots, a_n) \in RM(1,m) \mapsto ((-1)^{a_1}, \ldots, (-1)^{a_n}) \in \mathbb{R}^n$$

com $n = 2^m$.
Isso é usado para um algoritmo de decodificação específico para este código.

Códigos MDS

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

- Se $H = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_n]$ e $\mathbf{v} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ tem coordenadas não-nulas $b_{i_1}, \ldots, b_{i_r}$ com $r \leq d-1$, então $\mathbf{v} \notin C$

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

- Se $H = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_n]$ e $\mathbf{v} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ tem coordenadas não-nulas $b_{i_1}, \ldots, b_{i_r}$ com $r \leq d-1$, então $\mathbf{v} \notin C$

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

- Se $H = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_n]$ e $\mathbf{v} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ tem coordenadas não-nulas $b_{i_1}, \ldots, b_{i_r}$ com $r \leq d-1$, então $\mathbf{v} \notin C$, portanto

$$H\mathbf{v}^T = b_{i_1}\mathbf{h}_{i_1} + \cdots + b_{i_r}\mathbf{h}_{i_r} \neq \mathbf{0}.$$

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

- Se $H = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_n]$ e $\mathbf{v} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ tem coordenadas não-nulas $b_{i_1}, \ldots, b_{i_r}$ com $r \leq d-1$, então $\mathbf{v} \notin C$, portanto

$$H\mathbf{v}^T = b_{i_1}\mathbf{h}_{i_1} + \cdots + b_{i_r}\mathbf{h}_{i_r} \neq \mathbf{0}.$$

- Então todo subdeterminante $(d-1) \times (d-1)$ é não-nulo

Códigos Lineares - Limitante de Singleton

$\mathbb{F} = \mathbb{F}_q$.

- Seja H matriz $(n-k) \times n$ de posto $n-k$, C o código linear, com $d(C) = d$, definido por

$$\mathbf{v} \in C \iff H\mathbf{v}^T = \mathbf{0}.$$

- Se $H = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_n]$ e $\mathbf{v} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ tem coordenadas não-nulas $b_{i_1}, \ldots, b_{i_r}$ com $r \leq d-1$, então $\mathbf{v} \notin C$, portanto

$$H\mathbf{v}^T = b_{i_1}\mathbf{h}_{i_1} + \cdots + b_{i_r}\mathbf{h}_{i_r} \neq \mathbf{0}.$$

- Então todo subdeterminante $(d-1) \times (d-1)$ é não-nulo
- Segue que

$$d - 1 \leq \text{posto } H.$$

Códigos Lineares - Limitante de Singleton

- Sendo d a distância mínima de C, segue que

$$d - 1 \leq \text{posto}\, H = n - k$$

Códigos Lineares - Limitante de Singleton

- Sendo d a distância mínima de C, segue que

$$d - 1 \leq \text{posto}\, H = n - k$$

- Limitante de Singleton: se C é um código de parâmetros $[n, k, d]$ então

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

Códigos Lineares - Limitante de Singleton

- Sendo d a distância mínima de C, segue que

$$d - 1 \leq \text{posto}\, H = n - k$$

- Limitante de Singleton: se C é um código de parâmetros $[n, k, d]$ então

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

- Um código é MDS quando vale a igualdade. ("*maximum distance separable*")

Códigos de Reed-Solomon

Códigos de Reed-Solomon

$\mathbb{F} = \mathbb{F}_q$.

Códigos de Reed-Solomon

$\mathbb{F} = \mathbb{F}_q$. Tome $1 \leq m < n \leq q$,

Códigos de Reed-Solomon

$\mathbb{F} = \mathbb{F}_q$. Tome $1 \leq m < n \leq q$,

$$X = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F},$$
$$R_m = \{p(x) \in \mathbb{F}[x]; p = 0 \text{ ou } \text{grau}(p) \leq m\} \subset \mathbb{F}[x].$$

Códigos de Reed-Solomon

$\mathbb{F} = \mathbb{F}_q$. Tome $1 \leq m < n \leq q$,

$$X = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F},$$
$$R_m = \{p(x) \in \mathbb{F}[x]; p = 0 \text{ ou } \text{grau}(p) \leq m\} \subset \mathbb{F}[x].$$

Identificamos $\mathbb{F}^{m+1}$ com R_m pela bijeção linear

$$(a_0, a_1, \ldots, a_m) \mapsto a_0 + a_1 x + \cdots + a_m x^m.$$

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rcl} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rcl} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

- T é linear, e é injetora:

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rcl} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

- T é linear, e é injetora:

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rccc} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

- T é linear, e é injetora:

$$f(\alpha_1) = f(\alpha_2) = \cdots = f(\alpha_n) = 0,$$

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rccc} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

- T é linear, e é injetora:

$$f(\alpha_1) = f(\alpha_2) = \cdots = f(\alpha_n) = 0,$$

$$\text{grau}(f) \leq m < n \implies f = 0.$$

Códigos de Reed-Solomon

- (I. Reed, S. Solomon, 1960)

$$\begin{array}{rccc} T : R_m & \longrightarrow & \mathbb{F}^n \\ f(x) & \mapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

- T é linear, e é injetora:

$$f(\alpha_1) = f(\alpha_2) = \cdots = f(\alpha_n) = 0,$$

$$\text{grau}(f) \leq m < n \implies f = 0.$$

- O código de Reed-Solomon C gerado por X e R_m é o conjunto dos vetores

$$(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n))$$

com $f(x)$ em R_m.

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

  $\omega(T(f))$ = coordenadas não-nulas de $T(f)$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

  $\omega(T(f))$ = coordenadas não-nulas de $T(f)$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

$$\begin{aligned} \omega(T(f)) &= \text{coordenadas não-nulas de } T(f) \\ &= n - (\text{número de } \alpha_i \text{ tais que } f(\alpha_i) = 0) \end{aligned}$$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

$$\begin{aligned} \omega(T(f)) &= \text{coordenadas não-nulas de } T(f) \\ &= n - (\text{número de } \alpha_i \text{ tais que } f(\alpha_i) = 0) \\ &\geq n - (\text{número de raízes de } f) \end{aligned}$$

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

$$\begin{aligned} \omega(T(f)) &= \text{coordenadas não-nulas de } T(f) \\ &= n - (\text{número de } \alpha_i \text{ tais que } f(\alpha_i) = 0) \\ &\geq n - (\text{número de raízes de } f) \\ &\geq n - m \end{aligned}$$

quando $f \neq 0$.

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

  $$\begin{aligned} \omega(T(f)) &= \text{coordenadas não-nulas de } T(f) \\ &= n - (\text{número de } \alpha_i \text{ tais que } f(\alpha_i) = 0) \\ &\geq n - (\text{número de raízes de } f) \\ &\geq n - m \end{aligned}$$

  quando $f \neq 0$.
- $f(x) = (x - \alpha_1) \cdots (x - \alpha_m) \implies \omega(T(f)) = n - m$.

Códigos de Reed-Solomon

- $C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in R_m\}$
- $k = \dim(C) = \dim(R_m) = m + 1$
- $d = d(C) = n - m$.

  $$\begin{aligned} \omega(T(f)) &= \text{coordenadas não-nulas de } T(f) \\ &= n - (\text{número de } \alpha_i \text{ tais que } f(\alpha_i) = 0) \\ &\geq n - (\text{número de raízes de } f) \\ &\geq n - m \end{aligned}$$

  quando $f \neq 0$.
- $f(x) = (x - \alpha_1) \cdots (x - \alpha_m) \implies \omega(T(f)) = n - m$.
- Daí

  $$k + d = (m + 1) + (n - m) = n + 1.$$

  e C é *MDS*.

Códigos de Reed-Solomon

- Existem códigos MDS que não são do tipo RS, mas

  Os códigos binários MDS têm péssimos parâmetros:

  Códigos de repetição;
  Código total $\mathbb{F}_2^n$;
  Código com um dígito verificador (“ISBN binário”).

Códigos de Reed-Solomon

- Existem códigos MDS que não são do tipo RS, mas

  Os códigos binários MDS têm péssimos parâmetros:

  Códigos de repetição;
  Código total $\mathbb{F}_2^n$;
  Código com um dígito verificador ("ISBN binário").

- É necessário utilizar corpos finitos mais "sofisticados" do que os corpos $\mathbb{Z}_p$ mesmo para aplicações práticas, nas quais trabalha-se em geral com $q = 2^r$.

Códigos de Reed-Solomon, $q = 11$: ISBN-10

ISBN-10: as mensagens codificadas moram no código C sobre $\mathbb{F} = \mathbb{Z}_{11}$, de

- comprimento $n = 10$,
- dimensão $k = 9$

dado por

$$T : \mathbb{F}^9 \to \mathbb{F}^{10}, \quad (a_i) \mapsto (a_1, \ldots, a_9, \sum_{j=0}^{9} j a_j).$$

Códigos de Reed-Solomon, $q = 11$: ISBN-10

ISBN-10: as mensagens codificadas moram no código C sobre $\mathbb{F} = \mathbb{Z}_{11}$, de

- comprimento $n = 10$,
- dimensão $k = 9$

dado por

$$T : \mathbb{F}^9 \to \mathbb{F}^{10}, \quad (a_i) \mapsto (a_1, \ldots, a_9, \sum_{j=0}^{9} j a_j).$$

- $d(C) = 2$.
- C detecta 1 erro, não corrige erros.

Códigos de Reed-Solomon, $q = 11$: ISBN-10

ISBN-10: as mensagens codificadas moram no código C sobre $\mathbb{F} = \mathbb{Z}_{11}$, de

- comprimento $n = 10$,
- dimensão $k = 9$
- C detecta 1 erro, não corrige erros.

Códigos de Reed-Solomon, $q = 11$: ISBN-10

ISBN-10: as mensagens codificadas moram no código C sobre $\mathbb{F} = \mathbb{Z}_{11}$, de

- comprimento $n = 10$,
- dimensão $k = 9$
- C detecta 1 erro, não corrige erros.

Código de Reed-Solomon R com $m = 8, n = 11$ $(X = \mathbb{Z}_{11})$:

$$(a_1, \ldots, a_9) \mapsto f(x) = \sum_{j=1}^{9} a_{i-1} x^{i-i} \mapsto (f(0), f(1), \ldots, f(10))$$

Códigos de Reed-Solomon, $q = 11$: ISBN-10

ISBN-10: as mensagens codificadas moram no código C sobre $\mathbb{F} = \mathbb{Z}_{11}$, de

- comprimento $n = 10$,
- dimensão $k = 9$
- C detecta 1 erro, não corrige erros.

Código de Reed-Solomon R com $m = 8, n = 11$ $(X = \mathbb{Z}_{11})$:

$$(a_1, \ldots, a_9) \mapsto f(x) = \sum_{j=1}^{9} a_{i-1} x^{i-i} \mapsto (f(0), f(1), \ldots, f(10))$$

- $d = n + 1 - k = 11 + 1 - 9 = 3$.
- R detecta 2 erros e corrige 1 erro.

Codificação para o CD

Padrões de erros no CD

- $q = 2$, $n = 7$. Erros aleatórios em 3 coordenadas (35 ao total):

$$\begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ & & & \vdots & & & \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{matrix}$$

Padrões de erros no CD

- $q = 2$, $n = 7$. Erros aleatórios em 3 coordenadas (35 ao total):

$$\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ & & & \vdots & & & \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

- Erros do CD (arranhões, etc): erros de *rajada* (“bursts”):

$$\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Codificação no CD

- Cada onda $f(t)$ é representada por uma série de amostras $(t_k, f(t_k))$.

Codificação no CD

- Cada onda $f(t)$ é representada por uma série de amostras $(t_k, f(t_k))$.
- Cada amostra é um par de vetores de $\mathbb{F}_2^{16}$ (par = canal esquerdo e direito)

Codificação no CD

- Cada onda $f(t)$ é representada por uma série de amostras $(t_k, f(t_k))$.
- Cada amostra é um par de vetores de $\mathbb{F}_2^{16}$ (par = canal esquerdo e direito)
- Um "byte" é um vetor de $\mathbb{F}_2^8$; cada amostra corresponde a dois bytes por canal. A codificação é feita começando dos bytes.

Codificação no CD

- Cada onda $f(t)$ é representada por uma série de amostras $(t_k, f(t_k))$.
- Cada amostra é um par de vetores de $\mathbb{F}_2^{16}$ (par = canal esquerdo e direito)
- Um "byte" é um vetor de $\mathbb{F}_2^8$; cada amostra corresponde a dois bytes por canal. A codificação é feita começando dos bytes.
- Identificaremos $\mathbb{F}_2^8$ e $\mathbb{F}_{2^8}$ como espaços vetoriais sobre $\mathbb{F}_2$.

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.
- **Quadro**: sequência de 6 amostras =

$$E_1 D_1 E_2 D_2 E_3 D_3 E_4 D_4 E_5 D_5 E_6 D_6 \in \mathbb{F}_{2^8}^{24}$$

onde cada E_k (cada D_k) corresponde a dois bytes.

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.
- **Quadro**: sequência de 6 amostras =

$$E_1 D_1 E_2 D_2 E_3 D_3 E_4 D_4 E_5 D_5 E_6 D_6 \in \mathbb{F}_{2^8}^{24}$$

onde cada E_k (cada D_k) corresponde a dois bytes.

- Resumo:

$$\mathbb{F}_{2^8}^{24} \xrightarrow[\text{emb.}]{} \mathbb{F}_{2^8}^{24} \xrightarrow[\text{cod.}[28,24,5]]{} \mathbb{F}_{2^8}^{28} \xrightarrow[\text{emb.}]{} \mathbb{F}_{2^8}^{28} \xrightarrow[\text{cod.}[32,28,5]]{} \mathbb{F}_{2^8}^{32}$$

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.
- **Quadro**: sequência de 6 amostras =

$$E_1 D_1 E_2 D_2 E_3 D_3 E_4 D_4 E_5 D_5 E_6 D_6 \in \mathbb{F}_{2^8}^{24}$$

onde cada E_k (cada D_k) corresponde a dois bytes.

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.
- **Quadro**: sequência de 6 amostras =

$$E_1 D_1 E_2 D_2 E_3 D_3 E_4 D_4 E_5 D_5 E_6 D_6 \in \mathbb{F}_{2^8}^{24}$$

onde cada E_k (cada D_k) corresponde a dois bytes.

- Embaralhamento 1:

$$E_1 D_1 \overline{E_2 D_2} E_3 D_3 \overline{E_4 D_4} E_5 D_5 \overline{E_6 D_6}$$

onde $\overline{E_{2k} D_{2k}}$ vêm de dois quadros adiante.

Codificação no CD

- Usamos dois códigos de Reed-Solomon sobre $\mathbb{F}_{2^8}$.
- **Quadro**: sequência de 6 amostras =

$$E_1 D_1 E_2 D_2 E_3 D_3 E_4 D_4 E_5 D_5 E_6 D_6 \in \mathbb{F}_{2^8}^{24}$$

onde cada E_k (cada D_k) corresponde a dois bytes.

- Embaralhamento 1:

$$E_1 D_1 \overline{E_2 D_2} E_3 D_3 \overline{E_4 D_4} E_5 D_5 \overline{E_6 D_6}$$

onde $\overline{E_{2k} D_{2k}}$ vêm de dois quadros adiante.

- Embaralhamento 2:

$$E_1 E_3 E_5 D_1 D_3 D_5, \overline{E_2 E_4 E_6 D_2 D_4 D_6}$$

Codificação no CD

- Embaralhamento 2:

$$E_1 E_3 E_5 D_1 D_3 D_5, \overline{E_2 E_4 E_6 D_2 D_4 D_6}$$

Codificação no CD

- Embaralhamento 2:

$$E_1 E_3 E_5 D_1 D_3 D_5, \overline{E_2 E_4 E_6 D_2 D_4 D_6}$$

- **Codificação 1**: a mensagem m acima tem 24 bytes, isto é, está em $\mathbb{F}_{2^8}^{24}$. Usamos um código RS sobre $\mathbb{F}_{2^8}$, de parâmetros $[28, 24, 5]$, que faz

$$m \mapsto m' = (m, P_1, P_2) \in \mathbb{F}_{2^8}^{28}$$

Codificação no CD

- Embaralhamento 2:

$$E_1 E_3 E_5 D_1 D_3 D_5, \overline{E_2 E_4 E_6 D_2 D_4 D_6}$$

- **Codificação 1**: a mensagem m acima tem 24 bytes, isto é, está em $\mathbb{F}_{2^8}^{24}$. Usamos um código RS sobre $\mathbb{F}_{2^8}$, de parâmetros $[28, 24, 5]$, que faz

$$m \mapsto m' = (m, P_1, P_2) \in \mathbb{F}_{2^8}^{28}$$

- Novo embaralhamento...

$$(m, P_1, P_2) \mapsto E_1 E_3 E_5 D_1 D_3 D_5 \mathbf{P_1 P_2} \overline{E_2 E_4 E_6 D_2 D_4 D_6}$$

Codificação no CD

- **Codificação 2**: codificamos mais uma vez, agora com um *RS* $[32, 28, 5]$ e chegamos a uma palavra em $\mathbb{F}_{2^8}^{32}$.

Codificação no CD

- **Codificação 2**: codificamos mais uma vez, agora com um *RS* [32, 28, 5] e chegamos a uma palavra em $\mathbb{F}_{2^8}^{32}$.
- É esta palavra, reescrita em bytes (sequências de 0s e 1s de comprimento 8) por um isomorfismo linear $\mathbb{F}_{2^8} \to \mathbb{F}_2^8$, que é gravada no CD.

Codificação no CD

- **Codificação 2**: codificamos mais uma vez, agora com um *RS* $[32, 28, 5]$ e chegamos a uma palavra em $\mathbb{F}_{2^8}^{32}$.
- É esta palavra, reescrita em bytes (sequências de 0s e 1s de comprimento 8) por um isomorfismo linear $\mathbb{F}_{2^8} \to \mathbb{F}_2^8$, que é gravada no CD.
- Ainda há mais detalhes dos quais vocês serão poupados...resumindo

$$\mathbb{F}_{2^8}^{24} \underset{\text{emb.}}{\to} \mathbb{F}_{2^8}^{24} \underset{\text{cod.}[28,24,5]}{\to} \mathbb{F}_{2^8}^{28} \underset{\text{emb.}}{\to} \mathbb{F}_{2^8}^{28} \underset{\text{cod.}[32,28,5]}{\to} \mathbb{F}_{2^8}^{32}$$

Codificação no CD

- Codificação final (com + bits de controle e outros...) cada amostra de $6 \times (4 \times 8) = 192$ bits vira uma sequência de $33 \times 17 = 588$ bits. Taxa $k/n \cong 0,326 \cong 1/3$.

Codificação no CD

- Codificação final (com + bits de controle e outros...) cada amostra de $6 \times (4 \times 8) = 192$ bits vira uma sequência de $33 \times 17 = 588$ bits. Taxa $k/n \cong 0,326 \cong 1/3$.
- Vantagens: Rajadas longas são quebradas em rajadas mais curtas, com mais possibilidade de correção.

Codificação no CD

- Codificação final (com + bits de controle e outros...) cada amostra de $6 \times (4 \times 8) = 192$ bits vira uma sequência de $33 \times 17 = 588$ bits. Taxa $k/n \cong 0,326 \cong 1/3$.
- Vantagens: Rajadas longas são quebradas em rajadas mais curtas, com mais possibilidade de correção.
- Capacidade de correção: até 2.8 mm de comprimento ao longo de uma faixa (!)

Decodificação no CD (= leitura)

- Decodificação 1:

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo
  - corrige-se até 1 erro (veja que o código $[32, 28, 5]$ corrige até 2). Qualquer erro extra é deixado para ser corrigido pelo código 1.

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo
  - corrige-se até 1 erro (veja que o código $[32, 28, 5]$ corrige até 2). Qualquer erro extra é deixado para ser corrigido pelo código 1.
- Decodificação 2:

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo
  - corrige-se até 1 erro (veja que o código $[32, 28, 5]$ corrige até 2). Qualquer erro extra é deixado para ser corrigido pelo código 1.
- Decodificação 2:
  - volta-se ao primeiro *RS* em $\mathbb{F}_{2^8}^{28}$ e decodifica-se (qdo possível).

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo
  - corrige-se até 1 erro (veja que o código $[32, 28, 5]$ corrige até 2). Qualquer erro extra é deixado para ser corrigido pelo código 1.
- Decodificação 2:
  - volta-se ao primeiro *RS* em $\mathbb{F}_{2^8}^{28}$ e decodifica-se (qdo possível).
  - se algum erro ainda sobreviver em uma palavra na decodificação do código 1, faz-se uma interpolação linear entre as amostras adjacentes.

Decodificação no CD (= leitura)

- Decodificação 1:
  - tiram-se os bits extras (controle)
  - desembaralhamos tudo
  - corrige-se até 1 erro (veja que o código $[32, 28, 5]$ corrige até 2). Qualquer erro extra é deixado para ser corrigido pelo código 1.
- Decodificação 2:
  - volta-se ao primeiro *RS* em $\mathbb{F}_{2^8}^{28}$ e decodifica-se (qdo possível).
  - se algum erro ainda sobreviver em uma palavra na decodificação do código 1, faz-se uma interpolação linear entre as amostras adjacentes.
  - se as adjacentes também estiverem com problemas...usa-se um “emudecimento” (que dura alguns milissegundos; em geral é imperceptível).

Leitura e pesquisa

Recomendo fortemente o livro

- Abramo Hefez e Maria L.T. Vilela, Introdução aos Códigos Corretores de Erros. IMPA.

Leitura e pesquisa

Recomendo fortemente o livro

- Abramo Hefez e Maria L.T. Vilela, Introdução aos Códigos Corretores de Erros. IMPA.

Temas de pesquisa atuais:

- Códigos MDS
- Códigos de geometria algébrica
- Métricas alternativas (Lee, Rosenbloom-Tsfasman, rank metric)
- Quantum error-correcting codes
- Reticulados em $\mathbb{R}^n$

algumas referências

- L. Egghe, R. Rousseau, *The Detection of Double Errors in ISBN- and ISSN-like Codes*. Mathematical and Computer Modelling 33 (2001) 943-955.
- Abramo Hefez e Maria L.T. Vilela, Introdução aos Códigos Corretores de Erros. IMPA.
- R. Lidl e H. Niederreiter, Introduction to Finite Fields and their Applications (revised edition), caps 2, 3, 8. Cambridge.
- W.C. Huffman, Vera Pless, Fundamentals of Error-Correcting Codes. Cambridge.