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

2a Aula

Matriz geradora

Matriz de paridade

Códigos de Hamming

Códigos perfeitos

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;
  - $\mathbf{u} \in C, \alpha \in \mathbb{F} \implies \alpha\mathbf{u} \in C$.

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;
  - $\mathbf{u} \in C, \alpha \in \mathbb{F} \implies \alpha\mathbf{u} \in C$.
- Os códigos de repetição são códigos lineares sobre $\mathbb{Z}_2$.

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;
  - $\mathbf{u} \in C, \alpha \in \mathbb{F} \implies \alpha\mathbf{u} \in C$.
- Os códigos de repetição são códigos lineares sobre $\mathbb{Z}_2$.
- O ISBN-10 não é linear,

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;
  - $\mathbf{u} \in C, \alpha \in \mathbb{F} \implies \alpha\mathbf{u} \in C$.
- Os códigos de repetição são códigos lineares sobre $\mathbb{Z}_2$.
- O ISBN-10 não é linear,

Códigos Lineares - revisão

- Código **linear** em $\mathbb{F}^n$:
  - $\mathbf{u}, \mathbf{v} \in C \implies \mathbf{u} + \mathbf{v} \in C$;
  - $\mathbf{u} \in C, \alpha \in \mathbb{F} \implies \alpha\mathbf{u} \in C$.
- Os códigos de repetição são códigos lineares sobre $\mathbb{Z}_2$.
- O ISBN-10 não é linear, mas está contido em um código linear sobre $\mathbb{Z}_{11}$: as soluções

$$(a_1, a_2, \ldots, a_{10}) \in (\mathbb{Z}_{11})^{10}$$

da equação

$$\sum_{j=1}^{10} (11 - j)x_j = 0.$$

Códigos Lineares - revisão

- Todo código linear em $\mathbb{F}^n$ é imagem de uma função **injetora**

$$f : \mathbb{F}^k \to \mathbb{F}^n$$

que é **linear**, isto é,
dados $u, v \in \mathbb{F}^k, \alpha \in \mathbb{F}$,

$$f(u+v) = f(u) + f(v)$$

e

$$f(\alpha u) = \alpha \cdot f(u)$$

Códigos Lineares - revisão

- Todo código linear em $\mathbb{F}^n$ é imagem de uma função **injetora**

$$f : \mathbb{F}^k \to \mathbb{F}^n$$

que é **linear**, isto é,
dados $u, v \in \mathbb{F}^k, \alpha \in \mathbb{F}$,

$$f(u+v) = f(u) + f(v)$$

e

$$f(\alpha u) = \alpha \cdot f(u)$$

- A **dimensão** de C é k.

Códigos Lineares - revisão

- Código do ISBN-10:

$$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

Códigos Lineares - revisão

- Código do ISBN-10:

$$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

Códigos Lineares - revisão

- Código do ISBN-10:

$$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

$$\sum_{j=1}^{10} (11 - j) a_j = 0$$

Códigos Lineares - revisão

- Código do ISBN-10:

$$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

$$\sum_{j=1}^{10} (11 - j) a_j = 0 \implies a_{10} = -\sum_{j=1}^{10} (11 - j) a_j = \sum_{j=1}^{10} j a_j$$

Códigos Lineares - revisão

- Código do ISBN-10:

$$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

$$\sum_{j=1}^{10} (11 - j) a_j = 0 \implies a_{10} = -\sum_{j=1}^{10} (11 - j) a_j = \sum_{j=1}^{10} j a_j$$

Dimensão 9 sobre $\mathbb{Z}_{11}$.

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código
  - k = dimensão do código (subespaço vetorial)

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código
  - k = dimensão do código (subespaço vetorial)
  - $d = d(C)$ = distância mínima = $\min\{\omega(\mathbf{c}); \mathbf{c} \in C, \mathbf{c} \neq 0\}$.

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código
  - k = dimensão do código (subespaço vetorial)
  - $d = d(C)$ = distância mínima = $\min\{\omega(\mathbf{c}); \mathbf{c} \in C, \mathbf{c} \neq 0\}$.
- Parâmetros “derivados”:

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código
  - k = dimensão do código (subespaço vetorial)
  - $d = d(C)$ = distância mínima = $\min\{\omega(\mathbf{c}); \mathbf{c} \in C, \mathbf{c} \neq 0\}$.
- Parâmetros “derivados”:
  - k/n = taxa (de informação) do código

Códigos lineares - revisão

- Parâmetros fundamentais de um código linear $C \subset \mathbb{F}^n$:
  - n = comprimento do código
  - k = dimensão do código (subespaço vetorial)
  - $d = d(C)$ = distância mínima = $\min\{\omega(\mathbf{c}); \mathbf{c} \in C, \mathbf{c} \neq 0\}$.
- Parâmetros "derivados":
  - k/n = taxa (de informação) do código
  - $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ = capacidade de correção do código

Matriz geradora

Matriz de paridade

Códigos Lineares: Matriz geradora

- Código C dado por $f : \mathbb{F}^k \to \mathbb{F}^n$ linear.

Códigos Lineares: Matriz geradora

- Código C dado por $f : \mathbb{F}^k \to \mathbb{F}^n$ linear.
- Matriz geradora:

$$G = \begin{pmatrix} f(\mathbf{e}_1) \\ \vdots \\ f(\mathbf{e}_k) \end{pmatrix}_{k \times n}$$

onde $\mathbf{e}_j = (0, 0, \ldots, 1, 0, \ldots, 0)$.

Códigos Lineares: Matriz geradora

- Código C dado por $f : \mathbb{F}^k \to \mathbb{F}^n$ linear.
- Matriz geradora:

$$G = \begin{pmatrix} f(\mathbf{e}_1) \\ \vdots \\ f(\mathbf{e}_k) \end{pmatrix}_{k \times n}$$

  onde $\mathbf{e}_j = (0, 0, \ldots, 1, 0, \ldots, 0)$.

- $$f(\mathbf{v}) = \mathbf{v} \cdot G.$$

Códigos Lineares: Matriz geradora

$$\begin{aligned}\mathbf{v} &= (a_1, \ldots, a_k) \\ &= (a_1, 0, \ldots, 0) + (a_1, 0, \ldots, 0) + \ldots + (0, 0, \ldots, a_k) \\ &= a_1\mathbf{e}_1 + \cdots + a_k\mathbf{e}_k\end{aligned}$$

Códigos Lineares: Matriz geradora

$$\begin{aligned}\mathbf{v} &= (a_1, \ldots, a_k) \\ &= (a_1, 0, \ldots, 0) + (a_1, 0, \ldots, 0) + \ldots + (0, 0, \ldots, a_k) \\ &= a_1\mathbf{e}_1 + \cdots + a_k\mathbf{e}_k\end{aligned}$$

logo

$$\begin{aligned}f((a_1, \ldots, a_k)) &= \\ &= f(a_1\mathbf{e}_1 + \cdots a_k\mathbf{e}_k) \\ &= a_1 f(\mathbf{e}_1) + \cdots a_k f(\mathbf{e}_k) \\ &= \mathbf{v} \cdot G\end{aligned}$$

Códigos Lineares: Matriz geradora

Exemplo: ISBN-10

- $$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

Códigos Lineares: Matriz geradora

Exemplo: ISBN-10

- $$f : \mathbb{Z}_{11}^{9} \to \mathbb{Z}_{11}^{10}, \quad (a_1, \ldots, a_9) \mapsto (a_1, \ldots, a_9, \sum_{j=1}^{9} j a_j)$$

- Matriz geradora 9×10 :

$$\begin{pmatrix} 1 & & & & & & & & & 1 \\ & 1 & & & & & & & & 2 \\ & & 1 & & & & & & & 3 \\ & & & 1 & & & & & & 4 \\ & & & & 1 & & & & & 5 \\ & & & & & 1 & & & & 6 \\ & & & & & & 1 & & & 7 \\ & & & & & & & 1 & & 8 \\ & & & & & & & & 1 & 9 \end{pmatrix}$$

Códigos Lineares: Matriz geradora

Exemplo: ISBN-10

- Veja que o formato é

$$G = [I_9 \mid \mathbf{v}],$$

I_9 a matriz identidade de ordem 9,
$\mathbf{v}$ é a matriz 9×1

$$\mathbf{v}^T = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$$

Códigos Lineares - matriz de paridade

- Todo código linear C em $\mathbb{F}^n$ com dimensão k pode ser escrito como o conjunto de soluções de um sistema linear

$$H\mathbf{x} = 0$$

em que H é matriz de ordem $n - k \times n$, de **posto máximo**: há um subdeterminante não-nulo de ordem $n - k$.

Códigos Lineares - matriz de paridade

- Todo código linear C em $\mathbb{F}^n$ com dimensão k pode ser escrito como o conjunto de soluções de um sistema linear

$$H\mathbf{x} = 0$$

em que H é matriz de ordem $n - k \times n$, de **posto máximo**: há um subdeterminante não-nulo de ordem $n - k$.

Códigos Lineares - matriz de paridade

- Todo código linear C em $\mathbb{F}^n$ com dimensão k pode ser escrito como o conjunto de soluções de um sistema linear

$$H\mathbf{x} = 0$$

em que H é matriz de ordem $n - k \times n$, de **posto máximo**: há um subdeterminante não-nulo de ordem $n - k$.

Dizemos que C é o núcleo da matriz H.

Códigos Lineares - matriz de paridade

- Todo código linear C em $\mathbb{F}^n$ com dimensão k pode ser escrito como o conjunto de soluções de um sistema linear

$$H\mathbf{x} = 0$$

em que H é matriz de ordem $n - k \times n$, de **posto máximo**: há um subdeterminante não-nulo de ordem $n - k$.

Dizemos que C é o núcleo da matriz H.

H é uma matriz de paridade de C (“parity check matrix”).

Códigos Lineares - matriz de paridade

- O código de repetição de comprimento $2m+1$ é o núcleo da matriz

$$\begin{bmatrix} U & I_{2m} \end{bmatrix}$$

em que U é a matriz coluna $A = [11\ldots1]^T$.

Para $m = 1$,

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Códigos Lineares - matriz de paridade

- O código de repetição de comprimento $2m+1$ é o núcleo da matriz

$$\begin{bmatrix} U & I_{2m} \end{bmatrix}$$

em que U é a matriz coluna $A = [11\ldots1]^T$.

Para $m = 1$,

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

- O código do ISBN-10 tem a matriz de paridade 1×10

$$\begin{bmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Códigos Lineares - matriz de paridade

Para o ISBN-10, que tem $k = 9$ e $n = 10$, logo $n - k = 1$,

- Uma matriz geradora é da forma

$$G = [I_9 \mid \mathbf{v}]$$

Códigos Lineares - matriz de paridade

Para o ISBN-10, que tem $k = 9$ e $n = 10$, logo $n - k = 1$,

- Uma matriz geradora é da forma

$$G = [I_9 \mid \mathbf{v}]$$

- Uma matriz de paridade é

$$H = \begin{bmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & -2 & -3 & -4 & -5 & -6 & -7 & -8 & -9 & 1 \end{bmatrix}$$

$$= [-\mathbf{v}^T \mid I_1]$$

Códigos Lineares - matriz de paridade

Teorema

C código linear.

- Se *G* é matriz geradora e *H* é matriz de paridade então

$$H \cdot G^T = \mathbf{0}.$$

Códigos Lineares - matriz de paridade

Teorema

C código linear.

- Se G é matriz geradora e H é matriz de paridade então

$$H \cdot G^T = \mathbf{0}.$$

- $G = [I_k \mid A]$ é matriz geradora de C

$$\Longleftrightarrow$$

$H = [-A^T \mid I_{n-k}]$ é matriz de paridade de C.

Códigos Lineares - Decodificação por síndrome

- Fixada matriz de paridade H, a síndrome de $\mathbf{v} \in \mathbb{F}^n$ é

$$H \cdot \mathbf{v}.$$

Códigos Lineares - Decodificação por síndrome

- Fixada matriz de paridade H, a síndrome de $\mathbf{v} \in \mathbb{F}^n$ é

$$H \cdot \mathbf{v}.$$

- Se existe $\mathbf{r} \in \mathbb{F}^n$ tal que

$$H \cdot \mathbf{r} = H \cdot \mathbf{v}, \quad \omega(\mathbf{r}) \leq t$$

então tal $\mathbf{r}$ tem o menor peso com essas condições, e é único.

Códigos Lineares - Decodificação por síndrome

- Fixada matriz de paridade H, a síndrome de $\mathbf{v} \in \mathbb{F}^n$ é

$$H \cdot \mathbf{v}.$$

- Se existe $\mathbf{r} \in \mathbb{F}^n$ tal que

$$H \cdot \mathbf{r} = H \cdot \mathbf{v}, \quad \omega(\mathbf{r}) \leq t$$

então tal $\mathbf{r}$ tem o menor peso com essas condições, e é único.

- De fato, se $\mathbf{r}'$ satisfaz as mesmas duas condições,

$$H\mathbf{r} = H\mathbf{r}' \implies H(\mathbf{r} - \mathbf{r}') = \mathbf{0} \implies \mathbf{r} - \mathbf{r}' \in C.$$

Códigos Lineares - Decodificação por síndrome

- Fixada matriz de paridade H, a síndrome de $\mathbf{v} \in \mathbb{F}^n$ é

$$H \cdot \mathbf{v}.$$

- Se existe $\mathbf{r} \in \mathbb{F}^n$ tal que

$$H \cdot \mathbf{r} = H \cdot \mathbf{v}, \quad \omega(\mathbf{r}) \leq t$$

então tal $\mathbf{r}$ tem o menor peso com essas condições, e é único.

- De fato, se $\mathbf{r}'$ satisfaz as mesmas duas condições,

$$H\mathbf{r} = H\mathbf{r}' \implies H(\mathbf{r} - \mathbf{r}') = \mathbf{0} \implies \mathbf{r} - \mathbf{r}' \in C.$$

- Logo

$$\omega(\mathbf{r} - \mathbf{r}') = d(\mathbf{r}, \mathbf{r}') \leq \omega(\mathbf{r}) + \omega(\mathbf{r}') \leq 2t < d(C),$$

contradição.

Códigos Lineares - Decodificação por síndrome

Decodificação por síndrome: dado $\mathbf{v} \in \mathbb{F}^n$,

- Calcule $H\mathbf{v}$.

Códigos Lineares - Decodificação por síndrome

Decodificação por síndrome: dado $\mathbf{v} \in \mathbb{F}^n$,

- Calcule $H\mathbf{v}$.
- Se $H\mathbf{v} = \mathbf{0}$ então $\mathbf{v} \in C$.

Códigos Lineares - Decodificação por síndrome

Decodificação por síndrome: dado $\mathbf{v} \in \mathbb{F}^n$,

- Calcule $H\mathbf{v}$.
- Se $H\mathbf{v} = \mathbf{0}$ então $\mathbf{v} \in C$.
- Se $H\mathbf{v} \neq \mathbf{0}$ mas existe $\mathbf{r} \in \mathbb{F}^n$ tal que

$$H\mathbf{v} = H\mathbf{r}, \quad \omega(\mathbf{r}) \leq t,$$

faça $\mathbf{c} = \mathbf{v} - \mathbf{r}$.

Códigos Lineares - Decodificação por síndrome

Decodificação por síndrome: dado $\mathbf{v} \in \mathbb{F}^n$,

- Calcule $H\mathbf{v}$.
- Se $H\mathbf{v} = \mathbf{0}$ então $\mathbf{v} \in C$.
- Se $H\mathbf{v} \neq \mathbf{0}$ mas existe $\mathbf{r} \in \mathbb{F}^n$ tal que

$$H\mathbf{v} = H\mathbf{r}, \quad \omega(\mathbf{r}) \leq t,$$

  faça $\mathbf{c} = \mathbf{v} - \mathbf{r}$.
- Se $H\mathbf{v} \neq \mathbf{0}$ e

$$H\mathbf{v} = H\mathbf{r} \implies \omega(\mathbf{r}) > t,$$

  ocorreram erros além da capacidade de correção de C.

Códigos de Hamming

Códigos de Hamming (R. Hamming, 1947)

- Seja $\mathcal{H}_3 \subset (\mathbb{F}_2)^7$ o núcleo da matriz

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

cujas colunas são todos os elementos não-nulos de $(\mathbb{F}_2)^3$, que também são as expansões binárias dos números de 1 a 7.

Códigos de Hamming

$$1 = 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

Códigos de Hamming

$$1 = 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$
$$2 = 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$
$$3 = 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$
$$4 = 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$$
$$5 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$
$$6 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$
$$7 = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Códigos de Hamming

- Seja $\mathcal{H}_3 \subset (\mathbb{F}_2)^7$ o núcleo da matriz

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

  cujas colunas são todos os elementos não-nulos de $(\mathbb{F}_2)^3$, que também são as expansões binárias dos números de 1 a 7.

- $\text{posto}(H) = 3 \implies k = 4$.

Códigos de Hamming

- Seja $\mathcal{H}_3 \subset (\mathbb{F}_2)^7$ o núcleo da matriz

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

  cujas colunas são todos os elementos não-nulos de $(\mathbb{F}_2)^3$, que também são as expansões binárias dos números de 1 a 7.

- $\text{posto}(H) = 3 \implies k = 4$.
- $d = 3$.

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

$$H\mathbf{v}^T = a_1\mathbf{h}_1 + \cdots + a_n\mathbf{h}_n.$$

- O elemento $(1, 1, 1, 0, 0, 0, 0)$ está no código $\Longrightarrow$ $d \leq 3$

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

$$H\mathbf{v}^T = a_1\mathbf{h}_1 + \cdots + a_n\mathbf{h}_n.$$

- O elemento $(1, 1, 1, 0, 0, 0, 0)$ está no código $\Longrightarrow$ $d \leq 3$
- Não há duas colunas iguais $\Longrightarrow$ não há elemento de peso 2

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

$$H\mathbf{v}^T = a_1\mathbf{h}_1 + \cdots + a_n\mathbf{h}_n.$$

- O elemento $(1, 1, 1, 0, 0, 0, 0)$ está no código $\Longrightarrow$ $d \leq 3$
- Não há duas colunas iguais $\Longrightarrow$ não há elemento de peso 2
- Não há coluna nula $\Longrightarrow$ não há elemento de peso 1.

Códigos de Hamming

- Observe que se as colunas de uma matriz H são

$$\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$$

e $\mathbf{v} = (a_1, \ldots, a_n)$, então

$$H\mathbf{v}^T = a_1\mathbf{h}_1 + \cdots + a_n\mathbf{h}_n.$$

- O elemento $(1, 1, 1, 0, 0, 0, 0)$ está no código $\Longrightarrow$ $d \leq 3$
- Não há duas colunas iguais $\Longrightarrow$ não há elemento de peso 2
- Não há coluna nula $\Longrightarrow$ não há elemento de peso 1.
- $\mathcal{H}_3$ é o código de Hamming $\mathcal{H}_3$ de parâmetros $[7, 4, 3]$.

Códigos de Hamming

Processo de decodificação/correção (decodificação por síndrome):

- vetor recebido com 1 erro: $\mathbf{r} = \mathbf{c} + \mathbf{e}_j$

Códigos de Hamming

Processo de decodificação/correção (decodificação por síndrome):

- vetor recebido com 1 erro: $\mathbf{r} = \mathbf{c} + \mathbf{e}_j$
- $$H\mathbf{r} = H\mathbf{c} + H\mathbf{e}_j = \mathbf{h}_j$$

Códigos de Hamming

Processo de decodificação/correção (decodificação por síndrome):

- vetor recebido com 1 erro: $\mathbf{r} = \mathbf{c} + \mathbf{e}_j$
- $$H\mathbf{r} = H\mathbf{c} + H\mathbf{e}_j = \mathbf{h}_j$$
- a j-ésima coluna é a expansão binária de j

Códigos de Hamming

Processo de decodificação/correção (decodificação por síndrome):

- vetor recebido com 1 erro: $\mathbf{r} = \mathbf{c} + \mathbf{e}_j$
- $$H\mathbf{r} = H\mathbf{c} + H\mathbf{e}_j = \mathbf{h}_j$$
- a j-ésima coluna é a expansão binária de j
- correção: $\mathbf{r} \mapsto \mathbf{r} - \mathbf{e}_j = \mathbf{c}$.

Códigos de Hamming de comprimento maior (M.Golay, 1949)

- H_m é uma matriz cujas colunas são os elementos não-nulos de $(\mathbb{F}_2)^m$
- $d = 3$, logo $t = 1$
- $n = 2^m - 1$
- $k = 2^m - m - 1$.

Códigos de Hamming de comprimento maior (M.Golay, 1949)

- H_m é uma matriz cujas colunas são os elementos não-nulos de $(\mathbb{F}_2)^m$
- $d = 3$, logo $t = 1$
- $n = 2^m - 1$
- $k = 2^m - m - 1$.
- taxa: $\dfrac{2^m - m - 1}{2^m - 1} = 1 - \dfrac{m}{2^m - 1}$.

Códigos de Hamming não-binários (M.Golay, 1949)

- Corpo $\mathbb{F}_q$
- Matriz $H_{q,m}$: bijeção

$$\text{colunas de } H_{q,m} \iff \text{retas em } (\mathbb{F}_q)^m$$

- $d = 3$, logo $t = 1$
- $n = \dfrac{q^m - 1}{q - 1}$
- $k = \dfrac{q^m - 1}{q - 1} - m.$

Códigos de Hamming não-binários (M.Golay, 1949)

- Corpo $\mathbb{F}_q$
- Matriz $H_{q,m}$: bijeção

$$\text{colunas de } H_{q,m} \iff \text{retas em } (\mathbb{F}_q)^m$$

- $d = 3$, logo $t = 1$
- $n = \dfrac{q^m - 1}{q - 1}$
- $k = \dfrac{q^m - 1}{q - 1} - m.$
- taxa: $1 - \dfrac{m}{q^m - 1}.$

Matriz geradora e forma sistemática

Matriz geradora

Os códigos C e C' são equivalentes se C' é obtido de C por

1. permutação de coordenadas;
2. multiplicação de coordenadas por escalares.

Matriz geradora

Os códigos C e C' são equivalentes se C' é obtido de C por

1. permutação de coordenadas;
2. multiplicação de coordenadas por escalares.

Dois códigos equivalentes têm os mesmos parâmetros n, k, d.

Matriz geradora

Teorema

1. Todo código linear é equivalente a um código com matriz geradora da forma

$$\left[I_k \mid A \right]$$

Matriz geradora

Teorema

1. Todo código linear é equivalente a um código com matriz geradora da forma
$$\left[I_k \mid A \right]$$
2. $G = [I_k \mid A]$ é matriz geradora de C
$\Longleftrightarrow$
$H = [-A^T \mid I_{n-k}]$ é matriz de paridade de C.

Matriz geradora

Teorema

1. Todo código linear é equivalente a um código com matriz geradora da forma
$$\left[I_k \mid A \right]$$
2. $G = [I_k \mid A]$ é matriz geradora de C
$\Longleftrightarrow$
$H = [-A^T \mid I_{n-k}]$ é matriz de paridade de C.

Matriz geradora

Teorema

1. Todo código linear é equivalente a um código com matriz geradora da forma
$$\left[I_k \mid A \right]$$
2. $G = [I_k \mid A]$ é matriz geradora de C
$\Longleftrightarrow$
$H = [-A^T \mid I_{n-k}]$ é matriz de paridade de C.

O código está na forma sistemática se tomamos G como em (1).

Forma sistemática para $\mathcal{H}_3$

- Permutação de coordenadas corresponde a permutação de colunas na matriz de paridade.

Forma sistemática para $\mathcal{H}_3$

- Permutação de coordenadas corresponde a permutação de colunas na matriz de paridade.
-

$$\left[\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right] \mapsto \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Forma sistemática para $\mathcal{H}_3$

- Permutação de coordenadas corresponde a permutação de colunas na matriz de paridade.
-

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \mapsto \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

- A segunda matriz está na forma

$$H = [B \mid I_3].$$

Forma sistemática para $\mathcal{H}_3$

- $$H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] = [B \mid I_3].$$

Forma sistemática para $\mathcal{H}_3$

- $$H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] = [B \mid I_3].$$
- $G = [I_4 | B^T]$,

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Forma sistemática para $\mathcal{H}_3$

- $G = [I_4|B^T]$,

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Forma sistemática para $\mathcal{H}_3$

- $G = [I_4|B^T]$,

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

- Codificação sistemática:

$$(d_1, d_2, d_3, d_4) \mapsto$$

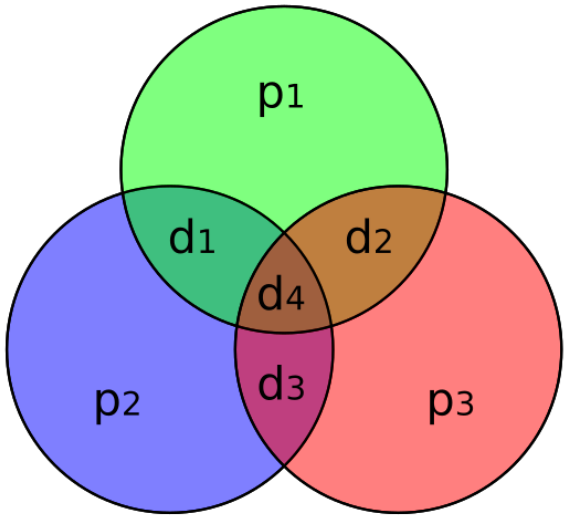
$$(d_1, d_2, d_3, d_4 \mid \underbrace{d_2 + d_3 + d_4}, \underbrace{d_1 + d_3 + d_4}, \underbrace{d_1 + d_2 + d_4})$$

Forma sistemática para $\mathcal{H}_3$

Codificação sistemática:

$$(d_1, d_2, d_3, d_4) \mapsto$$

$$(d_1, d_2, d_3, d_4 \mid \underbrace{d_2 + d_3 + d_4}, \underbrace{d_1 + d_3 + d_4}, \underbrace{d_1 + d_2 + d_4})$$



(https://en.wikipedia.org/wiki/Hamming_code)

Códigos perfeitos

Códigos perfeitos

Um código C com capacidade de correção t é perfeito se

$$\mathbf{v} \in \mathbb{F}^n \implies d(\mathbf{v}, \mathbf{c}) \leq t \text{ para algum } \mathbf{c} \in C.$$

Códigos perfeitos

Um código C com capacidade de correção t é perfeito se

$$\mathbf{v} \in \mathbb{F}^n \implies d(\mathbf{v}, \mathbf{c}) \leq t \text{ para algum } \mathbf{c} \in C.$$

($\mathbf{c}$ é necessariamente único)

Códigos perfeitos

Um código C com capacidade de correção t é perfeito se

$$\mathbf{v} \in \mathbb{F}^n \implies d(\mathbf{v}, \mathbf{c}) \leq t \text{ para algum } \mathbf{c} \in C.$$

($\mathbf{c}$ é necessariamente único)

contra-exemplo: o código de repetição de comprimento 4.

Códigos perfeitos

Um código C com capacidade de correção t é perfeito se

$$\mathbf{v} \in \mathbb{F}^n \implies d(\mathbf{v}, \mathbf{c}) \leq t \text{ para algum } \mathbf{c} \in C.$$

($\mathbf{c}$ é necessariamente único)

contra-exemplo: o código de repetição de comprimento 4.

- $t = 1$
- $d((0,0,1,1), \mathbf{c}) > 1$ para todo $\mathbf{c} \in C$.

Códigos perfeitos

Geometricamente:

- Dado $r \geq 0$, $\mathbf{u} \in \mathbb{F}^n$,

$$B(\mathbf{u}, r) = \{\mathbf{v} \in \mathbb{F}^n; d(\mathbf{u}, \mathbf{v}) \leq r\}.$$

Códigos perfeitos

Geometricamente:

- Dado $r \geq 0$, $\mathbf{u} \in \mathbb{F}^n$,

$$B(\mathbf{u}, r) = \{\mathbf{v} \in \mathbb{F}^n; d(\mathbf{u}, \mathbf{v}) \leq r\}.$$

- Pela definição de capacidade de correção (e pela desigualdade triangular), se C tem capacidade de correção t então

$$B(\mathbf{c}, t) \cap B(\mathbf{c}', t) = \varnothing$$

quando $\mathbf{c}, \mathbf{c}'$ são palavras distintas de C.

Códigos perfeitos

Geometricamente:

- Dado $r \geq 0$, $\mathbf{u} \in \mathbb{F}^n$,

$$B(\mathbf{u}, r) = \{\mathbf{v} \in \mathbb{F}^n; d(\mathbf{u}, \mathbf{v}) \leq r\}.$$

- Pela definição de capacidade de correção (e pela desigualdade triangular), se C tem capacidade de correção t então

$$B(\mathbf{c}, t) \cap B(\mathbf{c}', t) = \varnothing$$

quando $\mathbf{c}, \mathbf{c}'$ são palavras distintas de C.

- C é perfeito se

$$\mathbb{F}^n = \bigcup_{\mathbf{c} \in C} B(\mathbf{c}, t).$$

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$
- $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ vetor de peso r, $\mathbf{v} \notin \mathcal{H}_m$.

$$H_m\mathbf{v} = \mathbf{h}_{i_1} v_{i_1} + \cdots + \mathbf{h}_{i_r} v_{i_r} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} \neq \mathbf{0}$$

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$
- $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ vetor de peso r, $\mathbf{v} \notin \mathcal{H}_m$.

$$H_m\mathbf{v} = \mathbf{h}_{i_1} v_{i_1} + \cdots + \mathbf{h}_{i_r} v_{i_r} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} \neq \mathbf{0}$$

- Cada elemento não-nulo de $\mathbb{F}^{2m}$ aparece como uma coluna de H_m.

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$
- $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ vetor de peso r, $\mathbf{v} \notin \mathcal{H}_m$.

$$H_m\mathbf{v} = \mathbf{h}_{i_1} v_{i_1} + \cdots + \mathbf{h}_{i_r} v_{i_r} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} \neq \mathbf{0}$$

- Cada elemento não-nulo de $\mathbb{F}^{2m}$ aparece como uma coluna de H_m.

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$
- $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ vetor de peso r, $\mathbf{v} \notin \mathcal{H}_m$.

$$H_m\mathbf{v} = \mathbf{h}_{i_1} v_{i_1} + \cdots + \mathbf{h}_{i_r} v_{i_r} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} \neq \mathbf{0}$$

- Cada elemento não-nulo de $\mathbb{F}^{2m}$ aparece como uma coluna de H_m. Logo, existe um índice s tal que

$$\begin{aligned} H_m\mathbf{v} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} = \mathbf{h}_{i_s} &= H_m\mathbf{e}_{i_s} \\ \Longrightarrow \quad H_m(\mathbf{v} - \mathbf{e}_{i_s}) &= \mathbf{0} \\ \Longrightarrow \quad \mathbf{v} &= (\mathbf{v} - \mathbf{e}_{i_s}) + \mathbf{e}_{i_s} \end{aligned}$$

Códigos perfeitos

O código binário de Hamming $\mathcal{H}_m$ é perfeito.

- $t = 1$
- $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ vetor de peso r, $\mathbf{v} \notin \mathcal{H}_m$.

$$H_m\mathbf{v} = \mathbf{h}_{i_1} v_{i_1} + \cdots + \mathbf{h}_{i_r} v_{i_r} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} \neq \mathbf{0}$$

- Cada elemento não-nulo de $\mathbb{F}^{2m}$ aparece como uma coluna de H_m. Logo, existe um índice s tal que

$$\begin{aligned} H_m\mathbf{v} = \mathbf{h}_{i_1} + \cdots + \mathbf{h}_{i_r} = \mathbf{h}_{i_s} &= H_m\mathbf{e}_{i_s} \\ \Longrightarrow \quad H_m(\mathbf{v} - \mathbf{e}_{i_s}) &= \mathbf{0} \\ \Longrightarrow \quad \mathbf{v} &= (\mathbf{v} - \mathbf{e}_{i_s}) + \mathbf{e}_{i_s} \end{aligned}$$

com $\mathbf{c} = \mathbf{v} - \mathbf{e}_{i_s} \in C$, e $d(\mathbf{v}, \mathbf{c}) = 1$.

Códigos perfeitos

Teorema

Os códigos lineares perfeitos binários são

- Os códigos triviais (nulo, $\mathbb{F}_2^n$, repetição $[2n+1, 1, 2n+1]$);
- Os códigos de Hamming $\mathcal{H}_m$ $[2^m - 1, 2^m - m - 1, 3]$;
- O código binário de Golay $\mathcal{G}_{24}$ $[23, 12, 7]$.

Códigos perfeitos

Teorema

Os códigos lineares perfeitos q-ários são

- Os códigos triviais;
- Os códigos de Hamming $\mathcal{H}_{q,m}$ $[q^m - 1/q - 1, q^m - 1/q - 1 - m, 3]_q$;
- O código ternário de Golay $\mathcal{G}_{11}$ $[11, 6, 5]_3$.

references

- 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.