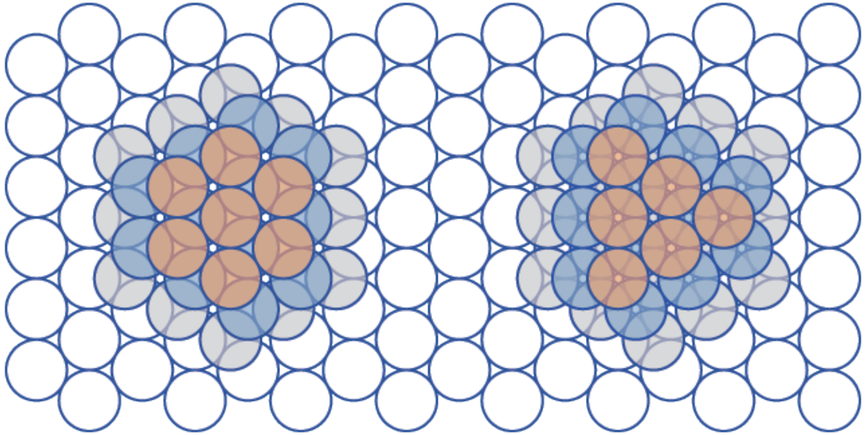
A vida secreta dos polinómios



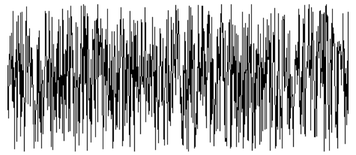
João Ribeiro

IT & IST

O problema da comunicação com ruído

Jantamos às 8!

canal com ruído

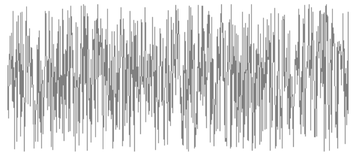


Jintamms bs 9!

O problema da comunicação com ruído

Jantamos às 8!

canal com ruído

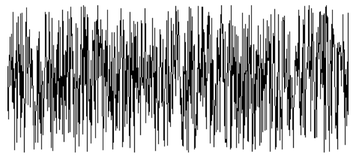


Jintamms bs 9!

m

comprimento k

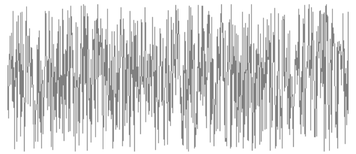
canal com ruído



O problema da comunicação com ruído

Jantamos às 8!

canal com ruído



Jintamms bs 9!

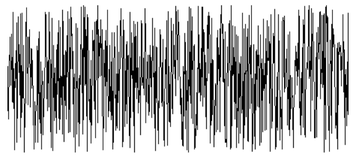
m

comprimento k

codificação

$\longrightarrow \quad c \in C$

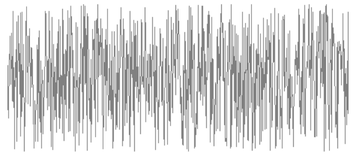
canal com ruído



O problema da comunicação com ruído

Jantamos às 8!

canal com ruído



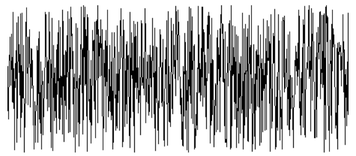
Jintamms bs 9!

codificação

$m \longrightarrow c \in C$

comprimento k comprimento $n > k$

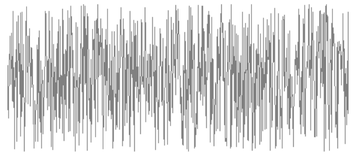
canal com ruído



O problema da comunicação com ruído

Jantamos às 8!

canal com ruído



Jintamms bs 9!

m

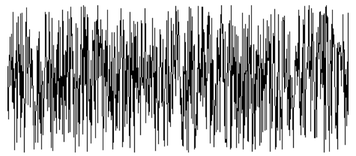
comprimento k

codificação

$c \in C$

comprimento $n > k$

canal com ruído

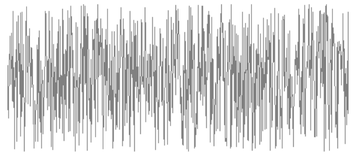


$\tilde{c}$

O problema da comunicação com ruído

Jantamos às 8!

canal com ruído



Jintamms bs 9!

m

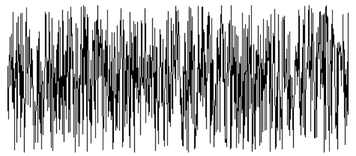
comprimento k

codificação

$c \in C$

comprimento $n > k$

canal com ruído



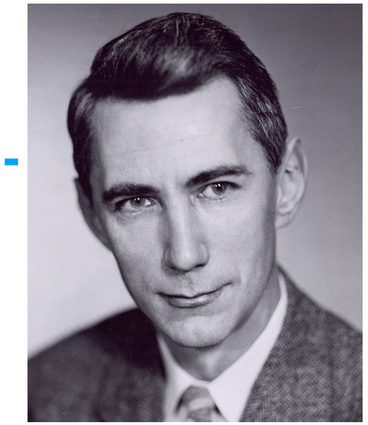
$\tilde{c}$

descodificação

m

Modelos de erro

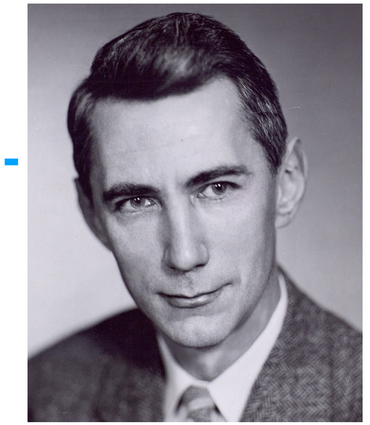
Modelos de erro



A perspectiva probabilística (Shannon)

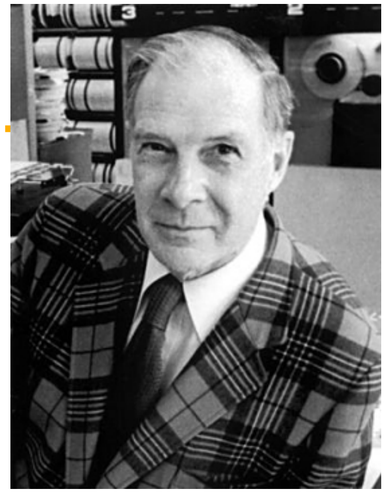
- Canal introduz erros aleatórios:
  - Cada símbolo rasurado de forma independente com probabilidade p;
  - Cada símbolo substituído por outro de forma independente com probabilidade p.

Modelos de erro



A perspectiva probabilística (Shannon)

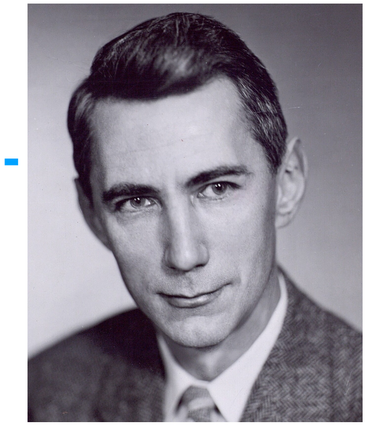
- Canal introduz erros aleatórios:
  - Cada símbolo rasurado de forma independente com probabilidade p;
  - Cada símbolo substituído por outro de forma independente com probabilidade p.



A perspectiva combinatorial (Hamming)

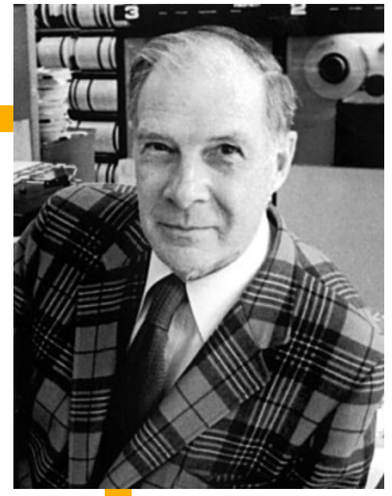
- Canal introduz um número limitado t de erros de forma adversarial:
  - Canal pode rasurar quaisquer t símbolos;
  - Canal pode substituir quaisquer t símbolos por quaisquer outros símbolos.

Modelos de erro



A perspectiva probabilística (Shannon)

- Canal introduz erros aleatórios:
  - Cada símbolo rasurado de forma independente com probabilidade p;
  - Cada símbolo substituído por outro de forma independente com probabilidade p.



A perspectiva combinatorial (Hamming)

- Canal introduz um número limitado t de erros de forma adversarial:
  - Canal pode rasurar quaisquer t símbolos;
  - Canal pode substituir quaisquer t símbolos por quaisquer outros símbolos.

A geometria dos erros

A geometria dos erros

Distância de Hamming:

$$d(c, \tilde{c}) = |\{i : c_i \neq \tilde{c}_i\}| = \text{nr. coordenadas em que } c \text{ e } \tilde{c} \text{ diferem}$$

A geometria dos erros

Distância de Hamming:

$$d(c, \tilde{c}) = |\{i : c_i \neq \tilde{c}_i\}| = \text{nr. coordenadas em que } c \text{ e } \tilde{c} \text{ diferem}$$

$$B(c, t) = \{\tilde{c} \in \Sigma^n : d(c, \tilde{c}) \leq t\}$$

A geometria dos erros

$c \in \Sigma^n \longrightarrow$ [$\leq t$ erros de substituição] $\longrightarrow \tilde{c} \in \Sigma^n$

Distância de Hamming:

$$d(c, \tilde{c}) = |\{i : c_i \neq \tilde{c}_i\}| = \text{nr. coordenadas em que } c \text{ e } \tilde{c} \text{ diferem}$$

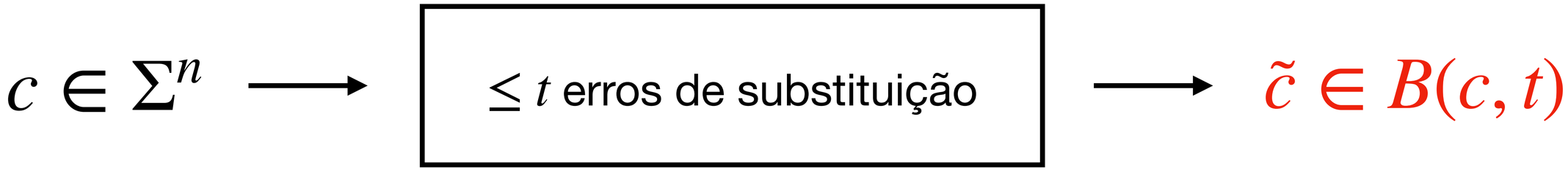
$$B(c, t) = \{\tilde{c} \in \Sigma^n : d(c, \tilde{c}) \leq t\}$$

$c \in \Sigma^n \longrightarrow$ [$\leq t$ erros de substituição] $\longrightarrow \tilde{c} \in B(c, t)$

Códigos = Empacotamentos de esferas

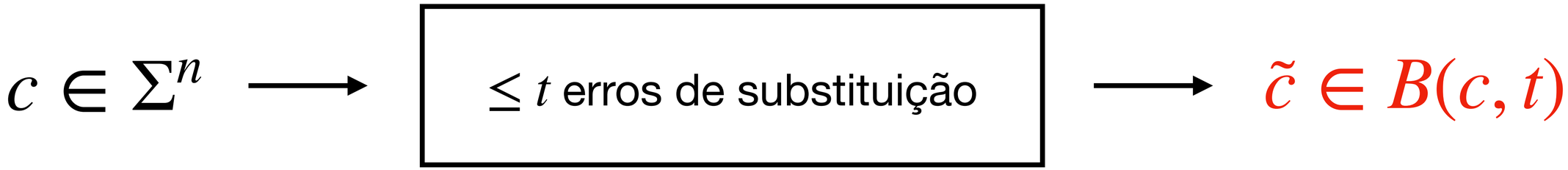
$c \in \Sigma^n$ ⟶ $\leq t$ erros de substituição ⟶ $\tilde{c} \in B(c, t)$

Códigos = Empacotamentos de esferas



- Um código com comprimento n e alfabeto Σ é um subconjunto $C \subseteq \Sigma^n$.

Códigos = Empacotamentos de esferas



- Um código com comprimento n e alfabeto Σ é um subconjunto $C \subseteq \Sigma^n$.
- C corrige t erros se $B(c,t) \cap B(c',t) = \varnothing$ para quaisquer $c, c' \in C$ distintos.

Códigos = Empacotamentos de esferas

$c \in \Sigma^n \longrightarrow$ $\leq t$ erros de substituição $\longrightarrow \tilde{c} \in B(c, t)$

- Um código com comprimento n e alfabeto Σ é um subconjunto $C \subseteq \Sigma^n$.
- C corrige t erros se $B(c, t) \cap B(c', t) = \emptyset$ para quaisquer $c, c' \in C$ distintos.

$$\min_{c,c' \in C : c \neq c'} d(c, c') \geq d \iff C \text{ corrige } t = \left\lfloor \frac{d-1}{2} \right\rfloor \text{erros.}$$

Códigos = Empacotamentos de esferas

$c \in \Sigma^n \longrightarrow$ $\leq t$ erros de substituição $\longrightarrow \tilde{c} \in B(c, t)$

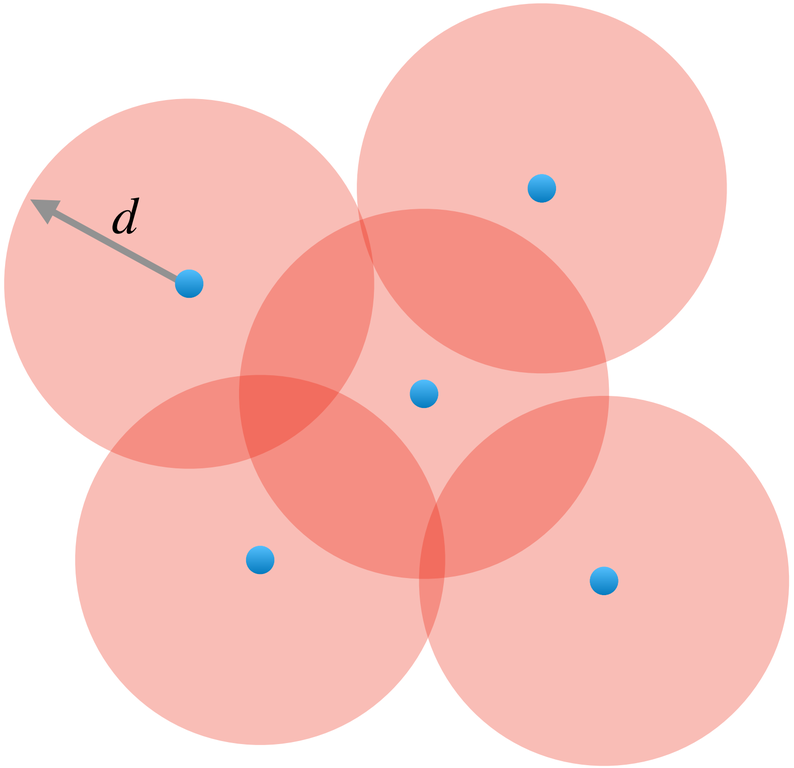
- Um código com comprimento n e alfabeto Σ é um subconjunto $C \subseteq \Sigma^n$.
- C corrige t erros se $B(c, t) \cap B(c', t) = \emptyset$ para quaisquer $c, c' \in C$ distintos.

$$\min_{c,c' \in C : c \neq c'} d(c, c') \geq d \iff C \text{ corrige } t = \left\lfloor \frac{d-1}{2} \right\rfloor \text{erros.}$$

distância mínima de C

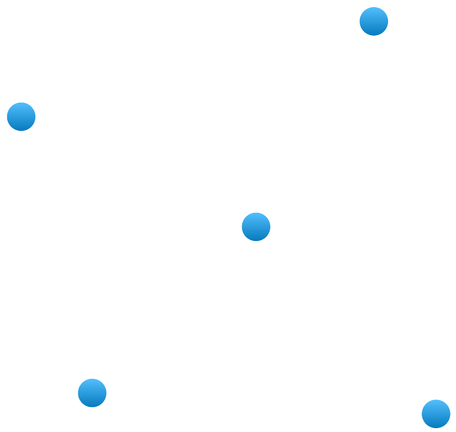
Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$



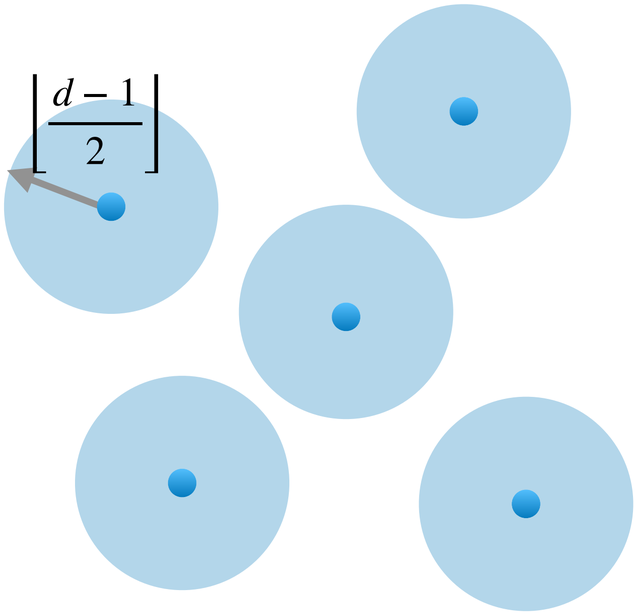
Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$



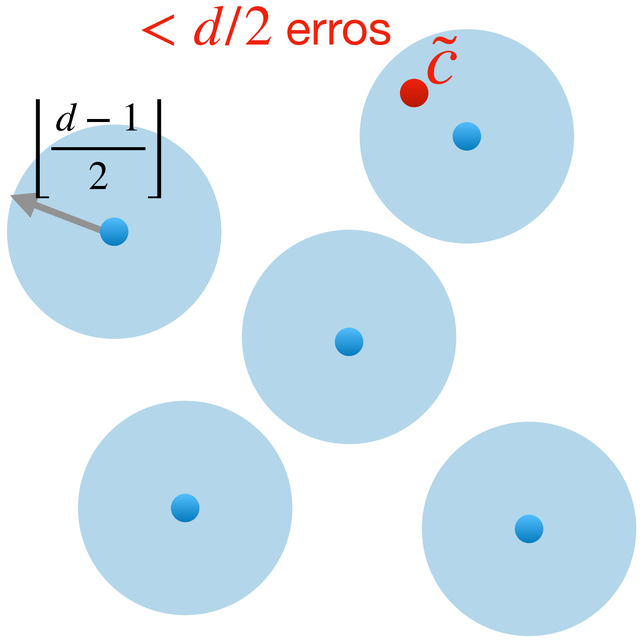
Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$



Códigos = Empacotamentos de esferas

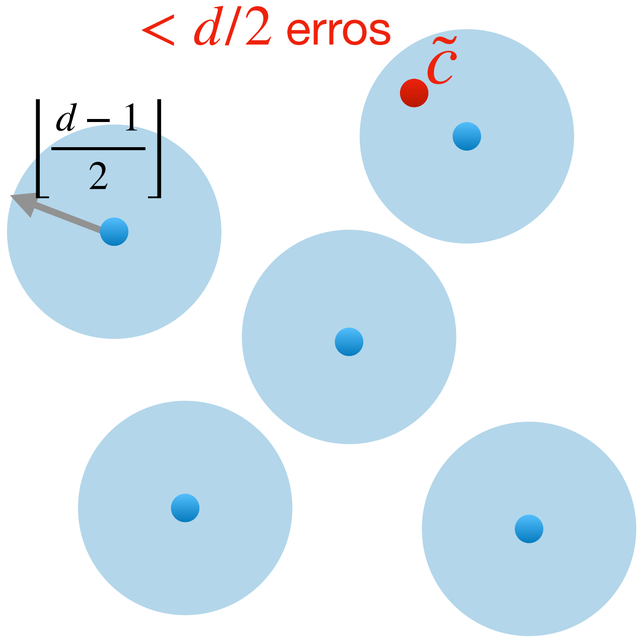
Código com distância mínima $\geq d$



Códigos = Empacotamentos de esferas

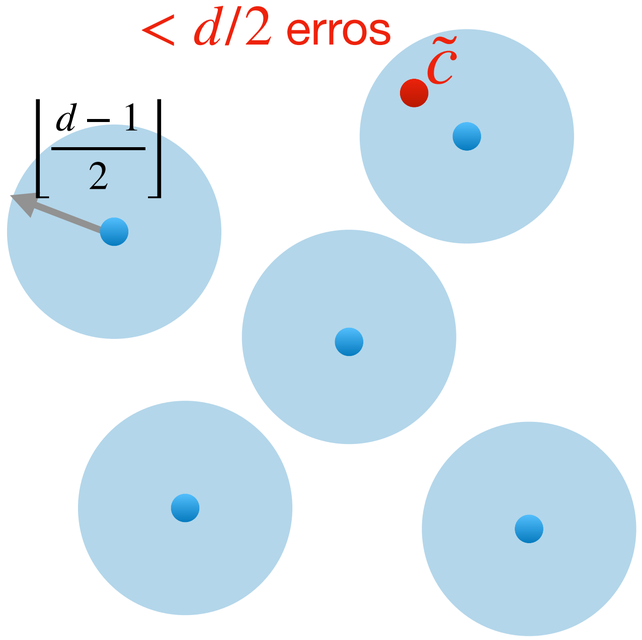
Código com distância mínima $\geq d$

Empacotar mais esferas $\Longrightarrow$ **Mais mensagens que podemos transmitir**



Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$

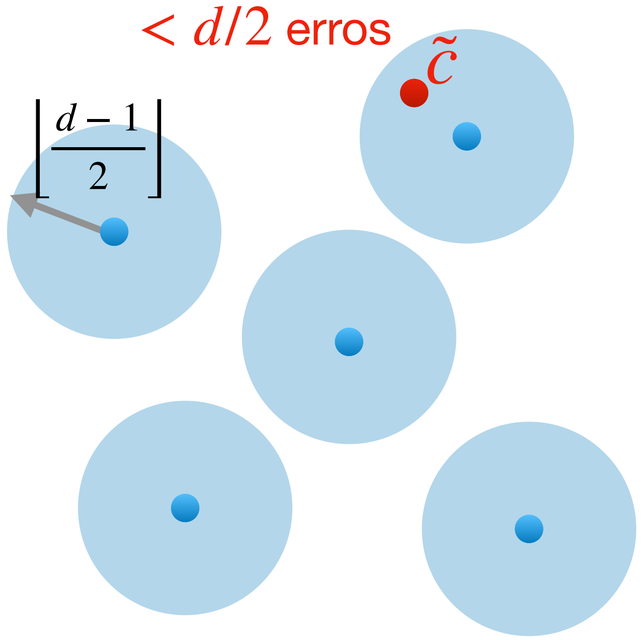


Empacotar mais esferas $\Longrightarrow$ **Mais mensagens que podemos transmitir**

As questões mais básicas:

Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$



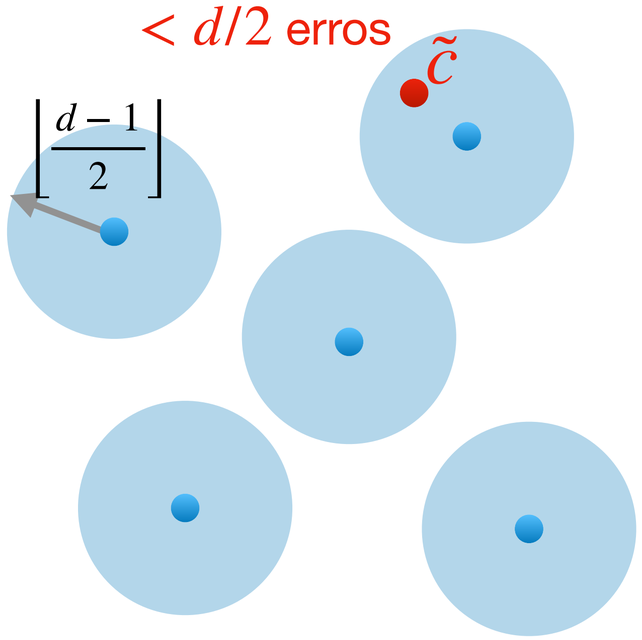
Empacotar mais esferas $\Longrightarrow$ **Mais mensagens que podemos transmitir**

As questões mais básicas:

- Qual o tamanho do maior código com comprimento n, tamanho de alfabeto q, e distância mínima d ?

Códigos = Empacotamentos de esferas

Código com distância mínima $\geq d$



Empacotar mais esferas $\Longrightarrow$ **Mais mensagens que podemos transmitir**

As questões mais básicas:

- Qual o tamanho do maior código com comprimento n, tamanho de alfabeto q, e distância mínima d ?
- Conseguimos desenvolver algoritmos de codificação e descodificação eficientes?

Desigualdade de Singleton

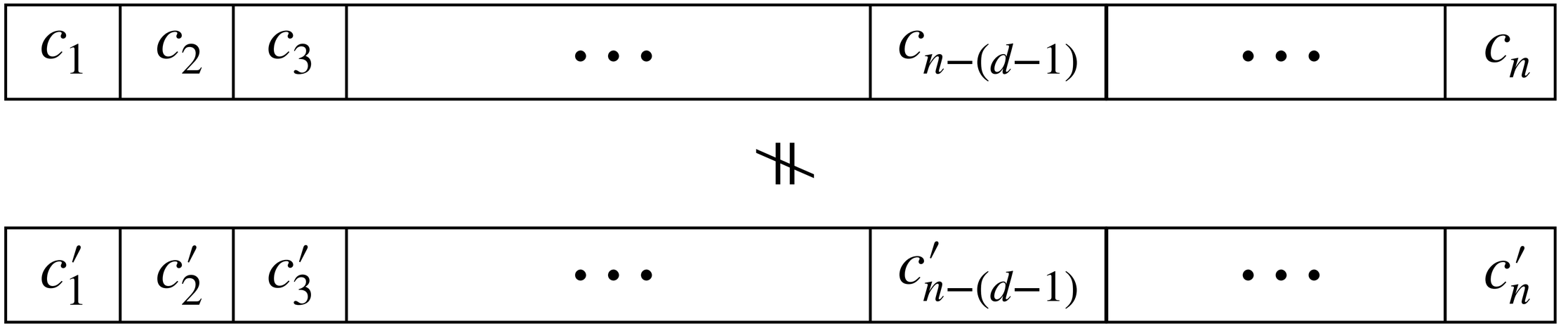
Qualquer código $C \subseteq \Sigma^n$ com $q = |\Sigma|$ e distância mínima d satisfaz

$$|C| \leq q^{n-(d-1)}.$$

Desigualdade de Singleton

Qualquer código $C \subseteq \Sigma^n$ com $q = |\Sigma|$ e distância mínima d satisfaz

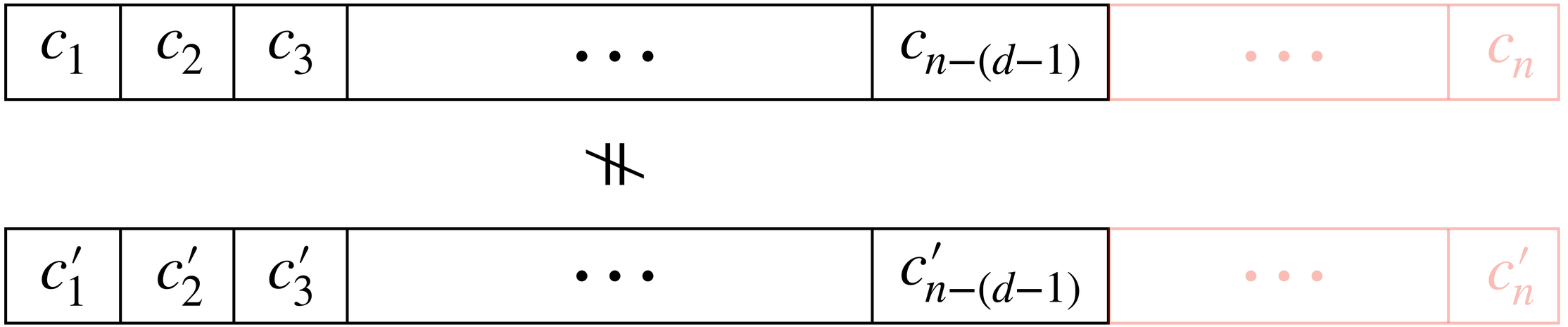
$$|C| \leq q^{n-(d-1)}.$$



Desigualdade de Singleton

Qualquer código $C \subseteq \Sigma^n$ com $q = |\Sigma|$ e distância mínima d satisfaz

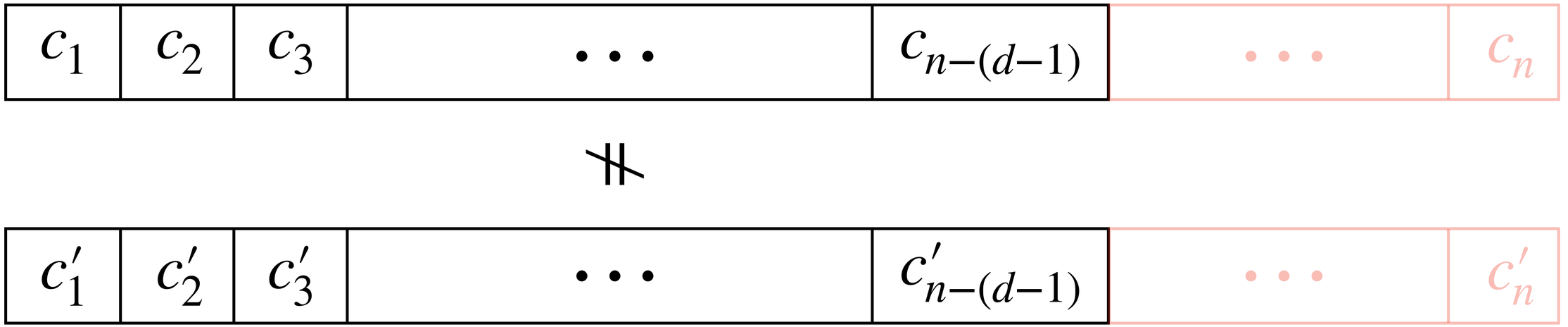
$$|C| \leq q^{n-(d-1)}.$$



Desigualdade de Singleton

Qualquer código $C \subseteq \Sigma^n$ com $q = |\Sigma|$ e distância mínima d satisfaz

$$|C| \leq q^{n-(d-1)}.$$



Caso contrário $d(c, c') \leq d((c_{n-(d-1)+1}, \ldots, c_n), (c'_{n-(d-1)+1}, \ldots, c'_n)) \leq d - 1.$

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mod p$$

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mod p$$

- Codificar m através de “avaliações” de f_m

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mod p$$

- Codificar m através de "avaliações" de f_m

$$\text{Enc}(m) = (f_m(\alpha_1), f_m(\alpha_2), \ldots, f_m(\alpha_n))$$

Códigos a partir de polinómios

Quão longe está a desigualdade de Singleton da verdade?

Irving Reed + Gustave Solomon (1960):

- Alfabeto $\Sigma = \mathbb{Z}_p$ com p primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mod p$$

- Codificar m através de "avaliações" de f_m

$$\text{Enc}(m) = (f_m(\alpha_1), f_m(\alpha_2), \ldots, f_m(\alpha_n))$$

com $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p$ distintos.

Códigos Reed-Solomon: Distância mínima

Mensagens $m, m' \in \mathbb{Z}_p^k$ distintas.

$$\text{Enc}(m) - \text{Enc}(m') = (f_m(\alpha_1) - f_{m'}(\alpha_1), \ldots, f_m(\alpha_n) - f_{m'}(\alpha_n))$$

Códigos Reed-Solomon: Distância mínima

Mensagens $m, m' \in \mathbb{Z}_p^k$ distintas.

$$\text{Enc}(m) - \text{Enc}(m') = (f_m(\alpha_1) - f_{m'}(\alpha_1), \ldots, f_m(\alpha_n) - f_{m'}(\alpha_n))$$

Definimos $g(x) = f_m(x) - f_{m'}(x)$, que é um polinómio de grau $\leq k - 1$

Códigos Reed-Solomon: Distância mínima

Mensagens $m, m' \in \mathbb{Z}_p^k$ distintas.

$$\text{Enc}(m) - \text{Enc}(m') = (f_m(\alpha_1) - f_{m'}(\alpha_1), \ldots, f_m(\alpha_n) - f_{m'}(\alpha_n))$$

Definimos $g(x) = f_m(x) - f_{m'}(x)$, que é um polinómio de grau $\leq k - 1$

$$\text{Enc}(m) - \text{Enc}(m') = (g(\alpha_1), \ldots, g(\alpha_n)) \implies d(\text{Enc}(m), \text{Enc}(m')) \geq n - \#\text{ raízes de } g$$

Códigos Reed-Solomon: Distância mínima

Mensagens $m, m' \in \mathbb{Z}_p^k$ distintas.

$$\text{Enc}(m) - \text{Enc}(m') = (f_m(\alpha_1) - f_{m'}(\alpha_1), \ldots, f_m(\alpha_n) - f_{m'}(\alpha_n))$$

Definimos $g(x) = f_m(x) - f_{m'}(x)$, que é um polinómio de grau $\leq k - 1$

$$\text{Enc}(m) - \text{Enc}(m') = (g(\alpha_1), \ldots, g(\alpha_n)) \implies d(\text{Enc}(m), \text{Enc}(m')) \geq n - \#\text{ raízes de } g$$

Um polinómio $g \in \mathbb{Z}_p[x]$ de grau r tem no máximo r raízes.

Códigos Reed-Solomon: Distância mínima

Mensagens $m, m' \in \mathbb{Z}_p^k$ distintas.

$$\text{Enc}(m) - \text{Enc}(m') = (f_m(\alpha_1) - f_{m'}(\alpha_1), \ldots, f_m(\alpha_n) - f_{m'}(\alpha_n))$$

Definimos $g(x) = f_m(x) - f_{m'}(x)$, que é um polinómio de grau $\leq k - 1$

$$\text{Enc}(m) - \text{Enc}(m') = (g(\alpha_1), \ldots, g(\alpha_n)) \implies d(\text{Enc}(m), \text{Enc}(m')) \geq n - \#\text{ raízes de } g$$

Um polinómio $g \in \mathbb{Z}_p[x]$ de grau r tem no máximo r raízes.

$$\implies d(\text{Enc}(m), \text{Enc}(m')) \geq n - \deg g \geq n - (k - 1)$$

Resumindo…

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k - 1$

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k - 1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mapsto \text{Enc}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n))$$

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k - 1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mapsto \text{Enc}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n))$$

- Distância mínima $d = n - (k - 1)$

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k - 1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mapsto \text{Enc}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n))$$

- Distância mínima $d = n - (k - 1)$
- Tamanho do código $|C| = p^k = p^{n-(d-1)}$

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k - 1$

$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mapsto \text{Enc}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n))$$

- Distância mínima $d = n - (k - 1)$
- Tamanho do código $|C| = p^k = p^{n-(d-1)}$

Desigualdade de Singleton!

Resumindo…

- Alfabeto $\Sigma = \mathbb{Z}_p$ com $p \geq n$ primo.
- Interpretar mensagem $m \in \mathbb{Z}_p^k$ como polinómio de grau $\leq k-1$

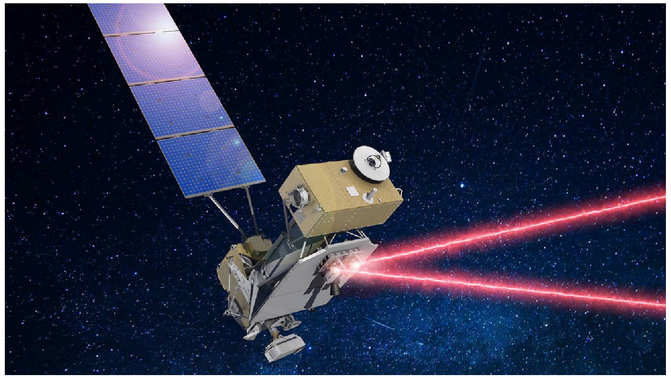
$$m \mapsto f_m(x) = \sum_{i=1}^{k} m_i x^{i-1} \mapsto \text{Enc}(m) = (f_m(\alpha_1), \ldots, f_m(\alpha_n))$$

- Distância mínima $d = n - (k-1)$
- Tamanho do código $|C| = p^k = p^{n-(d-1)}$

Desigualdade de Singleton!

Conclusão: Códigos Reed-Solomon são optimais (para alfabetos de tamanho primo $\geq n$)!

Aplicações de códigos Reed-Solomon



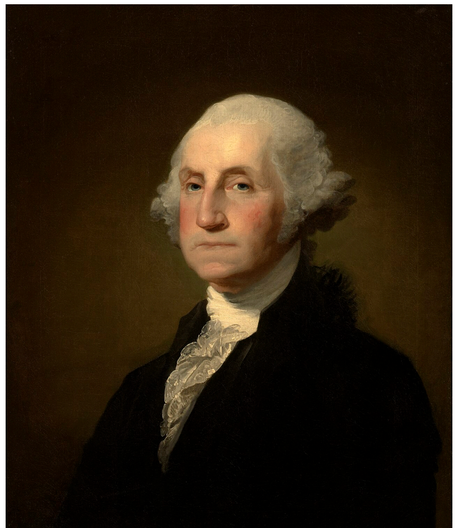
Google

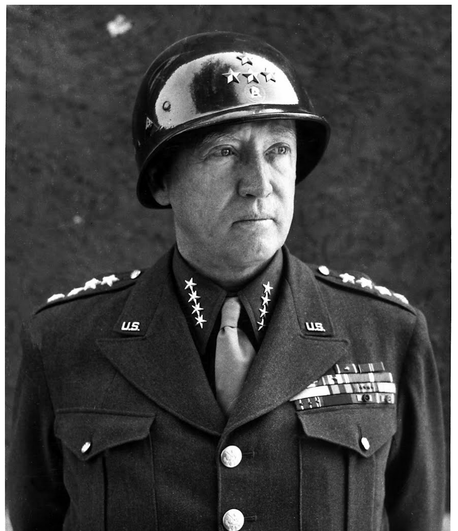
aws

Como partilhar um segredo

segredo s

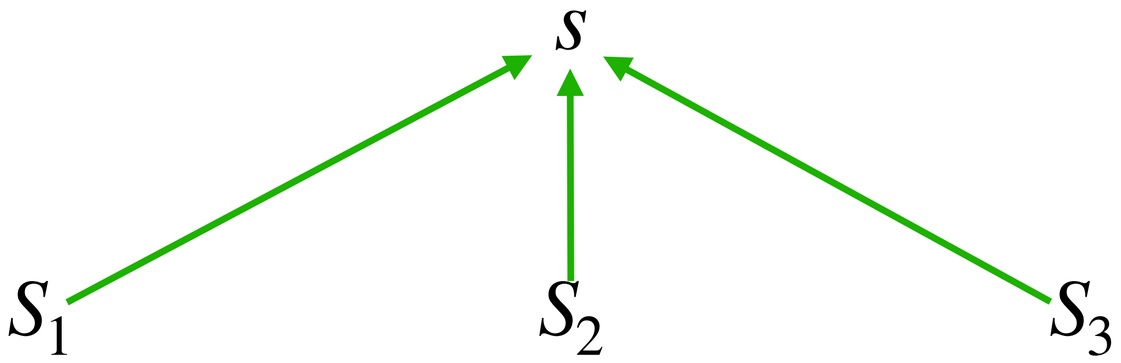
S_1 S_2 S_3 S_4 S_5



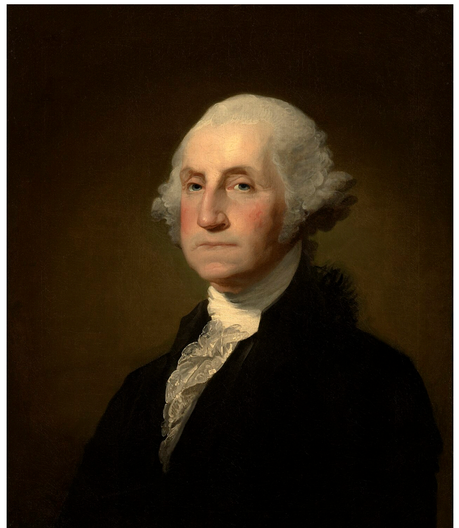


Como partilhar um segredo

segredo s



S_4 S_5

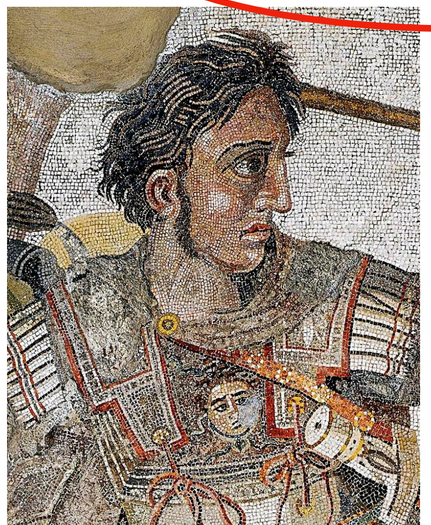


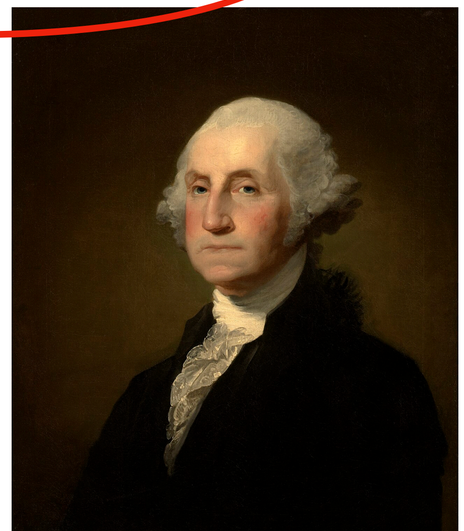
Como partilhar um segredo

segredo s

$s = ?????$

S_1 S_2 S_3 S_4 S_5





Como partilhar um segredo

Partilha de segredos “t-de-n” (Blakley, Shamir, 1979)

Como partilhar um segredo

Partilha de segredos "t-de-n" (Blakley, Shamir, 1979)

$$s \in \{0,1\} \mapsto (S_1, S_2, \ldots, S_n)$$

Como partilhar um segredo

Partilha de segredos "t-de-n" (Blakley, Shamir, 1979)

$$s \in \{0,1\} \mapsto (S_1, S_2, \ldots, S_n)$$

(Reconstrução) Qualquer subconjunto de t partes determina s

Como partilhar um segredo

Partilha de segredos "t-de-n" (Blakley, Shamir, 1979)

$$s \in \{0,1\} \mapsto (S_1, S_2, \ldots, S_n)$$

(Reconstrução) Qualquer subconjunto de t partes determina s

(Privacidade) Qualquer subconjunto de $t-1$ partes não revela informação sobre s

Como partilhar um segredo

Partilha de segredos "t-de-n" (Blakley, Shamir, 1979)

$$s \in \{0,1\} \mapsto (S_1, S_2, \ldots, S_n)$$

(Reconstrução) Qualquer subconjunto de t partes determina s

(Privacidade) Qualquer subconjunto de $t-1$ partes não revela informação sobre s

Dado segredo s e primo $p > n$, construímos

$$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i \text{ , com } \beta_i \in \mathbb{Z}_p \text{ escolhidos "ao calhas".}$$

Como partilhar um segredo

Partilha de segredos "t-de-n" (Blakley, Shamir, 1979)

$$s \in \{0,1\} \mapsto (S_1, S_2, \ldots, S_n)$$

(Reconstrução) Qualquer subconjunto de t partes determina s

(Privacidade) Qualquer subconjunto de $t-1$ partes não revela informação sobre s

Dado segredo s e primo $p > n$, construímos

$$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i \text{ , com } \beta_i \in \mathbb{Z}_p \text{ escolhidos "ao calhas".}$$

Definimos $S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \backslash \{0\}$.

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Polinómio de grau $\leq t - 1$ é completamente determinado por t pontos.

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Polinómio de grau $\leq t - 1$ é completamente determinado por t pontos.

Equivalente a correcção de rasuras por código Reed-Solomon!

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Polinómio de grau $\leq t - 1$ é completamente determinado por t pontos.

Equivalente a correcção de rasuras por código Reed-Solomon!

(Privacidade) Qualquer subconjunto de $t - 1$ partes não revela informação sobre s

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Polinómio de grau $\leq t - 1$ é completamente determinado por t pontos.

Equivalente a correcção de rasuras por código Reed-Solomon!

(Privacidade) Qualquer subconjunto de $t - 1$ partes não revela informação sobre s

Fixamos $y_1, \ldots, y_{t-1}$ arbitrários. Para qualquer segredo s existe *exatamente um* polinómio g de grau $\leq t - 1$ tal que $g(0) = 0$ e $g(\alpha_i) = y_i$ para $i = 1, \ldots, t - 1$.

Como partilhar um segredo

$f(x) = s + \sum_{i=1}^{t-1} \beta_i x^i$, com $\beta_i \in \mathbb{Z}_p$ escolhidos “ao calhas”.

$S_i = (\alpha_i, f(\alpha_i))$ para $\alpha_1, \ldots, \alpha_n$ distintos em $\mathbb{Z}_p \setminus \{0\}$.

(Reconstrução) Qualquer subconjunto de t partes determina s

Polinómio de grau $\leq t - 1$ é completamente determinado por t pontos.

Equivalente a correcção de rasuras por código Reed-Solomon!

(Privacidade) Qualquer subconjunto de $t - 1$ partes não revela informação sobre s

Fixamos $y_1, \ldots, y_{t-1}$ arbitrários. Para qualquer segredo s existe *exatamente um* polinómio g de grau $\leq t - 1$ tal que $g(0) = 0$ e $g(\alpha_i) = y_i$ para $i = 1, \ldots, t - 1$.

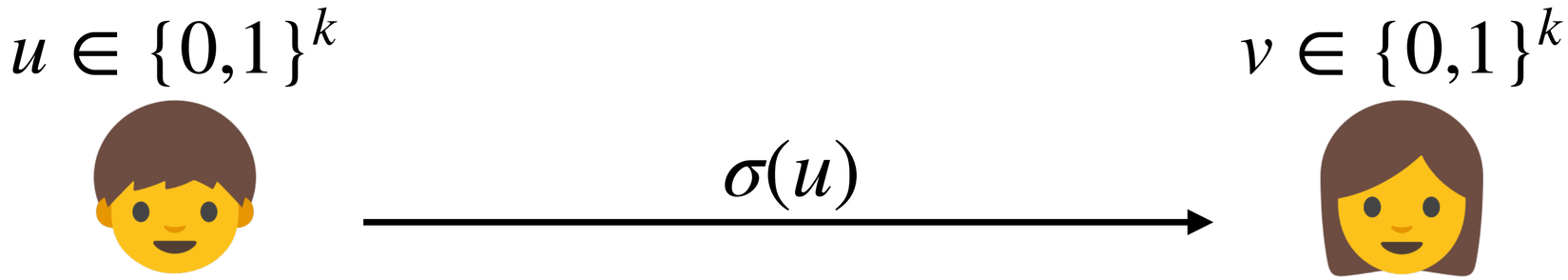
Equivalente a “códigos Reed-Solomon atingem a desigualdade de Singleton”!

Computação distribuída

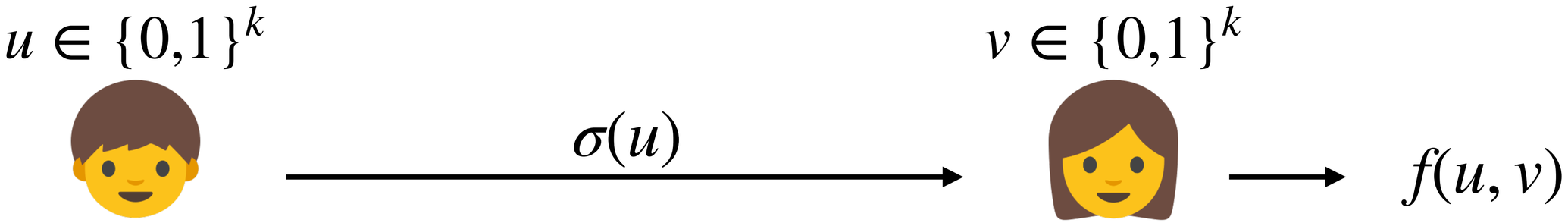
$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

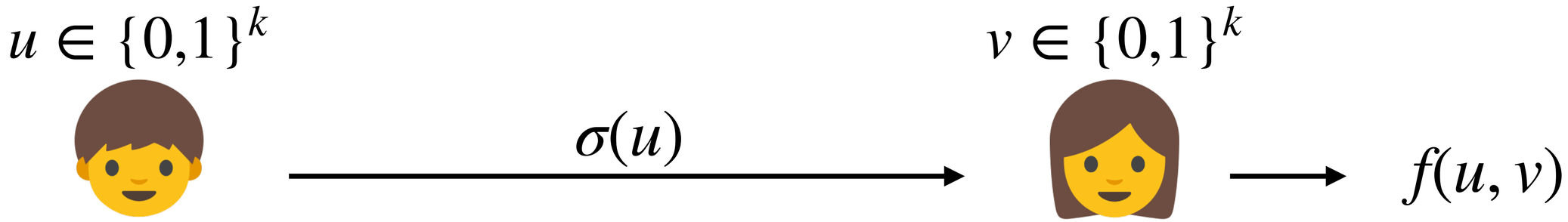
Computação distribuída



Computação distribuída

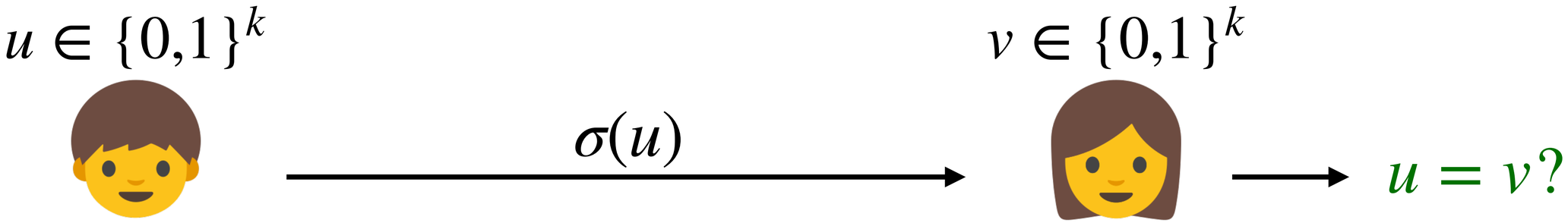


Computação distribuída

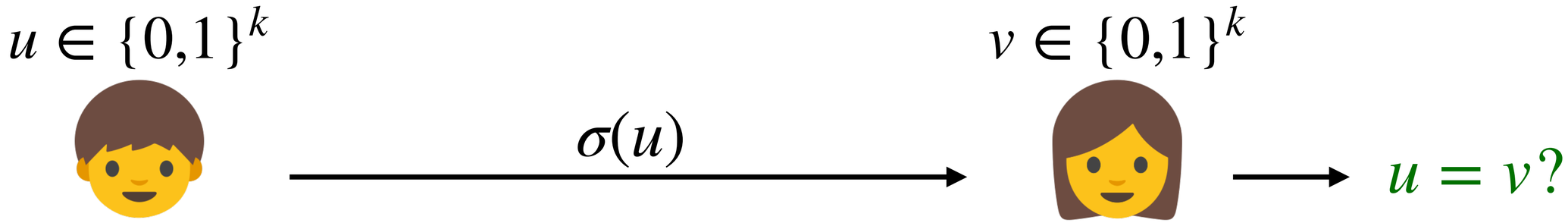


Quantos bits de comunicação são necessários para a Alice calcular $f(u, v)$?

Complexidade de comunicação da igualdade

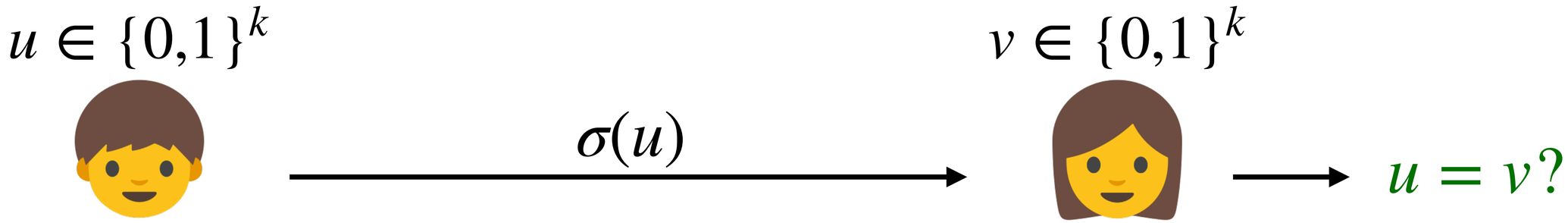


Complexidade de comunicação da igualdade



Se quisermos que a Alice acerte sempre, precisamos de comunicar k bits…

Complexidade de comunicação da igualdade



Se quisermos que a Alice acerte sempre, precisamos de comunicar k bits…

E se aceitarmos uma pequena probabilidade de erro?

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

$(\alpha, f_u(\alpha))$

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

$(\alpha, f_u(\alpha))$

$f_u(\alpha) = f_v(\alpha)?$

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

$(\alpha, f_u(\alpha))$ →

$f_u(\alpha) = f_v(\alpha)?$

Pr[Alice erra] < 0.01.

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

$(\alpha, f_u(\alpha))$ →

$f_u(\alpha) = f_v(\alpha)?$

Pr[Alice erra] < 0.01.

Se $u \neq v$...

$$|\{\alpha \in \mathbb{Z}_p : f_u(\alpha) = f_v(\alpha)\}| < k \leq \frac{p}{100}$$

Menos comunicação via polinómios

$u \in \{0,1\}^k$

$v \in \{0,1\}^k$

comunicação:

$\approx 2 \log p \propto \log k$ bits

$p \geq 100k$ primo

$$f_u(x) = \sum_{i=1}^{k} u_i x^{i-1} \mod p$$

$\alpha \leftarrow \mathbb{Z}_p$ ao calhas

$(\alpha, f_u(\alpha))$ →

$f_u(\alpha) = f_v(\alpha)?$

$\Pr[\text{Alice erra}] < 0.01.$

Se $u \neq v$...

$$|\{\alpha \in \mathbb{Z}_p : f_u(\alpha) = f_v(\alpha)\}| < k \leq \frac{p}{100}$$

Concluindo…

- Polinómios são MUITO úteis na prática (e na teoria)!

Concluindo…

- Polinómios são MUITO úteis na prática (e na teoria)!
- Podemos chegar MUITO longe sabendo apenas que

Concluindo…

- Polinómios são MUITO úteis na prática (e na teoria)!
- Podemos chegar MUITO longe sabendo apenas que

> Um polinómio $g \in \mathbb{Z}_p[x]$ de grau r tem no máximo r raízes.

Concluindo…

- Polinómios são MUITO úteis na prática (e na teoria)!
- Podemos chegar MUITO longe sabendo apenas que

> Um polinómio $g \in \mathbb{Z}_p[x]$ de grau r tem no máximo r raízes.

OBRIGADO! :)