Criptografia com códigos corretores de erros

Thales Paiva
thalespaiva@gmail.com

25 de novembro de 2016

Escola Politécnica - USP
PCS5734 - Prof. Dr. Marcos Antonio Simplicio Junior

Sumário

Teoria de Códigos

Teoria de Códigos

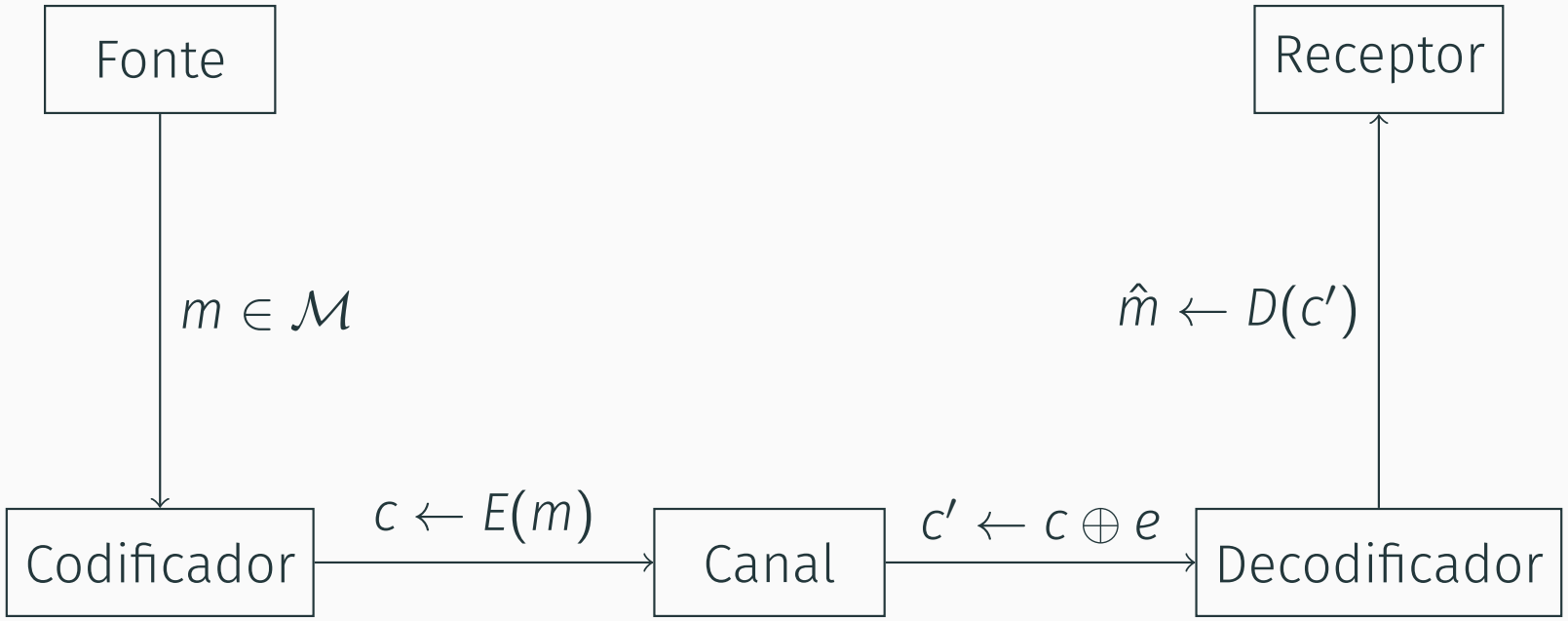


Figura 1: Transmissão de uma palavra m através de um canal ruidoso.

Exemplo de transmissão

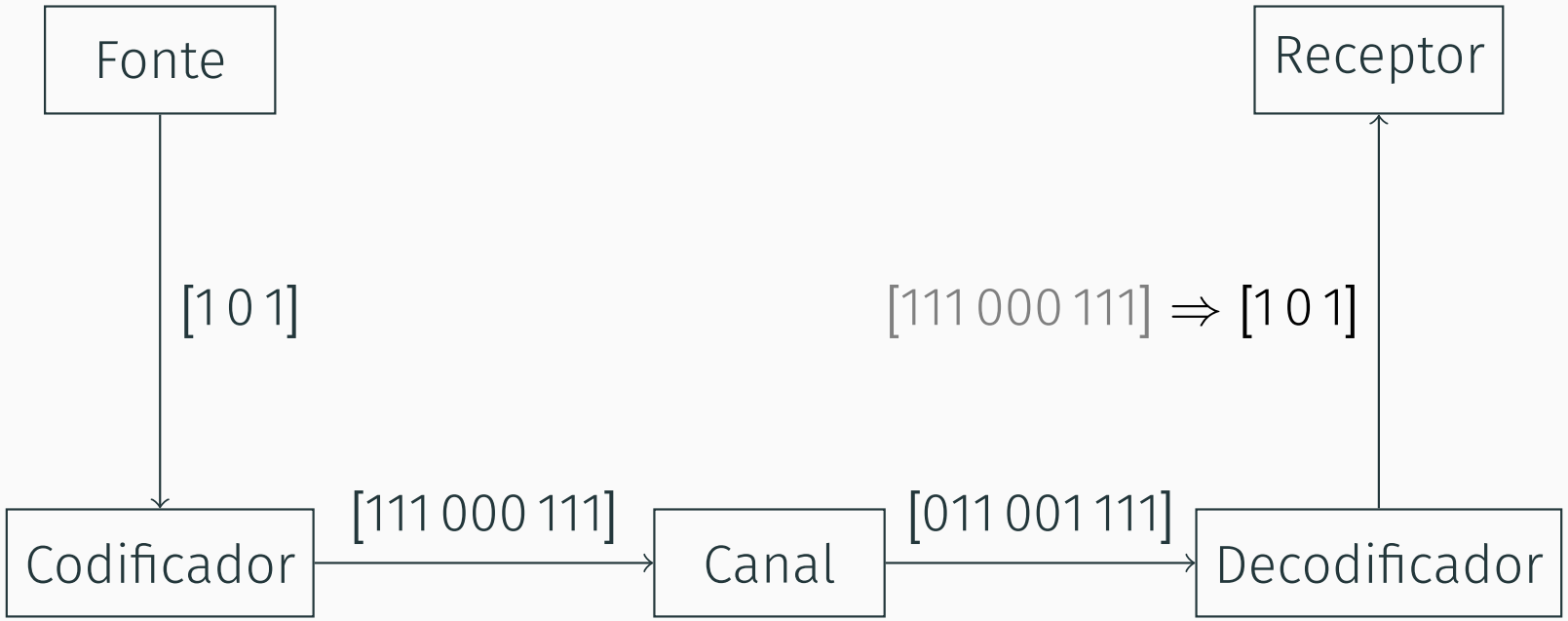


Figura 2: Exemplo de transmissão de uma palavra m através de um canal que produziu o erro $e = [100\,001\,000]$, usando um Código de Repetição.

Códigos Lineares

Definição

Um ***código binário*** $[n, k]$***-linear*** *é um subespaço vetorial de dimensão* k *do espaço* $\mathbb{F}_2^n$.

Matrizes Geradoras e de Paridade

Então, se $\mathcal{C}$ é um código $[n, k]$-linear:

Matrizes Geradoras e de Paridade

Então, se $\mathcal{C}$ é um código $[n, k]$-linear:

- $\mathcal{C}$ pode ser descrito por sua **imagem** ou por seu **núcleo**

Matrizes Geradoras e de Paridade

Então, se $\mathcal{C}$ é um código $[n, k]$-linear:

- $\mathcal{C}$ pode ser descrito por sua **imagem** ou por seu **núcleo**
- Chama-se **matriz geradora** toda $G \in \mathbb{F}_2^{k \times n}$ tal que

$$\mathcal{C} = \left\{ mG : m \in \mathbb{F}_2^k \right\}$$

Matrizes Geradoras e de Paridade

Então, se $\mathcal{C}$ é um código $[n, k]$-linear:

- $\mathcal{C}$ pode ser descrito por sua **imagem** ou por seu **núcleo**
- Chama-se **matriz geradora** toda $G \in \mathbb{F}_2^{k \times n}$ tal que

$$\mathcal{C} = \left\{ mG : m \in \mathbb{F}_2^k \right\}$$

- Chama-se **matriz de paridade** toda $H \in \mathbb{F}_2^{(n-k) \times n}$ tal que

$$\mathcal{C} = \left\{ c \in \mathbb{F}_2^n : cH^T = 0 \right\}$$

Codificação de Mensagens

Fixe G, H matrizes geradora e de paridade de $\mathcal{C}$:

Codificação de Mensagens

Fixe G, H matrizes geradora e de paridade de $\mathcal{C}$:

- Uma mensagem m é codificada como

$$c = mG$$

Codificação de Mensagens

Fixe G, H matrizes geradora e de paridade de $\mathcal{C}$:

- Uma mensagem m é codificada como

$$c = mG$$

- É sobredeterminado o sistema

$$mG = c$$

Codificação de Mensagens

Fixe G, H matrizes geradora e de paridade de $\mathcal{C}$:

- Uma mensagem m é codificada como

$$c = mG$$

- É sobredeterminado o sistema

$$mG = c$$

- A **síndrome** de um vetor $\bar{c} \in \mathbb{F}_2^n$ é o vetor

$$s = cH^T \implies \bar{c} \in \mathcal{C} \Leftrightarrow s = 0$$

Codificação de Mensagens

Fixe G, H matrizes geradora e de paridade de $\mathcal{C}$:

- Uma mensagem m é codificada como

$$c = mG$$

- É sobredeterminado o sistema

$$mG = c$$

- A **síndrome** de um vetor $\bar{c} \in \mathbb{F}_2^n$ é o vetor

$$s = cH^T \implies \bar{c} \in \mathcal{C} \Leftrightarrow s = 0$$

- Se $\bar{c} = c \oplus e$, então

$$s = \bar{c}H^T = (c \oplus e)H^T = cH^T \oplus eH^T = eH^T$$

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

$$c = mG = [0\,0\,1\,1\,0\,0\,1].$$

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

$$c = mG = [0\,0\,1\,1\,0\,0\,1].$$

- Somando o erro $e = [0\,1\,0\,0\,0\,0\,0]$ a c obtemos

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

$$c = mG = [0\,0\,1\,1\,0\,0\,1].$$

- Somando o erro $e = [0\,1\,0\,0\,0\,0\,0]$ a c obtemos

$$\bar{c} = c \oplus e = [0\,1\,1\,1\,0\,0\,1].$$

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

$$c = mG = [0\,0\,1\,1\,0\,0\,1].$$

- Somando o erro $e = [0\,1\,0\,0\,0\,0\,0]$ a c obtemos

$$\bar{c} = c \oplus e = [0\,1\,1\,1\,0\,0\,1].$$

- A síndrome de $\bar{c}$ é o vetor

Exemplo com um Código de Hamming

Considere o código $[7, 4]$-linear $\mathcal{C}$ que tem matriz geradora G e matriz de paridade H tais que:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- A codificação de $m = [1\,0\,0\,1]$ é

$$c = mG = [0\,0\,1\,1\,0\,0\,1].$$

- Somando o erro $e = [0\,1\,0\,0\,0\,0\,0]$ a c obtemos

$$\bar{c} = c \oplus e = [0\,1\,1\,1\,0\,0\,1].$$

- A síndrome de $\bar{c}$ é o vetor

$$s = \bar{c}H^T = [0\,1\,0].$$

Algumas definições

Sejam u, v palavras de $\mathbb{F}_2^n$:

Algumas definições

Sejam u, v palavras de $\mathbb{F}_2^n$:

- O **peso** de u é o número de coordenadas não nulas de u:

$$w([1\,0\,0\,1]) = 2$$

Algumas definições

Sejam u, v palavras de $\mathbb{F}_2^n$:

- O **peso** de u é o número de coordenadas não nulas de u:

$$w([1\,0\,0\,1]) = 2$$

- A **distância de Hamming** entre u e v é o número de coordenadas em que u e v diferem:

$$d(u, v) = w(u \oplus v)$$
$$d([1\,0\,0\,1], [1\,1\,0\,1]) = 1$$

Decodificação

Dada uma palavra $\bar{c} \in \mathbb{F}_2^n$, queremos encontrar uma palavra c tal que

$$d(\bar{c}, c) \leq d(\bar{c}, u), \text{ para qualquer } u \in \mathbb{F}_2^n.$$

Decodificação

Dada uma palavra $\bar{c} \in \mathbb{F}_2^n$, queremos encontrar uma palavra c tal que

$$d(\bar{c}, c) \leq d(\bar{c}, u), \text{ para qualquer } u \in \mathbb{F}_2^n.$$

- Decodificação $\mathcal{NP}$-difícil no pior caso [1]

Decodificação

Dada uma palavra $\bar{c} \in \mathbb{F}_2^n$, queremos encontrar uma palavra c tal que

$$d(\bar{c}, c) \leq d(\bar{c}, u), \text{ para qualquer } u \in \mathbb{F}_2^n.$$

- Decodificação $\mathcal{NP}$-difícil no pior caso [1]
- Conjecturada tipicamente difícil para códigos aleatórios

Decodificação

Dada uma palavra $\bar{c} \in \mathbb{F}_2^n$, queremos encontrar uma palavra c tal que

$$d(\bar{c}, c) \leq d(\bar{c}, u), \text{ para qualquer } u \in \mathbb{F}_2^n.$$

- Decodificação $\mathcal{NP}$-difícil no pior caso [1]
- Conjecturada tipicamente difícil para códigos aleatórios
- É preciso desenhar bons códigos que admitam a construção de decodificadores

Decodificação

Dada uma palavra $\bar{c} \in \mathbb{F}_2^n$, queremos encontrar uma palavra c tal que

$$d(\bar{c}, c) \leq d(\bar{c}, u), \text{ para qualquer } u \in \mathbb{F}_2^n.$$

- Decodificação $\mathcal{NP}$-difícil no pior caso [1]
- Conjecturada tipicamente difícil para códigos aleatórios
- É preciso desenhar bons códigos que admitam a construção de decodificadores
  - Reed-Muller
  - Goppa
  - LDPC

Esquema de McEliece

Esquema de McEliece

Elaborado por McEliece em 1978 [8]

- Primeiro esquema baseado no problema da decodificação
- Primeiro que usa procedimento aleatório na encriptação
- Operações mais rápidas do que as respectivas do RSA e CE

Porém ficou esquecido pois

- Chaves públicas muito grandes: $\lambda = 100 \Rightarrow$ tamanho ≥ 100 kB
- Esquema de assinatura parecia ser impossível, até CFS [3]

Até que Shor [10] mostra algoritmo quântico que resolve log discreto

Códigos de Goppa

Usa códigos de Goppa binários e irredutíveis:

- Cada código é gerado por um polinômio irredutível g de $\mathbb{F}_{2^m}[X]$
- A capacidade de correção é igual ou superior ao grau t de g
- É fácil construir t-decodificadores eficientes conhecendo g
- Não se conhece algoritmo eficiente para construir decodificadores sem conhecer g
- É difícil em geral distinguir matrizes geradoras de Goppa e geradoras de aleatórios
  Embora seja possível para k próximo de n [4]

Parâmetros para cada nível de segurança

Tabela 1: Parâmetros de famílias de códigos de Goppa para cada nível de segurança λ [2].

λ	n	k	t	m	tamanho da chave pública (Bytes)
81	2048	1751	27	11	65006
95	2048	1608	40	11	88440
105	2480	1940	45	12	130950
119	2690	2018	56	12	169512
146	3408	2604	67	12	261702
187	4624	3389	95	13	523177
263	6960	5413	119	13	1046739

Geração de Chaves

Algoritmo 1: KeyGen para a geração de chaves

Entrada: λ nível de segurança.

Saída: $(K_{\text{SEC}}, K_{\text{PUB}})$ o par de chaves secreta e pública.

1 **início**

2 Tome n, t, e k que permitam nível de segurança λ Tabela 1

3 $g \leftarrow$ polinômio gerador de um código de Goppa aleatório $\mathcal{G}$

4 $\bar{G} \leftarrow$ matriz $k \times n$ geradora de $\mathcal{G}$

5 $\Phi \leftarrow$ algoritmo t-decodificador para $\mathcal{G}$

6 $S \leftarrow$ matriz $k \times k$ não singular aleatória

7 $P \leftarrow$ matriz de permutação $n \times n$ aleatória

8 $G \leftarrow S\bar{G}P$

9 $\hat{G} \leftarrow S\bar{G}$

10 $K_{\text{SEC}} \leftarrow (\hat{G}, P, \Phi)$

11 $K_{\text{PUB}} \leftarrow (G, t)$

12 **devolva** (K_{SEC}, K_{PUB})

Encriptação

Algoritmo 2: ENC para a encriptação

Entrada: m mensagem que Beto quer enviar a Alice.
K_{PUB} a chave pública de Alice.

Saída: c o texto cifrado da mensagem m.

1 **início**
2 $(G, t) \leftarrow K_{\text{PUB}}$
3 $e \leftarrow$ vetor aleatório de $\mathbb{F}_2^n$ de peso t
4 $c \leftarrow mG \oplus e$
5 **devolva** c

Decriptação

Algoritmo 3: DEC para a encriptação

Entrada: c texto cifrado recebido por Alice.
K_{SEC} a chave secreta de Alice.

Saída: m a decifração de c.

1 **início**
2 $(\hat{G}, P, \Phi) \leftarrow K_{\text{SEC}}$
3 $c_1 \leftarrow cP^{-1} = (mG \oplus e)P^{-1} = m\hat{G} \oplus eP^{-1}$
4 $c_2 \leftarrow \Phi(c_1) = m\hat{G}$
5 $m \leftarrow$ solução do sistema sobredeterminado $m\hat{G} = c_2$
6 **devolva** m

Segurança

Mas não resiste a ataques de:

- Mensagem parcialmente conhecida
- Mensagem relacionada (e.g. reenvio de mensagens)
- Reação
- Maleabilidade

O esquema de McEliece é apenas OWE

- Conversões de segurança obrigatórias

Conversão IND-CCA2 de Kobara e Imai

Algoritmo 4: Conversão IND-CCA2 de Enc [7]

Entrada: m mensagem que Beto quer enviar a Alice.
K_{PUB} a chave pública de Alice.

Saída: c o texto cifrado da mensagem m.

1 **início**
2 $(G, t) \leftarrow K_{\text{PUB}}$
3 $r \leftarrow$ número aleatório ≈ 160 bits
4 $z \leftarrow \text{Hash}(r \| m)$
5 $y \leftarrow \text{PRNG}(z) \oplus (r \| m)$
6 $e_z \leftarrow \text{IntParaErro}(z, t)$
7 $c \leftarrow (yG \oplus e_z)$
8 **devolva** c

Conversão IND-CCA2 de Kobara e Imai

Algoritmo 5: Conversão IND-CCA2 de DEC [7]

Entrada: c texto cifrado recebido por Alice.
K_{SEC} a chave secreta de Alice.

Saída: m a decifração de c.

1 **início**
2 $y \leftarrow \text{DEC}(\text{ESQUERDA}(c, k), K_{SEC})$
3 $e_z \leftarrow \text{ESQUERDA}(\text{C}, \text{K}) \oplus yG$
4 $z \leftarrow \text{ERROPARAINT}(e_z)$
5 $r \| m \leftarrow \text{PRNG}(z) \oplus (y)$
6 **se** $z = \textit{HASH}(r \| m)$ **então**
7 **devolva** m
8 **senão**
9 **devolva** $\perp$

Ataque Genérico por Conjunto de Informação

Decodificação por Conjunto de Informação - ISD

- Selecionar k colunas de c' que não estão com erro
- Se as k colunas de $\hat{G}$ formarem matriz inversível G'
- Pode-se recuperar m ao resolver o sistema $mG' = c'$

Ataque Genérico por Conjunto de Informação

Decodificação por Conjunto de Informação - ISD

- Selecionar k colunas de c' que não estão com erro
- Se as k colunas de $\hat{G}$ formarem matriz inversível G'
- Pode-se recuperar m ao resolver o sistema $mG' = c'$

Ocorre com baixa probabilidade de

$$\frac{\binom{n-t}{k}}{\binom{n}{k}}$$

Ataque Genérico por Conjunto de Informação

Decodificação por Conjunto de Informação - ISD

- Selecionar k colunas de c' que não estão com erro
- Se as k colunas de $\hat{G}$ formarem matriz inversível G'
- Pode-se recuperar m ao resolver o sistema $mG' = c'$

Ocorre com baixa probabilidade de

$$\frac{\binom{n-t}{k}}{\binom{n}{k}}$$

E assim o trabalho esperado é limitado inferormente

$$\frac{\binom{n}{k}}{\binom{n-t}{k}}$$

Reduzir Tamanhos das Chaves

Ideias para Reduzir Tamanhos de Chaves:

- Usar códigos que corrigem mais erros

Reduzir Tamanhos das Chaves

Ideias para Reduzir Tamanhos de Chaves:

- Usar códigos que corrigem mais erros
- Usar códigos que permitem representações compactas

Reduzir Tamanhos das Chaves

Ideias para Reduzir Tamanhos de Chaves:

- Usar códigos que corrigem mais erros
- Usar códigos que permitem representações compactas
  1. Códigos de Goppa Quase-Cíclicos (QC-Goppa)
  2. Códigos de Goppa Quase-Diádicos (QD-Goppa)
  3. Códigos QC com Matriz de Paridade de Baixa Densidade (QC-LDPC)
  4. Códigos QC-LDPC com Densidade Moderada (QC-MDPC)

Reduzir Tamanhos das Chaves

Ideias para Reduzir Tamanhos de Chaves:

- Usar códigos que corrigem mais erros
- Usar códigos que permitem representações compactas
  1. Códigos de Goppa Quase-Cíclicos (QC-Goppa)
  2. Códigos de Goppa Quase-Diádicos (QD-Goppa)
  3. Códigos QC com Matriz de Paridade de Baixa Densidade (QC-LDPC)
  4. Códigos QC-LDPC com Densidade Moderada (QC-MDPC)
- Apenas as propostas 2 e 4 chegaram até 2016, mas
  - Faugere, Perret e Portzamparc quebraram QD-Goppa [5]
  - Guo, Johansson e Stankovski mostraram ataque de reação a QC-MDPC [6]

QC-MDPC McEliece

Códigos LDPC

Definição

Um código binário e linear com matriz de paridade H é dito um código LDPC se o número de elementos não nulos de H é $\mathcal{O}(n)$.

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

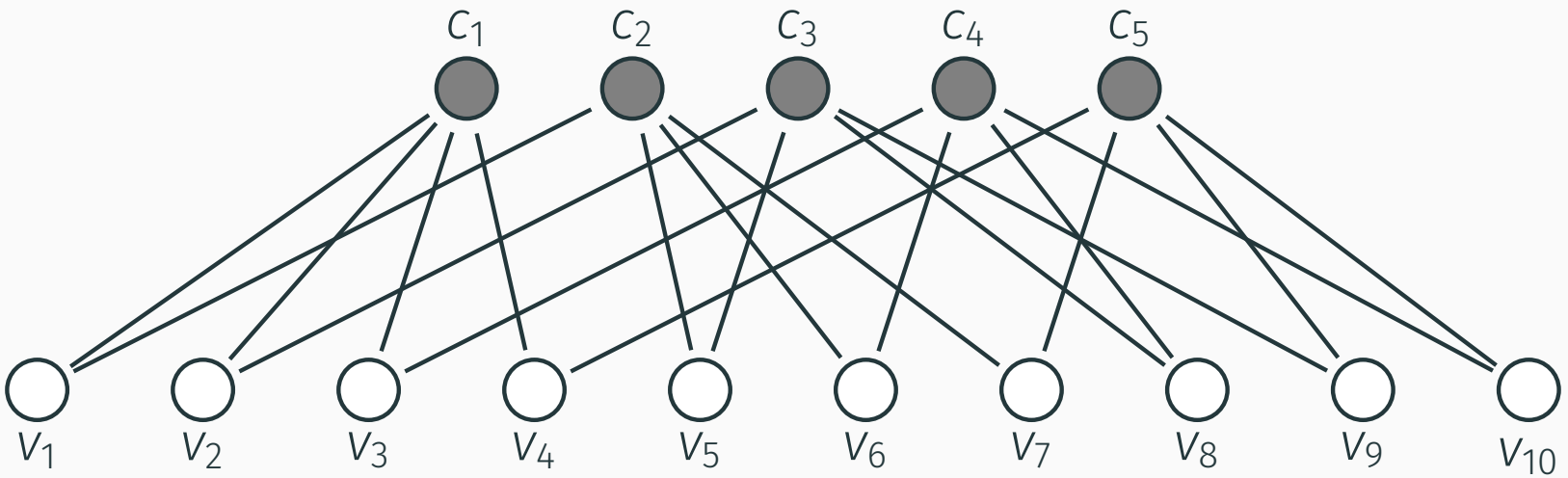


Figura 3: Grafo de Tanner da matriz H.

Algoritmo de Decodificação por *bit-flipping*

$$
\begin{aligned}
m &\leftarrow [0\,1\,1\,0\,0\,0] \\
c &\leftarrow mG = [0\,1\,1\,0\,0\,0\,0\,0\,1\,1] \\
e &\leftarrow [0\,0\,0\,0\,0\,0\,0\,1\,0\,0] \\
c' &\leftarrow c \oplus e = [0\,1\,1\,0\,0\,0\,0\,1\,1\,1]
\end{aligned}
$$

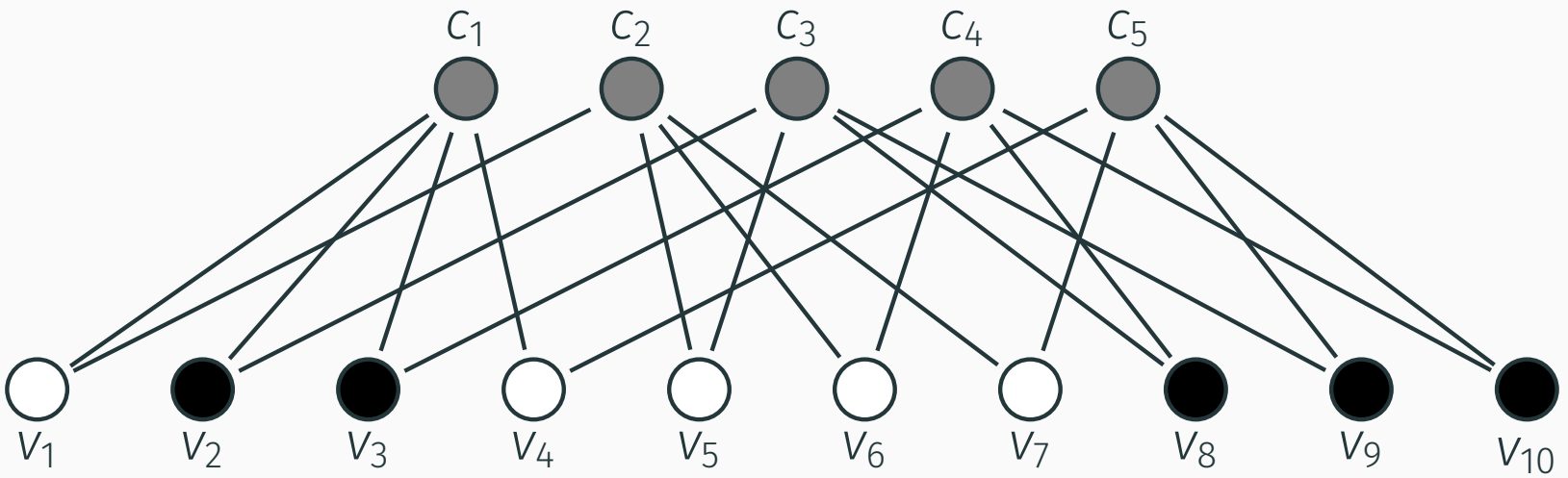


Figura 4: Funcionamento do algoritmo de *bit-flipping*.

Algoritmo de Decodificação por *bit-flipping*

$$
\begin{aligned}
m &\leftarrow [0\,1\,1\,0\,0\,0] \\
c &\leftarrow mG = [0\,1\,1\,0\,0\,0\,0\,0\,1\,1] \\
e &\leftarrow [0\,0\,0\,0\,0\,0\,0\,1\,0\,0] \\
c' &\leftarrow c \oplus e = [0\,1\,1\,0\,0\,0\,0\,1\,1\,1]
\end{aligned}
$$

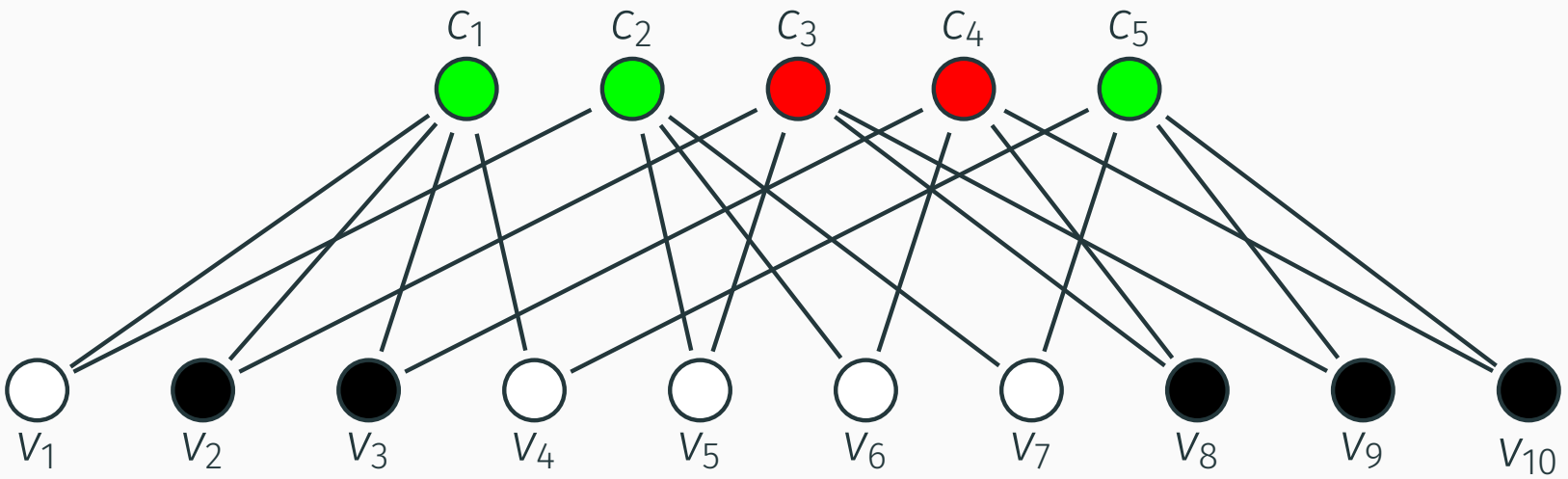


Figura 4: Funcionamento do algoritmo de *bit-flipping*.

Algoritmo de Decodificação por *bit-flipping*

$$m \leftarrow [0\,1\,1\,0\,0\,0]$$
$$c \leftarrow mG = [0\,1\,1\,0\,0\,0\,0\,0\,1\,1]$$
$$e \leftarrow [0\,0\,0\,0\,0\,0\,0\,1\,0\,0]$$
$$c' \leftarrow c \oplus e = [0\,1\,1\,0\,0\,0\,0\,1\,1\,1]$$

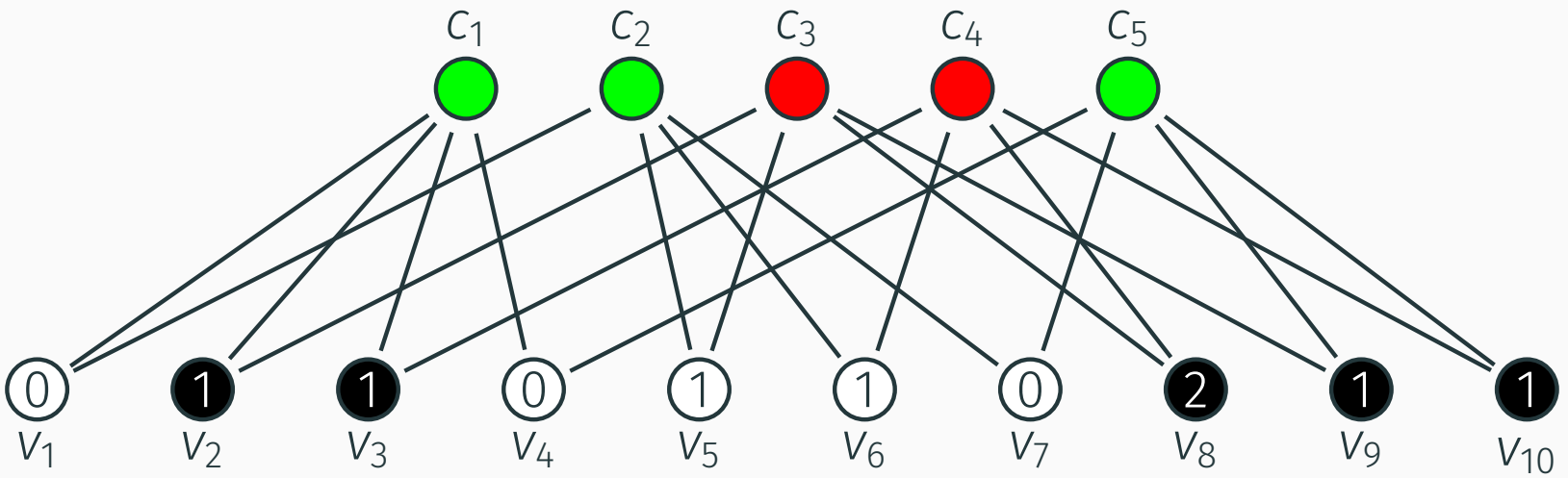


Figura 4: Funcionamento do algoritmo de *bit-flipping*.

Algoritmo de Decodificação por *bit-flipping*

$$
\begin{aligned}
m &\leftarrow [0\,1\,1\,0\,0\,0] \\
c &\leftarrow mG = [0\,1\,1\,0\,0\,0\,0\,0\,1\,1] \\
e &\leftarrow [0\,0\,0\,0\,0\,0\,0\,1\,0\,0] \\
c' &\leftarrow c \oplus e = [0\,1\,1\,0\,0\,0\,0\,1\,1\,1]
\end{aligned}
$$

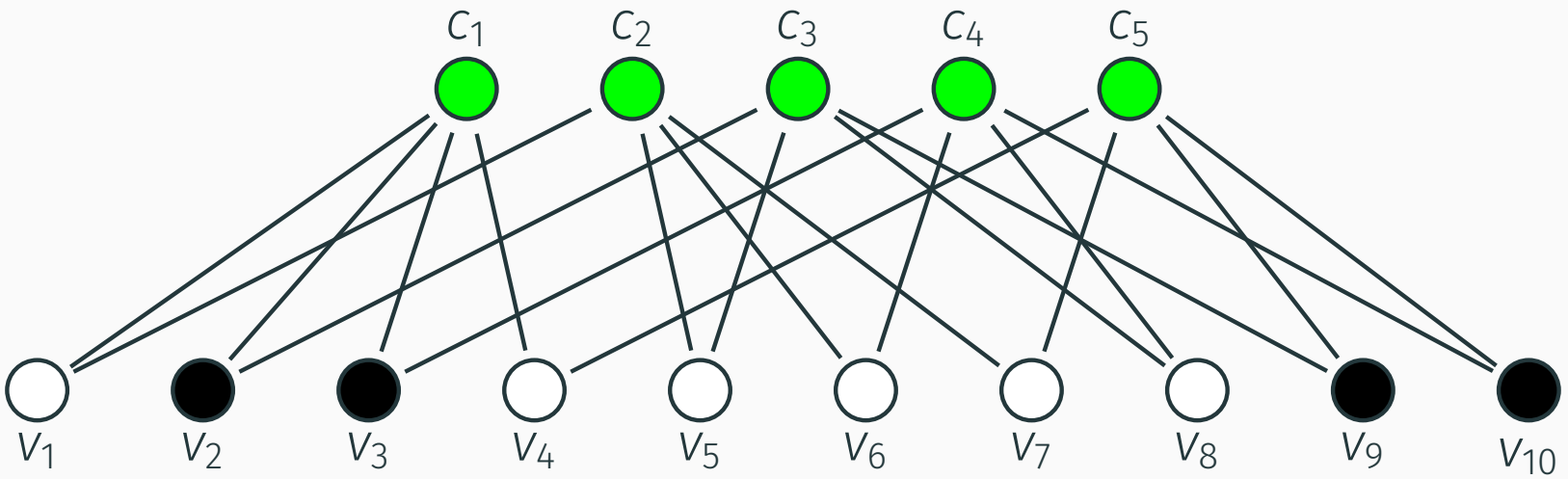


Figura 4: Funcionamento do algoritmo de *bit-flipping*.

Algoritmo de *bit-flipping*

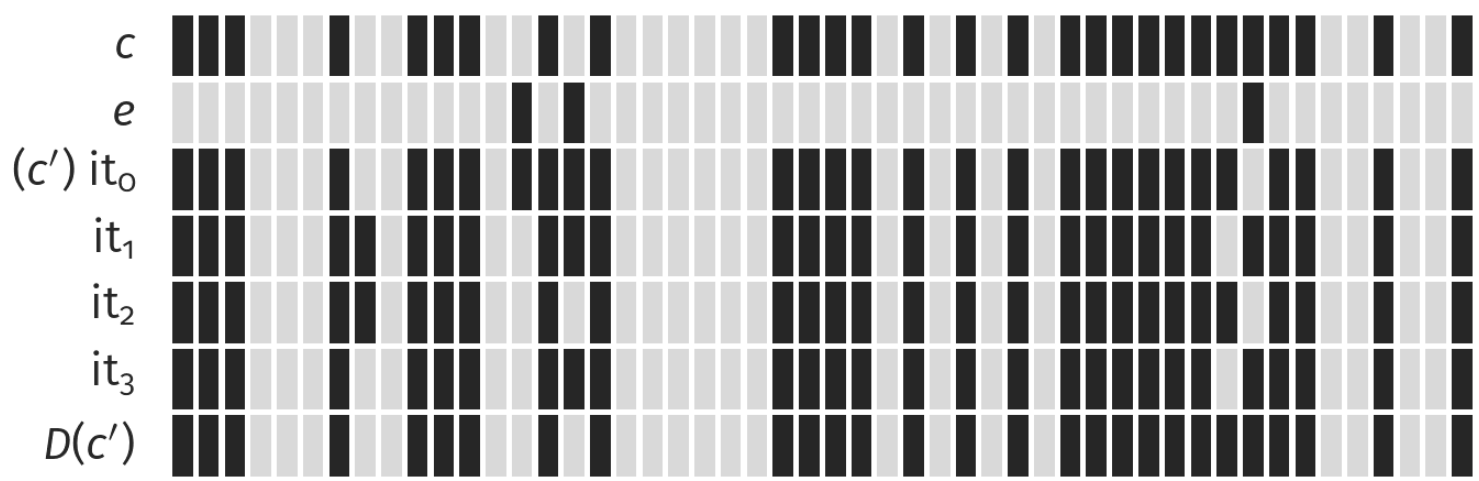
Algoritmo 6: Algoritmo de *bit-flipping*

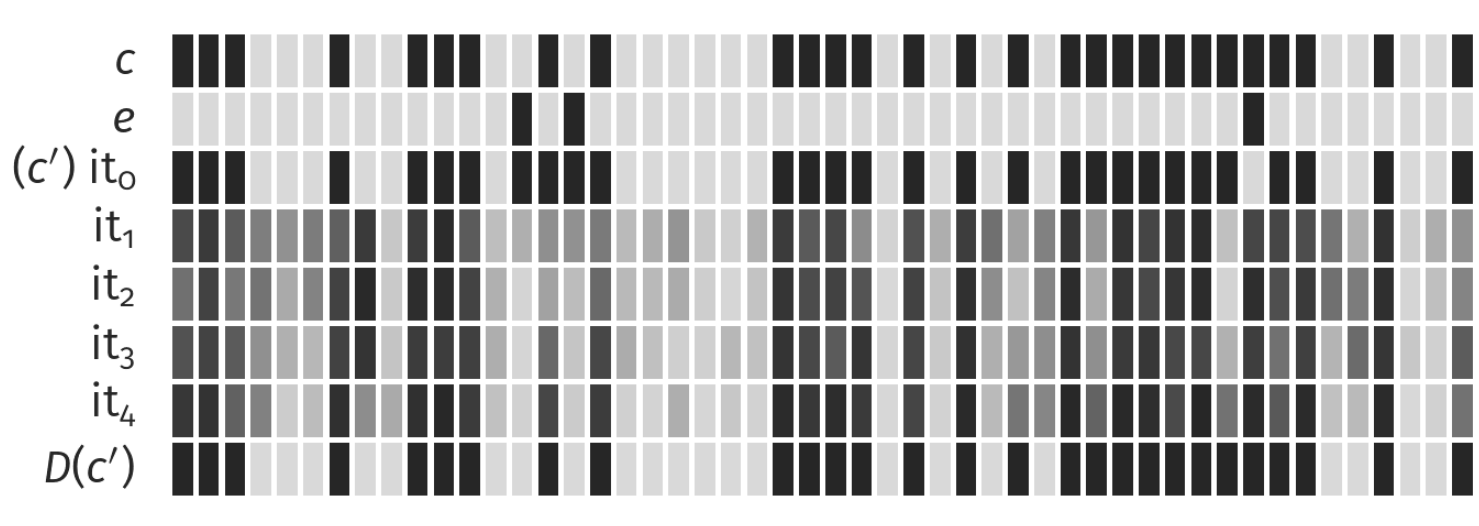
Entrada: $H, y, \texttt{max\_it}$

Saída: Decodificação de y, ou $\perp$ se exceder número de iterações

início
- $\texttt{it} \leftarrow 0$
- **enquanto** $yH^T \neq 0$ *e* $\texttt{it} < \texttt{max\_it}$ **faça**
  - **para** *cada* $j = 1, 2, \ldots, n$ **faça**
    - $f_j \leftarrow$ Número de vizinhos de v_j insatisfeitos
  - $\texttt{max\_upc} \leftarrow \max\{f_j\}$
  - **para** *cada* $j = 1, 2, \ldots, n$ **faça**
    - **se** $f_j \geq \texttt{max\_upc} - \delta$ **então**
      - $y_j \leftarrow \bar{y}_j$
- **se** $yH^T = 0$ **então**
  - devolva y
- **senão**
  - devolva $\perp$

Decodificação por Decisões Abruptas e Suaves





Códigos LDPC no esquema de McEliece

Uso no esquema de McEliece

- Códigos LDPC são ótimos códigos corretores de erros
- Porém são inseguros pois é possível recuperar a matriz esparsa

Ideia de Misoczki [9]

- Usar códigos LDPC com matriz ligeiramente mais densa
- Código fica mais forte contra ataques
- Ainda é possível usar algoritmos de decodificação para LDPC

Códigos QC-MDPC

Definição

Um **código** (n, r, w)**-MDPC** *é um código linear de comprimento* n*, e codimensão* r*, que admite uma matriz de verificação de paridade* H *cujas linhas têm mesmos pesos iguais a* $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!
- Matriz de paridade composta de blocos cíclicos

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!
- Matriz de paridade composta de blocos cíclicos
- Matriz geradora sistemática também de blocos cíclicos

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.*

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!
- Matriz de paridade composta de blocos cíclicos
- Matriz geradora sistemática também de blocos cíclicos
- Matriz geradora pode ser sistemática com conversão IND-CCA2

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a* $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!
- Matriz de paridade composta de blocos cíclicos
- Matriz geradora sistemática também de blocos cíclicos
- Matriz geradora pode ser sistemática com conversão IND-CCA2
- Matrizes são descritas pela **primeira linha e número de blocos**

Códigos QC-MDPC

Definição

Um ***código*** (n, r, w)***-MDPC*** *é um código linear de comprimento n, e codimensão r, que admite uma matriz de verificação de paridade H cujas linhas têm mesmos pesos iguais a* $w = \mathcal{O}\left(\sqrt{n \log n}\right)$.

O problema é que a matriz geradora pode ser densa

- Usar códigos **quase cíclicos**!
- Matriz de paridade composta de blocos cíclicos
- Matriz geradora sistemática também de blocos cíclicos
- Matriz geradora pode ser sistemática com conversão IND-CCA2
- Matrizes são descritas pela **primeira linha e número de blocos**

Definição

Quando H é quase cíclica, um código MDPC é dito um **código** (n, r, w)**-QC-MDPC**.

Matriz de paridade de um código QC-MDPC

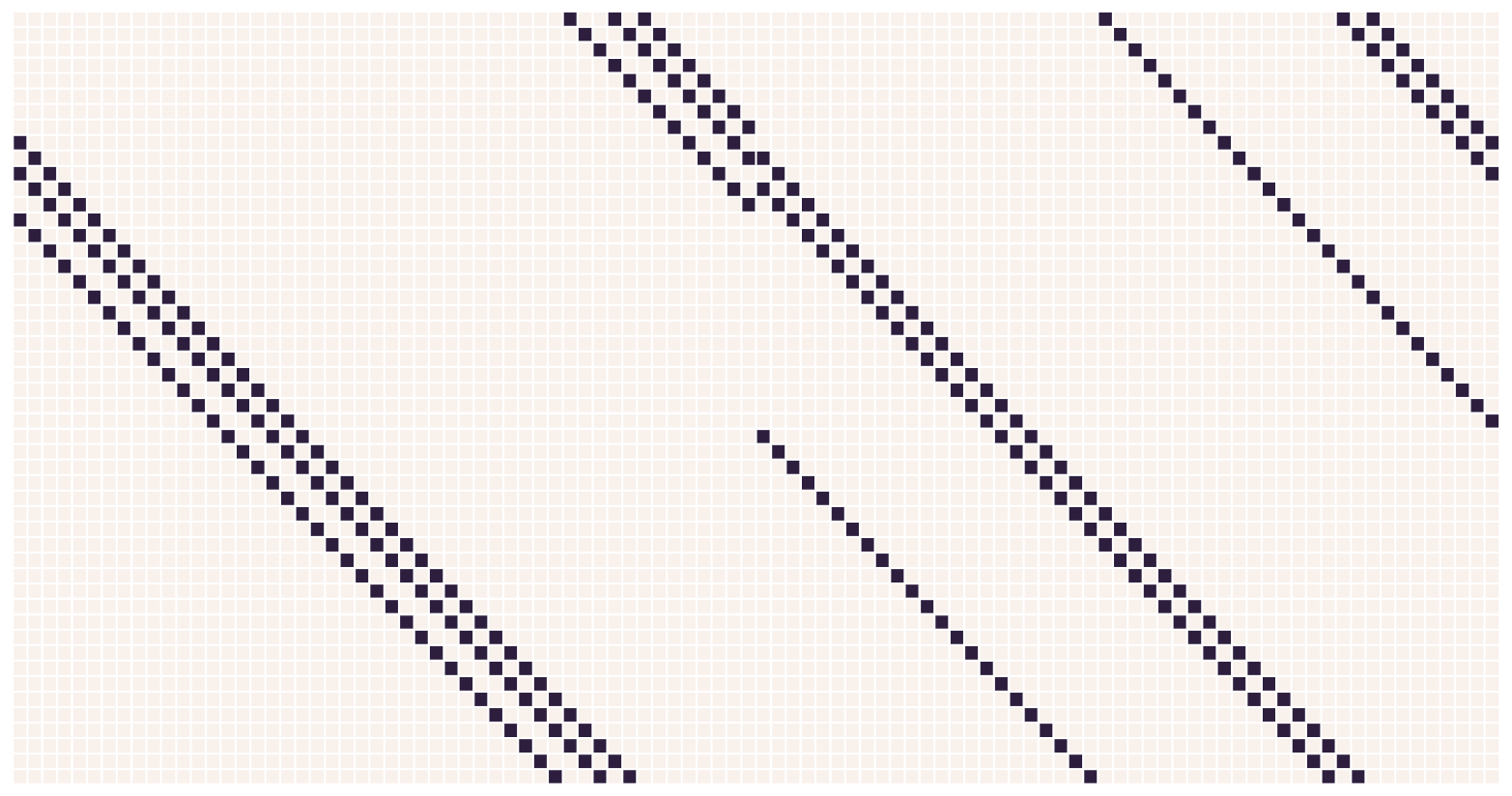


Figura 5: Matriz de paridade de código QC-MDPC com dois blocos e $w = 6$.

Matriz geradora de um código QC-MDPC

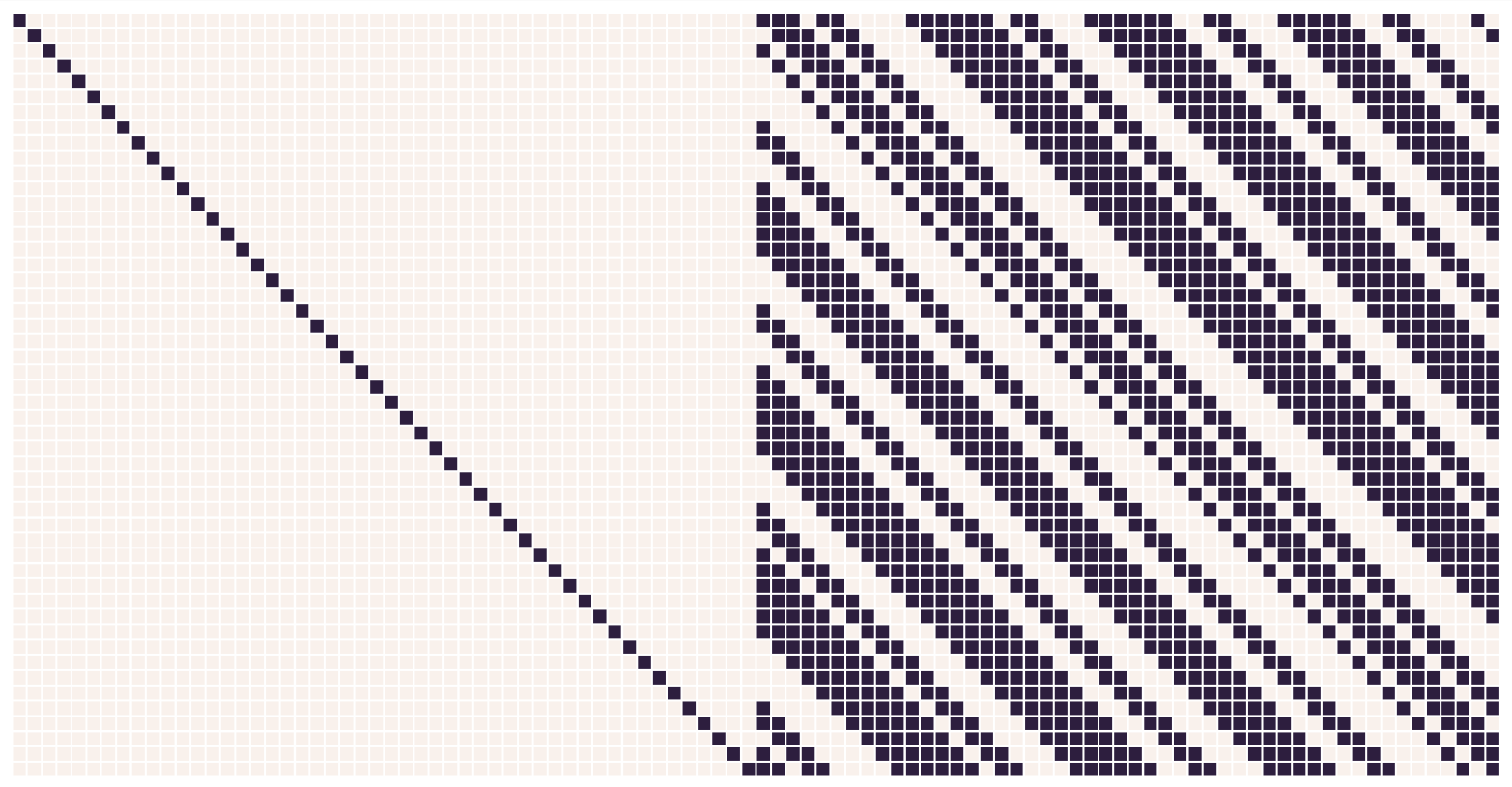


Figura 6: Matriz geradora de código QC-MDPC com dois blocos.

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa
- Segurança baseada na dificuldade de encontrar palavras de baixo peso

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa
- Segurança baseada na dificuldade de encontrar palavras de baixo peso
- Dispensa o uso das matrizes embaralhadoras S e P!

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa
- Segurança baseada na dificuldade de encontrar palavras de baixo peso
- Dispensa o uso das matrizes embaralhadoras S e P!
- Encriptação idêntica à do McEliece original

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa
- Segurança baseada na dificuldade de encontrar palavras de baixo peso
- Dispensa o uso das matrizes embaralhadoras S e P!
- Encriptação idêntica à do McEliece original
- Decriptação usa algoritmo de *bit-flipping*

QC-MDPC McEliece

Descrição do esquema com códigos QC-MDPC

- Chave pública é
  - g a primeira linha do segundo bloco da matriz G e
  - t número de erros que o código corrige com alta probabilidade
- Chave privada é a primeira linha esparsa
- Segurança baseada na dificuldade de encontrar palavras de baixo peso
- Dispensa o uso das matrizes embaralhadoras S e P!
- Encriptação idêntica à do McEliece original
- Decriptação usa algoritmo de *bit-flipping*
- Se o algoritmo falhar, peça reenvio de mensagem

Parâmetros sugeridos para QC-MDPC

Baseado nos melhores ataques de decodificação

Tabela 2: Parâmetros sugeridos para cada nível de segurança.

Segurança	n_0	n	r	w	t	Tamanho da Chave
80	2	9602	4801	90	84	4801
128	2	19714	9857	142	134	9857
256	2	65542	32771	274	264	32771

Perguntas?

Referências i


E. R. Berlekamp, R. J. McEliece, and H. C. Van Tilborg.
On the inherent intractability of certain coding problems.
IEEE Transactions on Information Theory, 24(3):384–386, 1978.


D. J. Bernstein, T. Chou, and P. Schwabe.
Mcbits: fast constant-time code-based cryptography.
In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 250–272. Springer, 2013.


N. T. Courtois, M. Finiasz, and N. Sendrier.
How to achieve a mceliece-based digital signature scheme.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 157–174. Springer, 2001.

Referências ii

J.-C. Faugere, V. Gauthier-Umana, A. Otmani, L. Perret, and J.-P. Tillich.

A distinguisher for high-rate mceliece cryptosystems.

IEEE Transactions on Information Theory, 59(10):6830–6844, 2013.

J.-C. Faugere, A. Otmani, L. Perret, F. De Portzamparc, and J.-P. Tillich.

Structural cryptanalysis of mceliece schemes with compact keys.

Designs, Codes and Cryptography, 79(1):87–112, 2016.

Referências iii


Q. Guo, T. Johansson, and P. Stankovski.
A key recovery attack on mdpc with cca security using decoding errors.
In *22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT), 2016*, 2016.


K. Kobara and H. Imai.
Semantically secure mceliece public-key cryptosystems-conversions for mceliece pkc.
In *International Workshop on Public Key Cryptography*, pages 19–35. Springer, 2001.


R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
Deep Space Network Progress Report, 44:114–116, 1978.

Referências iv

R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. Barreto.
Mdpc-mceliece: New mceliece variants from moderate density parity-check codes.
In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE, 2013.

P. W. Shor.
Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM Journal on Computing, 26(5):1481–1509, 1997.