Tópicos Avançados em Ciência da Computação I: Introdução à Teoria de Códigos para Criptografia Pós-quântica

Daniel Panario
School of Mathematics and Statistics
Carleton University

IC - Unicamp, Sala 351 do IC-3
das 13:30 as 18:30 em 16-17 de janeiro de 2020,
das 13:30 as 17:30 em 20-24 de janeiro de 2020

Introdução à Teoria de Códigos: Parte I

Daniel Panario
School of Mathematics and Statistics
Carleton University

16-24 de janeiro de 2020

Conteúdo da aula

- Introdução à teoria de códigos
- Códigos lineares
- Distância mínima
- Decodificação por síndrome
- Cotas
- Código dual
- Códigos cíclicos (introdução)
- Códigos quase-cíclicos (introdução)

Introdução à teoria de códigos

A teoria de códigos trata da detecção e correção de erros nas transmissões. Quando uma mensagem m é enviada por um canal, devido ao "ruído" no canal, podemos receber uma mensagem diferente da mensagem original.

Como podemos detectar que houve erros, e como podemos corrigir os erros?

Uma estratégia simples é mandar várias cópias da mensagem, e escolher a maioria em cada símbolo ("majority vote"). Se os erros não são muito frequentes podemos ter certa certeza sobre a corretude da mensagem recebida. O problema com essa estratégia é o custo do processo, que aumenta consideravelmente. O foco na teoria de códigos é combinar uma probabilidade pequena de erro com um custo razoável.

Na teoria de códigos uma suposição importante é que os erros não ocorrem frequentemente. Vamos supor isso nesse curso.

Introdução à teoria de códigos

A teoria de códigos trata da detecção e correção de erros nas transmissões. Quando uma mensagem m é enviada por um canal, devido ao "ruído" no canal, podemos receber uma mensagem diferente da mensagem original.

Como podemos detectar que houve erros, e como podemos corrigir os erros?

Uma estratégia simples é mandar várias cópias da mensagem, e escolher a maioria em cada símbolo ("majority vote"). Se os erros não são muito frequentes podemos ter certa certeza sobre a corretude da mensagem recebida. O problema com essa estratégia é o custo do processo, que aumenta consideravelmente. O foco na teoria de códigos é combinar uma probabilidade pequena de erro com um custo razoável.

Na teoria de códigos uma suposição importante é que os erros não ocorrem frequentemente. Vamos supor isso nesse curso.

Introdução à teoria de códigos (cont)

Claude Shannon introduziu, em 1948, o embasamento para a existência de códigos que possam transmitir informação com uma taxa ("rate") próxima da capacidade do canal, com uma probabilidade pequena e arbitrária de erro.

Outros trabalhos importantes desses anos incluem o código Golay (1949), e especialmente Hamming (1950) para códigos lineares. Nos 1960's, os trabalhos fundamentais na teoria algébrica de códigos apareceram: códigos BCH (devidos a Bose, Ray-Chaudhuri e Hocquenghem), e Reed-Solomon. Esses trabalhos estabelecem forte conexão com os corpos finitos.

Associando cada dígito de certo código com um elemento num corpo finito, é possivel derivar uma equação algébrica cujas raizes representam o lugar dos erros na transmissão. Assim, estamos na área dos polinômios sobre corpos finitos que, como veremos, também têm um papel crucial em vários tipos de códigos usados em criptografia pós-quântica.

Introdução à teoria de códigos (cont)

Há muitas conexões entre os corpos finitos e a teoria de códigos junto a outras áreas matemáticas tais como a geometria algébrica, os planejamentos combinatórios e a geometria projetiva. Não veremos essas conexões neste curso.

Uma revolução na teoria de códigos aconteceu nos 1990's com o surgimento de métodos que atingem taxas de transmissão próximas da capacidade do canal estabelecida por Shannon. Esses métodos (códigos LDPC, turbo e polares, entre outros) usam majoritariamente outras áreas matemáticas como a teoria de probabilidade e a teoria de grafos.

Idéia

Queremos transmitir uma mensagem através de um canal com ruído. A mensagem consiste de uma sequência finita de k símbolos de um certo alfabeto. Consideramos o alfabeto como sendo um corpo finito.

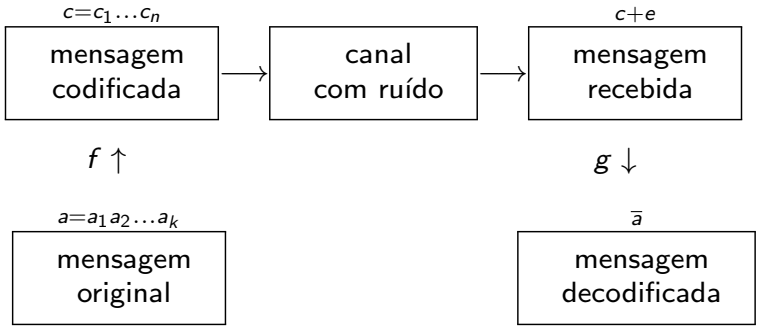
A mensagem a é codificada por uma palavra-código c de n símbolos, por meio de uma função f chamada de esquema de codificação:

$$\begin{array}{rccc} f: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & a = (a_1, \ldots, a_k) & \longmapsto & c = (c_1, \ldots, c_n) \end{array},$$

onde $n > k$. A idéia é enviar a palavra $c = f(a)$ no canal, de maneira que a mensagem recebida, digamos, $c + e$, seja tal que o erro e possa ser detectado e/ou corrigido.

O código é o conjunto imagem de f, ou seja, o conjunto de todas as palavras-código. A função $g : \mathbb{F}_q^n \to \mathbb{F}_q^k$, que associa a mensagem recebida à mensagem decodificada, é chamada de esquema de decodificação. O seguinte diagrama reúne todos esses conceitos:

Idéia (cont)



- Esquema de codificação: $(n > k)$

$$\begin{array}{rccc} f: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & a = (a_1, \ldots, a_k) & \longmapsto & c = (c_1, \ldots, c_n) \end{array}$$

- c = palavra-código; e = erro
- Objetivo: detectar e/ou corrigir e

Códigos lineares

Definição

Seja H uma matriz $(n-k) \times n$ com elementos em $\mathbb{F}_q$. Dizemos que

$$C = \{c \in \mathbb{F}_q^n : Hc^T = 0\}$$

é um código linear sobre $\mathbb{F}_q$, também denotado por $C(n,k)$, onde n é o comprimento e k é a dimensão do código. Os elementos de C são chamados palavras-código e H é chamada de matriz de paridade de C. Se $q = 2$, dizemos que C é um código binário.
Se G é uma matriz $k \times n$ cujo espaço gerado pelas linhas é igual a C, então dizemos que G é uma matriz geradora de C.

Obs.: $C(n,k)$ é um subespaço k-dimensional de $\mathbb{F}_q^n$.

Exemplo

Seja H uma matriz de paridade sobre $\mathbb{F}_2$:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Temos que $n = 7$, $n - k = 3$, então $k = 4$. O código é um subespaço de $\mathbb{F}_2^7$ de dimensão 4 (ou seja, temos $2^4 = 16$ palavras de código (dos $128 = 2^7$ elementos do espaço).

As palavras de código satisfazem $Hc^T = 0$. Temos que uma base para o subespaço código é (verificar!):

$$\{(1,0,0,0,1,1,0),(0,1,0,0,1,0,1),(0,0,1,0,0,1,1),(0,0,0,1,1,1,1)\}.$$

Códigos em forma sistemática

Se a matriz de paridade H é da forma $H = (A\, I_{n-k})$, então C é um código em forma sistemática.

Nesse caso temos que a matriz geradora do código satisfaz $G = (I_k \; -A^T)$.

(No caso particular em que $q = 2$, temos A em vez de $-A$.)

A propriedade importante dessa matrix é que gera o código.
De fato, como $Hc^T = 0$ com $H = (A\, I_{n-k})$, temos que

$$c^T = \begin{pmatrix} I_k \\ -A \end{pmatrix} a^T = \left[a \left(I_k \; -A^T \right) \right]^T,$$

onde $a = (a_1, a_2, \ldots, a_k)$, $c = (c_1, c_2, \ldots, c_n)$. Como $\left(I_k \; -A^T\right)$ é G, temos que G pode ser usada para gerar o código:

$$aG = c.$$

Exemplo (cont)

Consideremos de novo a matriz de paridade H sobre $\mathbb{F}_2$:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Temos que $n = 7$, $n - k = 3$, então $k = 4$.
Como H está dada em forma sistemática $H = (A\, I_{n-k}) = (A\, I_3)$, temos que $G = (I_k \ -A^T) = (I_4 \ -A^T)$ e, como estamos em $\mathbb{F}_2$ obtemos:

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

Excercício: verificar que G é uma matriz geradora do código, gerando todas as palavras-código calculando $aG = c$ para todo $a \in \mathbb{F}_2^4$.

Código verificador de paridade

Esquema de codificação binária f:

$$(a_1 a_2 \cdots a_k) \quad \longmapsto \quad (c_1 c_2 \cdots c_k c_{k+1}),$$

onde $c_i = a_i$ para $i = 1, \ldots, k$ e $c_{k+1} = \sum_{i=1}^{k} a_i$, que é o símbolo de controle pois, em $\mathbb{F}_2$,

$$\sum_{i=1}^{k+1} c_i = \sum_{i=1}^{k} a_i + c_{k+1} = 2 \sum_{i=1}^{k} a_i = 0.$$

Assim, se a soma dos dígitos recebidos não é 0, há um erro.
Este código detecta um erro, mas não o corrige, pois não há como identificar a coordenada do erro.

Se há dois erros, eles compensarão a paridade. Logo, este código não é capaz de detectar dois ou mais erros.

Neste caso, $H = (11 \cdots 1)$ e $G = (I_k \ \mathbf{1})$ (verificar!).

Código de repetição

Cada palavra-código contém um símbolo de mensagem e $n-1$ símbolos de controle, de maneira que

$$c_2 = c_3 = \cdots = c_n = a_1.$$

Logo, $f : \mathbb{F}_q \to \mathbb{F}_q^n$ é dado por

$$a_1 \quad \longmapsto \quad (a_1 a_1 \cdots a_1).$$

A matriz de paridade é $H = (-\mathbf{1}\, I_{n-1})$.

Este código detecta até $n-1$ erros, já que se há quaisquer dois símbolos com valores diferentes, deve haver algum erro. Se todos os símbolos são os mesmos, então não podemos detectar se houve ou não mudanças na transmissão.

Código de repetição (cont)

Por outro lado, o código de repetição pode corrigir até $\lfloor (n-1)/2 \rfloor$ erros. De fato, se há no máximo $\lfloor (n-1)/2 \rfloor$ erros, então é possível deduzir a mensagem original corretamente.

Exemplo: Suponhamos que $n = 10$ e que a mensagem original seja 1. Então, se recebermos três 0's e sete 1's, saberemos que houve erros. Como há, no máximo, $\lfloor (10-1)/2 \rfloor = 4$ erros, sabemos que a mensagem original é 1.

Distância

Necessitamos a noção de distância para corrigir erros:

1. $d(x, y) \geq 0$, com igualdade somente quando $x = y$;
2. $d(x, y) = d(y, x)$ para todo $x, y \in \mathbb{F}_q^n$;
3. $d(x, z) \leq d(x, y) + d(y, z)$ para todo $x, y, z \in \mathbb{F}_q^n$.

Definição

Se x, $y \in \mathbb{F}_q^n$, então

1. *A distância de Hamming $d(x, y)$ entre x e y é o número de coordenadas em que x e y diferem.*
2. *O peso de Hamming $w(x)$ é o número de coordenadas de x que são diferentes de 0.*

Temos que $d(x, y) = w(x - y)$.

Exemplo: $d((1, 0, 1, 0, 1), (0, 1, 1, 1, 0)) = 4 = w(1, 1, 0, 1, 1)$

Distância (cont)

Exercício: provar que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$.

Na teoria de códigos usam-se outras métricas. Por exemplo, a métrica de Lee, que se define sobre um alfabeto de q elementos como

$$\text{dist}(x, y) = \sum_{i=1}^{n} \min\{x_i - y_i, q - (x_i - y_i)\}.$$

Para $q = 2$ e $q = 3$ a métrica de Lee coincide com a métrica de Hamming. Quando o alfabeto é o grupo aditivo $\mathbb{Z}_q$, a distância de Lee está relacionada com o caminho mais curto no grafo de Cayley.

As propostas ao NIST, Rollo e RQC, como veremos, usam a métrica do posto (rank).

Distância entre vetores

Agora podemos definir erro.

Definição

Se c é uma palavra de código e $y \in \mathbb{F}_q^n$ é a palavra recebida, então o erro é definido como $e = y - c$. É um vetor $e_1 e_2 \dots e_n$.

Definição

Seja t um inteiro positivo. Um código $C \in \mathbb{F}_q^n$ corrige t erros se, para cada palavra recebida $y \in \mathbb{F}_q^n$, há, no máximo, um $c \in C$ tal que $d(c, y) \leq t$.

A correção do erro é então feita por verossimilhança.

Distância entre vetores

Agora podemos definir erro.

Definição

Se c é uma palavra de código e $y \in \mathbb{F}_q^n$ é a palavra recebida, então o erro é definido como $e = y - c$. É um vetor $e_1 e_2 \dots e_n$.

Definição

Seja t um inteiro positivo. Um código $C \in \mathbb{F}_q^n$ corrige t erros se, para cada palavra recebida $y \in \mathbb{F}_q^n$, há, no máximo, um $c \in C$ tal que $d(c, y) \leq t$.

A correção do erro é então feita por verossimilhança.

Definição

A distância mínima de um código C é definida por $d_C = \min_{\substack{u,v \in C \\ u \neq v}} d(u,v)$.

Teorema

Um código C pode corrigir até t erros, se $d_C \geq 2t+1$.

Demonstração.

Seja $B_t(x) = \{y \in \mathbb{F}_q^n : d(x,y) \leq t\}$. A decodificação por verossimilhança garante que cada palavra recebida com no máximo t erros deve estar numa bola com centro na palavra transmitida e raio t. Suponhamos que $u \in B_t(x) \cap B_t(y)$ onde $x, y \in C$. Então $d(x,y) \leq d(x,u) + d(u,y) \leq 2t$, o que é uma contradição. □

Definição

A distância mínima de um código C é definida por $d_C = \min_{\substack{u,v \in C \\ u \neq v}} d(u,v)$.

Teorema

Um código C pode corrigir até t erros, se $d_C \geq 2t+1$.

Demonstração.

Seja $B_t(x) = \{y \in \mathbb{F}_q^n : d(x,y) \leq t\}$. A decodificação por verossimilhança garante que cada palavra recebida com no máximo t erros deve estar numa bola com centro na palavra transmitida e raio t. Suponhamos que $u \in B_t(x) \cap B_t(y)$ onde $x, y \in C$. Então $d(x,y) \leq d(x,u) + d(u,y) \leq 2t$, o que é uma contradição. □

Exemplo (cont)

Seja, de novo, H uma matriz de paridade sobre $\mathbb{F}_2$:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Vimos que esse código é um subespaço de $\mathbb{F}_2^7$ de dimensão 4 com base:

$$\{(1,0,0,0,1,1,0),(0,1,0,0,1,0,1),(0,0,1,0,0,1,1),(0,0,0,1,1,1,1)\}.$$

Considerando todas as palavras deste código, temos que a distância mínima satisfaz $d_C \geq 3$ (excercício!).

Portanto, esse código pode corrigir até 1 erro.

Teorema

Um código linear C com matriz de paridade H tem distância mínima $d_C \geq s+1$, se e somente se quaisquer s colunas de H são linearmente independentes.

Demonstração.

Suponhamos que H tenha s colunas ld's: $D_{i_1}, D_{i_2}, \ldots, D_{i_s}$. Então, existem constantes $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_s}$, não todas nulas, tais que $\sum_{j=1}^{s} \alpha_{i_j} D_{i_j} = 0$. Seja $c \in \mathbb{F}_q^n$ tal que $c_{i_j} = \alpha_{i_j}$, para $j = 1, 2, \ldots, s$, e todas as outras coordenadas de c são nulas. Temos que $Hc^T = \sum_{j=1}^{s} \alpha_{i_j} D_{i_j} = 0$. Logo, $c \in C$. Além disso, $c \neq 0$ e, assim, $d_C \leq s$.
Por outro lado, se quaisquer s colunas de H são li's, então não existe $c \in C$ não nulo de peso no máximo s. De fato, se existe uma palavra-código $c \neq 0$ com $w(c) \leq s$, então $\sum_{j=1}^{s} c_{i_j} H_{i_j} = 0$ implica que $c_{i_j} = 0$, para todo $j = 1, 2, \ldots, s$. Assim, o único $c \in C$ com $w(c) \leq s$ é $c = 0$. □

Teorema

Um código linear C com matriz de paridade H tem distância mínima $d_C \geq s+1$, se e somente se quaisquer s colunas de H são linearmente independentes.

Demonstração.

Suponhamos que H tenha s colunas ld's: $D_{i_1}, D_{i_2}, \ldots, D_{i_s}$. Então, existem constantes $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_s}$, não todas nulas, tais que $\sum_{j=1}^{s} \alpha_{i_j} D_{i_j} = 0$. Seja $c \in \mathbb{F}_q^n$ tal que $c_{i_j} = \alpha_{i_j}$, para $j = 1, 2, \ldots, s$, e todas as outras coordenadas de c são nulas. Temos que $Hc^T = \sum_{j=1}^{s} \alpha_{i_j} D_{i_j} = 0$. Logo, $c \in C$. Além disso, $c \neq 0$ e, assim, $d_C \leq s$.
Por outro lado, se quaisquer s colunas de H são li's, então não existe $c \in C$ não nulo de peso no máximo s. De fato, se existe uma palavra-código $c \neq 0$ com $w(c) \leq s$, então $\sum_{j=1}^{s} c_{i_j} H_{i_j} = 0$ implica que $c_{i_j} = 0$, para todo $j = 1, 2, \ldots, s$. Assim, o único $c \in C$ com $w(c) \leq s$ é $c = 0$. □

Exemplo (cont)

Seja, de novo, H uma matriz de paridade sobre $\mathbb{F}_2$:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Quaisquer duas colunas de H são linearmente independentes.
Assim, $d_C \geq 3$. No entanto, como

$$\text{coluna } 4 = \text{coluna } 3 + \text{coluna } 5,$$

temos que $d_C < 4$, ou seja, $d_C = 3$. Logo, C corrige um erro.

Exemplo (cont.)

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Temos que $n = 7$ e $n - k = 3$, então $k = 4$, e $Hc^T = 0$ gera o sistema

$$\begin{array}{ccccccccc} c_1 & +c_2 & +0 & +c_4 & +c_5 & +0 & +0 & = & 0 \\ c_1 & +0 & +c_3 & +c_4 & +0 & +c_6 & +0 & = & 0 \\ 0 & +c_2 & +c_3 & +c_4 & +0 & +0 & +c_7 & = & 0 \end{array}$$

As palavras código são da seguinte forma, onde $c_i \in \mathbb{F}_2$,

$$(c_1, c_2, c_3, c_4, c_1 + c_2 + c_4, c_1 + c_3 + c_4, c_2 + c_3 + c_4).$$

Por exemplo $(1, 0, 0, 0, 1, 1, 1)$ não está no código (verifique!).

Decodificação

Definição

O vetor $S(y) = Hy^T \in \mathbb{F}_q^{n-k}$ é chamado de síndrome de y.

Teorema

1. $S(y) = 0$ *se e somente se* $y \in C$.
2. $S(y) = S(z)$ *se e somente se* $y + C = z + C$.

Demonstração.

(1) segue imediatamente da definição de S. Para provar (2), observamos que $S(y) = S(z)$ se e somente se $H(y - z)^T = 0$. Isto significa que $y - z \in C$. □

Definição

Seja $C(n,k)$ um código linear sobre $\mathbb{F}_q$. Um elemento de peso mínimo em $a+C \in \mathbb{F}_q^n/C$ é um líder da classe lateral. Se há mais de um vetor com peso mínimo em $a+C$, escolhemos qualquer um deles para ser o líder.

linha / mensagem	$00\ldots0$	$00\ldots01$	$\ldots$	$(q-1)\ldots(q-1)$
palavras-código	$c^{(1)}$	$c^{(2)}$	$\ldots$	$c^{(q^k)}$
classes laterais	$a^{(1)}+c^{(1)}$	$a^{(1)}+c^{(2)}$	$\ldots$	$a^{(1)}+c^{(q^k)}$
	$a^{(2)}+c^{(1)}$	$a^{(2)}+c^{(2)}$	$\ldots$	$a^{(2)}+c^{(q^k)}$
	$\vdots$	$\vdots$	$\ddots$	$\vdots$
restantes	$\underbrace{a^{(s)}+c^{(1)}}_{\text{coluna dos líderes}}$	$a^{(s)}+c^{(2)}$	$\ldots$	$a^{(s)}+c^{(q^k)}$

Definição

Seja $C(n,k)$ um código linear sobre $\mathbb{F}_q$. Um elemento de peso mínimo em $a+C \in \mathbb{F}_q^n/C$ é um líder da classe lateral. Se há mais de um vetor com peso mínimo em $a+C$, escolhemos qualquer um deles para ser o líder.

linha / mensagem	$00\ldots0$	$00\ldots01$	$\ldots$	$(q-1)\ldots(q-1)$
palavras-código	$c^{(1)}$	$c^{(2)}$	$\ldots$	$c^{(q^k)}$
classes laterais	$a^{(1)}+c^{(1)}$	$a^{(1)}+c^{(2)}$	$\ldots$	$a^{(1)}+c^{(q^k)}$
	$a^{(2)}+c^{(1)}$	$a^{(2)}+c^{(2)}$	$\ldots$	$a^{(2)}+c^{(q^k)}$
	$\vdots$	$\vdots$	$\ddots$	$\vdots$
restantes	$\underbrace{a^{(s)}+c^{(1)}}_{\text{coluna dos líderes}}$	$a^{(s)}+c^{(2)}$	$\ldots$	$a^{(s)}+c^{(q^k)}$

Observações

- Queremos decodificar y. Digamos que $y \in a^{(i)} + C$, onde $0 \leq i \leq s$. Então, $e = y - c \in a^{(i)} + C$.
- Pela decodificação por verossimilhança, o erro é o líder da classe lateral de y.
- Assim $e = a^{(i)}$ e a mensagem transmitida é

$$x = y - e = a^{(i)} + c^{(j)} - a^{(i)} = c^{(j)}.$$

- Como encontrar e? Calcule $S(y)$ e procure pelo líder e, tal que $S(e) = S(y)$.

Exemplo

Seja $C(4, 2)$ um código binário linear com matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ e } H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

linha / mensagem	00	01	10	11	Síndrome
palavras-código	0000	0110	1011	1101	$\binom{0}{0}$
	0001	0111	1010	1100	$\binom{0}{1}$
classes	0010	0100	1001	1111	$\binom{1}{0}$
laterais restantes	1000 (coluna dos líderes)	1110	0011	0101	$\binom{1}{1}$

Se $y = 0101$, então $S(y) = \binom{1}{1}$ e

$$x = y - e = 0101 - 1000 = (1101 + 1000) - 1000 = 1101.$$

A palavra transmitida é 1101 com mensagem original 11.

Exemplo

Seja $C(4,2)$ um código binário linear com matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ e } H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

linha / mensagem	00	01	10	11	Síndrome
palavras-código	0000	0110	1011	1101	$\binom{0}{0}$
	0001	0111	1010	1100	$\binom{0}{1}$
classes	0010	0100	1001	1111	$\binom{1}{0}$
laterais restantes	$\underbrace{1000}_{\text{coluna dos líderes}}$	1110	0011	0101	$\binom{1}{1}$

Se $y = 0101$, então $S(y) = \binom{1}{1}$ e

$$x = y - e = 0101 - 1000 = (1101 + 1000) - 1000 = 1101.$$

A palavra transmitida é 1101 com mensagem original 11.

Teorema

Num código binário linear $C(n,k)$ com matriz de paridade H, a síndrome é a soma das colunas de H que correspondem às posições onde os erros ocorreram.

Demonstração.

Sejam $y \in \mathbb{F}_2^n$ a mensagem recebida, x a palavra-código transmitida e e o erro. Vamos supor que as coordenadas não nulas de e sejam $e_{i_1}, e_{i_2}, \ldots, e_{i_k}$. Temos que

$$\begin{aligned} S(y) &= S(x+e) = S(x) + S(e) = Hx^T + He^T = He^T \\ &= H_{i_1} e_{i_1} + H_{i_2} e_{i_2} + \cdots + H_{i_k} e_{i_k} = H_{i_1} + H_{i_2} + \cdots + H_{i_k}, \end{aligned}$$

onde H_i é a i-ésima coluna de H. □

Teorema

Num código binário linear $C(n,k)$ com matriz de paridade H, a síndrome é a soma das colunas de H que correspondem às posições onde os erros ocorreram.

Demonstração.

Sejam $y \in \mathbb{F}_2^n$ a mensagem recebida, x a palavra-código transmitida e e o erro. Vamos supor que as coordenadas não nulas de e sejam $e_{i_1}, e_{i_2}, \ldots, e_{i_k}$. Temos que

$$\begin{aligned} S(y) &= S(x+e) = S(x) + S(e) = Hx^T + He^T = He^T \\ &= H_{i_1} e_{i_1} + H_{i_2} e_{i_2} + \cdots + H_{i_k} e_{i_k} = H_{i_1} + H_{i_2} + \cdots + H_{i_k}, \end{aligned}$$

onde H_i é a i-ésima coluna de H. □

Cotas

Consideramos códigos lineares. Um código $[n,k,d]$ é um código de comprimento n, dimensão k e distância mínima d. Em aplicacões, geralmente, queremos códigos com distância mínima d grande, já que, se o canal de transmisão troca no máximo $(d-1)/2$ símbolos numa palavra w, transformando-a numa n-tupla w', então w é a única palavra de código cuja distância de w' é, no máximo, $(d-1)/2$ e a n-tupla w' recebida é decodificada como w.

Também é desejavel ter uma dimensão k grande; isto significa que o código pode transmitir grandes quantidades de informacão. Porém, para um comprimento n fixo, não podemos ter d e k grandes, devido à cota de Singleton.

Cota de Singleton

Teorema (Cota de Singleton)

Seja C um código $[n, k, d]$ linear sobre $\mathbb{F}_q$. Então

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

Demonstração.

Seja W o subespaço de $\mathbb{F}_q^n$ dado por $W = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ para todo } i \geq d\}$. Como $d(w, 0) \leq d - 1$ para todos os $w \in W$, temos $W \cap C = \{0\}$. De $\dim W = d - 1$ obtemos $k + (d - 1) \leq n$, que prova o teorema. □

Códigos com $d = n - k + 1$ são chamados MDS (distância máxima separável). Esses códigos conseguem atingir a distância mínima mais alta possível. São códigos importantes na prática com usos em criptografia simétrica, mas não vamos nos aprofundar neles neste curso.

Cota de Singleton

Teorema (Cota de Singleton)

Seja C um código $[n, k, d]$ linear sobre $\mathbb{F}_q$. Então

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

Demonstração.

Seja W o subespaço de $\mathbb{F}_q^n$ dado por $W = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ para todo } i \geq d\}$. Como $d(w, 0) \leq d - 1$ para todos os $w \in W$, temos $W \cap C = \{0\}$. De $\dim W = d - 1$ obtemos $k + (d - 1) \leq n$, que prova o teorema. □

Códigos com $d = n - k + 1$ são chamados MDS (distância máxima separável). Esses códigos conseguem atingir a distância mínima mais alta possível. São códigos importantes na prática com usos em criptografia simétrica, mas não vamos nos aprofundar neles neste curso.

Cota de Hamming

Teorema (Cota de Hamming)

Seja C un código corretor de t erros sobre $\mathbb{F}_q$ de comprimento n, com M palavras de código. Então,

$$M\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\leq q^n.$$

Demonstração.

Consideremos as bolas de raio t e centro c em C. Contando os elementos nas bolas, temos

$$1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t.$$

O primeiro termo representa a palavra de código; os termos seguintes representam os elementos nas bolas cuja distância ao centro c é $1,2,\ldots,t$, respectivamente. Como C corrige t erros, as bolas são disjuntas. □

Cota de Hamming

Teorema (Cota de Hamming)

Seja C un código corretor de t erros sobre $\mathbb{F}_q$ de comprimento n, com M palavras de código. Então,

$$M\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\leq q^n.$$

Demonstração.

Consideremos as bolas de raio t e centro c em C. Contando os elementos nas bolas, temos

$$1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t.$$

O primeiro termo representa a palavra de código; os termos seguintes representam os elementos nas bolas cuja distância ao centro c é $1,2,\ldots,t$, respectivamente. Como C corrige t erros, as bolas são disjuntas. □

Exemplo: códigos com $n = 17$, $k = 10$ e $q = 2$ não podem corrigir 2 erros dado que a seguinte desigualdade não é satisfeita:

$$2^{10}\left(1 + \binom{17}{1} + \binom{17}{2}\right) \leq 2^{17}.$$

Observação: há outras cotas importantes devidas a Plotkin e a Gilbert-Varshamov.

Código dual

Consideremos o produto interno usual em $\mathbb{F}_q^n$, denotado por $\langle\ ,\ \rangle$.

Definição

Se $C \subset \mathbb{F}_q^n$ é um código, então

$$C^{\perp} := \{w \in \mathbb{F}_q^n : \langle w, v\rangle = 0 \ \textit{para todo}\ v \in C\}$$

chama-se o código dual de C.

Propriedades dos códigos duais

Pode-se provar que $H_C = G_{C^\perp}$. Então, o espaço das linhas de H do código C é $C^\perp$. Ainda mais, temos as seguintes propriedades:

1. Se o código C é um subespaço k–dimensional de $\mathbb{F}_q^n$, então o código dual é um subespaço $(n-k)$–dimensional de $\mathbb{F}_q^n$.
2. Se C tem matriz de paridade H, então $C^\perp$ tem matriz geradora H.
3. Se C tem matriz geradora G, então $C^\perp$ tem matriz de paridade G.

Introdução aos códigos cíclicos

Definição

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico, se $(c_0, \ldots, c_{n-1}) \in C$ implica que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Exemplo: $C = \{000, 110, 101, 011\}$ é um código cíclico.

Códigos cíclicos podem ser caracterizados com polinômios.

Teorema

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico se e somente se C é um ideal de $\mathbb{F}_q[x]/(x^n-1)$.

Vamos retornar a esse teorema após rever importantes resultados de polinômios sobre corpos finitos.

Introdução aos códigos cíclicos

Definição

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico, se $(c_0,\ldots,c_{n-1}) \in C$ implica que $(c_{n-1},c_0,\ldots,c_{n-2}) \in C$.

Exemplo: $C = \{000, 110, 101, 011\}$ é um código cíclico.

Códigos cíclicos podem ser caracterizados com polinômios.

Teorema

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico se e somente se C é um ideal de $\mathbb{F}_q[x]/(x^n-1)$.

Vamos retornar a esse teorema após rever importantes resultados de polinômios sobre corpos finitos.

Introdução aos códigos quase-cíclicos

Definição

Um código é quase-cíclico se existe um inteiro s tal que cada deslocamento cíclico de s posições de uma palavra de código resulta numa palavra de código.

Claramente, um código cíclico é um código quase-cíclico com $s = 1$.

Exemplo: $C = \{0000, 0011, 1100, 0101\}$ é um código quase-cíclico com $s = 2$.

Códigos quase-cíclicos também podem ser caracterizados com polinômios sobre corpos finitos.

Introdução aos códigos quase-cíclicos

Definição

Um código é quase-cíclico se existe um inteiro s tal que cada deslocamento cíclico de s posições de uma palavra de código resulta numa palavra de código.

Claramente, um código cíclico é um código quase-cíclico com $s = 1$.

Exemplo: $C = \{0000, 0011, 1100, 0101\}$ é um código quase-cíclico com $s = 2$.

Códigos quase-cíclicos também podem ser caracterizados com polinômios sobre corpos finitos.

Exemplo de código quase-cíclico

Exercício: mostrar que a matriz de paridade seguinte é de um código quase-cíclico com $s = 2$:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Sugestão:

Primeiro achar todas as palavras do código. Depois verificar que é um código quase-cíclico com $s = 2$.

É também quase-cíclico para algum outro valor de s? Dá para inferir algum resultado?

Há várias construções desses códigos. Uma das mais comuns usa matrizes circulantes.

Introdução aos códigos quase-cíclicos (cont)

Uma matriz circulante é uma matriz quadrada onde cada linha é um deslocamento circular de uma posição à direita da linha anterior; assim, a última posição de uma linha se torna a primeira posição da linha seguinte. Essas matrizes são completamente definidas pela primeira linha.

Uma matriz circulante por blocos é formada pela concatenação de matrizes circulantes quadradas de mesmo tamanho. O tamanho da matriz é a ordem da matriz. O índice de uma matriz circulante por blocos é o número de blocos circulantes na linha.

Definição

Um código quase-cíclico (QC) de índice n_0 e ordem r é um código linear com uma matriz circulante por blocos como matriz geradora. Um QC-código $[n_0, k_0]$ é um código quase-cíclico de índice n_0, comprimento $n_0 r$ e dimensão $k_0 r$.