Uma Introdução à Teoria de Códigos

Fábio Meneghetti

Instituto de Matemática, Estatística e Computação Científica
Universidade Estadual de Campinas

24 de agosto de 2016

História

Figura: Richard Hamming

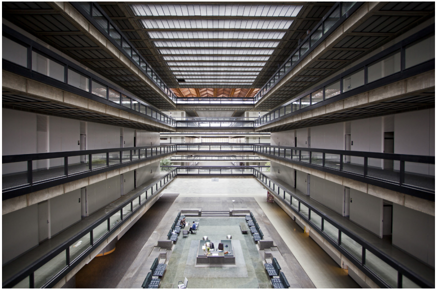


Figura: Bell Labs

Introdução

Definição

Seja $A = \{a_1, \dots, a_n\}$ um conjunto finito, denominado *alfabeto*. Um *código de bloco* C sobre A é um subconjunto de A^n.
Um elemento $c \in C$ é chamado de *palavra*, e o inteiro n é o *comprimento* das palavras.

- Dado $q = p^k$, $k \in \mathbb{N}$ e p primo, existe um único corpo com q elementos, a menos de isomorfismo. Esse corpo, chamado de *corpo de Galois com q elementos*, será denotado $\mathbb{F}_q$.

- Na teoria de códigos corretores de erros, é geralmente utilizado como alfabeto um corpo finito. É possível também trabalhar com códigos sobre anéis, e nesse caso poderíamos usar o alfabeto $\mathbb{Z}_q$.

Exemplo

Se considerarmos o alfabeto $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$, então

$$C = \{0000, 0101, 1000\}$$

é um código *binário* de comprimento 4.

Dado um alfabeto $A = \{a_1, \ldots, a_q\}$, o código

$$C = \left\{ \underbrace{a_1 \ldots a_1}_{n}, \ldots, \underbrace{a_q \ldots a_q}_{n} \right\}$$

é chamado de *código de repetição*.

Métrica

A correção de erros consiste em encontrar a palavra conhecida mais 'próxima' da palavra recebida. Para ter essa noção de proximidade, é necessário definir uma métrica.

A métrica mais comumente utilizada é a *métrica de Hamming*. Dado um código C definimos a distância de Hamming como:

$$d(x, y) = \left|\{i : x_i \neq y_i\}\right|,$$

onde $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$.

- De fato, d define uma métrica:
    1. $d(x, y) \geq 0$;
    2. $d(x, y) = d(y, x) \; \forall x, y \in C$;
    3. $d(x, z) \leq d(x, y) + d(y, z) \; \forall x, y, z \in C$

- $d = \min_{x \neq y} \{d(x, y)\}$ é chamada a *distância mínima* do código C.

Teorema

Seja C um código com distância mínima d, e

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

Então é possível detectar até $d-1$ erros, e corrigir até κ erros.

Um dos problemas principais da teoria de códigos consiste em construir códigos que consigam corrigir o maior número de erros possível, com a menor redundância possível, e com o maior número de palavras possível.

Otimizar esses valores pode ser difícil, mas existem limitantes que podem ajudar.

Teorema (Cota de Singleton)

Seja $A_q(n, d)$ o maior número de palavras possível em um código de comprimento n e distância mínima d. Então

$$A_q(n, d) \leq q^{n-d+1}$$

Teorema (Cota de Hamming)

Seja C um código em $\mathbb{F}_q$ de comprimento n, e distância mínima d. Então

$$M \leq \frac{q^n}{\sum_{t=0}^{\kappa} \binom{n}{t}(q-1)^t}$$

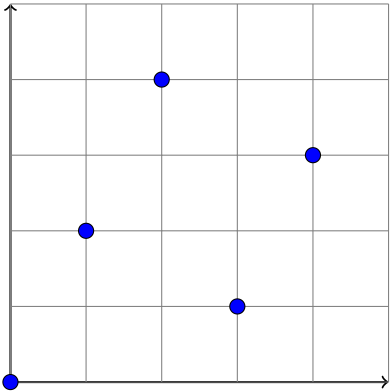
Códigos Lineares

Um tipo de códigos amplamente estudados são os códigos lineares. Um código linear é um subconjunto de $\mathbb{F}_q^n$ que também é um subespaço vetorial.

Se C é um código linear em $\mathbb{F}_q$ com comprimento n, dimensão k e distância mínima d, dizemos que C é um $[n, k, d]$-código linear.

Exemplo

$C = \langle (1,2) \rangle \subset \mathbb{Z}_5^2$.



Uma forma simples de representar um código linear é colocando os vetores geradores deste código como linhas de uma matriz. Essa matriz é chamada de *matriz geradora* do código, ou matriz de codificação.

Dessa forma, se C é um $[n, k, d]$-código linear com matriz geradora G, podemos definir o código como uma transformação linear $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, dada por:

$$\varphi(x) = x \cdot G.$$

Definição

Uma matriz geradora que está na forma $[I_k|A]$, onde I_k é a matriz identidade $k \times k$ e A é uma matriz $(n-k) \times k$ é dita estar na *forma padrão*.

Podemos trabalhar apenas com matrizes geradoras na forma padrão, pois toda matriz geradora pode ser transformada na forma padrão através de escalonamento e troca de coordenadas.

Exemplo

Seja C o código linar em $\mathbb{Z}_5$ gerado pelos vetores $(110344), (100112)$ e (001314). Então uma matriz geradora para o código C é dada por

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 2 & 3 & 2 \\ 0 & 0 & 1 & 3 & 1 & 4 \end{bmatrix}.$$

Assim, multiplicando todos os elementos de $\mathbb{Z}_5^3$ à esquerda da matriz G, obtemos todos os vetores do código C.

Matriz de Verificação

Definição

Seja C um $[n, k, d]$-código linear. Então uma matriz H tal que

$$yH^\top = 0 \; \forall y \in C$$

é denominada uma *matriz de verificação* do código linear C.

A matriz de verificação serve para verificar se uma palavra recebida pertence ao código ou não.
O valor $yH^\top$ é chamado de *síndrome* de y.

Se C é um código linear com matriz geradora $G = [I_k|P]$, então temos que $H = [-P^\top|I_{n-k}]$ é uma matriz de vetificação, pois a relação

$$GH^\top = 0$$

deve ser satisfeita.

Decodificação

Definição

Seja C um código linear. Dado $x \in C$, a classe lateral de x é definida como o conjunto $x + C$.

Para decodificar uma palavra y recebida, deve-se calcular sua síndrome $yH^\top$. Se $yH^\top = 0$, não houve erro. Se $yH^\top \neq 0$, devemos procurar a palavra de $y + C$ que tem o menor peso.
Assim, encontrada a palavra com o menor peso, digamos ê, esse será o menor erro possível, e portanto y deve ser decodificada como $\hat{x} = y - ê$.

Teorema (Cota de Singleton)

Seja C um $[n, k, d]$-código linear. Então

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

Teorema

Seja C um código com matriz geradora $G = [I_k|P]$ na forma padrão. C atinge a cota de Singleton, i.e, $d = n - k + 1$ se, e somente se, todas as submatrizes de P são singulares.

O Código de Hamming

Um exemplo de código importante é o código de Hamming.

Definição

Seja $r \geq 2$ e C um código linear binário com $n = 2^r - 1$, cuja matriz verificadora é tal que as colunas são os todos os vetores não-nulos em $\mathbb{F}_q^r$.

Exemplo

Tomando $r = 3$, temos que o código de Hamming é dado pelas matrizes

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

e

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

Este é um exemplo de um código que corrige exatamente 1 erro, e detecta até 2 erros.