Teoria dell'Informazione

Simone Alessandro Casciaro
12 Dicembre 2024

Lezione 14: Codici Lineari

I codici possono essere usati nel Source Coding per la compressione (primo teorema di Shannon) oppure nel Channel Coding (secondo teorema di Shannon).

Codici Lineari

Codici a Ripetizioni tripla

Nei codici a ripetizione tripla, ogni bit viene ripetuto due volte.
Considerando ad esempio i primi 3 caratteri x_1, x_2, x_3, si ha:

$$\begin{cases} x_2 = x_3 = 0 & x_1 = 0 \\ x_2 = x_3 = 1 & x_1 = 1 \end{cases}$$

Quando riceviamo un messaggio y, possiamo usare i due caratteri di controllo per controllare la presenza di un errore:

$$\begin{cases} x_1 + x_2 = 0 \mod 2 \land x_1 + x_3 = 0 \mod 2 & \text{Errore non rilevato} \\ x_1 + x_2 = 1 \mod 2 \lor x_1 + x_3 = 1 \mod 2 & \text{Errore rilevato} \end{cases}$$

> Esempio
> Chiamiamo p la probabilità d'errore e $1 - p$ la probabilità di non avere errori.
> Qual è la probabilità di spedire la stringa 000 e di ricevere 001 in caso di rumore bianco?
> $\mathbb{P}(Y = 001 \cap X = 000) = \mathbb{P}(X = 000) \cdot \mathbb{P}(Y = 001 | X = 000) = \frac{1}{2}(1 - p)^2 p$

Codici di correzione degli errori

Sia un codice C di tipo (n, k), dove n sono i bit totali della codifica e k sono i bit di

informazione.

Si dice che C è un t-error correcting code (corregge t errori) e un z-error detecting code (rileva z errori).
In generale, $t \leq z$.
Definiamo anche il code rate: $\frac{k}{n}$ il rapporto tra i bit di informazione e i bit totali.

Introduciamo due matrici G e H:

- G è la matrice generatrice che permette di generare le parole del codice attraverso una combinazione lineare delle sue righe
- H è la matrice di parità che rappresenta un sistema di equazioni omogeneo utile a controllare che la parola ricevuta faccia parte del codice

> Esempio
> Nel caso del codice a ripetizione tripla, abbiamo un code rate di $\frac{1}{3}$.
> Dato che un messaggio $x = (x_1, x_2, x_3) \in C$ è tale per cui $x_1 = x_2 = x_3$, abbiamo che
> $\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} = s \cdot \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$, dove $s = 0$ oppure $s = 1$ e $G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$
> H è la matrice di parità ed è definita dalle condizioni di correttezza $x_1 + x_2 = 0$ e $x_1 + x_3 = 0$
> Dunque la matrice $H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$
>
> Quando riceviamo un messaggio y, effettuiamo il prodotto matriciale $H \cdot y^T \mod 2$ e, se otteniamo l'array 0 non rileviamo l'errore, altrimenti sì.
>
> Ad esempio, se riceviamo $y = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$, il calcolo diventa
>
> $$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
>
> Se invece riceviamo $y = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$, il calcolo diventa
>
> $$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

> Dunque $\begin{pmatrix}1 & 1 & 1\end{pmatrix}$ è una parola del codice, mentre $\begin{pmatrix}1 & 0 & 1\end{pmatrix}$ non lo è.

NOTA: è possibile che venga corretto il bit sbagliato o che non venga rilevato un errore. Ad esempio, se la parola spedita fosse 111 ma riceviamo 100, la tentazione sarebbe quella di correggere il primo bit, sbagliando. Oppure, se ricevessimo 000, non ci accorgeremmo proprio dell'errore perché 000 fa parte del codice.

Definizioni

Sia C un codice correttore di tipo (n, k) che mappa k bit di informazione della parola s in n bit della parola x.
Diciamo che C è un codice lineare se esistono G matrice generatrice di dimensione $k \times n$ e H matrice di parità di dimensione $(n-k) \times n$ tali che:

- s mappata in x sia: $\begin{pmatrix}x_1 & \dots & x_n\end{pmatrix} = \begin{pmatrix}s_1 & \dots & s_k\end{pmatrix} \cdot G$
- controllo: $Hx^T = 0^T$

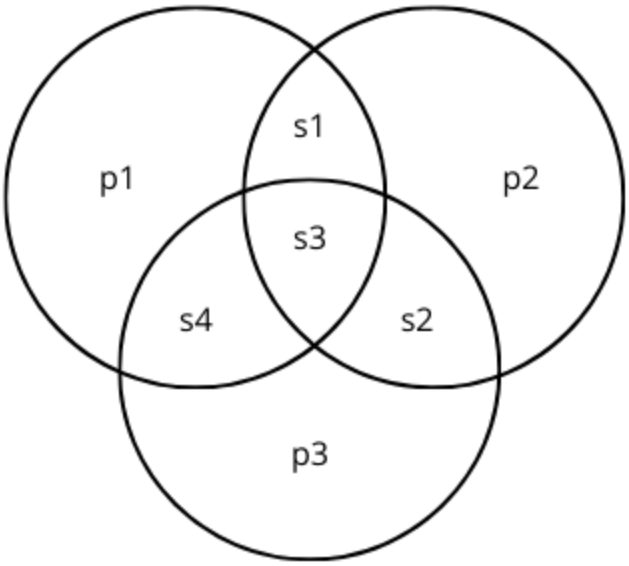
$\forall s \in S$ e $\forall x \in C$, s è il messaggio spedito e x è la parola del codice.

Codice di Hamming

Il codice di Hamming è un codice di correzione di tipo $(7, 4)$ che mappa $s = \begin{pmatrix}s_1 & s_2 & s_3 & s_4\end{pmatrix}$ in $x = \begin{pmatrix}p_1 & p_2 & p_3 & s_1 & s_2 & s_3 & s_4\end{pmatrix}$

I 3 bit di controllo p_1, p_2, p_3 controllano un sottoinsieme dei bit di informazione:

$$\begin{cases} p_1 = s_1 + s_3 + s_4 \mod 2 \\ p_2 = s_1 + s_2 + s_3 \mod 2 \\ p_3 = s_2 + s_3 + s_4 \mod 2 \end{cases}$$



Come correggiamo l'errore?

Se riceviamo $y = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$, ci accorgiamo che

$$\begin{cases} p_1 \neq s_1 + s_3 + s_4 \mod 2 \\ p_2 \neq s_1 + s_2 + s_3 \mod 2 \\ p_3 = s_2 + s_3 + s_4 \mod 2 \end{cases}$$

p_1 e p_2 sono errati! L'unico bit in comune è s_1, dunque correggiamo quello.

Proviamo a rifare lo stesso calcolo usando la matrice H:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

110 è la colonna di s_1 se letta dal basso verso l'alto, dunque l'errore è lì.

Perché succede?

Definiamo il messaggio ricevuto come $x' = x + e$ ovvero il messaggio originariamente spedito x più un errore e.
Se calcoliamo $H \cdot x'^T$ otteniamo $H \cdot (x^T + e^T) = H \cdot x^T + H \cdot e^T$
Il primo termine è 0 perché x è una parola del codice, rimane solo $H \cdot e^T$, il cui risultato è la colonna in cui è presente l'errore, a patto che il vettore e abbia solo un elemento a 1. Se gli errori sono due o più, Hamming non è in grado di correggere l'errore.

Distanza di Hamming

Date due parole del codice x e x', la distanza tra x e x' è data dal numero di bit in cui x e x' differiscono:

$$D = \sum_{i=1}^{n} (x_i \oplus x'_i)$$

La distanza euclidea non sarebbe utilizzabile, poiché stiamo lavorando in modulo 2: la distanza tra $\begin{pmatrix} 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 1 & 1 \end{pmatrix}$ sarebbe $\sqrt{1^2 + 1^2} = \sqrt{2} \equiv \sqrt{0} = 0$

Sia C un codice di correzione (n, k). Assumiamo che due parole abbiano distanza di Hamming $\geq d$. Allora C corregge $\left\lfloor \frac{d-1}{2} \right\rfloor$ errori e rileva $d - 1$ errori.

> Esempio
> Codice binario a ripetizione quadrupla di ordine 12: $n = 12$ e $k = 3$ con rumore bianco e una probabilità d'errore $p = \frac{1}{4}$
>
> Calcoliamo:
> $$\mathbb{P}(errore = 1) = \binom{12}{1} p^1 (1-p)^{11} = 12 \cdot \frac{1}{4} \cdot \left(\frac{3}{4}\right)^{11} = \frac{3^{12}}{4^{11}}$$
> $$\mathbb{P}(errore = 2) = \binom{12}{2} p^2 (1-p)^{10} = \frac{12!}{2!10!} \cdot \left(\frac{1}{4}\right)^2 \cdot \left(\frac{3}{4}\right)^{10} = 11 \cdot 6 \cdot \frac{1}{16} \cdot \frac{3^{10}}{4^{10}}$$
> $$\mathbb{P}(errore = k) = \binom{12}{k} p^k (1-p)^{12-k} = \binom{12}{3} p^3 (1-p)^9$$
> $$\mathbb{P}(errore \leq k) = \sum_{i=1}^{k} \binom{12}{i} p^i (1-p)^{12-i}$$