Teoria dell'Informazione

Simone Alessandro Casciaro

20 Dicembre 2024

Lezione 15: Ultime Definizioni e Teoremi

Definizione

Un codice C rileva z errori se $\forall x \in C$ e $\forall x' \in M_n$ (spazio lineare di dimensione n, ovvro tutte le parole del codice più gli errori) con $x \neq x'$ tali che:

$$0 < d(x, x') \leq z \quad \forall x' \in C$$

Definizione

Un codice C corregge t errori se $\forall x, y \in C$ con $x \neq y$ e $\forall x' \in M_n$:

$$d(x, x') \leq t \land d(x', y) > t$$

Teorema

$$P \text{ rileva } z \text{ errori} \iff d(P) \geq z + 1$$

$d(P)$ è la distanza di Hamming minima tra due parole di P

Teorema

$$P \text{ corregge } t \text{ errori} \iff d(P) \geq 2t + 1$$

Definizione

$w(P)$ è il peso minimo di una parola del codice esclusa la parola vuota. Nel caso di un codice lineare, questa definizione equivale al numero di 1 all'interno di una parola.

Definizione

Dato A un campo finito, chiamiamo spazio dei messaggi di ordine n su A lo spazio lineare $M_n = \{x = [x_1, \ldots, x_n] | x_j \in A\}$ dove:

- $\forall x, x' \in M_n : x + x' = [x_1 + x'_1, \ldots, x_n + x'_n]$
- $\forall x \in M_n$ e $\forall s \in A : s \cdot x = [s \cdot x_1, \ldots, s \cdot x_n]$

M_n è uno spazio lineare di dimensione n e $|M_n| = 2^n$
Un codice C è un sottospazio di M_n, ha cardinalità 2^k e dimensione k.

k sono i bit di informazione e $n - k$ sono i bit di correzione.

Fisso una base $B = \{e_1, \ldots, e_k\}$ per il codice; $\forall x \in C \quad \exists! u : x = u \cdot \begin{bmatrix} e_1 \\ \vdots \\ e_k \end{bmatrix}$

L'insieme delle soluzioni $x = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix}$ di un sistema lineare omogeneo di $n - k$ equazioni in n incognite sul campo è un codice lineare.

Definizione

Sia $x \in C$ una parola spedita sul canale e $y \in M_n$ la parola ricevuta.
Chiamiamo Schema d'errore $e = y - x$

Definizione

La Sindrome s(x) il resto della divisione $\dfrac{y(x)}{g(x)}$, dove $g(x)$ è il polinomio generatore (definito più avanti in questi appunti)

Definizione

La Matrice di Parità del codice C è la matrice H dei coefficienti del sistema lineare $H \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$ di dimensione $(n - k) \times n$.
H non è univoca (posso ad esempio scambiare le colonne).

Definizione

La Matrice Generatrice di un codice lineare C è la matrice G di dimensione $k \times n$ le cui righe sono i k vettori di una base di C.
$\forall x \in C \quad x = s \cdot G$ dove s è la parola che vogliamo spedire

Definizione

La matrice G è in forma canonica se

$$\underbrace{G}_{k \times n} = \left[I_k \middle| \underbrace{D}_{k \times (n-k)} \right]$$

Definizione

Sia G una matrice generatrice scritta in forma canonica $G = [I_k | D]$.
La matrice di parità associata è della forma $\underbrace{H}_{(n-k) \times n} = \left[\underbrace{-D^T}_{(n-k) \times k} \middle| I_{n-k} \right]$

Definizione

Un codice lineare C si dice ciclico se $\forall x \in C$:

$$x = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix} \in C \implies \begin{bmatrix} x_n & x_1 & \dots & x_{n-1} \end{bmatrix} \in C$$

Definizione

Definiamo il grado di una parola come il massimo grado del polinomio x che usiamo per rappresentarla.
Il grado di un polinomio costante è 0.

Teorema

Sia C un codice ciclico di ordine n e $a(x) \in C$ una parola appartenente al codice, espressa come polinomio.

$$\forall q(x) : \quad \mathrm{gr}[q(x) \cdot a(x)] < n \implies q(x) \cdot a(x) \in C$$

Teorema

Sia C un codice ciclico di tipo (n, k).
Allora

1. C contiene almeno una parola $g(x)$ (polinomio generatore) di grado $n-k$ tale che:

$$\forall p(x) \in C \quad p(x) = a(x) \cdot g(x)$$

2. Trovata $g(x)$, la costruzione di G è fatta così:

$$G = \begin{bmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \vdots \\ x^{k-1} \cdot g(x) \end{bmatrix}$$

Teorema

Sia $g(x)$ il polinomio generatore di un codice ciclico di tipo (n, k).
Allora $g(x)$ è un divisore proprio di $x^n - 1$.

Teorema

Ogni divisore proprio di grado r di $x^n - 1$ genera un codice ciclico di tipo $(n, n-r)$

Definizione

Sia C un codice ciclico di ordine n generato da $g(x)$.
Chiamiamo polinomio di parità di C il polinomio quoziente di $\dfrac{x^n - 1}{g(x)}$ e lo indichiamo con $\pi(x)$.

Teorema

Sia C un codice ciclico di tipo (n, k) e sia $\pi(x) = \pi_0 + \pi_1 x + \cdots + x^k$ il suo polinomio di parità.

Allora, la matrice di parità H è fatta così:

$$H = \begin{bmatrix} x^{n-k+1} \cdot \pi'(x) \\ \vdots \\ x \cdot \pi'(x) \\ \pi'(x) \ \underbrace{000}_{n-(k+1)} \end{bmatrix}$$

con $\pi'(x) = 1 + \pi_{k-1}x + \cdots + \pi_0 x^k$, ovvero il polinomio di parità con i coefficienti invertiti.

Esercizi

1. Costruire un codice ciclico binario di tipo (n, k) con $n = 7$ e $k = 4$ generato da un polinomio irriducibile $g(x)$ di grado $n - k = 3$.

   Cerchiamo un divisore proprio di $x^7 - 1$ ricordandoci che i coefficienti sono in $\mathbb{Z}_2$.
   $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$.
   Scegliamo $g(x) = x^3 + x^2 + 1$ e calcoliamo G.

   $$G = \begin{bmatrix} 1 + x^2 + x^3 \\ x + x^3 + x^4 \\ x^2 + x^4 + x^5 \\ x^3 + x^5 + x^6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

   Scriviamo G in forma canonica, ottenendo una matrice identità sulla sinistra.
   Se al posto della riga 1 scriviamo la riga $1+3+4$ e al posto della riga 2 scriviamo la riga $2+4$, otteniamo

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

   Costruiamo ora H' effettuando la matrice trasposta della parte verde (D) con la matrice identità al fianco.

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

Calcoliamo il polinomio di parità $\pi(x)$ e $\pi'(x)$:

$$\pi(x) = \frac{x^7 - 1}{x^3 + x^2 + 1} = (x+1)(x^3 + x + 1) = 1 + x^2 + x^3 + x^4$$

e dunque $\pi'(x) = 1 + x + x^2 + x^4$

Calcoliamo la matrice di parità H:

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

Abbiamo costruito in questo modo un codice ciclico a partire dalla scelta di n e k.
È possibile effettuare il percorso inverso: si definiscono t e z, il numero di errori che il codice deve poter rilevare e correggere, e si definisce il codice ciclico tramite i campi di Galois, arrivando in ultimo a calcolare n e k.
I codici BCH lavorano in questo modo.