Teoria dell'Informazione

Simone Alessandro Casciaro
04 Ottobre 2024

Lezione 2: Shannon

L'idea di Shannon

L'idea di Shannon prevede:

- Massimizzare l'informazione $\forall$ utilizzo del canale. (NOTA: è importante specificare l'utilizzo perché stiamo specificando non solo quanta informazione deve essere inserita nel canale, ma anche il lasso di tempo in cui questa deve avvenire). Questa fase riguarda la fase di Source Coding
- Minimizzare il numero di errori. Dipenderà dal rumore e riguarda la fase di Codifica e del Canale.

Definizioni Importanti

Definiamo:

$$\begin{gathered}\mathbb{X} \text{ insieme finito dei simboli del messaggio} \\ \boldsymbol{x} = (x_1, \dots, x_m) \in \mathbb{X}^m \text{ messaggio} \\ m \text{ lunghezza del messaggio} \\ D \text{ insieme finito dei simboli della codifica} \\ c : \mathbb{X} \to D^+ \text{ funzione di codifica} \\ l_c(x_i) \text{ lunghezza della codifica del simbolo } x_i \\ p(x_i) \text{ probabilità del simbolo } x_i \text{ nel messaggio}\end{gathered}$$

> Esempio
> $\mathbb{X} = \{\heartsuit, \diamondsuit, \clubsuit, \spadesuit\}$
> $d = 2$
> $c : X \to \{0,1\}^+$
>
> Delle possibili scelte di c sono:
> $c(\heartsuit) = 0 \quad c(\diamondsuit) = 010 \quad c(\clubsuit) = 01 \quad c(\spadesuit) = 10$
> $c(\heartsuit) = 0 \quad c(\diamondsuit) = 1 \quad c(\clubsuit) = 01 \quad c(\spadesuit) = 10$
> $c(\heartsuit) = 00 \quad c(\diamondsuit) = 01 \quad c(\clubsuit) = 10 \quad c(\spadesuit) = 11$
> $c(\heartsuit) = 0 \quad c(\diamondsuit) = 00 \quad c(\clubsuit) = 000 \quad c(\spadesuit) = 0000$

Modellizzazione della Sorgente

La sorgente viene modellata attraverso la coppia $< \mathbb{X}, \mathbb{P} >$ dove $\mathbb{X}$ è l'insieme dei simboli del messaggio e $\mathbb{P}$ è lo spazio delle probabilità.
Nella realtà, la probabilità che un simbolo compaia in un messaggio è influenzata dalla presenza dei simboli vicini (Ad esempio: in italiano, dopo la "q" c'è quasi sempre la "u".) Shannon non considera questo aspetto al fine di semplificare i calcoli, considerando i simboli tra loro indipendenti.
Considereremo dunque questa relazione

$$p(\boldsymbol{x}) = p(x_1, \dots, x_n) = \prod_{i=1}^{m} p(x_i)$$

Data una sorgente $< \mathbb{X}, \mathbb{P} >$, dato $d > 1$ e data $c : \mathbb{X} \to D^+$ vogliamo che:

$$\mathbb{E}(l_c) = \sum_{x \in \mathbb{X}} l_c(x) p(x) \text{ sia minimo}$$

Codice Non Singolare

Dato $c : \mathbb{X} \to D^+$, diciamo che c è non singolare se c è una funzione iniettiva.

$$c(x_1) = c(x_2) \implies x_1 = x_2$$

Codici non singolari $\subset$ Codici

Definizione

Dato $c : \mathbb{X} \to D^+$, consideriamo un'estensione di c a una concatenazione di elementi di $\mathbb{X}$ e la chiamiamo

$$C : \mathbb{X}^+ \to D^+$$

> Esempio
> Considerando la prima funzione c definita nel precedente esempio, abbiamo:
> $01001 \begin{cases} C(\heartsuit, \spadesuit, \clubsuit) \\ C(\diamondsuit, \clubsuit) \\ C(\spadesuit, \heartsuit, \clubsuit) \end{cases}$
> La funzione C non è "non singolare"

Notiamo quindi che se c è non singolare, non è detto C lo sia. Questo rende la decodifica impossibile (o meglio, ambigua).

Vogliamo che anche C sia non singolare.

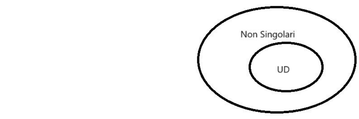
Codice Univocamente Decodificabile

Se C è non singolare, allora c è univocamente decodificabile

$$C \text{ non singolare} \implies c \text{ univocamente decodificabile}$$

Come si capisce se un codice è univocamente decodificabile? Esiste un algoritmo (Sardinas-Patterson) che ermette di stabilirlo.
La Complessità Computazionale di questo algoritmo è $O(m * L)$ dove $m = |\mathbb{X}|$ e $L = \sum_{x \in \mathbb{X}} l_c(x)$

Codice Univocamente Decodificabile $\subset$ Codice Non Singolare



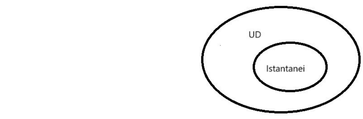
> Esempio
> Consideriamo $c(\heartsuit) = 10 \quad c(\diamondsuit) = 00 \quad c(\clubsuit) = 11 \quad c(\spadesuit) = 110$
> Questo codice è univocamente decodificabile. Tuttavia, se dobbiamo decodificare la stringa $110...0$, il numero di 0 influenza la decodifica ($\clubsuit, \diamondsuit, \diamondsuit, \diamondsuit, ...$ oppure $\spadesuit, \diamondsuit, \diamondsuit, \diamondsuit, ...$). Questo obbliga ad aspettare la fine della stringa per decodificarla, creando problemi ad esempio in caso di streaming. Vogliamo essere in grado di decodificare subito una stringa.

Codici Istantanei

Un codice è istantaneo quando non esiste una parola nell'insieme D dei simboli che è prefisso di un'altra parola.
Definiamo provvisariamente l'insieme $\mathbb{C}$ come l'insieme delle codifiche della funzione c.
$\mathbb{C} \subseteq D^+$

$$\nexists\, x, y \in \mathbb{C}, z \in D^+ : y = x * z \implies c \text{ è istantaneo}$$

dove $x * z$ rappresenta la concatenazione di x e z.
Codici Istantanei $\subset$ Codice Univocamente Decodificabile



Codici a Virgola

Tra i codici istantanei, esistono i codici a virgola, dove ogni codifica termina con un carattere terminatore.

> Esempio
> con $d = 3$, possiamo avere:
> $c(\heartsuit) = 102$
> $c(\diamondsuit) = 002$
> $c(\clubsuit) = 112$
> $c(\spadesuit) = 1102$
>
> con $d = 2$ invece possiamo avere:
> $c(\heartsuit) = 0$
> $c(\diamondsuit) = 10$
> $c(\clubsuit) = 110$
> $c(\spadesuit) = 111$
> Quando il carattere terminatore è sulla codifica di lunghezza maggiore, si può omettere.

Un codice istantaneo è univocamente decodificabile?

Vogliamo dimostrare che

$$c \text{ istantaneo} \implies c \text{ univocamente decodificabile}$$

Per dimostrarlo, pensiamo alla contronominale.

$$c \text{ non univocamente decodificabile} \implies c \text{ non istantaneo}$$

Sia $c : \mathbb{X} \to D^+$ e $C : \mathbb{X}^+ \to D^+$ la sua estensione.
Se c non è univocamente decodificabile, allora $\exists \boldsymbol{x}, \boldsymbol{x}' \in \mathbb{X}^+, \boldsymbol{x} \neq \boldsymbol{x}' : C(\boldsymbol{x}) = C(\boldsymbol{x}')$.

Possono esistere due casi:

1.

$\boldsymbol{x}'$ è prefisso di $\boldsymbol{x}$. Per far sì che le due codifiche siano uguali, la parte che "eccede" $\boldsymbol{x}'$ in $\boldsymbol{x}$ deve essere codificata nella parola vuota $\emptyset$. Questo è assurdo, perché $C : \mathbb{X}^+ \to D^+$ e $\emptyset$ non fa parte del codominio. In ogni caso, se anche considerassimo un'ulteriore estensione di $\hat{C} : \mathbb{X}^+ \to D^*$ che comprende anche la parola vuota nel codominio, tale parola sarebbe prefissa di ogni altra e questo renderebbe il codice non istantaneo.

2.

$\boldsymbol{x}$ e $\boldsymbol{x}'$ condividono una parte comune, salvo differire nella parte finale. La parte comune avrà chiaramente la stessa codifica, dunque ci concentriamo sulla parte non comune.
Supponiamo per semplicità che la parte non comune sia formata da due caratteri ciascuna. La loro codifica totale sarà la stessa, ma dal disegno si può vedere come la codifica di "C" sia prefisso della codifica di "A", rendendo il codice non istantaneo.

Esercizio

$GF(4) = GF(2^2)$. Il campo di Galois è $\mathbb{Z}_2[x] \mod x^2 + x + 1$
Effettuiamo la Pre-Computazione del campo sia per l'operazione $+$ sia per l'operazione $*$

+	0	1	x	x+1
0	0	1	x	x+1
1	0	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x