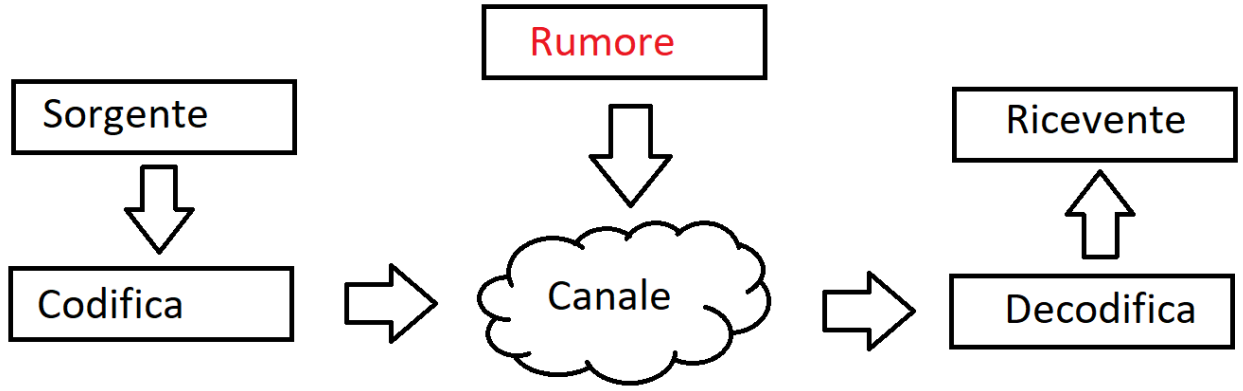
Teoria dell'Informazione

Simone Alessandro Casciaro
01 Ottobre 2024

Lezione 1: Introduzione

Storia

La Teoria dell'Informazione e della Trasmissione fa riferimento al seguente schema.



Da questo schema, notiamo che:

- La fase della Sorgente viene chiamata `Source Coding`
- La fase di Codifica e di Decodifica fanno riferimento alla seconda parte del corso, chiamata `Teoria della Trasmissione`
- Il Rumore sarà un'entità esterna di cui terremo conto nell'utilizzo del Canale, ma che non approfondiremo troppo in questo corso.

Protagonisti della storia della Teoria dell'Informazione

Ci si pone l'obbiettivo di spedire, attraverso un canale, più informazione possibile da una sorgente a una destinazione.
Gli studiosi che si sono posti il problema sono **Claude Shannon** e **Andrej Kolmogorov**.
Shannon si occupa di studiare il problema nel suo caso medio, a livello statistico, ignorando

dunque l'applicazione al caso reale, che è invece studio di Kolmogorov.
A loro si aggiunge anche **Richard Hamming**, che ha studiato un algoritmo per correggere gli errori, dando vinta al primo Codice di Rilevazione e Correzione degli errori. Il corso di `Teoria dell'Informazione` si baserà sugli studi di Shannon.

Per inviare un messaggio, sono importanti due operazioni:

- Compressione -> Trovare pattern comuni in modo da inviare informazioni ripetute una volta sola
- Aggiungere Ridondanza -> Si ripetono le informazioni rilevanti per poterle, eventualmente, correggere in fase di decodifica.

Studieremo i due teoremi di Shannon, in due punti diversi dello schema soprastante:

- 1° Teorema di Shannon, fase di Source Coding: si cerca di massimizzare la compressione
- 2° Teorema di Shannon, fase di Codifica e di uso del Canale: si cerca di minimizzare il numero di errori

Shannon, per modellare il canale, usa una matrice stocastica che indica la probabilità di ricevere un determinato carattere dopo averne inviato un altro sul canale.

> Esempio di Matrice Stocastica

IN/OUT	a	b	c	d	e
a	0.7	0	0.1	0.1	0.1
b	0	1	0	0	0
c	0.4	0	0.5	0	0.1
d	0	0.3	0.1	0.6	0
e	0.2	0	0.1	0	0.7

Quali sono i messaggi che contengono più informazione?

Supponiamo di disporre di 2 monete, una truccata e l'altra no. Lanciandole entrambe 5 volte, i risultati sono i seguenti: TCCTC, TTTTT. Quale di questi due lanci contiene più informazione?

La risposta è: la moneta non truccata, perché quando effettueremo un sesto lancio, per entrambe le monete, sarà più facile prevedere il risultato della moneta truccata, rispetto a quella non truccata.
In generale, laddove c'è meno entropia nel messaggio, c'è anche meno informazione e viceversa.

Campo di Galois

Un Campo di Galois viene indicato con la dicitura $GF(p^n)$ dove p è un numero primo e n è un qualunque numero positivo. L'idea dei campi di Galois è di costruire un campo con p^n elementi, partizionando l'insieme del polinomi di grado n a coefficienti in $\mathbb{Z}_p$ usando come modulo un polinomio irriducibile di grado esattamente n.

Radice Primitiva

In un campo, un elemento si dice Radice Primitiva se quel numero elevato per tutti gli elementi del campo genera tutti gli elementi del campo, eccetto lo 0.

> Esempio
> In $\mathbb{Z}_5$, 2 è una radice primitiva.
> $2^1 = 2$
> $2^2 = 4$
> $2^3 = 8 \equiv 3$
> $2^4 = 16 \equiv 1$
>
> In $\mathbb{Z}_7$, 2 non è una radice primitiva.
> $2^1 = 2$
> $2^2 = 4$
> $2^3 = 8 \equiv 1$
> $2^4 = 16 \equiv 2$
> $2^5 = 32 \equiv 4$
> $2^6 = 64 \equiv 1$

Esercizio

Trovare l'inverso moltiplicativo degli elementi di $\mathbb{Z}_{10}$

$\mathbb{Z}_{10}$	a^{-1}
1	1
2	
3	7
4	
5	
6	
7	3
8	
9	9

Trovare l'inverso moltiplicativo degli elementi di $\mathbb{Z}_5$

$\mathbb{Z}_5$	a^{-1}
1	1
2	3
3	2
4	4