

La teoria dell'informazione è alla base di importanti settori dell'informatica e delle telecomunicazioni, come la compressione e la trasmissione dati, l'apprendimento automatico e la crittografia. Le principali teorie formali del concetto di informazione sono due:

1. Quella di Claude Shannon (USA, 1916–2001) formulata nel 1948 e basata sulla teoria della probabilità.
2. Quella di Andrey Kolmogorov (URSS, 1903–1987) formulata nel 1965 e basata sulla teoria della computazione. La stessa teoria venne indipendentemente proposta anche da Gregory Chaitin (USA, 1947– ) e Ray Solomonoff (USA, 1926–2009),

In un certo senso, la teoria di Kolmogorov è più astratta di quella di Shannon, che —per contro— ha una maggiore rilevanza applicativa

La teoria dell'informazione di Shannon è stata formulata nel lavoro “A Mathematical Theory of Communication”, pubblicato dai Bell Labs nel 1948. Il problema che la teoria di Shannon affronta è quello di trasmettere informazione attraverso un canale affetto da rumore.

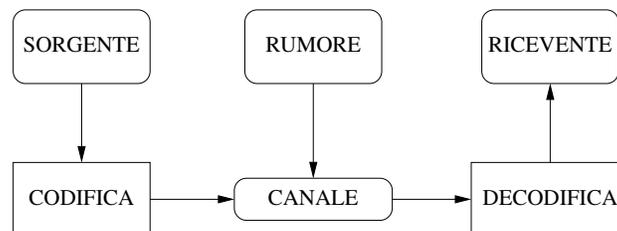


Figura 1: Modello di canale con rumore.

Più precisamente, si vuole codificare i messaggi in modo da massimizzare l'informazione trasmessa ad ogni utilizzo del canale, minimizzando simultaneamente gli errori di trasmissione dovuti alla presenza di rumore. Il problema è che l'informazione non è distribuita in modo uniforme nel messaggio. Di conseguenza è difficile controllare gli errori di trasmissione. La metodologia ideata da Shannon consiste nel separare il problema in due sottoproblemi da affrontare separatamente: prima codifico in modo da concentrare l'informazione eliminando la ridondanza nel messaggio, poi ricodifico al fine di minimizzare gli errori di trasmissione.

In pratica, bisogna quindi sviluppare due codifiche separate.

1. **Source Coding** (I teorema di Shannon). Codice per rappresentare il messaggio in modo da massimizzare la compressione (per esempio, ZIP).

2. **Channel Coding** (II teorema di Shannon). Codice per rappresentare il messaggio in modo da minimizzare gli errori di trasmissione.

La codifica sorgente (source coding) elimina la maggior parte della ridondanza nel messaggio, concentrando l'informazione. La codifica di canale (channel coding) reintroduce ridondanza in modo controllato al fine di contrastare la distorsione prodotta dal rumore.

Il primo e secondo teorema di Shannon vengono poi combinati per dimostrare il teorema di codifica congiunta sorgente-canale. Questo teorema dimostra che la codifica a due stadi, dove prima comprimiamo la sorgente e poi creiamo un codice canale per trasmettere i simboli compressi, è ottima. Questo non è scontato, infatti il codice sorgente ignora il canale, mentre il codice canale ignora la sorgente. Il teorema invece dimostra che non c'è modo di avere una codifica più efficiente anche considerando simultaneamente sorgente e canale.