L’INFORMAZIONE E LE CODIFICHE

UN PO' DI STORIA

- La Teoria dell'informazione è nata nella seconda metà del 900, sebbene il termine *informazione* sia antico (dal latino *mettere in forma*)

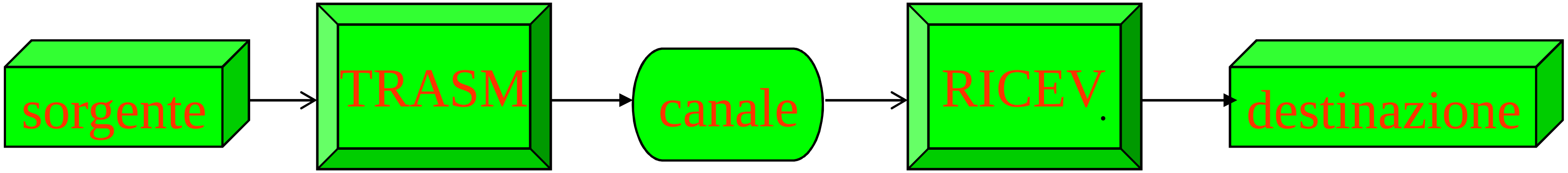
- I nomi più importanti sono Nyquist, Hartley, Wiener ma soprattutto Shannon con un suo lavoro del 1948 in cui sistematizzò la teoria.

- L'ambito della teoria dell'informazione è, informalmente, lo studio di come poter trasferire nel tempo e nello spazio un *messaggio* da parte di una sorgente fino ad un destinatario. Più formalmente la teoria dell'informazione studia i problemi legati alla riproduzione in un punto dello spazio ad un dato istante, in modo quanto più esatto possibile, di un messaggio selezionato in un altro punto dello spazio, in un altro momento (*passato o presente*). Non sono quindi pertinenti problemi come: significato del messaggio *(semantica)*, *interpretazione* ed *efficacia*.

- Shannon ha *quantificato* l'informazione di un messaggio introducendo una grandezza, detta *Entropia* (dal greco εν τροπε, "caos interno") in analogia formale e concettuale con la omonima funzione di stato utilizzata in Termodinamica (punto di vista *macroscopico* dei sistemi) e Meccanica Statistica (punto di vista *microscopico* dei sistemi). In questi contesto vale quanto segue: 1) dal punto microscopico qualunque sistema evolve verso uno stato di massima probabilità (o massimo disordine) 2) dal punto di vista macroscopico l'entropia di un sistema evolve sempre verso un valore massimo

- Vedremo nel seguito in cosa consiste questa equivalenza trovata da Shannon

ELEMENTI ESSENZIALI DI UN SISTEMA DI COMUNICAZIONE



- SORGENTE: Entità logica o fisica che trasmette il messaggio

- TRASMETTITORE: Dispositivo che trasforma i messaggi in segnali adatti ad essere trasmessi

- CANALE: Mezzo fisico utilizzato per la trasmissione

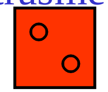
- RICEVITORE: Dispositivo che esegue le stesse operazioni del trasmettitore ma in ordine inverso

- DESTINAZIONE: Entità alla quale è destinato il messaggio

COME MISURARE L'INFORMAZIONE

- Dato che non esiste una *definizione operativa* di informazione occorre rifarsi a ragionamenti euristici cioè basati su considerazioni intuitive

- Shannon partì dalla considerazione che in un esperimento, l'entropia è la misura delle possibilità (esiti o combinazioni) offerte: nel lancio di una moneta gli esiti possibili sono solo due (testa o croce), mentre nel lancio di un dado sono sei. Quindi l'entropia di un dado è maggiore dell'entropia di una moneta

- Supponiamo ora di avere due messaggi A e B: la sorgente trasmette A se nel lancio di una moneta esce "TESTA" mentre B se nel lancio di un dado esce 

- Supponiamo che il destinatario sia a conoscenza di questa associazione: si "aspetta" quindi di ricevere il messaggio A perché più "probabile" del messaggio B (1/2 contro 1/6). Se riceve il messaggio B quindi resterà "sorpreso".

- Se associamo la quantità di informazione alla sorpresa che il ricevere il messaggio provoca nel destinatario, possiamo concludere che l'informazione di B è maggiore di quella di A, proprio come l'entropia del dado (e quindi di B) è maggiore della moneta (e quindi di A).

- Concludiamo quindi che:

1) Un evento è tanto più sorprendente quanto più è improbabile
2) La quantità di informazione di un evento è legata alla sorpresa che esso genera
3) La quantità di informazione è tanto maggiore quanto più un evento è improbabile

UNA MISURA DELL'INFORMAZIONE

- Supponiamo di avere un sacchetto con N palline: 8 **rosse**, 7 **verdi**, 5 **gialle** ed una **nera**
- Supponiamo di utilizzare la seguente tabella di associazione

COLORE	LETTERA	PROBABILITA'
	A	
	C	
	I	
	Q	

- Supponiamo di estrarre una pallina rossa: non ne saremo stupiti perché esse sono di più. Lo stesso vale anche per le verdi (una in meno). Se invece esce la nera la nostra sorpresa sarà maggiore.
- Ad ogni estrazione, l'incertezza sui simboli successivi che si potrebbero ricevere diminuisce sempre di più. Se esce la pallina nera si ha la massima eliminazione di incertezza, essendo ora noi sicuri che potremmo ricevere solo A, C o I.
- Quindi, possiamo concludere anche che la quantità di informazione e la quantità di incertezza rimossa coincidono

L’INFORMAZIONE E LA SUA MISURA

- Dalle regolarità osservate potremmo dire che, se **Q** indica la quantità di informazione contenuta nel messaggio **m** che ha probabilità **P** di essere emesso, avremo:

$$Q(m) = f(1/P(m))$$

- Q(m) è tale che:

$$Q(m_1, m_2) = Q(m_1) + Q(m_2) \text{ [} m_1 \text{ e } m_2 \text{ sono messaggi generici]}$$

- P(m) è tale che:

$$P(m_1, m_2) = P(m_1)P(m_2) \text{ [dal calcolo delle prob.con } m_1\ m_2 \text{ indipendenti]}$$

- Dunque:

$$Q(m_1, m_2) = Q(m_1) + Q(m_2) = P(m_1, m_2) = P(m_1)\ P(m_2)$$

- *f* è quindi tale che:

$$f(1/P(m_1)) + f(1/P(m_2)) = f(1/P(m_1)*1/P(m_2))$$

$$\mathbf{f} \Longrightarrow \mathbf{log}$$

INFORMAZIONE UNITARIA

- Come base per il logaritmo si sceglie quella che corrisponde alla quantità di *informazione unitaria*

- Definiamo *informazione unitaria* quella associata ad una sorgente con un *alfabeto* di due soli *simboli* equiprobabili (es. una moneta)

In questo caso:

$$Q(m) \equiv 1;\ P(m) = 0.5$$

da cui l'equazione

$$\log_x (1/0.5) = 1 \Rightarrow \mathbf{x = 2}$$

- In definitiva

$$Q(m) = \log_2 (1/P(m)) = - \log_2 (P(m)) \quad \text{o}$$

$$\mathbf{Q = - \log_2 (P)}$$

- **Q** si misura in **bit (binary digit)**

- In generale, si avrà nel caso di un alfabeto con *n* simboli, ognuno dotato di probabilità P_k:

$$Q = -\sum_{k=1}^{n} \log_2 P_k$$

$$P_k = \frac{1}{n} \quad \forall k \Rightarrow Q = n \log_2 n$$

QUANTITA' DI INFORMAZIONE MEDIA

- Se i simboli non sono *equiprobabili* si introduce il valor medio **H** della quantità di informazione valutato su tutti i simboli dell'alfabeto della sorgente.
- Se l'alfabeto ha n simboli, si può dimostrare che (cfr. *distr. prob.*):

$$H = -\sum_{i=1}^{n} P_i \log_2 \left(P_i \right)$$

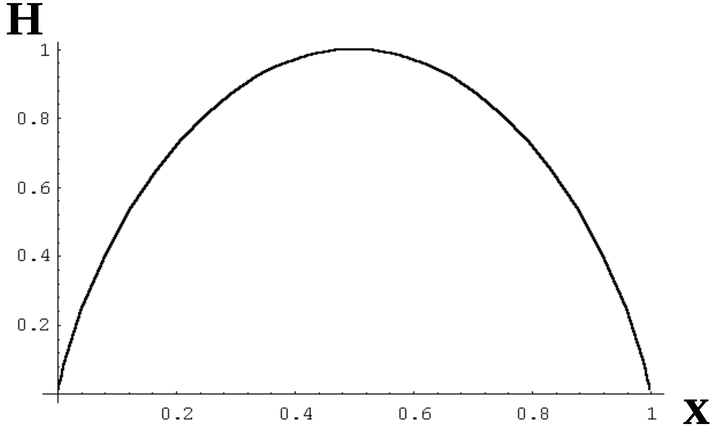
- H è detta ENTROPIA della sorgente e si misura in **bit/simbolo** (essendo infatti una *informazione media* su N simboli)

- Se si ha $P_i = 1/n \ \forall i \Rightarrow \mathbf{H = \log_2 n} \Rightarrow H = Q/n$

- Si dimostra che in questo caso l'entropia è massima

- Infatti se N = 2, $P_1 + P_2 = 1$, ponendo $P_1 = x$ si ha $P_2 = 1 - x$

$$H(x) = -x \log_2 \left(x \right) - (1-x) \log_2 \left(1-x \right)$$



$$\mathbf{H_{MAX} = \log_2 n}$$

CODIFICHE DI SORGENTE

- Servono per ottimizzare la trasmissione dati

- Esistono codici a lunghezza *variabile* e *fissa*:

Alfabeto: {[

Lunghezza variabile

Simbolo	Codice
♥	{
♣	[
♠	{[
♦	[{

Lunghezza fissa:

Simbolo	Codice
♥	{{
♣	{[
♠	[{
♦	[[

- Se un alfabeto ha *k lettere*, *n* il numero di *simboli* da trasmettere, la lunghezza minima di un messaggio deve essere

$$L_{\min} \geq \log_k n \xrightarrow{k = 2} L_{\min} \geq H_{MAX}$$

- Nel caso precedente n = 4, k = 2 e $L_{\min} = 2$

CODIFICHE DI SORGENTE ED ENTROPIA

- Il concetto di Entropia può essere utile per definire alcuni parametri di una sorgente di messaggi binari, quali la lunghezza media L, l'efficienza η e la ridondanza γ di codice. In particolare si ha:

$$\overline{L} = \sum_{i=1}^{n} P_i m_i$$

m_i è il numero di lettere con cui è codifica l'i-esimo simbolo

$$\eta = \frac{H}{\overline{L}}$$

$$\gamma = 1 - \eta$$

- Nel caso in cui i simboli siano equiprobabili, e se si utilizza una codifica a lunghezza fissa si ha:

$$\overline{L} = \sum_{i=1}^{n} P_i m_i = \sum_{i=1}^{n} \frac{1}{n} L_{\min} = L_{\min}$$

- Se si utilizza un alfabeto binario (0 e 1) avremo

$$\overline{L} = L_{\min} = \log_2 n = H_{MAX}$$

- Avremo quindi

$$\eta = \frac{H}{H_{MAX}} \qquad \gamma = 1 - \frac{H}{H_{MAX}}$$