

# Fondamenti di Informatica

Prof. V.L. Plantamura  
Informatica e Comunicazione Digitale  
a.a. 2005-2006

---

---

---

---

---

---

---

---

## Cosa è l'informazione

- L'informazione è qualcosa che si possiede e si può dare ad un altro senza perderne il possesso.
  - L'Informazione non attesa non può essere ricevuta
  - Essa richiede una incertezza da parte di colui che la riceve
  - Non deve essere Ambigua

---

---

---

---

---

---

---

---

## A cosa serve

Per risolvere una incertezza  
Per prendere decisioni



Per risolvere problemi

---

---

---

---

---

---

---

---

## Condizioni necessarie

- Sorgente e Ricevente hanno un codice in comune
- L'incertezza del Ricevente è tra un numero ben definito di possibilità

---

---

---

---

---

---

---

---

## Messaggio

- Il Sorgente [S] produce un Messaggio [M]
- Il Messaggio modifica lo stato del Ricevente [R]



---

---

---

---

---

---

---

---

## Definizione di *Informazione*

- **Livello semantico:** il significato
- **Livello sintattico:** la forma o struttura
- **Livello pragmatico:** reazione del ricevente

---

---

---

---

---

---

---

---

## Struttura dell'informazione

- La struttura delle informazioni influisce sui tempi di accesso alle informazioni stesse
- La struttura delle informazioni nasconde l'informazione rispetto ad accessi diversi da quelli per cui la struttura è stata creata

---

---

---

---

---

---

---

---

## Codice

- Numero o sigla alfanumerica sostitutive, allo scopo di facilitare il trattamento delle informazioni, la descrizione di cose, persone e situazioni.  
*(Voc. Zanichelli)*
- In senso informatico è una regola per far corrispondere dei nomi (i dati) a degli oggetti (le informazioni)

---

---

---

---

---

---

---

---

## Definizione di Shannon

- L'informazione è tutto ciò che può consentire di ridurre il nostro grado di incertezza su un evento che si può verificare

---

---

---

---

---

---

---

---

## Processo comunicativo

- È composto da cinque parti:
  - Un **mittente**: che produce un messaggio da comunicare ad un'altra entità
  - Un **trasmettitore**: che codifica il messaggio in modo che possa viaggiare su un canale di comunicazione
  - Un **canale di comunicazione**
  - Un **ricevitore**: che riceve ciò che viaggia sul canale e lo decodifica per riconoscere il messaggio
  - Un **destinatario**: al quale giunge un messaggio

---

---

---

---

---

---

---

---

## Ipotesi di Shannon

- La trasmissione dei simboli lungo il canale costituisce un fenomeno discreto
  - Ovvero, l'invio di ciascun simbolo richiede una certa quantità di tempo, finita e non nulla
- Esiste una sorgente di rumore
  - Agisce sul canale modificando il contenuto sintattico dell'informazione, la sua forma

---

---

---

---

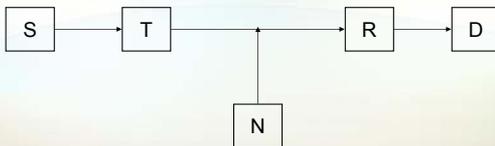
---

---

---

---

## Processo comunicativo di Shannon



S = Sorgente; T = Trasmettitore; R = Ricevitore;  
D = Destinatario; N = Sorgente di Rumore

---

---

---

---

---

---

---

---

## Problemi da affrontare

- Come misurare la quantità di informazione che viaggia lungo il canale
- Come garantire trasmissioni sicure
- Come garantire trasmissioni affidabili

---

---

---

---

---

---

---

---

## Definizione di Entropia

- L'entropia è la misura del disordine di un sistema
- Più ordinato o strutturato è un sistema minore è l'entropia e viceversa

---

---

---

---

---

---

---

---

## Concetto di Incertezza

- Più grande è la nostra incertezza su ciò che dovrà contenere un messaggio, e maggiore sarà l'informazione che riceveremo quando il messaggio sarà arrivato

---

---

---

---

---

---

---

---

## Misura dell'informazione

- È dunque logico fondare la misura dell'informazione associata ad un messaggio sulla **probabilità** che il messaggio stesso si verifichi

---

---

---

---

---

---

---

---

## Misura dell'informazione

- Supponiamo che la sorgente emetta simboli discreti ciascuno dei quali si suppone abbia la stessa durata degli altri

$$H = -\log P$$

- H indica la misura dell'informazione
- P è la probabilità del simbolo
- Il logaritmo è in una base che determina l'unità di misura dell'informazione

$$H = -\log_2 P \text{ bit}$$

---

---

---

---

---

---

---

---

## Informazione media di più simboli

- Si consideri una sorgente avente i tre simboli A, B e C, che vengono emessi con probabilità  $P(A)$ ,  $P(B)$  e  $P(C)$
- L'informazione associata ad A è:

$$H(A) = -\log_2 P(A) \text{ bit}$$

per A che viene emesso per circa  $P(A)$ -esimi di tempo

---

---

---

---

---

---

---

---

## Entropia della sorgente

- Per una sorgente  $x$ , con  $m$  simboli, se l' $i$ -esimo simbolo ha una probabilità  $P(i)$

$$H(x) = -\sum_{i=1}^m P(i) \log P(i) \text{ bit/simbolo}$$

$H$  prende il nome di entropia della sorgente

---

---

---

---

---

---

---

---

## Proprietà 1

- Se tutte le  $P(i)$ , una sola esclusa, sono nulle, allora  $H(x)=0$   
non essendovi incertezza sul risultato, non v'è neppure informazione

---

---

---

---

---

---

---

---

## Proprietà 2

- Se tutte le  $P(i)$  sono uguali  $\left(P(i) = \frac{1}{m}\right)$

allora  $H(x)$  è massima:

$$H(x) = -\sum_{i=1}^m \frac{1}{m} \log \frac{1}{m} = \log m$$

---

---

---

---

---

---

---

---

## Proprietà 3 - Entropia congiunta

- Siano in gioco due simboli,  $x$  e  $y$ , con  $m$  possibilità per  $x$  e  $n$  per  $y$
- Se  $P(i,j)$  è la probabilità congiunta dell'emissione dell' $i$ -esimo simbolo di  $x$  e dell' $j$ -esimo simbolo di  $y$ , allora l'entropia della sorgente doppia è definita da:

$$H(x,y) = - \sum_{i=1}^m \sum_{j=1}^n P(i,j) \log P(i,j)$$

---

---

---

---

---

---

---

---

## Indipendenza dei simboli

- La relazione precedente include le sorgenti discrete in cui i simboli non sono indipendenti
- Esiste una effettiva interdipendenza fra i simboli, la cui influenza può essere introdotta nell'entropia

---

---

---

---

---

---

---

---

## Interdipendenza

- Siano  $x$  e  $y$  due gruppi di simboli come nella proprietà 3
- Per ogni valore  $i$  che  $x$  può assumere esiste una probabilità condizionale  $P(j|i)$  che  $y$  valga  $j$

---

---

---

---

---

---

---

---

## Entropia Condizionale

- L'entropia condizionale di  $y$  sotto la condizione che lo preceda  $x$  è:

$$H(y|x) = -\sum_{i=1}^m \sum_{j=1}^n P(i, j) \log P(j|i)$$

---

---

---

---

---

---

---

---

## Probabilità congiunte

- Le probabilità congiunte sono legate a quelle condizionali dalla relazione:

$$P(i, j) = P(i)P(j|i)$$

- Sostituendo questa relazione in quella definita nella proprietà 3 si ha:

$$H(x, y) = -\sum_{i=1}^m \sum_{j=1}^n P(i)P(j|i) \log P(i)P(j|i)$$

---

---

---

---

---

---

---

---

## ossia...

$$H(x, y) = -\sum_{i=1}^m \sum_{j=1}^n P(i)P(j|i) \log P(i) - \sum_{i=1}^m \sum_{j=1}^n P(i, j) \log P(j|i)$$

Se  $i$  è costante:

$$\sum_{j=1}^n P(i)P(j|i) \log P(i) = P(i) \log P(i)$$

e quindi:

$$H(x, y) = -\sum_{i=1}^m P(i) \log P(i) - \sum_{i=1}^m \sum_{j=1}^n P(i, j) \log P(j|i)$$

---

---

---

---

---

---

---

---

## Entropia Congiunta

- Il primo termine non è altro che  $H(x)$ , mentre il secondo termine è  $H(y|x)$

$$H(x, y) = H(x) + H(y|x)$$

- Se i simboli sono indipendenti allora:

$$H(x, y) = H(x) + H(y)$$

---

---

---

---

---

---

---

---

## Entropia Congiunta

- Se due sorgenti producono una successione di simboli che non hanno relazioni o legami fra loro, allora l'entropia congiunta di una coppia di simboli qualsiasi è data dalla somma delle entropie relative ai due simboli

---

---

---

---

---

---

---

---

## Esempio 1

- Si consideri il lancio di una moneta
- Sia all'uscita testa che croce è associata una informazione pari a:  $-\log_2 \frac{1}{2} = 1 \text{ bit}$
- L'informazione media o entropia è:

$$H = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = 1 \text{ bit/simbolo}$$

---

---

---

---

---

---

---

---

## Esempio 2

- Consideriamo una sorgente con 6 simboli A, B, C, D, E, F le cui probabilità sono:

$$P(A) = 1/2 \quad P(D) = 1/16$$

$$P(B) = 1/4 \quad P(E) = 1/32$$

$$P(C) = 1/8 \quad P(F) = 1/32$$

---

---

---

---

---

---

---

---

## L'informazione media

$$H = - \left( \frac{1}{2} \log \frac{1}{2} + \frac{1}{4} \log \frac{1}{4} + \frac{1}{8} \log \frac{1}{8} + \frac{1}{16} \log \frac{1}{16} + \frac{1}{32} \log \frac{1}{32} + \frac{1}{32} \log \frac{1}{32} \right) = 115/16 \text{ bit/simbolo}$$

---

---

---

---

---

---

---

---

## Entropia in bit al secondo

- L'entropia espressa in bit per simbolo è indicata con  $H$
- L'entropia misura in bit/secondo è indicata con  $H'$
- Se  $s$  è il tasso di invio dei simboli (numero di bit trasmessi in un secondo) allora:  $H' = sH$

---

---

---

---

---

---

---

---

## Esempio 3

P(i)		P(j i)			P(i,j)=P(i)P(j i)				
i	P(i)	i   j	A	B	C	i   j	A	B	C
A	9/27	A	0	4/5	1/5	A	0	4/15	1/15
B	16/27	B	1/2	1/2	0	B	8/27	8/27	0
C	2/27	C	1/2	2/5	1/10	C	1/27	4/135	1/135

---

---

---

---

---

---

---

---

## Ridondanza

- È evidente che la presenza di una interdipendenza fra i simboli diminuisce l'entropia della sorgente rispetto ad una che abbia simboli tutti indipendenti.
- Una successione di simboli che dipendono gli uni dagli altri si dice **ridondante**.
- Misuriamo la ridondanza di una successione di simboli calcolando di quanto è stata ridotta l'entropia.
- La ridondanza è quindi definita come:

$$E = 1 - \frac{H(y|x)}{H(x)}$$

---

---

---

---

---

---

---

---

## Canale discreto

- La capacità di trasmettere informazioni in un canale discreto si può misurare mediante il numero di bit per unità di tempo che possono venire trasmessi.
- La capacità è quindi:

$$C = \lim_{T \rightarrow \infty} \frac{\log N(T)}{T}$$

---

---

---

---

---

---

---

---

## Teorema

- Siano  $H$  (bit/simbolo) e  $C$  (bit/secondo), rispettivamente, l'entropia di una sorgente e la capacità di un canale senza rumore;
- È possibile codificare i simboli emessi dalla sorgente in modo di trasmettere in media:  
 $(C/H) - \epsilon$  simboli al secondo
- ove  $\epsilon$  è un numero positivo arbitrario ( $< C/H$ ).
- Non è possibile trasmettere con velocità superiore a  $C/H$  simboli al secondo.

---

---

---

---

---

---

---

---

## Esempio

- Poniamo a 120 persone la domanda:
  - Sei destro o mancino?
- La risposta sarà  $D$ =Destro o  $M$ =Mancino e sono equiprobabili e indipendenti:
- Supponiamo che la risposta sia trasmessa nell'ordine giusto in cui è data:
  - DDDMDDMDMDDDDMD...
- Non ci basta sapere quanti sono  $D$  e quanti  $M$

---

---

---

---

---

---

---

---

## Esempio

- Supponiamo che, in media, solo il 5% della popolazione è mancina.
- L'informazione media delle risposte è:  
 $H = -0,95 \log 0,95 - 0,05 \log 0,05 = 0,2864 \text{ bit / simbolo}$
- La capacità di canale è 1 bit/sec
- Possiamo ridurre la capacità di canale necessaria se codifichiamo il messaggio
- Pertanto, la capacità di canale si riduce a 0,35 bit/sec

---

---

---

---

---

---

---

---

## Efficienza di codificazione

- Diciamo efficienza di codificazione il rapporto fra entropia del messaggio originale e la capacità di canale richiesta

$$\eta_c = \frac{H}{C} \times 100\%$$

- Per l'esempio precedente risulta:

$$\eta_c = \frac{0,2864}{0,35} \times 100\% = 84,6\%$$

---

---

---

---

---

---

---

---

## Canali discreti con rumore

- Consideriamo ora il caso in cui la trasmissione non è perfetta a causa della presenza di rumore nel canale.
- Supponiamo che il disturbo su un simbolo sia indipendente dai simboli precedenti e successivi.

---

---

---

---

---

---

---

---

## Entropie

- $H(x)$  = entropia della sorgente o d'ingresso del canale
- $H(y)$  = entropia del ricevente o d'uscita del canale
- $H(y/x)$  = entropia dell'uscita, nota l'entrata
- $H(x/y)$  = entropia dell'entrata, nota l'uscita
- $H(x,y)$  = entropia congiunta dell'ingresso e dell'uscita

- Relazioni

$$H(x,y) = H(x) + H(y/x)$$

$$H(x,y) = H(y) + H(x/y)$$

---

---

---

---

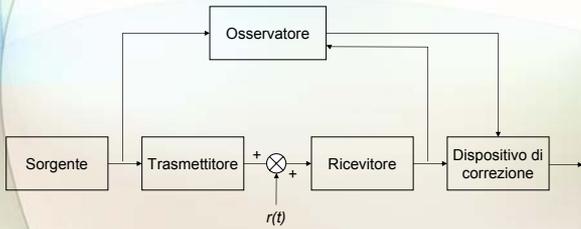
---

---

---

---

## Sistema ideale di comunicazioni



---

---

---

---

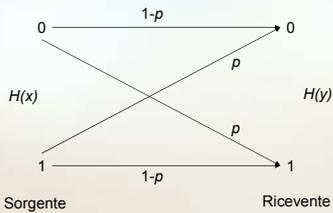
---

---

---

---

## Canale binario simmetrico



---

---

---

---

---

---

---

---

## L'informazione

$$P(\text{nessun errore}) = P(0) = P(\hat{e}1)P\left(\frac{1}{1}\right) + P(\hat{e}0)P\left(\frac{0}{0}\right)$$

- Ossia:  $P(0) = \frac{1}{2}(1-p) + \frac{1}{2}(1-p) = 1-p$

- La probabilità che l'osservatore invii un 1 è:

$$P(\text{errore}) = P(1) = \frac{1}{2}p + \frac{1}{2}p = p$$

- L'entropia del segnale è:

$$-p \log p - (1-p) \log(1-p)$$

---

---

---

---

---

---

---

---

## Tasso di trasmissione del canale

- Si dimostra che la formula precedente è uguale ed  $H(x/y)$

$$\tau = H'(x) - H'(x/y) \text{ bit/sec}$$

- $H(x/y)$  viene detto *equivocazione* e rappresenta l'informazione perduta per la presenza di rumore nel canale

---

---

---

---

---

---

---

---

## Rumore non influente

- Se il rumore nel canale non provoca errori allora si ha:

$$\tau = H'(x) = H'(y) \text{ bit/sec}$$

---

---

---

---

---

---

---

---

## Capacità di un canale discreto

- La capacità di un canale discreto senza rumore era data dal massimo tasso di informazione che il canale permetteva di trasmettere
- La capacità di canale con rumore è definita come il tasso massimo con cui il canale può fornire informazione al ricevitore:

$$C = \max\{H'(x) - H'(x/y)\} \text{ bit/sec}$$

---

---

---

---

---

---

---

---