

Teoria dell'Informazione

Federico Matteoni

A.A. 2019/20

Indice

1	Introduzione	5
----------	---------------------	----------

1.1	Assiomi di Shannon	5
-----	------------------------------	---

Capitolo 1

Introduzione

Francesco Romani `romani@di.unipi.it`
Mathematical Theory of Communication, Shannon.

Teoria Fondamentale per l'informatica, passata in secondo piano rispetto alle nuove architetture, linguaggi moderni, multi-processing. Cambia tutto con la preponderanza della rete e con la diffusione degli smartphone. La base della trasmissione e della comunicazione, sia per 0/1 che per segnali, è basata sui concetti in questo corso. Importante perché le varie generazioni di reti telefoniche, differiscono per bande di frequenza ecc..., ma per aumentare la trasmissione non si aumenta la potenza di trasmissione del segnale (rischi per la salute, diminuzione durata batteria). Piuttosto con algoritmi di trasmissioni più furbi, sistemi sofisticati di riconoscimento dei segnali, errori...
Noi partiamo da più lontano.

Esperimento finito Estrazione su un alfabeto discreto. Probabilità uscita di un elemento può essere diversa dalle altre.

$$p(x_1) \neq p(x_k)$$

Ogni esperimento ha una sua incertezza. Detto così il concetto è vago, ma ci sono esperimenti più incerti di altri. Un indice di incertezza dei risultati sportivi sono le quote. L'incertezza non è influenzata da nozioni sull'esperimento.

1.1 Assiomi di Shannon

Shannon definì una funzione di incertezza con tre assiomi:

1. Incertezza di p_1, p_2, \dots, p_k è una funzione continua delle p_i . p_i sono probabilità, quindi sommano a 1.
2. Incertezza di un oggetto con k esperimenti equiprobabili è strettamente minore di quello con $k+1$ esperimenti.
3. Esperimento composto. Faccio esperimento con certo n risultati. Per ognuno di questi faccio esperimento con certo m risultati. L'incertezza totale è l'incertezza del primo esperimento sommata all'incertezza di ciascuno esperimento successivo pesata con la probabilità del risultato corrispondente.

Postulato Definizione che si dà per vero a priori senza dimostrazione.

Assioma Definizioni che si mettono a base di una teoria, senza che siano per forza veri nella realtà.

Gli assiomi sono posizioni **ragionevoli** di Shannon su cui ha costruito la teoria. Consentono di trovare il valore di H incertezza.

Lemma 1.1 Se f positiva... **dim**

Lemma 1.2 L'incertezza di un esperimento ripetuto n volte è n volte l'incertezza dell'esperimento. $H(Y^n) = nH(Y)$ quindi $H(Y^n) = H(Y) + H(Y^{n-1})$ **dim**

Lemma 1.3 L'incertezza associata ad un esperimento con k uscite equiprobabili è $C \log(k)$

Teorema 1.1 L'unica funzione H che soddisfa i tre assiomi è

$$-C \sum_{i=1}^k p_i \log(p_i)$$

Entropia Incertezza associata ad un esperimento X , con $C=1/\log 2$, quindi incertezza in bit. Un bit è per definizione la quantità di incertezza associata all'esperimento con due sole uscite equiprobabili. Vale 1 quindi per il caso $p=1/2$, lancio di una moneta fedele.

Perché Shannon la definisce entropia? Perché è ha la stessa formula in fisica, ed è la stessa cosa (entropia dell'informazione e entropia fisica).

Lemma del logaritmo Quando i q tendono ai p questa espressione arriva ad un minimo.

Entropia Compresa tra 0 e $\log k$