(F1X) Teoria dell'Informazione e della Trasmissione

Simulazione di variabili casuali con lanci di monete

Docente: *Nicolò Cesa-Bianchi* versione 23 marzo 2016

Mostriamo ora come possiamo attribuire all'entropia un significato che la lega al numero medio di lanci indipendenti di una moneta non truccata per simulare l'estrazione di un simbolo da una sorgente $\langle \mathcal{X}, p \rangle$.

Cominciamo con la seguente osservazione: sia $\langle \mathcal{X}, p \rangle$ dove $p = (p_1, \ldots, p_m)$ è tale che ogni p_i è della forma $p_i = 2^{-j}$ per un qualche intero positivo j possibilmente diverso per ogni i. Sorgenti di questo tipo si chiamano diadiche. È immediato dedurre che un codice binario di Shannon $c : \mathcal{X} \to \{0,1\}^+$ è ottimo in questo caso. Infatti, se $p_i = 2^{-j}$ allora $\ell_c(x_i) = \log_2 \frac{1}{p_i} = j$. Quindi,

$$\mathbb{E}\big[\ell_c\big] = \sum_{i=1}^{m} p_i \, \ell_c(x_i) = \sum_{i=1}^{m} p_i \log_2 \frac{1}{p_i} = H(X) \ .$$

Dato che sappiamo anche che nessun altro codice istantaneo ha lunghezza media inferiore all'entropia della sorgente, deduciamo che c è ottimo.

Se ora disegnamo l'albero di codifica per c notiamo che, siccome $p_i = 2^{-j}$, allora x_i è codificata con una parola di codice $c(x_i) = (c_1, \ldots, c_j) \in \{0,1\}^j$ a profondità j nell'albero. Questo implica il seguente fatto interessante: per estrarre un simbolo X dalla sorgente posso partire dalla radice dell'albero di codifica e percorrerlo a caso fino ad arrivare ad una foglia. La probabilità di arrivare alla foglia $c(x_i)$ è esattamente $p_i = 2^{-j}$, in quanto per j volte ho scelto se andare a destra o a sinistra.

A questo punto possiamo fare due osservazioni. Primo, se estraggo un simbolo da una sorgente diadica allora i bit della sua codifica istantanea ottima sono casuali. Questo conferma che stiamo comprimendo al massimo, infatti non mi aspetto di poter comprimere ulteriormente una sequenza casuale di bit. Secondo, posso usare un codice istantaneo ottimo per simulare l'estrazione di un simbolo da una sorgente diadica usando dei lanci di moneta per percorrere l'albero di codifica. Il numero medio di lanci che mi occorre è pari all'entropia della sorgente.

Abbiamo quindi visto che, nel caso di sorgenti diadiche posso usare dei lanci di moneta per simulare l'estrazione di un simbolo dalla sorgente. Il numero atteso di lanci è pari all'entropia della sorgente. Dato che la distribuzione di n lanci indipendenti di moneta ha un'entropia pari ad n, posso estrarre un simbolo da una sorgente diadica di entropia n usando un'altra sorgente con la stessa entropia. È possibile estendere questa analisi al caso di sorgenti non necessariamente diadiche. In questo caso, il numero atteso di lanci è compreso fra $H(X)$ e $H(X) + 2$.