Complementi di Algoritmi e Strutture Dati

L'estrattore di von Neumann

Docente: *Nicolò Cesa-Bianchi* versione 15 giugno 2017

Un estrattore di causalità è una funzione che trasforma una sorgente non perfettamente casuale in una completamente casuale. Il più semplice estrattore è quello ideato da John von Neumann e risponde alla domanda: come è possibile usare una moneta truccata per simulare dei lanci di moneta non truccata?

Più precisamente, abbiamo una moneta con probabilità sconosciuta $0 < p < 1$ di restituire testa ogni volta che viene lanciata e vogliamo usarla per simulare una sequenza di lanci di una moneta con probabilità $\frac{1}{2}$ di restituire testa.

Siano $X_1, X_2, \ldots$ le variabili casuali Bernoulliane indipendenti con $\mathbb{P}(X_t = 1) = p$ che modellano i lanci della moneta truccata. Consideriamo le coppie $(X_1, X_2), (X_3, X_4), \ldots$ e notiamo che i valori possibili per ogni coppia sono:

$(0,0)$	con probabilità $(1-p)^2$
$(1,1)$	con probabilità p^2
$(0,1)$ e $(1,0)$	ciascuna con probabilità $p(1-p)$.

Quindi, per ogni coppia (X_{2k-1}, X_{2k}) gli eventi $(X_{2k-1}, X_{2k}) = (0,1)$ e $(X_{2k-1}, X_{2k}) = (1,0)$ sono equiprobabili e forniscono la sequenza di lanci desiderata.

Algorithm 1 (estrattore di von Neumann)

Input: Sequenza di lanci $X_1, X_2, \ldots$

```
for k = 1, 2, ... do
    if X_{2k-1} ≠ X_{2k} then                          ▷ coppia utile
        if X_{2k-1} = 1 then
            Print "Testa"
        else
            Print "Croce"
        end if
    end if
end for
```

Possiamo ora calcolare quanti lanci di moneta truccata mi servono in media per simulare un lancio di moneta non truccata. Data una sequenza $Z_1, Z_2, \ldots$ di variabili Bernoulliane indipendenti tali che $\mathbb{P}(Z_k = 1) = q$ per $k \geq 1$, la variabile casuale Geometrica G è definita come $G = \min\{k = 1, 2, \ldots : Z_k = 1\}$. Chiaramente, $\mathbb{P}(G = 1) = q$ e $\mathbb{P}(G = n) = (1-q)^{n-1}q$ per ogni $n > 1$. Non è difficile dimostrare che $\mathbb{E}[G] = \frac{1}{q}$.

Consideriamo ora la sequenza $Z_1, Z_2, \ldots$ di variabili Bernoulliane indipendenti tali che

$$Z_k = \begin{cases} 1 & X_{2k-1} \neq X_{2k} \\ 0 & \text{altrimenti.} \end{cases}$$

Per quanto detto prima, $\mathbb{P}(Z_k = 1) = 2p(1-p)$. Sia G la variabile geometrica associata alla sequenza delle Z_k. Quindi, il numero medio di lanci che mi servono è

$$2\,\mathbb{E}[G] = \frac{1}{p(1-p)} \ .$$