Protocollo Montecarlo Pedemonte Giacomo s4861715 Relazione

Prima di tutto specifichiamo le specifiche appunto per il raggiungimento del consenso Bizantino.

Tabella 1: Specifiche per il raggiungimento del consenso bizantino

Durante ogni *round* ogni processo spedisce un *bit* a ogni altro processo
Prima dell'inizio di un nuovo *round* ogni processo ha ricevuto un *bit* da ogni altro processo
Nello stesso *round* ogni processo affidabile spedisce lo stesso *bit* a ogni altro processo

Seguendo questo protocollo, ogni processo affidabile, termina con una decisione finale che consiste nell' accordo (stesso valore del bit di informazione) per tutti questi processi.

Usiamo quindi il Protocollo Monte Carlo per risolvere l'accordo Bizantino nel caso minimale.

```
Numero di round per avere probabilita' di raggiungere un accordo > del 99.9% e': 10

MEDIA ROUND:1.7475
Mentre la varianza: 2.63174
```

Questi valori riportanti nell'esecuzione del codice contenuto in "protocollo_Montecarlo.cpp" sono stati ricavati grazie all' utilizzo di una matrice di appoggio che per ogni round si teneva conto dei consensi raggiunti, così per 10^4 iterazioni per ottenere il numero di round dopo il quale è possibile trovare un accordo con una probabilità maggiore del 99.9%.

Dopo queste iterazioni il risultato finale ci riporta che questo numero di round è 10.

La MEDIA ROUND riportata nel risultato sopra inserito è stata calcolata tra tutti e soli questi round che "portavano" questa percentuale di raggiungimento di un accordo.

Per concludere.

Sappiamo che:

Se **$n \geq 3t + 1$** (→dove n è il numero di processi e t il numero di processi inaffidabili),

il consenso può essere sempre raggiunto e in un numero di round dell'ordine di **$O(t + 1)$**

Questo valore, nel nostro caso è 2, quindi la MEDIA ROUND nel risultato conferma la stima.

La probabilità di raggiungere un accordo è maggiore del 99.9% dopo 10 round perché ad ogni round con probabilità 1/2 dopo l'esito del lancio della prima moneta tutti i processi affidabili "saranno d'accordo"

Infatti:

1-(0.5^10) = 0.999.