Protocollo *MonteCarlo*

Il seguente laboratorio riprende l'argomento svolto a lezione del problema del consenso bizantino dove ci sono n generali e di cui n-1 è un traditore. Prendendo in considerazione il seguente caso abbiamo un sistema distribuito in cui abbiamo n=4 processi di cui 1, il quarto, è inaffidabile. Ogni processo affidabile segue il protocollo Montecarlo e dopo un certo numero di round si arriva ad una decisione, le scelte sono due o 1 o 0, perciò b(i) $\in$ {0,1} se i processi affidabili assumono valore uguale si arriva al consenso.
Un risultato classico dimostra che è sufficiente e necessario avere n>= 3t+1 con t=1 ed il consenso può sempre essere raggiunto in un numero di round nell'ordine di O(t + 1).

Avendo n=4 processi affidabili e 1 inaffidabile e fissando l'ipotesi che a ogni round il risultato del lancio di una moneta globale con probabilità Pr(testa) = Pr(croce) = 1/2 e` comunicato a tutti i processi, l'algoritmo del protocollo Montecarlo.
Nel codice troviamo la dichiarazione della matrice in cui verranno memorizzate le varie scelte dei generali, si entra nel ciclo di ripetizioni in cui viene fatta la trasmissione del bit i-esimo ai n-1 processi e scelta opposta per il processo inaffidabile, dopodiché finchè non si raggiunge l'accordo si ripetono i giri/round e qui viene effettuato l'algoritmo del protocollo Montecarlo
loop = TRUE while (*loop*)

1. trasmetti b(i) agli altri n−1 processi

2. ricevi i valori spediti dagli altri n−1 processi

3. maj(i) ← valore maggioritario tra i ricevuti (incluso il proprio)

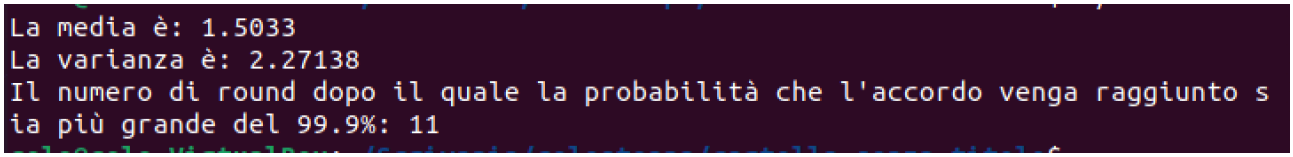
4. tally(i) ← numero dei valori uguali a maj(i)

5. if tally(i)≥2t+1
   then b(i) ← maj(i) else if testa
   then b(i) ← 1 else b(i) ← 0

Quando si raggiunge il consenso si aggiungono in un vettore il numero di round necessario per raggiungere l'accordo, necessario per poter successivamente calcolare media e varianza del numero di

round necessari per raggiungere l'accordo e per determinare il numero di *round* dopo il quale la probabilità che l'accordo è raggiunto è più grande del 99.9%.

I risultati iterando 10000 volte riporta i seguenti risultati come



come già detto precedentemente se abbiamo n>=3t+1 dove n=4 cioè i processi totali e t=1 il processo inaffidabile il consenso può sempre essere raggiunto in un numero di round nell'ordine di O(t + 1), quindi O(2), da ciò traiamo che la media è corretta. I processi inaffidabili sono al più t, quindi 1, questo implica che non ci sarà un processo j per cui tally(j)>=2t+1, ovvero 3, con maj(j)=1-maj(i)=0, perciò la probabilità di raggiungere un accordo è maggiore del 99.9% dopo 11 round perché ad ogni round con probabilità 1/2 dopo l'esito del lancio della prima moneta tutti i processi affidabili avranno raggiunto il consenso ed infatti 1-(0.5^11) = 0.999.