

Relazione accordo bizantino , Ferrari Luca s4784573

Nel main(), vengono inizializzate e create le strutture dati (in questo caso array) e le variabili che ci serviranno per raggiungere l'accordo.

Subito dopo troviamo un ciclo il quale itererà per 10^4 volte su l'inizializzazione della nostra matrice a [][] e appunto sul codice per trovare l'accordo ovvero:

```
maj(i) ← valore maggioritario tra i ricevuti (incluso il proprio)
tally(i) ← numero dei valori uguali a maj(i)
if tally(i) ≥ 2t + 1
    then b(i) ← maj(i)
else if testa
    then b(i) ← 1
else b(i) ← 0
```

Preceduto dalla condizione while(loop != false).

Subito dopo il while abbiamo un iterazione con una variabile i sulle righe della matrice (ovvero 3 righe, ciclo for)

controllo che verifica che la matrice inizializzata non sia già in accordo, in quel caso viene settato il numero di round (in questo caso 0) , loop a false e si esce dal ciclo for con un break.

Altrimenti vengono calcolati maj e tally tramite le funzioni mj e ty.

Calcolato maj e tally ho seguito riga per riga lo pseudo codice.

Finita l'iterazione sulle 3 righe si controlla appunto se si è raggiunto un accordo tramite l'if di preconditione se ciò avviene viene settato il numero di round e si esce , altrimenti si continua fino a quando l'accordo non viene trovato l'accordo.

Trovato l'accordo e finite le 10^4 iterazioni fuori dal for ci aspetta il calcolo della media, la varianza e il numero di round dopo il quale la probabilità di raggiungere un accordo è maggiore del 99.9%

Calcolate tramite le funzioni:

- media()
- varianza()
- accprob()

Iterando codice per 10^4 voltesi ha una media di 1.7563 round, una varianza di 2.64911 e chela probabilità di raggiungere un accordo è maggiore del 99.9% dopo 10 round.

```
MEDIA ROUND:1.7563
Il numero di round dopo il quale la probabilita di raggiungere un accordo > del 99.9% p: 10
varianza: 2.64911
```

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 $O(t + 1)$, che nel nostro caso è 2, quindi il valore che ci esce come media 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 avranno raggiunto il consenso ed infatti $1-(0.5^{10}) = 0.999$.