Ninivaggi Luca 5312342

# ACCORDO BIZANTINO

Supponiamo P1,P2 (Generali) processi favorevoli con P3 processo “faulty” (Traditore).

Indichiamo con $\Delta_1$ e $\Delta_2$ i valori iniziali che assumono rispettivamente P1 e P2.

Con $M(P_i, P_j, N)$ indichiamo il messaggio che il processo i ha inviato al processo j al round N.

Supponiamo che tutti i messaggi siano inviati (e successivamente ricevuti) nello stesso momento se appartenenti allo stesso round: il traditore non può aspettare di averli ricevuti prima di inviare il suo.

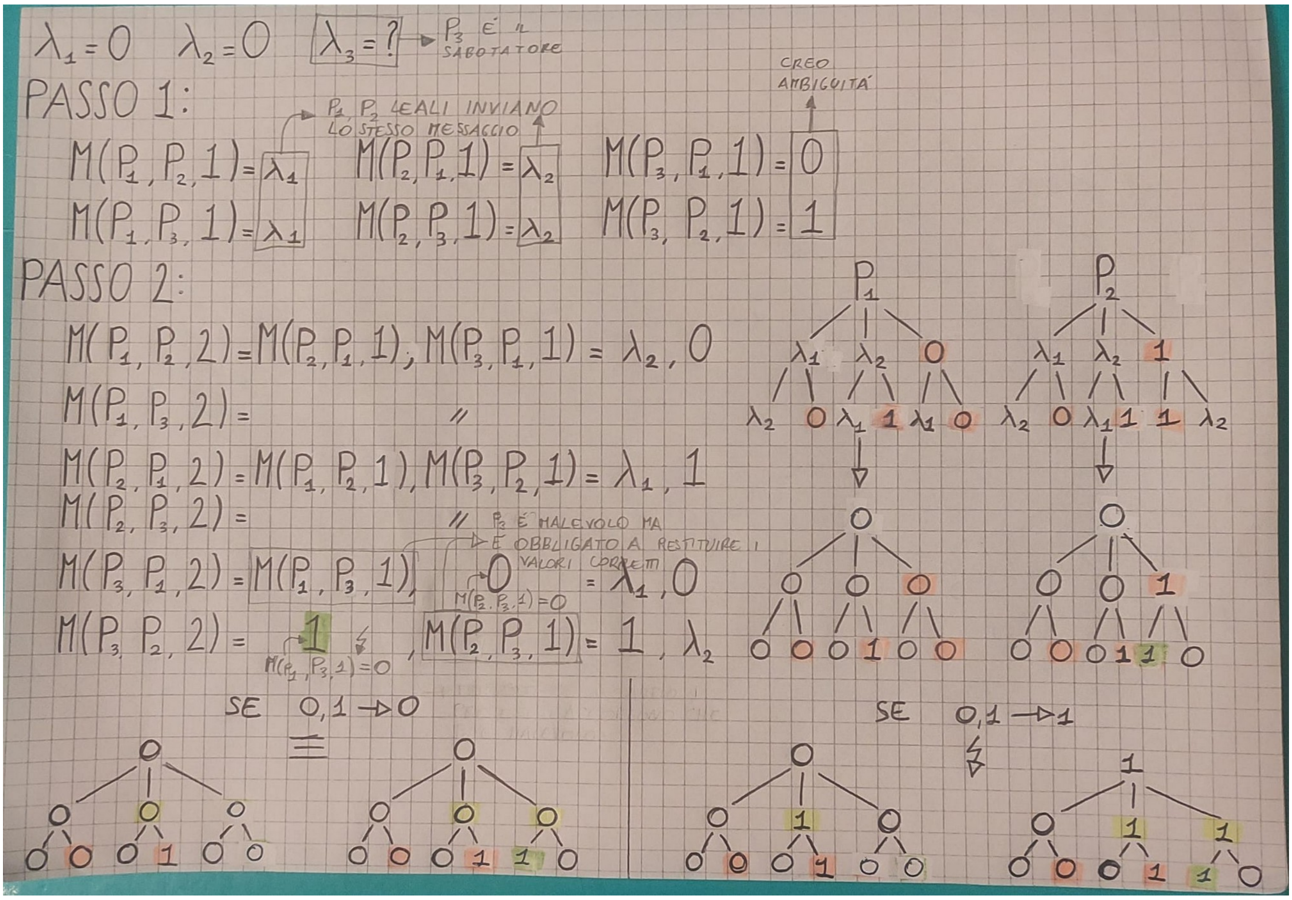
Come limitazione al traditore, deve comunicare nel round 2 a un $P_i$ il valore che effettivamente $P_i$ ha comunicato di avere (ovvero $\Delta_1$): altrimenti ,$P_i$ si accorgerebbe della falsificazione, scoprendo il traditore.

Nelle foto seguenti, alla destra dei passi osserviamo gli alberi dei relativi processi, e al di sotto vediamo effettivamente i valori calcolati.

In fondo alla pagina è esplicitato il calcolo ottenuto dallo studio “bottom-up” dell’ albero.

In arancione indichiamo i valori decisi da P3, in verde quelli “modificati” da P3 (ovvero figli del fatto che P3 non deve dire la verità) mentre in giallo i nodi che vengono calcolati in modo arbitrario (ovvero se sono in pareggio).

## P1 e P2 CONCORDANTI



Al passo 1 notiamo come P1 e P2 comunichino a tutti il proprio valore, mentre P3 fornisce risultati contrastanti ai 2 processi: in questo modo, non si preclude la possibilità di poterli ingannare (siano i valori iniziali 1,0 0,1 1,1 o 0,0 la prima mossa di P3 non cambia).

Al secondo passo, P1 e P2 comunicano i valori ottenuti in precedenza: di fatto, comunicano le loro "opinioni" sui valori degli altri processi.

P3 si trova obbligato a dover comunicare al processo destinatario il valore corretto (altrimenti si accorgerebbe che sta barando), mentre può scegliere in modo arbitrario la "credenza" sull' altro processo: Nel nostro esempio, "mente" a P2, dicendogli "P1 mi ha inviato il valore 1".

L' ambiguità risiede infatti nella difficoltà che ha P2 di chi scegliere di cui fidarsi: P1 o P3.

Come possiamo vedere nei risultati, P1 calcola sempre il suo valore = 0, poiché non è stato vittima di inganni e perciò non si trova in difficoltà.

P2 ottiene invece 2 sottoalberi su 3 in parità, entrambi con 0,1: in caso di parità, definiamo un valore scelto a caso tra 0,1 (dal punto di vista pratico, il lancio della moneta).

Se la moneta ha un esito congruente al valore $\Delta$ ovvero al valore calcolato correttamente da P1, allora anche P2 materializzerà il risultato corretto.

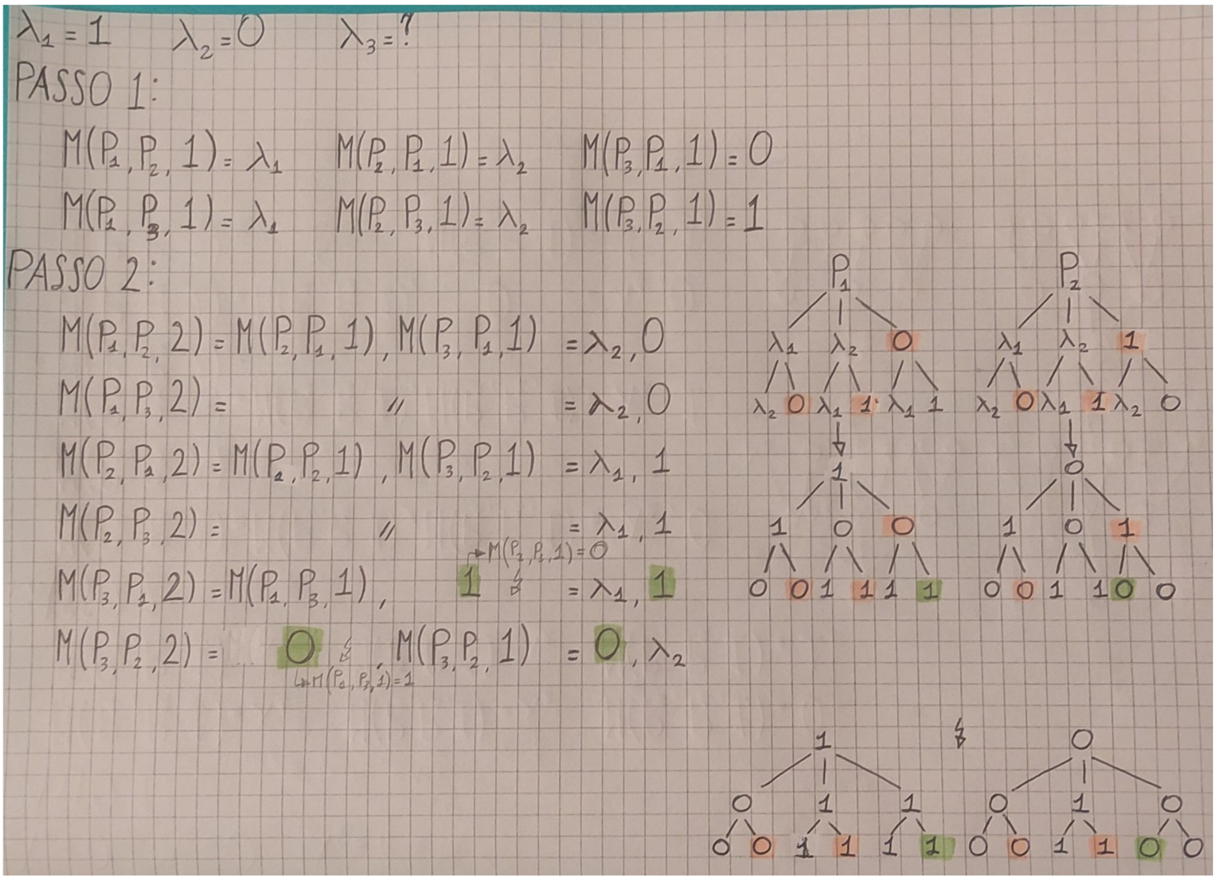
Se invece il risultato della moneta non coinciderà con $\Delta$, allora il "traditore" avrà vinto.

Osserviamo come al passo 2, il traditore si concentri su un solo processo a cui far cambiare previsione: se al passo 2 mentisse a entrambi (e quindi anche a P1 mandasse un 1, falsificato), avremmo 2 alberi di P1, P2 analoghi, e quindi entrambi i valori assumerebbero il valore del lancio, ponendoli in accordo tra loro e facendo fallire il traditore.

Possiamo quindi concludere che se inizialmente in accordo, il traditore ha ½ di probabilità di vincere.

Otteniamo le stesse conclusioni se $\Delta_1 = \Delta_2 = 1$ oppure se i valori iniziali 0,1 inviati da P3 sono invertiti: anche in questo caso, sarà nuovamente il processo con il valore ricevuto diverso dal suo delta a poter essere ambiguo.

# P1 e P2 IN DISACCORDO




Analogamente all’ esempio precedente, P3 invia al passo 1 messaggi discordanti.

Osserviamo come se P3 inviasse a P1 il valore $\Delta_1$, e allo stesso modo anche a P2 inviasse $\Delta_2$, otterremmo su 2 nodi su 3, in entrambi gli alberi, un pareggio: il valore convergerebbe sul lancio della moneta, decretando la vittoria dei generali qualsiasi sia l’ esito.

Osservando tutto ciò, possiamo dire che P3 ha ½ di possibilità di sconfitta se $\Delta_1$ è diverso da $\Delta_2$.

Supponiamo che P1 riceva da P3 il valore diverso dal suo $\Delta_1$, e in modo analogo per P2 riceva diverso da $\Delta_2$.

Al passo 2, entrambi i processi ricevono una menzogna da P3, che serve a confermare la relativa idea (P3 comunica a $P_i$ che la sua idea è giusta, ed entrambi sceglieranno $\Delta_i$): in questo modo, mantengono i valori del relativo Δ, e concludono in maniera discordante.

# CONCLUSIONI

P3 ha quindi ½ di probabilità di poter vincere, indipendentemente dalla condizione di partenza di P1 e P2.

- Se $\Delta_1$¿$\Delta_2$ allora la casualità è data dal lancio della moneta
- Se $\Delta_1 \neq \Delta_2$ allora la casualità è data dalla scelta che P3 compie al primo passo, ovvero a chi mandare il valore 1 e a chi il valore 0