SEMANTICA DEI CONNETTIVI MODALI n-ARI

Sia S un insieme e $R \subseteq \underbrace{S \times \dots \times S}_{n+1 \text{ volte}}$ una relazione $(n+1)$-aria su S e M un modello su (S,R). Sia $w \in S$. Scriviamo $M \models_w \square(F_1, \dots, F_n) \iff \forall v_1, \dots, v_n \in S \mid (w, v_1, \dots, v_n) \in R$. Si ha che $M \models_{v_1} F_1, \dots, M \models_{v_n} F_n$

LOGICHE TEMPORALI LTL

(LINEAR-TIME TEMPORAL LOGIC)

Queste logiche hanno tre connettivi modali 1-ari:

- X → NEXT STATE
- F → SOME FUTURE STATE
- G → GLOBALLY (=ALL) FUTURE STATES

E tre connettivi 2-ari:

- U → UNTIL
- R → RELEASE
- W → WEAK-UNTIL

SEMANTICA

Sia (S,R), con $R \subseteq S \times S$, un frame | R sia non riflessiva. Con R^* indichiamo la chiusura transitiva e riflessiva di R, ossia ogni volta che abbiamo $x \to y \to z$ in R, abbiamo
$$\begin{tikzcd} x \arrow[r] \arrow[rr, bend left] & y \arrow[r] & z \end{tikzcd}$$
in R^* e
$$\begin{tikzcd} x \arrow[loop above] \end{tikzcd}$$
in R^* $\forall x \in S$.

1) X È DA CONSIDERARE COME IL CONNETTIVO MODALE $\Box$ SUL FRAME (S,R)

2) G È DA CONSIDERARE COME IL CONNETTIVO MODALE $\Box$ SUL FRAME (S,R^*)

3) F È DA CONSIDERARSI COME IL CONNETTIVO MODALE $\Diamond$ SUL FRAME (S,R^*)

$\Rightarrow F\varphi = \neg G \neg \varphi \ \forall$ FORMULA φ

4) U È UN CONNETTIVO MODALE 2-ARIO DEFINITO DA $M \models_x U(\varphi,\psi) \Leftrightarrow$

- $\exists z \in S \mid (x,z) \in R^* \wedge M \models_z \psi$
- $M \models_y \varphi \ \forall y \in S \mid (x,y) \in R^* \wedge (y,z) \in R^* \wedge y \neq z$

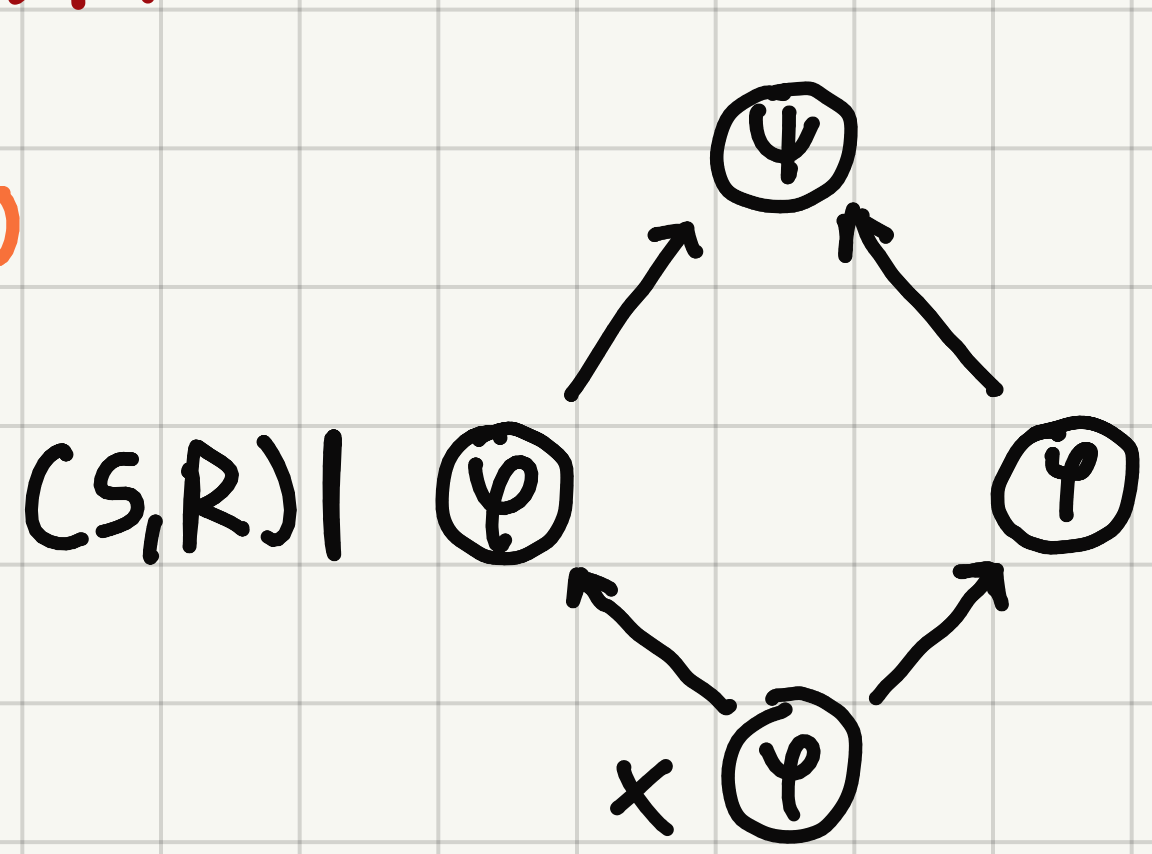
5) $W(\varphi,\psi) \Leftrightarrow U(\varphi,\psi) \vee G\varphi$

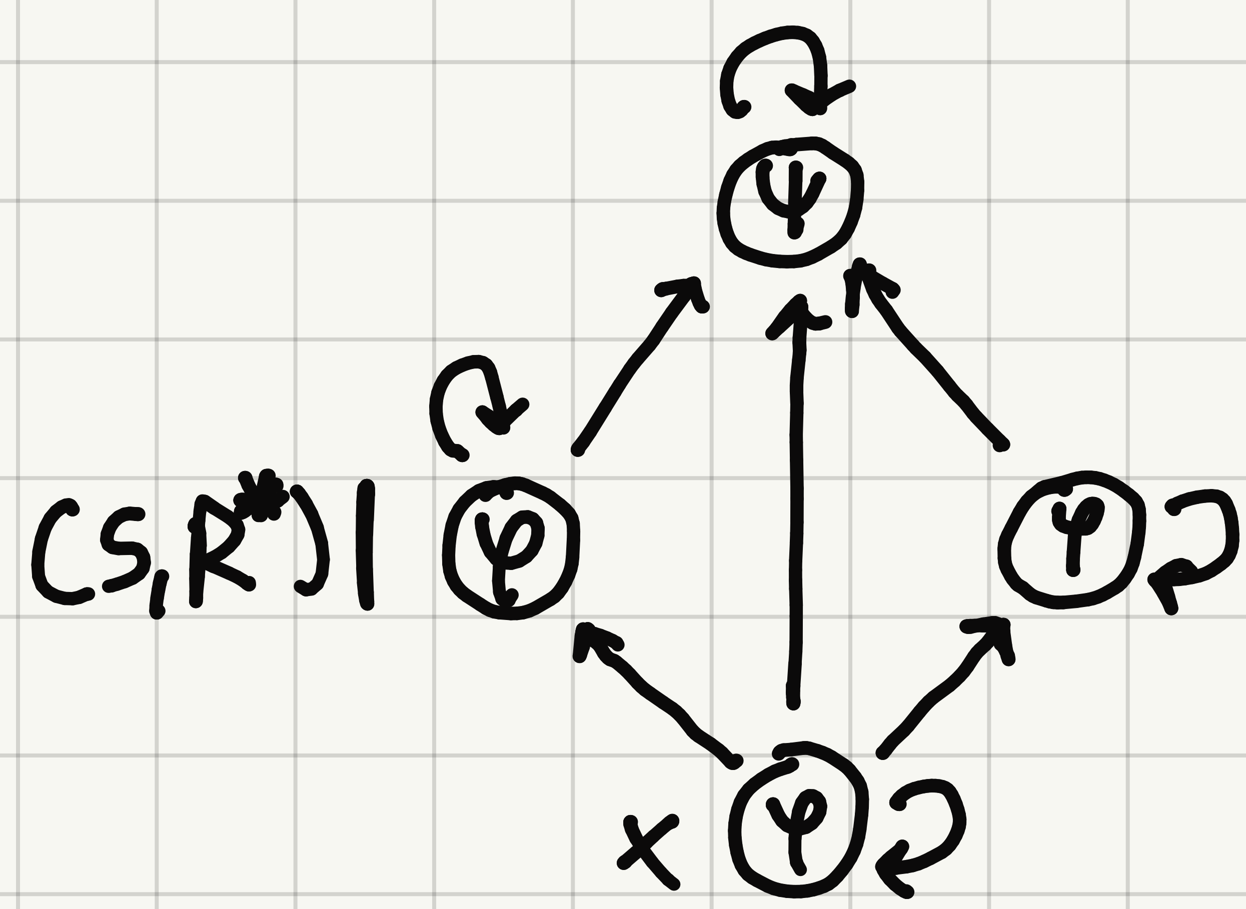
6) $R(\varphi,\psi) \Leftrightarrow \neg U(\neg\varphi,\neg\psi)$

QUINDI, GLI UNICI CONNETTIVI MODALI PER DEFINIRE QUESTA LOGICA X, G E U. GLI ALTRI SONO ESPRIMIBILI IN TERMINI DI QUESTI

ESEMPI:

a)





$M \models_x X\varphi$, $M \not\models_x G\varphi$, $M \models_x F\varphi$, $M \models_x U(\varphi,\psi)$, $M \models_x W(\varphi,\psi)$, $M \models_x R(\varphi,\psi)$

b) (S,R) |

$$\begin{tikzcd} x\ \psi \arrow[r] & \psi \arrow[r] & \varphi\wedge\psi\ y \end{tikzcd}$$

(S,R^*) |

$$\begin{tikzcd} x\ \psi \arrow[r] \arrow[rr, bend left] \arrow[loop below] & \psi \arrow[r] \arrow[loop below] & \varphi\wedge\psi\ y \arrow[loop below] \end{tikzcd}$$

$M \models_x X\psi$, $M \models_x G\psi$, $M \models_y G\psi$, $M \not\models_x X\varphi$, $M \not\models_x G\varphi$,

$M \models_y G\varphi$, $M \models_x F\varphi$, $M \models_x U(\psi,\varphi)$, $M \models_x W(\psi,\varphi)$,

$M \models_x R(\varphi,\psi)$

$\varphi R \psi : \neg U(\neg\varphi, \neg\psi)$

$M \models_x \neg U(\neg\varphi,\neg\psi) \Leftrightarrow M \not\models_x U(\neg\varphi,\neg\psi) \Leftrightarrow$

$\Leftrightarrow (\forall z \in S \mid (x,z) \in R^*, M \models_z \psi) \vee (\forall z \in S \mid (x,z)\in R^*, M \models_z \neg\psi)$

$\exists y \in S \mid (x,y) \in R^*, (y,z) \in R^*, y \neq z, M \models_y \varphi$

ψ DEVE ESSERE VERA FINO AL PUNTO IN CUI INIZIA AD ESSERE VERA φ, OSSIA φ RILASCIA ψ

LOGICHE TEMPORALI CTL

(COMPUTATIONAL TREE LOGIC)

IN QUESTE LOGICHE MODALI, QUANTIFICHIAMO SUI CAMMINI DEL GRAFO DIRETTO CHE RAPPRESENTA IL FRAME (S,R). I CONNETTIVI MODALI SONO:

$\left.\begin{array}{l} AX, EX \\ AF, EF \\ AG, EG \end{array}\right\}$ 1-ARI

AU, EU 2-ARI

A → ALONG ALL PATHS

E → ALONG AT LEAST ONE PATH

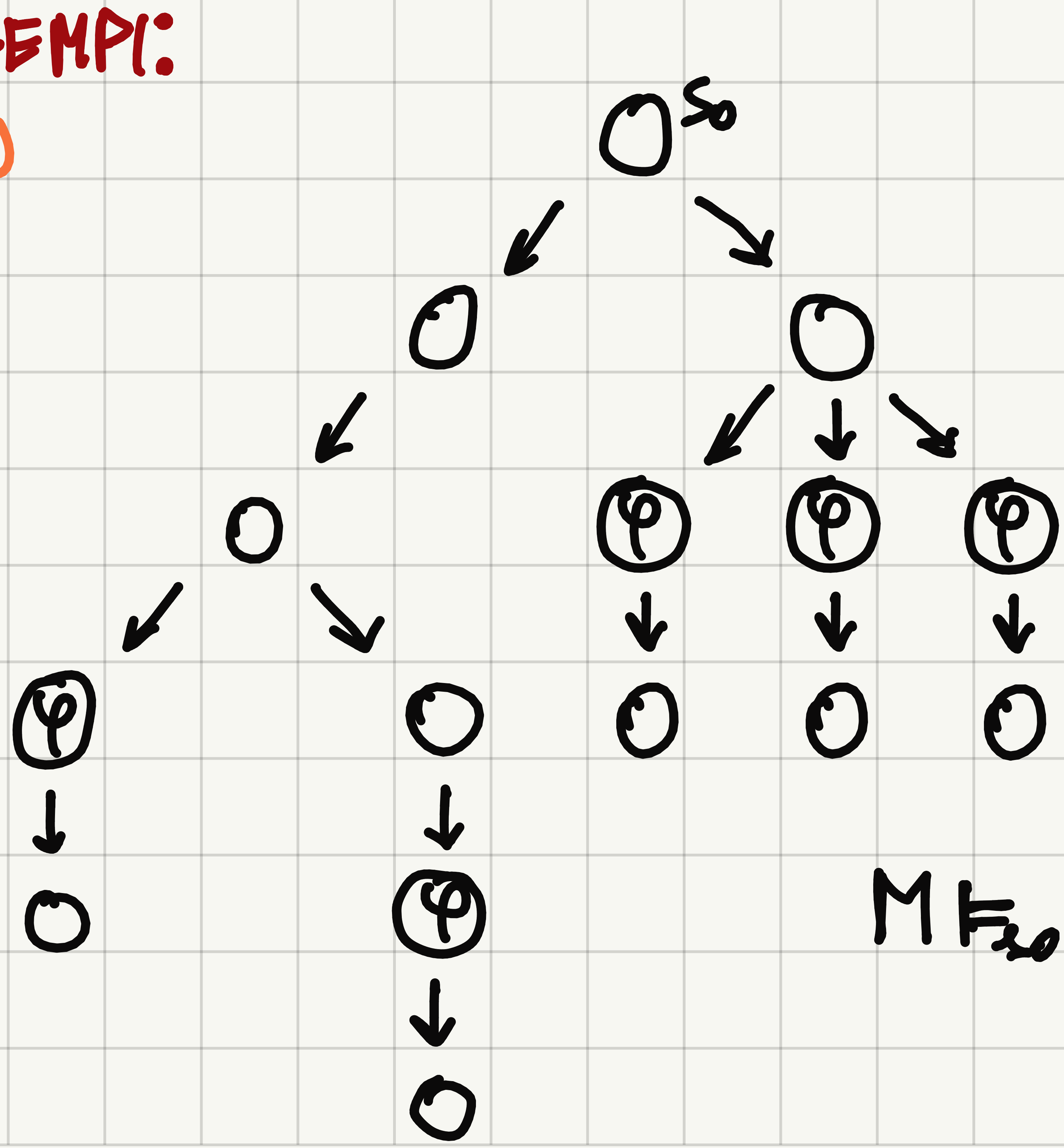
SEMANTICA

- $M \models_w AX\varphi \Leftrightarrow \forall s \in S \mid w \to s$ ABBIAMO $M \models_s \varphi$, OSSIA SI COMPORTA COME $\Box$ SUL FRAME (S, R)
- $M \models_w EX\varphi \Leftrightarrow \exists s \in S \mid w \to s$ ABBIAMO $M \models_s \varphi$, OSSIA SI COMPORTA COME $\Diamond$ SUL FRAME (S, R)
- AG SI COMPORTA COME $\Box$ SUL FRAME (S, R^*)
- $M \models_w EG\varphi \Leftrightarrow \exists$ CAMMINO $s_0 := w \to s_1 \to s_2 \to \dots$ IN $(S, R) \mid M \models_{s_i} \varphi \ \forall s_i$
- $M \models_w EU(\varphi, \psi) \Leftrightarrow \exists$ CAMMINO $s_0 := w \to s_1 \to s_2 \to \dots$ IN $(S, R) \mid M \models_w U(\varphi, \psi)$ SU QUESTO CAMMINO (IL CAMMINO $w \to s_1 \to \dots$ POSSIAMO VEDERLO COME UN SOTTOFRAME DI (S, R))

ANALOGAMENTE, SI DEFINISCONO GLI ALTRI CONNETTIVI MODALI

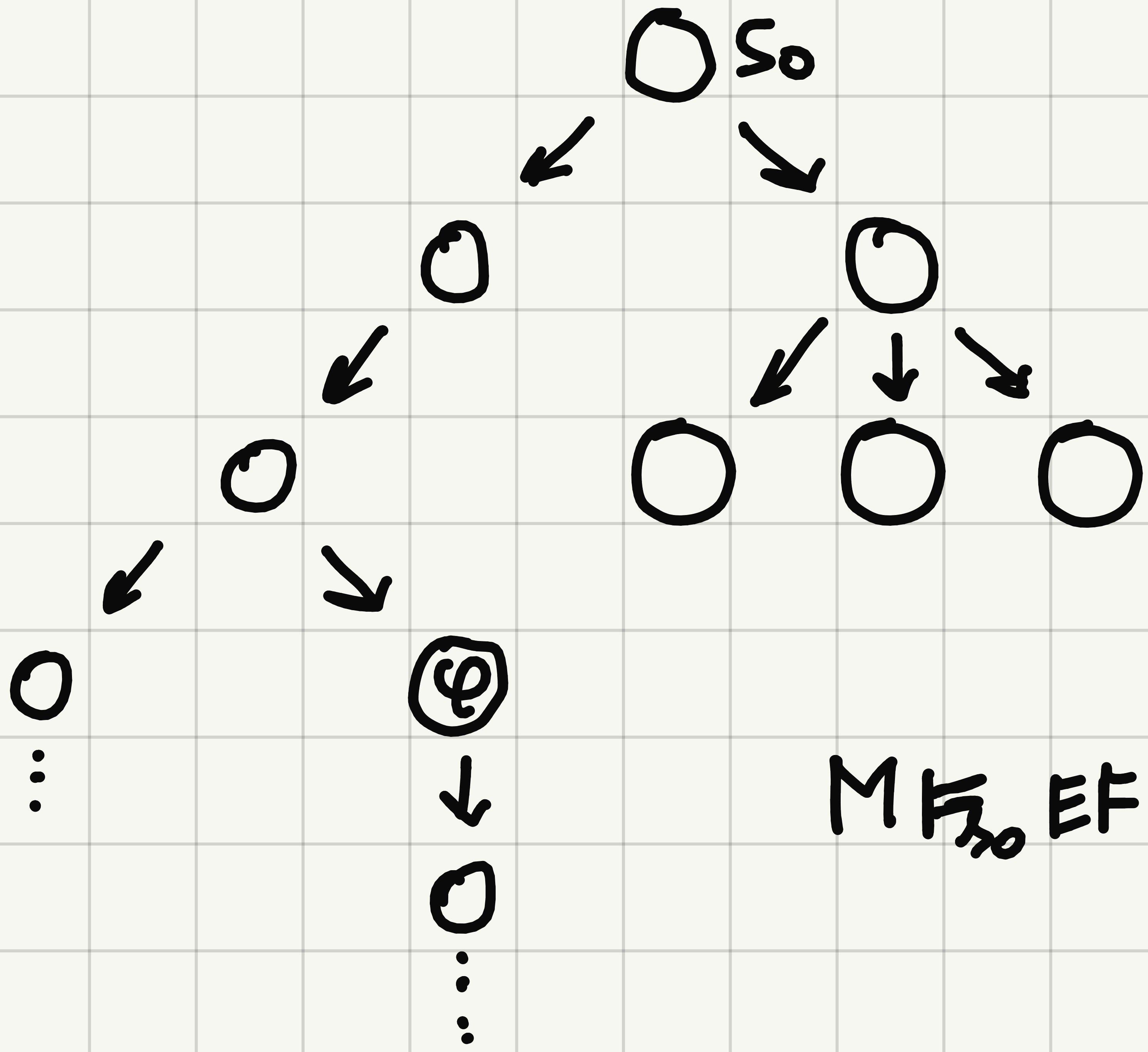
ESEMPI:

a)



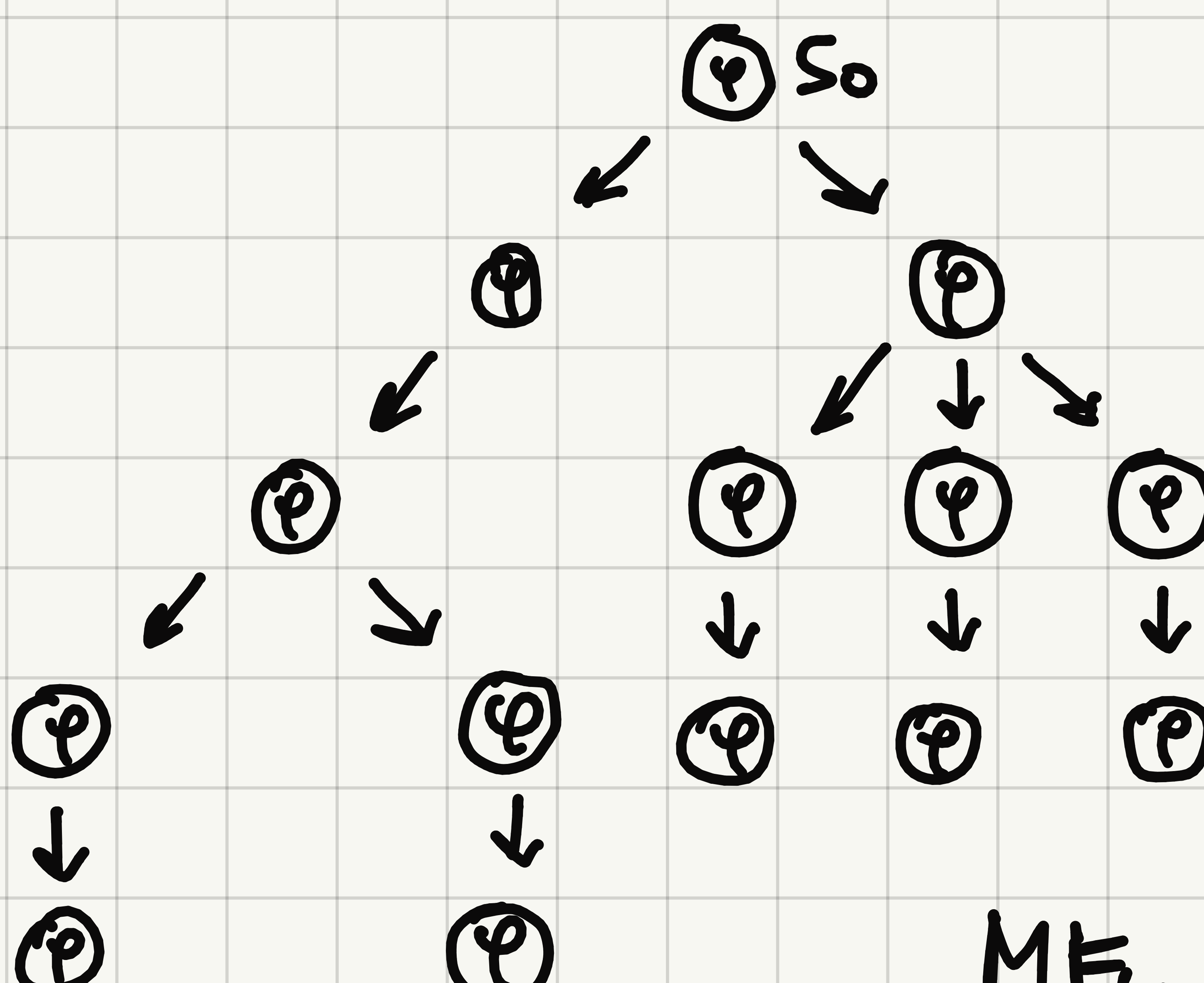
$M \models_{s_0} AF\varphi$

b)



$M \models_{s_0} EF\varphi$

c)



$M \models_{s_0} AG\varphi$

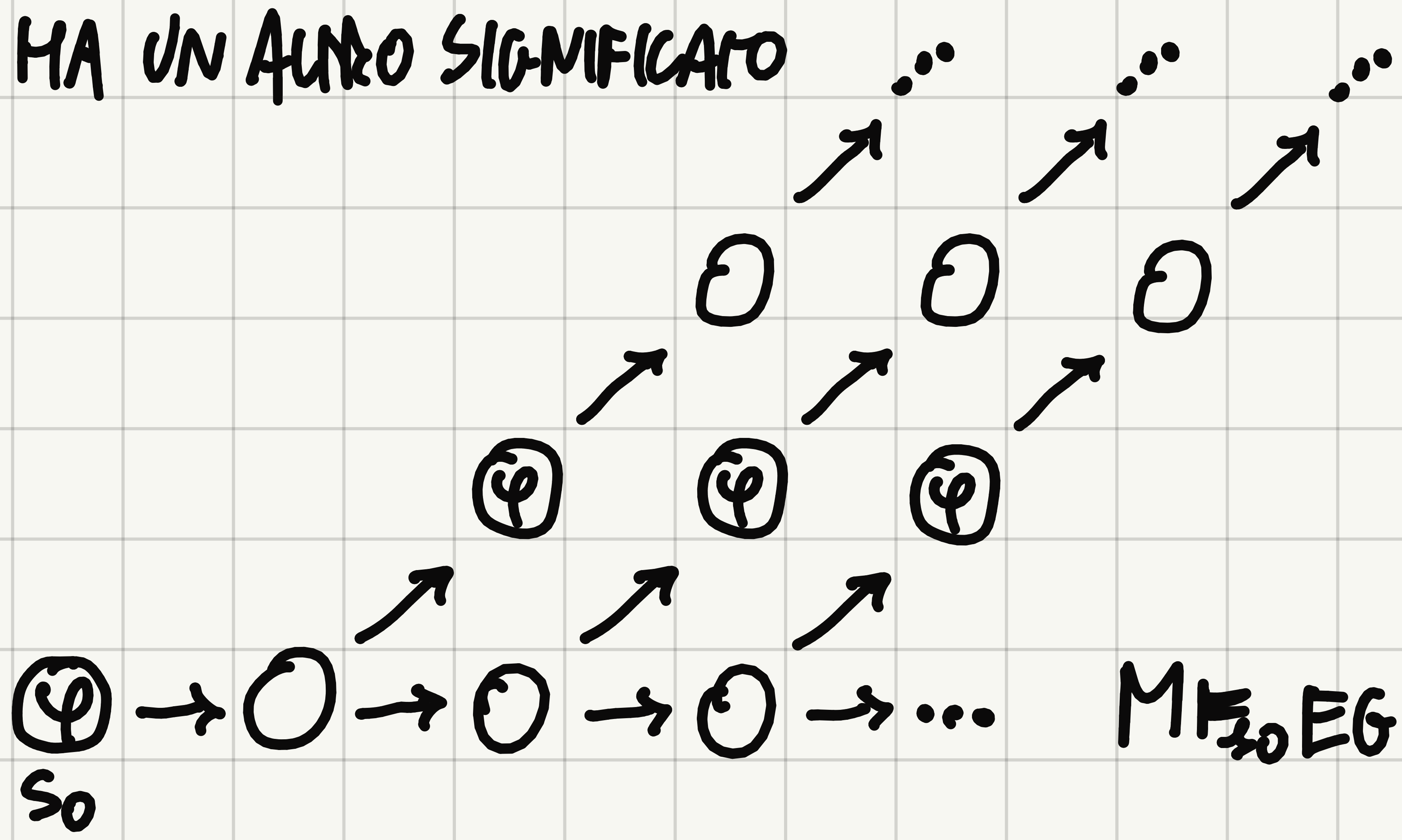
LOGICHE TEMPORALI CTL*

LE LOGICHE CTL* HANNO LA SEMANTICA DI LTL, A CUI AGGIUNGIAMO I QUANTIFICATORI SUI CAMMINI (A, E). QUINDI CTL* CONTIENE LTL E CTL. IN LTL POSSIAMO ESPRIMERE L'AFFERMAZIONE "TUTTI I CAMMINI IN CUI APPARE φ APPARE ANCHE ψ": $F\varphi \Rightarrow F\psi$. IN CTL NON POSSIAMO ESPRIMERE TALE AFFERMAZIONE. IN CTL* SÌ PERCHÉ CONTIENE LTL. L'AFFERMAZIONE

"C'È UN CAMMINO IN CUI φ APPARE INFINITE VOLTE" POSSIAMO ESPRIMERLA IN CTL^* CON LA FORMULA $E(GF\varphi)$.

NOTE:

- TALE AFFERMAZIONE PUÒ ESSERE ESPRESSA IN LTL SOLO NEL CASO IN CUI IL FRAME (S,R) NON ABBIA UN SOLO CAMMINO.
- TALE AFFERMAZIONE NON È ESPRIMIBILE IN CTL, DOVE LA FORMULA $EG(EF\varphi)$ HA UN ALTRO SIGNIFICATO



$M \models_{s_0} EG(EF\varphi)$

MODEL CHECKING: UN ESEMPIO

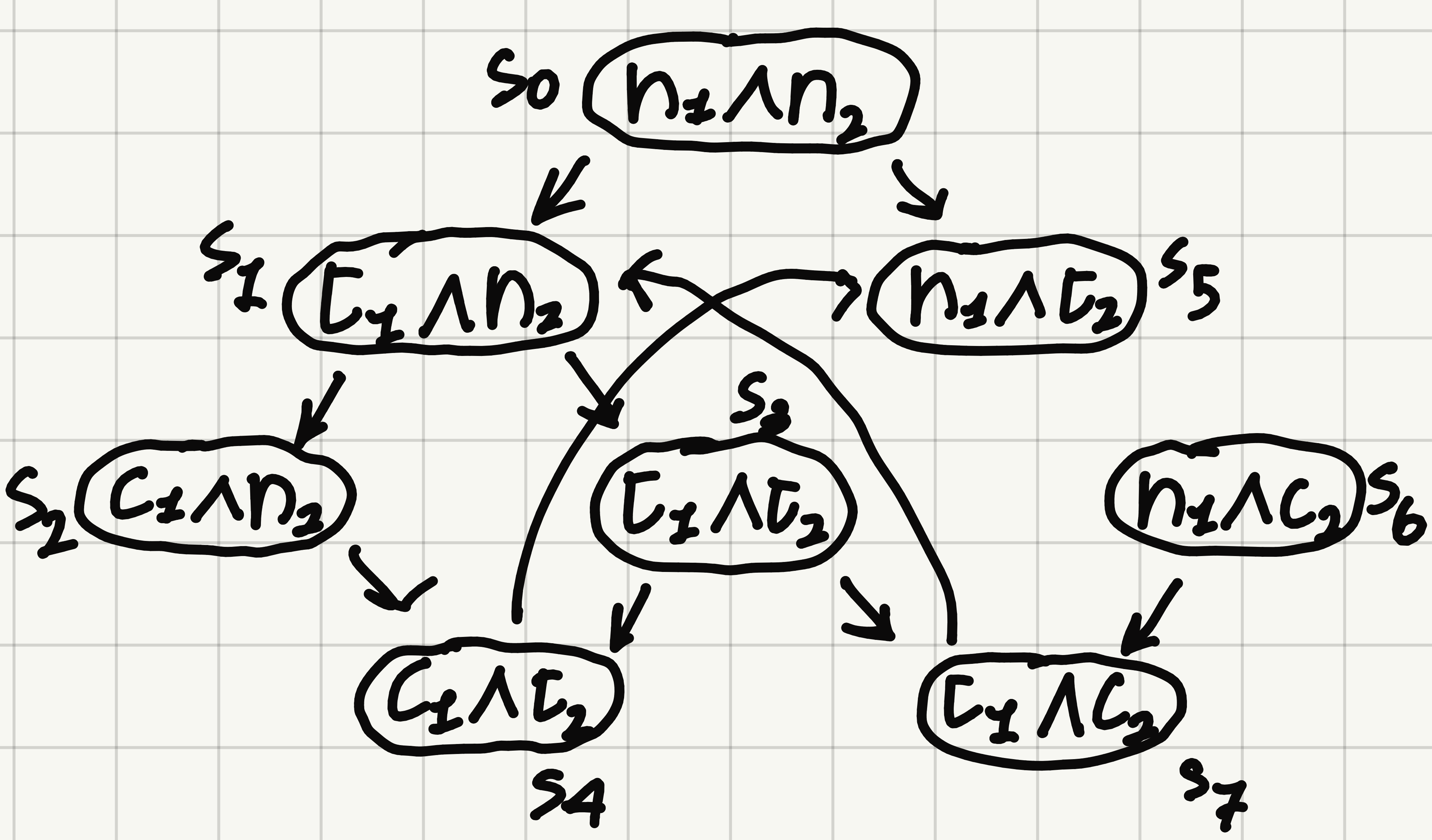
QUANDO PIÙ PROCESSI SI MUOVONO IN CONTEMPORANEA, SE CONDIVIDONO UNA RISORSA POTREBBE ESSERE NECESSARIO ASSICURARE CHE NON ACCEDANO NELLO STESSO MOMENTO ALLA RISORSA. AD ESEMPIO, NON VORREMMO CHE PIÙ DI UN PROCESSO MODIFICHI UN FILE NELLO STESSO MOMENTO. QUINDI DEFINIAMO DELLE "SEZIONI CRITICHE" PER OGNI CODICE DEL PROCESSO E LE DISPONIAMO IN MODO CHE DUE PROCESSI NON STIANO NELLA STESSA SEZIONE CRITICA CONTEMPORANEAMENTE.

QUINDI, VOGLIAMO CHE VALGA LA PROPRIETÀ DI SICUREZZA: UN PROCESSO ALLA VOLTA PUÒ STARE NELLA SEZIONE CRITICA.

ESEMPIO: ABBIAMO DUE PROCESSI. CONSIDERIAMO LE VARIABILI:

- n_1 := "IL PROCESSO 1 NON STIA IN UNO STATO CRITICO"
- n_2 := "IL PROCESSO 2 NON STIA IN UNO STATO CRITICO"
- c_1 := "IL PROCESSO 1 STIA IN UNO STATO CRITICO"
- c_2 := "IL PROCESSO 2 STIA IN UNO STATO CRITICO"
- t_1 := "IL PROCESSO 1 PROVA AD ENTRARE IN UNO STATO CRITICO"
- t_2 := "IL PROCESSO 2 PROVA AD ENTRARE IN UNO STATO CRITICO"

CONSIDERIAMO IL SEGUENTE FRAME IN CUI VALE $M \models_{s_0} \varphi_1 \wedge \varphi_2$



SICUREZZA: È ESPRIMIBILE IN LTL COME $\varphi_1 := G\neg(c_1 \wedge c_2)$ OSSIA, CONSIDERANDO LO STATO INIZIALE s_0, $M \models_{s_0} G\neg(c_1 \wedge c_2)$. UN'ALTRA CONDIZIONE DA SODDISFARE È LA VITALITÀ: OGNI VOLTA CHE UN PROCESSO CHIEDE NELLA

SUA SEZIONE CRITICA, GLI SARÀ PERMESSO IN UN CERTO MOMENTO. QUESTA CONDIZIONE È ESPRIMIBILE IN CTL COME $M \models_{s_0} (AG t_1 \Rightarrow EF c_1) \wedge \underbrace{(AG t_2 \Rightarrow EF c_2)}_{\varphi_2}$. ESISTONO ALGORITMI PER VERIFICARE LA VALIDITÀ DI TALI FORMULE IN CTL*, OSSIA VERIFICARE CHE $M \models_s \varphi_1 \wedge \varphi_2$.