Capitolo 1

Teoria

1. **Definizione FSM**:

   Una FSM è una tripla (S, I, δ), dove S è l'insieme degli stati, I l'insieme finito degli input e $\delta : S \times I \to S$ funzione di transizione

2. **Dare uno schema ASM per una FSM**:

   Una FSM può essere descritta come una FSM tramite il seguente schema: Dove:

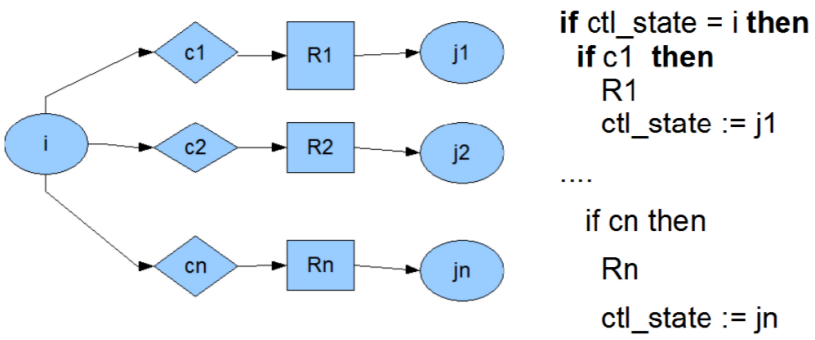


Figura 1.1: FSM in ASM

   - ctl_state: variabile che rappresenta lo stato corrente
   - R_n: azioni della macchina
   - c_n: condizioni di input
   - $i, j_1, \ldots, j_n$: stati interni di controllo, ovvero i valori assunti da ctl_state

   Le ASM sono analoghe alle FSM con differenze che riguardano gli stati, che nelle FSM è dall'unico stato ctl_state, e dalle condizioni di input e azioni di output che nelle FSM è un alfabeto finito e nelle ASM sono infinite.

3. **Stato ASM**:

   Fissato un vocabolario Σ contenente nomi di funzioni, uno stato A del vocabolario è un insieme non vuoto X, chiamato superuniverso di A, contenente

le interpretazioni dei nomi di funzioni. Se f è un nome di funzione n-aria di Σ, allora la sua interpretazione f^A è una funzione $X^n \to X$

4. **Locazione e aggiornamento ASM**:

   In ASM una locazione è definita dalla coppia $(f, (v_1, \ldots, v_n)) = loc$, dove f è il nome di funzione e gli $v_1, \ldots, v_n$ i suoi argomenti, e rappresenta l'interpretazione della funzione in un determinato stato (in memoria).

   Un aggiornamento (update) è dato da $(loc, b) = ((f, (v_1, \ldots, v_n)), b)$, ovvero l'interpretazione di f cambia attraverso la modifica dei valori $v_1, \ldots, v_n$ al valore b.

5. **Update Set e consistenza**:

   Un update set è un insieme di aggiornamenti, ognuno della forma $(loc, b) = ((f, (v_1, \ldots, v_n)), b)$

   Dato un update set U, diciamo che questo insieme di aggiornamenti è consistente quando per ogni locazione $(f, (v_1, \ldots, v_n))$, se $((f, (v_1, \ldots, v_n)), b) \in U$ e $((f, (v_1, \ldots, v_n)), c) \in U$ allora si avrà che $b = c$. Se non vale che i valori di b e c sono uguali all'ora l'update si dice inconsistente.

6. **Classificazioni funzioni**:

   Sia M una ASM e sia *env* l'ambiente di M, definiamo le funzioni in base a due principali categorie:

   - Basic
   - Derivate

   a loro volta queste due tipologie si dividono in

   - Statiche: la loro interpretazione non cambia nel corso dell'esecuzione
   - Dinamiche: I loro valori dipendono dagli stati di M. Si dividono a loro volta in
     - Monitorate (in): Scritte da env e lette ma non aggiornate da M
     - Out: Scritte da M e lette da env
     - Controllate: Scritte e lette da M
     - Condivise (Shared): Scritte e lette da M e da env

7. **Definizione ASM**:

   Una Abstract State Machine M è una terna (Σ, A, R), dove:

   - Σ: vocabolario
   - A: stato iniziale per Σ
   - R: insieme di nomi di regole, con un nome di regola di arietà zero chiamata "main rule" che rappresenta il punto di inizio per l'esecuzione della macchina

La semantica delle regole di transizione è data dall'insieme di tutti gli aggiornamenti.

8. **Non determinismo**:

   In ASM il non determinismo è implementato attraverso la choose-rule. La sintassi del costrutto è la seguente: choose x with ϕ do $R[x]$, ovvero scegli casualmente un x che soddisfa la condizione ϕ ed esegui $R[x]$.

   Un esempio:

```
choose i in {0,...,9}, j in {0,...,9} with i < j
and vect(i) > vect(j) do
swap[vect(i),vect(j)]
```

9. **Parallelismo sincrono**:

   In ASM il parallelismo sincrono è implementato attraverso la forall-rule. La sintassi del costrutto è la seguente: forall x with ϕ do $R[x]$, ovvero esegui R in parallelo per ogni x che soddisfa la condizione ϕ.

10. **Parallelismo limitato (sincrono)**:

    In ASM il parallelismo limitato è implementato attraverso la Block rule (composizione parallela). La sintassi del costrutto è la seguente: par R,S endpar, ovvero esegui R ed S in parallelo. Il parallelismo è implementato quindi sia dalla block rule che dalla forall, per la block si parla di parallelismo bounded, per la forall di parallelismo unbounded. Entrambe possono causare aggiornamenti inconsistenti.

```
signature
    [...]

definitions:
rule r_rule1 = skip
rule r_rule2 = skip

main rule r_Main
    par
        r_rule1[]
        r_rule2[]
    endpar
```

11. **Run ASM agente singolo**:

    Data una ASM M, una run (o esecuzione) è definita come una sequenza finita o infinita di stati di M $S_0, \ldots, S_n$ dove S_0 è lo stato iniziale e ciascuno S_{i+1} stato è ottenuto dal precedente S_i eseguendo simultaneamente tutte le regole di transizione che sono eseguibili in S_i

12. **Validazione e verifica sistema**:

    Validazione e verifica sono due approcci volti all'analisi di un modello. La validazione è necessaria a controllare che il sistema soddisfi i requisiti richiesti e questa attività dovrebbe essere svolta prima della verifica in modo da individuare errori e specifiche non corrette il prima possibile. La verifica, invece, è necessaria a garantire proprietà (es. safety, liveness, reachability,...). Forme di analisi sul ground model sono ad esempio le invarianti e la validazione tramite scenari.

13. **Invarianti**:

    Le invarianti in un modello ASM sono utilizzate per esprimere vincoli su funzioni e/o regole che devono essere garantiti in ogni stato. Le invarianti vanno dichiarate prima della main rule e sono dichiarate attraverso la parola chiave *invariant*

14. **ASM multiagente**:

    Le ASM multi-agent descrivono un modello distribuito di computazione attraverso l'esecuzione concorrente di Agenti sincroni o asincroni che hanno in comune stati globali condivisi. La classificazione è quindi tra

    - Sincrone: ogni agente esegue il suo programma parallelamente agli altri sulla base di un clock di sistema condiviso
    - Asincrone: ogni agente esegue il suo programma in parallelo, ma in modo indipendente tra loro. Ciascuno ha il proprio clock che regola la durata di una mossa e ciascuno opera nel proprio stato locale

15. **ASM sincrone: computazione**:

    Una ASM multi-agent con agenti sincroni ha una "quasi-sequential run", ovvero una sequenza di stati $S_0, \ldots, S_n$ dove ciascuno stato S_i è ottenuto dal precedente S_{i-1} eseguendo in parallelo le regole di tutti gli agenti

16. **ASM asincrone: computazione**:

    Una ASM multi-agent con agenti asincroni ha una "run parzialmente ordinata", ovvero un insieme parzialmente ordinato $(M, <)$ di mosse m che soddisfano le seguenti proprietà:

    (a) Storia finita: ad un certo istante t, la sequenza di mosse che ha condotto dallo stato S_0 allo stato S_t è finita, ovvero ciascuna mossa ha un numero finito di predecessori. Formalmente $\forall m \in M$ l'insieme $\{m' \mid m' < m\}$ è finito

    (b) Sequenzialità degli agenti: Ogni agente opera in modo sequenziale (le sue mosse sono sequenziali). Formalmente, dato l'agente $a \in Agent$ l'insieme di mosse $\{m \mid m \in M\}$, m eseguita da a, è linearmente ordinato per $<$

(c) Coerenza: Ogni stato di M è il risultato delle mosse di agenti. Formalmente, dato un segmento iniziale finito X, sottoinsieme chiuso a sinistra di $(M, <)$ e sia $\sigma(X)$ lo stato associato ad X, ovvero $\sigma(X)$ è il risultato di tutte le mosse di X. Ciascun segmento iniziale finito X di $(M, <)$ ha uno stato associato $\sigma(X)$ che è il risultato dell'applicazione della mossa m nello stato $\sigma(X - \{m\})$ per ogni elemento massimale $m \in X$

17. **Ground model e raffinamento**:

Il ground model è un modello utilizzato in fase di specifica dei requisiti all'interno del processo di progettazione e sviluppo. Rappresenta il primo modello corretto ma non necessariamente completo dei requisiti e che permette quindi di specificare in forma di definizione matematica ciò che il sistema deve fare. Il GM deve rispettare alcune proprietà:

- Preciso: rispetto al livello di astrazione prescelto
- Flessibile: tale da essere modificato ed esteso
- Semplice e conciso
- Astratto ma corretto rispetto ai requisiti e completo sul livello di dettaglio desiderato
- Validabile

18. **Raffinamento**:

Il raffinamento è quel processo attraverso il quale, a partire da una GM, si passa da una versione astratta ad una più raffinata e concreta. Questo processo è applicato iterativamente fino al raggiungimento del livello desiderato. Il metodo di raffinamento per le ASM non è basato su alcun principio di sostituzione, ma sulle commutazioni algebriche.

Esistono due tipologie di raffinamento:

- Orizzontale (Estensione conservativa): raffinamento incrementale utilizzato per l'introduzione di nuovi comportamenti o adattamenti a condizioni dell'ambiente
- Verticale: aumenta il dettaglio degli elementi del modello

19. **Corretto raffinamento**:

Fissata la nozione di equivalenza $\equiv$ tra gli stati di interesse e fissati gli stati iniziali e finali, una ASM Mraff è detta corretta raffinamento di M se e solo se:

$\forall$ Mraff-run raffinata $\widetilde{S}_0, \widetilde{S}_1, \ldots$, esiste una M-run $S_0, S_1, \ldots$ e sequenze $i_0 < i_1 < \ldots$ e $j_0 < j_1 < \ldots$ tali che $i_0 = j_0 = 0$ e $S_{ik} \equiv \widetilde{S}_{jk}$ per ogni k e si verifica una delle due condizioni:

- Entrambe le run terminano e gli stati finali sono l'ultima coppia di stati equivalenti; oppure

- Entrambe le run sono infinite

20. **Corretto raffinamento stuttering**:

    Fissata la nozione di equivalenza $\equiv$ tra gli stati di interesse e fissati gli stati iniziali e finali, una ASM Mraff è detta corretta raffinamento di M se e solo se:
    ogni Mraff-run raffinata $Sr_0, Sr_1, \ldots$ può essere ripartita in sotto-run $\rho_0, \rho_1, \ldots$ ed esiste una M-run $S_0, S_1, \ldots$ tale che $\forall \rho_i$ vale che $\forall Sr \in \rho_i : Sr \equiv S_i$

21. **Automa di Kripke**:

    Un modello per l'interpretazione di una formula CTL è data dall'automa di Kripke con relazione di serialità. Formalmente un automa di Kripke è definito dalla quadrupla $M = (S, \Delta, I, L)$, dove:

    - S: insieme degli stati
    - Δ (o anche $\rightarrow$): funzione di transizione, tale che $\forall s \in S \quad \exists s' \in S$ con $s \rightarrow s'$
    - I: insieme degli stati iniziali
    - L: funzione di etichettatura definita come $L : S \rightarrow 2^{PA}$, con PA insieme delle parti Si impone l'assenza di deadlock con un eventuale aggiunta di uno stato fittizio s_d

22. **Verifica di formule CTL ben formate**:

    Per verificare che una formula CTL sia ben formata è necessario costruire il relativo albero di parsing. Un albero di parsing è un albero costruito a partire da una formula CTL leggendola da sinistra a destra e associando ad ogni nodo un operatore. Gli operatori si dividono in due categorie:

    - Operatori unari: $\neg, AG, EG, AF, EF, AX, EX$
    - Operatori binari: $\wedge, \vee, \rightarrow, AU, EU$

    Vediamo il significato delle lettere:

    - A: lungo tutti i percorsi
    - E: lungo almeno un percorso
    - X: successivo
    - F: qualche stato futuro
    - G: tutti gli stati futuri (globalmente)

    A ed E danno indicazioni sui path a partire dallo stato corrente. E è il duale di A. Invece X,F,G riguardano gli stati presenti all'interno di quei path.

23. **Semantica dei connettivi CTL**:

    - $M, s \models AX\phi$ sse per ogni s_1 tale che $s \rightarrow s_1$ è vero che $M, s_1 \models \phi$. AX significa in tutti gli stati successivi (ad s)

- $M, s \models EX\phi$ sse per qualche s_1 tale che $s \to s_1$ vale che $M, s_1 \models \phi$ .EX significa in qualche stato successivo (ad s)
- $M, s \models AG\phi$: In tutti i path a partire da s vale sempre la condizione ϕ
- $M, s \models EG\phi$ sse esiste un path $s_1 \to s_2 \to \ldots$, con $s_1 = s$, in cui $\forall i, M, s_i \models \phi$. Esiste almeno un path di computazione a partire dallo stato corrente s in cui è sempre verificata la condizione ϕ (in quel path per ogni stato vale ϕ).
- $M, s \models AF\phi$ sse per tutti i path $s1 \to s_2$, con s_1 uguale ad s, esiste almeno un s_i in cui $M, s_i \models \phi$. In tutti i path a partire da s esiste almeno uno stato futuro s_i in cui la proprietà ϕ è soddisfatta
- $M, s \models EF\phi$ sse esiste un path $s_1 \to s_2 \to \ldots$, con s_1 uguale ad s, in cui $M, s_i \models \phi$. Ovvero esiste un path di computazione che inizia da s in cui esiste uno stato in cui la proprietà ϕ è soddisfatta
- $A(\phi_1 U \phi_2)$: In tutti i path vale ϕ_1 fino allo stato in cui poi vale ϕ_2
- $EU(\phi_1 U \phi_2)$: Esiste un path di computazione che inizia con s e in cui è vero $\phi_1 U \phi_2$

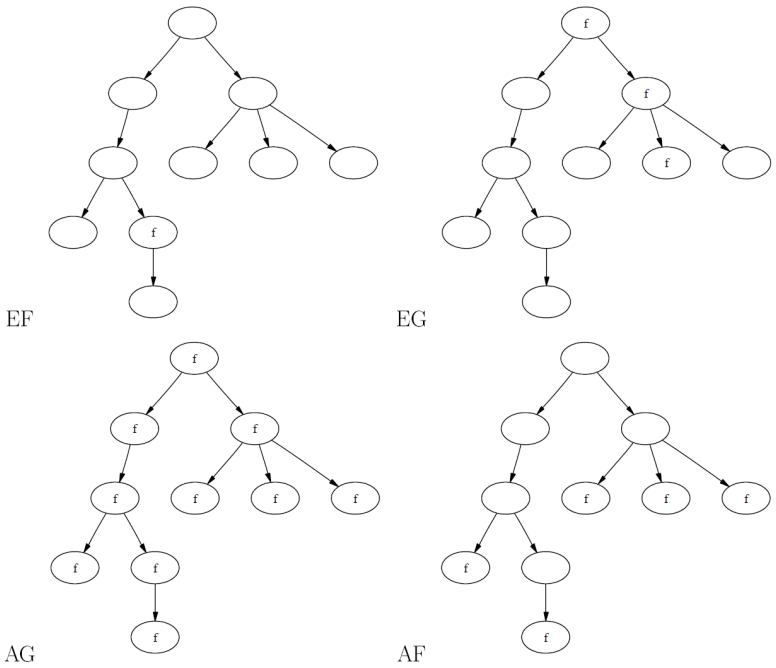


Figura 1.2: Tree CTL

24. **Equivalenza formule**

- $\neg AF\phi \leftrightarrow EG\neg\phi$
- $\neg EF\phi \leftrightarrow AG\neg\phi$
- $\neg AX\phi \leftrightarrow EX\neg\phi$
- $AF\phi \leftrightarrow A(\top\ U\ \phi)$
- $EF\phi \leftrightarrow E(\top\ U\ \phi)$

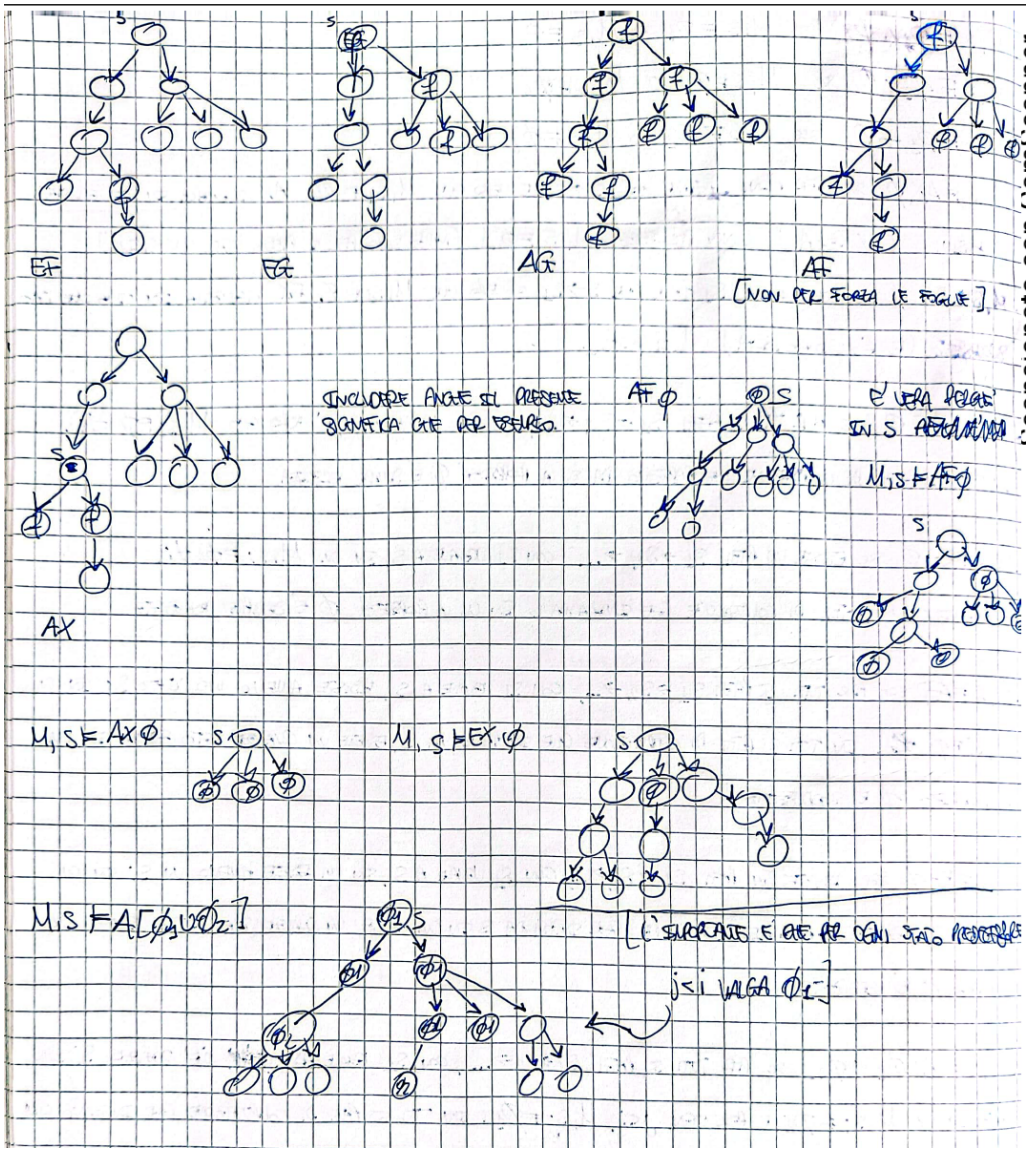


Figura 1.3: Enter Caption

Possiamo dimostrare l'equivalenza di alcune di queste formule:

Dimostrazione. $\neg AF\phi \leftrightarrow EG\neg\phi$.

Per fare ciò è necessario dimostrare le due direzioni di equivalenza.

(a) $\neg AF\phi \rightarrow EG\neg\phi$
Per ipotesi $\forall M, \forall s$ supponiamo valga $M, s \models \neg AF\phi$. Negare $AF\phi$ significa dire che esisterà un cammino in cui la *phi* non varrà mai. Ovvero $\exists$ un path $s_1 \rightarrow s_2 \rightarrow \ldots$ tale che $s_1 = s$ e $\forall i, M, s_i \models \neg\phi$. Questo per definizione equivale a dire $M, s \models EG\neg\phi$

(b) $EG\neg\phi \rightarrow \neg AF\phi$
Ragioniamo per assurdo (negando la tesi). Supponiamo che $\forall M, \forall s$. $M, s \models AF\phi$. Se ciò è vero, stando alla definizione si avrà che per ogni cammino a partire da s esisterà uno stato in cui vale ϕ. Ma questa affermazione contraddice l'ipotesi $EG\neg\phi$.

□

Dimostrazione. $\neg AX\phi \leftrightarrow EX\neg\phi$.

Per fare ciò è necessario dimostrare le due direzioni di equivalenza.

(a) $\neg AX\phi \rightarrow EX\neg\phi$
Per ipotesi $\forall M, \forall s$ supponiamo valga $M, s \models \neg AX\phi$. Negare $AX\phi$ significa dire che esisterà uno stato successivo $s', s \rightarrow s'$ in cui la ϕ non varrà. Questo per definizione equivale a dire $M, s \models EX\neg\phi$

(b) $EX\neg\phi \rightarrow \neg AX\phi$
Ragioniamo per assurdo (negando la tesi). Supponiamo che $\forall M, \forall s$. $M, s \models AX\phi$. Ovvero esiste uno stato successivo allo stato presente in cui vale ϕ. Questa affermazione contraddice l'ipotesi per cui rimuoviamo l'assurdo e affermiamo quanto detto.

□

Normalmente nella dimostrazione dell'equivalenza di due formule ci si riconduce sempre a dimostrare che la prima equivalenza è vera per definizione e la seconda (quella di negazione) va fatta per assurdo.

25. **Algoritmo di labelling**:

Quando si svolgono esercizi per il model checking bisogna ricondurre ogni formula CTL ad una ad esse equivalente contenente solamente i simboli: $\bot$, $\wedge, \neg, AF, EU, EX$. Alcune riscritture possono essere:

- $\top = \neg \bot$
- $\phi_1 \vee \phi_2 = \neg(\neg\phi_1 \wedge \neg\phi_2)$
- $\phi_1 \rightarrow \phi_2 = (\neg\phi_1 \vee \phi_2)$
- $AX(\phi) = (\neg EX\neg\phi)$

- $EF(\phi) = E(\top U \phi)$
- $EG(\phi) = (\neg AF \neg \phi)$
- $AG(\phi) = (\neg EF \neg \phi)$
- $A(\phi_1 U \phi_2) = \neg(E\,[\neg\phi_2 U(\neg\phi_1 \wedge \neg\phi_2)] \vee \neg AF\phi_2)$

Algoritmo di model checking utilizzato per verificare per quali stati vale una determinata proprietà dato un automa in figura.

26. **Model checking - SAT**:

function SAT(ϕ)
begin
case
ϕ è $\top$: **return** S
ϕ è $\bot$: **return** $\emptyset$
ϕ è un atomo : **return** $\{s \in S \mid \phi \in L(s)\}$
ϕ è $\neg\phi$: **return** $S-$SAT(ϕ)
ϕ è $\phi_1 \wedge \phi 2$: **return** SAT(ϕ_1) $\cap$ SAT(ϕ_2)
ϕ è $\phi_1 \vee \phi 2$: **return** SAT(ϕ_1) $\cup$ SAT(ϕ_2)
ϕ è $\phi_1 \rightarrow \phi 2$: **return** SAT($\neg\phi_1 \vee \phi_2$)
ϕ è AX(ϕ_1) : **return** SAT($\neg$EX$\neg\phi_1$)
ϕ è EX(ϕ_1) : **return** SAT$_{EX}(\phi_1)$
ϕ è A(ϕ_1 U ϕ_2) : **return** SAT($\neg$(E[$\neg\phi_2$ U ($\neg\phi_1 \wedge \neg\phi 2$)] $\vee$ EG$\neg\phi_2$))
ϕ è E(ϕ_1 U ϕ_2) : **return** SAT$_{EU}(\phi_1, \phi_2)$
ϕ è EF(ϕ_1) : **return** SAT(E($\top$ U ϕ_1)
ϕ è EG(ϕ_1) : **return** SAT($\neg$AF$\neg\phi_1$)
ϕ è AF(ϕ_1) : **return** SAT$_{AF}(\phi_1)$
ϕ è AG(ϕ_1) : **return** SAT($\neg$EF$\neg\phi_1$)
end case
end function

Figura 1.4: Algoritmo di SAT

27. **Model checking -** $SAT_{AF}(\phi)$:

Vengono utilizzati gli insiemi X e Y come variabili. X è inizializzato con tutti gli stati della macchina. Y viene invece inizializzato con gli stati che soddisfano il SAT di ϕ. L'algoritmo inizia e si ripete finché X e Y non saranno uguali.

Quando il repeat inizia X viene inizializzato a Y e Y è uguale a se stesso unito l'insieme degli stati che hanno *tutti* i successori aventi Y.

Alla fine viene restituito Y

function $\mathrm{SAT}_{AF}(\phi)$
local var X, Y
begin
  $X := S$;
  $Y := \mathrm{SAT}(\phi)$;
  repeat until $X = Y$
  begin
    $X := Y$;
    $Y := Y \cup \{s \mid \forall s' \text{ con } s \to s' \text{ e } s' \in Y\}$
  end
  return Y
end function

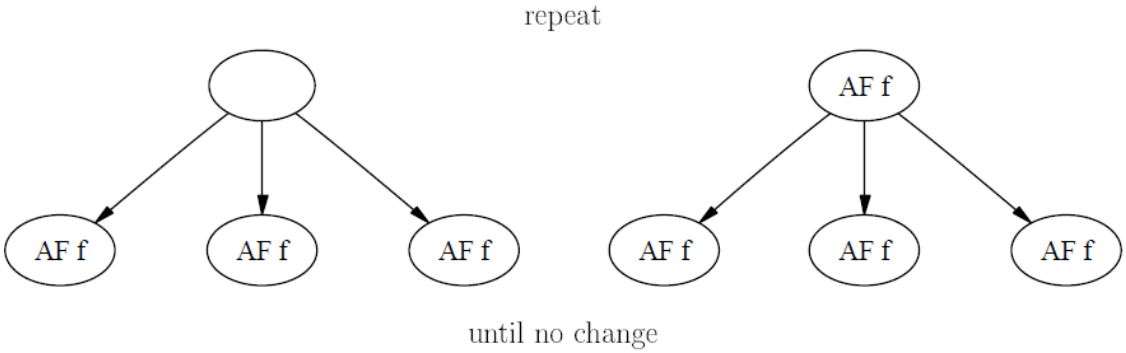


Figura 1.5: SAT AF

28. **Model checking -** $SAT_{EU}(\phi, \psi)$:

    Vengono utilizzati gli insiemi W,X ed Y come variabili. All'inizio W è inizializzato con il $SAT(\phi)$, X con l'insieme degli stati e Y con il $SAT(\psi)$.

    Quando il repeat inizia X viene inizializzato a Y e Y è uguale a se stesso unito a W intersecato con tutti gli stati che hanno come successore Y.

    Alla fine viene restituito Y

29. **Model checking -** $SAT_{EX}(\phi)$:

    Vengono utilizzati gli insiemi X e Y come variabili. X è inizializzato con gli stati che soddisfano il SAT di ϕ, Y invece con gli stati i cui successori appartengono ad X. L'algoritmo non si ripete ma ha una sola esecuzione.

    Alla fine viene restituito Y

30. **Reduced Ordered Binary Decision Diagram - ROBDD**:

    Un automa di Kripke in ROBDD viene rappresentato tramite le seguenti regole:

function $\mathrm{SAT}_{EU}(\phi, \psi)$
local var W, X, Y
begin
  $W := \mathrm{SAT}(\phi)$;
  $X := S$;
  $Y := \mathrm{SAT}(\psi)$;
  repeat until $X = Y$
  begin
    $X := Y$;
    $Y := Y \cup (\mathrm{W} \cap \{s \mid \exists s' \text{ con } s \to s' \text{ e } s' \in Y\}$
  end
  return Y
end function

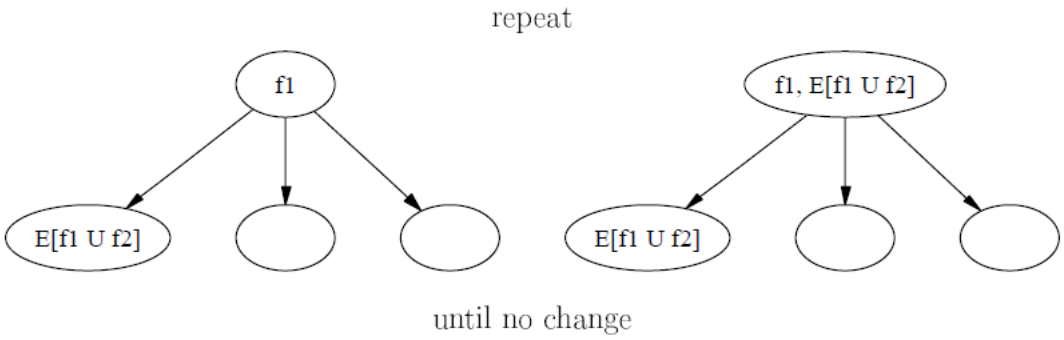


Figura 1.6: SAT EU

function $\mathrm{SAT}_{EX}(\phi)$
local var X, Y
begin
  $X := \mathrm{SAT}(\phi)$;
  $Y := \{s_0 \in S \mid s_0 \to s_1 \text{ per qualche } s_1 \in X\}$
  return Y
end function

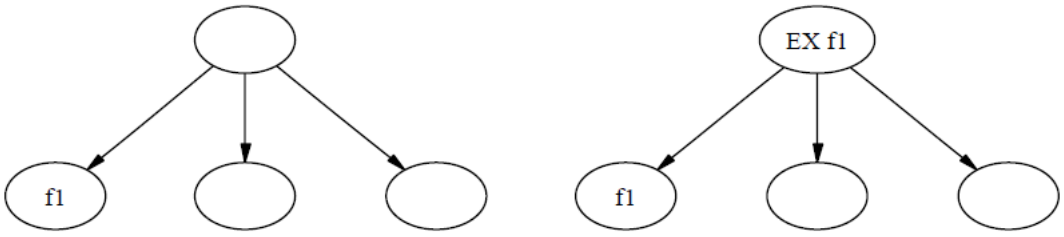


Figura 1.7: SAT EX

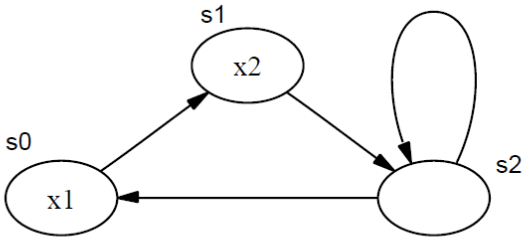
(a) Viene fissato un ordinamento sull'insieme di formule atomiche x_1, x_2, x_n (i valori presenti all'interno di ogni stato)

(b) Gli stati dell'automa vengono rappresentati in ROBDD attraverso vettori booleani. Dunque $\forall s \in S$ viene associato un vettore booleano $v_1, \ldots, v_n$ tale che $v_i = 1$ se la formula atomica vi e soddisfatta in quello stato.

(c) Ogni stato viene dunque rappresentato da un vettore $v_1, \ldots, v_n$ dove $v_i = x_i$ e $v_i = 1 \iff xi \in L(s)$ altrimenti vi $= 0$

(d) L'insieme di stati $S = s_1, s_2, s_n$ è rappresentato dalla funzione booleana data dalla congiunzione dei vettori booleani di ogni stato.

(e) Le transizioni in ROBDD di un automa di Kripke sono rappresentate da coppie di vettori boooleani in congiunzione.



Consideriamo il modello CTL dato in figura, con ordinamento [x_1,x_2]:

$$\begin{aligned} S &= \{s_0, s_1, s_2\} \\ \rightarrow &= \{(s_0, s_1), (s_1, s_2), (s_2, s_0), (s_2, s_2)\} \\ L(s_0) &= \{x_1\} \\ L(s_1) &= \{x_2\} \\ L(s_2) &= \emptyset \end{aligned}$$

set of states	boolean values	boolean function
$\emptyset$		$\bot$
$\{s_0\}$	(1,0)	$x_1 \wedge \neg x_2$
$\{s_1\}$	(0,1)	$\neg x_1 \wedge x_2$
$\{s_2\}$	(0,0)	$\neg x_1 \wedge \neg x_2$
$\{s_0, s_1\}$	(1,0),(0,1)	$x_1 \wedge \neg x_2 \vee \neg x_1 \wedge x_2$
$\{s_0, s_2\}$	(1,0),(0,0)	$x_1 \wedge \neg x_2 \vee \neg x_1 \wedge \neg x_2$
$\{s_1, s_2\}$	(0,1),(0,0)	$\neg x_1 \wedge x_2 \vee \neg x_1 \wedge \neg x_2$
$\{s_0, s_1, s_2\}$	(1,0),(0,1),(0,0)	$x_1 \wedge \neg x_2 \vee \neg x_1 \wedge x_2 \vee \neg x_1 \wedge \neg x_2$

Figura 1.8: ROBDD esercizio

g

31. **Proprietà di raggiungibilità**:

Afferma che determinate situazioni particolari possono essere raggiunte. In

CTL si esprime con $EF\phi$, ovvero esiste un cammino dallo stato corrente lungo cui un qualche stato soddisfa ϕ.

Si parla di raggiungibilità condizionata quando una condizione restringe la forma dei cammini che raggiungono lo stato desiderato. In CTL si usa il connettivo EU.

La raggiungibilità inoltre può essere inoltre applicata a stati raggiungibili. La raggiungibilità da stati raggiungibili richiede l'annidamento di EF e di AG.

32. **Proprietà di safety**

    Afferma che, sotto certe condizioni, un evento non può mai accadere (cose cattive non si verificano mai). In CTL si esprime con $AG\phi$. Ogni stato di ogni cammino dallo stato corrente soddisfa ϕ e la ϕ esprime proprio l'evento o fatto che non si deve verificare.

    La safety condizionata utilizza il connettivo AU come: $AU\,[\phi U\psi]$: ϕ non deve verificarsi finché non si verifica ψ (per esprimere ciò la ϕ va messa col $\neg$).

    Safety = not-reachability. Nella maggior parte dei casi una proprietà di safety si esprime come la negazione di una proprietà di raggiungibilità: the system can not reach a state in which: $\neg EF(...)$ (oppure $AG())$

33. **Proprietà di liveness**

    Afferma che, sotto certe condizioni, un qualche evento alla fine accadrà, ovvero cose buone prima o poi se verificano. In CTL si esprime con: $AG + AF$ oppure $AG + EF$.

34. **Assenza di deadlock**

    Afferma che il sistema non si troverà in una condizione in cui non è possibile alcun progresso (situazione di stallo). In CTL si esprime con: $AG\ EX\ true$, ovvero qualunque sia lo stato raggiunto (AG), esiste uno stato immediatamente successore ($EX\ true$)

35. **Proprietà di fairness**

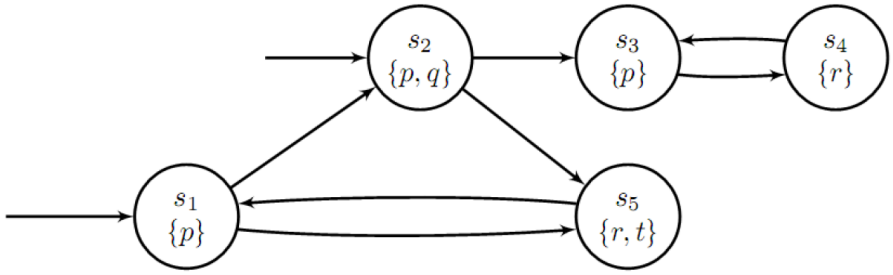
    Afferma che, sotto certe condizioni, un evento accadrà infinitamente spesso. Le proprietà di fairness non possono essere espresse in pura CTL perché manca l'operatore $F^{\propto}$, ovvero un numero infinito di volte o infinitamente spesso. In SMV le ipotesi di fairness vanno specificate come parte del modello piuttosto che ricorrere alla logica CTL+fairness.

36. **NuSMV**:

    Un programma in NuSMV è formato da un modulo main e tre parti principali:

    - VAR: parte di codice in cui vengono definite le variabili

- ASSIGN: vengono inizializzate le variabili e vengono descritte le "evolution"
- CTLSPEC: definisce le proprietà da verificare In questo modo si mappa un automa di Kripke in un modello NuSMV:




```
MODULE main
    VAR
        state: {s1, s2, s3, s4, s5};
    DEFINE
        p := state in {s1, s2, s3};
        q := state = s2;
        r := state in {s4, s5};
        t := state = s5;
```

```
ASSIGN
    init(state) := {s1, s2};
    next(state) :=
        case
            state = s1: {s2, s5};
            state = s2: {s3, s5};
            state = s3: s4;
            state = s4: s3;
            state = s5: s1;
            TRUE: state;
        esac;

CTLSPEC AF r
```

Figura 1.9: Automa di Kripke modellato in NuSMV

Capitolo 2

PRATICA

Per ogni esercizio creo un project generico che mi va a creare una cartella all'interno della mia workspace. Una volta fatto ciò vado a creare all'interno della cartella appena creata un file contenente il nome del mio esercizio con ".asm".

Cosa da fare in ordine:

1. import StandardLibrary
2. signature: dichiarazione variabili
3. definitions: definizioni variabili e funzioni
4. main rule r_Main=
5. default init s0: possibile definire un insieme di stati iniziali, solo domini concreti dinamici e solo funzioni controllate (no monitorate)

2.1 Dichiarazione dei domini

I domini rappresentano i tipi assunti dalle variabili nei normali linguaggi di programmazione.

ATTENZIONE: I NOMI DEI DOMINI INIZIANO CON LA LETTERE MAIUSCOLA PER CONVENZIONE

Attualmente i domini implementati in AsmetaL possono essere dei seguenti tipi:

- **Type-domain**: Tipi di domini
  - **basic type domains** : definiti nella standard library
    - basic domain Complex
    - basic domain Real
    - basic domain Integer
    - basic domain Natural
    - basic domain Char
    - basic domain String

    - basic domain Boolean
    - basic domain Undef
  - **enum**: enumerazione. Domini che assumono valori finiti di valori definiti da noi.

    enum domain <nomeDominio> = {VALORE1 | VALORE 2 | ...}
  - abstract: elementi di natura "astratta", non definiti se non attraverso funzioni definite su tale dominio. Agent e Reserve definiti nella standard library sono domini astratti.

    asbtract domain <nomeDominio>
  - concrete domain:

    domain <nomeDominio> subset of basicType

- **Concrete domain**: sottoinsiemi dei type domain definiti dall'utente

  [dynamic] domain D subsetof td

  dov D è il nome del dominio da dichiarare, td è il type-domain di cui D è sottoinsieme. La parola chiave dynamic è opzionale e denota che l'insieme è dinamico. Per default, un dominio è statico e va definito nella sezione definitions.

2.2 Funzioni

Le funzioni rappresentano le variabili di un normale linguaggio di programmazione

- Static: funzioni invariate durante la run
- Dynamic: aggiornate durante la run
- Monitored: modificato dall'ambiente (letto dalla macchina)
- Controlled: modificato dalle regole come azioni dell'agente
- Shared: modificato dall'ambiente e dalle regole
- Derived: definito da uno schema fisso in termini di altre funzioni (statiche o dinamiche).

2.3 Prod – Prodotto cartesiano

Prod (con la P maiuscola) rappresenta Il prodotto cartesiano dei domini d1,...,dn, cioè quell'insieme che contiene tutte le combinazioni tra gli elementi:

derived winner : Prod(Play, Play) -> Winner

Viene spesso utilizzato nelle funzioni derivate per fare dei confronti oppure per creare una matrice, ad esempio una scacchiera. Un esempio classico è quello della morra cinese, dei filosofi, o la scelta tra due giocatori che estraggono un valore e bisogna vedere chi vince.

2.4 CTL

Le CTL vanno definite all'interno della sezione **definitions:** e vanno dichiarate tramite keyword:

CTL(ctlSpecificata)

ctlSpecificata è una formula in logica CTL

Vediamo alcuni esempi per facilitare la scrittura:

- In ogni stato: ACLSPEC(ag(condizione))
- Esiste uno stato in cui vale che: ACLSPEC(ef(condizione))

2.5 AVALLA - Creazione scenari

Utilizzo per creare gli scenari per il nostro modello asm.

I file avalla hanno estensione ".avalla" e sono strutturati come segue:

1. scenario "nomeScenario"
2. load "nomeFile.asm"

Le azioni che possono essere specificate sono le seguenti:

- set funzione := valoreFunzione
- check funzione = valoreFunzione
- step -> effettua uno step della macchina

2.6 Agenti

In Asmeta il dominio di un agente va dichiarato come:

domain "nomeDominioAgente" subsetof Agent

In seguito un agente è definito statico come:

static "nomeAgente": "nomeDominioAgente"

Quando si lavora con gli agenti, cosa importante è andare a definire nello *default init s0* l'associazione tra un agente e la rule a cui esso deve riferirsi. L'associazione va fatta in questo modo:

agent "nomeDominioAgente": "nomeRule[ ]"

Questo perché poi all'interno del main, quasi sempre formato da un par in cui c'è una

forall per gli agenti, non vengono chiamate direttamente le rule ma si usa il costrutto:

program("nomeAgente)

L'agente avrà già associata la rule grazie a quanto definito nel default init. Nota che all'interno della rule nel caso bisogna riferirsi all'agent stesso si usa la parola chiave **self**

2.7 Timer

Le fasi per utilizzare dei timer all'interno di un programma Asmeta sono i seguenti:

1. import TimeLibrary
2. signature: static timer[tempo][unitàTempo]Passed: Timer

   es: static timer10MinPassed: Timer

   N.B.: I TIMER A LORO VOLTA SONO FUNZIONI CHE RESTITUISCONO INTEGER
3. default init s0: In questa sezione bisogna settare tre componenti:
   - Unità di tempo: Bisogna fissare le unità di tempo che si vuole modellare con quel Timer. Per cui per ogni timer presente nel nostro programma dovremmo andarlo a settare con un if

     function timerUnit($t in Timer) =
     if $t = timerxMinPassed then MIN
     else if $t = timerxhPassed then HOUR
     endif endif
   - Durata: La durata va settata normalmente riferendosi all'unità di misura precedentemente fissata. Per cui i numeri interi rappresentano una unità nell'unità di misura scelta per quello specifico timer. Anche in questo caso la spcecifica va effettuata con l'if nel modo seguente:

     function duration($t in Timer) =
     if $t = timerxMinPassed then x
     else if $t = timerxhPassed then x
     endif endif
   - Start (FISSO): **function start($t in Timer) = currentTime($t)**

Alcune tra le funzioni associate ai timer che possono servire all'interno degli esercizi per effettuali verifiche o controlli di vario genere:

- derived currentTime: Timer-> Integer
- derived expired: Timer -> Boolean
- macroruler_reset_timer($t inTimer)

Capitolo 3

Domande esami

Le risposte alle domande sono i numeri assegnati alle definizioni teoriche del capitolo precedente :)

3.1 Teoriche

- Dare la definizione di una locazione ASM e di aggiornamento di una locazione. Portare un esempio di aggiornamento inconsistente causato dal non determinismo di una funzione monitorata → **4**
- Descrivere come si rappresentano stati e transizioni di un Automa di Kripke in ROBDD. Dare la rappresentazione per la figura in basso e la sua implementazione in NuSVM:
- Descrivere i meccanismi in ASM che permettono di modellare il non determinismo. Portare degli esempi (almeno 1 per meccanismo) → **8**
- Dare lo schema ASM per una FSM → **2**
- Descrivere la classificazione delle funzioni in una ASM → **6**
- Dare la definizione di ASM multi-agenti e di run in caso di agenti sincroni. Portare un esempio di multi-agenti sincroni la cui computazione può causare l'inconsistenza di aggiornamento per una locazione, e portare un esempio di schedulazione degli agenti che evita tale inconsistenza → **14**
- Date la definizione di automa di Kripke → **21**
- Dare la definizione e la formula in logica temporale per esprime le proprietà di safety, liveness, e reachability
- Dare la definizione di aggiornamenti inconsistenti per un modello ASM. Portare un esempio di multi-agenti sincroni la cui computazione può causare l'inconsistenza di aggiornamento per una locazione, e portare un esempio di schedulazione degli agenti che evita tale inconsistenza → **5**
- Verificare l'equivalenza logica tra le seguenti formule $\neg AX\phi = EX\neg\phi$
- Verificare l'equivalenza logica tra le seguenti formule $\neg EF\phi = AG\neg\phi$

- Dare la sintassi e la semantica del costruttore di regola forall. Portare un semplice esempio di modello ASM che usa questo operatore
- Dare la definizione di stato ASM e di update set →**4,5**
- Descrivere come si modella l'ambiente in ASM e come questo può causare il non-determinismo del sistema. Discutere se esistono altre forme di non-determinismo interne. Per ciascuno dei concetti, portare un semplice esempio di modello ASM non-deterministico
- Dare la definizione di verifica e di validazione di un sistema. Indicare quali metodi possono essere applicati per l'espletamento delle due attività → **12**
- Dare la definizione di ground model nella modellazione ASM. Descrivere cosa vuol dire fare un passo di raffinamento del ground model →**17**
- Descrivere come si rappresentano stati e transizioni di un Automa di Kripke in ROBDD. Dare la rappresentazione per la figura in basso e la sua implementazione in NuSVM.
- Descrivere come in logica CTL si esprime una proprietà di safety→**32**
- Descrivere come in logica CTL si esprime una proprietà di raggiungibilità e di non raggiungibilità →**31**
- Descrivere come in ASM è possibile modellare sistemi paralleli
- Dare la semantica della regola ASM: R) seq T,S, endseq, con T ed S due regole ASM. Scrivere le regole per una ASM equivalente senza la seq rule R
- Descrivere come in logica CTL si esprime una proprietà di liveness→**33**
- Definire quando un modello ASM Mraff è il corretto raffinamento di un modello ASM M →**19**
- Descrivere come viene gestita la chiamata $SAT_{EF}(\phi)$ nell' algoritmo di model checking

3.2 CTL

- Se l'evento p accade, allora nel futuro gli eventi s e t accadranno simultaneamente su tutti i cammini di computazione
- Se x>y ed y viene successivamente (nel tempo) incrementato, allora prima o poi vale x>0 e y>0.
- Se l'evento p accade, allora nel futuro gli eventi s e t accadranno in almeno un cammino di computazione
- Formalizzare in logica CTL la seguente proprietà:

  - Nello stato iniziale, se un evento p accade, allora in futuro sarà probabile un evento q.
  - In una qualsiasi configurazione, se l'evento p accade, allora nel futuro l'evento q deve accadere.

- Dopo che il lucchetto è stato chiuso, il lucchetto verrà aperto solo se è nota la sua combinazione: $AG(Chiuso \rightarrow EF(aperto \rightarrow combinazione)$

- Mario è andato al cinema e poi a casa, ma nel frattempo non è mai tornato a casa: $AG(Cinema \rightarrow A(\neg casaUcasa)$

- Dopo che la casa è costruita, la casa non verrà mai distrutta finché rimane agli stessi proprietari: $AF \rightarrow A(\neg distruttaUCambioproprietari)$

- Se Giorgio studia, allora subito dopo va in palestra finché fa la doccia: $AG(s \rightarrow AX(A(palestraUdoccia)))$

- Se la porta è chiusa, si apre con 3 mandate a sinistra:
  $AG(chiusa \rightarrow EF(sinistra \rightarrow ex(sinistra \rightarrow ex(sinistra))))$

- Un montacarichi che si trova al primo piano ed è direzionato verso l'alto, non cambia la direzione di moto se chiamato al piano 7 fino a che non raggiunge tale piano.

- Un ascensore può rimanere in stato idle al piano 5 con le porte chiuse. (Nota: può rimanere, non è detto che rimanga sempre)

- Se Giorgio studia, allora subito dopo va in palestra finché fa la doccia:

3.3 Model checking - SAT

Per risolvere questi esercizi bisogna fare vari passaggi:

  - Convertire le proprietà temporali in quelli minimali secondo le regole definite dal SAT
  - FARSI CACCA ADDOSSO

- Dare la semantica in logica CTL dell'operatore $EG\phi$. Tramite l'algoritmo di model checking verificare per quali stati s vale la proprietà $M, s \models EG(r)$ nell'automa in figura 3.1

- Dare la semantica in logica CTL dell'operatore $EG\phi$. Tramite l'algoritmo di model checking verificare per quali stati s vale la proprietà $M, s \models AX(r)$ nell'automa in figura 3.1

- Dare la semantica in logica CTL dell'operatore $EG\phi$. Utilizzando l'algoritmo di SAT verificare per quali stati s vale la proprietà $M, s \models AG(p- > EF(r))$ considerando l'automa in figura 3.1

- Dare la semantica in logica CTL dell'operatore $EF\phi$ ed utilizzando l'algoritmo di SAT verificare per quali stati s vale la proprietà $M, s \models EF(AG(r))$ considerando l'automa in figura 3.2

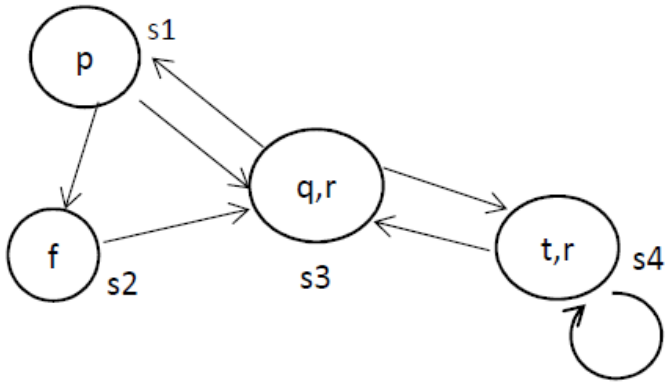


Figura 3.1: Automa n.1

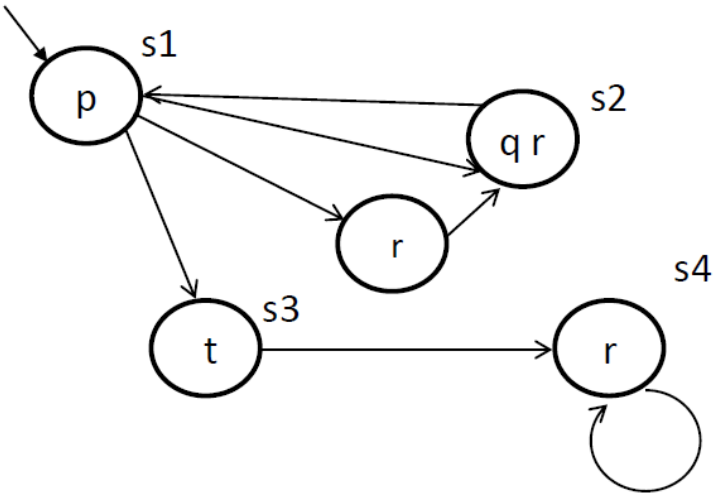


Figura 3.2: Automa n.2

3.4 Modellare

- Modellare in ASM il comportamento del seguente sistema di controllo di due semafori per la viabilità alternata. Il sistema di controllo è costituito da due semafori collegati ad un computer che, per ciascuna semaforo, ne determina lo stato VERDE, GIALLO e ROSSO. Il funzionamento dei semafori è controllato dal computer in base al seguente ciclo fisso di quattro fasi: fase1, per 30 secondi, entrambe i semafori sono in GIALLO; fase2, per 120 secondi un semaforo è in VERDE e l'altro è in ROSSO; fase3, per 30 secondi entrambi i semafori sono in GIALLO nuovamente; fase4, per 120 secondi il semaforo che prima era in VERDE passa da GIALLO a ROSSO mentre l'altro passa da GIALLO a VERDE. Ed il ciclo si ripete.

- Specificare un modello ASM multi agente (luce e controllore) per modellare il

comportamento del seguente sistema d'illuminazione dell'atrio di una casa. Se è giorno, la luce non viene accesa. Se è notte, la luce viene accesa per 10 minuti appena viene aperto il cancello di casa. In presenza di malfunzionamento, il sistema va in stato di errore.

- Specificare un modello ASM per il funzionamento di apertura e chiusura delle porte di una metropolitana. La porta è controllata via software da un controllore: all'arrivo del treno (segnalato dal sensore arrivo) il controller apre le porte della metro e le richiude dopo 1 minuto dall'apertura completa. Le porte seguono il ciclo: chiuse, inApertura, aperte e inChiusura. Se la porta è inChiusura e un passeggero entra in metro (segnalato dal sensore passaPersona), il controller riapre le porte (la politica di chiusura è la stessa).

  - Specificare una proprietà di raggiungibilità, una di safety del sistema ed una di liveness relative al modello al punto precedente.
  - Descrivere con in logica temporale di esprime una proprietà di raggiungibilità condizionata. Portare un esempio relativo al modello precedente.