Specifica formale

La correttezza di un programma è **relativa a una determinata specifica**: la verifica formale è connessa alle specifiche

Linguaggi di specifica

- Automi
- LTL (Linear Temporal Logic): una specifica LTL si può tradurre in un automa
- CTL (Computational Tree Logic)

Logica Temporale Lineare (LTL)

Logica temporale e verifica di proprietà dei programmi
(dispense)

http://cialdea.dia.uniroma3.it/teaching/logica/materiale/dispense-LTL.pdf

La logica classica è statica: rappresenta stati.

Logiche Modali: descrivono relazioni tra stati.

Una logica modale estende la logica classica mediante:

- uno o più operatori modali (sintassi)
- assunzioni sulle proprietà degli operatori modali (semantica e apparato deduttivo)

Operatori modali

Modalità: in che modo una proposizione è vera?

È vera solo **contingentemente**, è **necessariamente** vera, è **possibile** che sia vera? Modalità **aletiche:**

- contingenza: *piove*
- necessità: $\Box$*piove*
- possibilità: $\Diamond$*piove*

Contingenza, necessità, possibilità sono concetti **intensionali** (non vero-funzionali):

$$\Box(piove \vee \neg piove)$$

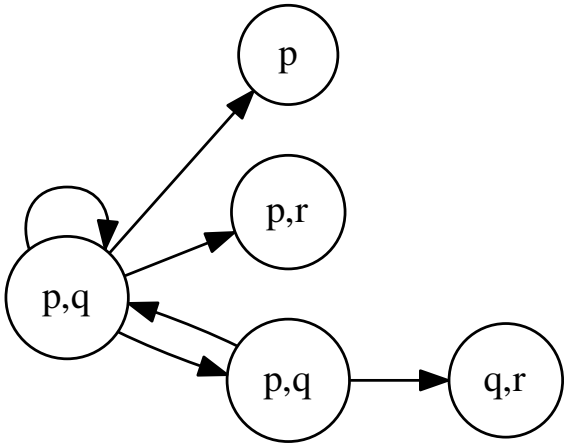
Ma, anche se $\neg$*piove* è vero, non è vero $\Box\neg$*piove*

Quali sono le proprietà di $\Box$ e $\Diamond$?

$$\Box(p \wedge q) \rightarrow \Box p \wedge \Box q?$$
$$\Box p \rightarrow p?$$
$$\Box p \rightarrow \Box\Box p?$$

(Necessità logica, necessità fisica,...)

Semantica dei “mondi possibili” (semantica di Kripke)



$\Box p$: in tutti i mondi visibili è vero p

$\Diamond \neg r$: esiste un mondo visibile in cui r è falso

$\Diamond \Box r$: esiste un mondo visibile tale che in tutti i mondi per esso visibili è vero r

$\Box A$ vero in un mondo w sse $\forall w'$ (se w vede w' allora A vero in w')

$\Box$ ha un significato “universale”

$\Diamond A$ vero in un mondo w sse $\exists w'$ tale che (w vede w' e A vero in w')

$\Diamond$ ha un significato “esistenziale”

Semantica degli operatori modali

Secondo la semantica di Kripke, alcune proprietà degli operatori modali valgono sempre:

$$\Diamond A \equiv \neg\Box\neg A$$
$$\Box(A \wedge B) \rightarrow \Box A \wedge \Box B$$
$$\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$$
$\Box A$ se A è classicamente valida

Altre proprietà dipendono dall'interpretazione degli operatori. Ad esempio:

Interpretazione epistemica

$\Box p$: l'agente conosce p ($K\,p$)

$\Diamond p$: p è compatibile con le conoscenze dell'agente (l'agente non conosce la negazione di p: $\neg K \neg p$)

Insieme dei mondi "accessibili": stati di cose compatibili con quello che l'agente conosce.

Conoscenza = opinione vera: $\Box p \rightarrow p$

Capacità introspettiva dell'agente: $\Box p \rightarrow \Box\Box p$ (so di sapere)
$\Diamond p \rightarrow \Box\Diamond p$ (so di non sapere)

Interpretazione temporale

Logica temporale **lineare**: il tempo è una sequenza lineare di stati: la relazione di "accessibilità" è transitiva e connessa ($\forall s, t(sRt \vee s = t \vee tRs)$), cioè è un ordine lineare

L'insieme degli stati è isomorfo a $\mathbb{N}$

$\Box$: always	$\Box p$:	p sarà sempre vero
$\Diamond$: eventually	$\Diamond p$:	p sarà vero almeno una volta in futuro

Quindi:

$\Box p \to \Diamond p$	perché il tempo è infinito nel futuro
$\Box p \to \Box\Box p$	perché il futuro è transitivo: se p sarà sempre vero, allora sarà sempre vero che sarà sempre vero

Ma non sempre, ad esempio:

$$\Diamond p \to \Box\Diamond p$$

Operatori temporali del futuro

(dove il futuro include il presente)

Oltre a $\Box$ e $\Diamond$:

Always $\Box A$: A sarà sempre vero nel futuro (stato attuale incluso)

Eventually $\Diamond A$: A sarà vero in qualche stato futuro (oppure nello stato attuale)

La struttura lineare della sequenza di stati consente di introdurre altri operatori:

Next $\bigcirc A$: A è vero nello stato successivo a quello attuale

Until $A \mathcal{U} B$: B sarà vero in futuro e A vale da adesso al momento in cui sarà vero B (escludendo tale stato)

Release $A \mathcal{R} B$: il "duale" di $\mathcal{U}$, $A \mathcal{R} B \leftrightarrow \neg(\neg A \mathcal{U} \neg B)$

(D'ora in poi Until e Release ve li risparmio!)

Esempi

$\Box\Diamond A$:

Operatori temporali del futuro

(dove il futuro include il presente)

Oltre a $\Box$ e $\Diamond$:

Always $\Box A$: A sarà sempre vero nel futuro (stato attuale incluso)

Eventually $\Diamond A$: A sarà vero in qualche stato futuro (oppure nello stato attuale)

La struttura lineare della sequenza di stati consente di introdurre altri operatori:

Next $\bigcirc A$: A è vero nello stato successivo a quello attuale

Until $A \mathcal{U} B$: B sarà vero in futuro e A vale da adesso al momento in cui sarà vero B (escludendo tale stato)

Release $A \mathcal{R} B$: il "duale" di $\mathcal{U}$, $A \mathcal{R} B \leftrightarrow \neg(\neg A \mathcal{U} \neg B)$

(D'ora in poi Until e Release ve li risparmio!)

Esempi

$\Box\Diamond A$: A vale infinitamente spesso

$\Diamond\Box A$:

Operatori temporali del futuro

(dove il futuro include il presente)

Oltre a $\Box$ e $\Diamond$:

Always $\Box A$: A sarà sempre vero nel futuro (stato attuale incluso)

Eventually $\Diamond A$: A sarà vero in qualche stato futuro (oppure nello stato attuale)

La struttura lineare della sequenza di stati consente di introdurre altri operatori:

Next $\bigcirc A$: A è vero nello stato successivo a quello attuale

Until $A \mathcal{U} B$: B sarà vero in futuro e A vale da adesso al momento in cui sarà vero B (escludendo tale stato)

Release $A \mathcal{R} B$: il "duale" di $\mathcal{U}$, $A \mathcal{R} B \leftrightarrow \neg(\neg A \mathcal{U} \neg B)$

(D'ora in poi Until e Release ve li risparmio!)

Esempi

$\Box\Diamond A$: A vale infinitamente spesso

$\Diamond\Box A$: da un certo punto in poi, A sarà sempre vera

LTL proposizionale: sintassi

Dato un insieme P di lettere proposizionali:

1. $\top$ e $\bot$ sono formule;
2. se $p \in P$ allora p è una formula;
3. se A è una formula allora $\neg A$, $\Box A$, $\Diamond A$, $\bigcirc A$ sono formule;
4. se A e B sono formule, allora $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \,\mathcal{U}\, B$, $A \,\mathcal{R}\, B$ sono formule.

Nota: in alcuni testi (tra cui quello di Katoen) gli operatori $\bigcirc$, $\Box$ e $\Diamond$ vengono denotati, rispettivamente, da ***X***, ***G*** e ***F***.

LTL: semantica

Interpretazione: sequenza infinita di interpretazioni classiche (stati).

Rappresentiamo un'interpretazione proposizionale classica mediante un insieme di atomi: l'insieme degli atomi veri nell'interpretazione.

Se $\mathbb{N}$ è l'insieme dei numeri naturali, ordinati secondo l'abituale relazione $<$, allora:

Un'interpretazione temporale $\mathcal{M}$ del linguaggio P è una funzione che associa a ogni $k \in \mathbb{N}$ un sottoinsieme di P:

$$\mathcal{M} : \mathbb{N} \rightarrow 2^P$$

Ogni $k \in \mathbb{N}$ rappresenta uno **stato**. 0 è lo stato iniziale.

Verità di un formula **in uno stato** di un'interpretazione $\mathcal{M}$:

$$\mathcal{M}_k \models A$$

Verità di un formula in un'interpretazione:

$$\mathcal{M} \models A \text{ sse } \mathcal{M}_0 \models A$$

LTL: Semantica (II)

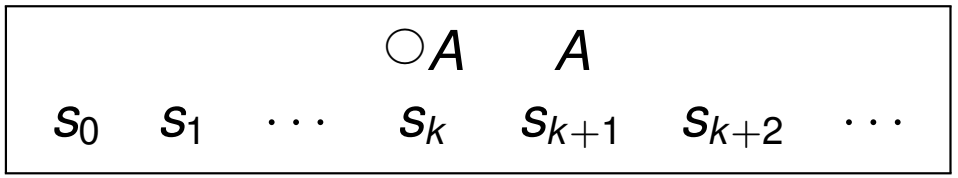
- $\mathcal{M}_k \models \top$ e $\mathcal{M}_k \not\models \bot$;
- $\mathcal{M}_k \models p$ sse $p \in \mathcal{M}(k)$;
- $\mathcal{M}_k \models \neg A$ sse $\mathcal{M}_k \not\models A$;
- $\mathcal{M}_k \models A \wedge B$ sse $\mathcal{M}_k \models A$ e $\mathcal{M}_k \models B$;
- $\mathcal{M}_k \models A \vee B$ sse $\mathcal{M}_k \models A$ oppure $\mathcal{M}_k \models B$;
- $\mathcal{M}_k \models A \rightarrow B$ sse $\mathcal{M}_k \not\models A$ oppure $\mathcal{M}_k \models B$;

  Quindi se A è una formula proposizionale classica,

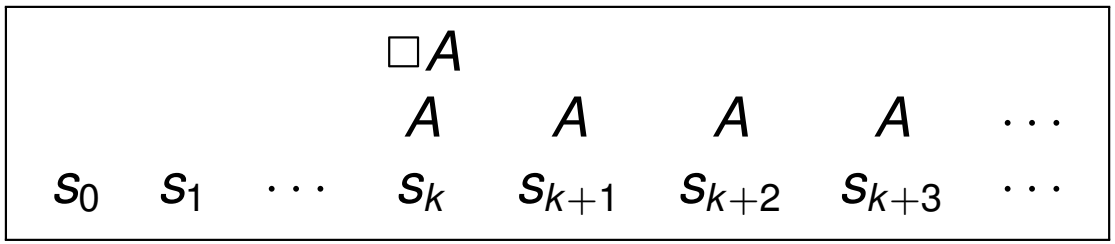
$$\mathcal{M}_k \models A \textbf{ se e solo se } \mathcal{M}(k) \models A$$

LTL: Semantica (III)

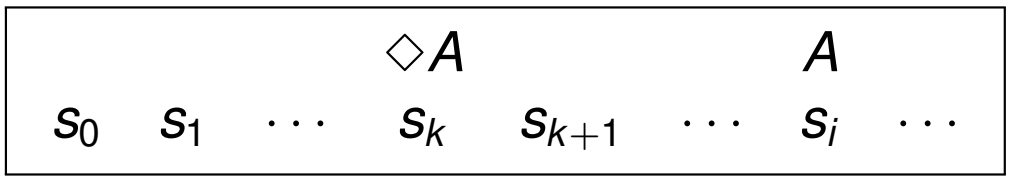
- $\mathcal{M}_k \models \bigcirc A$ sse $\mathcal{M}_{k+1} \models A$



- $\mathcal{M}_k \models \Box A$ sse per ogni $i \geq k$ $\mathcal{M}_i \models A$



- $\mathcal{M}_k \models \Diamond A$ sse esiste $i \geq k$ tale che $\mathcal{M}_i \models A$



Verità e validità

Una formula A è **vera** in un'interpretazione $\mathcal{M}$ (e $\mathcal{M}$ è un **modello** di A) sse A è vera nel suo stato iniziale:

$$\mathcal{M} \models A \text{ sse } \mathcal{M}_0 \models A$$

Se S è un insieme di formule e $\mathcal{M}$ un'interpretazione:

- $\mathcal{M}_k \models S$ sse $\mathcal{M}_k \models A$ per ogni formula $A \in S$;
- $\mathcal{M}$ è un modello di S ($\mathcal{M} \models S$) sse $\mathcal{M} \models A$ per ogni formula $A \in S$.

Una formula A è **valida** ($\models A$) sse per ogni interpretazione $\mathcal{M}$ e ogni $k \in \mathbb{N}$, $\mathcal{M}_k \models A$.

Proprietà della validità: una formula A è valida sse per ogni interpretazione $\mathcal{M}$, $\mathcal{M}_0 \models A$.

(la verità in ogni interpretazione e la verità in ogni stato di ogni interpretazione coincidono)

Conseguenza logica, equivalenza logica e falsità di una formula in uno stato

Se S è un insieme di formule e A una formula, A è una **conseguenza logica** di S (e S **implica logicamente** A)

$$S \models A$$

sse per ogni interpretazione $\mathcal{M}$ e $k \in \mathbb{N}$:

$$\text{se } \mathcal{M}_k \models S \text{ allora } \mathcal{M}_k \models A.$$

Due formule A e B sono **logicamente equivalenti** ($A \leftrightarrow B$) se per ogni interpretazione $\mathcal{M}$ e stato $k \in \mathbb{N}$, $\mathcal{M}_k \models A$ se e solo se $\mathcal{M}_k \models B$.

Quando una formula è falsa in uno stato?

- $\mathcal{M}_k \not\models \bigcirc A$ sse $\mathcal{M}_{k+1} \not\models A$
- $\mathcal{M}_k \not\models \Box A$ sse esiste $i \geq k$ tale che $\mathcal{M}_i \not\models A$
- $\mathcal{M}_k \not\models \Diamond A$ sse per ogni $i \geq k$, $\mathcal{M}_i \not\models A$

Proprietà degli operatori temporali

$\Diamond$ e $\Box$ sono duali:

$$\Box A \leftrightarrow \neg\Diamond\neg A$$
$$\Diamond A \leftrightarrow \neg\Box\neg A$$

Il Next ($\bigcirc$) è duale di se stesso

$$\bigcirc A \leftrightarrow \neg\bigcirc\neg A$$

Poiché $\leq$ è riflessiva e transitiva:

$$\models \Box A \rightarrow A$$
$$\models A \rightarrow \Diamond A$$
$$\models \Box A \rightarrow \Box\Box A$$

Proprietà del Next

$$\models \Box A \rightarrow \bigcirc A$$
$$\models \bigcirc A \rightarrow \Diamond A$$
$$\neg\bigcirc A \leftrightarrow \bigcirc\neg A$$
$$\models \bigcirc(A \rightarrow B) \rightarrow (\bigcirc A \rightarrow \bigcirc B)$$

Proprietà di Always:

$$\models \Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$$
$$\models A \wedge \Box(A \rightarrow \bigcirc A) \rightarrow \Box A$$
$$\Box \mathbf{A} \leftrightarrow \mathbf{A} \wedge \bigcirc\Box \mathbf{A}$$

Proprietà di Eventually:

$$\Diamond \mathbf{A} \leftrightarrow \mathbf{A} \vee \bigcirc\Diamond \mathbf{A}$$

Esempio di dimostrazione semantica

$$\Box A \models A \wedge \bigcirc \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, se $\mathcal{M}_k \models \Box A$ allora $\mathcal{M}_k \models A \wedge \bigcirc \Box A$

Assumiamo **per assurdo** che esistano $\mathcal{M}$ e k tali che:

- $\mathcal{M}_k \models \Box A$, cioè
  - **1)** per ogni $j \geq k$: $\mathcal{M}_j \models A$
- $\mathcal{M}_k \not\models A \wedge \bigcirc \Box A$. I casi sono due:
  - **2a)** o $\mathcal{M}_k \not\models A$
  - **2b)** oppure $\mathcal{M}_k \not\models \bigcirc \Box A$

$\Longrightarrow$

Esempio di dimostrazione semantica

$$\Box A \models A \wedge \bigcirc \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, se $\mathcal{M}_k \models \Box A$ allora $\mathcal{M}_k \models A \wedge \bigcirc \Box A$

Assumiamo **per assurdo** che esistano $\mathcal{M}$ e k tali che:

- $\mathcal{M}_k \models \Box A$, cioè
  - **1)** per ogni $j \geq k$: $\mathcal{M}_j \models A$
- $\mathcal{M}_k \not\models A \wedge \bigcirc \Box A$. I casi sono due:
  - **2a)** o $\mathcal{M}_k \not\models A$
  - **2b)** oppure $\mathcal{M}_k \not\models \bigcirc \Box A$
    $\Longrightarrow \mathcal{M}_{k+1} \not\models \Box A$
    $\Longrightarrow$

Esempio di dimostrazione semantica

$$\Box A \models A \wedge \bigcirc \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, se $\mathcal{M}_k \models \Box A$ allora $\mathcal{M}_k \models A \wedge \bigcirc \Box A$

Assumiamo **per assurdo** che esistano $\mathcal{M}$ e k tali che:

- $\mathcal{M}_k \models \Box A$, cioè
  - **1)** per ogni $j \geq k$: $\mathcal{M}_j \models A$
- $\mathcal{M}_k \not\models A \wedge \bigcirc \Box A$. I casi sono due:
  - **2a)** o $\mathcal{M}_k \not\models A$
  - **2b)** oppure $\mathcal{M}_k \not\models \bigcirc \Box A$
    $\Longrightarrow \mathcal{M}_{k+1} \not\models \Box A$
    $\Longrightarrow$ esiste $n \geq k+1$: $\mathcal{M}_n \not\models A$
    $\Longrightarrow$ esiste $n > k$: $\mathcal{M}_n \not\models A$

Il caso 2a è assurdo perché

Esempio di dimostrazione semantica

$$\Box A \models A \wedge \bigcirc \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, se $\mathcal{M}_k \models \Box A$ allora $\mathcal{M}_k \models A \wedge \bigcirc \Box A$

Assumiamo **per assurdo** che esistano $\mathcal{M}$ e k tali che:

- $\mathcal{M}_k \models \Box A$, cioè
  - **1)** per ogni $j \geq k$: $\mathcal{M}_j \models A$
- $\mathcal{M}_k \not\models A \wedge \bigcirc \Box A$. I casi sono due:
  - **2a)** o $\mathcal{M}_k \not\models A$
  - **2b)** oppure $\mathcal{M}_k \not\models \bigcirc \Box A$
    $\Longrightarrow \mathcal{M}_{k+1} \not\models \Box A$
    $\Longrightarrow$ esiste $n \geq k+1$: $\mathcal{M}_n \not\models A$
    $\Longrightarrow$ esiste $n > k$: $\mathcal{M}_n \not\models A$

Il caso 2a è assurdo perché 1 implica $\mathcal{M}_k \models A$ $(k \geq k)$.

Anche il caso 2b è assurdo perché

Esempio di dimostrazione semantica

$$\Box A \models A \wedge \bigcirc \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, se $\mathcal{M}_k \models \Box A$ allora $\mathcal{M}_k \models A \wedge \bigcirc \Box A$

Assumiamo **per assurdo** che esistano $\mathcal{M}$ e k tali che:

- $\mathcal{M}_k \models \Box A$, cioè
  - **1)** per ogni $j \geq k$: $\mathcal{M}_j \models A$
- $\mathcal{M}_k \not\models A \wedge \bigcirc \Box A$. I casi sono due:
  - **2a)** o $\mathcal{M}_k \not\models A$
  - **2b)** oppure $\mathcal{M}_k \not\models \bigcirc \Box A$
    $\Longrightarrow \mathcal{M}_{k+1} \not\models \Box A$
    $\Longrightarrow$ esiste $n \geq k+1$: $\mathcal{M}_n \not\models A$
    $\Longrightarrow$ esiste $n > k$: $\mathcal{M}_n \not\models A$

Il caso 2a è assurdo perché 1 implica $\mathcal{M}_k \models A$ ($k \geq k$).

Anche il caso 2b è assurdo perché se $n > k$, allora $n \geq k$ e 1 implica che $\mathcal{M}_n \models A$.

Quindi l'ipotesi che esistano $\mathcal{M}$ e k tali che $\mathcal{M}_k \models \Box A$ è assurda: la tesi è dimostrata.

Esempio 2: l'assioma di induzione

$$A \wedge \Box(A \rightarrow \bigcirc A) \rightarrow \Box A$$

Tesi: per ogni $\mathcal{M}$ e k, $\mathcal{M}_k \models A \wedge \Box(A \rightarrow \bigcirc A) \rightarrow \Box A$, cioè:
o $\mathcal{M}_k \not\models A \wedge \Box(A \rightarrow \bigcirc A)$ oppure $\mathcal{M}_k \models \Box A$

Siano $\mathcal{M}$ e k qualsiasi, tali che: $\mathcal{M}_k \models A \wedge \Box(A \rightarrow \bigcirc A)$, cioè

1a) $\mathcal{M}_k \models A$ e

1b) $\mathcal{M}_k \models \Box(A \rightarrow \bigcirc A)$, cioè per ogni $j \geq k$, o $\mathcal{M}_j \not\models A$ oppure $\mathcal{M}_{j+1} \models A$.

Dimostriamo che $\mathcal{M}_k \models \Box A$, cioè che per ogni $n \geq k$: $\mathcal{M}_n \models A$.

Sia n qualsiasi tale che $n \geq k$, cioè per qualche $h \in \mathbb{N}$, $n = k + h$.

Dimostriamo che $\mathcal{M}_n \models A$ **per induzione su *h***.

- Caso base: $h = 0$, quindi $n = k$. $\mathcal{M}_n \models A$ vale per 1a.
- Passo induttivo: $h > 0$. Assumiamo che $\mathcal{M}_{k+(h-1)} \models A$ (ipotesi induttiva) e dimostriamo che $\mathcal{M}_{k+h} \models A$.
  Se $h > 0$, allora $k + h - 1 \geq k$, quindi, per 1b, $\mathcal{M}_{k+h-1} \not\models A$ oppure $\mathcal{M}_{k+h-1+1} \models A$.

  Per l'ipotesi induttiva $\mathcal{M}_{k+h-1} \models A$, quindi $\mathcal{M}_{k+h} \models A$, cioè $\mathcal{M}_n \models A$.

Di conseguenza, per ogni $n \geq k$, $\mathcal{M}_n \models A \Longrightarrow \mathcal{M}_k \models \Box A$.

Esempio 3

Come dimostrare che una relazione di conseguenza logica **non** vale.

$$\Diamond A \not\models \Box\Diamond A$$

(dove A è una formula qualsiasi).

Tesi: esistono una formula A, un'interpretazione $\mathcal{M}$ e $k \in \mathbb{N}$ tali che $\mathcal{M}_k \models \Diamond A$ ma $\mathcal{M}_k \not\models \Box\Diamond A$.

Siano $A = p$ e $\mathcal{M}$ tale che: $\mathcal{M}(0) = \{p\}$ e $\mathcal{M}(i) = \emptyset$ per ogni $i > 0$.

Dimostriamo che:

- $\mathcal{M}_0 \models \Diamond p$
  $\iff$ esiste $i \geq 0$ tale che $\mathcal{M}_i \models p$.
  Poiché $\mathcal{M}(0) = \{p\}$, $\mathcal{M}_0 \models p$, quindi, per $i = 0$, $\mathcal{M}_i \models p$.
- $\mathcal{M}_0 \not\models \Box\Diamond p$
  $\iff$ esiste $i \geq 0$ tale che $\mathcal{M}_i \not\models \Diamond p$
  $\iff$ esiste $i \geq 0$ tale che, per ogni $j \geq i$, $\mathcal{M}_j \not\models p$.
  Per ogni $i > 0$, $\mathcal{M}(i) = \emptyset \implies$ per ogni $i > 0$, $\mathcal{M}_i \not\models p$.
  Prendendo $i = 1$ si ha dunque che per ogni $j \geq i$, $\mathcal{M}_j \not\models p$.

Esercizi

Dare dimostrazioni semantiche di delle altre proprietà riportate nella slide 14.

Dimostrare inoltre che:

1. $\models \Diamond \top$
2. $\models \Box \top$
3. $\not\models \Box A \vee \Box \neg A$
4. $\Diamond(A \vee B) \leftrightarrow \Diamond A \vee \Diamond B$
5. $\Diamond A \wedge \Diamond B \not\models \Diamond(A \wedge B)$
6. $\Diamond(A \wedge B) \models \Diamond A \wedge \Diamond B$
7. $\Box(A \wedge B) \leftrightarrow \Box A \wedge \Box B$
8. $\Box(A \vee B) \not\models \Box A \vee \Box B$
9. $\Box A \vee \Box B \models \Box(A \vee B)$

Sistemi assiomatici per LTL

Assiomatizzazione di LTL (proposizionale, senza $\mathcal{U}$).

A un qualsiasi sistema di assiomi per la logica proposizionale classica si aggiungono gli assiomi seguenti:

- A1. $\neg\Diamond A \equiv \Box\neg A$
- A2. $\Box(A\rightarrow B)\rightarrow(\Box A\rightarrow\Box B)$
- A3. $\Box A\rightarrow(A\wedge\bigcirc\Box A)$
- A4. $\bigcirc\neg A\equiv\neg\bigcirc A$
- A5. $\bigcirc(A\rightarrow B)\rightarrow(\bigcirc A\rightarrow\bigcirc B)$
- A6. $\Box(A\rightarrow\bigcirc A)\rightarrow(A\rightarrow\Box A)$

e la regola di inferenza (*regola di necessitazione*):

$$\frac{A}{\Box A}$$

LTL con quantificatori: indecidibile (ovviamente) e non semi-decidibile.

Verifica di sistemi con LTL: approcci basati sulla deduzione

Il comportamento del sistema $\mathcal{S}$ è descritto da un insieme S di formule di LTL e la proprietà da verificare da una formula F:

$$\mathcal{S} \text{ soddisfa la specifica } F \text{ se e solo se } S \models F$$

Verifica di sistemi con LTL: approcci basati sul “model checking” (o “model based”)

Il sistema è modellato da una struttura di Kripke $\mathcal{S}$ (un grafo con stati iniziali, ai cui stati sono associate interpretazioni proposizionali).

- ogni cammino massimale in $\mathcal{S}$ è un’interpretazione temporale
- ogni esecuzione del sistema corrisponde a un cammino massimale in $\mathcal{S}$
- il sistema è modellato dall’insieme delle sue esecuzioni (anziché da un insieme di formule, da un insieme di interpretazioni)

Identifichiamo il modello $\mathcal{S}$ del sistema con l’insieme delle sue esecuzioni (i cammini massimali in $\mathcal{S}$), diciamo che:

$\mathcal{S} \models A$: tutte le esecuzioni di $\mathcal{S}$ soddisfano A,
cioè $\mathcal{M} \models A$ per ogni $\mathcal{M} \in \mathcal{S}$

$\mathcal{S} \not\models A$: non tutte le esecuzioni di $\mathcal{S}$ soddisfano A,
cioè esiste $\mathcal{M} \in \mathcal{S}$ tale che $\mathcal{M} \not\models A$

Quindi

il sistema soddisfa la specifica F se e solo se $\mathcal{S} \models F$

Sistemi modellati da automi con vincoli di fairness

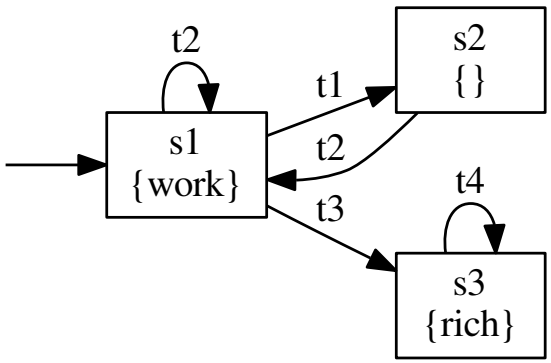
I vincoli di fairness semplici si possono esprimere mediante formule della forma $\Box\Diamond F$.

Assumiamo che il sistema sia modellato da una struttura di Kripke $\mathcal{S}$ con vincoli di fairness $\{F_1, ..., F_n\}$ (dove le F_i sono formule).

Allora le esecuzioni del sistema sono rappresentate da tutte e solo le interpretazioni $\mathcal{M} \in \mathcal{S}$ tali che $\mathcal{M} \models \Box\Diamond F_i$ per ogni $i = 1, ..., n$:

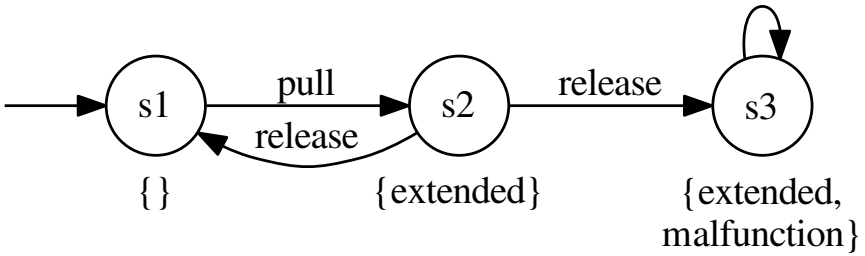
F_i si verifica infinitamente spesso

In alcuni casi, comunque, i vincoli di fairness si possono esprimere mediante formule più semplici.



Vincolo di fairness $F = \{s3\} \Longrightarrow \Diamond rich$

Specifica delle proprietà di un sistema, esempio 1: l'elastico

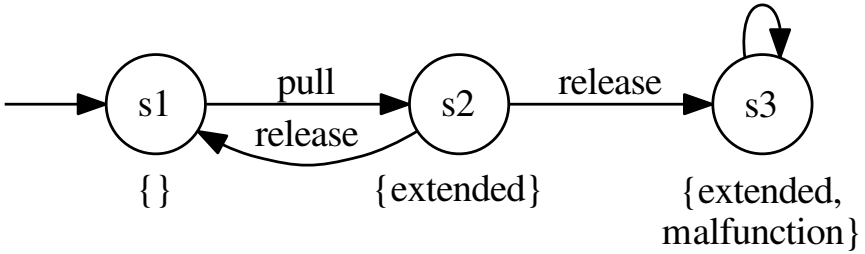


Questo sistema ha infinite esecuzioni: tutte le sequenze infinite della forma $s_1 s_2 (s_1 s_2)^* s_3^\omega$, oltre all'esecuzione $(s_1 s_2)^\omega$.

Sia $\mathcal{M} = s_1 s_2 s_1 s_2 s_3 s_3 s_3 s_3 \ldots$

$$\mathcal{M} \not\models \mathit{extended} \qquad \mathcal{M} \models \bigcirc \mathit{extended}$$
$$\mathcal{M} \not\models \bigcirc\bigcirc \mathit{extended} \qquad \mathcal{M} \models \Diamond \mathit{extended}$$
$$\mathcal{M} \not\models \Box \mathit{extended} \qquad \mathcal{M} \models \Diamond\Box \mathit{extended}$$

Esempio 1: l'elastico (II)

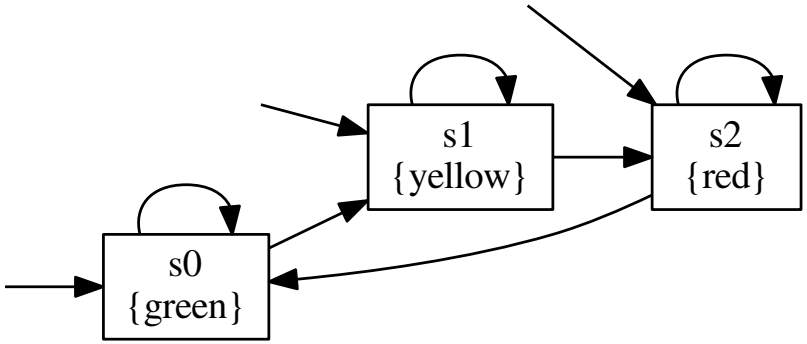


$\mathcal{S} \models \Diamond \mathit{extended}$
$\mathcal{S} \models \Box(\neg \mathit{extended} \rightarrow \bigcirc \mathit{extended})$
$\mathcal{S} \not\models \Box(\mathit{extended} \rightarrow \bigcirc \neg \mathit{extended})$ $(s_1 s_2 s_3^\omega)$
$\mathcal{S} \not\models \Diamond\Box \mathit{extended}$ $((s_1 s_2)^\omega)$
$\mathcal{S} \not\models \neg\Diamond\Box \mathit{extended}$ $(s_1 s_2 s_3^\omega)$
$\mathcal{S} \not\models \Box\Diamond\neg \mathit{extended}$

Esempio di fairness constraint: prima o poi l'elastico perde elasticità ($\{s3\} \Longrightarrow \Diamond \mathit{malfunction}$): si esclude $(s_1 s_2)^\omega$

Con questo vincolo il sistema soddisfa $\Diamond\Box \mathit{extended}$

Specifica delle proprietà di un sistema, esempio 2: il semaforo



Invariante: esattamente un colore alla volta

$$\Box((green \vee yellow \vee red) \wedge \\ \neg(green \wedge yellow) \wedge \neg(green \wedge red) \wedge \neg(yellow \wedge red))$$

Dal giallo prima o poi si passa sempre al rosso

$$\Box(yellow \rightarrow \Diamond red)$$

Dopo il giallo il semaforo diventa rosso

$$\Box(yellow \rightarrow \bigcirc(yellow \vee red))$$

Proprietà di programmi concorrenti, esempio: uso di una risorsa condivisa

Due utenti, u_1 e u_2 possono utilizzare la stessa stampante, ma non contemporaneamente.

request_i :	u_i chiede l'uso della stampante ($i = 1, 2$)
printing_i :	u_i sta stampando ($i = 1, 2$)

Verifica di correttezza del sistema: le formule seguenti devono essere verificate dal modello del sistema:

$\Box\neg(printing_1 \wedge printing_2)$	(mutual exclusion)
$\Box(request_1 \rightarrow \Diamond printing_1)$	(responsiveness)
$\Box(request_2 \rightarrow \Diamond printing_2)$	(responsiveness)
$\Box(printing_1 \rightarrow \Diamond\neg printing_1)$	
$\Box(printing_2 \rightarrow \Diamond\neg printing_2)$	