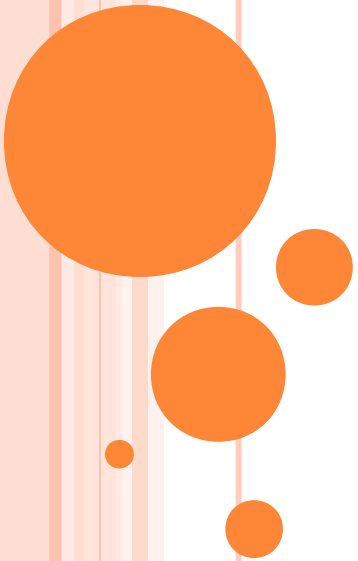

REGOLE DI INFERENZA PER TRIPLE DI HOARE

Corso di Logica per la Programmazione

A.A. 2012/13

RIASSUNTO

- Una tripla {P} C {R} è costituita da precondizione-comando-postcondizione
- La tripla {P} C {R} è **soddisfatta** se: per ogni stato σ che soddisfa P ($\sigma \models P$), l'esecuzione di C a partire da σ **termina**, e lo stato σ' in cui termina soddisfa R ($\sigma' \models R$)
- Obiettivo principale: **verificare che una tripla sia soddisfatta** (come *dimostrare che una proposizione è una tautologia* nel CP, o *dimostrare che una formula è valida* in LP1)
- Diremo anche, più semplicemente: **verificare una tripla**
- A volte: **completare una tripla in modo che sia soddisfatta**
- Quindi: introduciamo un **proof system** per verificare le triple
  - Assiomi – alcune triple che sono sempre soddisfatte
  - Regole di inferenza – per induzione strutturale
- Come per LP1, possiamo verificare la correttezza di assiomi + regole di inferenza confrontando la definizione di "tripla soddisfatta" con la semantica informale dei comandi

PROOF SYSTEM: ALCUNE **REGOLE** DI INFERENZA (GIA' VISTE)

$$\frac{P \Rightarrow P' \qquad \{P'\}\ C\ \{R'\} \qquad R' \Rightarrow R}{\{P\}\ C\ \{R\}} \qquad \text{(PRE-POST)}$$

$$\frac{P \Rightarrow P' \qquad \{P'\}\ C\ \{R\}}{\{P\}\ C\ \{R\}} \qquad \text{(PRE)}$$

$$\frac{\{P\}\ C\ \{R'\} \qquad R' \Rightarrow R}{\{P\}\ C\ \{R\}} \qquad \text{(POST)}$$

La correttezza di queste regole segue facilmente dalle definizioni

ASSIOMA PER SKIP

- **Assioma** per il comando vuoto:

$$\{P\}\ \textbf{skip}\ \{P\} \qquad \text{(SKIP)}$$

- Correttezza? Ovvia...

- Infatti ricordiamo il *significato informale:*
  - L'esecuzione di **skip** a partire dallo stato σ porta nello stato σ

ASSIOMA PER ASSEGNAMENTO SEMPLICE

- **Assioma** per l'assegnamento semplice

$$\{def(E) \wedge P[E/x]\} \quad x := E \quad \{P\} \qquad (ASS)$$

  dove *def*(E) è vera in uno stato σ se il valore di E in σ (cioè ***E***(E,σ)) è ben definito (vedi prossima pagina...)
- L'idea è che affinché l'asserzione P sia soddisfatta dopo l'assegnamento, la stessa P deve essere soddisfatta dallo stato precedente l'assegnamento quando all'identificatore di variabile è sostituita l'espressione
- La correttezza della regola si vede confrontando l'assioma con la semantica informale:
  - L'esecuzione dell'assegnamento **x := E** a partire dallo stato σ porta nello stato $\sigma[\boldsymbol{E}(E,\sigma)/x]$

DEFINIZIONE DI ESPRESSIONI

- La funzione *def(_)*, applicata a un'espressione *E,* restituisce una asserzione tale che $\sigma \models def(E)$ se esiste un v tale che $\boldsymbol{E}(E, \sigma) = v$.
- Serve per garantire che la valutazione di *E* sia definita e termini.

$$
\begin{array}{rcll}
def(c) & = & \mathbf{tt} & \text{se} \quad c \in \texttt{Num} \text{ o } c \in \texttt{Bool} \\
def(x) & = & \mathbf{tt} & \text{se} \quad x \in \texttt{Ide} \\
def(E \ op \ E') & = & def(E) \wedge def(E') & \text{se} \quad op \in \left\{ \begin{array}{l} +, -, <, >, \leq, \geq \\ =, \neq, and, or \end{array} \right\} \\
def(E \ op \ E') & = & def(E) \wedge def(E') \wedge E' \neq 0 & \text{se} \quad op \in \{div, mod\} \\
def(not \ E) & = & def(E) & \\
def((E)) & = & def(E) &
\end{array}
$$

ASSIOMA PER ASSEGNAMENTO MULTIPLO

- L'**assioma** per l'assegnamento multiplo generalizza quello per l'assegnamento singolo

$$\{def(E_1) \wedge \ldots \wedge def(E_k) \wedge P^{E_1,\ldots,E_k}_{x_1,\ldots,x_k}\}\ x_1, \ldots, x_k := E_1, \ldots, E_k\ \{P\} \quad \text{(ASS)}$$

- Tutte le espressioni vengono valutate PRIMA di tutti gli assegnamenti: confrontiamo con la semantica informale
  - L'esecuzione dell'assegnamento **x1, ..., xn := E1, ..., En** a partire dallo stato σ porta nello stato σ[*E(E1,σ)*/x1, ..., *E(En,σ)*/xn]
- Nota che gli assiomi per l'assegnamento consentono di **completare** una tripla di cui si conosce solo il comando (l'assegnamento) e la postcondizione.
- Vedremo che sono utili per "propagare all'indietro" le asserzioni in una sequenza di comandi.

UNA REGOLA PER L'ASSEGNAMENTO

- Combinando la regola (pre) con l'assioma per l'assegnamento semplice, si ottiene la seguente regola, utile per **verificare** che una tripla data sia soddisfatta:

$$\frac{R \Rightarrow \mathit{def}(E) \wedge P[E/x]}{\{R\}\ x := E\ \{P\}}\ (ASS)$$

- Infatti abbiamo la seguente istanza di (pre), in cui la seconda premessa scompare perché è un assioma:

$$\frac{R \Rightarrow \mathit{def}(E) \wedge P[E/x] \qquad \{\mathit{def}(E) \wedge P[E/x]\}\ x := E\ \{P\}}{\{R\}\ x := E\ \{P\}}$$

- Esempio: Verificare la seguente tripla:
  - $\{x = 5\}\ x := x + 1\ \{x > 2\}$

REGOLA PER LA SEQUENZA DI COMANDI

- Regola per verifica di una tripla in cui il comando è una sequenza, per induzione strutturale:

$$\frac{\{P\}\ C\ \{R\} \qquad \{R\}\ C'\ \{Q\}}{\{P\}\ C\ ;C'\ \{Q\}}\ (SEQ)$$

- Convinciamoci della correttezza confrontandola con la semantica informale:
  - L'esecuzione di **C;C'** a partire dallo stato σ porta nello stato σ' ottenuto eseguendo **C'** a partire dallo stato σ" ottenuto dall'esecuzione di **C** nello stato σ.
- Si verifichi che la seguente tripla è soddisfatta
  - {x >= y - 1} x := x+1; y := y - 1 {x > y}

ESEMPIO DI SEQUENZA DI COMANDI

Verificare la tripla: $\{x >= y - 1\}\ x := x+1; y := y - 1\ \{x > y\}$

- Per la **Regola per la Sequenza**, dobbiamo trovare una asserzione **R** e verificare le seguenti triple:

1) $\{x \geq y - 1\}\ x := x+1\ \{\mathbf{R}\}$
2) $\{\mathbf{R}\}\ y := y - 1\ \{x > y\}$

- Per determinare **R**, usiamo l'**Assioma dell'Assegnamento** nella seconda tripla. Sappiamo infatti che la seguente è verificata:

$$\{def(y-1) \wedge (x > y)[y-1/y]\}\ y := y - 1\ \{x > y\}$$

- Quindi fissiamo **R** = $def(y-1) \wedge x > y-1$. Resta da verificare:

$$\{x \geq y - 1\}\ x := x+1\ \{def(y-1) \wedge x > y-1\}$$

- Usando la **Regola per l'Assegnamento**, basta dimostrare:

$$x \geq y - 1 \Rightarrow def(x+1) \wedge (def(y-1) \wedge x > y-1)[x+1/x]$$

- **Esercizio:** completare la dimostrazione

SEQUENZA CON **VARIABILI DI SPECIFICA**

Determinare E in modo che la tripla sia verificata:

$$\{x = N \wedge y = M\}\ t := E;\ \ x := y;\ \ y := t\ \ \{x = M \wedge y = N\}$$

- Per la **Regola per la Sequenza**, dobbiamo trovare **R1** e **R2** tali che:

1) $\{x = N \wedge y = M\}\ t := E\ \{\mathbf{R1}\}$
2) $\{\mathbf{R1}\}\ x := y\ \{\mathbf{R2}\}$
3) $\{\mathbf{R2}\}\ y := t\ \ \{x = M \wedge y = N\}$

Nota: M e N sono **variabili di specifica**: non possono essere usate nei comandi

- Per determinare **R2**, usiamo l'**Assioma dell'Assegnamento** in 3):

$$\{def(t) \wedge x = M \wedge y = N)[t/y]\}\ y := t\ \ \{x = M \wedge y = N\}$$

- Fissiamo **R2 =** $(x = M \wedge t = N)$. Per **R1**, usiamo l'assioma in 2):

$$\{def(y) \wedge (x = M \wedge t = N)[y/x]\}\ x := y\ \{x = M \wedge t = N\}$$

- Fissiamo **R1 =** $(y = M \wedge t = N)$. Resta da verificare:

$$\{x = N \wedge y = M\}\ t := E\ \{y = M \wedge t = N\}$$

- Usando la **Regola per l'Assegnamento**, basta trovare un E tale che:

$$x = N \wedge y = M\ \Rightarrow def(E)\ \wedge (y = M \wedge t = N)[E/t]$$

ESERCIZI

- Verificare la seguente tripla:
  - $\{s = (\Sigma\ i: i \in [0, x).\ i)\}$
    $x, s := x + 1, s + x$
    $\{s = (\Sigma\ i: i \in [0, x).\ i)\}$
- La seguente tripla non è soddisfatta. Mostrare formalmente perché.
  - $\{z = 5 \wedge y = 7 \wedge x = 3\}$ x:= 0; y := z **div** x $\{z > 4\}$
- Le seguenti triple sono soddisfatte? Perché?
  - $\{x = N \wedge y = M\}$ x := y; y:= x $\{x = M \wedge y = N\}$
  - $\{x = N \wedge y = M\}$ x, y := y, x $\{x = M \wedge y = N\}$