

# Logica per la Programmazione

## Lezione 17

- ▶ Sistema di Dimostrazioni per le Triple di Hoare
- ▶ Sequenze (Array) e Aggiornamento Selettivo

## Sequenze: Sintassi

- ▶ Estendiamo il linguaggio per usare *array* o *sequenze*
- ▶ Con **a : array [0,n) of T** diciamo che **a** è una variabile di tipo:

“sequenza di elementi di tipo **T** con dominio **[0,n)**”

dove **T** può essere **int** o **bool**

- ▶ Il dominio di **a** viene indicato come **dom(a)**
- ▶ Scriviamo **a[E]** per denotare l'elemento di **a** di posizione **E**. Ad esempio: **a[0]**, **a[4]**, **a[2\*x+1]**, **a[a[0]+a[4]]**, ...
- ▶ La sintassi delle espressioni diventa:

$$Exp ::= Const \mid Id \mid \text{Ide}[Exp] \mid (Exp) \mid Exp \text{ Op } Exp \mid not \ Exp$$

## Sequenze: Semantica

- ▶ Ricordiamo che uno **stato**  $\sigma$  è una funzione  $\sigma : Ide \rightarrow (\mathbb{Z} \cup \mathbb{B})$
- ▶ Estendiamo il concetto di stato: se  $\mathbf{a}$  è un array di tipo  $\mathbf{T}$ , allora

$$\begin{cases} \sigma(a) : dom(a) \rightarrow \mathbb{B} & \text{se } \mathbf{T} = \mathbf{bool} \\ \sigma(a) : dom(a) \rightarrow \mathbb{Z} & \text{se } \mathbf{T} = \mathbf{int} \end{cases}$$

- ▶ Esempio:  $\mathbf{a}$ : **array [0,4) of int**

2	1	10	6
---	---	----	---

$$\sigma(\mathbf{a}) : [0, 4) \rightarrow \mathbf{int}$$

$$\sigma(\mathbf{a}) = \{0 \mapsto 2, 1 \mapsto 1, 2 \mapsto 10, 3 \mapsto 6\}$$

- ▶ Estendiamo la funzione di interpretazione semantica:

$$\mathcal{E}(Ide[Exp], \sigma) = \sigma(Ide)(\mathcal{E}(Exp, \sigma)) \quad \text{se } \mathcal{E}(Exp, \sigma) \in dom(Ide)$$

- ▶ Esempio:

$$\mathcal{E}(a[0], \sigma) = \sigma(a)(\mathcal{E}(0, \sigma)) = \sigma(a)(0) = 2$$

## Sequenze: Semantica (2)

Esempio: valutazione di  $\mathbf{a[a[0]+a[1]]}$  nello stato  $\sigma$  tale che

$$\sigma(\mathbf{a}) : [0, 4) \rightarrow \mathbf{int}$$

$$\sigma(\mathbf{a}) = \{0 \mapsto 2, 1 \mapsto 1, 2 \mapsto 10, 3 \mapsto 6\}$$

2	1	10	6
---	---	----	---

$$\begin{aligned} \mathcal{E}(a[a[0] + a[1]], \sigma) &= \\ \sigma(a)(\mathcal{E}(a[0] + a[1], \sigma)) &= \\ \sigma(a)(\mathcal{E}(a[0], \sigma) + \mathcal{E}(a[1], \sigma)) &= \\ \sigma(a)(\sigma(a)(0) + \sigma(a)(1)) &= \\ \sigma(a)(2 + 1) &= \\ \sigma(a)(3) &= \\ 6 \end{aligned}$$

## Sequenze: Semantica (3)

- ▶ **Attenzione:**  $\text{Ide}[Exp]$  non è sempre definito
- ▶ Estendiamo la funzione  $\text{def}$ :

$$\text{def}(\text{Ide}[Exp]) = \text{def}(Exp) \wedge Exp \in \text{dom}(\text{Ide})$$

- ▶ Quindi abbiamo i seguenti casi in cui un'espressione potrebbe non essere definita:
  - ▶  $\text{def}(E \text{ mod } E') = \text{def}(E \text{ div } E') = \text{def}(E) \wedge \text{def}(E') \wedge E' \neq 0$
  - ▶  $\text{def}(\text{Ide}[Exp]) = \text{def}(Exp) \wedge Exp \in \text{dom}(\text{Ide})$

## Sequenze: Ridefinizione locale di sequenza

- ▶ Sia **a**: **array** [0,n) **of** **T** una sequenza.
- ▶ Con  $a[E_1/E_2]$  intendiamo l'array **a** modificato in modo tale che nella posizione  $E_2$  abbia il valore  $E_1$ .
- ▶ Quindi la valutazione di  $a[E_1/E_2][E]$  in uno stato  $\sigma$  è data da:

$$\mathcal{E}(a[E_1/E_2][E], \sigma) = \begin{cases} \mathcal{E}(E_1, \sigma) & \text{se } \mathcal{E}(E, \sigma) = \mathcal{E}(E_2, \sigma) \\ \mathcal{E}(a[E], \sigma) & \text{altrimenti} \end{cases}$$

- ▶ **Nota:** le operazioni non possono essere applicate a sequenze, ma solo a singoli elementi di sequenze.
  - ▶ Per esempio, possiamo scrivere  $a[2] < b[3]$ ,  $a[2] * y + x$
  - ▶ ma non  $a + b$ !

## Aggiornamento Selettivo

- ▶ Ogni elemento di una sequenza è una variabile, quindi può comparire a sinistra di un assegnamento. Es:  $a[3] := 5$
- ▶ Estendiamo il comando di assegnamento:

$$Ide\_List := Exp\_List$$

- ▶ Formalmente, cambia la definizione di  $Ide\_List$  come segue:

$$Ide\_List ::= Ide \mid Ide, Ide\_List \mid Ide[Exp] \mid Ide[Exp], Ide\_List$$

- ▶ Un comando di assegnamento del tipo  $v[E] := E'$  è chiamato **aggiornamento selettivo**.
- ▶ L'effetto è di transire, a partire da uno stato  $\sigma$ , allo stato  $\sigma[w/v]$ , dove  $w = v[\mathcal{E}(E', \sigma)/\mathcal{E}(E, \sigma)]$ , a patto che le due espressioni  $E$  ed  $E'$  siano definite in  $\sigma$ , e che il valore di  $E$  in  $\sigma$  stia nel dominio di  $v$ .

## Aggiornamento Selettivo: Semantica

- ▶ La semantica del comando di aggiornamento selettivo è data dal seguente assioma (AGG-SEL):

$$\boxed{\begin{array}{c} \{ \text{def}(E) \wedge \text{def}(E') \wedge E \in \text{dom}(v) \wedge P[\mathbf{w}/v] \} \ v[E] := E' \ \{P\} \\ \text{dove } \mathbf{w} = v[E'/E] \end{array}}$$

- ▶ **Domanda:** Perché l'assioma (ASS) non funzionerebbe in questo caso?
- ▶ Si può usare anche la seguente regola derivata (da (AGG-SEL) e (PRE)):

$$\boxed{\frac{R \Rightarrow \text{def}(E) \wedge \text{def}(E') \wedge E \in \text{dom}(v) \wedge P[\mathbf{w}/v] \quad \mathbf{w} = v[E'/E]}{\{R\} \ v[E] := E' \ \{P\}}}$$

## Esempio: Aggiornamento selettivo

- ▶ Si verifichi la seguente tripla di Hoare (assumendo **a**: **array [0, n) of int**):

$$\{k \in [1, n) \wedge (\forall i. i \in [0, k) \Rightarrow (a[i] = (\sum x : x \in [0, i].x)))\}$$

$$a[k] := a[k-1] + k$$

$$\{(\forall i. i \in [0, k) \Rightarrow (a[i] = (\sum x : x \in [0, i].x)))\}$$

- ▶ Per dimostrare le tripla applichiamo la regola dell'Aggiornamento Selettivo (o l'Assioma dell'Aggiornamento selettivo e la Regola di Inferenza PRE).
- ▶ Quindi dobbiamo dimostrare la seguente implicazione:

$$k \in [1, n) \wedge (\forall i. i \in [0, k) \Rightarrow (a[i] = (\sum x : x \in [0, i].x))) \Rightarrow$$

$$def(k) \wedge def(a[k-1] + k) \wedge k \in dom(a) \wedge$$

$$(\forall i. i \in [0, k) \Rightarrow (b[i] = (\sum x : x \in [0, i].x)))$$

dove  $b = a \left[ \frac{a^{[k-1]+k}}{k} \right]$ .

## Soluzione

## ► Partiamo dalla conseguenza:

$$\begin{aligned}
& def(k) \wedge def(a[k-1] + k) \wedge k \in dom(a) \wedge (\forall i. i \in [0, k] \Rightarrow (b[i] = (\sum x : x \in [0, i].x))) \\
\equiv & \quad \{ \text{definizione di def} \} \\
& k-1 \in dom(a) \wedge k \in dom(a) \wedge (\forall i. i \in [0, k] \Rightarrow (b[i] = (\sum x : x \in [0, i].x))) \\
\equiv & \quad \{ \mathbf{lp}: k \in [1, n) \wedge dom(a) = [0, n) \} \\
& (\forall i. i \in [0, k] \Rightarrow (b[i] = (\sum x : x \in [0, i].x))) \\
\equiv & \quad \{ (\text{Intervallo-}\forall) \} \\
& (\forall i. i \in [0, k] \Rightarrow (b[i] = (\sum x : x \in [0, i].x)) \wedge b[k] = (\sum x : x \in [0, k].x) \\
\equiv & \quad \{ \text{def di } b, \mathbf{lp}: (\forall i. i \in [0, k] \Rightarrow (a[i] = (\sum x : x \in [0, i].x))), (\forall i. i \in [0, k] \Rightarrow i \neq k) \} \\
& b[k] = (\sum x : x \in [0, k].x) \\
\equiv & \quad \{ \mathbf{lp}: \text{def di } b, \text{ sostituzione} \} \\
& a[k-1] + k = (\sum x : x \in [0, k].x) \\
\equiv & \quad \{ (\text{Intervallo-}\Sigma) \} \\
& a[k-1] + k = (\sum x : x \in [0, k].x) + k \\
\equiv & \quad \{ \mathbf{lp}: (\forall i. i \in [0, k] \Rightarrow (a[i] = (\sum x : x \in [0, i].x))) \} \\
& (\sum x : x \in [0, k-1].x) + k = (\sum x : x \in [0, k].x) + k \\
\equiv & \quad \{ \text{calcolo} \} \\
& \mathbf{T}
\end{aligned}$$

## Esempio: Incremento di Sequenza

Si consideri il seguente programma annotato che incrementa tutti gli elementi di un array **a**: **array [0, n) of int**.

```

{  $n \geq 0 \wedge a : \text{array}[0, n) \text{ of int} \wedge (\forall k. k \in [0, n) \Rightarrow a[k] = V[k])$  }
x := 0;
{ Inv :  $x \in [0, n] \wedge (\forall k. k \in [0, x) \Rightarrow a[k] = V[k] + 1) \wedge$ 
   $(\forall k. k \in [x, n) \Rightarrow a[k] = V[k])$  } { t :  $n - x$  }
while x < n do
  a[x] := a[x] + 1; x := x + 1
endw
{ Inv  $\wedge \neg(x < n)$  }
{  $(\forall k. k \in [0, n) \Rightarrow a[k] = V[k] + 1)$  }

```

- ▶ Si analizzi l'invariante, cercando di capirne la struttura
- ▶ Scrivere e dimostrare la Condizione di Invarianza
- ▶ Scrivere e dimostrare la Condizione di Terminazione
- ▶ Scrivere e dimostrare la Condizione di Progresso

## Incremento di Sequenza: Condizione di Invarianza

$$\{ x \in [0, n] \wedge (\forall k . k \in [0, x] \Rightarrow a[k] = V[k] + 1) \wedge$$

$$(\forall k . k \in [x, n] \Rightarrow a[k] = V[k]) \wedge x < n \}$$

$$a[x] := a[x] + 1; \quad x := x + 1$$

$$\{ x \in [0, n] \wedge (\forall k . k \in [0, x] \Rightarrow a[k] = V[k] + 1) \wedge$$

$$(\forall k . k \in [x, n] \Rightarrow a[k] = V[k]) \wedge \text{def}(x < n) \}$$

- ▶ Per la regola della sequenza dobbiamo determinare **R** in modo che siano verificate:

1.  $\{ \text{Inv} \wedge x < n \} \quad a[x] := a[x] + 1 \quad \{ R \}$

2.  $\{ R \} \quad x := x + 1 \quad \{ \text{Inv} \wedge \text{def}(x < n) \}$

- ▶ Per l'assioma (ASS), la seconda tripla è verificata per
- ▶  $R \equiv \text{def}(x + 1) \wedge x + 1 \in [0, n] \wedge (\forall k . k \in [0, x + 1] \Rightarrow a[k] = V[k] + 1) \wedge (\forall k . k \in [x + 1, n] \Rightarrow a[k] = V[k])$

## Incremento di Sequenza: Condizione di Invarianza

Per la prima tripla, applicando la regola dell'aggiornamento selettivo dobbiamo mostrare

$$x \in [0, n] \wedge (\forall k. k \in [0, x] \Rightarrow a[k] = V[k] + 1) \wedge$$

$$(\forall k. k \in (x, n) \Rightarrow a[k] = V[k]) \wedge x < n$$

$\Rightarrow$

$$x + 1 \in [0, n] \wedge (\forall k. k \in [0, x] \Rightarrow b[k] = V[k] + 1) \wedge$$

$$(\forall k. k \in (x, n) \Rightarrow b[k] = V[k]) \wedge x \in [0, n] \wedge \text{def}(a[x] + 1)$$

con  $b = a[a[x] + 1/x]$

Alcune osservazioni:

1.  $\text{def}(a[x] + 1) \equiv x \in [0, n)$  che quindi possiamo omettere
2.  $(\forall k. k \in [0, x] \vee k \in (x, n) \Rightarrow b[k] = a[k])$
3.  $b[x] = a[x] + 1$

## Incremento di Sequenza: Condizione di Invarianza

Partiamo dalla conseguenza:

$$\begin{aligned}
 & x + 1 \in [0, n] \wedge (\forall k . k \in [0, x] \Rightarrow b[k] = V[k] + 1) \wedge \\
 & \quad (\forall k . k \in (x, n) \Rightarrow b[k] = V[k]) \wedge x \in [0, n] \wedge \text{def}(a[x] + 1) \\
 & \equiv \{\text{Ip} : x \in [0, n], x < n \text{ quindi } x + 1 \in [0, n]\} \\
 & (\forall k . k \in [0, x] \Rightarrow b[k] = V[k] + 1) \wedge (\forall k . k \in (x, n) \Rightarrow b[k] = V[k]) \\
 & \equiv \{(\text{Intervallo-}\forall), x \in [0, x]\} \\
 & (\forall k . k \in [0, x] \Rightarrow b[k] = V[k] + 1) \wedge b[x] = V[x] + 1 \wedge \\
 & (\forall k . k \in (x, n) \Rightarrow b[k] = V[k]) \\
 & \equiv \{\text{Osservazioni (2) e (3) precedenti}\} \\
 & (\forall k . k \in [0, x] \Rightarrow a[k] = V[k] + 1) \wedge a[x] + 1 = V[x] + 1 \wedge \\
 & (\forall k . k \in (x, n) \Rightarrow a[k] = V[k]) \\
 & \equiv \{\text{Ip} : \forall k . k \in [0, x] \Rightarrow a[k] = V[k] + 1\} \\
 & a[x] + 1 = V[x] + 1 \wedge (\forall k . k \in (x, n) \Rightarrow a[k] = V[k]) \\
 & \equiv \{\text{calcolo, intervallo-}\forall \text{ al contrario}\} \\
 & (\forall k . k \in [x, n) \Rightarrow a[k] = V[k]) \text{ vero per ipotesi}
 \end{aligned}$$