



# **TRIPLE DI HOARE: SEQUENZE (ARRAY) E AGGIORNAMENTO SELETTIVO**

**Corso di Logica per la Programmazione**

# SEQUENZE: SINTASSI

- Estendiamo il linguaggio per usare *array* o *sequenze*
- Scriviamo **a : array [0,n) of T** per dire 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**
  - Esempio: **a[0]**, **a[4]**, **a[2\*x+1]**, **a[a[0]+a[4]]**, ...
- La **sintassi** delle espressioni diventa:

Exp ::= Const | Id | **Ide[Exp]** | (Exp) | Exp Op Exp | not Exp



# SEQUENZE: SEMANTICA

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

$$\sigma(\mathbf{a}) : \text{dom}(\mathbf{a}) \rightarrow \mathbf{B} \quad \text{se } \mathbf{T} = \mathbf{bool}$$

$$\sigma(\mathbf{a}) : \text{dom}(\mathbf{a}) \rightarrow \mathbf{Z} \quad \text{se } \mathbf{T} = \mathbf{int}$$

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

2	1	10	6
0	1	2	3

- $\sigma(\mathbf{a}) : [0,4) \rightarrow \mathbf{int} = \{ \langle 0,2 \rangle, \langle 1,1 \rangle, \langle 2,10 \rangle, \langle 3,6 \rangle \}$

- Estendiamo la funzione di **interpretazione semantica**:

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

- Esempio:  $E(\mathbf{a}[0], \sigma) = E(\mathbf{a}, \sigma)(E(0, \sigma)) = \sigma(\mathbf{a})(0) = 2$



# SEQUENZE: SEMANTICA

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

- $\sigma(\mathbf{a}): [0,4) \rightarrow \mathbf{int} = \{ \langle 0,2 \rangle, \langle 1,1 \rangle, \langle 2,10 \rangle, \langle 3,6 \rangle \}$

2	1	10	6
0	1	2	3

$$E(\mathbf{a}[\mathbf{a}[0] + \mathbf{a}[1]], \sigma) =$$

$$E(\mathbf{a}, \sigma) (E(\mathbf{a}[0], \sigma) + E(\mathbf{a}[1], \sigma)) =$$

$$\sigma(\mathbf{a})(E(\mathbf{a}, \sigma)(0) + E(\mathbf{a}, \sigma)(1)) =$$

$$\sigma(\mathbf{a})(\sigma(\mathbf{a})(0) + \sigma(\mathbf{a})(1)) =$$

$$\sigma(\mathbf{a})(2+1) =$$

$$\sigma(\mathbf{a})(3) =$$

6



# SEQUENZE: SEMANTICA

- **Attenzione:**  $\text{Ide}[\text{Exp}]$  non è sempre definito

- Estendiamo la funzione  $\text{def}$ :

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

- Quindi abbiamo i seguenti casi in cui un'espressione potrebbe non essere definita:

- $\text{def}(E \text{ mod } E') = \text{def}(E \text{ div } E') = \text{def}(E) \wedge \text{def}(E') \wedge E' \neq 0$
- $\text{def}(\text{Ide}[\text{Exp}]) = \text{def}(\text{Exp}) \wedge \text{Exp} \in \text{dom}(\text{Ide})$

- Nota: le operazioni non possono essere applicate a sequenze, ma solo a singoli elementi di sequenze.

Es:  $\mathbf{a[2]} < \mathbf{b[3]}$ ,  $\mathbf{a[2]} * \mathbf{y} + \mathbf{x}$ , ma non  $\mathbf{a} + \mathbf{b}$  !



# 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:  
$$\text{Ide\_List} ::= \text{Ide} \mid \text{Ide}, \text{Ide\_List} \mid \text{Ide}[\text{Exp}] \mid \text{Ide}[\text{Exp}], \text{Ide\_List}$$
- 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  
$$\sigma[w/v], \quad \text{dove} \quad w = v[E(E', \sigma)/E(E, \sigma)],$$
  
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

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

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

dove  $\mathbf{w} = v[E'/E]$

- Con  $v[E'/E]$  intendiamo l'array  $v$  modificato in modo tale che nella posizione  $E$  abbia il valore  $E'$ . Quindi se  $\mathbf{w} = v[E'/E]$ ,
  - $w(x) = E'$                       se  $x = E$ ,
  - $w(x) = v(x)$                   altrimenti
- Si può usare anche la seguente regola derivata:

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

---

$$\{R\} \quad v[E] := E' \quad \{P\}$$



# ESEMPIO DI AGGIORNAMENTO SELETTIVO

- Si verifichi la tripla:

$$\{k \in \text{dom}(v) \wedge (\forall i . i \in \text{dom}(v) \wedge i \neq k \Rightarrow v[i] > 0)\}$$

$$v[k] := 3$$

$$\{(\forall i . i \in \text{dom}(v) \Rightarrow v[i] > 0)\}$$

- Applicando la regola (AGG-SEL), è sufficiente dimostrare:

$$k \in \text{dom}(v) \wedge (\forall i . i \in \text{dom}(v) \wedge i \neq k \Rightarrow v[i] > 0) \Rightarrow \\ \text{def}(k) \wedge \text{def}(3) \wedge k \in \text{dom}(v) \wedge (\forall i . i \in \text{dom}(w) \Rightarrow w[i] > 0)$$

dove  $w = v[3/k]$

- **Esercizio:** si completi la dimostrazione sfruttando la regola dell'intervallo per la quantificazione universale:

$$\{(\forall x.P \wedge x \neq k \Rightarrow Q) \wedge Q[k/x] \quad \text{se } P[k/x]$$

- $(\forall x.P \Rightarrow Q) \equiv \{$   
 $\quad \{ (\forall x.P \wedge x \neq k \Rightarrow Q) \quad \text{se } \sim P[k/x]$





# ESERCIZIO: SCANSIONE DI SEQUENZA

- Verificare il seguente programma annotato che conta il numero di elementi maggiori di zero in un array **a**: **array [0, n) of int**.

```
{a : array [0, n) of int }  
x, c := 0, 0;  
{Inv : c = #{j : j ∈ [0, x) ∧ a[j] > 0 } ∧ x ∈ [0, n] } {t : n - x}  
while x < n do  
    if (a[x] > 0) then c := c+1 else skip fi ;  
    x := x + 1  
endw  
{Inv ∧ ~(x < n)}  
{ c = #{j : j ∈ [0, n) ∧ a[j] > 0 } }
```

- Scrivere e dimostrare la Condizione di Invarianza
- Scrivere e dimostrare la Condizione di Terminazione
- Scrivere e dimostrare la Condizione di Progresso



# ESERCIZIO: 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**

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

**endw**

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

- Scrivere e dimostrare la Condizione di Invarianza
- Scrivere e dimostrare la Condizione di Terminazione
- Scrivere e dimostrare la Condizione di Progresso



- SOLUZIONE: Condizione di invarianza

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

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

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

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

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

- Per la regola della sequenza dobbiamo determinare **R** in modo che

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

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

$$\mathbf{a[x] := a[x] + 1;$$

$$\{\mathbf{R}\}$$

$$\mathbf{x := x + 1}$$

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

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



- In questo caso  $\mathbf{R}$  viene determinata dall'assioma per l'assegnamento

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

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

INCREMENTO  
DI SEQUENZA

$$\mathbf{a[x] := a[x] + 1;}$$

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

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

$$\mathbf{x := x + 1}$$

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

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

- Ci resta da dimostrare la tripla

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

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

$$\mathbf{a[x] := a[x] + 1;}$$

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

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



○ Avendo a che fare con un aggiornamento selettivo, dobbiamo mostrare

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

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

$\Rightarrow$

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

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

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

INCREMENTO  
DI SEQUENZA

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)  $b[x] = a[x] + 1$



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

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

$$\equiv \{ \mathbf{Ip}: x \in [0, n) \}$$

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

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

$$\equiv \{ \text{Intervallo, } x \in [0, x] \}$$

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

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

$$\equiv \{ \text{Osservazioni (2) e (3) precedenti} \}$$

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

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

$$\equiv \{ \mathbf{Ip}: (\forall k. k \in [0, x) \Rightarrow a[k] = V[k] + 1) \}$$

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

$$\equiv \{ \text{calcolo, Intervallo} \}$$

$$(\forall k. k \in [x, n) \Rightarrow a[k] = V[k]), \text{ vero per ipotesi.}$$



# ESERCIZIO: Calcolo del fattoriale

- Si consideri la seguente specifica

$\{n > 0\} \text{ C } \{f = n!\}$

$\{n > 0\}$

$f, x := 1, 1;$

$\{Inv : ?\} \{t : ?\}$

**while**  $x \leq n$  **do**

$f, x := f * x, x + 1;$

**endw**

$\{Inv \wedge \sim(x \leq n)\}$

$\{f = n!\}$

- Come determinare l'invariante e la funzione di terminazione?



- Eseguiamo manualmente il programma (es: per  $n = 5$ ):

$\{n > 0\}$	x	f
f, x := 1, 1;	1	1
$\{Inv : ?\} \{t : ?\}$	2	1
<b>while</b> x <= n <b>do</b>	3	2
f, x := f * x, x + 1;	4	6
<b>endw</b>	5	24
$\{Inv \wedge \sim(x \leq n)\}$	6	120
$\{f = n!\}$		

- Osserviamo che, ad ogni iterazione, i valori di x e f sono legati dalla seguente relazione

$$f = (x - 1)!$$

- Scegliendo questa formula come invariante non riusciamo a dimostrare

$$f = (x - 1)! \wedge \sim(x \leq n) \Rightarrow f = n!$$





```

{n>0}
  f, x:= 1, 1;
{Inv : f = (x - 1)! ∧ x∈[0, n+1]} {t : ?}
while x ≤ n do
  f, x := f * x, x + 1;
endw
{Inv ∧ ¬(x ≤ n)}
{f = n!}

```

- Aggiungendo  $x \in [0, n+1]$  in *Inv* abbiamo:

$$Inv \wedge \sim(x \leq n) \Rightarrow f = n!$$

- Dimostrazione per esercizio



- Ipotesi di invarianza

$$\{f = (x-1)! \wedge x \in [0, n+1)\} f, x := f * x, x + 1 \quad \{f = (x-1)! \wedge x \in [0, n+1]\}$$

- Per la regola dell'assegnamento multiplo, basta dimostrare:

$$f = (x-1)! \wedge x \in [0, n+1) \Rightarrow \text{def}(f*x) \wedge \text{def}(x+1) \wedge f*x = x! \wedge x+1 \in [0, n+1]$$

- Partiamo dalla conseguenza (eliminando i  $\text{def}(\dots)$  che sono **T**):

$$f * x = x! \quad \wedge \quad x+1 \in [0, n+1]$$

$$\equiv \{ \mathbf{Ip}: f = (x-1)! \}$$

$$(x-1)! * x = x! \quad \wedge \quad x+1 \in [0, n+1]$$

$$\equiv \{ \text{def. fattoriale} \}$$

$$x+1 \in [0, n+1]$$

$$\equiv \{ \mathbf{Ip}: x \in [0, n+1), \text{ calcolo} \}$$

**T**

- La funzione di terminazione (che è molto semplice) è lasciata per esercizio.

