

# Progetto 1.

Si consideri il linguaggio IMP e la sua semantica operazionale definite nelle slide che seguono.

- 1) Si codifichi in Coq la sintassi e la semantica di IMP.
- 2) Si dimostri il teorema seguente in Coq.

## Proposition

$$\begin{array}{lcl} w & \equiv & \text{while } b \text{ do } c \\ w' & \equiv & \text{if } b \text{ then } c ; w \text{ else skip} \end{array} \quad \rightarrow \quad w \sim w'$$

dove la relazione di equivalenza  $\sim$  tra comandi è definita alla fine delle slide.

- 3) Sia **w** il programma **while**  $1 \leq x$  **do**  $(y := 2 * y; x := x - 1)$ . Si dimostri in Coq che  $\forall \sigma \exists \sigma^* \langle w, \sigma[2/x][3/y] \rangle \rightarrow \sigma^*$   
**OPPURE** dimostrare che dato lo stato  $\sigma$  tale che per ogni locazione  $i$   $\sigma(i) = 0$ , allora  $\exists \sigma^* \langle w, \sigma[2/x][3/y] \rangle \rightarrow \sigma^*$

## Syntactic Sets

- ➊ number  $N$
- ➋ truth values  $B$
- ➌ arithmetic expressions  $Aexp$
- ➍ boolean expression  $Bexp$
- ➎ commands,  $Com$
- ➏ locations  $Loc$

## formation rules

### • **Aexp**

$a := \text{n} \mid X \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$

### • **Bexp**

$b := \text{true} \mid \text{false} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \neg b \mid b_0 \wedge b_1 \mid b_0 \vee b_1$

### • **Com**

$c ::= \text{skip} \mid c_1 ; c_2 \mid \text{if } b \text{ then } c_0 \text{ else } c_1 \mid X := a \mid \text{while } b \text{ do } c$

## meta-variables

$n, m$  : range over  $\mathbf{N}$

$X, Y$ : range over  $\mathbf{Loc}$

$a$ : to represent an arbitrary element of  $\mathbf{Aexp}$

$b$ : to represent an arbitrary element of  $\mathbf{Bexp}$

$c$  : to represent an arbitrary element of  $\mathbf{Com}$

## Operational Semantics

● **evaluation** of arithmetic and boolean expression

● **execution** of commands

### ○ semantic sets

$\mathbf{Z}$  : set of “*machine number*”

$\Sigma$  : set of “*states*”

$\Sigma : \{\sigma | \sigma : \mathbf{Loc} \rightarrow \mathbf{Z}\}$

$\mathbf{C}$ : set of “*configurations*”

$\mathbf{C} = \{(p, \sigma) | p \in \mathbf{Aexp}, \mathbf{Bexp}, \mathbf{Com}, \sigma \in \Sigma\}$

FINE 9 GENN

## evaluation of **Aexp** elements

evalutation relation:  $\langle a, \sigma \rangle \rightarrow n \quad (n \in \mathbf{Z})$

*Numbers:*

$$\langle n, \sigma \rangle \rightarrow n$$

*locations:*

$$\langle X, \sigma \rangle \rightarrow \sigma(X)$$

*sums:*

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 + a_1, \sigma \rangle \rightarrow n_0 + n_1}$$

*subtractions:*

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 - a_1, \sigma \rangle \rightarrow n_0 - n_1}$$

*products:*

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 \times a_1, \sigma \rangle \rightarrow n_0 \times n_1}$$

## evaluation of **Bexp** elements

evalutation relation:  $\langle b, \sigma \rangle \rightarrow t \quad t \in \{\text{true}, \text{false}\}$

$$\langle \text{true}, \sigma \rangle \rightarrow \text{true}$$

$$\langle \text{false}, \sigma \rangle \rightarrow \text{false}$$

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 = a_1, \sigma \rangle \rightarrow \text{true}} \text{ when } n_0 = n_1$$

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 = a_1, \sigma \rangle \rightarrow \text{false}} \text{ when } n_0 \neq n_1$$

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 \leq a_1, \sigma \rangle \rightarrow \text{true}} \text{ when } n_0 \leq n_1$$

$$\frac{\langle a_0, \sigma \rangle \rightarrow n_0 \quad \langle a_1, \sigma \rangle \rightarrow n_1}{\langle a_0 \leq a_1, \sigma \rangle \rightarrow \text{false}} \text{ when } n_0 \not\leq n_1$$

$$\frac{\langle b, \sigma \rangle \rightarrow t}{\langle \neg b, \sigma \rangle \rightarrow \neg t}$$

$$\frac{\langle b_0, \sigma \rangle \rightarrow t_0 \quad \langle b_1, \sigma \rangle \rightarrow t_1}{\langle b_0 \wedge b_1, \sigma \rangle \rightarrow t_0 \wedge t_1}$$

$$\frac{\langle b_0, \sigma \rangle \rightarrow t_0 \quad \langle b_1, \sigma \rangle \rightarrow t_1}{\langle b_0 \vee b_1, \sigma \rangle \rightarrow t_0 \vee t_1}$$

$$b_0 \sim b_1 \text{ iff } (\forall t \in \{\text{false}, \text{true}\} \ \forall \sigma \in \sum . \langle b_0, \sigma \rangle \rightarrow t \Leftrightarrow \langle b_1, \sigma \rangle \rightarrow t)$$

## execution of commands

$$\begin{array}{c} \text{command execution} \\ \text{relation} \end{array} \quad \xrightarrow{\quad} \quad \langle c, \sigma \rangle \rightarrow \sigma'$$

we assume the existence of an *initial state*  $\sigma_0$  such that

$$(\forall X \in \mathbf{Loc}. \sigma_0(X) = 0)$$

$\langle c, \sigma \rangle \rightarrow \sigma'$   the execution of  $c$  in  $\sigma$  terminates in  $\sigma'$

**Notation.** Let  $\sigma$  be a state. Let  $m \in \mathbf{Z}$ . Let  $X \in \mathbf{Loc}$ . We write  $\sigma[m/X]$  for “the state obtained from  $\sigma$  by replacing the contents of  $X$  by  $m$ ”, i.e.

$$\sigma[m/X](Y) = \begin{cases} m & \text{if } Y = X \\ \sigma(Y) & \text{otherwise} \end{cases}$$

**Example:** consider  $\sigma$  such that  $\sigma(X) = 2$ ,  $\sigma(Y) = 4$ . Let  $\sigma'$  be  $\sigma[5/X]$ . We have that  $\sigma'(X) = 5$ ,  $\sigma'(Y) = 4$

*Atomic commands:*

$$\langle \text{skip}, \sigma \rangle \rightarrow \sigma$$

$$\frac{\langle a, \sigma \rangle \rightarrow m}{\langle X := a, \sigma \rangle \rightarrow \sigma[m/X]}$$

*Sequencing:*

$$\frac{\langle c_0, \sigma \rangle \rightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \rightarrow \sigma'}{\langle c_0 ; c_1, \sigma \rangle \rightarrow \sigma'}$$

*Conditionals:*

$$\frac{\langle b, \sigma \rangle \rightarrow \text{true} \quad \langle c_0, \sigma \rangle \rightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \rightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \text{false} \quad \langle c_1, \sigma \rangle \rightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \rightarrow \sigma'}$$

*While-loops:*

$$\frac{\langle b, \sigma \rangle \rightarrow \text{false}}{\langle \text{while } b \text{ do } c, \sigma \rangle \rightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow \text{true} \quad \langle c, \sigma \rangle \rightarrow \sigma'' \quad \langle \text{while } b \text{ do } c, \sigma'' \rangle \rightarrow \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \rightarrow \sigma'}$$

### **equivalence of commands**

$$c_0 \sim c_1 \text{ iff } (\forall \sigma, \sigma' \in \Sigma. \langle c_0, \sigma \rangle \rightarrow \sigma' \Leftrightarrow \langle c_1, \sigma \rangle \rightarrow \sigma')$$