CS101

Special Topics in Computer Science

Language-Based Security

Lecture 7: IMP — a Simple Imerative Language

Aleksey Nogin

October 26, 2005

IMP— a Simple Imperative Language

- Numbers (**N**): m, n
- Locations (**Loc**): X, Y
- Arithmetical expressions (**Aexp**):
  $a ::= n \mid X \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2$
- Boolean expressions (**Bexp**):
  $b ::= \mathbf{true} \mid \mathbf{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \mid$
  $\neg b \mid b_1 \vee b_2 \mid b_1 \wedge b_2$
- Commands (**Com**):
  $c ::= \mathbf{skip} \mid X := a \mid c_1; c_2 \mid \mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2 \mid$
  $\mathbf{while}\ b\ \mathbf{do}\ c$

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \mathbf{Loc} \to \mathbf{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \mathbf{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \mathbf{Loc} \to \mathbf{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \mathbf{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

- $\langle \sigma, n \rangle \longrightarrow$
- $\langle \sigma, X \rangle \longrightarrow$
- $\langle \sigma, a_1 + a_2 \rangle \longrightarrow$
- $\langle \sigma, a_1 - a_2 \rangle \longrightarrow$
- *etc*

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \texttt{Loc} \to \texttt{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \texttt{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

- $\langle \sigma, n \rangle \longrightarrow n$
- $\langle \sigma, X \rangle \longrightarrow$
- $\langle \sigma, a_1 + a_2 \rangle \longrightarrow$
- $\langle \sigma, a_1 - a_2 \rangle \longrightarrow$
- *etc*

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \texttt{Loc} \to \texttt{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \texttt{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

- $\langle \sigma, n \rangle \longrightarrow n$
- $\langle \sigma, X \rangle \longrightarrow \sigma(X)$
- $\langle \sigma, a_1 + a_2 \rangle \longrightarrow$
- $\langle \sigma, a_1 - a_2 \rangle \longrightarrow$
- *etc*

CS101 Lecture 7 IMP — a Simple Imerative Language October 26, 2005 – p. 3

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \texttt{Loc} \to \texttt{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \texttt{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

- $\langle \sigma, n \rangle \longrightarrow n$
- $\langle \sigma, X \rangle \longrightarrow \sigma(X)$
- $\dfrac{\langle \sigma, a_1 \rangle \longrightarrow n_1 \quad \langle \sigma, a_2 \rangle \longrightarrow n_2}{\langle \sigma, a_1 + a_2 \rangle \longrightarrow n}$, where $n = n_1 + n_2$.
- $\langle \sigma, a_1 - a_2 \rangle \longrightarrow$
- *etc*

CS101 Lecture 7 IMP — a Simple Imerative Language October 26, 2005 – p. 3

Evaluation: State

A *state* σ maps locations to numbers. $\Sigma = \texttt{Loc} \to \texttt{N}$ — set all all states. $\sigma(X)$ — contents of location X in state σ.

For $\sigma \in \Sigma$ and $a \in \texttt{Aexp}$ we will define a relation $\langle \sigma, a \rangle \longrightarrow n$:

- $\langle \sigma, n \rangle \longrightarrow n$
- $\langle \sigma, X \rangle \longrightarrow \sigma(X)$
- $\dfrac{\langle \sigma, a_1 \rangle \longrightarrow n_1 \quad \langle \sigma, a_2 \rangle \longrightarrow n_2}{\langle \sigma, a_1 + a_2 \rangle \longrightarrow n}$, where $n = n_1 + n_2$.
- $\dfrac{\langle \sigma, a_1 \rangle \longrightarrow n_1 \quad \langle \sigma, a_2 \rangle \longrightarrow n_2}{\langle \sigma, a_1 - a_2 \rangle \longrightarrow n}$, where $n = n_1 - n_2$.
- *etc*

CS101 Lecture 7 IMP — a Simple Imerative Language October 26, 2005 – p. 3

Evaluation of Booleans

- $\langle \sigma, \texttt{true} \rangle \longrightarrow \texttt{true}$ and $\langle \sigma, \texttt{false} \rangle \longrightarrow \texttt{false}$
- $\dfrac{\langle \sigma, a_1 \rangle \longrightarrow n_1 \quad \langle \sigma, a_2 \rangle \longrightarrow n_2}{\langle \sigma, a_1 = a_2 \rangle \longrightarrow \texttt{true}}$, if n_1 and n_2 are equal;
- $\dfrac{\langle \sigma, a_1 \rangle \longrightarrow n_1 \quad \langle \sigma, a_2 \rangle \longrightarrow n_2}{\langle \sigma, a_1 = a_2 \rangle \longrightarrow \texttt{false}}$, if n_1 and n_2 are unequal;
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true}}{\langle \sigma, \neg b \rangle \longrightarrow \texttt{false}}$ and $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false}}{\langle \sigma, \neg b \rangle \longrightarrow \texttt{true}}$
- *etc*

Evaluation of Commands

$\langle \sigma, c \rangle \longrightarrow ???$

Evaluation of Commands

$\langle \sigma, c \rangle \longrightarrow \sigma'$

Evaluation of Commands

$\langle \sigma, c \rangle \longrightarrow \sigma'$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow ???$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\langle \sigma, X := a \rangle \longrightarrow ???$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\langle \sigma, c_1; c_2 \rangle \longrightarrow ???$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$
- $\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow ???$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$

Evaluation of Commands

$$\langle \sigma, c \rangle \longrightarrow \sigma'$$

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow ???$

Evaluation of Commands

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma \qquad \dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow}$

Evaluation of Commands

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma \qquad \dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow}$

Evaluation of Commands

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma \qquad \dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c \rangle \longrightarrow \sigma' \quad \langle \sigma', \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma''}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow}$

Evaluation of Commands

- $\langle \sigma, \texttt{skip} \rangle \longrightarrow \sigma \qquad \dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$
- $\dfrac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1 ; c_2 \rangle \longrightarrow \sigma''}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{false}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma}$
  $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true} \quad \langle \sigma, c \rangle \longrightarrow \sigma' \quad \langle \sigma', \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma''}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \longrightarrow \sigma''}$

Small-Step Semantics

- $\langle \sigma, \texttt{skip}; c \rangle \ \rightarrow_1 \ \langle \sigma, c \rangle$
- $\dfrac{\langle \sigma, c_1 \rangle \ \rightarrow_1 \ \langle \sigma', c_1' \rangle}{\langle \sigma, c_1 ; c_2 \rangle \ \rightarrow_1 \ \langle \sigma', c_1' ; c_2 \rangle}$
- $\dfrac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \ \rightarrow_1 \ \langle \sigma[n/X], \texttt{skip} \rangle}$
- $\dfrac{\langle \sigma, b \rangle \longrightarrow \texttt{true}}{\langle \sigma, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rangle \ \rightarrow_1 \ \langle \sigma, c_1 \rangle}$
- $\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \ \rightarrow_1$
  $\langle \sigma, \texttt{if } b \texttt{ then } (c; \texttt{ while } b \texttt{ do } c) \texttt{ else skip} \rangle$