

CS101

Special Topics in Computer Science Language-Based Security

Lecture 7: IMP — a Simple Imperative Language

Aleksey Nogin

October 26, 2005



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 1

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**):
 $b ::= \text{true} \mid \text{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b \mid b_1 \vee b_2 \mid b_1 \wedge b_2$
- Commands (**Com**):
 $c ::= \text{skip} \mid X := a \mid c_1; c_2 \mid \text{if } b \text{ then } c_1 \text{ else } c_2 \mid \text{while } b \text{ do } c$



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 2

Evaluation: State

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 3

Evaluation: State

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

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 3

Evaluation: State

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

For $\sigma \in \Sigma$ and $a \in \text{Aexp}$ 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*



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 3

Evaluation: State

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

For $\sigma \in \Sigma$ and $a \in \text{Aexp}$ 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 Imperative Language

October 26, 2005 – p. 3

Evaluation: State

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

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 3

Evaluation: State

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

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 3

Evaluation of Booleans

- $\langle \sigma, \text{true} \rangle \rightarrow \text{true}$ and $\langle \sigma, \text{false} \rangle \rightarrow \text{false}$
- $\frac{\langle \sigma, a_1 \rangle \rightarrow n_1 \quad \langle \sigma, a_2 \rangle \rightarrow n_2}{\langle \sigma, a_1 = a_2 \rangle \rightarrow \text{true}}$, if n_1 and n_2 are equal;
- $\frac{\langle \sigma, a_1 \rangle \rightarrow n_1 \quad \langle \sigma, a_2 \rangle \rightarrow n_2}{\langle \sigma, a_1 = a_2 \rangle \rightarrow \text{false}}$, if n_1 and n_2 are unequal;
- $\frac{\langle \sigma, b \rangle \rightarrow \text{true}}{\langle \sigma, \neg b \rangle \rightarrow \text{false}}$ and $\frac{\langle \sigma, b \rangle \rightarrow \text{false}}{\langle \sigma, \neg b \rangle \rightarrow \text{true}}$
- etc



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 4



CS101 Lecture 7

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

Evaluation of Commands

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

$\langle \sigma, c \rangle \rightarrow \sigma'$
■ $\langle \sigma, \text{skip} \rangle \rightarrow ???$



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

- $\langle \sigma, \text{skip} \rangle \longrightarrow \sigma$
 - $$\frac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$$
 - $$\frac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$$
 - $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{true} \\ \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma' \end{array}}{\langle \sigma, b \rangle \longrightarrow \text{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'} \quad \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'$$



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

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

$$\blacksquare \frac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$$

- $\frac{\langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$
- $\frac{\langle \sigma, b \rangle \longrightarrow \text{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$

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

$$\frac{\langle \sigma, b \rangle \longrightarrow \mathbf{true}}{\langle \sigma \text{ while } b \text{ do } c \rangle \longrightarrow}$$



CS101 Lecture 7

IMB — a Simple Imperative Language

October 36, 2005 – p. 6

Evaluation of Commands

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

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



CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 5

Evaluation of Commands

$$\langle \sigma, \text{skip} \rangle \longrightarrow \sigma \quad \frac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]}$$

$$\blacksquare \frac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$$

- $\langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma'$
 $\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'$
- $\langle \sigma, b \rangle \longrightarrow \text{false} \quad \langle \sigma, c_2 \rangle \longrightarrow \sigma'$
 $\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'$

- $\frac{\langle \sigma, b \rangle \longrightarrow \text{false}}{\langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma}$

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



CS101 Lecture 7

IMR — a Simple Imperative Language

October 26, 2005 - p. 6

Evaluation of Commands

- $\langle \sigma, \text{skip} \rangle \longrightarrow \sigma \quad \langle \sigma, a \rangle \longrightarrow n \quad \langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]$
- $$\frac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma' \\ \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma' \end{array}}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{false} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma' \\ \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma' \end{array}}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{false} \\ \langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma \end{array}}{\langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma}$$
- $$\frac{\langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c \rangle \longrightarrow \sigma' \quad \langle \sigma', \text{while } b \text{ do } c \rangle \longrightarrow \sigma''}{\langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma''}$$

CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 6

Small-Step Semantics

- $\langle \sigma, \text{skip}; c \rangle \rightarrow_1 \langle \sigma, c \rangle$
- $$\frac{\langle \sigma, c_1 \rangle \rightarrow_1 \langle \sigma', c'_1 \rangle}{\langle \sigma, c_1; c_2 \rangle \rightarrow_1 \langle \sigma', c'_1; c_2 \rangle}$$
- $$\frac{\langle \sigma, a \rangle \longrightarrow n}{\langle \sigma, X := a \rangle \rightarrow_1 \langle \sigma[n/X], \text{skip} \rangle}$$
- $$\frac{\langle \sigma, b \rangle \longrightarrow \text{true}}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \rightarrow_1 \langle \sigma, c_1 \rangle}$$
- $$\frac{\langle \sigma, \text{while } b \text{ do } c \rangle \rightarrow_1 \langle \sigma, \text{if } b \text{ then } (c; \text{while } b \text{ do } c) \text{ else skip} \rangle}{\langle \sigma, \text{if } b \text{ then } (c; \text{while } b \text{ do } c) \text{ else skip} \rangle}$$

CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 7

Evaluation of Commands

- $\langle \sigma, \text{skip} \rangle \longrightarrow \sigma \quad \langle \sigma, a \rangle \longrightarrow n \quad \langle \sigma, X := a \rangle \longrightarrow \sigma[n/X]$
- $$\frac{\langle \sigma, c_1 \rangle \longrightarrow \sigma' \quad \langle \sigma', c_2 \rangle \longrightarrow \sigma''}{\langle \sigma, c_1; c_2 \rangle \longrightarrow \sigma''}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma' \\ \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma' \end{array}}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{false} \quad \langle \sigma, c_1 \rangle \longrightarrow \sigma' \\ \langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma' \end{array}}{\langle \sigma, \text{if } b \text{ then } c_1 \text{ else } c_2 \rangle \longrightarrow \sigma'}$$
- $$\frac{\begin{array}{l} \langle \sigma, b \rangle \longrightarrow \text{false} \\ \langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma \end{array}}{\langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma}$$
- $$\frac{\langle \sigma, b \rangle \longrightarrow \text{true} \quad \langle \sigma, c \rangle \longrightarrow \sigma' \quad \langle \sigma', \text{while } b \text{ do } c \rangle \longrightarrow \sigma''}{\langle \sigma, \text{while } b \text{ do } c \rangle \longrightarrow \sigma''}$$

CS101 Lecture 7

IMP — a Simple Imperative Language

October 26, 2005 – p. 6