Concepts of Programming Languages – Recitation 3: More Natural Operational Semantics

Oded Padon
odedp@mail.tau.ac.il

Reference:
Semantics with Applications by H. Nielson and F. Nielson – Ch. 2
http://www.daimi.au.dk/~bra8130/Wiley_book/wiley.html

The **While** Programming Language

- Abstract syntax
  S::= x := a | **skip** | S_1 ; S_2 | **if** b **then** S_1 **else** S_2 |
  while b do S
- Use parenthesizes for precedence
- Informal Semantics
  - **skip** behaves like no-operation
  - Import meaning of arithmetic and Boolean operations

Natural Operational Semantics

- Notations:
  - S – program construct (word in the While language)
  - s, s' – states (functions Var $\rightarrow$ N)
- <S, s> $\rightarrow$ s' means:
  If S is executed on state s, it terminates and the state after execution is s'
- Describe the "overall" effect of program constructs
- Ignores non terminating computations

Formally defining $\rightarrow$

- $\rightarrow$ is defined **inductively** using **inference rules**, with both **syntactic** conditions on S and **semantic** conditions on s

$$[\text{ass}_{\text{ns}}] \quad \langle x := a, s\rangle \rightarrow s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$[\text{skip}_{\text{ns}}] \quad \langle \texttt{skip}, s\rangle \rightarrow s$$

$$[\text{comp}_{\text{ns}}] \quad \frac{\langle S_1, s\rangle \rightarrow s', \langle S_2, s'\rangle \rightarrow s''}{\langle S_1;S_2, s\rangle \rightarrow s''}$$

$$[\text{if}^{\text{tt}}_{\text{ns}}] \quad \frac{\langle S_1, s\rangle \rightarrow s'}{\langle \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2, s\rangle \rightarrow s'} \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$[\text{if}^{\text{ff}}_{\text{ns}}] \quad \frac{\langle S_2, s\rangle \rightarrow s'}{\langle \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2, s\rangle \rightarrow s'} \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

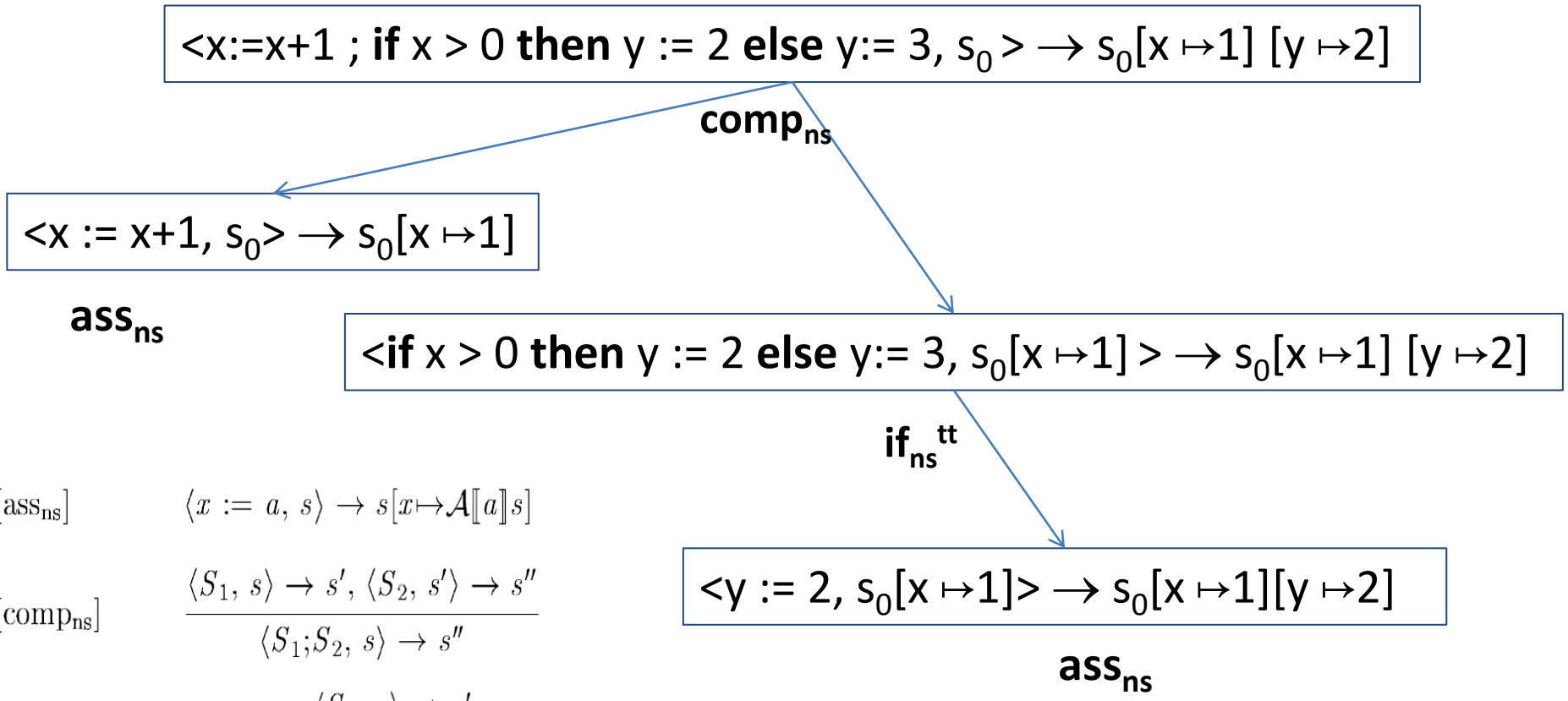
$$[\text{while}^{\text{tt}}_{\text{ns}}] \quad \frac{\langle S, s\rangle \rightarrow s', \langle \texttt{while } b \texttt{ do } S, s'\rangle \rightarrow s''}{\langle \texttt{while } b \texttt{ do } S, s\rangle \rightarrow s''} \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$[\text{while}^{\text{ff}}_{\text{ns}}] \quad \langle \texttt{while } b \texttt{ do } S, s\rangle \rightarrow s \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

Derivation Trees

- A derivation tree is a way to write applications of inference rules
- A derivation tree is a "proof" that <S, s> $\rightarrow$s'
- The root of tree is <S, s> $\rightarrow$s'
- Each node is a conclusion from its children using an inference rule
- Leaves are instances of axioms (rules with no premises)
- Non-leaves are instances of inference rules with premises
  - Immediate children match rule premises
  - The semantic condition is satisfied

Example Derivation Tree



$$[\text{ass}_{\text{ns}}] \qquad \langle x := a,\ s\rangle \to s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$[\text{comp}_{\text{ns}}] \qquad \frac{\langle S_1,\ s\rangle \to s',\ \langle S_2,\ s'\rangle \to s''}{\langle S_1; S_2,\ s\rangle \to s''}$$

$$[\text{if}^{\text{tt}}_{\text{ns}}] \qquad \frac{\langle S_1,\ s\rangle \to s'}{\langle \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2,\ s\rangle \to s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \text{tt}$$

$$[\text{if}^{\text{ff}}_{\text{ns}}] \qquad \frac{\langle S_2,\ s\rangle \to s'}{\langle \texttt{if } b \texttt{ then } S_1 \texttt{ else } S_2,\ s\rangle \to s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \text{ff}$$

Alternative Notation

$$\textbf{ass}_{ns}\ \frac{}{\langle y := 2,\ s_0[x \mapsto 1]\rangle \rightarrow s_0[x \mapsto 1][y \mapsto 2]}$$

$$\textbf{ass}_{ns}\ \frac{}{\langle x := x+1,\ s_0\rangle \rightarrow s_0[x \mapsto 1]} \qquad \frac{}{\langle \textbf{if } x > 0 \textbf{ then } y := 2 \textbf{ else } y := 3,\ s_0[x \mapsto 1]\rangle \rightarrow s_0[x \mapsto 1]\ [y \mapsto 2]}\ \textbf{if}_{ns}^{tt}$$

$$\textbf{comp}_{ns}\ \frac{}{\langle x := x+1 \ ;\ \textbf{if } x > 0 \textbf{ then } y := 2 \textbf{ else } y := 3,\ s_n\rangle \rightarrow s_0[x \mapsto 1]\ [y \mapsto 2]}$$

$$[\mathrm{ass}_{\mathrm{ns}}] \qquad \langle x := a,\ s\rangle \rightarrow s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$[\mathrm{comp}_{\mathrm{ns}}] \qquad \frac{\langle S_1,\ s\rangle \rightarrow s',\ \langle S_2,\ s'\rangle \rightarrow s''}{\langle S_1; S_2,\ s\rangle \rightarrow s''}$$

$$[\mathrm{if}_{\mathrm{ns}}^{\mathrm{tt}}] \qquad \frac{\langle S_1,\ s\rangle \rightarrow s'}{\langle \mathtt{if}\ b\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2,\ s\rangle \rightarrow s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \mathrm{tt}$$

$$[\mathrm{if}_{\mathrm{ns}}^{\mathrm{ff}}] \qquad \frac{\langle S_2,\ s\rangle \rightarrow s'}{\langle \mathtt{if}\ b\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2,\ s\rangle \rightarrow s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \mathrm{ff}$$

Semantic Equivalence

- Two statements S_1 and S_2 are **semantically equivalent** ($S_1 \approx S_2$) if for any two states s, s' we have:

$$<S_1, s> \rightarrow s' \quad \textbf{iff} \quad <S_2, s> \rightarrow s'$$

- Examples:
  - S ; skip ≈ S ?
  - skip ; S ≈ S ?
  - S1 ; S2 ≈ S2 ; S1 ?
  - (S1 ; S2) ; S3) ≈ (S1 ;(S2 ; S3)) ?
  - x := 2 ; y := x + 3 ≈ y := 5; x := 2 ?
  - while b do S ≈ if b then (S ; while b do S) else skip ?
  - while true do x:=x+1 ≈ while true do x:=x+2 ?

Proving Semantic Equivalence

- Two statements S_1 and S_2 are **semantically equivalent** ($S_1 \approx S_2$) if for any two states s, s' we have:

$$<S_1, s> \rightarrow s' \quad \textbf{iff} \quad <S_2, s> \rightarrow s'$$

- To prove semantic equivalence:
  1. Assume $<S_1, s> \rightarrow s'$, show $<S_2, s> \rightarrow s'$
  2. Assume $<S_2, s> \rightarrow s'$, show $<S_1, s> \rightarrow s'$

- The proof is usually by manipulating derivation trees

Example: S ; skip ≈ S

- To prove semantic equivalence:
  1. Assume <S, s> $\rightarrow$ s' , show <S;skip, s> $\rightarrow$ s'
  2. Assume <S;skip, s> $\rightarrow$ s' , show <S, s> $\rightarrow$ s'

1.

$$\frac{T}{\langle S, s\rangle \rightarrow s'} \Rightarrow \frac{\dfrac{T}{\langle S, s\rangle \rightarrow s'} \qquad \dfrac{}{\langle skip, s'\rangle \rightarrow s'}\ \textbf{skip}_{ns}}{\langle S;skip, s\rangle \rightarrow s'}\ \textbf{comp}_{ns}$$

Example: S ; skip ≈ S

- To prove semantic equivalence:
  1. Assume <S, s> $\rightarrow$ s' , show <S;skip, s> $\rightarrow$ s'
  2. Assume <S;skip, s> $\rightarrow$ s' , show <S, s> $\rightarrow$ s'

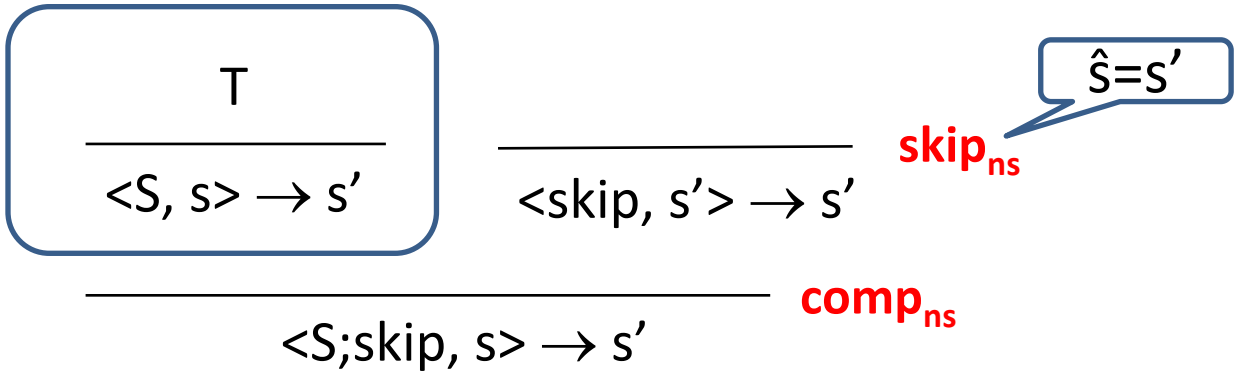
2.

$$\dfrac{\dfrac{T}{\langle S, s\rangle \rightarrow \hat{s}} \qquad \dfrac{}{\langle skip, \hat{s}\rangle \rightarrow s'}\ \textbf{skip}_{ns}}{\langle S;skip, s\rangle \rightarrow s'}\ \textbf{comp}_{ns}$$

Example: S ; skip ≈ S

- To prove semantic equivalence:
  1. Assume <S, s> → s' , show <S;skip, s> → s'
  2. Assume <S;skip, s> → s' , show <S, s> → s'

2.



Example: while loop

Prove: while b do S $\approx$ if b then (S ; while b do S) else skip

W

1. Assume <W, s> $\rightarrow$ s'' , show < if b then (S ; W) else skip, s> $\rightarrow$ s''
   Two cases:

$$\frac{T_1 \qquad T_2}{\dfrac{\langle S, s\rangle \rightarrow s' \qquad \langle \text{while b do S}, s'\rangle \rightarrow s''}{\langle \text{while b do S}, s\rangle \rightarrow s''}\ \textbf{while}_{ns}^{tt}}$$

$\mathcal{B}$[b] s = **tt**

$$\frac{}{\langle \text{while b do S}, s\rangle \rightarrow s}\ \textbf{while}_{ns}^{ff}$$

$\mathcal{B}$[b] s = **ff**

s = s''

$$[\text{while}_{ns}^{tt}] \qquad \frac{\langle S, s\rangle \rightarrow s', \langle \texttt{while}\ b\ \texttt{do}\ S, s'\rangle \rightarrow s''}{\langle \texttt{while}\ b\ \texttt{do}\ S, s\rangle \rightarrow s''} \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$[\text{while}_{ns}^{ff}] \qquad \langle \texttt{while}\ b\ \texttt{do}\ S, s\rangle \rightarrow s \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

Case $\textbf{while}_{ns}^{ff}$

$$\frac{}{\langle \text{while b do S}, s\rangle \to s}\ \textbf{while}_{ns}^{ff} \qquad \mathcal{B}[\![b]\!]\, s = \textbf{ff}, \quad s = s''$$

$$\frac{}{\langle \text{skip}, s\rangle \to s}\ \textbf{skip}_{ns}$$

$$\frac{}{\langle \text{if b then (S;W) else skip}, s\rangle \to s}\ \textbf{if}_{ns}^{ff}$$

$$[\text{if}_{\text{ns}}^{\text{tt}}] \quad \frac{\langle S_1,\ s\rangle \to s'}{\langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2,\ s\rangle \to s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$[\text{if}_{\text{ns}}^{\text{ff}}] \quad \frac{\langle S_2,\ s\rangle \to s'}{\langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2,\ s\rangle \to s'} \quad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

Case $\textbf{while}_{\textbf{ns}}^{\textbf{tt}}$

$$\dfrac{\dfrac{T_1}{\langle S, s\rangle \to s'} \quad \dfrac{T_2}{\langle \text{while b do S}, s'\rangle \to s''}}{\langle \text{while b do S}, s\rangle \to s''}\ \textbf{while}_{\textbf{ns}}^{\textbf{tt}} \qquad \mathcal{B}[\![b]\!]\, s = \textbf{tt}$$

$$\dfrac{\dfrac{\dfrac{T_1}{\langle S, s\rangle \to s'} \quad \dfrac{T_2}{\langle W, s'\rangle \to s''}}{\langle S;W, s\rangle \to s''}\ \textbf{comp}_{\textbf{ns}}}{\langle \text{if b then (S;W) else skip}, s\rangle \to s''}\ \textbf{if}_{\textbf{ns}}^{\textbf{tt}}$$

Direction 2

2. Assume < if b then (S ; W) else skip, s> $\rightarrow$ s'', show <W, s> $\rightarrow$ s''
   Two cases:

$$\dfrac{\dfrac{\dfrac{T_3}{\langle S, s\rangle \rightarrow s'} \quad \dfrac{T_4}{\langle W, s'\rangle \rightarrow s''}}{\langle S;W, s\rangle \rightarrow s''}\ \mathbf{comp}_{ns}}{\langle \text{if b then (S;W) else skip}, s\rangle \rightarrow s''}\ \mathbf{if}_{ns}^{tt}$$

$\mathcal{B}$[b] s = **tt**

$$\dfrac{\dfrac{}{\langle \text{skip}, s\rangle \rightarrow s}\ \mathbf{skip}_{ns}}{\langle \text{if b then (S;W) else skip}, s\rangle \rightarrow s}\ \mathbf{if}_{ns}^{ff}$$

$\mathcal{B}$[b] s = **ff**

s = s''

Case $\mathbf{if}_{ns}^{ff}$

$$\frac{}{\langle skip, s\rangle \rightarrow s}\ \mathbf{skip}_{ns}$$

$$\frac{}{\langle \text{if b then (S;W) else skip}, s\rangle \rightarrow s}\ \mathbf{if}_{ns}^{ff}$$

$\mathcal{B}$[b] s = **ff**

s = s''

$$\frac{}{\langle \text{while b do S}, s\rangle \rightarrow s}\ \mathbf{while}_{ns}^{ff}$$

Case $\mathbf{if}_{ns}^{tt}$

$$\dfrac{\dfrac{\dfrac{T_3}{\langle S, s\rangle \to s'} \quad \dfrac{T_4}{\langle W, s'\rangle \to s''}}{\langle S;W, s\rangle \to s''}\ \mathbf{comp}_{ns}}{\langle \text{if } b \text{ then } (S;W) \text{ else skip}, s\rangle \to s''}\ \mathbf{if}_{ns}^{tt}$$

$\mathcal{B}[b]\ s = \mathbf{tt}$

$$\dfrac{\dfrac{T_3}{\langle S, s\rangle \to s'} \quad \dfrac{T_4}{\langle \text{while } b \text{ do } S, s'\rangle \to s''}}{\langle \text{while } b \text{ do } S, s\rangle \to s''}\ \mathbf{while}_{ns}^{tt}$$

Adding Semantics of Conditions with Side Effects

Add semantics of:

$$\text{if } (x:=e) \text{ then } S_1 \text{ else } S_2$$

$$\textbf{if-ass}_{ns}^{tt} \quad \frac{\langle x:=e , s\rangle \rightarrow s' \qquad \langle S_1 , s'\rangle \rightarrow s''}{\langle \text{if } (x:=e) \text{ then } S_1 \text{ else } S_2, s\rangle \rightarrow s''} \qquad \text{if } \mathbf{A}[\![x]\!]s' \neq 0$$

$$\textbf{if-ass}_{ns}^{ff} \quad \frac{\langle x:=e , s\rangle \rightarrow s' \qquad \langle S_2 , s'\rangle \rightarrow s''}{\langle \text{if } (x:=e) \text{ then } S_1 \text{ else } S_2, s\rangle \rightarrow s''} \qquad \text{if } \mathbf{A}[\![x]\!]s' = 0$$

Adding Semantics of 3-Way Case

Add semantics of:

$$\text{case } (b_1: S_1),(b_2: S_2),(\text{else}: S_3)$$

$$\textbf{case}_{ns}^{1} \quad \frac{\langle S_1 , s\rangle \rightarrow s'}{\langle \text{case } (b_1: S_1),(b_2: S_2),(\text{else}: S_3) , s\rangle \rightarrow s'} \quad \text{if } \mathbf{B}[\![b_1]\!]s = \mathbf{tt}$$

$$\textbf{case}_{ns}^{2} \quad \frac{\langle S_2 , s\rangle \rightarrow s'}{\langle \text{case } (b_1: S_1),(b_2: S_2),(\text{else}: S_3) , s\rangle \rightarrow s'} \quad \text{if } \mathbf{B}[\![b_1]\!]s = \mathbf{ff} \text{ and } \mathbf{B}[\![b_2]\!]s = \mathbf{tt}$$

$$\textbf{case}_{ns}^{\text{else}} \quad \frac{\langle S_3 , s\rangle \rightarrow s'}{\langle \text{case } (b_1: S_1),(b_2: S_2),(\text{else}: S_3) , s\rangle \rightarrow s'} \quad \text{if } \mathbf{B}[\![b_1]\!]s = \mathbf{ff} \text{ and } \mathbf{B}[\![b_2]\!]s = \mathbf{ff}$$