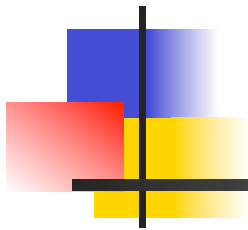


# CS477 Formal Software Development Methods



---

Elsa L Gunter  
2112 SC, UIUC

Based in part on slides used in CS 421 FA 2019



# Model Theory for Hoare Logic

---

- Seen Proof Theory for Hoare Logic
- What are its Models?
- Need a notion of evaluation
- Need a notion of state
- $\{P\} C \{Q\}$   
means for all states  $m_1$  and  $m_2$  if  $m_1$  satisfies (models)  $P$  and starts in  $m_1$  and evaluates ending in  $m_2$  then  $m_2$  satisfies  $Q$
- But what is “evaluates”?



# Natural Semantics

---

- Aka Structural Operational Semantics, aka “Big Step Semantics”
- Provide value for a program by rules and derivations, similar to provability
- Rule conclusions look like

$$(C, m) \Downarrow m'$$

or

$$(E, m) \Downarrow v$$



# Simple Imperative Programming Language

---

- $I \in \textit{Identifiers}$
- $N \in \textit{Numerals}$
- $E ::= N \mid I \mid E + E \mid E * E \mid E - E$
- $B ::= \text{true} \mid \text{false} \mid B \ \& \ B \mid B \ \text{or} \ B \mid \text{not } B$   
|  $E < E \mid E = E$
- $C ::= C; C \mid I := E \mid \text{if } B \text{ then } C \text{ else } C \text{ fi}$   
|  $\text{while } B \text{ do } C \text{ od}$



# Natural Semantics of Atomic Expressions

---

- Identifiers:  $(I, m) \Downarrow m(I)$
- Numerals are values:  $(N, m) \Downarrow N$
- Booleans:  $(\text{true}, m) \Downarrow \text{true}$   
 $(\text{false}, m) \Downarrow \text{false}$



# Arithmetic Expressions

---

$$\frac{(E, m) \Downarrow U \quad (E', m) \Downarrow V \quad U \text{ op } V = N}{(E \text{ op } E', m) \Downarrow N}$$

where  $N$  is the specified value for  $U \text{ op } V$   
 $\text{op}$  in  $\{ +, *, - \}$

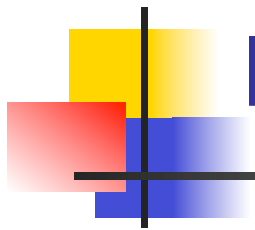


# Relations

---

$$\frac{(E, m) \Downarrow U \quad (E', m) \Downarrow V \quad U \sim V = b}{(E \sim E', m) \Downarrow b}$$

- By  $U \sim V = b$ , we mean does (the meaning of) the relation  $\sim$  hold on the meaning of  $U$  and  $V$
- May be specified by a mathematical expression/equation or rules matching  $U$  and  $V$



# Booleans:

$$\frac{(B, m) \Downarrow \text{false}}{(B \& B', m) \Downarrow \text{false}}$$

$$\frac{(B, m) \Downarrow \text{true} \quad (B', m) \Downarrow b}{(B \& B', m) \Downarrow b}$$

$$\frac{(B, m) \Downarrow \text{true}}{(B \text{ or } B', m) \Downarrow \text{true}}$$

$$\frac{(B, m) \Downarrow \text{false} \quad (B', m) \Downarrow b}{(B \text{ or } B', m) \Downarrow b}$$

$$\frac{(B, m) \Downarrow \text{true}}{(\text{not } B, m) \Downarrow \text{false}}$$

$$\frac{(B, m) \Downarrow \text{false}}{(\text{not } B, m) \Downarrow \text{true}}$$





# Commands

---

Skip:  $(\text{skip}, m) \Downarrow m$

Assignment: 
$$\frac{(E, m) \Downarrow V}{(I := E, m) \Downarrow m + [I \mapsto V]}$$

Sequencing: 
$$\frac{(C, m) \Downarrow m' \quad (C', m') \Downarrow m''}{(C; C', m) \Downarrow m''}$$



## If Then Else Command

---

$$\frac{(B, m) \Downarrow \text{true} \quad (C, m) \Downarrow m'}{(\text{if } B \text{ then } C \text{ else } C' \text{ fi}, m) \Downarrow m'}$$

$$\frac{(B, m) \Downarrow \text{false} \quad (C', m) \Downarrow m'}{(\text{if } B \text{ then } C \text{ else } C' \text{ fi}, m) \Downarrow m'}$$



# While Command

---

$$(B, m) \Downarrow \text{false}$$

---

$$(\text{while } B \text{ do } C \text{ od}, m) \Downarrow m$$
$$(B, m) \Downarrow \text{true} \quad (C, m) \Downarrow m' \quad (\text{while } B \text{ do } C \text{ od}, m') \Downarrow m''$$

---

$$(\text{while } B \text{ do } C \text{ od}, m) \Downarrow m''$$



## Example: If Then Else Rule

---

---

(if  $x > 5$  then  $y := 2 + 3$  else  $y := 3 + 4$  fi,  
 $\{x \rightarrow 7\}) \Downarrow ?$



# Example: If Then Else Rule

---

---

$(x > 5, \{x \rightarrow 7\}) \Downarrow ?$

---

$(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?$



# Example: Arith Relation

---

? > ? = ?

$(x, \{x \rightarrow 7\}) \Downarrow ? \quad (5, \{x \rightarrow 7\}) \Downarrow ?$

---

$(x > 5, \{x \rightarrow 7\}) \Downarrow ?$

---

(if  $x > 5$  then  $y := 2 + 3$  else  $y := 3 + 4$  fi,  
 $\{x \rightarrow 7\}) \Downarrow ?$



## Example: Identifier(s)

---

$7 > 5 = \text{true}$

$(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5$

$(x > 5, \{x \rightarrow 7\}) \Downarrow ?$

---

$(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?$



# Example: Arith Relation

---

$7 > 5 = \text{true}$

$(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5$

---

$(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}$

---

$(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?$





# Example: If Then Else Rule

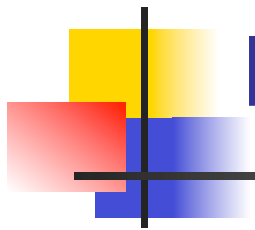
---

$7 > 5 = \text{true}$

$\frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}}$

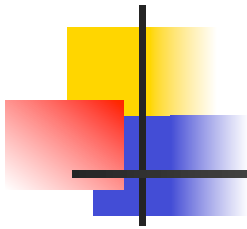
$\frac{(y := 2 + 3, \{x \rightarrow 7\}) \Downarrow ?}{(y := 2 + 3, \{x \rightarrow 7\}) \Downarrow ?}$

$\frac{(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true} \quad (y := 2 + 3, \{x \rightarrow 7\}) \Downarrow ?}{(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?}$



# Example: Assignment

$$\begin{array}{c}
 7 > 5 = \text{true} \\
 \hline
 (x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5 \\
 \hline
 (x > 5, \{x \rightarrow 7\}) \Downarrow \text{true} \\
 \hline
 (\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi,} \\
 \{x \rightarrow 7\}) \Downarrow ?
 \end{array}
 \qquad
 \begin{array}{c}
 \hline
 (2+3, \{x \rightarrow 7\}) \Downarrow ? \\
 \hline
 (y := 2 + 3, \{x \rightarrow 7\}) \\
 \Downarrow ? \\
 \hline
 \end{array}$$



# Example: Arith Op

$$? + ? = ?$$

$$\frac{(2, \{x \rightarrow 7\}) \Downarrow ? \quad (3, \{x \rightarrow 7\}) \Downarrow ?}{}$$

$$7 > 5 = \text{true}$$

$$\frac{(2+3, \{x \rightarrow 7\}) \Downarrow ?}{}$$

$$\frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{}$$

$$(y := 2 + 3, \{x \rightarrow 7\}) \Downarrow ?$$

$$(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}$$

$$\Downarrow ?$$

$$\frac{(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true} \quad (y := 2 + 3, \{x \rightarrow 7\}) \Downarrow ?}{(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?}$$



# Example: Numerals

---

$$2 + 3 = 5$$

$$\frac{(2, \{x \rightarrow 7\}) \Downarrow 2 \quad (3, \{x \rightarrow 7\}) \Downarrow 3}{\quad}$$

$$7 > 5 = \text{true}$$

$$\frac{(2+3, \{x \rightarrow 7\}) \Downarrow ?}{\quad}$$

$$\frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{\quad}$$

$$(y := 2 + 3, \{x \rightarrow 7\})$$

$$(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}$$

$$\Downarrow ?$$

$$\frac{\quad}{(\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi,}$$

$$\{x \rightarrow 7\}) \Downarrow ?$$



# Example: Arith Op

---

$$2 + 3 = 5$$

$$\frac{(2, \{x \rightarrow 7\}) \Downarrow 2 \quad (3, \{x \rightarrow 7\}) \Downarrow 3}{\quad}$$

$$7 > 5 = \text{true}$$

$$\frac{(2+3, \{x \rightarrow 7\}) \Downarrow 5}{\quad}$$

$$\frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{\quad}$$

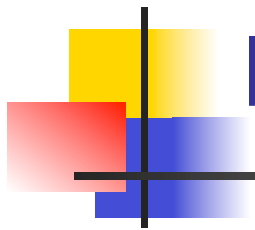
$$(y := 2 + 3, \{x \rightarrow 7\})$$

$$(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}$$

$$\Downarrow ?$$

---


$$(if\ x > 5\ then\ y := 2 + 3\ else\ y := 3 + 4\ fi,\ \{x \rightarrow 7\}) \Downarrow ?$$



# Example: Assignment

$$2 + 3 = 5$$

$$\frac{(2, \{x \rightarrow 7\}) \Downarrow 2 \quad (3, \{x \rightarrow 7\}) \Downarrow 3}{\quad}$$

$$7 > 5 = \text{true}$$

$$\frac{(2+3, \{x \rightarrow 7\}) \Downarrow 5}{\quad}$$

$$\frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{\quad}$$

$$(y := 2 + 3, \{x \rightarrow 7\})$$

$$(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}$$

$$\Downarrow \{x \rightarrow 7, y \rightarrow 5\}$$

$$\frac{(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true} \quad (y := 2 + 3, \{x \rightarrow 7\}) \Downarrow \{x \rightarrow 7, y \rightarrow 5\}}{\text{(if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi, } \{x \rightarrow 7\}) \Downarrow ?}$$

# Example: If Then Else Rule

$$\begin{array}{c}
 2 + 3 = 5 \\
 \frac{(2, \{x \rightarrow 7\}) \Downarrow 2 \quad (3, \{x \rightarrow 7\}) \Downarrow 3}{(2+3, \{x \rightarrow 7\}) \Downarrow 5} \\
 7 > 5 = \text{true} \\
 \frac{(x, \{x \rightarrow 7\}) \Downarrow 7 \quad (5, \{x \rightarrow 7\}) \Downarrow 5}{(x > 5, \{x \rightarrow 7\}) \Downarrow \text{true}} \quad \frac{(y := 2 + 3, \{x \rightarrow 7\}) \Downarrow 5}{\Downarrow \{x \rightarrow 7, y \rightarrow 5\}} \\
 \hline
 (\text{if } x > 5 \text{ then } y := 2 + 3 \text{ else } y := 3 + 4 \text{ fi,} \\
 \{x \rightarrow 7\}) \Downarrow \{x \rightarrow 7, y \rightarrow 5\}
 \end{array}$$