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

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

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

where N is the specified value for $U \; op \; V$

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:

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

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

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

Commands

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

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

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

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

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

Example: If Then Else Rule

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

Example: If Then Else Rule

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

Example: Arith Relation

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

Example: Identifier(s)

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

Example: Arith Relation

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

Example: If Then Else Rule

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

Example: Assignment

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

Example: Arith Op

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

Example: Numerals

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

Example: Arith Op

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

Example: Assignment

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

Example: If Then Else Rule

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