

1. Exercise sheet *Semantics and Verification of Software WS0809*

Due to Mon., 27 Oct. 2008, *before* the exercise course begins.

Exercise 1.1:

(2 points)

In this exercise we will discuss *alternative evaluation strategies* for Boolean expressions.

- (a) *Sequential evaluation*: Define operational rules for Boolean expressions of the form $b_1 \wedge b_2$ and $b_1 \vee b_2$ which do *not* evaluate b_2 provided that the value of b_1 is **false** (**true**, respectively). (In these cases, the value of b_2 does not contribute to the overall result.)
- (b) *Parallel evaluation*: Define operational rules which evaluate a Boolean expression of the form $b_1 \vee b_2$ to **true** if b_1 or b_2 evaluates to **true**, and which do not evaluate b_2 (b_1 , respectively) in this case.

Solution

Definition from the lecture:

$$\frac{\langle b_1, \sigma \rangle \rightarrow t_1 \quad \langle b_2, \sigma \rangle \rightarrow t_2}{\langle b_1 \wedge b_2, \sigma \rangle \rightarrow t} \quad \text{where } t = t_1 \wedge t_2$$

Sequential evaluation:

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{false}}{\langle b_1 \wedge b_2, \sigma \rangle \rightarrow \text{false}}$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{true} \quad \langle b_2, \sigma \rangle \rightarrow t_2}{\langle b_1 \wedge b_2, \sigma \rangle \rightarrow t_2}$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{true}}{\langle b_1 \vee b_2, \sigma \rangle \rightarrow \text{true}}$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{false} \quad \langle b_2, \sigma \rangle \rightarrow t_2}{\langle b_1 \vee b_2, \sigma \rangle \rightarrow t_2}$$

Parallel evaluation:

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{true}}{\langle b_1 \vee b_2, \sigma \rangle \rightarrow \text{true}}$$

$$\frac{\langle b_2, \sigma \rangle \rightarrow \text{true}}{\langle b_1 \vee b_2, \sigma \rangle \rightarrow \text{true}}$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow \text{false} \quad \langle b_2, \sigma \rangle \rightarrow \text{false}}{\langle b_1 \vee b_2, \sigma \rangle \rightarrow \text{false}}$$

□

Exercise 1.2:

(2+2 points)

In the lecture we have defined a so-called *bigstep semantics* for expressions, i.e., a relation $\rightarrow \subseteq (AExp \cup BExp) \times \Sigma \times (\mathbb{Z} \cup \mathbb{B})$ which yields the value of an expression within one step: $\langle (3 + 3) * (9 - 2), \sigma \rangle \rightarrow 42$. (Thus the intermediate results of the computation are “hidden” in the derivation tree.)

Alternatively it is possible to explicitly represent the intermediate steps by defining a *single-step semantics*: $\langle (3 + 3) * (9 - 2), \sigma \rangle \rightarrow \langle 6 * (9 - 2), \sigma \rangle \rightarrow \langle 6 * 7, \sigma \rangle \rightarrow \langle 42, \sigma \rangle \rightarrow 42$. Give a complete specification of the single-step relation

(a) $\rightarrow_1^a \subseteq (AExp \times \Sigma) \times (AExp \times \Sigma \cup \mathbb{Z})$ for arithmetic expressions and

(b) $\rightarrow_1^b \subseteq (BExp \times \Sigma) \times (BExp \times \Sigma \cup \mathbb{B})$ for Boolean expressions.

Solution

Arithmetic expressions: $z, x, -, +, *$

$$(Az) \quad \frac{}{\langle z, \sigma \rangle \rightarrow_1^a z}$$

$$(Ax) \quad \frac{}{\langle x, \sigma \rangle \rightarrow_1^a \langle \sigma(x), \sigma \rangle}$$

$$(A-1) \quad \frac{\langle a_1, \sigma \rangle \rightarrow_1^a \langle a'_1, \sigma \rangle}{\langle a_1 - a_2, \sigma \rangle \rightarrow_1^a \langle a'_1 - a_2, \sigma \rangle}$$

$$(A-2) \quad \frac{\langle a_2, \sigma \rangle \rightarrow_1^a \langle a'_2, \sigma \rangle}{\langle z_1 - a_2, \sigma \rangle \rightarrow_1^a \langle z_1 - a'_2, \sigma \rangle} \quad \text{Note: The 2nd expression is not evaluated until the 1st one is!}$$

$$(A-3) \quad \frac{}{\langle z_1 - z_2, \sigma \rangle \rightarrow_1^a \langle z, \sigma \rangle} \quad \text{where } z = z_1 - z_2$$

For addition and product, just replace $-$ by $+$, $*$ respectively.

Boolean expressions: $t, =, \leq, \neg, \wedge, \vee$

$$(Bt) \quad \overline{\langle t, \sigma \rangle \rightarrow_1^b t}$$

$$(B = 1) \quad \frac{\langle b_1, \sigma \rangle \rightarrow_1^b \langle b'_1, \sigma \rangle}{\langle b_1 = b_2, \sigma \rangle \rightarrow_1^b \langle b'_1 = b_2, \sigma \rangle}$$

$$(B = 2) \quad \frac{\langle b_2, \sigma \rangle \rightarrow_1^b \langle b'_2, \sigma \rangle}{\langle z_1 = b_2, \sigma \rangle \rightarrow_1^b \langle z_1 = b'_2, \sigma \rangle}$$

Note: The 2nd expression is not evaluated until the 1st one is!

$$(B = \text{true}) \quad \overline{\langle z = z, \sigma \rangle \rightarrow_1^b \langle \text{true}, \sigma \rangle}$$

$$(B = \text{false}) \quad \overline{\langle z_1 = z_2, \sigma \rangle \rightarrow_1^b \langle \text{false}, \sigma \rangle} \quad \text{where } z_1 \neq z_2$$

$$(B\neg 1) \quad \frac{\langle b, \sigma \rangle \rightarrow_1^b \langle b', \sigma \rangle}{\langle \neg b, \sigma \rangle \rightarrow_1^b \langle \neg b', \sigma \rangle}$$

$$(B\neg\text{false}) \quad \overline{\langle \neg\text{true}, \sigma \rangle \rightarrow_1^b \langle \text{false}, \sigma \rangle}$$

$$(B\neg\text{true}) \quad \overline{\langle \neg\text{false}, \sigma \rangle \rightarrow_1^b \langle \text{true}, \sigma \rangle}$$

$$(B \wedge 1) \quad \frac{\langle b_1, \sigma \rangle \rightarrow_1^b \langle b'_1, \sigma \rangle}{\langle b_1 \wedge b_2, \sigma \rangle \rightarrow_1^b \langle b'_1 \wedge b_2, \sigma \rangle}$$

$$(B \wedge 2) \quad \frac{\langle b_2, \sigma \rangle \rightarrow_1^b \langle b'_2, \sigma \rangle}{\langle t_1 \wedge b_2, \sigma \rangle \rightarrow_1^b \langle t_1 \wedge b'_2, \sigma \rangle}$$

$$(B \wedge \text{true}) \quad \overline{\langle \text{true} \wedge \text{true}, \sigma \rangle \rightarrow_1^b \langle \text{true}, \sigma \rangle}$$

$$(B \wedge \text{false}1) \quad \overline{\langle \text{false} \wedge t_2, \sigma \rangle \rightarrow_1^b \langle \text{false}, \sigma \rangle}$$

$$(B \wedge \text{false}2) \quad \overline{\langle t_1 \wedge \text{false}, \sigma \rangle \rightarrow_1^b \langle \text{false}, \sigma \rangle}$$

For \leq and \vee analogously.

Example: $(x + 3) * (y - 2)$ with $\sigma(x) = 3$ and $\sigma(y) = 9$:

$$\begin{array}{ll}
 \langle (x + 3) * (y - 2), \sigma \rangle & (Ax)(A + 1)(A * 1) \\
 \rightarrow_1 \langle (\mathbf{3} + \mathbf{3}) * (y - 2), \sigma \rangle & (A + 3)(A * 1) \\
 \rightarrow_1 \langle \mathbf{6} * (y - 2), \sigma \rangle & (Ax)(A - 1)(A * 2) \\
 \rightarrow_1 \langle \mathbf{6} * (\mathbf{9} - \mathbf{2}), \sigma \rangle & (A - 3)(A * 2) \\
 \rightarrow_1 \langle \mathbf{6} * \mathbf{7}, \sigma \rangle & (A * 3) \\
 \rightarrow_1 \langle \mathbf{42}, \sigma \rangle & (Az) \\
 \rightarrow_1 42 &
 \end{array}$$

First step in detail:

$$\frac{\frac{\overline{\langle x, \sigma \rangle \rightarrow_1^a \langle 3, \sigma \rangle} (Ax)}{\langle x + 3, \sigma \rangle \rightarrow_1^a \langle 3 + 3, \sigma \rangle} (A + 1)}{\langle (x + 3) * (y - 2), \sigma \rangle \rightarrow_1^a \langle (3 + 3) * (y - 2), \sigma \rangle} (A * 1)$$

Exercise 1.3:

(2 points)

Prove by mathematical induction that the property $P(n)$ holds for all natural numbers $n \geq 1$ i.e.,:

$$P(n) \iff \sum_{i=1}^n (2i - 1)^3 = n^2(2n^2 - 1)$$

Solution

The base case:

$$P(1) \iff 1 = 1$$

The induction hypotheses:

$$P(n) \iff \sum_{i=1}^n (2i - 1)^3 = n^2(2n^2 - 1)$$

Now we have to prove that property P holds for $n + 1$:

$$\begin{aligned}
 P(n + 1) &= \sum_{i=1}^{n+1} (2i - 1)^3 = \sum_{i=1}^n (2i - 1)^3 + (2(n + 1) - 1)^3 \\
 &\stackrel{\text{I.H.}}{=} n^2(2n^2 - 1) + (2n + 1)^3 \\
 &= 2n^4 + 8n^3 + 11n^2 + 6n + 1 \\
 &= 2n^3(n + 1) + 6n^3 + 11n^2 + 6n + 1 \\
 &= 2n^3(n + 1) + 6n^2(n + 1) + 5n^2 + 5n + n + 1 \\
 &= 2n^3(n + 1) + 6n^2(n + 1) + 5n(n + 1) + (n + 1) \\
 &= (n + 1)(2n^3 + 6n^2 + 5n + 1) \\
 &= (n + 1)(2n^2(n + 1) + 4n^2 + 5n + 1) \\
 &= (n + 1)(2n^2(n + 1) + 4n(n + 1) + n + 1) \\
 &= (n + 1)^2(2n^2 + 4n + 1) \\
 &= (n + 1)^2(2(n + 1)^2 - 1)
 \end{aligned}$$
