

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

Due to Monday, 10 Nov. 2008, *before* the exercise course begins.

Exercise 3.1:

(2 points)

Show that the operational and the denotational semantics of arithmetic expressions coincide, i.e., prove the following result.

For every $a \in \mathbf{AExp}$, $\sigma \in \Sigma$, and $z \in \mathbb{Z}$:

$$\langle a, \sigma \rangle \rightarrow z \quad \text{iff} \quad \mathfrak{A}[[a]](\sigma) = z.$$

Solution _____

Let $a \in \mathbf{AExp}$, $\sigma \in \Sigma$ and $z \in \mathbb{Z}$. By structural induction.

Base case:

- $a = z$: $\langle a, \sigma \rangle \rightarrow z$ and $\mathfrak{A}[[a]](\sigma) = z$
- $a = x$: $\langle a, \sigma \rangle \rightarrow \sigma(x)$ and $\mathfrak{A}[[a]](\sigma) = \sigma(x)$

Claims for a_1 and a_2 hold by induction hypothesis.

Induction step:

- $a = a_1 + a_2$: $\langle a_1 + a_2, \sigma \rangle \rightarrow z \iff \exists z_1, z_2 \in \mathbb{Z} :$
 $\langle a_1, \sigma \rangle \rightarrow z_1$
 $\wedge \langle a_2, \sigma \rangle \rightarrow z_2$
 $\wedge z = z_1 + z_2$
 $\xleftrightarrow{\text{ind.hyp.}} \iff \exists z_1, z_2 \in \mathbb{Z} :$
 $\mathfrak{A}[[a_1]](\sigma) = z_1$
 $\wedge \mathfrak{A}[[a_2]](\sigma) = z_2$
 $\wedge z = z_1 + z_2$
 $\iff \mathfrak{A}[[a_1 + a_2]](\sigma) = \mathfrak{A}[[a_1]](\sigma) + \mathfrak{A}[[a_2]](\sigma) = z_1 + z_2 = z$

- $-$, $*$ analogously

□

Exercise 3.2:

(2+2 points)

Consider the following fragment of the program to compute sum (see Exercise 2.3):

while $\neg(x = 1)$ **do** $(y := y + x; x := x - 1)$.

- (a) Determine the corresponding functional $\Phi : (\Sigma \rightarrow \Sigma) \rightarrow (\Sigma \rightarrow \Sigma)$.
- (b) Give at least two fixpoints of Φ and prove their fixpoint properties.

Solution

a) (see Ex. 2.3)

while $\overbrace{\neg(x=1)}^b$ **do** $\overbrace{y := y + x; x := x - 1}^c$

$$\begin{aligned}\Phi(f) &= \mathbf{cond}(\mathfrak{B}[[b]], f \circ \mathfrak{C}[[c]], \mathbf{id}_\Sigma) \\ \Phi(f)(\sigma) &= \mathbf{cond}(\mathfrak{B}[[b]], f \circ \mathfrak{C}[[c]], \mathbf{id}_\Sigma)(\sigma) \\ &= \begin{cases} f(\mathfrak{C}[[c]](\sigma)) & \text{if } \mathfrak{B}[[b]](\sigma) = \mathbf{true} \\ \sigma & \text{otherwise} \end{cases} \\ &\stackrel{\pm}{=} \begin{cases} f(\sigma[y \mapsto \sigma(y) + \sigma(x), x \mapsto \sigma(x) - 1]) & \text{if } \sigma(x) \neq 1 \\ \sigma & \text{otherwise} \end{cases}\end{aligned}$$

since

$$\begin{aligned}\mathfrak{B}[[b]](\sigma) &= \begin{cases} \mathbf{true} & \text{if } \mathfrak{B}[[x=1]](\sigma) = \mathbf{false} \\ \mathbf{false} & \text{otherwise} \end{cases} = \begin{cases} \mathbf{true} & \text{if } \sigma(x) \neq 1 \\ \mathbf{false} & \text{otherwise} \end{cases} \\ \mathfrak{C}[[c]](\sigma) &= \mathfrak{C}[[x := x - 1]](\mathfrak{C}[[y := y + x]](\sigma)) \\ &= \mathfrak{C}[[x := x - 1]](\sigma[y \mapsto \sigma(y) + \sigma(x)]) \\ &= \sigma[y \mapsto \sigma(y) + \sigma(x), x \mapsto \sigma(x) - 1]\end{aligned}$$

b) The fixpoint candidates are:

$$\begin{aligned}f_1(\sigma) &= \begin{cases} \overbrace{\sigma[y \mapsto \sigma(y) + \frac{\sigma(x)(\sigma(x)-1)}{2}, x \mapsto 1]}^{l(\sigma)} & \text{if } \sigma(x) \geq 1 \\ \mathit{undefined} & \text{otherwise} \end{cases} \\ f_2(\sigma) &= \begin{cases} l(\sigma) & \text{if } \sigma(x) \geq 1 \\ \overbrace{\sigma[y \mapsto 0, x \mapsto 0]}^{\sigma_0} & \text{otherwise} \end{cases}\end{aligned}$$

In the following, we check the fixpoint property of f_1 and f_2 (by showing that for $i \in \{1, 2\}$, $\Phi(f_i)(\sigma) = f_i(\sigma)$):

$$\begin{aligned}\Phi(f_1)(\sigma) &= \begin{cases} \overbrace{f_1(\sigma[y \mapsto \sigma(y) + \sigma(x), x \mapsto \sigma(x) - 1])}^{m(\sigma)} & \text{if } \sigma(x) \geq 1 \\ \mathit{undefined} & \text{otherwise} \end{cases} \\ &= \begin{cases} l(m(\sigma)) & \text{if } \sigma(x) \neq 1, m(\sigma)(x) \geq 1 \\ \mathit{undefined} & \text{if } \sigma(x) \neq 1, m(\sigma)(x) < 1 \\ \sigma & \text{if } \sigma(x) = 1 \end{cases} \\ &= \begin{cases} l(m(\sigma)) & \text{if } \sigma(x) > 1 \\ \mathit{undefined} & \text{if } \sigma(x) < 1 \\ \sigma & \text{if } \sigma(x) = 1 \end{cases} \\ &= \begin{cases} \sigma[y \mapsto \sigma(y) + (\sigma(x) - 1) + \frac{(\sigma(x)-1)(\sigma(x)-2)}{2}, x \mapsto 1] & \text{if } \sigma(x) > 1 \\ \mathit{undefined} & \text{if } \sigma(x) < 1 \\ \sigma & \text{if } \sigma(x) = 1 \end{cases} \\ &\stackrel{(*)}{=} \begin{cases} l(\sigma) & \text{if } \sigma(x) > 1 \\ \mathit{undefined} & \text{if } \sigma(x) < 1 \\ \sigma & \text{if } \sigma(x) = 1 \end{cases} = f_1(\sigma)(x)\end{aligned}$$

which implies that f_1 is a fixpoint of Φ .

$$(\sigma(x) - 1) + \frac{(\sigma(x) - 1)(\sigma(x) - 2)}{2} = \frac{\sigma^2(x) - \sigma(x)}{2} = \frac{\sigma(x)(\sigma(x) - 1)}{2} \quad (*)$$

For f_2 , a similar proof applies by replacing $\mathit{undefined}$ by σ_0 in the above proof.

□

Exercise 3.3:**(2+1 points)**

Given a partial order (D, \sqsubseteq) a **maximal element** of D is a $d_{\max} \in D$ such that

$$\forall d \in D. d_{\max} \sqsubseteq d \implies d_{\max} = d.$$

A **minimal element** of D is a $d_{\min} \in D$ such that

$$\forall d \in D. d \sqsubseteq d_{\min} \implies d_{\min} = d.$$

- (a) Prove that a partial order (D, \sqsubseteq) with D finite has at least one maximal element.
- (b) Let $D = \{\{1, 2\}, \{1, 2, 5\}, \{1, 2, 3\}, \{2, 3\}, \{2, 3, 5\}\}$ and define \sqsubseteq as the set inclusion. Find all minimal and maximal elements of D .

Solution

a) We prove by induction on the size n of the set D . Lets assume that A is the set of all maximal elements for the set D of size n .

- (a) The base case: $n=1$. Then $D = \{d\}$ and $A = \{d\}$ due to the reflexivity property of the preorder.
- (b) We assume that the property holds for any D of size n (induction hypothesis). Now we have to show the induction step i.e., we add a new element d' to D and we have to prove that the property holds for the set $D' = D \cup \{d'\}$ of size $n+1$. From I.H. we know that $A \neq \emptyset$ is the set of all maximal elements from D . Then, if $\exists d \in A$ such that $d \sqsubseteq d'$ then $A' = (A \cup \{d'\}) \setminus \{d\}$ or if $d' \sqsubseteq d$ then $A' = A$. If such d does not exist and $\exists d'' \in D \setminus A$ such that $d'' \sqsubseteq d'$ then $A' = A \cup \{d'\}$ or if $d' \sqsubseteq d''$ then $A' = A$. Notice that the size of A' is always equal or greater than one given that A is equal or greater than one.

b) The minimal elements are $\{1, 2\}$ and $\{2, 3\}$. The maximal elements are $\{1, 2, 5\}, \{1, 2, 3\}, \{2, 3, 5\}$. □

Exercise 3.4:**(3 points)**

Develop a proof for Lemma 5.5 of the course, stating that the set of partial state transformations, $\Sigma \dashrightarrow \Sigma$, together with the relation \sqsubseteq given by graph inclusion forms a partial order.

Solution

Let $\Sigma \dashrightarrow \Sigma = \{f \mid f : \Sigma \dashrightarrow \Sigma\}$

$$f \sqsubseteq g \iff \text{graph}(f) \subseteq \text{graph}(g)$$

Encoding state transformations into a graph structure:

$$\text{graph}(f) := \{(\sigma, \sigma') \mid \sigma' = f(\sigma) \text{ defined}\} \subseteq \Sigma \times \Sigma$$

Partial order $\mathcal{R} \subseteq X \times X$:

- reflexive: $\forall x \in X : x \mathcal{R} x$
- transitive: $\forall x, y, z \in X : x \mathcal{R} y \wedge y \mathcal{R} z \implies x \mathcal{R} z$
- anti-symmetric: $\forall x, y \in X : x \mathcal{R} y \wedge y \mathcal{R} x \implies x = y$

Partial order \sqsubseteq :

- reflexive: $\text{graph}(f) \subseteq \text{graph}(f) \implies f \sqsubseteq f$
- transitive:
 - $f \sqsubseteq g, g \sqsubseteq h$
 - $\implies \text{graph}(f) \subseteq \text{graph}(g) \subseteq \text{graph}(h)$
 - $\implies \text{graph}(f) \subseteq \text{graph}(h)$
 - $\implies f \sqsubseteq h$
- anti-symmetric:
 - $f \sqsubseteq g, g \sqsubseteq f$
 - $\implies \text{graph}(f) \subseteq \text{graph}(g), \text{graph}(g) \subseteq \text{graph}(f)$
 - $\implies \text{graph}(f) = \text{graph}(g)$
 - $\implies f = g$

□