

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

Due to Monday, 17 Nov. 2008, *before* the exercise course begins.

Exercise 4.1:

(1+2 points)

- (a) Show that the least upper bound of a chain (Definition 6.4) is unique (if it exists).
 (b) Give a subset of $\Sigma \dashrightarrow \Sigma$ which does not have an upper bound.

Solution

- (a) Let (D, \sqsubseteq) be a PO, and let $S \subseteq D$ be a chain.

Assumption: $d, d' \in D$ are least upper bounds of S
 $\Rightarrow S \sqsubseteq d$ and $S \sqsubseteq d'$ Def. of upper bound
 $\Rightarrow d' \sqsubseteq d$ and $d \sqsubseteq d'$ Def. of least upper bound
 $\Rightarrow d = d'$ \sqsubseteq is PO, antisymmetry

- (b) Required: subset $S \subseteq \Sigma \dashrightarrow \Sigma$ without upper bound.

Remark: S cannot be a chain (see Lemma 6.9)

Claim: $S := \{f_1, f_2\}$ where $f_i : \Sigma \dashrightarrow \Sigma : \sigma \mapsto \sigma[x \mapsto i]$ for some fixed $x \in \mathbf{Var}$ has no upper bound.

Proof: Assume $g : \Sigma \dashrightarrow \Sigma$ is upper bound of S
 $\Rightarrow f_1 \sqsubseteq g$ and $f_2 \sqsubseteq g$
 $\Rightarrow \sigma[x \mapsto 1] = f_1(\sigma) \stackrel{*}{=} g(\sigma) \stackrel{*}{=} f_2(\sigma) = \sigma[x \mapsto 2]$ for every $\sigma \in \Sigma$

(*) Def. of \sqsubseteq : $f(\sigma) = \sigma' \Rightarrow g(\sigma) = \sigma'$

This is a contradiction to the assumption and thus our claim holds.

Remark: there are non-chains with an upper bound.

$f_0(\sigma) = \text{undefined}$

$f_1(\sigma) = \begin{cases} \sigma & \text{if } \sigma(x) \text{ even} \\ \text{undefined} & \text{otherwise} \end{cases}$

$f_2(\sigma) = \begin{cases} \sigma & \text{if } \sigma(x) \text{ odd} \\ \text{undefined} & \text{otherwise} \end{cases}$

$f_3(\sigma) = \sigma$

$\Rightarrow S := \{f_0, f_1, f_2\}$ no chain, but $S \sqsubseteq f_3$

Exercise 4.2:**(1+1+1 points)**

Which of the following functionals of type $(\Sigma \dashrightarrow \Sigma) \rightarrow (\Sigma \dashrightarrow \Sigma)$ are monotonic with respect to the partial order \sqsubseteq given by graph inclusion?

(a) $\Phi_1(f) = f$

(b) $\Phi_2(f) = \begin{cases} g_1 & \text{if } f = g_2 \\ g_2 & \text{otherwise} \end{cases}$ (where $g_1, g_2 : \Sigma \dashrightarrow \Sigma$ with $g_1 \neq g_2$)

(c) $\Phi_3(f)(\sigma) = \begin{cases} f(\sigma) & \text{if } \sigma(x) \neq 0 \\ \sigma & \text{otherwise} \end{cases}$

Solution

Monotonicity of Φ : $f \sqsubseteq g \Rightarrow \Phi(f) \sqsubseteq \Phi(g)$

(a) $f \sqsubseteq g$
 $\Rightarrow \Phi_1(f) = f \sqsubseteq g = \Phi_1(g)$
 $\Rightarrow \Phi_1$ monotonic

(b) Three cases:

- $g_1 \sqsubset g_2$ and $g_1 \neq g_2$:
 $\Phi_2(g_1) = g_2 \not\sqsubseteq g_1 = \Phi_2(g_2)$ (in graph representation arrow changes direction)
 $\Rightarrow \Phi_2$ not monotonic
- $g_2 \sqsubset g_1$ and $g_2 \neq g_1$: same as above...
- g_1, g_2 incomparable, i.e. $g_1 \not\sqsubseteq g_2$ and $g_2 \not\sqsubseteq g_1$:
 $\Rightarrow g_2 \neq f_\emptyset$ (otherwise $g_2 \sqsubseteq g_1$) and $f_\emptyset \sqsubseteq g_2$ but $\Phi_2(f_\emptyset) = g_2 \not\sqsubseteq g_1 = \Phi_2(g_2)$
 $\Rightarrow \Phi_2$ not monotonic

(c) Let $f, g : \Sigma \dashrightarrow \Sigma$ and $\sigma, \sigma' \in \Sigma$ such that $f \sqsubseteq g$

$$\Phi_3(f)(\sigma) = \begin{cases} f(\sigma) & \text{if } \sigma(x) \neq 0 \\ \sigma & \text{otherwise} \end{cases} \quad \Phi_3(g)(\sigma) = \begin{cases} g(\sigma) & \text{if } \sigma(x) \neq 0 \\ \sigma & \text{otherwise} \end{cases}$$

Case 1: $\sigma(x) \neq 0$:For $f(\sigma)$ undefined there is nothing to show, otherwise

$$\Phi_3(f)(\sigma) = f(\sigma) = \sigma' \xrightarrow{*} \sigma' = g(\sigma) = \Phi_3(g)(\sigma)$$

(*): Def. of \sqsubseteq Case 2: $\sigma(x) = 0$: $\Phi_3(f)(\sigma) = \sigma = \Phi_3(g)(\sigma)$ $\Rightarrow \Phi$ is monotonic.

□

Exercise 4.3:**(4 points)**

Investigate

$$\mathcal{C}[[z := 0; \text{while } y \leq x \text{ do } (z := z + 1; x := x - y)]]$$

in analogy to the factorial example 7.3.

Solution

For every $\sigma_{init} \in \Sigma$, $c \equiv z := 0$; **while** b **do** c'

$$\mathfrak{C}[[c]](\sigma_{init}) = \mathbf{fix}(\Phi)(\sigma)$$

where $\sigma = \sigma_{init}[z \mapsto 0]$ and for every $f : \Sigma \dashrightarrow \Sigma$ and $\sigma \in \Sigma$,

$$\Phi(f)(\sigma) = \begin{cases} f(\sigma') & \text{if } \sigma(y) \leq \sigma(x) \\ \sigma & \text{otherwise} \end{cases}$$

where $\sigma' = \sigma[z \mapsto \sigma(z) + 1, x \mapsto \sigma(x) - \sigma(y)]$.

Approximation $\Phi^n(f_\emptyset)(\sigma)$ for $n \in \mathbb{N}$ and $\sigma_{init}(x) \geq 0$ and $\sigma_{init}(y) > 0$:

$$\Phi^0(f_\emptyset)(\sigma) = f_\emptyset(\sigma) = \text{undefined}$$

$$\begin{aligned} \Phi^1(f_\emptyset)(\sigma) &= \begin{cases} f_\emptyset(\sigma') & \text{if } \sigma(y) \leq \sigma(x) \\ \sigma & \text{otherwise} \end{cases} \\ &= \begin{cases} \text{undefined} & \text{if } \sigma(y) \leq \sigma(x) \\ \sigma & \text{otherwise} \end{cases} \end{aligned}$$

$$\Phi^1(f_\emptyset)(\sigma_{2,3,0}) = \sigma_{2,3,0} \quad (2/3 = 0 \text{ remainder } 2)$$

$$\Phi^1(f_\emptyset)(\sigma_{5,3,0}) \text{ is undefined}$$

$$\begin{aligned} \Phi^2(f_\emptyset)(\sigma) &= \Phi(\Phi(f_\emptyset))(\sigma) \\ &= \begin{cases} \Phi(f_\emptyset)(\sigma') & \text{if } \sigma(y) \leq \sigma(x) \\ \sigma & \text{otherwise} \end{cases} \\ &= \begin{cases} \text{undefined} & \text{if } \sigma(y) \leq \sigma(x) \text{ and } \sigma'(y) \leq \sigma'(x) \\ \sigma' & \text{if } \sigma(y) \leq \sigma(x) \text{ and } \sigma'(y) > \sigma'(x) \\ \sigma & \text{otherwise} \end{cases} \\ &= \begin{cases} \text{undefined} & \text{if } \sigma(y) \leq \sigma(x) \text{ and } \sigma(y) \leq \sigma(x) - \sigma(y) \\ \sigma' & \text{if } \sigma(y) \leq \sigma(x) \text{ and } \sigma(y) > \sigma(x) - \sigma(y) \\ \sigma & \text{otherwise} \end{cases} \\ &= \begin{cases} \text{undefined} & \text{if } 2 \cdot \sigma(y) \leq \sigma(x) \\ \sigma' & \text{if } \sigma(y) \leq \sigma(x) < 2 \cdot \sigma(y) \\ \sigma & \text{otherwise} \end{cases} \end{aligned}$$

$$\Phi^2(f_\emptyset)(\sigma_{5,3,0}) = \sigma_{2,3,1} \quad (5/3 = 1 \text{ remainder } 2)$$

$$\begin{aligned} \Phi^3(f_\emptyset)(\sigma) &= \Phi(\Phi(\Phi(f_\emptyset)))(\sigma) \\ &= \dots \end{aligned}$$

$$= \begin{cases} \text{undefined} & \text{if } 3 \cdot \sigma(y) \leq \sigma(x) \\ \sigma'' & \text{if } 2 \cdot \sigma(y) \leq \sigma(x) < 3 \cdot \sigma(y) \\ \sigma' & \text{if } \sigma(y) \leq \sigma(x) < 2 \cdot \sigma(y) \\ \sigma & \text{otherwise} \end{cases}$$

$$\Phi^n(f_\emptyset)(\sigma) = \begin{cases} \text{undefined} & \text{if } n \cdot \sigma(y) \leq \sigma(x) \\ \sigma[z \mapsto k, x \mapsto \sigma(x) - k \cdot \sigma(y)] & \text{if } k \cdot \sigma(y) \leq \sigma(x) < (k+1) \cdot \sigma(y) \text{ for } k \in \{1, \dots, n\} \\ \sigma & \text{otherwise} \end{cases}$$

$$\text{Fixpoint: } \mathbf{fix}(\Phi)(\sigma) = \begin{cases} \sigma[z \mapsto \sigma(x) \mathbf{div} \sigma(y), x \mapsto \sigma(x) \mathbf{mod} \sigma(y)] & \text{if } 0 < y \leq x \\ \text{undefined} & \text{if } y \leq x \leq 0 \\ \sigma & \text{if } x < y \end{cases}$$

where **div** and **mod** are defined as usual for $x \geq 0, y > 0$ only.

□

Exercise 4.4:

(1+3 points)

- (a) Define the denotational semantics of the **repeat** c **until** b construct.
 (b) Using this semantics, show that the following semantic equivalence holds:

$$\mathbf{repeat} \ c \ \mathbf{until} \ b \sim c; \ \mathbf{while} \ \neg b \ \mathbf{do} \ c.$$

(**Hint:** The proof can be given by complete induction over the fixpoint iteration index n .)

Solution

- (a) Semantics defined by: $\mathcal{C}[\mathbf{repeat} \ c \ \mathbf{until} \ b] = \mathbf{fix}(\Psi)$

First comes the body then evaluate b The body has to be executed at least once

$$\text{where } \Psi(f) = \mathbf{cond}[\overbrace{\mathfrak{B}[b] \circ \mathcal{C}[c]}^{\text{First comes the body then evaluate b}}, \overbrace{\mathcal{C}[c]}^{\text{The body has to be executed at least once}}, f \circ \mathcal{C}[c]]$$

- (b)

$$c_1 = \mathbf{repeat} \ c \ \mathbf{until} \ b$$

$$c_2 = c; \ \mathbf{while} \ b \ \mathbf{do} \ c$$

$$\begin{aligned} \mathcal{C}[c_1] &= \bigsqcup_{n \in \mathbb{N}} \Psi^n(f_\emptyset) \\ \mathcal{C}[c_2] &= \mathcal{C}[\mathbf{while} \ \neg b \ \mathbf{do} \ c] \circ \mathcal{C}[c] \\ &= (\bigsqcup_{n \in \mathbb{N}} \Phi^n(f_\emptyset)) \circ \mathcal{C}[c] \quad \text{where } \Phi(f) = \mathbf{cond}(\mathfrak{B}[\neg b], f \circ \mathcal{C}[c], \mathbf{id}_\Sigma) \\ &= \bigsqcup_{n \in \mathbb{N}} (\Phi^n(f_\emptyset) \circ \mathcal{C}[c]) \end{aligned}$$

By induction over \mathbb{N} we will show that $\Psi^n(f_\emptyset) = \Phi^n(f_\emptyset) \circ \mathcal{C}[c]$

(I.B.) $n = 0$:

$$\Psi^0(f_\emptyset) = f_\emptyset = f_\emptyset \circ \mathcal{C}[c] = \Phi^0(f_\emptyset) \circ \mathcal{C}[c]$$

since $f_\emptyset(\sigma)$ is undefined for every $\sigma \in \Sigma$

(I.H.) $\Psi^n(f_\emptyset) = \Phi^n(f_\emptyset) \circ \mathcal{C}[c]$

(I.S.) $n \rightarrow n + 1$:

$$\begin{aligned} \Phi^{n+1}(f_\emptyset) \circ \mathcal{C}[c] &= \Phi(\Phi^n(f_\emptyset)) \circ \mathcal{C}[c] \\ &= \mathbf{cond}(\mathfrak{B}[\neg b], \Phi^n(f_\emptyset) \circ \mathcal{C}[c], \mathbf{id}_\Sigma) \circ \mathcal{C}[c] \\ &= \mathbf{cond}(\mathfrak{B}[\neg b] \circ \mathcal{C}[c], \Phi^n(f_\emptyset) \circ \mathcal{C}[c] \circ \mathcal{C}[c], \mathcal{C}[c]) \\ \text{(I.H.)} &= \mathbf{cond}(\mathfrak{B}[\neg b] \circ \mathcal{C}[c], \Psi^n(f_\emptyset) \circ \mathcal{C}[c], \mathcal{C}[c]) \\ \text{(negation)} &= \mathbf{cond}(\mathfrak{B}[b] \circ \mathcal{C}[c], \mathcal{C}[c], \Psi^n(f_\emptyset) \circ \mathcal{C}[c]) \\ &= \Psi(\Psi^n(f_\emptyset)) \\ &= \Psi^{n+1}(f_\emptyset) \end{aligned}$$

□