CS 4110 - 9/19/25

Lab #11 - Denotational Semantics

Suppose we extend IMP with two new commands?

$c ::= \ldots$

$\quad |$ for a do c

$\quad |$ if b do c

Informally, a for-loop evaluates a to an integer n and then executes c n times, unless n is negative, in which case it behaves like skip. A one-armed conditional executes c if b evaluates to true and otherwise behaves like skip.

Here are big-step operational semantics for these constructs:

$$\frac{\langle \sigma, a\rangle \Downarrow n \qquad n \leq 0}{\langle \sigma, \text{for } a \text{ do } c\rangle \Downarrow \sigma}
\qquad
\frac{\langle \sigma, a\rangle \Downarrow n \qquad n > 0 \qquad \langle \sigma, c\rangle \Downarrow \sigma'' \qquad \langle \sigma'', \text{for } n-1 \text{ do } c\rangle \Downarrow \sigma'}{\langle \sigma, \text{for } a \text{ do } c\rangle \Downarrow \sigma'}$$

$$\frac{\langle \sigma, b\rangle \Downarrow \text{false}}{\langle \sigma, \text{if } b \text{ do } c\rangle \Downarrow \sigma}
\qquad
\frac{\langle \sigma, b\rangle \Downarrow \text{true} \qquad \langle \sigma, c\rangle \Downarrow \sigma'}{\langle \sigma, \text{if } b \text{ then } c\rangle \Downarrow \sigma'}$$

How do we define their denotational semantics? 2

$$\mathcal{C}[\![\text{for } a \text{ do } c]\!] = \{(\sigma,\sigma') \mid (\sigma,n) \in \mathcal{A}[\![a]\!] \wedge n \geq 0 \wedge (\sigma,\sigma') \in \mathcal{C}[\![c]\!]^n\}$$
$$\cup \{(\sigma,\sigma) \mid (a,n) \in \mathcal{A}[\![a]\!] \wedge n < 0\}$$

where

$$f^0 = \{(\sigma,\sigma)\}$$
$$f^{i+1} = \{(\sigma,\sigma') \mid \exists \sigma''\ (\sigma,\sigma'') \in f \wedge (\sigma'',\sigma') \in f^i\}$$

$$\mathcal{C}[\![\text{if } b \text{ do } c]\!] = \{(\sigma,\sigma) \mid (\sigma,\text{false}) \in \mathcal{B}[\![b]\!]\}$$
$$\cup \{(\sigma,\sigma') \mid (\sigma,\text{true}) \in \mathcal{B}[\![b]\!] \wedge (\sigma,\sigma') \in \mathcal{C}[\![c]\!]\}$$

How do we show

```
while b do c   ~   while b do
                     while b do c
```

Using the denotational semantics?

Intuitively, the second loop has the first inside. So it seems easy. But how to do it formally?

Let's calculate

$$\mathcal{C}[\![\text{while } b \text{ do } c]\!] = \text{fix}(F)$$

where $F(f) = \{(\sigma,\sigma) \mid (\sigma,\text{false}) \in \mathcal{B}[\![b]\!]\}$
$\quad \cup \{(\sigma,\sigma') \mid \exists \sigma''. (\sigma,\text{true}) \in \mathcal{B}[\![b]\!] \land (\sigma,\sigma'') \in \mathcal{C}[\![c]\!] \land (\sigma'',\sigma') \in f\}$

$$\mathcal{C}[\![\text{while } b \text{ do } (\text{while } b \text{ do } c)]\!] = \text{fix}(G)$$

where $G(g) = \{(\sigma,\sigma) \mid (\sigma,\text{false}) \in \mathcal{B}[\![b]\!]\}$
$\quad \cup \{(\sigma,\sigma') \mid \exists \sigma''. (\sigma,\sigma'') \in \mathcal{B}[\![b]\!] \land (\sigma,\sigma'') \in \mathcal{C}[\![\text{while } b \text{ do } c]\!] \land$
$\quad (\sigma'',\sigma') \in g\}.$

<u>Lemma 1</u> $\forall i.\ (\sigma,\sigma') \in F^i(\emptyset) \Rightarrow (\sigma',\text{false}) \in \mathcal{B}[\![b]\!]$.

<u>Proof.</u> By induction on i.

<u>Case 0:</u> vacuously holds as $F^0(\emptyset) = \emptyset$. ✓✓

<u>Case i+1:</u>

Let $(\sigma,\sigma') \in F^{i+1}(\emptyset)$. We analyze two cases.

Subcase $(\sigma,\text{false}) \in \mathcal{B}[\![b]\!]$:

By def'n F, we have $\sigma = \sigma'$ and the result is immediate. by defn F

Subcase $(\sigma,\text{true}) \in \mathcal{B}[\![b]\!]$:

By def'n F, $\exists \sigma''.\ (\sigma,\sigma'') \in \mathcal{C}[\![c]\!]$ and $(\sigma'',\sigma') \in F^i(\emptyset)$.

By IH, $(\sigma',\text{false}) \in \mathcal{B}[\![b]\!]$. ✓✓ $\square$

Lemma 2: $\forall i.\ (\sigma, \text{false}) \in \mathcal{B}[\![b]\!] \wedge (\sigma,\sigma') \in F^i(\emptyset) \Rightarrow \sigma = \sigma'$. 4

Proof by induction on i.

Case 0: vacuously holds as $(\sigma,\sigma') \in F^0(\emptyset) = \emptyset$ is a contradiction ✓✓

Case $i+1$: By assumption, $(\sigma, \text{false}) \in \mathcal{B}[\![b]\!]$, and $(\sigma,\sigma') \in F^{i+1}(\emptyset)$.
By defn F, we have $\sigma = \sigma'$. ✓✓ □

Lemma 3: $\forall i.\ (\sigma, \text{false}) \in \mathcal{B}[\![b]\!] \wedge (\sigma,\sigma') \in G^i(\emptyset) \Rightarrow \sigma = \sigma'$.

Proof: analogous to proof of Lemma 1.

Lemma 4: $\forall j > 1.\ G^j(\emptyset) = \bigcup_i F^i(\emptyset)$.

Proof. By induction on j.

Case 0: vacuously holds as $0 > 1$ is a contradiction. ✓✓

Case $j+1$: We analyze two subcases.

Subcase $j+1 = 1$: vacuously holds as $1 > 1$ is a contradiction ✓✓

Subcase $j+1 > 1$: We'll prove each inclusion separately.

($\subseteq$) Let $(\sigma,\sigma') \in G^{j+1}(\emptyset)$. We analyze two subsubcases:

Subsubcase $(\sigma, \text{false}) \in \mathcal{B}[\![b]\!]$:

By Lemma 3, we have $\sigma = \sigma'$.
By defn F, $(\sigma,\sigma) \in F(\emptyset) \subseteq \bigcup_i F^i(\emptyset)$.
Hence $(\sigma,\sigma) \in \bigcup_i F^i(\emptyset)$. ✓✓

Subsubcase $(\sigma, \text{true}) \in \mathcal{B}[\![b]\!]$:

By defn G, we have:

$$\exists \sigma''.\ (\sigma, \sigma'') \in \mathcal{C}[\![\text{while } b \text{ do } c]\!] \wedge (\sigma'', \sigma') \in G^{j}(\emptyset).$$

By Lemma 1, we have $(\sigma'', \text{false}) \in \mathcal{B}[\![b]\!]$.

By Lemma 3, we have $\sigma'' = \sigma'$.

By defn $\mathcal{C}[\![\cdot]\!]$, we have $\mathcal{C}[\![\text{while } b \text{ do } c]\!] = \text{fix}(F) = \bigcup_i F^i(\emptyset)$

Hence, $(\sigma, \sigma') \in \bigcup_i F^i(\emptyset)$. ✓✓

(2) Let $(\sigma, \sigma') \in \bigcup_i F^i(\emptyset)$.

We analyze two subsubcases.

Subsubcase $(\sigma, \text{false}) \in \mathcal{B}[\![b]\!]$:

By Lemma 2, $\forall i.\ (\sigma, \sigma') \in F^i(\emptyset) \Rightarrow \sigma = \sigma'$.

Hence, $\sigma = \sigma'$.

By defn G, and $j+1 \geq 1$, we have $(\sigma, \sigma) \in G^{j}(\emptyset)$. ✓✓

Subsubcase $(\sigma, \text{true}) \in \mathcal{B}[\![b]\!]$:

By defn $\mathcal{C}[\![\cdot]\!]$, we have $\mathcal{C}[\![\text{while } b \text{ do } c]\!] = \text{fix}(F) = \bigcup_i F^i(\emptyset)$.

Hence, $(\sigma, \sigma') \in \mathcal{C}[\![\text{while } b \text{ do } c]\!]$.

By Lemma 1, we have $(\sigma', \text{false}) \in \mathcal{B}[\![b]\!]$.

By defn G, and $j+1 > 1$ we have $(\sigma', \sigma') \in G^{j}(\emptyset)$.

Hence, $(\sigma, \sigma') \in G^{j+1}(\emptyset)$ ✓✓ $\square$

Theorem: while b do c $\sim$ while b do (while b do c)

$$\mathcal{C}[\![\text{while } b \text{ do } c]\!]$$

$$= fix(F)$$

$$= \bigcup_i F^i(\emptyset)$$

$$= \emptyset \cup \{(\sigma,\sigma) \mid (\sigma, false) \in \mathcal{B}[\![b]\!]\} \cup \bigcup_i F^i(\emptyset) \cup \bigcup_i F_i(\emptyset) \cup \ldots$$

$$= G^0(\emptyset) \cup G(\emptyset) \cup G^2(\emptyset) \cup G_3(\emptyset) \cup \ldots \qquad \text{(By Lemma 4)}$$

$$= \bigcup_j G^j(\emptyset)$$

$$= fix(G)$$

$$= \mathcal{C}[\![\text{while } b \text{ do } (\text{while } b \text{ do } c)]\!] \qquad \square$$