Assignment 4 on Program Semantics

Adrián Enríquez Ballester

January 9, 2022

Given the function $F : (\mathbf{State} \to \mathbf{State}_\perp) \to (\mathbf{State} \to \mathbf{State}_\perp)$ defined as follows:

$$F(f) = cond\,(\mathcal{B}[\![n > 0]\!], f \circ \mathcal{S}[\![x := 2 * x;\ n := n - 1]\!], id)$$

(a) Give an explicit definition for $F\,(\lambda\sigma.\perp)$, $F^2\,(\lambda\sigma.\perp)$ and $F^3\,(\lambda\sigma.\perp)$.

For the first application of F, as any function right-composed with $\lambda\sigma.\perp$ is the same as $\lambda\sigma.\perp$, we have

$$F\,(\lambda\sigma.\perp) = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) > 0 \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases}$$

For its second application, let $g : \mathbf{State} \to \mathbf{State}$ be the function

$$\begin{aligned} g &= S[\![x := 2 * x;\ n := n - 1]\!] \\ &= \lambda\sigma.\sigma\,[x \mapsto 2 \cdot \sigma(x), n \mapsto \sigma(n) - 1] \end{aligned}$$

As it subtracts 1 to n, by matching the corresponding cases of $F(\lambda\sigma.\perp)$ after applying g, we have

$$F(\lambda\sigma.\perp) \circ g = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) > 1 \\ g(\sigma) & \text{if } \sigma(n) \leq 1 \end{cases}$$

which, once the case of $n \leq 0$ is absorbed by *cond*, becomes into

$$F^2\,(\lambda\sigma.\perp) = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) > 1 \\ \sigma\,[x \mapsto 2 \cdot \sigma(x), n \mapsto 0] & \text{if } \sigma(n) = 1 \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases}$$

In a similar way, as

$$F^2(\lambda\sigma.\perp) \circ g = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) > 2 \\ g(g(\sigma)) & \text{if } \sigma(n) = 2 \\ g(\sigma) & \text{if } \sigma(n) \leq 1 \end{cases}$$

we reach the next power of F:

$$F^3(\lambda\sigma.\perp) = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) > 2 \\ \sigma[x \mapsto 4 \cdot \sigma(x), n \mapsto 0] & \text{if } \sigma(n) = 2 \\ \sigma[x \mapsto 2 \cdot \sigma(x), n \mapsto 0] & \text{if } \sigma(n) = 1 \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases}$$

(b) From the results above, conjecture a general defintion for $F^i(\lambda\sigma.\perp)$ where $i \geq 1$. [Optional] Prove by induction on i that your conjecture is correct.

Our conjecture is the following:

$$F^i(\lambda\sigma.\perp) = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) \geq i \\ g^{\sigma(n)}(\sigma) & \text{if } 0 < \sigma(n) < i \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases}$$

where $g^j(\sigma) = \sigma\left[x \mapsto 2^j \cdot \sigma(x), n \mapsto \sigma(n) - j\right]$. Note that when $j = \sigma(n)$ it yields $\sigma\left[x \mapsto 2^j \cdot \sigma(x), n \mapsto 0\right]$, but we have written it in a more general way for the ease of the following proof.

It has been shown to hold when $i = 1$ (i.e. recall $F(\lambda\sigma.\perp)$ from the previous section). For proceeding with the inductive proof, suppose that it holds for some i, then

$$F^i(\lambda\sigma.\perp) \circ g = \lambda\sigma. \begin{cases} \perp & \text{if } \sigma(n) \geq i+1 \\ g^{\sigma(n)-1}(g(\sigma)) & \text{if } 1 < \sigma(n) < i+1 \\ g(\sigma) & \text{if } \sigma(n) \leq 1 \end{cases}$$

and the case of $\sigma(n) = 1$ is $g(\sigma) = g^0(g(\sigma)) = g^{\sigma(n)-1}(g(\sigma))$, thus it can be merged with the $1 < \sigma(n) < i+1$ case. By gathering all these results we obtain

$$\begin{aligned} F^{i+1}(\lambda\sigma.\perp) &= \begin{cases} F^i(\lambda\sigma.\perp) \circ g & \text{if } \sigma(n) > 0 \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases} \\ &= \begin{cases} \perp & \text{if } \sigma(n) \geq i+1 \\ g^{\sigma(n)}(\sigma) & \text{if } 0 < \sigma(n) < i+1 \\ \sigma & \text{if } \sigma(n) \leq 0 \end{cases} \end{aligned}$$

(c) Give an explicit definition for $\sqcup_i F^i\,(\lambda\sigma.\bot)$.

$$\sqcup_i F^i\,(\lambda\sigma.\bot) = \lambda\sigma.\begin{cases}\sigma\left[x \mapsto 2^{\sigma(n)}\cdot\sigma(x), n \mapsto 0\right] & \text{if } \sigma(n) > 0\\ \sigma & \text{if } \sigma(n) \leq 0\end{cases}$$

This function is greater than $F^i(\lambda\sigma.\bot)$ $\forall i \geq 1$ in the sense that it has always less values of its domain mapped to $\bot$ (i.e. none at all) and it matches the same image for those of $F^i(\lambda\sigma.\bot)$ which are not mapped to $\bot$.

(d) Which is the least fixed point of F? Justify you answer.

The least fixed point of F is the function $\sqcup_i F^i$ stated in the previous section.

This result follows by $\left(\mathbf{State} \to \mathbf{State}_\bot, \sqsubseteq\right)$ being a *ccpo* for the order relation which we are using, the function F being monotonically increasing and continuous, and a theorem which states that, under these conditions, $\sqcup_i F^i$ is the least fixed point of F.

(e) Given the above, compute the state resulting from the execution of the following program

$$x := 1;\ \texttt{while}\ n > 0\ \texttt{do}\ \ (x := 2 * x;\ n := n - 1)$$

under the initial state $\sigma = [n \mapsto 4]$.

The denotational semantics for its sequenced substatements are:

$$\begin{aligned}\mathcal{S}[\![x := 1]\!] &= \lambda\sigma.\sigma\,[x \mapsto 1]\\ \mathcal{S}[\![\ \texttt{while}\ n > 0\ \texttt{do}\ \ (x := 2 * x;\ n := n - 1)]\!] &= lfp\ F\end{aligned}$$

where the required least fixed point is precisely the one which we have been obtaining in this exercise:

$$lfp\ F = \lambda\sigma.\begin{cases}\sigma\left[x \mapsto 2^{\sigma(n)}\cdot\sigma(x), n \mapsto 0\right] & \text{if } \sigma(n) > 0\\ \sigma & \text{if } \sigma(n) \leq 0\end{cases}$$

The whole program semantics consist of its composition

$$lfp\ F \circ \lambda\sigma.\sigma\,[x \mapsto 1]$$

so let us apply it to the initial state in order to get the final one:

$$\begin{aligned}\left(lfp\ F \circ \lambda\sigma.\sigma\,[x \mapsto 1]\,\right)\left([n \mapsto 4]\right) &= \left(lfp\ F\right)\left([x \mapsto 1, n \mapsto 4]\right)\\ &= [x \mapsto 2^4, n \mapsto 0]\end{aligned}$$