# Assignments 2 and 3 on Program Semantics

Adrián Enríquez Ballester

January 9, 2022

2. Assume we extend the syntax of *While* statements with a new construct: `repeat` $S$ `until` $b$. This statement is executed as follows:

   (1) Execute $S$.

   (2) Check whether $b$ is false. In this case, step back to (1). Otherwise, finish.

   Define the big-step and small-step semantic rules for this new construct. You cannot rely on the rules of `while` to define the rules of `repeat`. Finally, prove that `repeat` $S$ `until` $b$ is equivalent to ($S$; `while` $\neg b$ `do` $S$).

   Its big-step semantics can be stated by the rules

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \quad \mathcal{B}[\![b]\!]\sigma' = \mathit{true}}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'}\,[\text{RepeatT}_{\text{BS}}]$$

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \quad \mathcal{B}[\![b]\!]\sigma' = \mathit{false} \quad \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \Downarrow \sigma''}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma''}\,[\text{RepeatF}_{\text{BS}}]$$

   and its small-step semantics can be defined as

$$\frac{}{\begin{array}{l}\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \longrightarrow \\ \quad \langle S; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma\rangle\end{array}}\,[\text{Repeat}_{\text{SS}}]$$

   We know by a theorem that both big-step and small-step semantics are equivalent for the current constructs of *While*, so let us check that it is also true for our new construct definition.

   On the one hand, suppose that $\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'$. According to the big-step rules, the simplest possibility is that the premises $\langle S, \sigma\rangle \Downarrow \sigma'$ and $\mathcal{B}[\![b]\!]\sigma' = \mathit{true}$ are satisfied. By applying the rule induction hypothesis on the proof subtree, we have $\langle S, \sigma\rangle \longrightarrow^* \sigma'$, so

$$\begin{aligned}
&\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow \langle S; \texttt{if}\ \ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow^{*} \langle \texttt{if}\ \ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \\
&\qquad\qquad \longrightarrow \langle \texttt{skip}, \sigma'\rangle \\
&\qquad\qquad \longrightarrow \sigma'
\end{aligned}$$

where the sequencing derivation chain step comes from a known lemma whose proof can be easily revisited for taking into account this new construct.

Another possibility is that the satisfied premises are $\langle S, \sigma\rangle \Downarrow \sigma''$, $\mathcal{B}[\![b]\!]\sigma'' = \mathit{false}$ and $\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma''\rangle \Downarrow \sigma'$. By applying the induction hypothesis to both proof subtrees, this time we have

$$\begin{aligned}
\langle S, \sigma\rangle &\longrightarrow^{*} \sigma'' \\
\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma''\rangle &\longrightarrow^{*} \sigma'
\end{aligned}$$

so, with all this together and the same sequencing lemma, we conclude with

$$\begin{aligned}
&\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow \langle S; \texttt{if}\ \ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow^{*} \langle \texttt{if}\ \ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma''\rangle \\
&\qquad\qquad \longrightarrow \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma''\rangle \\
&\qquad\qquad \longrightarrow^{*} \sigma'
\end{aligned}$$

On the other hand, suppose that $\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \longrightarrow^{k} \sigma'$, so the derivation chain must have the following shape:

$$\begin{aligned}
&\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow \langle S; \texttt{if}\ \ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma\rangle \\
&\qquad\qquad \longrightarrow^{k-1} \sigma'
\end{aligned}$$

By using a second known lemma for sequencing derivation chains, whose proof can be easily revisited for taking into account this new construct of the language, there must exist a $\sigma''$ such that

$$\langle S, \sigma \rangle \longrightarrow^{k_1} \sigma''$$
$$\langle \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma'' \rangle \longrightarrow^{k_2} \sigma'$$

with $k_1$ and $k_2$ smaller than $k-1$, thus also smaller that $k$.

By induction hypothesis on the length of the derivation chain for the leftmost side, we have $\langle S, \sigma \rangle \Downarrow \sigma''$ and now there are two cases to distinguish:

- If $\mathcal{B}[\![b]\!]\sigma'' = \mathit{true}$, then $\langle \texttt{skip}, \sigma'' \rangle \longrightarrow \sigma'$, so $\sigma' = \sigma''$ and we can conclude with $\langle \texttt{repeat } S \texttt{ until } b, \sigma \rangle \Downarrow \sigma'$.
- If $\mathcal{B}[\![b]\!]\sigma'' = \mathit{false}$, then $\langle \texttt{repeat } S \texttt{ until } b, \sigma'' \rangle \longrightarrow^{k_2 - 1} \sigma'$ and, as $k_2 - 1$ is also smaller than $k$, the induction hypothesis can be applied to the rightmost side to obtain $\langle \texttt{repeat } S \texttt{ until } b, \sigma'' \rangle \Downarrow \sigma'$. This path also leads to all the premises satisfied for concluding with $\langle \texttt{repeat } S \texttt{ until } b, \sigma \rangle \Downarrow \sigma'$.

Once the big-step and small-step semantics have been reaffirmed to be equivalent even with this added construct, any of them can be chosen for proving the requested statements equivalence. We are going to proceed using the big-step semantics.

For one of the implications, suppose that $\langle \texttt{repeat } S \texttt{ until } b, \sigma \rangle \Downarrow \sigma'$. One of the possible rules requires that $\langle S, \sigma \rangle \Downarrow \sigma'$ and $\mathcal{B}[\![b]\!]\sigma' = \mathit{true}$ so, as $\mathcal{B}[\![\neg b]\!]\sigma' = \neg\mathcal{B}[\![b]\!]\sigma' = \mathit{false}$, it holds that $\langle \texttt{while } \neg b \texttt{ do } S, \sigma' \rangle \Downarrow \sigma'$ and therefore $\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \Downarrow \sigma'$.

The other possible rule requires that $\langle S, \sigma \rangle \Downarrow \sigma''$, $\mathcal{B}[\![b]\!]\sigma'' = \mathit{false}$ and $\langle \texttt{repeat } S \texttt{ until } b, \sigma'' \rangle \Downarrow \sigma'$. By applying the induction hypothesis to the proof subtree of the latter premise, we have

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'' \rangle \Downarrow \sigma'$$

This sequencing requires itself $\langle S, \sigma'' \rangle \Downarrow \sigma'''$ and $\langle \texttt{while } \neg b \texttt{ do } S, \sigma''' \rangle \Downarrow \sigma'$ which, by knowing $\mathcal{B}[\![\neg b]\!]\sigma'' = \neg\mathcal{B}[\![b]\!]\sigma'' = \mathit{true}$ imply

$$\langle \texttt{while } \neg b \texttt{ do } S, \sigma'' \rangle \Downarrow \sigma'$$

and finally

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \Downarrow \sigma'$$

For the converse implication, suppose that $\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \Downarrow \sigma'$, which requires $\langle S, \sigma \rangle \Downarrow \sigma''$ and $\langle \texttt{while } \neg b \texttt{ do } S, \sigma'' \rangle \Downarrow \sigma'$.

If $\mathcal{B}[\![\neg b]\!]\sigma'' = \mathit{false}$, then $\mathcal{B}[\![b]\!]\sigma'' = \neg\neg\mathcal{B}[\![b]\!]\sigma'' = \neg\mathcal{B}[\![\neg b]\!]\sigma'' = \mathit{true}$ and $\sigma' = \sigma''$, so $\langle \texttt{repeat } S \texttt{ until } b, \sigma \rangle \Downarrow \sigma'$.

Finally, if $\mathcal{B}[\![\neg b]\!]\sigma'' = \mathit{true}$, then the `while` rule requires $\langle S, \sigma'' \rangle \Downarrow \sigma'''$ and $\langle \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma''' \rangle \Downarrow \sigma'$, so $\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'' \rangle \Downarrow \sigma'$ and, by rule induction on this last proof subtree, we have

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'' \rangle \Downarrow \sigma'$$

which, by knowing that $\mathcal{B}[\![b]\!]\sigma'' = \neg\neg\mathcal{B}[\![b]\!]\sigma'' = \neg\mathcal{B}[\![\neg b]\!]\sigma'' = \mathit{false}$ yields to all the premises satisfied for

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma \rangle \Downarrow \sigma'$$

2. Add the following iterative construct to *While*: $\texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S$. Define its big-step and small-step semantic rules. You cannot rely on the `while` or `repeat` construct to do this exercise.

   Assuming that we want to be able to traverse both increasing and decreasing sequences, and include the ending value, we can define its big-step semantic rules to be

$$\frac{\mathcal{A}[\![e_2 - e_1]\!]\sigma =_{\mathbb{Z}} 0_{\mathbb{Z}} \quad \langle S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle \Downarrow \sigma'}{\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \Downarrow \sigma'}\ [\mathrm{ForEQ_{BS}}]$$

$$\frac{\begin{array}{r}\mathcal{A}[\![e_2 - e_1]\!]\sigma >_{\mathbb{Z}} 0_{\mathbb{Z}} \quad \langle S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle \Downarrow \sigma' \\ \langle \texttt{for}\ x := e_1 + 1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma' \rangle \Downarrow \sigma''\end{array}}{\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \Downarrow \sigma''}\ [\mathrm{ForGT_{BS}}]$$

$$\frac{\begin{array}{r}\mathcal{A}[\![e_2 - e_1]\!]\sigma <_{\mathbb{Z}} 0_{\mathbb{Z}} \quad \langle S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle \Downarrow \sigma' \\ \langle \texttt{for}\ x := e_1 - 1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma' \rangle \Downarrow \sigma''\end{array}}{\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \Downarrow \sigma''}\ [\mathrm{ForLT_{BS}}]$$

   If we want to admit only increasing sequences, we can omit the $[\mathrm{ForLT_{BS}}]$ rule. $[\mathrm{ForEQ_{BS}}]$ can also be easily modified in order to avoid the ending sequence value.

   Keeping the same assumptions followed for the big-step semantics, its small-step semantics can be defined as

$$\frac{\mathcal{A}[\![e_2 - e_1]\!]\sigma =_{\mathbb{Z}} 0_{\mathbb{Z}}}{\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \longrightarrow \langle S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle}\ [\mathrm{ForEQ_{SS}}]$$

$$\frac{\mathcal{A}[\![e_2 - e_1]\!]\sigma >_{\mathbb{Z}} 0_{\mathbb{Z}}}{\begin{array}{l}\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \longrightarrow \\ \quad \langle S; \texttt{for}\ x := e_1 + 1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle\end{array}}\ [\mathrm{ForGT_{SS}}]$$

$$\frac{\mathcal{A}[\![e_2 - e_1]\!]\sigma <_{\mathbb{Z}} 0_{\mathbb{Z}}}{\begin{array}{l}\langle \texttt{for}\ x := e_1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma \rangle \longrightarrow \\ \quad \langle S; \texttt{for}\ x := e_1 - 1\ \texttt{to}\ e_2\ \texttt{do}\ S, \sigma\,[x \mapsto \mathcal{A}[\![e_1]\!]\sigma] \rangle\end{array}}\ [\mathrm{ForLT_{SS}}]$$

   where it is easy to adapt the rules if we want to change the construct requirements in the same way as discussed for the big-step semantics.