Assignment 2

Javier Sagredo

October 27, 2021

Exercise 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

- **Big-step semantics** we are going to define $\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma'$. This is a straightforward definition considering the specification.

$$\frac{\langle S,\sigma\rangle \Downarrow \sigma'' \qquad \mathcal{B}[\![b]\!]\sigma'' = false \qquad \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma''\rangle \Downarrow \sigma'}{\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma'}\ [RepeatF_{BS}]$$

$$\frac{\langle S,\sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = true}{\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma'}\ [RepeatT_{BS}]$$

- **Small-step semantics**: The small step semantics will be defined with a simple rewriting step.

$$\frac{}{\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \rightarrow \langle S; \texttt{if}\ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma\rangle}\ [Repeat_{SS}]$$

- **Proofs:** We will do the following proofs now:
  1. Proof of equivalence on big-step semantics

2. Proof of equivalence on small-step semantics
3. Proof of determinism on big-step semantics
4. Proof of determinism on small-step semantics

We need to do these proofs because proving that there is equivalence on big-step semantics doesn't necessarily imply that there is equivalence on small-step semantics. And in order to assert that transitions (either through big-step or small-step) always yield the same value, we need to prove the determinism on both. We could alternatively prove equivalence and determinism for one of the semantics and prove that there is equivalence on the semantics including this construct into the `While` language. More concisely, we are going to prove this:

$$\begin{array}{ccc} \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma' & \overset{\text{Uses determinism on } \Downarrow}{\Longleftrightarrow} & \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \Downarrow \sigma' \\ & & \Updownarrow \text{Proved in class} \\ \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \to^* \sigma' & \overset{\text{Uses determinism on } \to}{\Longleftrightarrow} & \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \to^* \sigma' \end{array}$$

But one could alternatively prove the following diagram:

$$\begin{array}{ccc} \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma' & \overset{\text{Uses determinism on } \Downarrow}{\Longleftrightarrow} & \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \Downarrow \sigma' \\ \Updownarrow & & \Updownarrow \text{Proved in class} \\ \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \to^* \sigma' & & \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \to^* \sigma' \end{array}$$

Proof of equivalence on big-step semantics
We shall prove that:

$$\begin{array}{c} \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \Downarrow \sigma'' \\ \Updownarrow \\ \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \Downarrow \sigma'' \end{array}$$

Prove $\Rightarrow$**)** We will make the proof by induction on the shape of the derivation tree.

Base case: Using the axiom $[RepeatT_{BS}]$, we can derive the following tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = true}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'}\,[RepeatT_{BS}]$$

With those same two premises, namely $\langle S, \sigma\rangle \Downarrow \sigma'$ and $\mathcal{B}[\![b]\!]\sigma' = true$, rephrased as $\mathcal{B}[\![\neg b]\!]\sigma' = false$, we can assemble the following derivation tree using the $[WhileF_{BS}]$ and $[Seq_{BS}]$ rules:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \dfrac{\mathcal{B}[\![\neg b]\!]\sigma' = false}{\langle \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma'}\,[WhileF_{BS}]}{\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma\rangle \Downarrow \sigma'}\,[Seq_{BS}]$$

Note that we can do this because $\langle S, \sigma\rangle \Downarrow \sigma'$ is deterministic.

Induction Hypothesis: We can define from this point on the following Induction Hypothesis:

$$\langle \texttt{repeat } S \texttt{ until } b, \sigma_{in}\rangle \Downarrow \sigma'_{in} \Rightarrow \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma_{in}\rangle \Downarrow \sigma'_{in}$$

Where this hypothesis can be applied on a subtree of the initial one.

Inductive case: Then using the $[RepeatF_{BS}]$, we can derive the following tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = false \qquad \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \Downarrow \sigma''}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma''}\,[RepeatF_{BS}]$$

Where we can use the premises, $\langle S, \sigma\rangle \Downarrow \sigma'$ (thanks to it being deterministic) and $\mathcal{B}[\![b]\!]\sigma' = false$ rephrased as $\mathcal{B}[\![\neg b]\!]\sigma' = true$, and apply the induction hypothesis on $\langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \Downarrow \sigma''$ to get $\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''$. Through this process, we arrive at the following derivation tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![\neg b]\!]\sigma' = true \qquad \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}{T}$$

Where we can use the rules $[WhileT_{BS}]$ and $[Seq_{BS}]$ to complete the proof in this direction:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \dfrac{\mathcal{B}[\![\neg b]\!]\sigma' = true \qquad \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}{\langle \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}\,[WhileT_{BS}]}{\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma\rangle \Downarrow \sigma''}\,[Seq_{BS}]$$

Prove $\Leftarrow$) We will follow a similar approach and apply induction on the derivation tree.

Base case: Using the axiom $[WhileF_{BS}]$ together with the rule $[Seq_{BS}]$ we can construct the following tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \dfrac{\mathcal{B}[\![\neg b]\!]\sigma' = false}{\langle \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma'}\,[WhileF_{BS}]}{\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma\rangle \Downarrow \sigma'}\,[Seq_{BS}]$$

Using the same premises $\langle S, \sigma\rangle \Downarrow \sigma'$ (thanks to it being deterministic) and $\mathcal{B}[\![\neg b]\!]\sigma' = false$ rephrased as $\mathcal{B}[\![b]\!]\sigma' = true$ we can apply the $[RepeatT_{BS}]$ axiom in a straightforward manner:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = true}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'}\,[RepeatT_{BS}]$$

Induction Hypothesis: We can define from this point on the following Induction hypothesis:

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma_{in}\rangle \Downarrow \sigma'_{in} \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma_{in}\rangle \Downarrow \sigma'_{in}$$

Where this hypothesis can be applied on a subtree of the initial one.

Inductive case: Then using the $[WhileT_{BS}]$ and $[Seq_{BS}]$ rules, we can derive the following tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \dfrac{\mathcal{B}[\![\neg b]\!]\sigma' = true \qquad \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}{\langle \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}\,[WhileT_{BS}]}{\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''}\,[Seq_{BS}]$$

Where we can use the premises, $\langle S, \sigma\rangle \Downarrow \sigma'$ (thanks to it being deterministic) and $\mathcal{B}[\![\neg b]\!]\sigma' = true$ rephrased as $\mathcal{B}[\![b]\!]\sigma' = false$, and apply the induction hypothesis on $\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''$ to get $\langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \Downarrow \sigma''$. Through this process, we arrive at the following derivation tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = false \qquad \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \Downarrow \sigma''}{T}$$

Where we can use the rule $[RepeatF_{BS}]$ to complete the proof in this direction:

$$\frac{\langle S,\sigma\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]\sigma' = false \qquad \langle \texttt{repeat } S \texttt{ until } b,\sigma'\rangle \Downarrow \sigma''}{\langle \texttt{repeat } S \texttt{ until } b,\sigma\rangle \Downarrow \sigma''}\,[RepeatF_{BS}]$$

Proof of equivalence on small-step semantics
We shall prove the following:

$$\langle \texttt{repeat } S \texttt{ until } b,\sigma\rangle \rightarrow^* \sigma''$$
$$\Updownarrow$$
$$\langle S; \texttt{while } \neg b \texttt{ do } S,\sigma\rangle \rightarrow^* \sigma''$$

Note that during these proofs we are only concerned to the configurations where the execution terminates in a given state. So the statements should be read as "If A terminates in state x then B terminates in state x". We will not be concerned to the non-terminating executions.

Prove $\Rightarrow$) We will make the proof by induction on the length of the derivation sequence.

Base case: We will use:

- the rewriting step of $[Repeat_{SS}]$ followed by
- a finite sequence of steps executed through the $[Seq2_{SS}]$ rule
- finished with a $[Seq1_{ss}]$ rewriting
- and finally use the rule $[If1_{SS}]$.

Therefore we get the following derivation sequence:

$$\begin{aligned}
\langle \texttt{repeat } S \texttt{ until } b,\sigma\rangle &\overset{[Repeat_{SS}]}{\rightarrow} \langle S; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b,\sigma\rangle \\
&\overset{\langle S,\sigma\rangle \overset{[Seq2_{SS}]}{\rightarrow}{}^* \langle S',\sigma'\rangle}{\rightarrow^*} \langle S'; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b,\sigma'\rangle \\
&\overset{\langle S',\sigma'\rangle \overset{[Seq1_{SS}]}{\rightarrow} \sigma''}{\rightarrow} \langle \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b,\sigma''\rangle \\
&\overset{[If1_{SS}]}{\rightarrow} \langle \texttt{ skip },\sigma''\rangle \\
&\overset{[skip_{SS}]}{\rightarrow} \sigma''
\end{aligned}$$

Where we assumed the fact that $\mathcal{B}[\![b]\!]\sigma'' = true$. We can now reconstruct using these steps and the fact that $\langle S, \sigma\rangle \rightarrow^* \sigma''$ is deterministic, the following derivation sequence for $\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle$:

$$\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \overset{\langle S,\sigma\rangle \overset{[Seq2_{SS}]}{\rightarrow^*} \langle S',\sigma'\rangle}{\rightarrow^*} \langle S'; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle$$
$$\overset{\langle S',\sigma'\rangle \overset{[Seq1_{SS}]}{\rightarrow} \sigma''}{\rightarrow} \langle \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma''\rangle$$
$$\overset{[While1_{SS}]}{\rightarrow} \sigma''$$

Where by the determinism of $\langle S, \sigma\rangle \rightarrow^* \sigma''$ we can know that as previously $\mathcal{B}[\![b]\!]\sigma'' = true$, now $\mathcal{B}[\![\neg b]\!]\sigma'' = false$.

Induction Hypothesis: We have a finite number of steps to evaluate $\langle S, \sigma\rangle \rightarrow^{k_S} \sigma'$ which we will call k_S. We can construct the following induction hypothesis:

$$\langle \texttt{repeat}\ \ S\ \ \texttt{until}\ \ b, \sigma'\rangle \rightarrow^{k(2+k_S)+1} \sigma'' \Rightarrow \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \rightarrow^* \sigma''$$

Where the number of steps comes from:

- The $[skip_{SS}]$ step as a final step.
- The k_S steps to fully evaluate S plus the rewriting step of $[Repeat_{SS}]$ and the branching step of $[If1_{SS}]$ or $[If2_{SS}]$ which is to be executed k times.

Intuitively we are going to make induction on the number of unfolds of `repeat` dictated by the chain of small step rewriting steps.

Inductive case: We want to prove that provided the induction hypothesis, we can unfold one more `repeat` and still the property holds. Or more precisely, assuming:

$$\langle \texttt{repeat}\ \ S\ \ \texttt{until}\ \ b, \sigma'\rangle \rightarrow^{k(2+k_S)+1} \sigma'' \Rightarrow \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \rightarrow^* \sigma''$$

then

$$\langle \texttt{repeat}\ \ S\ \ \texttt{until}\ \ b, \sigma\rangle \rightarrow^{(k+1)(2+k_S)+1} \sigma'' \Rightarrow \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \rightarrow^* \sigma''$$

We can now break the derivation sequence into a right sequence of length $k(2\langle + k_S) + 1$ and a left sequence of length $(2 + k_S)$ steps:

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \rightarrow^{2+k_S} \langle S', \sigma'\rangle \rightarrow^{k(2+k_S)+1} \sigma''$$

If we now can make $S' = \texttt{repeat}\ S\ \texttt{until}\ b$ then we can apply the induction hypothesis and complete the proof. Let's now dive into the first chunk of derivation steps:

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \rightarrow^{2+k_S} \langle S', \sigma'\rangle$$

We know the only step we can apply is $[Repeat_{SS}]$ and then we can complete the evaluation of S (with $[Seq2_{SS}]$ and $[Seq1_{SS}]$) in k_S steps, so more concretely:

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \overset{[Repeat_{SS}]}{\rightarrow} \langle S; \texttt{if}\ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma\rangle \overset{\langle S,\sigma\rangle \rightarrow^{k_S} \sigma'}{\rightarrow} \langle \texttt{if}\ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma'\rangle$$

Now we depend on the value of $\mathcal{B}[\![b]\!]\sigma'$ but if it was $true$ we would be in the base case again, so in this case (disjoint from the one mentioned) it must be $false$. We can therefore apply the rule $[If2_{SS}]$ to make one more rewriting step:

$$\langle \texttt{if}\ b\ \texttt{then skip else repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \overset{[If2_{SS}]}{\rightarrow} \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'\rangle$$

And now it holds, precisely as we were requiring, the following derivation sequence:

$$\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma\rangle \rightarrow^{2+k_S} \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \rightarrow^{k(2+k_S)+1} \sigma''$$

Where we can apply the induction hypothesis to assert that the right side is equivalent to $\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \rightarrow^* \sigma''$. Now we can, using the same rules that were applied before, recover a derivation sequence as follows:

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

Considering the determinism of the language and that $\langle S, \sigma\rangle \rightarrow^{k_S} \sigma'$, we can dive deeper into the derivation sequence:

$$\langle S', \sigma\rangle \rightarrow^* \langle S; S'', \sigma\rangle \rightarrow^{k_S} \langle S'', \sigma'\rangle \rightarrow^* \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \rightarrow^* \sigma''$$

Which states that starting on some configuration $\langle S', \sigma \rangle$ we can make a finite amount of derivations to arrive to $\langle S; S'', \sigma \rangle$, point at which with k_s derivations we will arrive to $\langle S'', \sigma' \rangle$ and on a finite number of steps we will arrive to the desired situation. The only rule that can be applied on the second star (due to 1. the state not changing 2. yielding a expression with `while` inside 3. $\mathcal{B}[\![b]\!]\sigma' = false$ or conversely $\mathcal{B}[\![\neg b]\!]\sigma' = true$) is $[WhileT_{SS}]$, so $S'' =$ `while` $\neg b$ `do` S:

$$\langle S', \sigma \rangle \rightarrow^* \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \rightarrow^{k_S} \langle \texttt{while } \neg b \texttt{ do } S, \sigma' \rangle \overset{[WhileT_{SS}]}{\rightarrow} \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma' \rangle \rightarrow^* \sigma''$$

And now we can even vanish the first star as we already have the derivation sequence we needed, starting on the appropriate state σ and finishing in σ'', completing then the derivation sequence:

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

So now the inductive step is complete and we have that assuming:

$$\langle \texttt{repeat } S \texttt{ until } b, \sigma' \rangle \rightarrow^{k(2+k_S)+1} \sigma'' \Rightarrow \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma' \rangle \rightarrow^* \sigma''$$

it holds that

$$\langle \texttt{repeat } S \texttt{ until } b, \sigma \rangle \rightarrow^{(k+1)(2+k_S)+1} \sigma'' \Rightarrow \langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \rightarrow^* \sigma''$$

completing then the proof by induction.

Prove $\Leftarrow$**)** We will make the proof by induction on the length of the derivation sequence.

Base case: We will use:

- a finite sequence of steps executed through the $[Seq2_{SS}]$ rule
- finished with a $[Seq1_{ss}]$ rewriting
- the non-recursive rule $[While1_{SS}]$.

Therefore we get the following derivation sequence:

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma \rangle \overset{[Seq2_{SS}]}{\rightarrow^*} \langle S'; \texttt{while } \neg b \texttt{ do } S, \sigma' \rangle \overset{\langle S', \sigma' \rangle \overset{[Seq1_{SS}]}{\rightarrow} \sigma''}{\rightarrow} \langle \texttt{while } \neg b \texttt{ do } S, \sigma'' \rangle \overset{[While1_{SS}]}{\rightarrow} \sigma''$$

Where we assumed the fact that $\mathcal{B}[\![\neg b]\!]\sigma'' = false$. We can now reconstruct using these steps and the fact that $\langle S, \sigma\rangle \rightarrow^* \sigma''$ is deterministic, the following derivation sequence for $\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle$:

$$\begin{aligned}
\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle &\overset{[Repeat_{SS}]}{\rightarrow} \langle S; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma\rangle \\
&\overset{\langle S,\sigma\rangle \overset{[Seq2_{SS}]}{\rightarrow^*} \langle S',\sigma'\rangle}{\rightarrow^*} \langle S'; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma'\rangle \\
&\overset{\langle S',\sigma'\rangle \overset{[Seq1_{SS}]}{\rightarrow} \sigma''}{\rightarrow} \langle \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma''\rangle \\
&\overset{[If1_{SS}]}{\rightarrow} \langle \texttt{skip}, \sigma''\rangle \\
&\overset{[skip_{SS}]}{\rightarrow} \sigma''
\end{aligned}$$

Where by the determinism of $\langle S, \sigma\rangle \rightarrow^* \sigma''$ we can know that as previously $\mathcal{B}[\![\neg b]\!]\sigma'' = false$, now $\mathcal{B}[\![b]\!]\sigma'' = true$.

Induction Hypothesis: We have a finite number of steps to evaluate $\langle S, \sigma\rangle \rightarrow^{k_S} \sigma'$ which we will call k_S. We can construct the following induction hypothesis:

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \rightarrow^{k(1+k_S)} \sigma'' \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \rightarrow^* \sigma''$$

Where the number of steps comes from:

- The k_S steps to fully evaluate S plus the rewriting step of $[While1_{SS}]$ or $[While2_{SS}]$.
- Which is to be executed k times.

Intuitively we are going to make induction on the number of unfolds of `while` dictated by the chain of small step rewriting steps.

Inductive case: We want to prove that provided the induction hypothesis, we can unfold one more `while` and still the property holds. Or more precisely, assuming:

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \rightarrow^{k(1+k_S)} \sigma'' \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \rightarrow^* \sigma''$$

then

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma\rangle \rightarrow^{(k+1)(1+k_S)} \sigma'' \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \rightarrow^* \sigma''$$

We can now break the derivation sequence into a right sequence of length $k(1 + k_S)$ and a left sequence of length $(1 + k_S)$ steps:

$$\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \rightarrow^{1+k_S} \langle S', \sigma'\rangle \rightarrow^{k(1+k_S)} \sigma''$$

If we now can make $S' = S; \texttt{while}\ \neg b\ \texttt{do}\ S$ then we can apply the induction hypothesis and complete the proof. Let's now dive into the first chunk of derivation steps:

$$\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \rightarrow^{1+k_S} \langle S', \sigma'\rangle$$

We know the only first steps we can apply are to complete the evaluation of S (with $[Seq2_{SS}]$ and $[Seq1_{SS}]$) in k_S steps, so more concretly:

$$\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \overset{\langle S,\sigma\rangle \rightarrow^{k_S} \sigma'}{\rightarrow} \langle \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle$$

Now we depend on the value of $\mathcal{B}[\![\neg b]\!]\sigma'$ but if it was $false$ we would be in the base case again, so in this case (disjoint from the one mentioned) it must be $true$. We can therefore apply the rule $[While2_{SS}]$ to make one more rewriting step:

$$\langle \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \overset{[While2_{SS}]}{\rightarrow} \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle$$

And now it holds, precisely as we were requiring, the following derivation sequence:

$$\langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma\rangle \rightarrow^{1+k_S} \langle S; \texttt{while}\ \neg b\ \texttt{do}\ S, \sigma'\rangle \rightarrow^{k(1+k_S)} \sigma''$$

Where we can apply the induction hypothesis to assert that the right side is equivalent to $\langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \rightarrow^* \sigma''$. Now we can, using the same rules that were applied before, recover a derivation sequence as follows:

$$\langle S', \sigma\rangle \rightarrow^* \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \rightarrow^* \sigma''$$

Considering the determinism of the language and that $\langle S, \sigma\rangle \rightarrow^{k_S} \sigma'$, we can dive deeper into the chain of derivations:

$$\langle S', \sigma\rangle \rightarrow^* \langle S; S'', \sigma\rangle \rightarrow^{k_S} \langle S'', \sigma'\rangle \rightarrow^* \langle \texttt{repeat}\ S\ \texttt{until}\ b, \sigma'\rangle \rightarrow^* \sigma''$$

By the determinism of $\langle S, \sigma\rangle \rightarrow^{k_S} \sigma'$ we know that $\mathcal{B}[\![\neg b]\!]\sigma'' = true$ as otherwise we would be in the base case. Therefore we can apply the $[If2_{SS}]$ rule on the second star, equating then:

$$S'' = \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b$$

So we have the following chain of derivations:

$$\begin{aligned}\langle S', \sigma\rangle &\rightarrow^* \langle S; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma\rangle \\ &\rightarrow^{k_S} \langle \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma'\rangle \\ &\overset{[If2_{SS}]}{\rightarrow} \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \\ &\rightarrow^* \sigma''\end{aligned}$$

But a rule we can put on the first star is $[Repeat_{SS}]$ yielding the following chain of derivations:

$$\begin{aligned}\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle &\overset{[Repeat_{SS}]}{\rightarrow} \langle S; \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma\rangle \\ &\rightarrow^{k_S} \langle \texttt{if } b \texttt{ then skip else repeat } S \texttt{ until } b, \sigma'\rangle \\ &\overset{[If2_{SS}]}{\rightarrow} \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \\ &\rightarrow^* \sigma''\end{aligned}$$

Or in a more succint way:

$$\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \rightarrow^* \sigma''$$

as wanted.

Therefore we have that assuming:

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma'\rangle \rightarrow^{k(1+k_S)} \sigma'' \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma'\rangle \rightarrow^* \sigma''$$

it holds that

$$\langle S; \texttt{while } \neg b \texttt{ do } S, \sigma\rangle \rightarrow^{(k+1)(1+k_S)} \sigma'' \Rightarrow \langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \rightarrow^* \sigma''$$

completing then the proof by induction.

Determinism of the big-step semantics

As this was used above, we need to extend the determinism result for this new construct, to be able to claim that $\langle S, \sigma\rangle \Downarrow \sigma'$ is deterministic no matter the value of S. We will do so using induction on the shape of the derivation tree.

If $\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'$ and $\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma''$ then $\sigma' = \sigma''$

Induction hypothesis: We will assume that on smaller derivation trees than the one we currently are demonstrating its determinism, those necessarily are deterministic, or more precisely:

$$\langle S, \sigma_{in}\rangle \Downarrow \sigma'_{in}$$

Where this hypothesis, as said, can be applied only on subtrees of the current tree.

- If $\mathcal{B}[\![b]\!]\sigma_{in} = true$ then by induction hypothesis on the determinism of $\langle S, \sigma\rangle \Downarrow \sigma_{in}$

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma_{in} \qquad \mathcal{B}[\![b]\!]\sigma_{in} = true}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma_{in}}\,[RepeatT_{BS}]$$

  and we have that $\sigma' = \sigma'' = \sigma_{in}$.

- If $\mathcal{B}[\![b]\!]\sigma_{in} = false$ then by induction hypothesis on both the determinism of $\langle S, \sigma\rangle \Downarrow \sigma_{in}$ and induction hypothesis on the shape of the derivation tree for $\langle \texttt{repeat } S \texttt{ until } b, \sigma_{in}\rangle \Downarrow \sigma'_{in}$, such expression must come from a finite derivation tree and therefore we have the following deterministic tree:

$$\frac{\langle S, \sigma\rangle \Downarrow \sigma_{in} \qquad \mathcal{B}[\![b]\!]\sigma_{in} = false \qquad \langle \texttt{repeat } S \texttt{ until } b, \sigma_{in}\rangle \Downarrow \sigma'_{in}}{\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \Downarrow \sigma'_{in}}\,[RepeatF_{BS}]$$

  and we have that $\sigma' = \sigma'' = \sigma'_{in}$.

Determinism of the small-step semantics

This one is straight-forward because there is only one rule to apply. We essentially have to prove ththe following:

$\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \to \gamma$ and $\langle \texttt{repeat } S \texttt{ until } b, \sigma\rangle \to \gamma'$ imply $\gamma = \gamma'$

Which as the only rule that can be applied is $[Repeat_{SS}]$, the configurations γ and γ' are indeed necessarily the same.

Exercise 3 *Add the following iterative construct to* While*:* `for` $x := e_1$ `to` e_2 `do` S*. Define its big-step and small-step semantic rules. You cannot rely on the* `while` *or* `repeat` *construct to do this exercise.*

- **Big-step semantics**: We will define two rules for the big step semantics of the `for` expression:

$$\frac{\mathcal{B}[\![e_1 \leq e_2]\!]\sigma = true \qquad \langle S, \sigma[x \mapsto \mathcal{A}[\![e_1]\!]\sigma]\!]\rangle \Downarrow \sigma' \qquad T'}{\langle \texttt{for } x := e_1 \texttt{ to } e_2 \texttt{ do } S, \sigma\rangle \Downarrow \sigma''} [ForT_{BS}]$$

  where $T' = \langle \texttt{for } x := e_1 + 1 \texttt{ to } e_2 \texttt{ do } S, \sigma'\rangle \Downarrow \sigma''$.

$$\frac{\mathcal{B}[\![e_1 \leq e_2]\!]\sigma = false}{\langle \texttt{for } x := e_1 \texttt{ to } e_2 \texttt{ do } S, \sigma\rangle \Downarrow \sigma[x \mapsto \mathcal{A}[\![e_1]\!]\sigma]} [ForF_{BS}]$$

- **Small-step semantics:** The small step semantics will consist of a rewriting step:

$$\frac{}{\langle \texttt{for } x := e_1 \texttt{ to } e_2 \texttt{ do } S, \sigma\rangle \rightarrow \langle x := e_1; \texttt{if } e_1 \leq e_2 \texttt{ then } S' \texttt{ else skip}, \sigma\rangle} [For_{SS}]$$

  where $S' = S; \texttt{for } x := e_1 + 1 \texttt{ to } e_2 \texttt{ do } S$