FM Chapter 5 – Language Based Security – Exercise 5.10

Lemma If $\langle q;\sigma\rangle \Longrightarrow_1^* \langle q';\sigma'\rangle$ then we also have $\langle q;\sigma\rangle \Longrightarrow_0^* \langle q';\sigma'\rangle$.

Proof. By induction on the size of the trace $\langle q;\sigma\rangle \Longrightarrow_1^* \langle q';\sigma'\rangle$.

- **Base case**: Holds vacuously, as there is no successor of $\langle q;\sigma\rangle$.
- **Induction Hypothesis**: Assume that if $\langle q;\sigma\rangle \Longrightarrow_1^n \langle q';\sigma'\rangle$ then we also have $\langle q;\sigma\rangle \Longrightarrow_0^n \langle q';\sigma'\rangle$.
- **Induction Step**: We need to show that if $\langle q;\sigma\rangle \Longrightarrow_1^{n+1} \langle q'';\sigma''\rangle$ then we can construct $\langle q;\sigma\rangle \Longrightarrow_0^{n+1} \langle q'';\sigma''\rangle$.

  With this we have that $\langle q;\sigma\rangle \Longrightarrow_1^n \langle q';\sigma'\rangle \overset{act}{\Longrightarrow}_1 \langle q'';\sigma''\rangle$. First notice that by IH on $\langle q;\sigma\rangle \Longrightarrow_1^n \langle q';\sigma'\rangle$ we get $\langle q;\sigma\rangle \Longrightarrow_0^n \langle q';\sigma'\rangle$.

  It now remains to show that if $\langle q';\sigma'\rangle \overset{act}{\Longrightarrow}_1 \langle q'';\sigma''\rangle$ then $\langle q';\sigma'\rangle \overset{act}{\Longrightarrow}_0 \langle q'';\sigma''\rangle$. We now have three cases for *act*:

  - Case $act = \texttt{skip}$. Because $\langle q';\sigma'\rangle \overset{\texttt{skip}}{\Longrightarrow}_1 \langle q'';\sigma''\rangle$, then we must have that $\mathcal{S}_1[\![\texttt{skip}]\!](\sigma') = \sigma'$, so $\sigma' = \sigma''$. Furthermore $\mathcal{S}_0[\![\texttt{skip}]\!](\sigma') = \sigma' = \sigma''$, and we now get that $\langle q';\sigma'\rangle \overset{\texttt{skip}}{\Longrightarrow}_0 \langle q'';\sigma''\rangle$.
  - Case $act = x := a\{X\}$. Because $\langle q';\sigma'\rangle \xrightarrow{x:=a\{X\}}_1 \langle q'';\sigma''\rangle$, then we must have that $\mathcal{A}[\![a]\!](\sigma')$ is defined and that $X \cup \mathsf{fv}(a) \rightrightarrows \{X\}$, which gives that $\mathcal{S}_1[\![x := a\{X\}]\!](\sigma') = \sigma'[x \mapsto \mathcal{A}[\![a]\!](\sigma')]$. So $\sigma'' = \sigma'[x \mapsto \mathcal{A}[\![a]\!](\sigma')]$.
    Because $\mathcal{A}[\![a]\!](\sigma')$ is defined and $0 = 0$, then we also have that $\mathcal{S}_0[\![x := a\{X\}]\!](\sigma') = \sigma''$, and we now get that $\langle q';\sigma'\rangle \xrightarrow{x:=a\{X\}}_0 \langle q'';\sigma''\rangle$.
  - Case $act = b$. Because $\langle q';\sigma'\rangle \overset{act}{\Longrightarrow}_1 \langle q'';\sigma''\rangle$ then we must have that $\mathcal{B}[\![b]\!](\sigma')$ is defined and holds, and we get that $\mathcal{S}_1[\![b]\!](\sigma') = \sigma'$. So $\sigma'' = \sigma'$.
    Because $\mathcal{B}[\![b]\!](\sigma')$ is defined and holds, then we get that $\mathcal{S}_0[\![b]\!](\sigma') = \sigma''$, and we now get that $\langle q';\sigma'\rangle \overset{b}{\Rightarrow}_0 \langle q'';\sigma''\rangle$. $\square$

The program in Try It Out 5.9 with $x \not\rightarrow y$ would be allowed to progress by the reference-monitor semantics $\Longrightarrow_0$, but is halted by the reference-monitor semantics $\Longrightarrow_1$. This will therefore give us that $\langle q;\sigma\rangle \Longrightarrow_0^* \langle q';\sigma'\rangle$ but where $\langle q;\sigma\rangle \not\Longrightarrow_1^* \langle q';\sigma'\rangle$.