LaTeX Rendering

February 2022

You can write your homework completely in HybLang!

We are tasked to show that

$$\boxed{\begin{array}{l}\mathcal{L}_{\mathsf{L}}\\ \hline \textsc{ctxt}(m \in \{\texttt{0},\texttt{1}\}):\\ \quad k \leftarrow \{\texttt{0},\texttt{1}\}\\ \quad c := k \oplus m\\ \quad \text{return } c\&m\end{array}} \equiv \boxed{\begin{array}{l}\mathcal{L}_{\mathsf{R}}\\ \hline \textsc{ctxt}(m \in \{\texttt{0},\texttt{1}\}):\\ \quad c \leftarrow \{\texttt{0},\texttt{1}\}\\ \quad \text{return } c\end{array}}$$

are interchangeable.

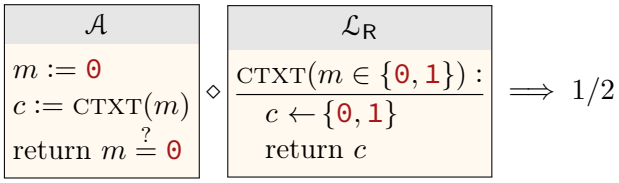
This obviously not the case, since the distinguishing program

$$\boxed{\begin{array}{l}\mathcal{A}\\ \hline m := \texttt{0}\\ c := \textsc{ctxt}(m)\\ \text{return } m \stackrel{?}{=} \texttt{0}\end{array}}$$

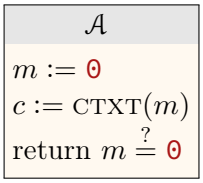
always returns true when linked to the L library. Since we have

$$\boxed{\begin{array}{l}\mathcal{A}\\ \hline m := \texttt{0}\\ c := \textsc{ctxt}(m)\\ \text{return } m \stackrel{?}{=} \texttt{0}\end{array}} \diamond \boxed{\begin{array}{l}\mathcal{L}_{\mathsf{L}}\\ \hline \textsc{ctxt}(m \in \{\texttt{0},\texttt{1}\}):\\ \quad k \leftarrow \{\texttt{0},\texttt{1}\}\\ \quad c := k \oplus m\\ \quad \text{return } c\&m\end{array}} \Longrightarrow \text{true}$$

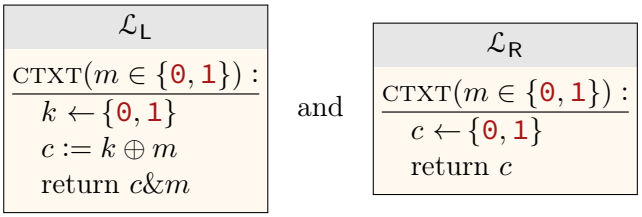
and



so we know that



is a distinguishing program, so it is not the case that



are interchangeable, thus proving a counterexample of the claim.