Formal Techniques – 2015-09-03

Exercise 1. *Let $f : A \to B$ be an arbitrary function between the DCPOs A, B. Assume that, for any directed $D \subseteq A$, we have that $\bigsqcup^B f[D]$ (exists and) is equal to $f(\bigsqcup^A D)$. Then, prove that f is monotonic.*

Exercise 2. *Consider the following protocol excerpt written in the* applied-pi *notation.*

$$\begin{aligned} ! \; . \; \mathit{out}\ \mathsf{a} \; . \; (\; & \mathit{in}\ X \; . \; \mathit{out}\ \mathsf{f}(X) \; . \; () \\ | \; & \mathit{out}\ \mathsf{b} \; . \; ()) \end{aligned}$$

Apply the control flow analysis to the protocol above, generating a tree automaton to over-approximate the message flow, as done by function gen(...). Provide a list of states for such automaton and the transitions among them. For each state, briefly hint to its relationship with the protocol above.

Exercise 3. *Consider the following tree automaton*

$$\begin{aligned}
&@a : \mathsf{cons}(@c, @b), \mathsf{cons}(@g, @f), \mathsf{enc}(@d, @e), \mathsf{dec}(@a, @a).\\
&@b : \mathsf{fst}(@a).\\
&@c : \mathsf{snd}(@a).\\
&@d : \mathsf{m}.\\
&@e : \mathsf{cons}(@f, @g).\\
&@f : \mathsf{k1}.\\
&@g : \mathsf{k2}.
\end{aligned}$$

and the rewriting rules

$$\mathsf{dec}(\mathsf{enc}(M, K), K) \Rightarrow M \qquad \mathsf{fst}(\mathsf{cons}(X, Y)) \Rightarrow X \qquad \mathsf{snd}(\mathsf{cons}(X, Y)) \Rightarrow Y$$

Apply the completion algorithm to the above automaton, building an over-approximation for the languages associated to its states. Assuming @a *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of message* m.

Exercise 4. *Formally prove the following formula exploiting the Curry-Howard isomorphism.*

$$\forall p, q : \mathsf{Prop}.\ ((p \to q) \vee q) \to (p \to q)$$

Exercise 5. *For each $i \in \{1, 2\}$, let $\mathcal{C}_i$ and $\mathcal{A}_i$ be CLs with a Galois connection $\alpha_i : \mathcal{C}_i \leftrightarrows \mathcal{A}_i : \gamma_i$. Construct a Galois connection*

$$\alpha : [\mathcal{C}_1 \to \mathcal{C}_2] \leftrightarrows [\mathcal{A}_1 \to \mathcal{A}_2] : \gamma$$

where $[- \to -]$ denotes the CL of Scott-continuous functions. Prove that yours is indeed a Galois connection.

Exercise 6. *Let A be a CL, and $f : A \to A$ be a monotonic function. Prove that $fix(f) = fix(f \circ f)$, where fix denotes the minimum fixed point.*