Formal Techniques – 2020-06-11

Exercise 1. *State and prove Kleene's fixed point theorem.*

Exercise 2. *Consider the following tree automaton*

$$\begin{array}{llll} @\mathsf{a} \to \mathsf{k1}, \mathsf{enc}(@\mathsf{b}, @\mathsf{c}), \mathsf{enc}(@\mathsf{d}, @\mathsf{e}), \mathsf{dec}(@\mathsf{a}, @\mathsf{a}) & & & \\ @\mathsf{b} \to \mathsf{k3}, \mathsf{k4} & @\mathsf{c} \to \mathsf{k1}, \mathsf{k5}, \mathsf{m} & @\mathsf{d} \to \mathsf{m} & @\mathsf{e} \to \mathsf{k2}, \mathsf{k5}, \mathsf{m} \end{array}$$

and the rewriting rule

$$\mathsf{dec}(\mathsf{enc}(M, K), K) \Rightarrow M$$

Apply the completion algorithm to the above automaton, building an over-approximation for the languages associated to its states which is closed under rewriting. 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 3. *Consider the following protocol excerpt written in the* applied-pi *notation.*

$$\begin{array}{ll} (& \mathit{out}\ \mathsf{a}\ .\ \mathit{in}\ X\ .\ !\ .\ (\mathit{out}\ \mathsf{b}\ .\ () \mid \mathit{in}\ Z\ .\ \mathit{out}\ \mathsf{g}(X, Z)\ .\ ()) \\ \mid & \mathit{in}\ Y\ .\ \mathit{out}\ \mathsf{f}(Y)\ .\ () \quad) \end{array}$$

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. Make each state clearly related to a part of the protocol above.

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

$$\forall p, q, r, s, t : \mathsf{Prop}.\ (p \to (q \wedge r)) \to [((s \vee r) \to t) \to [(p \vee s) \to (q \vee t)]]$$

Exercise 5.

1. *[25%] Let A be a poset, and B be a subposet of A (hence, $B \subseteq A$ and $(\sqsubseteq_B) = (\sqsubseteq_A) \cap B^2$). Let $X \subseteq B$ be any set such that there exists $x = \bigsqcup^A X$. Prove that, if $x \in B$, then there exists $\bigsqcup^B X$ and that coincides with x.*

2. *[10%] Let A, B, C be DCPOs, and let $\alpha : A \to C$ and $\beta : B \to C$ be two Scott-continuous functions.*

   A triple (X, f_A, f_B) is said to be a cone *when X is a DCPO, $f_A : X \to A$ and $f_B : X \to B$ are Scott-continuous, and $\alpha \circ f_A = \beta \circ f_B$.*

   Construct a cone (X, f_A, f_B) where $X \subseteq A \times B$ is a subposet and $\alpha \circ f_A = \beta \circ f_B$ directly holds "by definition of X". Your definition must also satisfy the property below.

3. *[15%] Prove that, if (Y, g_A, g_B) is a cone, then there is a <u>unique</u> Scott-continuous $m : Y \to X$ where $f_A \circ m = g_A$ and $f_B \circ m = g_B$.*

4. *[50%] Verify that the above subposet $X \subseteq A \times B$ is indeed a DCPO.*