Formal Techniques – 2014-07-24

Exercise 1. *State and prove the Kleene fixed point theorem.*

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

$$\begin{array}{l}(\; ! \; . \; in \; X \; . \; in \; Y \; . \; out \; \mathsf{enc}(X,Y) \; . \; () \\ \mid out \; \mathsf{m} \; . \; in \; Z \; . \; out \; \mathsf{h}(Z) \; . \; () \;)\end{array}$$

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. For each state, briefly hint to its relationship with the code.

Exercise 3. *Consider the following tree automaton*

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

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. 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.*

$$\forall p,q,r : \mathsf{Prop.} \; ((p \to r) \land (q \to r)) \to ((p \lor q) \to r)$$

Exercise 5. *Let $(A, \sqsubseteq_A)$ be a CL, and $f \in (A \to A)$ be a monotonic function satisfying $f \circ f = f \sqsupseteq \mathsf{id}_A$ (pointwise). Let $B = f[A] \subseteq A$ and $\sqsubseteq_B = \sqsubseteq_A \cap (B \times B)$. Prove that $(B, \sqsubseteq_B)$ is a CL and that:*

$$\forall X \subseteq B. \qquad \bigsqcup{}^B X = f\left(\bigsqcup{}^A X\right)$$

Try to be precise in your notation, annotating your operators with A or B when it matters.

Exercise 6. *Let $(A, \sqsubseteq_A)$ be a DCPO, and $f \in (A \to A)$ be a Scott-continuous function satisfying $f \circ f = f$. Let $B = f[A] \subseteq A$ and $\sqsubseteq_B = \sqsubseteq_A \cap (B \times B)$. Prove that $(B, \sqsubseteq_B)$ is a DCPO.*
Try to be precise in your notation, annotating your operators with A or B when it matters.