Formal Techniques – 2014-09-08

Exercise 1. *Prove that, if in a poset A a monotonic function $A \to A$ has a minimum prefixed point x, then x is also its minimum fixed point.*

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

$$! \ . \ \mathit{out}\ \mathsf{m} \ . \ \mathit{in}\ X \ . \ \mathit{out}\ \mathsf{h}(X) \ . \ ! \ . \ \mathit{in}\ Y \ . \ \mathit{out}\ \mathsf{g}(Y) \ . \ ()$$

Apply the control flow analysis to the protocol above, generating a tree automaton to over-approximate the message flow, as done by function gen$(\ldots)$. 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*

$@\mathsf{a} \to \mathsf{k1}, \mathsf{enc}(@\mathsf{b}, @\mathsf{c}), \mathsf{dec}(@\mathsf{b}, @\mathsf{a})$	$@\mathsf{b} \to \mathsf{enc}(@\mathsf{c}, @\mathsf{e}), \mathsf{enc}(@\mathsf{d}, @\mathsf{f})$
$@\mathsf{c} \to \mathsf{k2}, \mathsf{m2}$	$@\mathsf{d} \to \mathsf{m1}$
$@\mathsf{e} \to \mathsf{k1}, \mathsf{m3}$	$@\mathsf{f} \to \mathsf{k2}, \mathsf{m2}$

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 $@\mathsf{a}$ *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of message* $\mathsf{m1}, \mathsf{m2}, \mathsf{m3}$.

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

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

Exercise 5. *Let $(A, \sqsubseteq)$ be a CL satisfying $\forall x \in A, Y \subseteq A.\ \ x \sqcap \bigsqcup_{y \in Y} y = \bigsqcup_{y \in Y}(x \sqcap y)$. For any two elements x, y of A, define the* Heyting implication *operator as*

$$(x \to y) = \bigsqcup \{z \in A \mid z \sqcap x \sqsubseteq y\}$$

Prove the following, for any $x, y, z \in A$.

$$\begin{array}{rl} 1) & x \sqsubseteq y \to z \iff x \sqcap y \sqsubseteq z \\ 2) & x \sqcap (x \to y) = x \sqcap y \\ 3) & x \sqsubseteq y \iff x \to y = \top \\ 4) & x \to (y \to z) = (x \sqcap y) \to z \end{array}$$

Exercise 6. *Let $(A, \sqsubseteq_A)$ be a DCPO with $\bot_A$, and B be a set. Let f be a function $B \to (A \to A)$ such that $\forall b \in B.\ f(b)$ is a Scott-continuous function in $A \to A$. Define*

$$\begin{array}{l} h : (B \to A) \to (B \to A) \\ h(g) = \lambda b \in B.\ f(b)(g(b)) \end{array}$$

1. *Give a definition for the minimum element $\bot_{B \to A}$ of the DCPO $B \to A$.*
2. *Prove that h is Scott-continuous.*
3. *Prove that $\forall b_0 \in B.\ fix_A\ (f(b_0)) = (fix_{B \to A}\ h)(b_0)$*