Formal Techniques – 2015-06-15

Exercise 1. *Define the adjunction property between α and γ in a Galois connection. Then, prove that α uniquely determines γ.*

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

$$\begin{array}{l} (\,\mathit{out}\ \mathsf{m1}\ .\ \mathit{in}\ X\ .\ \mathit{out}\ \mathsf{h}(X)\ .()\\ \mid \mathit{out}\ \mathsf{m2}\ .\ \mathit{in}\ Y\ .\ \mathit{out}\ \mathsf{g}(Y)\ .\ ()) \end{array}$$

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

$$\begin{array}{l} \mathsf{@a} \to \mathsf{enc}(\mathsf{@c},\mathsf{@b}), \mathsf{enc}(\mathsf{@e},\mathsf{@f}), \mathsf{@f}, \mathsf{enc}(\mathsf{@d},\mathsf{@c}), \mathsf{dec}(\mathsf{@a},\mathsf{@a}), \mathsf{enc}(\mathsf{@a},\mathsf{@a})\\ \mathsf{@b} \to \mathsf{enc}(\mathsf{@e},\mathsf{@d}) \qquad \mathsf{@c} \to \mathsf{m} \qquad \mathsf{@d} \to \mathsf{b} \qquad \mathsf{@e} \to \mathsf{a} \qquad \mathsf{@f} \to \mathsf{k} \end{array}$$

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

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

Exercise 5. *Define a CL $(A, \sqsubseteq)$ and a Scott-continuous function $f : A \to A$ such that the following points can be answered:*

1. *[5% score] Find the minimum fixed point x of f.*
2. *[15% score] Find another fixed point $y \neq x$ of f.*
3. *[80% score] Find a prefixed point z of f which is not a fixed point. That is, $f(z) \sqsubset z$ is a strict inequality.*

Remember to justify your answers.

Exercise 6. *Let A, B be two DCPOs with a $\perp$ element, and $f : (A \times B) \to (A \times B)$ be a Scott-continuous function, with $fix_{A\times B}(f) = \langle \bar{a}, \bar{b}\rangle$. Define $f_A = \pi_1 \circ f : (A \times B) \to A$, and $f_B = \pi_2 \circ f : (A \times B) \to B$.*

Prove the equation below. Its main consequence is that, once $\bar{a}$ is known, $\bar{b}$ can be deduced from it through a minimum fixed point over B alone.

$$\bar{b} = fix_B(\lambda b : B.\ f_B(\bar{a}, b))$$

In your solution, you are not required to verify the continuity of functions built from $f, \pi_{1,2}, fix, \lambda$.

Hints: prove the direction $\sqsupseteq$ first. Remember that both DCPOs B and $A \times B$ have their own induction principle.