Formal Techniques – 2021-06-15

Exercise 1. *Provide the definition of Galois connection, and state its related adjunction property.*

Exercise 2. *Consider the following tree automaton*

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

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.*

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

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.*

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

Exercise 5. *An "ω-chain of DCPOs" is a sequence $D = (D_i, f_i : D_{i+1} \to D_i)_{i\in\mathbb{N}}$ where each D_i is a DCPO and each f_i is a continuous function. Given any such D, we define its limit as the following DCPO, ordered pointwise, and having pointwise suprema (you do not have to prove this claim):*

$$\lim_i D_i \ = \ \left\{ d \in \prod_{i\in\mathbb{N}} D_i \ \middle|\ \forall i \in \mathbb{N}.\ d_i = f_i(d_{i+1}) \right\}$$

Two DCPOs X, Y are said to be isomorphic *($X \cong Y$) iff there is a continuous bijection $X \to Y$ having a continuous inverse $Y \to X$.*
Prove that, for any ω-chain of DCPOs D (as above), there exists an isomorphism

$$(\lim_i D_i) \times (\lim_i D_i) \ \cong\ \lim_i (D_i \times D_i)$$

where the last limit refers to the ω-chain of DCPOs defined as the sequence $(D_i \times D_i, g_i : D_{i+1} \times D_{i+1} \to D_i \times D_i)_{i\in\mathbb{N}}$ with $g_i(x, y) = (f_i(x), f_i(y))$.