Formal Techniques – 2016-06-13

Exercise 1. *Provide the definition of the Scott topology $\mathcal{T}$. Then, define all the notions which are directly involved by the definition of $\mathcal{T}$. (No proof is required.)*

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

$$! \;.\; (\, in\ X \;.\; (\, out\ \mathsf{f}(X) \;.\; () \mid in\ Y \;.\; out\ \mathsf{g}(Y) \;.\; () \,)\,)$$

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

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

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.*

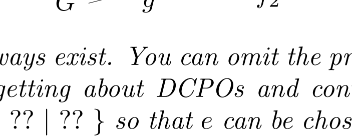
$$\forall p, q : \mathsf{Prop}.\ (p \to ((p \wedge p) \to q)) \to (p \to q)$$

Exercise 5. *Prove that these exist three CLs C, A_1, A_2, equipped with Galois connections $\alpha_i : C \leftrightarrows A_i : \gamma_i$ for $i \in \{1, 2\}$, and a point $c \in C$ such that the following property holds. Let $c_i = \gamma_i(\alpha_i(c))$ for $i \in \{1, 2\}$. Then, we have the* **strict** *inequality*

$$c \sqsubset (c_1 \sqcap c_2) \sqsubset c_i \qquad \textit{for any } i \in \{1, 2\}$$

Exercise 6. *Let f_1, f_2 be two (Scott-)continuous functions $A \to B$, with A, B DCPOs. An* equalizer *of f_1 and f_2 is a pair (E, e) satisfying the requirements:*

1. *E is a DCPO and $e : E \to A$ is continuous.*
2. *$f_1 \circ e = f_2 \circ e$*
3. *for each pair (G, g) satisfying the requirements above there is a unique continuous $m : G \to E$ with $g = e \circ m$.*



*Prove that equalizers always exist. You can omit the proof for the uniqueness of m. (*Hint*: start by forgetting about DCPOs and continuity, and define E explicitly as a set $E = \{x \in ?? \mid ??\}$ so that e can be chosen to be a very simple function, and requirement 2 directly follows. Then check that E is a DCPO and e is continuous.)*