Formal Techniques – 2016-09-05

Exercise 1. *Let A, C be two CLs, with functions $\alpha : C \to A$ and $\gamma : A \to C$ satisfying the adjunction property $\alpha(c) \sqsubseteq a \iff c \sqsubseteq \gamma(a)$ for all $a \in A, c \in C$. Prove that α is monotonic.*

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

$$(\ \mathit{in}\ X.\ \mathit{out}\ \mathsf{f}(X)\ .\ ()\ |\ \mathit{in}\ Y\ .\ \mathit{out}\ \mathsf{g}(Y)\ .\ ()\ |\ \mathit{in}\ Z\ .\ \mathit{in}\ W.\ \mathit{out}\ \mathsf{h}(Z, \mathsf{g}(W))\ .\ ()\ )$$

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*

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

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.*

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

Exercise 5. *Let A, B, C be DCPOs, and $f \in (A \times B \to C)$. Prove that f is Scott-continuous if and only if for all $a \in A$ the function $f(a, \bullet) \in B \to C$ is Scott-continuous, and, for all $b \in B$ the function $f(\bullet, b) \in A \to C$ is Scott-continuous.*

Exercise 6. *Let $DCPO_\perp$ denote the class of DCPOs having a bottom element. Given any two $DCPO_\perp$ a* coproduct *$A + B$ of A and B is a tuple (C, in_A, in_B) where:*

1. *C is a $DCPO_\perp$ and $in_A \in [A \to C]$, $in_B \in [B \to C]$ are Scott-continuous;*
2. *for any $DCPO_\perp$ X and any Scott-continuous $f_A \in [A \to X]$, $f_B \in [B \to X]$ there exists a* unique *Scott-continuous $m \in [C \to X]$ satisfying*

$$f_A = m \circ in_A \qquad f_B = m \circ in_B$$

$$\begin{tikzcd} A \arrow[dr, "in_A"] \arrow[drr, bend left, "f_A"] & & \\ & C \arrow[r, dotted, "\exists!\, m"] & X \\ B \arrow[ur, "in_B"] \arrow[urr, bend right, "f_B"'] & & \end{tikzcd}$$

Prove that all the following attempts **fail**, *in general, at defining a coproduct.*

1. *Take $C = A \uplus B$ to be the disjoint union of A and B.*
2. *Take $C = (A \uplus B)_\perp$ to be the lifted disjoint union of A and B.*
3. *Take $C = A \oplus B$ to be the disjoint union of A and B, where their respective bottoms $\perp_A, \perp_B$ have been identified.*

(Hint – attempt 1 fails for a trivial reason; for attempts 2,3 find f_A, f_B so that m does not exist or is not unique. Very small counterexamples exist.)