Formal Techniques – 2022-07-14

Exercise 1. *Let $\alpha : \mathcal{C} \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \mathcal{A} : \gamma$ be a Galois connection. Prove that α, γ satisfy the adjunction property.*

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

$$!\ .\ in\ X\ .\ !\ .\ out\ \mathsf{h}(X)\ .\ in\ Y\ .\ (\ in\ Z\ .\ out\ \mathsf{f}(X,Y,Z)\ .\ ()\ \mid\ out\ \mathsf{a}\ .\ ()\ )$$

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. Make each state clearly related to a part of the protocol above.

Exercise 3. *Consider the following tree automaton*

$$\mathsf{@a} \to \mathsf{dec}(\mathsf{@a},\mathsf{@a}), \mathsf{enc}(\mathsf{@b},\mathsf{@c}), \mathsf{enc}(\mathsf{@d},\mathsf{@e}), \mathsf{k2} \qquad \mathsf{@b} \to \mathsf{m}, \mathsf{enc}(\mathsf{@f},\mathsf{@d})$$
$$\mathsf{@c} \to \mathsf{dec}(\mathsf{@b},\mathsf{@e}) \quad \mathsf{@d} \to \mathsf{k1},\mathsf{k2} \quad \mathsf{@e} \to \mathsf{k2},\mathsf{k3} \quad \mathsf{@f} \to \mathsf{k1}$$

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* m*.*

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

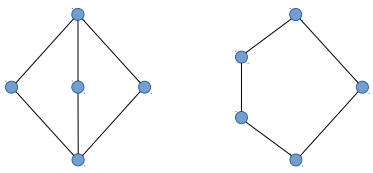
$$\forall p,q,r,s,t : \mathsf{Prop}.\ (p \to q) \to [(r \to s) \to [(p \wedge r) \to (s \wedge ((q \wedge p) \vee t))]]$$

Exercise 5. *Let $\mathcal{A}, \mathcal{B}$ be CLs. A function $f : \mathcal{A} \to \mathcal{B}$ is said to be an* embedding *when:*

$$\forall x, y \in \mathcal{A}.\quad x \sqsubseteq y \iff f(x) \sqsubseteq f(y)$$
$$\forall X \subseteq \mathcal{A}.\quad f(\bigsqcup X) = \bigsqcup f[X] \ \wedge\ f(\bigsqcap X) = \bigsqcap f[X]$$

Let $\mathcal{C}, \mathcal{D}$ be the CLs in the figure below. Let S be any set, and $\mathcal{P}(S)$ be the associated CL obtained ordering subsets by inclusion.

- *[10%] Prove that an embedding must be injective.*
- *[45%] Prove that there is no embedding $f : \mathcal{C} \to \mathcal{P}(S)$.*
- *[45%] Prove that there is no embedding $g : \mathcal{D} \to \mathcal{P}(S)$.*



$\mathcal{C}$ $\qquad$ $\mathcal{D}$