Formal Techniques – 2015-07-07

Exercise 1. *Assume $f : A \to B$ is a monotonic and Scott-continuous function between DCPOs A, B. Prove $f(\bigsqcup D) = \bigsqcup f[D]$ for any directed $D \subseteq^{dir} A$.*

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

$$(!\ .\ in\ X\ .\ out\ \mathsf{h}(X) \quad | \quad out\ \mathsf{a})$$

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. For each state, briefly hint to its relationship with the code.

Exercise 3. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*

1) Alice and Bob share two symmetric keys $K1, K2$. Alice chooses a random nonce N, encrypts it with $K1$, and then encrypt the result with $K2$. The result is sent to Bob.

2) Bob receives the message, learns N, and replies with the same message with the order of the encryptions swapped.

3) Alice receives the message, and checks whether it is indeed what Bob should have sent. In that case, she sends to Bob the message OK.

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

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

Exercise 5. *Let $A \subseteq \mathcal{P}(\mathbb{N})$. Find a maximal A such that $2\mathbb{N} \notin A$ and $(A, \subseteq)$ is a CL with $\bigsqcup^{A}_{n \in \mathbb{N}} \{2k \mid k < n\} = 2\mathbb{N} \cup \{1\}$. Prove A to be a CL and maximal.*

Exercise 6. *Given a set A, let B be the CL of the sets inference rules over A, i.e. $B \stackrel{def}{=} \mathcal{P}(\mathcal{P}_{fin}(A) \times A)$. Let $\mathcal{R}$ range over B, and let $\hat{\mathcal{R}}$ be the immediate consequences (continuous) operator induced by $\hat{\mathcal{R}}$:*

$$\hat{\mathcal{R}} : \mathcal{P}(A) \to \mathcal{P}(A) \qquad \hat{\mathcal{R}}(X) = \{a \in A \mid \exists Y \subseteq X.\ \langle Y, a \rangle \in \mathcal{R}\}$$

Consider the function

$$f : B \to \mathcal{P}(A) \qquad f(\mathcal{R}) = fix(\hat{\mathcal{R}})$$

where fix denotes the minimum fixed point operator. Prove that f is Scott-continuous. You can exploit this fact: $fix : [C \to C] \to C$ is continuous, where C is any DCPO and $[-]$ is the continuous functions space.