Formal Techniques – 2014-06-23

Exercise 1. *Let $(A, \sqsubseteq)$ be a poset, and let $B \subseteq A$ be such that $\bigsqcup B$ exists. Prove that, for any $x \in A$:*

$$\bigsqcup B \sqsubseteq x \iff \forall b \in B.\, b \sqsubseteq x$$

Exercise 2. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*

1) Alice (A) and Bob (B) share two symmetric keys $K1, K2$. A chooses a random nonce NA, hashes it, and sends the result to B after having encrypted it with $K1$. B performs the analogous steps, using his own nonce NB and using $K2$ for encryption.

2) After A has received the message from B, she sends NA to B, again after having encrypted it using $K1$. B does the same using NB and $K2$.

3) After receiving NB with the last message, A checks whether hashing the received NB indeed matches the hash she received before. In such case, she outputs the unencrypted XOR of NA and NB.

Exercise 3. *Consider the following tree automaton*

$$\begin{array}{ll} @\mathsf{a} \to \mathsf{k1}, \mathsf{enc}(@\mathsf{b}, @\mathsf{c}), \mathsf{dec}(@\mathsf{a}, @\mathsf{a}) & @\mathsf{b} \to \mathsf{enc}(@\mathsf{f}, @\mathsf{e}), \mathsf{enc}(@\mathsf{g}, @\mathsf{d}) \\ @\mathsf{c} \to \mathsf{k1}, \mathsf{k2} & @\mathsf{d} \to \mathsf{k2}, \mathsf{k3} \\ @\mathsf{e} \to \mathsf{k1}, \mathsf{k3} & @\mathsf{f} \to \mathsf{m1} \\ @\mathsf{g} \to \mathsf{m2} & \end{array}$$

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. Assuming @a *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of messages* m1, m2*.*

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

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

Exercise 5. *Let $\alpha \in (\mathcal{C} \to \mathcal{A})$ and $\gamma \in (\mathcal{A} \to \mathcal{C})$ be two <u>monotonic</u> functions between two complete lattices $\mathcal{A}, \mathcal{C}$. Assume that*

$$\forall a \in \mathcal{A}, c \in \mathcal{C}. \quad \alpha(c) \sqsubseteq_{\mathcal{A}} a \iff c \sqsubseteq_{\mathcal{C}} \gamma(a)$$

Prove that α is Scott-continuous.

Exercise 6. *Let A be a DCPO with a $\bot$ element. Write $F = [A \to A]$ for its associated DCPO of Scott-continuous functions. Given $n \in \mathbb{N}$, consider the operator which iterates a function n times:*

$$\begin{array}{l} iter_n \in (F \to F) \\ iter_n(f) = f^n \end{array}$$

Prove that $iter_n$ is Scott-continuous for any $n \in \mathbb{N}$. Then, define:

$$\begin{array}{l} fix \in (F \to A) \\ fix(f) = \text{minimum fixed point of } f \end{array}$$

Prove that fix is Scott-continuous.

Hint: you might need to exploit the fact that the composition operator $\circ \in (F \times F \to F)$ is Scott-continuous.