Formal Techniques – 2015-01-12

Exercise 1. *Formalize the following toy protocol using the* applied-pi *notation.*

Three participants A, B, C exchange data on a public network. Every communication between A and B is encrypted using a symmetric key kAB*, shared between them. Similarly, messages between B and C are encrypted with their key* kBC*. In the protocol, A wants to send a message* m *to C: for this, she sends* m *to B which then forwards it to C.*

In your formalization, include a Dolev-Yao adversary in the network. More in detail, you have to formalize an adversary who can 1) intercept and learn any message being sent over the network, 2) encrypt and decrypt messages using any key he knows, and 3) send over the network any message he can craft.

Exercise 2. *Consider the following tree automaton*

$$\begin{array}{ll}
\mathsf{@a} \to \mathsf{a}, \mathsf{enc}(\mathsf{@f}, \mathsf{@c}), \mathsf{enc}(\mathsf{@e}, \mathsf{@b}), \mathsf{dec}(\mathsf{@a}, \mathsf{@a}) & \mathsf{@b} \to \mathsf{pair}(\mathsf{@c}, \mathsf{@d}) \\
\mathsf{@c} \to \mathsf{a} & \mathsf{@d} \to \mathsf{b} \\
\mathsf{@e} \to \mathsf{m} & \mathsf{@f} \to \mathsf{pair}(\mathsf{@d}, \mathsf{@c})
\end{array}$$

and the rewriting rules

$$\mathsf{dec}(\mathsf{enc}(M, K), K) \Rightarrow M \qquad \mathsf{pair}(X, Y) \Rightarrow \mathsf{pair}(Y, X)$$

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 message* m*.*

Exercise 3. *Formally prove the following formula exploiting the Curry-Howard isomorphism.*

$$\forall p : \mathsf{nat} \to \mathsf{Prop}.\ (\forall n : \mathsf{nat}.\ p\,n \to p\,(n+1)) \ \to\ \forall m : \mathsf{nat}.\ p\,m \to p\,((m+1)+1)$$

Exercise 4. *Let $(A, \sqsubseteq)$ be a CL, and $f : A \to A$ be a monotonic function having a minimum fixed point $x \in A$. Then, prove the following "stronger" variant of the induction principle:*

$$\forall y \in A. \qquad f(y \sqcap x) \sqsubseteq y \implies x \sqsubseteq y$$

Exercise 5. *Prove that, in a CL, the set of the fixed points of a monotonic function is a CL.*

More precisely, let $(A, \sqsubseteq_A)$ be a CL, and $f : A \to A$ be a monotonic function. Let $B = \{x \in A | f(x) = x\} \subseteq A$, and let $\sqsubseteq_B = \sqsubseteq_A \cap (B \times B)$. Prove that $(B, \sqsubseteq_B)$ is a CL.

Hints: 1) For any $a \in A$, prove that $A_a = \{x \in A | a \sqsubseteq_A x\}$ is a CL with the induced ordering.

2) Given any $X \subseteq B \subseteq A$, take $a = \bigsqcup^A X$, and prove that $f[A_a] \subseteq A_a$. This allows us to reason about the monotonic restricted function $f|_{A_a} : A_a \to A_a$.