Formal Techniques – 2020-07-08

Exercise 1. *Let $\alpha : \mathcal{C} \overset{\leftarrow}{\to} \mathcal{A} : \gamma$ 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.*

$$(!\ .\ in\ X\ .\ out\ \mathsf{g}(X)\ .\ ()))\quad |\quad (!\ .\ in\ Y\ .\ out\ \mathsf{h}(Y)\ .\ ())\quad |\quad out\ \mathsf{k}\ .\ ()$$

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. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*
Initially, two symmetric keys $\mathsf{k_1}, \mathsf{k_2}$ are shared between Alice and Bob. Bob also knows a message m.
1) Alice generates and sends a nonce a *to Bob, encrypting it using $\mathsf{k_1}$.*
2) After receiving the nonce a*, Bob generates his own nonce* b*, computes the XOR of both nonces* c*, and sends to Alice message* m*, encrypted with* c *(as a symmetric key).*
3) Bob sends b *to Alice, encrypting it with $\mathsf{k_2}$.*
4) After all that, Alice sends to Bob the hash of message m.

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

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

Exercise 5. *Let A be a DCPO, and define*

$$K = \left\{ a \in A \;\middle|\; \forall D \subseteq^{dir} A.\quad a \sqsubseteq \bigsqcup D \implies \exists d \in D.\ a \sqsubseteq d \right\}$$

where $D \subseteq^{dir} A$ means that D is a directed subset of A.

1. *[50%] Find a counterexample (suitable A, k, x) to refute the following claim. Justify your answer.*

   "If $k \in K$ and $x \sqsubseteq k$, then $x \in K$."

2. *[50%] Let $X \subseteq K$ be a finite set such that there exists $x = \bigsqcup^A X$. Prove that $x \in K$.*