Formal Techniques – 2019-06-17

Exercise 1. *State and prove the result relating the least prefixed point and the least fixed point of a suitable function $f : A \to A$ on a poset A.*

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

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

Apply the control flow analysis to the protocol above, generating a tree automaton to over-approximate the message flow, as done by function gen(...). 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. Alice also knows a key k_3 and a message m.
1) Alice sends k_3 to Bob, encrypting it using k_1. Alice also sends m to Bob, encrypting it using k_2.
2) After receiving the messages, Bob generates a fresh nonce N, and sends the pair (m, N) back to Alice, encrypting it using k_3.
3) Alice receives the pair, and answers with the hash of N.
4) Bob checks the received hash, and then answers with the hash of m.

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

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

Exercise 5.

1. *[1%] Provide the statement of the adjunction property satisfied by the functions α, γ forming a Galois connection.*
2. *[99%] Let A be a poset, and let $B = A \times A$ be the poset given by the pointwise ordering. Define the function $\alpha : A \to B$ as $\alpha(a) = (a, a)$. Assume that $\gamma : B \to A$ is a function satisfying, with α, the same adjunction property above. (Note: we do* not *require that A, B are CLs – only posets. We also do* not *require that functions α, γ satisfy further conditions, e.g. continuity.)*

   Prove that A must have all binary infima: if $x, y \in A$, then there exists $x \sqcap y$ (i.e., $\bigsqcap\{x, y\}$) in A.

Exercise 6. *Let A be a poset with a $\bot$ element. Prove the equivalence between the following:*

- *A is an ω-CPO. (Recall than an ω-CPO is a poset where every ω-chain $x_0 \sqsubseteq x_1 \sqsubseteq x_2 \sqsubseteq \cdots$ admits a supremum $\bigsqcup_{n \in \mathbb{N}} x_n$.)*
- *For all monotonic $f : A \to A$ the supremum $\bigsqcup_{n \in \mathbb{N}} f^n(\bot)$ exists.*