Formal Techniques – 2023-07-19

Exercise 1. *Let A be a poset, and $f : A \to A$ be monotonic. Prove that the least prefixed point of f is also its least fixed point.*

Exercise 2. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*
Initially, two symmetric keys $\mathsf{k1}, \mathsf{k2}$ *are shared between Alice and Bob.*
1) Alice generates a pair of nonces N, M, encrypts such pair with $\mathsf{k1}$*, and sends it to Bob.*
2) After receiving the pair, Bob randomly generates a nonce P, and sends the new pair (M, P) to Alice, after encrypting it with $\mathsf{k2}$*.*
3) Alice checks that the received pair indeed contains her nonce M as its first component. If that is the case, she also recovers P and sends its hash to Bob.
4) Bob then receives the hash and verifies that it is indeed the hash of P. In such case, it sends the message ok *to Alice, encrypted with* $\mathsf{k2}$*.*

Exercise 3. *Consider the following tree automaton*

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

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 which is closed under rewriting. Assuming @a *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of* m*.*

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

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

Exercise 5. *Let $\mathcal{C}$ and $\mathcal{A}$ be two CLs, and let $\alpha : \mathcal{C} \leftrightarrows \mathcal{A} : \gamma$ be a Galois connection. Let $f, g : \mathcal{C} \to \mathcal{C}$ be two Scott-continuous functions. For any such function h, we write $h^\#$ for its corresponding best correct approximation.*

Consider the following three elements of $\mathcal{A}$:

$$a_1 = \alpha(\mathsf{fix}(g \circ f)) \qquad a_2 = \mathsf{fix}(g^\# \circ f^\#) \qquad a_3 = \mathsf{fix}((g \circ f)^\#)$$

1. *[30%] Find a_i, a_j, a_k permutation of a_1, a_2, a_3 such that $a_i \sqsubseteq a_j \sqsubseteq a_k$ always holds. Prove the two inequalities.*

2. *[35%] Prove that, in general, the inequality $a_j \sqsubseteq a_k$ can be strict. (Hint: you can choose $\mathcal{C} = \mathcal{P}(\mathbb{Z})$)*

3. *[35%] Prove that, in general, the inequality $a_i \sqsubseteq a_j$ can be strict.*