Formal Techniques – 2019-07-11

Exercise 1. *Let* $\alpha : \mathcal{C} \leftrightarrows \mathcal{A} : \gamma$ *be a Galois connection between the CLs* $\mathcal{C}$ *and* $\mathcal{A}$*. Let* $f : \mathcal{C} \to \mathcal{C}$ *and* $g : \mathcal{A} \to \mathcal{A}$ *be continuous functions. Assume that* g *is a correct approximation of* f*, prove that*

$$\mathsf{fix}(f) \sqsubseteq \gamma(\mathsf{fix}(g))$$

Exercise 2. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*
Initially, a symmetric key k_1 *is shared between Alice and Bob. Alice also knows keys* $\mathsf{k}_2, \mathsf{k}_3$ *and a message* m.
1) Alice sends k_3 *to Bob, encrypting it using* k_2*. Alice also sends* k_2 *to Bob, encrypting it using* k_1*, and sends* m*, encrypting it using* k_3.
2) After receiving the messages, Bob generates a fresh key J*, and sends to Alice the hash of* m*, encrypting it using* J*. He also sends* J*, encrypting it using* k_2.
3) Alice receives the messages, and checks that the hash of m *is correct. If so, it sends* ok *back to Bob.*

Exercise 3. *Consider the following tree automaton*

$$@\mathsf{a} \to \mathsf{enc}(@\mathsf{b}, @\mathsf{c}), \mathsf{dec}(@\mathsf{a}, @\mathsf{f}) \qquad @\mathsf{b} \to \mathsf{enc}(@\mathsf{d}, @\mathsf{e})$$
$$@\mathsf{c} \to \mathsf{k1}, \mathsf{k3} \qquad @\mathsf{d} \to \mathsf{m} \qquad @\mathsf{e} \to \mathsf{k2} \qquad @\mathsf{f} \to \mathsf{k1}, \mathsf{k4}$$

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 message* m.

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

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

Exercise 5. *Prove that the distributivity law* $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ *does not always hold in a CL* A*, for all elements* $x, y, z \in A$.
Then, prove that the law $x \sqcap (x \sqcup y) = x$ *instead always holds in any CL* A*, for all* $x, y \in A$.

Exercise 6. *An "*ω*-chain of DCPOs" is a sequence* $D = (D_i, f_i : D_{i+1} \to D_i)_{i\in\mathbb{N}}$ *where each* D_i *is a DCPO and each* f_i *is a continuous function. Given any such* D*, we define its limit as the following DCPO, ordered pointwise, and having pointwise suprema (you do not have to prove this claim):*

$$\lim_i D_i \;=\; \left\{ d \in \prod_{i\in\mathbb{N}} D_i \;\middle|\; \forall i \in \mathbb{N}.\ d_i = f_i(d_{i+1}) \right\}$$

Two DCPOs X, Y *are said to be* isomorphic *(*$X \cong Y$*) iff there is a continuous bijection* $X \to Y$ *having a continuous inverse* $Y \to X$.
Prove that, for any DCPO A *and any* ω*-chain of DCPOs* D *(as above), there exists an isomorphism*

$$A \times (\lim_i D_i) \;\cong\; \lim_i (A \times D_i)$$

where the last limit refers to the ω*-chain of DCPOs defined as the sequence* $(A \times D_i, g_i : A \times D_{i+1} \to A \times D_i)_{i\in\mathbb{N}}$ *with* $g_i(a, x) = (a, f_i(x))$.