Formal Techniques – 2017-06-06

Exercise 1. *Provide the definitions of upper bound, maximum, and supremum. Then, provide the statements of the Tarski's fixed point theorem and the Kleene's fixed point theorem.*

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

$$\begin{array}{l}(\mathit{in}\ W\ .\ \mathit{out}\ \mathsf{f}(W)\ .\ ()\\ \mid \mathit{in}\ X\ .\ (\mathit{in}\ Y\ .\ \mathit{out}\ \mathsf{g}(Y,X)\ .\ ()\mid \mathit{in}\ Z\ .\ \mathit{out}\ \mathsf{h}(X,Z)\ .\ ()\ )\quad)\end{array}$$

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, an asymmetric key pair is known by Alice, and another one is known by Bob. Further, Alice and Bob share a symmetric key K.
1) Alice and Bob exchange their own public keys, protecting the exchange by encrypting their communications with K.
2) Then, Alice generates a fresh nonce N*, and sends* N *to Bob after having encrypted it with Bob's public key.*
3) Bob answers by generating a fresh symmetric "session" key S*, and sending back the pair* N, S *to Alice, encrypted using Alice's public key.*
4) Alice sends message m *to Bob, encrypted with the session key* S.
5) Bob answers with the hash h(m).

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

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

Exercise 5. *Consider the CLs* $\mathcal{C} = \mathcal{P}(\mathbb{Z})$, *and* $\mathcal{A} = \mathcal{P}(\{0, 1, 2\})$, *both ordered by* $(\subseteq)$. *Define*

$$\begin{array}{ll}\alpha : \mathcal{C} \to \mathcal{A} & \alpha(C) = \{x \bmod 3 \mid x \in C\}\\ \gamma : \mathcal{A} \to \mathcal{C} & \gamma(A) = \{y + 3k \mid y \in A \wedge k \in \mathbb{Z}\}\\ f : \mathcal{C} \to \mathcal{C} & f(C) = \{2\} \cup \{2 \cdot x \mid x \in C\}\end{array}$$

1. *[15%] Verify that* α, γ *form a Galois connection. (You can neglect to check continuity.)*
2. *[15%] Determine the least fixed point* C *of* f.
3. *[50%] Define the best correct approximation* $f^{\#}$ *of* f*, providing a small table (or drawing) showing the result of* $f^{\#}$ *on all the elements of its domain.*
4. *[10%] Determine the least fixed point* A *of* $f^{\#}$.
5. *[10%] Discuss how we can compare* C *and* A *(one line suffices).*

Exercise 6. *For each* $i \in \mathbb{N}$, *let* $(A_i, \sqsubseteq_i)$ *be a DCPO equipped with a bottom element* $\bot_i$, *and let* $f_i : A_{i+1} \to A_i$ *be a Scott-continuous function. Then, consider the following poset* B *under the pointwise ordering* $\sqsubseteq_B$:

$$B = \left\{ \vec{b} \in \prod_{i \in \mathbb{N}} A_i \;\middle|\; \forall i \in \mathbb{N}.\ f_i(b_{i+1}) = b_i \right\}$$

Prove that:

1. *[20%]* $(B, \sqsubseteq_B)$ *is a DCPO, where suprema are taken pointwise.*
2. *[80%]* B *has a bottom element* $\bot_B$.

(Suggestion: for $\bot_B$, *map each* $\bot_k$ *with* $k \geq i$ *into an element* $a_{i,k} \in A_i$, *exploiting the available functions. Then, consider* $X_i = \{a_{i,k} \mid k \geq i\} \subseteq A_i$.*)*