Formal Techniques – 2017-07-07

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

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

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. *Consider the following tree automaton*

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

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 message* m.

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

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

Exercise 5. *Construct DCPOs A, B and a function $f : A \to A$ such that:*

1. *$B \subseteq A$ is a DCPO with the induced ordering,*
2. *f is Scott-continuous, and its restriction $f|_B$ is $B \to B$ and Scott-continuous (no proof is required for this point), and*
3. *for some $b \in B$, we have that $\{x \in B \mid f(x) = x \sqsupseteq_B b\}$ is nonempty but has no minimum, yet $\{x \in A \mid f(x) = x \sqsupseteq_A b\}$ has a minimum.*

Exercise 6. *Let $\mathcal{C}, \mathcal{A}_1, \mathcal{A}_2$ be CLs, ordered by $\sqsubseteq_{\mathcal{C}}, \sqsubseteq_{\mathcal{A}_1}, \sqsubseteq_{\mathcal{A}_2}$ respectively. Assume these CLs are related by two Galois connections $\alpha_i : \mathcal{C} \leftrightarrows \mathcal{A}_i : \gamma_i$ for $i \in \{1, 2\}$.*

1. *Construct a Galois connection $\alpha : \mathcal{C} \leftrightarrows (\mathcal{A}_1 \times \mathcal{A}_2) : \gamma$ exploiting the two Galois connections above, and prove it is such.*
   (Reminder: the product of two CLs has the pointwise ordering)

Now, take $\mathcal{C} = \mathcal{P}(\mathbb{Z})$, ordered by inclusion. Let $\mathcal{A}_1 = \{\bot, 0, 1, \ldots, 5, \top\}$, and $\mathcal{A}_2 = \{\bot, 0, 1, \ldots, 9, \top\}$, where different numbers are incomparable, and the rest of the elements are ordered in the natural way. Further consider

$$\begin{array}{lll} \gamma_1(\bot) = \emptyset & \gamma_1(n) = \{n + 6k \mid k \in \mathbb{Z}\} & \gamma_1(\top) = \mathbb{Z} \\ \gamma_2(\bot) = \emptyset & \gamma_2(n) = \{n + 10k \mid k \in \mathbb{Z}\} & \gamma_2(\top) = \mathbb{Z} \\ \alpha_1, \alpha_2 \textit{ defined accordingly} & & \end{array}$$

2. *Consider the following properties on pairs $a_1, a_2, a_3, a_4 \in (\mathcal{A}_1 \times \mathcal{A}_2)$ where α, γ are from point 1 above. (Mind the strict inequalities)*

$$\begin{array}{ll} \alpha(\gamma(a_1)) = a_1 & \alpha(\gamma(a_2)) \sqsubset a_2 \\ \alpha(\gamma(a_3)) \sqsupset a_3 & \alpha(\gamma(a_4)) \textit{ can not be compared to } a_4 \end{array}$$

   For each $i \in \{1, 2, 3, 4\}$, either provide a value for the pair a_i such that it satisfies its related property above, or prove that no such pair a_i exists.