Formal Techniques – 2018-07-06

Exercise 1. *Provide the definition of "complete lattice" (CL). Then prove that if* $(A, \sqsubseteq)$ *is a CL, then* $(A, \sqsubseteq)^{op} = (A, \sqsupseteq)$ *is also a CL.*

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

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

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*

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

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.*

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

Exercise 5. *Let* $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *be three CLs, and* $\alpha_1 : \mathcal{C} \leftrightarrows \mathcal{B} : \gamma_1$ *and* $\alpha_2 : \mathcal{B} \leftrightarrows \mathcal{A} : \gamma_2$ *be two Galois connections. Construct a Galois connection* $\alpha : \mathcal{C} \leftrightarrows \mathcal{A} : \gamma$ *and prove it is such.*

Exercise 6. *Let* $\mathcal{A}$ *be a CL, and* $w : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ *be a Scott-continuous function, and assume (1)* $\forall x, y \in \mathcal{A}.\ w(x, y) \sqsupseteq x \sqcup y$. *For any* ω*-chain* $a = (a_0 \sqsubseteq a_1 \sqsubseteq \ldots)$ *of elements of* $\mathcal{A}$ *denote with* a^w *the infinite sequence inductively given by* $a_0^w = a_0$ *and* $a_{n+1}^w = w(a_n^w, a_{n+1})$.

1. *[4%] Prove that for any* ω*-chain* a *the sequence* a^w *is also an* ω*-chain.*

   Further assume that (2) for each ω*-chain* a *the* ω*-chain* a^w *eventually stabilizes* ($\exists n. \forall m \geq n.\ a_n^w = a_m^w$). *Let* $f : \mathcal{A} \to \mathcal{A}$ *be a Scott-continuous function. Define an infinite sequence* f^w *as follows*

$$f_0^w = \bot$$
$$f_{n+1}^w = \begin{cases} f_n^w & \text{if } f(f_n^w) \sqsubseteq f_n^w \\ w(f_n^w, f(f_n^w)) & \text{otherwise} \end{cases}$$

2. *[4%] Prove that* f^w *is an* ω*-chain.*

3. *[92%] Prove that* f^w *eventually stabilizes. You can follow these hints.*

   (a) *Proceed by contradiction, assuming* f^w *never stabilizes. Prove that* $f(f_n^w) \sqsubseteq f_n^w$ *can not hold for any* n, *and simplify the definition of* f_{n+1}^w *accordingly.*

   (b) *Consider then the sequence* a *given by* $a_0 = \bot$ *and* $a_{n+1} = f(f_n^w)$. *Prove that* a *is an* ω*-chain, and that* $a^w = f^w$. *Exploit (2) and find a contradiction.*