Formal Techniques – 2018-06-28

Exercise 1. *Informally describe the four CTL formulae* $\mathsf{AF}\phi, \mathsf{AG}\phi, \mathsf{EF}\phi, \mathsf{EG}\phi$ *(where* ϕ *is atomic), providing for each one a brief description (1-3 lines), and one example where it holds.*

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

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

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. *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*
Initially, Alice knows symmetric keys $\mathsf{k}_1, \mathsf{k}_2$*. Further, Alice and Bob share a symmetric key* $\mathsf{k_s}$*.*
1) Alice sends k_1 *to Bob, encrypting it with* $\mathsf{k_s}$*.*
2) Then, Bob generates a fresh nonce N*, and sends* N *to Alice, encrypting it with* k_1*.*
3) Alice answers by generating a message containing two items: the key k_2 *and the hash of* N *encrypted with* k_2*. The whole message (a pair) is encrypted using* $\mathsf{k_s}$*.*
4) Bob finally retrieves the hash of N *from the received message, and sends such hash to Alice (without encrypting it).*

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

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

Exercise 5. *Let* $\alpha : \mathcal{C} \leftrightarrows \mathcal{A} : \gamma$ *be a Galois connection between two CLs* $\mathcal{C}, \mathcal{A}$*.*

1. *Prove that* $\gamma \circ \alpha \circ \gamma = \gamma$*.*
2. *Define* $\delta : \mathcal{A} \to \mathcal{A}$ *as the function* $\delta(a) = \bigsqcap\{a' | \gamma(a') = \gamma(a)\}$*. Prove that* $\delta = \alpha \circ \gamma$*.*

Exercise 6.

1. *Below, we write* $R \subseteq^{rs} X^2$ *when* R *is a binary relation over set* X*, and* R *is reflexive* ($\forall x \in X.\ xRx$) *and symmetric* ($\forall x, y \in X.\ xRy \implies yRx$)*.*

   For any $R \subseteq^{rs} X^2$*, define* $X_R = \{A \subseteq X \mid \forall x, y \in A.\ xRy\}$*.*

   Prove that $(X_R, \subseteq)$ *is a DCPO with* $\bigsqcup = \bigcup$ *and* $\bot = \emptyset$*.*

2. *Let* $A \sim_R B$ *mean* $\forall a \in A, b \in B.\ aRb$*. For any two relations* $R, S \subseteq^{rs} X^2$*, define*

   $$St(R,S) = \left\{ f : X_R \to X_S \;\middle|\; \begin{array}{l} f \text{ Scott-continuous} \wedge \\ \forall A, B \in X_R.\ A \sim_R B \implies f(A \cap B) = f(A) \cap f(B) \end{array} \right\}$$

   Prove that, if $R, S, T \subseteq^{rs} X$*,* $f \in St(R,S)$*, and* $g \in St(S,T)$*, then* $g \circ f \in St(R,T)$*.*