Formal Techniques – 2023-06-23

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.*

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

Apply the control flow analysis to the protocol above, generating a tree automaton to over-approximate the message flow, as done by function $gen(\ldots)$*. 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*

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

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 $\mathsf{@a}$ *models the set of messages being exchanged over a public channel, state what can be concluded about the secrecy of* m*.*

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

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

Exercise 5. *Let* $\mathcal{A}$ *be a CL, and let* $f,g,h : \mathcal{A} \to \mathcal{A}$ *be three Scott-continuous functions, with* $h(a) = f(a) \sqcap g(a)$ *for all* $a \in \mathcal{A}$*. Writing* fix *for the least fixed point operator, let*

$$x = \mathsf{fix}(h) \qquad y = \bigsqcup_{n\geq 0} f^n(x)$$

1. *[10%] Show that* $\bigsqcup_{n\geq 0} f^n(x)$ *is the supremum of a directed set.*
2. *[90%] Show that* $y = \mathsf{fix}(f)$*.*
3. *(Bonus) Show that, in general, when* b *is an arbitrary element of* $\mathcal{A}$*, then* $\bigsqcup_{n\geq 0} f^n(b)$ *does not always have to be a fixed point of* f*.*