# Formal Techniques – 2016-07-07

**Exercise 1.** *Prove that, in a DCPO, the union of two Scott-closed sets is a Scott-closed set.*

**Exercise 2.** *Formalize the following cryptographic protocol fragment using the* applied-pi *notation.*

*1) Alice and Bob share two symmetric keys* $\mathsf{K1}, \mathsf{K2}$*. Alice chooses a random nonce* $N$*, encrypts it with* $\mathsf{K1}$*, and then sends it to Bob.*

*2) Bob receives the message from Alice, learning* $N$*. Then, Bob computes the hash of* $N$*, encrypts it with* $\mathsf{K2}$*, and sends it back to Alice.*

*3) Alice receives the message, and checks whether it is indeed what Bob should have sent. In that case, she sends to Bob the message* $\mathsf{OK}$*.*

**Exercise 3.** *Consider the following tree automaton*

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

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

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

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

**Exercise 5.** *Let* $C, A$ *be CLs, and* $\alpha : C \overset{\leftarrow}{\to} A : \gamma$ *be a Galois connection. Let* $f : C \to C$ *be a Scott-continuous function, and define* $f^{\#} : A \to A$ *as* $\alpha \circ f \circ \gamma$*. Which of the following inequalities can be deduced? (Below,* $fix(-)$ *denotes the minimum fixed point.)*

$$fix(f) \sqsubseteq \gamma(fix(f^{\#})) \qquad fix(f) \sqsupseteq \gamma(fix(f^{\#}))$$

*Provide an example showing that the inequality which does hold can be strict. Provide another example showing that we can also have the equality* $fix(f) = \gamma(fix(f^{\#}))$*.*
Bonus*: in the examples above, also make* $\{f^n(\bot) \mid n \in \mathbb{N}\}$ *an infinite set.*

**Exercise 6.** *Let* $u, v$ *be sets, and* $A = \mathcal{P}(u)$ *and* $B = \mathcal{P}(v)$ *be CLs ordered by inclusion. Let* $f : A \to B$ *be a Scott-continuous function satisfying*

$$\forall x, y \in A.\ f(x \cap y) = f(x) \cap f(y)$$

*Prove the following statements:*

1. *for every* $a \in A$ *and* $b \in f(a)$ *there exists a finite* $\hat{a} \subseteq a$ *satisfying* $b \in f(\hat{a})$*.*
2. *if* $\hat{a}$ *is* $\subseteq$*-minimal in* $\{x \mid b \in f(x)\}$*, then* $\hat{a}$ *is also a minimum.*

*(Hint: consider* $\mathcal{P}^{fin}(x) = \{y \mid y \subseteq x \ \wedge\ y \text{ finite}\}$*.)*