ENS DE LYON

TD de Sémantique et Vérification

III– Fundamentals of Linear-Time Properties

Monday 25th February 2019

Henning Basold
henning.basold@ens-lyon.fr

In this set of exercises, we will alternative characterisations of safety and liveness properties. Ultimately, we will prove the so-called decomposition theorem.

Recommendation: The exercises are all purely pen and paper exercises. However, it is quite fun to implement notions from the course and the exercises. At the very end, you may obtain this way your very own model checker. This week, you may implement ω-regular expressions and their interpretation in terms of operations on linear-time properties. Note that your implementation will not be evaluated as part of the course.

Some Order Theory

We start with the introduction of some order theoretic notions.

- A *partially ordered set (poset)* is a set S with a relation $\leq \subseteq S \times S$, which is reflexive ($x \leq x$), transitive (if $x \leq y$ and $y \leq z$, then $x \leq z$), and anti-symmetric (if $x \leq y$ and $y \leq x$, then $x = y$).
- Let $(S, \leq_S)$ and $(T, \leq_T)$ be posets. A map $f : S \to T$ is *monotone* if $x \leq_S y$ implies $f(x) \leq_T f(y)$.
- Let $(S, \leq)$ be a poset and $X \subseteq S$ a subset of S. An element $l \in S$ is called a *lower bound* if for all $x \in X$, we have $l \leq x$. A *greatest lower bound* or *meet* of X is a lower bound l of X, such that $l' \leq l$ for any other lower bound l' of X. By anti-symmetry, one finds that the meet is unique and we denote it by $\bigwedge X$.

  Similarly we say that u is the *least upper bound* or *join* of X, if u is the least element in S with $x \leq u$ for all $x \in X$. We denote the join of X by $\bigvee X$. If $X = \{x, y\}$, we denote the join also by $x \vee y$.

  If S has all joins and meets, then we call $(S, \leq)$ a *complete lattice*.

  Finally, we say that $(S, \leq)$ has a *least element* (*greatest element*) if there is $\bot \in S$ ($\top \in S$), such that $\bot \leq x$ ($x \leq \top$) for all $x \in S$.
- Let $(S, \leq_S)$ and $(T, \leq_T)$ be posets. A pair of monotone functions (f, g) with $f\colon S \to T$ and $g\colon T \to S$ is called a *Galois connection* (or adjunction) if for all $x \in S$ and $y \in T$

$$f(x) \leq_T y \iff x \leq_S g(y).$$

  In this case we write $f \dashv g\colon S \leftrightarrow T$ and say that f is left-adjoint to g.
- Let $(S, \leq)$ be a poset and $c\colon S \to S$ a monotone map. We say that c is a *closure operator*, if for all $x \in S$ it holds that $x \leq c(x)$ and $c(c(x)) = c(x)$. The map c is a *Kuratowski closure*, if c is a closure operator and $c(\bot) = \bot$ and $c(x \vee y) = c(x) \vee c(y)$.

Exercise 1.
Let $(S, \leq_S)$ and $(T, \leq_T)$ be posets.

1. Suppose $(S, \leq_S)$ is a complete lattice. Show that S has a least element $\bot$.
2. Given a Galois connection $f \dashv g\colon S \leftrightarrow T$, we define $c\colon S \to S$ by $c = g \circ f$. This map is monotone because f and g are. Show that c is a closure operator. *Hint: First prove* $f(g(x)) \leq x$.
3. Suppose that the meet $\bigwedge X$ of $X \subseteq S$ exists. Show for a closure operator $c\colon S \to S$ that $f(\bigwedge X)$ is the meet of $c(X)$, that is, show that $c(\bigwedge X) = \bigwedge c(X)$.

Prefixes and Closure

Exercise 2.

Let L and L_f be the set of all subsets of, respectively $\mathcal{P}(\mathrm{AP})^\omega$ and $\mathcal{P}(\mathrm{AP})^*$. These are posets, where the order is given by set inclusion, meets by intersection, joins by union and the least element is the empty set. Recall that pref is a map $L \to L_f$ given by

$$\mathrm{pref}(P) = \{w \mid \exists \sigma.\ w \cdot \sigma \in P\}.$$

We define a map $\mathrm{cext}\colon L_f \to L$ by

$$\mathrm{cext}(P) = \{\sigma \mid \mathrm{pref}(\sigma) \subseteq P\},$$

which assigns to a predicate its consistent extensions. Finally, we define a map $\mathrm{cl}\colon L \to L$ by

$$\mathrm{cl}(P) = \{\sigma \mid \mathrm{pref}(\sigma) \subseteq \mathrm{pref}(P)\}.$$

Note that $\mathrm{cl} = \mathrm{cext} \circ \mathrm{pref}$.

1. Show that pref and cext are monotone. (**From previous sheet**)
2. Show that $\mathrm{pref} \dashv \mathrm{cext}$. (**From previous sheet**)
3. From the previous exercise we know that cl is a closure operator. Show that cl is a Kuratowski closure.

Exercise 3.

Let $P \subseteq \mathcal{P}(\mathrm{AP})^\omega$ be a linear-time property. (*Hint: Use* $\mathrm{pref} \dashv \mathrm{cext}$ *in the following.*)

1. Show that P is safety property if and only if $\mathrm{cl}(P) = P$.
2. Show that P is a liveness property if and only if $\mathrm{cl}(P) = \mathcal{P}(\mathrm{AP})^\omega$.

Exercise 4.

Consider the set $AP = \{A, B\}$ of atomic propositions. Formulate the following properties as LT properties and indicate which ones are safety properties. Compute also their closure.

1. A should never occur,
2. A should occur exactly once,
3. A and B alternate infinitely often,
4. A should eventually be followed by B.

Exercise 5.

Let $P \subseteq \mathcal{P}(\mathrm{AP})^\omega$ be a linear-time property, and define $P_{\text{safe}} = \mathrm{cl}(P)$ and $P_{\text{live}} = P \cup \mathrm{cl}(P)^\complement$. *Hint: Use the previous exercises in what follows.*

1. Show that P_{safe} is a safety property.
2. Show that P_{live} is a liveness property.
3. Show that $P = P_{\text{safe}} \cap P_{\text{live}}$, from which we conclude that every linear-time property can be decomposed into a safety and a liveness property. This is also called the *decomposition theorem*.

Traces and Safety Properties

Exercise 6.

Let TS and TS' be transition systems without terminal states and with the same set of propositions AP. Show that the following statements are equivalent:

1. Finite traces of TS are finite traces of TS'
2. For every safety property P, if TS' satisfies P, so does TS.