ENS DE LYON

TD de Sémantique et Vérification

II– Linear Time Properties (and a bit of Modelling)

Tuesday 12th February 2019

Henning Basold
henning.basold@ens-lyon.fr

In this set of exercises, we will discuss examples and properties of linear time properties.

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 representations of linear time properties, operations like concatenation on LT properties, and invariant checking. Note that your implementation will not be evaluated as part of the course.

Linear Time Properties

We will use the following notations.

- $P^{\complement} = \mathcal{P}(\mathrm{AP})^\omega \setminus P$
- If $w \in \left(2^{\mathrm{AP}}\right)^*$ and $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega$, then their concatenation is denoted by $w \cdot \sigma \in \left(2^{\mathrm{AP}}\right)^\omega$. Concatenation extends to languages in the obvious way.

Moreover, recall that

- P is a safety property if for each $\sigma \in P^{\complement}$, there exists a finite prefix $\hat{\sigma}$ such that $\hat{\sigma} \cdot (2^{\mathrm{AP}})^\omega \cap P = \emptyset$. The word $\hat{\sigma}$ is called a *bad prefix*.
- P is a liveness property if $\mathrm{pref}(P) = (2^{\mathrm{AP}})^*$.

Exercise 1.
Consider the set AP of atomic propositions defined by $AP = \{x = 0, x > 1\}$ and consider a non-terminating sequential computer program P that manipulates the variable x. You may assume that the program is given as LTS and that the propositions are mutually exclusive, that is, for every state s we have $\{x = 0, x > 1\} \nsubseteq L(s)$. Formulate the following informally stated properties as linear time properties and determine for each whether it is an invariance, a safety property, a liveness property or none of these.

1. false
2. x is always equal to zero
3. initially x is equal to zero
4. initially x differs from zero
5. initially x is equal to zero, but at some point x exceeds one
6. x exceeds one only finitely many times
7. x exceeds one infinitely often
8. true

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 and meets by intersection. A pair of monotone functions (f, g) with $f\colon L_f \to L$ and $g\colon L \to L_f$ is called a *Galois connection* (or adjunction) if for all $P \in L_f$ and $Q \in L$

$$f(P) \subseteq Q \iff P \subseteq g(Q). \tag{1}$$

In this case we write $f \dashv g$ and say that f is left-adjoint to g. Recall that pref is a map $L \to L_f$ given by

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

We define a map cext: $L_f \to L$ by

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

which assigns to a predicate its consistent extensions.

1. Show that pref and cext are monotone.
2. Show that pref $\dashv$ cext.

Exercise 3.

Let P and Q be liveness (safety) properties. Prove or disprove that

1. $P \cup Q$ is a liveness (safety) property,
2. $P \cap Q$ is a liveness (safety) property.

Deadlocks and Starvation

Exercise 4.

The dining philosophers (Dijkstra '69) Three philosophers are sitting at a round table with a bowl of rice in the middle. For the philosophers (being a little unworldly) life consists of thinking and eating (and waiting). To take some rice out of the bowl, a philosopher needs two chopsticks. In between two neighbouring philosophers, however, there is only a single chopstick. Thus, at any time only one of two neighbouring philosophers can eat. Of course, the use of the chopsticks is exclusive and eating with hands is forbidden.

Note that a deadlock scenario occurs when all philosophers possess a single chopstick. The problem is to design a protocol for the philosophers, such that the complete system is deadlock-free, that is, at least one philosopher can eat infinitely often. Additionally, a fair solution may be required with each philosopher being able to think and eat infinitely often. The latter characteristic is called freedom of *individual starvation*.

1. Model the scenario of three dining philosophers as a labelled transition system.
2. Can you express the following properties by linear-time properties?

   Mutual exclusion any two philosophers never eat at the same time;

   Deadlock freedom there is always at least one philosopher eating;

   No Starvation all philosophers are guaranteed to eat, sooner or later.
3. Check whether the above properties are respected by your model of the dining philosophers problem. If not, can you think of improvements?
4. Which of these properties are invariants and safety properties?

Traces

Exercise 5.

Each transition system TS (that probably has a terminal state) can be extended such that for each terminal state s in TS there is a new state s_{stop} , transition $s \to s_{stop}$ and s_{stop} is equipped with a self-loop, i.e., $s_{stop} \to s_{stop}$. The resulting "equivalent" transition system obviously has no terminal states.

1. Give a formal definition of this transformation $TS \mapsto TS^\star$
2. Prove that the transformation preserves trace-equivalence, i.e., show that if TS_1, TS_2 are transition systems (possibly with terminal states) such that $\text{Traces}(TS_1) = \text{Traces}(TS_2)$, then $\text{Traces}(TS_1^\star) = \text{Traces}(TS_2^\star)$.