ENS DE LYON

TD – Semantics and Verification

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

Monday 25th January 2021

TA: Ralph Sarkis
ralph.sarkis@ens-lyon.fr

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

Linear Time Properties

We will use the following notations.

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

Moreover, recall that P is a safety property if there exists a set $P_{\text{bad}} \subset (2^{\text{AP}})^*$ such that $P = \{\sigma \in (2^{\text{AP}})^\omega \mid \forall \hat{\sigma} \subseteq_{\text{finite}} \sigma, \hat{\sigma} \notin P_{\text{bad}}\}$.

We also define

- $\text{pref}(P) = \{\hat{\sigma} \text{ finite } | \exists \sigma \in P, \hat{\sigma} \subseteq \sigma\}$
- $\text{cl}(P) = \{\sigma | \text{pref}(\sigma) \subseteq \text{pref}(P)\}$

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 a safety property, an invariant property or neither. property.

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 exceeds one
6. x exceeds one only finitely many times
7. x exceeds one infinitely often
8. true

Exercise 2.

Let $P \subseteq (2^{AP})^\omega$ be a linear property. Show that

1. P is a safety property if and only if for each $\sigma \in P^{\complement}$, there exists a finite prefix $\hat{\sigma}$ such that $\hat{\sigma} \cdot (2^{\text{AP}})^\omega \cap P = \emptyset$,
2. P is a safety property if and only if $\text{cl}(P) = P$.

Exercise 3.

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

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

Regular Safety Properties

Exercise 4.

Let $P \subseteq (2^{AP})^\omega$ a bad property induced by a regular set $P_{bad} \subseteq (2^{AP})^*$. Fix a NFA $\mathcal{A}$ which recognizes P_{bad}.

Consider now a transition system TS over AP without terminal state:

$$\text{TS} \quad = \quad (S, \text{Act}, \to, I, \text{AP}, L)$$

We define the product transition system

$$\text{TS} \otimes \mathcal{A} \quad := \quad (S_\otimes, \text{Act}, \to_\otimes, I_\otimes, \text{AP}_\otimes, L_\otimes)$$

as follows:

- The set of states is $S_\otimes := S \times Q$.
- The transition relation $\to_\otimes$ is defined by the rule

$$\frac{s \xrightarrow{\mathsf{a}} s' \qquad (q, L(s'), q') \in \Delta}{(s, q) \xrightarrow{\mathsf{a}} (s', q')}$$

  Note that it is the label of the *target* state s' of $s \xrightarrow{\mathsf{a}} s'$ which is used as input letter of $\mathcal{A}$.
- The set of initial states $I_\otimes$ is the set of all pairs (s_0, q) such that s_0 is initial in TS ($s_0 \in I$) and such that we have $(q_0, L(s_0), q)$ for some initial $q_0 \in Q_0$.
- $\text{AP}_\otimes := Q$.
- $L_\otimes(s, q) := \{q\}$.

1. Show that we can assume that P_{bad} is suffix-closed (meaning that if $w \in P_{bad}$ then $w.(2^{AP})^* \subseteq P_{bad}$).
2. Show that TS $\models\!\!\approx P$ iff $\text{Traces}_{fin}(TS) \cap P_{bad} = \emptyset$.
3. Show that TS $\models\!\!\approx P$ iff TS $\otimes \mathcal{A} \models\!\!\approx \{\sigma \in (2^{\text{AP}})^\omega \mid \forall n, \forall q \in F, q \notin \sigma(n)\}$.

Deadlocks and Starvation

Exercise 5.

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 at any time, at least one philosopher is guaranteed to eat, sooner or later;

   No Starvation at any time, 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 or safety?