ENS DE LYON

TD de Sémantique et Vérification

III– Safety properties

Simon Castellan
simon.castellan@ens-lyon.fr

Exercise 1.

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, as we will see). To take some rice out of the bowl, a philosopher needs two chopsticks. In between two neighboring philosophers, however, there is only a single chopstick. Thus, at any time only one of two neighboring 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, i.e., 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 one are invariants and safety properties?
5. Compute the closure of the property "No starvation"

Exercise 2.

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

Remember that:

- P is a safety property when for each $\sigma \notin P$, there exists a finite prefix $\hat{\sigma}$ such that $\hat{\sigma} \cdot (2^{\mathrm{AP}})^{\omega} \cap P = \emptyset$ ($\hat{\sigma}$ is called a *bad prefix*)
- $\mathrm{cl}(P)$ is the set of words σ such that for each finite prefix $\hat{\sigma}$ of σ, there exists an infinite word β such that $\hat{\sigma} \cdot \beta \in P$.

Exercise 3.

Let $P \subseteq (2^{\mathrm{AP}})^{\omega}$ be a linear-time property. Show that P is safety property if and only if $\mathrm{cl}(P) = P$.

Exercise 4.

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.