



Tutorials for Verification Exercise sheet 3

Exercise 1: LT properties

- (a) Assume $AP = \{a, b\}$. Give a mathematical definition for the following properties as a set of traces (as in the lecture). If “state” is mentioned in the property, we mean a state in an execution of the transition system, not an arbitrary (possibly unreachable) state of the transition system. For example, the three states in the fourth property may also be the same state visited three times.
- (i) Every state satisfies a or b .
 - (ii) There is no state satisfying b before the first occurrence of a .
 - (iii) Every a will be eventually followed by an b .
 - (iv) Exactly three states satisfy a .
 - (v) If there are infinitely many a there are infinitely many b .
 - (vi) There are only finitely many a .
- (b) Which of the properties are invariance properties, which are safety properties, and which are liveness properties? If a property is neither a safety property nor a liveness property, express it as an intersection of a liveness and a safety property.

Exercise 2: Backward reachability

The following algorithm uses wlp to check an invariant ϕ . As on the first exercise sheet, wlp is defined as:

$$wlp(C) = \{s \in S \mid \forall s' \in S \forall \alpha \in Act. s \xrightarrow{\alpha} s' \Rightarrow s' \in C\}$$

1. Start with $C_0 = \{s \in S \mid s \models \phi\}$, and $i = 0$
2. Set $C_{i+1} = C_i \cap wlp(C_i)$, increase i .
3. If $C_i \neq C_{i+1}$ repeat step 2.
4. Check if the set of initial states is a subset of C_i .

Show that for finite transition systems the algorithm terminates and that $I \subseteq C_i$ in the last step if and only if the invariant ϕ holds for all reachable states.

Exercise 3: Limit and pref

Let Σ be a finite set. For a language $L \subseteq \Sigma^*$, its *all-limit language* and *limit language* are

$$\text{alim}(L) := \{\sigma \in \Sigma^\omega \mid \text{pref}(\sigma) \subseteq L\} \quad \text{and} \quad \text{lim}(L) := \{\sigma \in \Sigma^\omega \mid (\text{pref}(\sigma) \cap L) \text{ infinite}\}.$$

Show for $L, L_1, L_2 \subseteq \Sigma^\omega$ and $M, M_1, M_2 \subseteq \Sigma^*$ that

- (a) $\text{pref}(L) \subseteq M$ if and only if $L \subseteq \text{alim}(M)$;
- (b) pref and lim distribute over finite unions, alim over finite intersections:
 - (i) $\text{pref}(L_1 \cup L_2) = \text{pref}(L_1) \cup \text{pref}(L_2)$,
 - (ii) $\text{lim}(M_1 \cup M_2) = \text{lim}(M_1) \cup \text{lim}(M_2)$,
 - (iii) $\text{alim}(M_1 \cap M_2) = \text{alim}(M_1) \cap \text{alim}(M_2)$;
- (c) $\text{closure}(L) = \text{alim}(\text{pref} L) = \text{lim}(\text{pref} L)$.

Exercise 4: Properties of closure

Prove the following properties of *closure*:

- (a) $\text{closure}(\emptyset) = \emptyset$
- (b) $P \subseteq \text{closure}(P)$ (*closure is extensive*)
- (c) $\text{closure}(P) = \text{closure}(\text{closure}(P))$ (*closure is idempotent*)
- (d) $\text{closure}(P \cup Q) = \text{closure}(P) \cup \text{closure}(Q)$
- (e) $\text{closure}(P) = (2^{AP})^\omega$ if and only if P is a liveness property.

Exercise 5*: Closure, topology, metric

- (a) For a set S , show that any operator $cl : 2^S \rightarrow 2^S$ that satisfies the first four properties of Exercise 4 defines a topology, in which $\{cl(X) \mid X \subseteq \Sigma^\omega\}$ are exactly all the closed sets.
- (b) A metric for infinite sequences $\sigma_1, \sigma_2 \in \Sigma^\omega$ can be given as follows:

$$d(\sigma_1, \sigma_2) = \begin{cases} 0 & \sigma_1 = \sigma_2 \\ 1/n & \sigma_1[..n-1] = \sigma_2[..n-1] \wedge \sigma_1[n] \neq \sigma_2[n] \end{cases}$$

In other words, two sequences have the distance of $1/n$ iff they equal for $n-1$ elements and differ at the n th element.

This metric can be used to define the corresponding topology. A set P is open in this topology iff for every $\sigma \in P$ there is an ε such that all σ' with $d(\sigma, \sigma') < \varepsilon$ are in P .

- (i) Show that $\text{closure}(P) := \{\sigma \in \Sigma^\omega \mid \text{pref}(\sigma) \subseteq \text{pref}(P)\}$ is in fact the closure of the set P with respect to the above metric.
- (ii) How can safety properties be characterised in this topology?
- (iii) How can liveness properties be characterised in this topology?
- (iv) Give a topological proof for the decomposition theorem.