Exercise 1: Safety-Liveness Decomposition I 4 Points + 1 Bonus Points

The following theorem was discussed in the lecture. A proof is given below.

Theorem 1 (Decomposition). Let $AP$ be a set of atomic propositions, and let $\Sigma = 2^{AP}$. For every LT-property $E \subseteq \Sigma^\omega$, there exists a safety property $P_{safe}$ and a liveness property $P_{live}$ such that $E = P_{safe} \cap P_{live}$.

Proof. Recall that the (prefix) closure of a property $E$ is defined as

$$cl(E) := \{ \sigma \in \Sigma^\omega \mid \text{pref}(\sigma) \subseteq \text{pref}(E) \}$$

i.e., the set of all traces $\sigma$ such that for every finite prefix $w$ of $\sigma$, there exists some $\sigma' \in E$ such that $w$ is also a prefix of $\sigma'$.

We set $P_{safe} := cl(E)$, and $P_{live} := (\Sigma^\omega \setminus cl(E)) \cup E$. It is easy to show that $P_{safe} \cap P_{live} = cl(E) \cap ((\Sigma^\omega \setminus cl(E)) \cup E) \subseteq E$. It remains to show that $P_{safe}$ is a safety property, and $P_{live}$ is a liveness property. To show the former, we must prove that $cl(P_{safe}) = cl(cl(E)) \cup cl(E)$. This holds due to idempotence of $cl$.

To show the latter, we must show that $cl(P_{live}) = \Sigma^\omega$. It holds that

$$cl(P_{live}) = cl((\Sigma^\omega \setminus cl(E)) \cup E)$$

$$\subseteq cl(\Sigma^\omega \setminus cl(E)) \cup cl(E)$$

$$\supseteq \Sigma^\omega \setminus cl(E) \cup E$$

$$= \Sigma^\omega$$

As it is trivially the case that $cl(P_{live}) \subseteq \Sigma^\omega$, we conclude that indeed $P_{live} = \Sigma^\omega$ and $P_{live}$ is a liveness property.

Consider the set of atomic propositions $AP = \{a,b\}$. Apply Theorem 1 to the property

$$E = \{ A_0 A_1 A_2 \ldots \mid \exists i. b \in A_i \land (\forall j. j < i \rightarrow a \in A_j) \}$$

or, informally stated, “$a$ holds until $b$ holds” (and $b$ does eventually hold).

(a) Give the decomposition of this property into a safety property $P_{safe}$ and a liveness property $P_{live}$, following the construction in the proof. Prove that $E = P_{safe} \cap P_{live}$ (equation (♣)), that $P_{safe}$ is indeed a safety property (equation (♦)), and that $P_{live}$ is indeed a liveness property (equations (♠), (♥)).

(b) Consider the property $P'_{live} = \{ A_0 A_1 A_2 \mid \exists i. a \notin A_i \}$. Why can this property not be used in place of $P_{live}$ in part (a)?
Exercise 2: Satisfaction under Fairness Assumptions

The goal of this task is to train your ability to identify fair and unfair traces of a given transition system, in order to reason about properties of a system under given fairness assumptions.

Consider the following transition system:

For the fairness assumptions given in (a)–(h), perform the following tasks.

(i) For each of the fairness assumptions below, give an execution that fulfills the fairness assumption (a fair execution) and an execution that violates the fairness assumption (an unfair execution).

(ii) A system satisfies a property \( P \) under a given fairness assumption, if all fair traces (i.e., traces corresponding to fair executions) satisfy property \( P \).

Under which of the following fairness assumptions does the system satisfy the property “eventually \( a \)”? Justify your answer.

(a) unconditional fairness for \( A = \{ \gamma \} \)
(b) unconditional fairness for \( A_1 = \{ \alpha \} \) and for \( A_2 = \{ \gamma \} \)
(c) unconditional fairness for \( A = \{ \alpha, \gamma \} \)
(d) strong fairness for \( A = \{ \beta \} \)
(e) strong fairness for \( A_1 = \{ \alpha \} \) and for \( A_2 = \{ \beta \} \)
(f) strong fairness for \( A_1 = \{ \alpha \} \) and for \( A_2 = \{ \beta \} \) and for \( A_3 = \{ \eta \} \)
(g) weak fairness for \( A = \{ \eta \} \)
(h) weak fairness for \( A_1 = \{ \alpha \} \) and for \( A_2 = \{ \beta \} \) and for \( A_3 = \{ \eta \} \)