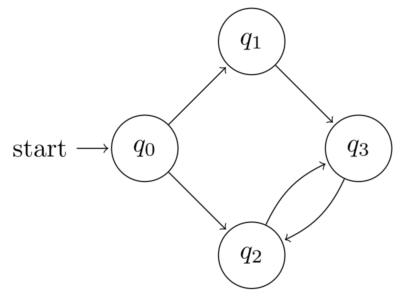
Concurrent Programming

Exercise Booklet 10: Model-Checking

Exercise 1. Consider the following transition system:



where S, I, and $\rightarrow$ are described above, $AP = \{a, b\}$, $Act = \{\tau\}$ (not drawn), $L(q_0) = \{a\}$, $L(q_1) = \emptyset$, $L(q_2) = \{a\}$ and $L(q_3) = \{a, b\}$. Give examples of

- finite and infinite path fragments
- finite and infinite paths
- traces

Exercise 2. Transition systems are assumed to have no terminal states for most of the results explored in class. A simple transformation of a TS with terminal states to an equivalent one that has no terminal states is, to add a distinguished state $\perp$ together with a loop on $\perp$ and, for each terminal state s, a new transition $s \rightarrow \perp$.

1. Give a formal definition of this transformation $TS \rightarrow TS^*$
2. Let $\mathsf{traces}(TS)$ denote the set of traces of a T.S. (i.e. the set of traces of all the paths of the TS). 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 $\mathsf{traces}(TS_1) = \mathsf{traces}(TS_2)$, then $\mathsf{traces}(TS_1*) = \mathsf{traces}(TS_2*)$.

Exercise 3.

(Definition 3.26. Prefix and Closure) For trace $\sigma \in (2^{AP})^\omega$, let $\mathit{pref}(\sigma)$ denote the set of finite prefixes of σ, i.e.,

$$\mathit{pref}(\sigma) = \{\sigma \in (2^{AP})^* | \sigma \textit{ is a finite prefix of } \sigma\}.$$

that is, if $\sigma = A0A1\ldots$ then $\mathit{pref}(\sigma) = \epsilon, A0, A0A1, A0A1A2, ...$ is an infinite set of finite words. This notion is lifted to sets of traces in the usual way. For property P over AP: $\mathit{pref}(P) = \bigcup_{\sigma \in P} \mathit{pref}(\sigma)$. The closure of LT property P is defined by

$$\mathit{closure}(P) = \{\sigma \in (2^{AP})^\omega | \mathit{pref}(\sigma) \subseteq \mathit{pref}(P)\}$$

For instance, for infinite trace $\sigma = ABABAB...$ (where $A, B \subseteq AP$) we have $\mathit{pref}(\sigma) = \epsilon, A, AB, ABA, ABAB, ...$ which equals the regular language given by the regular expression $(AB)^*(A + \epsilon)$.

Prove the following alternative characterization of safety properties (Lemma 3.27):

Let P be an LT property over AP. Then, P is a safety property iff $\mathit{closure}(P) = P$.

Exercise 4. Show that the semaphore-based solution to the MEP problem does not enjoy freedom from starvation by exhibiting an offending path and its trace.

Exercise 5. ($\Diamond$) Consider the set AP of atomic propositions defined by $AP = \{x = 0, x > 1\}$ and consider a nonterminating sequential computer program P that manipulates the variable x. Formulate the following informally stated properties as LT properties:

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

For each of the above, indicate whether they are safety or liveness properties.

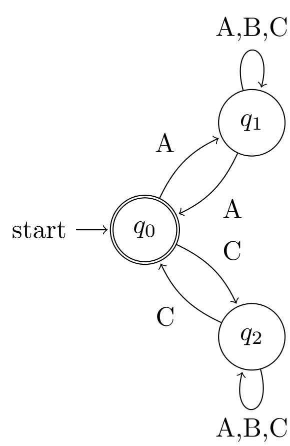
Exercise 6.

Depict an NBA for the language described by the ω-regular expression

$$(AB + C)^*((AA + B)C)^\omega + (A^*C)^\omega.$$

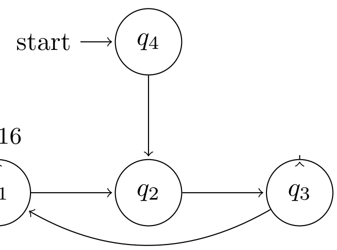
Note: You should consider having more than one initial state.

Exercise 7. Consider the following NBA A over the alphabet $\{A, B, C\}$:



Find the ω-regular expression for the language accepted by A.

Exercise 8.



1 Solutions to Selected Exercises

Answer to exercise 5

1. false: $P := \emptyset$
2. initially x is equal to zero: $P := \{x = 0\}(2^{AP})^{\omega}$.
3. initially x differs from zero: $P := (\emptyset + \{x > 1\})(2^{AP})^{\omega}$
4. initially x is equal to zero, but at some point x exceeds one: $P := \{x = 0\}(2^{AP})^{*}\{x > 1\}(2^{AP})^{\omega}$
5. x exceeds one only finitely many times: $P := (2^{AP})^{*}\{\{x = 0\}, \emptyset\}^{\omega}$
6. x exceeds one infinitely often: $P := ((2^{AP})^{*}\{x > 1\})^{\omega}$
7. the value of x alternates between zero and one
8. true