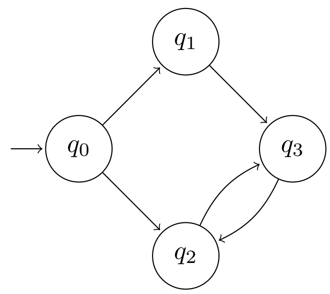
Concurrent Programming

Exercise Booklet 10: Model-Checking

Solutions to selected exercises (◊) are provided at the end of this document. Important: You should first try solving them before looking at the solutions. You will otherwise learn **nothing**. Some exercises are marked as optional (⋆), you do not need to solve them, but they do provide a deeper understanding of the topic.

1 Transition Systems and Linear Time Properties

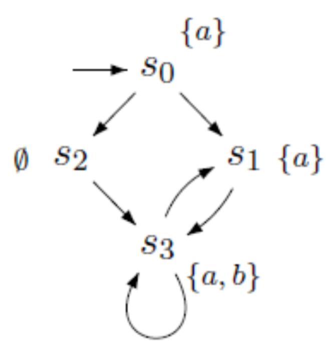
Exercise 1. Consider the following transition system:



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 an example of

1. A finite path fragment
2. An infinite path fragment
3. An infinite path
4. An infinite path fragment that are not a path
5. Are there any finite paths? Justify your answer
6. A trace

Exercise 2. Provide the traces on the set of $AP = \{a, b\}$ of the following transition system:



Exercise 3. (◊) 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 4. (◊) Let $AP = \{a, b, c\}$ be the set of atomic propositions. Consider the following linear time property: "a and b never hold at the same time".

1. Express this property using set-comprehension in three different ways
2. Why is the following incorrect?
   $P = \{A0, A1, ... \in (2^{AP})^{\omega} | \forall i \geq 0. a \in A_i \iff b \notin A_i\}$

Exercise 5. (◊) Let $AP = \{a, b, c\}$ be the set of atomic propositions. Consider the following linear time properties informally stated:

1. initially a holds and b does not hold
2. c holds only finitely many times
3. from some point on the truth value of a alternates between true and false
4. whenever c holds, then a holds sometime afterwards
5. b holds infinitely many times and whenever b holds then c holds afterwards
6. whenever c holds, then a or b must also hold
7. whenever c holds, then sometime afterwards a or b must also hold
8. a holds only finitely many times and c holds infinitely many times
9. whenever a holds then b and c holds after one step
10. never a and b hold at the same time and eventually c holds
11. at any point the number of times a held in the past is always greater than or equal to the number of times b held in the past.

For each property above, (a) formally write it as a set of infinite traces on 2^{AP} and (b) determine whether it is a safety, liveness or mixed (safety and liveness) linear time property. Justify your answers! Hint: you may use the special quantifiers $\overset{\infty}{\forall} i$ ("for nearly all i") and $\overset{\infty}{\exists} i$ ("there exists infinitely many is") as they are defined in the book.

Exercise 6. 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 7. ($\star$) 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 8. ($\star$)

(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 $\mathit{closure}(P) = P$.

2 ω-Regular Languages and Büchi Automata

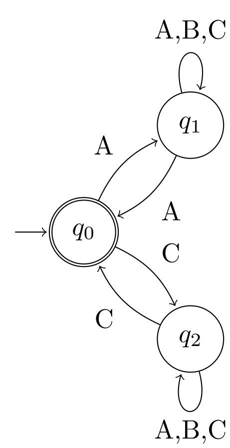
Exercise 9.

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.

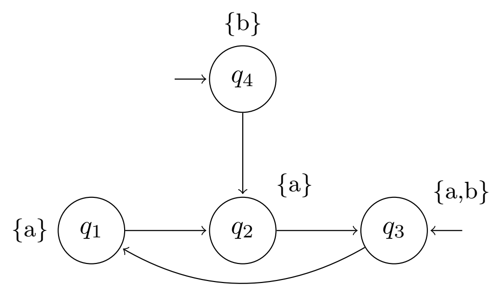
Exercise 10. Consider the following NBA A over the alphabet $\{A, B, C\}$:



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

3 LTL

Exercise 11. Consider the following transition system over the set of atomic propositions $\{a, b\}$:



Indicate for each of the following LTL formulae the set of states for which these formulae are fulfilled:

1. $\bigcirc a$
2. $\bigcirc\bigcirc\bigcirc a$
3. $\square b$
4. $\square\lozenge a$
5. $\square b \cup a$
6. $\lozenge a \cup b$

4 Solutions to Selected Exercises

Answer to exercise 3

1. false: $P := \emptyset$
2. initially x is equal to zero: $P = \{A_0, A_1, A2... \in (2^{AP})^\omega \,|\, x = 0 \in A_0\}$
3. initially x differs from zero: $P = \{A_0, A_1, A2... \in (2^{AP})^\omega \,|\, x = 0 \notin A_0\}$
4. initially x is equal to zero, but at some point x exceeds one: $P = \{A_0, A_1, A2... \in (2^{AP})^\omega \,|\, x = 0 \in A_0 \wedge \exists i > 0.(x > 0) \in A_i\}$
5. x exceeds one only finitely many times: $P = \{A_0, A_1, A_2... \in (2^{AP})^\omega | \exists i \geq 0.\forall j \geq i.(x > 1) \notin A_j\}$
6. x exceeds one infinitely often: $P = \{A_0, A_1, A_2... \in (2^{AP})^\omega \,|\, \forall i \geq 0.\exists j \geq i.(x > 1) \in A_j\}$
7. the value of x alternates between zero and one:

$$\begin{aligned} &P = \{A_0, A_1, A_2... \in (2^{AP})^\omega \,|\, [\forall i.((x = 0) \in A_i \rightarrow \{x > 1, x = 0\} \not\subseteq A_{i+1})] \\ &\wedge[\forall i.(\{x > 1, x = 0\} \not\subseteq A_i \rightarrow (x = 0) \in A_{i+1})] \\ &\wedge[\forall i.\{x = 0, x > 1\} \not\subseteq A_i\}] \\ &\wedge[x = 0 \in A_0 \vee x > 1 \in A_0]\} \end{aligned}$$

8. true: $P = (2^{AP})^\omega$

Answer to exercise 4

1. Three solutions:
   $P = \{A0, A1, ... \in (2^{AP})^\omega | (\forall i \geq 0.\{a, b\} \not\subseteq A_i)\}$
   $P = \{A0, A1, ... \in (2^{AP})^\omega | (\forall i \geq 0.(a \in A_i \implies b \notin A_i) \wedge (b \in A_i \implies a \notin A_i)\}$
   $P = \{A0, A1, ... \in (2^{AP})^\omega | (\forall i \geq 0.(a \in A_i \wedge b \notin A_i) \vee (a \notin A_i \wedge b \in A_i) \vee (a \notin A_i \wedge b \notin A_i)\}$
2. The word $\emptyset^\omega$ is not in P (and should be)

Answer to exercise 5

1. initially a holds and b does not hold
   $P = \{A0, A1, ... \in (2^{AP})^\omega \,|\, a \in A_0 \wedge b \notin A_0\}$
   This property is a SAFETY PROPERTY. A bad prefix can be any word in $(2^{AP})^\star$ starting with $\{\}$ or $\{b\}$ or $\{c\}$ or $\{a, b\}$ or $\{b, c\}$ or $\{a, b, c\}$.
2. c holds only finitely many times
   $P = \{A0, A1, ... \in (2^{AP})^\omega | \overset{\infty}{\forall} i.c \notin A_i\}$
   Recall that $\overset{\infty}{\forall} j.F$ is defined as $\exists i \geq 0.\forall j \geq i.F$ and stands for "for almost all $j \in \mathbb{N}$". This is a LIVENESS PROPERTY because no prefix can be classified as bad because the information on the occurrences of "c" in the tail of the word is missing.
3. from some point on the truth value of a alternates between true and false
   $P = \{A0, A1, ... \in (2^{AP})^\omega | \exists i \geq 0.\forall j \geq i.a \in A_j \leftrightarrow a \notin A_{j+i}\}$
   LIVENESS: no prefix can be classified as bad without the information on the tail of the word.
4. whenever c holds, then also a or b must hold
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | \forall i \geq 0.(c \in A_i \rightarrow a \in A_j \vee b \in A_j)\}$
   SAFETY: as above

5. whenever c holds, then a or be must hold sometime afterwards
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | \forall i \geq 0.(c \in A_i \rightarrow \exists j \geq i.a \in A_j \vee b \in A_j)\}$
   LIVENESS: as above.

6. b holds infinitely many times and whenever b holds then c holds afterwards
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | (\forall i \geq 0.\exists j \geq i.b \in A_i) \wedge (\forall i \geq 0.(b \in A_i \rightarrow \exists j \geq i : c \in A_j))\}$
   or,
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | (\overset{\infty}{\exists} i \geq 0.b \in A_i) \wedge (\forall i \geq 0.(b \in A_i \rightarrow \exists j \geq i : c \in A_j))\}$
   LIVENESS.

7. whenever c holds then also a or b holds
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | \forall i \geq 0.(c \in A_i \rightarrow (a \in A_i \vee b \in A_i))\}$
   SAFETY: a bad prefix is, for instance, $\{c\}\{\}\{\}\{\}$...

8. a holds only finitely many times and c holds infinitely many times
   $P = \{A0, A1, ... \in (2^{AP})^\omega | (\overset{\infty}{\forall} i \geq 0.a \notin A_i) \wedge (\overset{\infty}{\exists} i \geq 0.c \in A_i)\}$
   LIVENESS

9. whenever a holds then b and c holds after one step
   $P = \{A_0, A_1, ... \in (2^{AP})^\omega | \forall i \geq 0.a \in A_i \rightarrow (b \in A_{i+1} \wedge c \in A_{i+1})\}$
   SAFETY: a bad prefix is for instance $\{a\}\{a\}\{a\}$...

10. never a and b hold at the same time and eventually c holds
    $P = \{A0, A1, ... \in (2^{AP})^\omega | (\forall i \geq 0.\{a, b\} \nsubseteq A_i) \wedge (\exists i \geq 0.c \in A_i)\}$
    MIXED: a bad prefix for the first part is $\{a, b\}\{\}\{\}$... The part on “eventually” c cannot have a bad prefix, so it is liveness property.

11. at any point the number of times a held in the past is always greater than or equal to the number of times b held in the past.
    $P = \{A0, A1, ... \in (2^{AP})^\omega \ | \forall i \geq 0.|\{0 \leq j \ \leq i : a \in A_j\}| \geq |\{0 \leq j \leq i : b \in A_j\}|\}$
    where $|\{...\}|$ is set cardinality.
    SAFETY: a bad prefix for example $\{b\}\{\}\{\}$...