Reactive Systems Verification
alias
Model Checking I

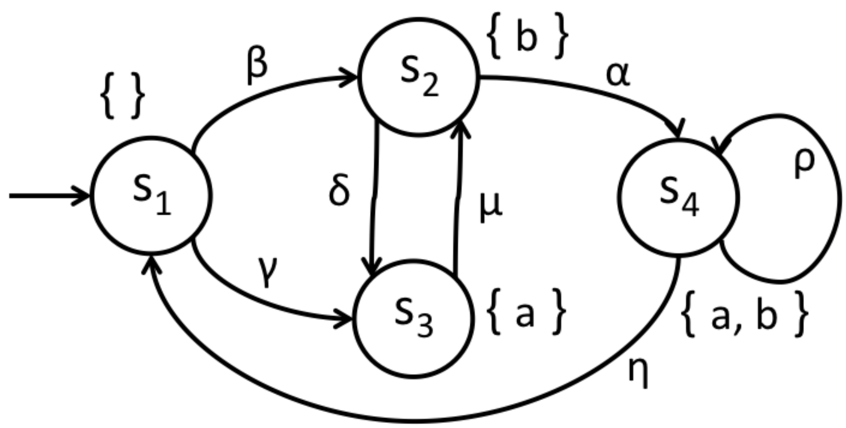
Solutions of Assignment 3

Luca Tesei

Academic Year 2015/16

Exercise 1

Consider the following LTS where the set of atomic propositions is $\mathrm{AP} = \{a, b\}$.



1. Specify formally the set of all the traces on the alphabet 2^{AP}.
2. For each of the following fairness conditions:

   (a) $\mathcal{F}_1 = \{\{\}, \{\}, \{\eta\}\}$
   (b) $\mathcal{F}_2 = \{\{\}, \{\eta\}, \{\}\}$
   (c) $\mathcal{F}_3 = \{\{\eta\}, \{\}, \{\}\}$
   (d) $\mathcal{F}_4 = \{\{\}, \{\}, \{\alpha\}\}$
   (e) $\mathcal{F}_5 = \{\{\}, \{\alpha\}, \{\}\}$
   (f) $\mathcal{F}_6 = \{\{\alpha\}, \{\}, \{\}\}$
   (g) $\mathcal{F}_7 = \{\{\}, \{\delta\}, \{\eta\}\}$
   (h) $\mathcal{F}_8 = \{\{\delta\}, \{\}, \{\eta\}\}$
   (i) $\mathcal{F}_9 = \{\{\eta\}, \{\delta\}, \{\}\}$
   (j) $\mathcal{F}_{10} = \{\{\delta, \eta\}, \{\}, \{\}\}$

   determine if the fairness condition is realizable and, if yes, specify the corresponding set of *fair* traces.

Solution of Exercise 1

1. The possible paths, with the corresponding traces, are the following:
   - paths of kind $\Pi_1 = s_1(s_2 + s_3s_2)(s_3s_2)^\omega$,
     with traces $T_1 = \{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^\omega$
   - paths of kind $\Pi_2 = s_1(s_2 + s_3s_2)(s_3s_2)^* s_4^\omega$,
     with traces $T_2 = \{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^* \{a, b\}^\omega$
   - paths of kind $\Pi_3 = (s_1(s_2 + s_3s_2)(s_3s_2)^* s_4^+)^+ s_1(s_2 + s_3s_2)(s_3s_2)^\omega$,
     with traces $T_3 = (\{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^* \{a, b\}^+)^+ \{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^\omega$
   - paths of kind $\Pi_4 = (s_1(s_2 + s_3s_2)(s_3s_2)^* s_4^+)^+ s_1(s_2 + s_3s_2)(s_3s_2)^* s_4^\omega$,
     with traces $T_4 = (\{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^* \{a, b\}^+)^+ \{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^* \{a, b\}^\omega$
   - paths of kind $\Pi_5 = (s_1(s_2 + s_3s_2)(s_3s_2)^* s_4^+)^\omega$,
     with traces $T_5 = (\{\}(\{b\} + \{a\}\{b\})(\{a\}\{b\})^* \{a, b\}^+)^\omega$

2. Let us now consider the various fairness conditions:

   (a) $\mathcal{F}_1 = \{\{\}, \{\}, \{\eta\}\}$
   the fairness condition is trivially realizable; the weak fairness on η forbids to cycle forever in state s_4, thus all the paths of kinds Π_2 and Π_4 must be discarded. The other kinds are all fair.

   (b) $\mathcal{F}_2 = \{\{\}, \{\eta\}, \{\}\}$
   the fairness condition is trivially realizable; the strong fairness on η forbids to cycle forever in state s_4, thus all the paths of kinds Π_2 and Π_4 must be discarded. The other kinds are all fair.

   (c) $\mathcal{F}_3 = \{\{\eta\}, \{\}, \{\}\}$
   the fairness condition is realizable, i.e. from each state it is possible to start a fair path. The only fair paths in this case are those of kind Π_5, the others are all unfair because η is not executed infinitely many times unconditionally.

   (d) $\mathcal{F}_4 = \{\{\}, \{\}, \{\alpha\}\}$
   the fairness condition is trivially realizable; the weak fairness on α in this case is never "activated" that is to say that in no path α is continuously enabled infinitely many times. Thus, all kinds of paths are fair under this condition.

   (e) $\mathcal{F}_5 = \{\{\}, \{\alpha\}, \{\}\}$
   the fairness condition is trivially realizable; the strong fairness on α forbids to cycle forever between states s_3 and s_2, thus all the paths of kinds Π_1 and Π_3 must be discarded. The other kinds are all fair.

   (f) $\mathcal{F}_6 = \{\{\alpha\}, \{\}, \{\}\}$
   the fairness condition is realizable, i.e. from each state it is possible to start a fair path. The only fair paths in this case are those of kind Π_5, the others are all unfair because α is not executed infinitely many times unconditionally.

   (g) $\mathcal{F}_7 = \{\{\}, \{\delta\}, \{\eta\}\}$
   the fairness condition is trivially realizable; the weak fairness on η forbids to cycle forever in state s_4, thus all the paths of kinds Π_2 and Π_4 must be discarded. It is easy to see that the strong fairness on δ is respected by all runs of kind Π_1 and Π_3. The paths of kind Π_5 should be divided into those that visit state s_3 infinitely many times and those that do not. The former are fair under this condition, while the latter must be discarded.

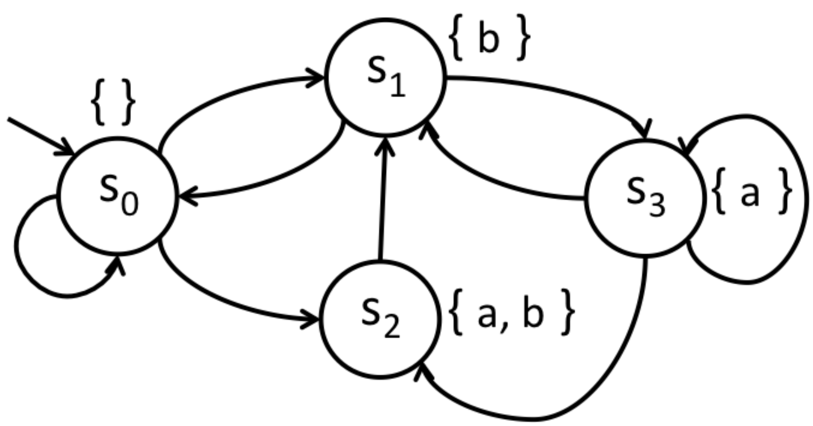
   (h) $\mathcal{F}_8 = \{\{\delta\}, \{\}, \{\eta\}\}$
   the fairness condition is realizable, i.e. from each state it is possible to start a fair path. The weak fairness on η forbids to cycle forever in state s_4, thus all the paths of kinds Π_2 and Π_4 must be discarded. The paths of kind Π_1 and Π_3 are obviously fair. The paths of kind Π_5 should be divided into those that visit state s_3 infinitely many times and those that do not. The former are fair under this condition, while the latter must be discarded.

(i) $\mathcal{F}_9 = \{\{\eta\}, \{\delta\}, \{\}\}$
the fairness condition is realizable, i.e. from each state it is possible to start a fair path. The paths of kind Π_5 should be divided into those that visit state s_3 infinitely many times and those that do not. The former are fair under this condition, while the latter must be discarded. The paths of kind Π_1, Π_2, Π_3 and Π_4 are all unfair and must be discarded.

(j) $\mathcal{F}_{10} = \{\{\delta, \eta\}, \{\}, \{\}\}$
the fairness condition is realizable, i.e. from each state it is possible to start a fair path. The paths of kind Π_1 and Π_3 are obviously fair. The paths of kind Π_5 are all fair. The paths of kind Π_2 and Π_4 are unfair and must be discarded.

Exercise 2

Consider the following transition system TS.

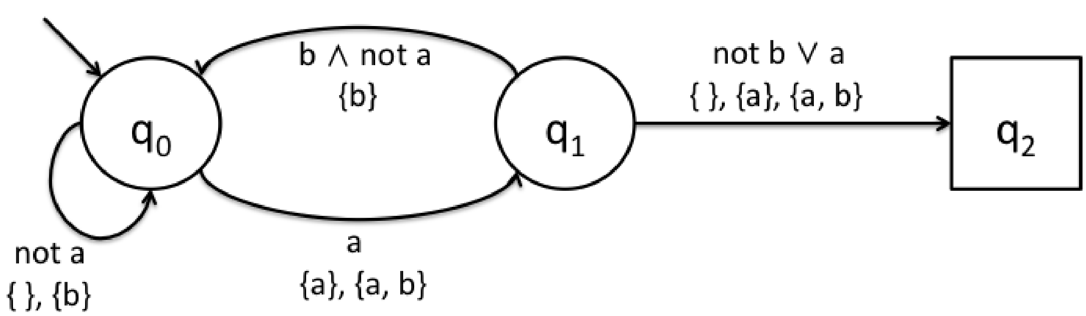


Consider a set of atomic propositions $\mathrm{AP} = \{a, b\}$ and the following safety property P_{safe}: "whenever a holds then after one step b holds and a does not hold".

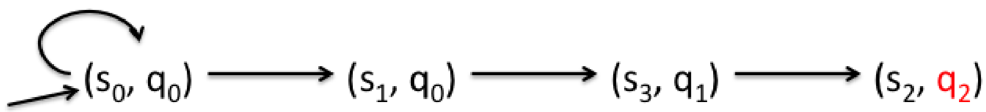
1. Draw a NFA A that accepts the set of *minimal bad prefixes* for P_{safe}.
2. Decide if $\mathrm{TS} \models P_{\text{safe}}$ by using the product $\mathrm{TS} \otimes A$. In case $\mathrm{TS} \not\models P_{\text{safe}}$, provide a counterexample.

Solution of Exercise 2

1. The NFA A accepting the set of minimal bad prefixes is the following



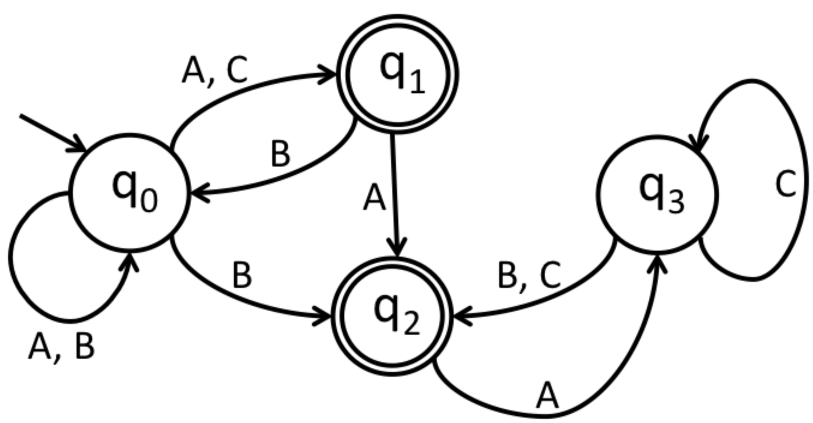
2. The following portion of the product TS $\otimes A$ shows that TS $\not\models P_{\text{safe}}$



Indeed, a state is reachable where the accepting state of the automaton A is present. The corresponding counter example is the path $s_0s_1s_3s_2$ corresponding to the trace $\{\}\{b\}\{a\}\{a,b\}$, i.e. after one step in which a held, a holds again violating the property.

Exercise 3

1. Write an ω-regular expression that denotes exactly the ω-regular language accepted by the following non-deterministic Büchi automaton:



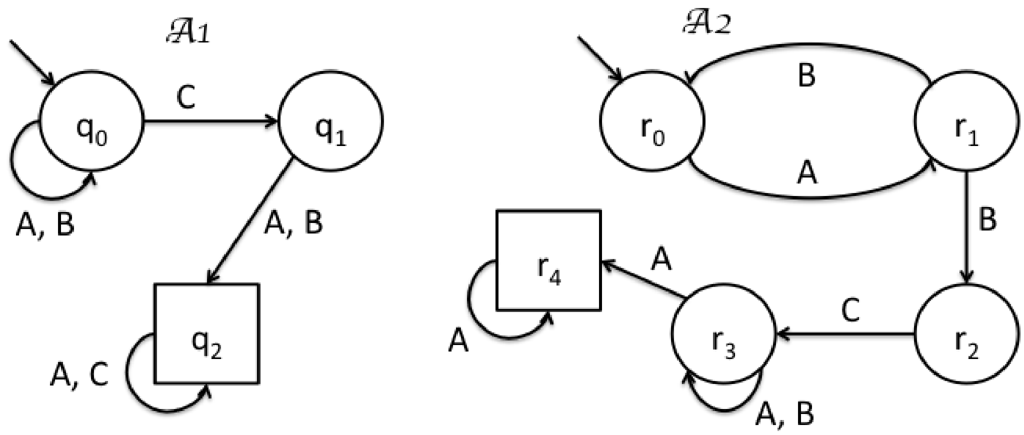
2. Draw two non-deterministic Büchi automata A_1 and A_2 such $\mathcal{L}(A_1)$ is the ω-regular language denoted by the ω-regular expression $(A{+}B)^*(CB{+}CA)(A{+}C)^\omega$ and $\mathcal{L}(A_2)$ is the ω-regular language denoted by the ω-regular expression $(AB)^+C(A+B)^*A^\omega$. Then, apply the product construction (using GNBA) to obtain an NBA A with $\mathcal{L}(A) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2)$.

Solution of Exercise 3

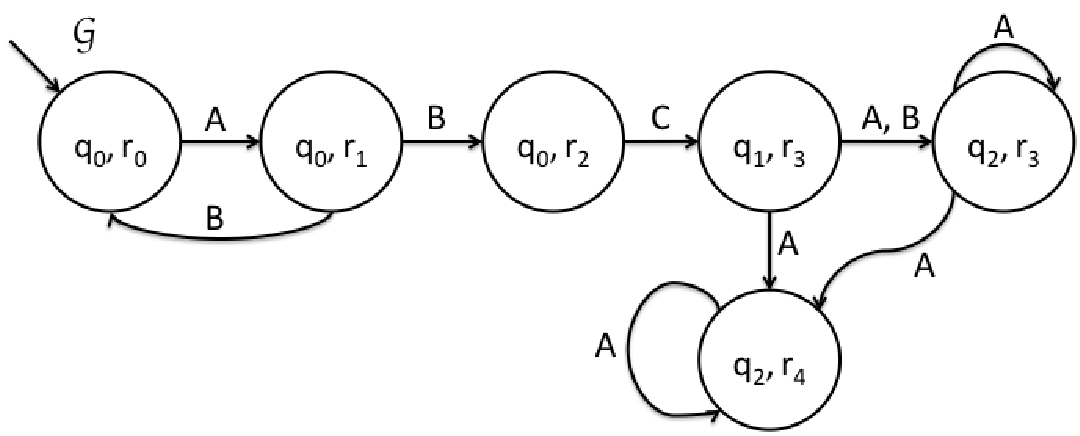
1. $\mathcal{L}_{q_0q_1} = [(A+B)^*(AB+CB)+(A+B)^*]^*(A+C)$
   $\mathcal{L}_{q_1q_1} = [B(A+B)^*(A+C)]^*$
   $\mathcal{L}_{q_1q_1}\backslash\{\epsilon\} = [B(A+B)^*(A+C)]^+$
   $\mathcal{L}_{q_0q_2} = [(A+B)^*(AB+CB)+(A+B)^*]^*(B+AA+CA)[AC^*(B+C)]^*$
   $\mathcal{L}_{q_2q_2} = [AC^*(B+C)]^*$
   $\mathcal{L}_{q_2q_2}\backslash\{\epsilon\} = [AC^*(B+C)]^+$

$$\begin{aligned}\mathcal{L}_\omega = \ & [(A+B)^*(AB+CB)+(A+B)^*]^*(A+C)[B(A+B)^*(A+C)]^\omega + \\ & [(A+B)^*(AB+CB)+(A+B)^*]^*(B+AA+CA)[AC^*(B+C)]^*[AC^*(B+C)]^\omega\end{aligned}$$

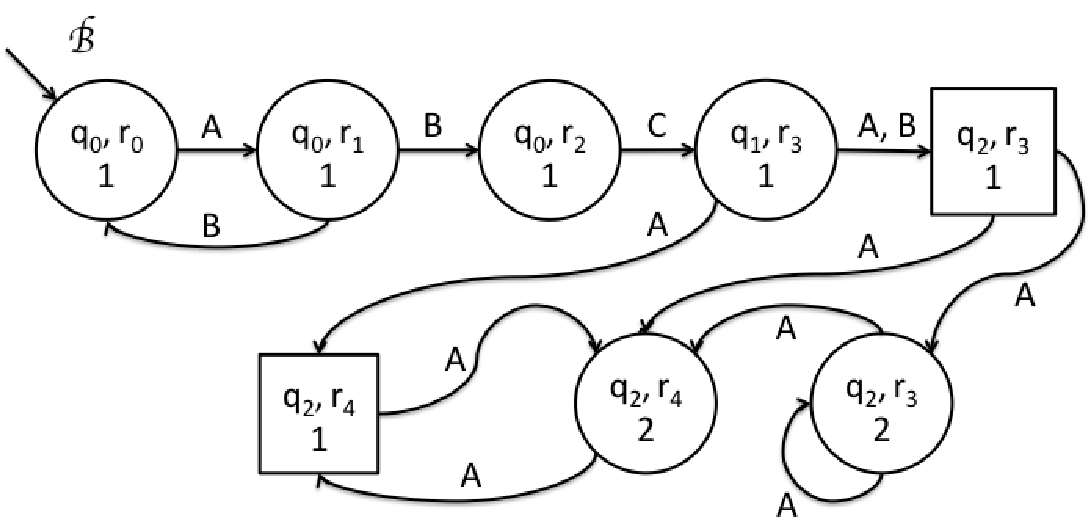
2. The two NBAs A_1 and A_2 are depicted in the following



The GNBA $\mathcal{G}$ resulting from the synchronous product of A_1 and A_2 is the following



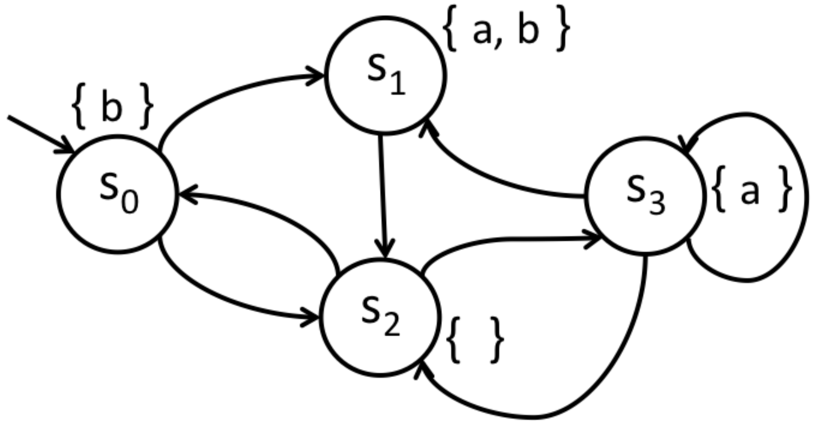
where the family of accepting states is $\mathcal{F}_{\mathcal{G}} = \{\{(q_2, r_3), (q_2, r_4)\}, \{(q_2, r_4)\}\}$.
By applying the construction to obtain an NBA from a GNBA, the following NBA B is obtained



accepting the language $(AB)^{+}C(A+B)A^{\omega}$, which is indeed the intersection $\mathcal{L}(A_1) \cap \mathcal{L}(A_2)$.

Exercise 4

Consider a set of atomic propositions $\mathrm{AP} = \{a, b\}$ and the following transition system TS.

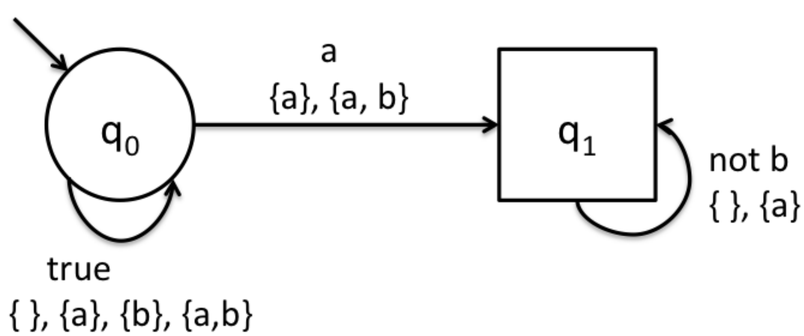


Consider the following liveness property P_{live}: "whenever a holds then b will eventually hold".

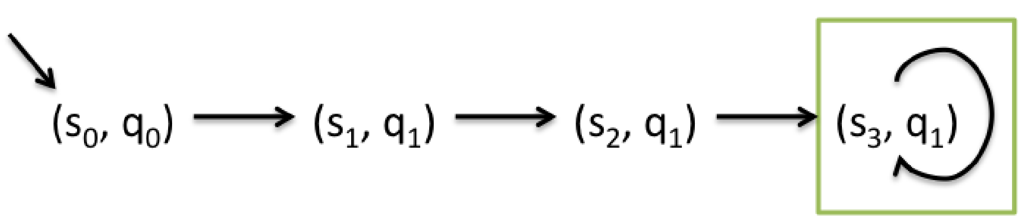
1. Draw a NBA A that accepts the set of *bad behaviours* for P_{live}.
2. Decide if $\mathrm{TS} \models P_{\text{live}}$ by using the product $\mathrm{TS} \otimes A$. In case $\mathrm{TS} \not\models P_{\text{live}}$, provide a counterexample.

Solution of Exercise 4

1. An NBA A accepting the set of *bad behaviours* for P_{live} is as follows



In the following a partial TS resulting from the product



showing that $\mathrm{TS} \not\models P_{\mathrm{live}}$ because a strongly connected component (surrounded in green) is reachable containing the accepting state q_1. The associated counterexample is the path $s_0 s_1 s_2 s_3^\omega$ corresponding to the trace $\{b\}\{a,b\}\{\}\{a\}^\omega$.