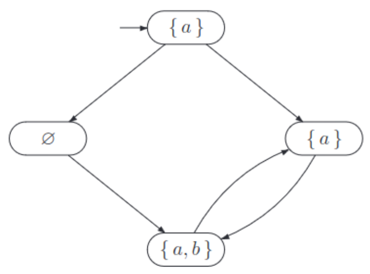
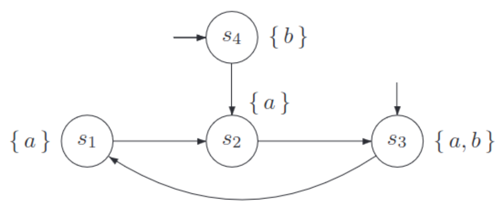
Model Checking: exercise set 1 - LTL

These exercises are from the *Principles of Model Checking* book.
Due date: February 4

3.1 Give the traces on the set of atomic propositions $\{a, b\}$ of the following transition system:



5.1 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:

(a) $\bigcirc a$

(b) $\bigcirc \bigcirc \bigcirc a$

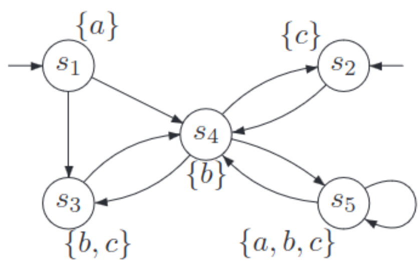
(c) $\Box b$

(d) $\Box \Diamond a$

(e) $\Box (b \,\mathsf{U}\, a)$

(f) $\Diamond (a \,\mathsf{U}\, b)$

5.2 Consider the transition system TS over the set of atomic propositions $\{a, b, c\}$:



Decide for each of the LTL formulae φ_i below, whether $TS \models \varphi_i$ holds. Justify your answers! If $TS \not\models \varphi_i$, provide a path $\pi \in Paths(TS)$ such that $\pi \not\models \varphi_i$.

$$\varphi_1 = \Diamond \Box c$$
$$\varphi_2 = \Box \Diamond c$$
$$\varphi_3 = \bigcirc \neg c \longrightarrow \bigcirc \bigcirc c$$
$$\varphi_4 = \Box a$$
$$\varphi_5 = a \,\mathsf{U}\, \Box (b \vee c)$$
$$\varphi_6 = (\bigcirc \bigcirc b) \,\mathsf{U}\, (b \vee c)$$

5.4 Suppose we have two users, *Peter* and *Betsy*, and a single printer device *Printer*. Both users perform several tasks, and every now and then they want to print their results on the *Printer*. Since there is only a single printer, only one user can print a job at a time. Suppose we have the following atomic propositions for *Peter* at our disposal:

- *Peter.request* ::= indicates that *Peter* requests usage of the printer;
- *Peter.use* ::= indicates that *Peter* uses the printer;
- *Peter.release* ::= indicates that *Peter* releases the printer.

For *Betsy*, similar predicates are defined. Specify in LTL the following properties:

(a) Mutual exclusion, i.e., only one user at a time can use the printer.

(b) Finite time of usage, i.e., a user can print only for a finite amount of time.

(c) Absence of individual starvation, i.e., if a user wants to print something, he/she eventually is able to do so.

(d) Absence of blocking, i.e., a user can always request to use the printer

(e) Alternating access, i.e., users must strictly alternate in printing.

5.6 Which of the following equivalences are correct? Prove the equivalence or provide a counterexample that illustrates that the formula on the left and the formula on the right are not equivalent.

(a) $\Box\varphi \longrightarrow \Diamond\psi \equiv \varphi \,\mathsf{U}\, (\psi \vee \neg\varphi)$

(b) $\Diamond\Box\varphi \longrightarrow \Box\Diamond\psi \equiv \Box(\varphi \,\mathsf{U}\, (\psi \vee \neg\varphi))$

(c) $\Box\Box(\varphi \vee \neg\psi) \equiv \neg\Diamond(\neg\varphi \wedge \psi)$

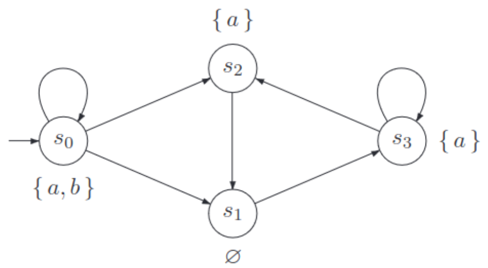
(d) $\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$

(e) $\Box\varphi \wedge \bigcirc\Diamond\varphi \equiv \Box\varphi$

(f) $\Diamond\varphi \wedge \bigcirc\Box\varphi \equiv \Diamond\varphi$

5.14 *This is a challenging question to get your hands dirty on the LTL model checking algorithm. This exercise is* ***optional****.*

Consider the transition system TS in the figure below with the atomic propositions $\{a, b\}$.



Sketch the main steps of the LTL model-checking algorithm applied to TS and the LTL formulae:

$$\varphi_1 = \Box\Diamond a \longrightarrow \Box\Diamond b \text{ and } \varphi_2 = \Diamond(a \wedge \bigcirc a).$$

To that end, carry out the following steps:

(a) Depict an NBA A_i for $\neg\varphi_i$.

(b) Depict the reachable fragment of the product transition system $TS \otimes A_i$

(c) Explain the main steps of the nested DFS in $TS \otimes A_i$ by illustrating the order in which the states are visited during the "outer" and "inner" DFS.

(d) If $TS \not\models \varphi_i$, provide the counterexample resulting from the nested DFS.