cover the full class of ω-regular LT properties, Vardi and Wolper introduced an extension of LTL by automata formulae [424, 425, 411, 412].

LTL model checking. Vardi and Wolper also developed the automata-based model checking algorithm for LTL presented in this chapter. The presented algorithm to construct an NBA from a given LTL formula is, in our opinion, the simplest and most intuitive one. In the meantime, various alternative techniques have been developed that generate more compact NBAs or that attempt to minimize a given NBA, see e.g. [166, 110, 148, 375, 162, 149, 167, 157, 389, 369]. Alternative LTL model-checking algorithms that do not use Büchi automata, but a so-called tableau for the LTL formula, were presented by Lichtenstein and Pnueli [273] and Clarke, Grumberg, and Hamaguchi [88]. The results about the complexity of LTL model checking and the satisfiability problem are due to Sistla and Clarke [372].

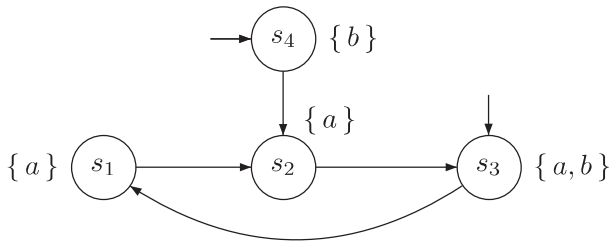
There is a variety of surveys and textbooks; see, e.g.,[245, 138, 173, 283, 158, 284, 92, 219, 379, 365], where several other aspects of LTL and related logics, such as deductive proof systems, alternative model-checking algorithms, or more details about the expressiveness, are treated.

Examples. The garbage collection algorithm presented in Example 5.31 is due to Ben-Ari [41]. Several leader election protocols that fit into the shape of Example 5.13 have been suggested; see, e.g., [280].

LTL model checkers. SPIN is the most well-known LTL model checker and has been developed by Holzmann [209]. Transition systems are described in the modeling language Promela, and LTL formulae are checked using the algorithm advocated by Gerth et al. [166]. LTL model checking using a tableau construction is supported by NuSMV [83].

5.5 Exercises

Exercise 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) $\bigcirc\, \bigcirc\, \bigcirc\, a$

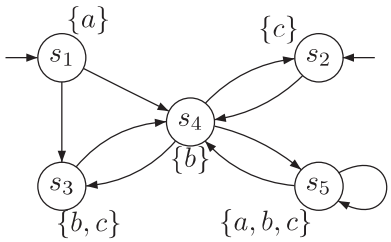
(c) $\Box\, b$

(d) $\Box \Diamond\, a$

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

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

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



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 $\pi \not\models \varphi_i$.

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

EXERCISE 5.3. Consider the sequential circuit in Figure 5.24 and let $AP = \{\, x, y, r_1, r_2 \,\}$. Provide LTL formulae for the following properties:

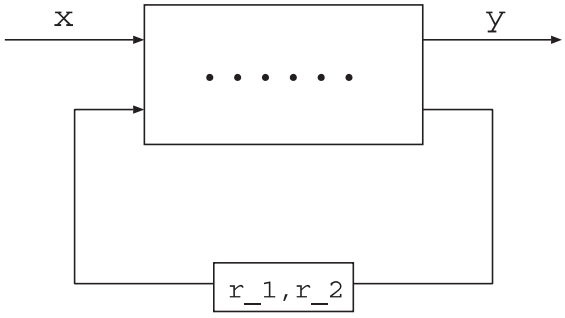


Figure 5.24: Circuit for Exercise 5.3.

(b) Prove that $\varphi \,\mathsf{R}\, \psi \equiv (\neg\varphi \wedge \psi)\,\mathsf{W}\,(\varphi \wedge \psi)$.

(c) Prove that $\varphi_1 \,\mathsf{W}\, \varphi_2 \;\equiv\; (\neg\varphi_1 \vee \varphi_2)\,\mathsf{R}\,(\varphi_1 \vee \varphi_2)$.

(d) Prove that $\varphi_1 \,\mathsf{U}\, \varphi_2 \;\equiv\; \neg(\neg\varphi_1 \,\mathsf{R}\, \neg\varphi_2)$.

EXERCISE 5.9. Consider the LTL formula

$$\varphi \;=\; \neg\Big((\Box a) \rightarrow \big((a \wedge \neg c)\,\mathsf{U}\,\neg(\bigcirc b)\big)\Big) \wedge \neg(\neg a \vee \bigcirc \Diamond c).$$

Transform φ into an equivalent LTL formula in PNF

(a) using the weak-until operator W,

(b) using the release operator R.

EXERCISE 5.10. Provide an example for a sequence (φ_n) of LTL formulae such that the LTL formula ψ_n is in weak-until PNF, $\varphi_n \equiv \psi_n$, and ψ_n is exponentially longer than φ_n. Use the transformation rules in Section 5.1.5

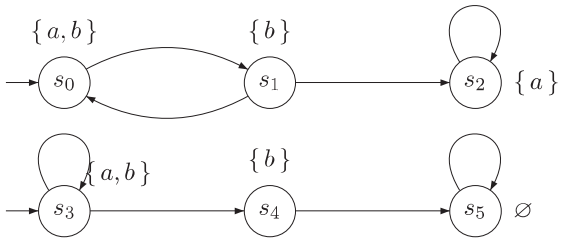


Figure 5.25: Transition system for Exercise 5.11.

EXERCISE 5.11. Consider the transition system TS in Figure 5.25 with the set $AP = \{ a, b, c \}$ of atomic propositions. Note that this is a single transition system with two initial states. Consider the LTL fairness assumption

$$\mathit{fair} \;=\; \big(\Box\Diamond(a \wedge b) \;\rightarrow\; \Box\Diamond\neg c\big) \;\wedge\; \big(\Diamond\Box(a \wedge b) \rightarrow \Box\Diamond\neg b\big).$$

Questions:

(a) Determine the fair paths in TS, i.e., the initial, infinite paths satisfying *fair*

(b) For each of the following LTL formulae:

$$\begin{aligned}
\varphi_1 &= \Diamond\Box a \\
\varphi_2 &= \bigcirc\neg a \;\longrightarrow\; \Diamond\Box a \\
\varphi_3 &= \Box a \\
\varphi_4 &= b\,\mathsf{U}\;\Box\neg b \\
\varphi_5 &= b\,\mathsf{W}\;\Box\neg b \\
\varphi_6 &= \bigcirc\bigcirc\, b\,\mathsf{U}\,\Box\neg b
\end{aligned}$$

determine whether $TS \models_{fair} \varphi_i$. In case $TS \not\models_{fair} \varphi_i$, indicate a path $\pi \in \mathit{Paths}(TS)$ for which $\pi \not\models \varphi_i$.

EXERCISE 5.12. Let $\varphi = (a \rightarrow \bigcirc \neg b)\,\mathsf{W}\,(a \wedge b)$ and $P = \mathit{Words}(\varphi)$ where $AP = \{\, a, b \,\}$.

(a) Show that P is a safety property.

(b) Define an NFA $\mathcal{A}$ with $\mathcal{L}(\mathcal{A}) = \mathit{BadPref}(P)$.

(c) Now consider $P' = \mathit{Words}\big((a \rightarrow \bigcirc \neg b)\,\mathsf{U}\,(a \wedge b)\big)$. Decompose P' into a safety property P_{safe} and a liveness property P_{live} such that

$$P' = P_{safe} \cap P_{live}.$$

Show that P_{safe} is a safety and that P_{live} is a liveness property.

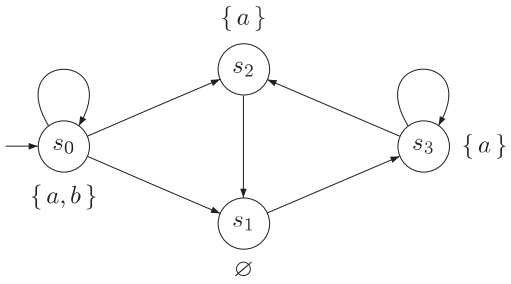


Figure 5.26: Transition system for Exercise 5.14.

EXERCISE 5.13. Provide an NBA for each of the following LTL formulae:

$$\Box(a \vee \neg \bigcirc\, b) \quad \text{and} \quad \Diamond a \;\vee\; \Box\Diamond(a \leftrightarrow b) \quad \text{and} \quad \bigcirc\, \bigcirc\, (a \vee \Diamond\Box b).$$

EXERCISE 5.14. Consider the transition system TS in Figure 5.26 with the atomic propositions $\{\, a, b \,\}$. Sketch the main steps of the LTL model-checking algorithm applied to TS and the LTL formulae

$$\varphi_1 \;=\; \Box\Diamond a \rightarrow \Box\Diamond b \quad \text{and} \quad \varphi_2 \;=\; \Diamond(a \wedge \bigcirc\, a).$$

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 $TS \otimes \mathcal{A}_i$.

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