Principles of Model Checking
Solutions to exercise class 3

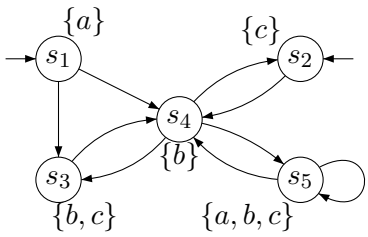
Linear temporal logic

Prof. Dr. Joost-Pieter Katoen, Dr. Taolue Chen, and Ir. Mark Timmer

September, 28, 2012

Problem 1

We have to decide the validity of the given LTL formulas with respect to the transition system on the right. This yields:



$\varphi_1 = \Box\Diamond c$	yes
$\varphi_2 = \bigcirc\neg c \rightarrow \bigcirc\bigcirc c$	yes
$\varphi_3 = a \mathsf{U} \Box(b \vee c)$	yes
$\varphi_4 = (\bigcirc\bigcirc b) \mathsf{U} (b \vee c)$	no

For φ_1 this is easy to see: we will infinitely often be in s_2, s_3 or s_5, so indeed always eventually c. For φ_2, notice that $\bigcirc\neg c$ only holds on a path starting with either $s_1 s_4$ or $s_2 s_4$. These will continue to go to either s_2, s_3 or s_5, which all satisfy c. Hence, initially $\bigcirc\bigcirc c$.

To see why φ_3 holds, notice that every path starts with either $s_1 s_3$, $s_1 s_4$, or $s_2 s_4$. The first two kinds indeed start with an a-state and then enter a state from which only states are reachable that have at least a b or a c label, so from which indeed always $b \vee c$. Hence, these paths satisfy $a \mathsf{U} \Box(b \vee c)$. The third kind of paths immediately starts in a state in which b or c holds (namely c), and can only reach such states. Hence, it satisfies $\Box(b \vee c)$ and thus also $a \mathsf{U} \Box(b \vee c)$.

For φ_4, consider a path starting with $s_1 s_4 s_2 \ldots$. Such a path doesn't satisfy $\bigcirc\bigcirc b$, and neither does it satisfy $b \vee c$. Hence, the property does not hold.

Problem 2

1. $\Box\varphi \rightarrow \Diamond\psi \equiv \varphi \mathsf{U}(\psi \vee \neg\varphi)$. To see why:

   - $\mathit{Words}(\Box\varphi \rightarrow \Diamond\psi) \subseteq \mathit{Words}(\varphi \mathsf{U}(\psi \vee \neg\varphi))$

     Let $\sigma \in \mathit{Words}(\Box\varphi \rightarrow \Diamond\psi)$. We make a case distinction based on whether or not $\sigma \models \Box\varphi$.

     - If $\sigma \models \Box\varphi$, then by assumption also $\sigma \models \Diamond\psi$. Clearly, these two facts imply $\sigma \models \varphi \mathsf{U} \psi$. It is easy to see that this implies $\sigma \models \varphi \mathsf{U}(\psi \vee \neg\varphi)$.
     - If $\sigma \not\models \Box\varphi$, then for one or more j we have $\sigma[j...] \not\models \varphi$. Let k be the smallest such index. So, $\sigma[k...] \not\models \varphi$ and also $\forall i < j.\ \sigma[i...] \models \varphi$. This immediately implies that $\sigma \models \varphi \mathsf{U} \neg\varphi$, and hence $\sigma \models \varphi \mathsf{U}(\psi \vee \neg\varphi)$.

     So, $\sigma \in \mathit{Words}(\varphi \mathsf{U}(\psi \vee \neg\varphi))$.

   - $\mathit{Words}(\varphi \mathsf{U}(\psi \vee \neg\varphi)) \subseteq \mathit{Words}(\Box\varphi \rightarrow \Diamond\psi)$

     Let $\sigma \in \mathit{Words}(\varphi \mathsf{U}(\psi \vee \neg\varphi))$. To show $\sigma \in \mathit{Words}(\Box\varphi \rightarrow \Diamond\psi)$, we assume that $\sigma \models \Box\varphi$ and prove that $\sigma \models \Diamond\psi$. Since by assumption $\sigma \models \varphi \mathsf{U}(\psi \vee \neg\varphi)$, at some point $\psi \vee \neg\varphi$ must hold. Because of $\sigma \models \Box\varphi$, this can only be the case if eventually ψ holds. Hence, $\sigma \models \Diamond\psi$.

2. $\Box\Diamond\varphi \rightarrow \Box\Diamond\psi \not\equiv \Box(\varphi \rightarrow \Diamond\psi)$. To see why:

   Take $AP = \{a, b\}$, let $\varphi = a$ and $\psi = b$, and consider the infinite trace $\sigma = \varnothing\{a\}\varnothing^{\omega}$. The left-hand side of the LTL property is fulfilled by σ, as its premise $\Box\Diamond\varphi$ is false. On the other hand, σ does not fulfill the right-hand side. After all, at some point φ holds, but ψ never holds afterwards.

Problem 3

1. The fair paths of TS are those that satisfy

$$fair = (\Box\Diamond\,(a \wedge b) \rightarrow \Box\Diamond\neg c) \wedge (\Diamond\Box\,(a \wedge b) \rightarrow \Box\Diamond\neg b)$$

Note that the part $\Diamond\Box\,(a \wedge b) \rightarrow \Box\Diamond\neg b$ holds if $\Diamond\Box\,(a \wedge b)$ does not hold, as well as if $\Diamond\Box\,(a \wedge b)$ and $\Box\Diamond\neg b$ both hold. The latter option can never happen, since $\Diamond\Box\,(a \wedge b)$ implies $\Diamond\Box b$, which means that from some point b always holds. Hence, from that point $\Diamond\neg b$ does not hold anymore, so initially $\Box\Diamond\neg b$ does not hold. So, $\Diamond\Box\,(a \wedge b)$ cannot hold for any fair path. This excludes the path $\pi = (s_3)^\omega$.

Since there is no c-state in the system, clearly $\Box\Diamond\neg c$ holds for every path. Therefore, also $\Box\Diamond\,(a \wedge b) \rightarrow \Box\Diamond\neg c$ holds for every path. Hence, the path π above is the only unfair path in TS. This yields

$$\mathit{FairPaths}(TS) = \mathcal{L}_\omega\left((s_0 s_1)^\omega + (s_0 s_1)^+ (s_2)^\omega + (s_3)^+ s_4 (s_5)^\omega\right)$$

2. - $TS \not\models_{\mathit{fair}} \bigcirc\neg a \rightarrow \Diamond\Box a$:

Consider the path $\pi_1 = s_3 s_4\,(s_5)^\omega \in \mathit{FairPaths}(TS)$. For its corresponding trace

$$\sigma_1 = \mathit{trace}(\pi_1) = \{a, b\}\{b\}\varnothing^\omega$$

we find $\sigma_1 \in \mathit{Words}(\bigcirc\neg a)$, but $\sigma_1 \notin \mathit{Words}(\Diamond\Box a)$. Hence, $\sigma_1 \notin \mathit{Words}(\bigcirc\neg a \rightarrow \Diamond\Box a)$ and thus $TS \not\models_{\mathit{fair}} \bigcirc\neg a \rightarrow \Diamond\Box a$.

- $TS \not\models_{\mathit{fair}} b\mathsf{U}\Box\neg b$:

Consider the path $\pi_2 = (s_0 s_1)^\omega \in \mathit{FairPaths}(TS)$. For its corresponding trace

$$\sigma_2 = \mathit{trace}(\pi_2) = (\{a, b\}\{b\})^\omega$$

we find $\sigma_2 \notin \mathit{Words}(b\mathsf{U}\Box\neg b)$, since there exists no $i \geq 0$ such that $\sigma_2[i...] \models \Box\neg b$. Hence, $TS \not\models_{\mathit{fair}} b\mathsf{U}\Box\neg b$.

- $TS \models_{\mathit{fair}} b\mathsf{W}\Box\neg b$:

The property $b\mathsf{W}\Box\neg b$ holds for each path that either (i) always satisfies b, or (ii) satisfies b until a point from which it never satisfies b anymore. The path $(s_0 s_1)^\omega$ satisfies (i), while paths of the form $(s_0 s_1)^+ s_2^\omega$ and $(s_3)^+ s_4 (s_5)^\omega$ satisfy (ii). Hence, $TS \models_{\mathit{fair}} b\mathsf{W}\Box\neg b$.

Note that the fairness assumption did not influence any of the claims above. Clearly, any LTL formula that doesn't hold under *fair* also wouldn't hold without fairness. Additionally, also the unfair path $(s_3)^\omega$ would have satisfied $b\mathsf{W}\Box\neg b$.

Problem 4

Given $\varphi = a \mathsf{U} \bigcirc a$, we construct a GNBA $\mathcal{G}_\varphi = \big(Q, 2^{\{a\}}, \delta, Q_0, \mathcal{F}\big)$ such that $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$. Therefore, we first need to compute the elementary sets with respect to $\mathit{closure}(\varphi)$, as these are the states of $\mathcal{G}_\varphi$. Note that

$$\mathit{closure}(\varphi) = \{a, \neg a, \bigcirc a, \neg \bigcirc a, a \mathsf{U} \bigcirc a, \neg (a \mathsf{U} \bigcirc a)\}$$

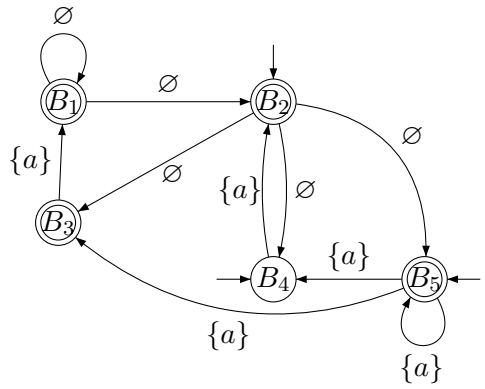
The elementary sets are as follows:

$$\begin{aligned} B_1 &= \{\neg a, \neg \bigcirc a, \neg (a \mathsf{U} \bigcirc a)\} \\ B_2 &= \{\neg a, \bigcirc a, a \mathsf{U} \bigcirc a\} \\ B_3 &= \{a, \neg \bigcirc a, \neg (a \mathsf{U} \bigcirc a)\} \\ B_4 &= \{a, \neg \bigcirc a, a \mathsf{U} \bigcirc a\} \\ B_5 &= \{a, \bigcirc a, a \mathsf{U} \bigcirc a\} \end{aligned}$$

Hence, $Q = \{B_1, B_2, B_3, B_4, B_5\}$. The set of initial states contains precisely those sets B_i such that $\varphi \in B$, so $Q_0 = \{B_2, B_4, B_5\}$.

The acceptance set contains one set $F_{\varphi_i \mathsf{U} \psi_i}$ for each subformula $\varphi_i \mathsf{U} \psi_i$ of φ. In our case, there is only one such subformula. Hence, $\mathcal{F} = \{F_{a \mathsf{U} \bigcirc a}\}$. This set $F_{a \mathsf{U} \bigcirc a}$ contains precisely all elementary sets B_i such that either $\bigcirc a \in B_i$ or $a \mathsf{U} \bigcirc a \notin B_i$. Hence, $F_{a \mathsf{U} \bigcirc a} = \{B_1, B_2, B_3, B_5\}$.

Finally, the transition relation δ is depicted below:



This picture was constructed by having a transition $B_i \xrightarrow{A} B_j$ if and only if A contains precisely the atomic propositions that hold in B_i, and B_j contains only formulas that could hold in a state directly after having been in a state where all formulas in B_i were true.