Solutions to TD7

1 Exercise 1

1. Suppose we have some function red satisfying (C1). Consider a state s and suppose there exists a in $red(s)$ and b in $en(s) \setminus red(s)$ such that a and b are not independent from each other. Then there exists t such that $s \xrightarrow{b} t$ in $\mathcal{K}$ and the path $s \xrightarrow{b} t$ violates (C1): this is a contradiction.

2. Consider the Kripke structure described in Figure 1, with $red(s) = en(s)$ for $s \neq s_0$ and $red(s_0) = \{a\}$. This satisfies (C0),(C1'),(C2),(C3) because a and b are independent from each other and a is invisible. One is able to differentiate between the original Kripke structure and its reduction thanks to a formula such as $\neg p \,\mathsf{U}\, (p \,\mathsf{U}\, \neg p)$, which is satisfied by the run $s_0 \to s_2 \to s_1 \to s_3$.

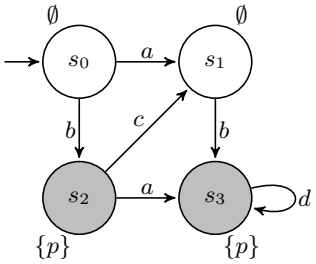
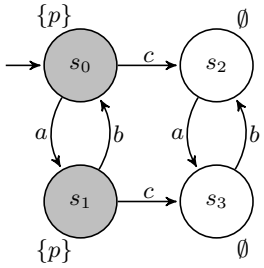


Figure 1: A Kripke structure.

2 Exercise 2



In the Kripke structure defined above, the assignments $red(s_0) = \{a\}$, $red(s_1) = \{b\}$, $red(s_2) = \{a\}$ and $red(s_3) = \{b\}$ satisfy (C0)-(C2) but result in a Kripke structure where states s_2 and s_3 are unattainable. Thus the LTL formula $p \,\mathsf{U}\, \mathsf{G}\, \neg p$ is able to differentiate between the original and the reduced Kripke structures.

Remark: Using the same idea, one can easily construct a counterexample that uses only two states.

3 Exercise 3

(Solution follows *Principles of Model Checking, Baier and Katoen*)

Assume there is some possibly unreachable state t in $\mathcal{K}_1$ with $t \models a$. (If there is no such state, then it can just be added.)

Introduce actions α, β, γ that are not in $\mathcal{K}_1$. Construct $\mathcal{K}_2$ as follows: as given in the hint, add a self-loop labeled with β to every state in $\mathcal{K}_1$. We also add a state *trap* which has a self-loop labeled with γ and a transition from each state in $\mathcal{K}_1$ where a is true to *trap* and label the transition with α.

We choose the ample sets for $\mathcal{K}_2$ given by *red* such that $red(s_0) = \{\lambda\}$ and $red(s) = en(s)$ for all other s in $\mathcal{K}_2$.

The first observation is that in $\mathcal{K}_2$, action β is independent of all actions in $\mathrm{Act}(\mathcal{K}_1)$ and is dependent on α.

We show that $\mathcal{K}_1 \models_\exists \mathsf{F}\, a$ if and only if the choice of *red* in $\mathcal{K}_2$ violates (C1).

1. ($\Rightarrow$) Suppose there exists t reachable from s_0 in $\mathcal{K}_1$ with $t \models a$. Then the following path exists in $\mathcal{K}_2$:
$$s_0 \to \cdots \to t \xrightarrow{\alpha} trap$$
where all transitions before $\xrightarrow{\alpha}$ come from $\mathcal{K}_1$. Since α depends on $red(s_0) = \{\beta\}$, this violates (C1).

2. Suppose (C1) is violated in $\mathcal{K}_2$. Then there exists a path in $\mathcal{K}_2$ of the form:
$$v \xrightarrow{\gamma_1} s_1 \xrightarrow{\gamma_2} \ldots \xrightarrow{\gamma_n} s_n \xrightarrow{\gamma} s'$$
where γ depends on some action in $red(v)$ and $\gamma_1, \ldots, \gamma_n \notin red(v)$. As s_0 is the only state in $\mathcal{K}_2$ where $red(s_0) \neq en(s_0)$, we must have $v = s_0$. Since $red(s_0) = \{\beta\}$ and β is independent of all actions except α, we have $\gamma = \alpha$. Thus $\mathcal{K}_2 \models_\exists \mathsf{F}\, a$. Finally, as *trap* has no outgoing transitions, s_n must be reachable from v in $\mathcal{K}_1$. Thus $\mathcal{K}_1 \models \mathsf{F}\, a$.

4 Exercise 4

1. (C0), (C2) and (C3) are trivially satisfied. (C1) is satisfied as well because a and b on one side, a and c on the other side are independant from each other.

2. $\mathsf{E}(\top\, \mathsf{U}\, (\mathsf{E}(p\, \mathsf{U}\, q) \wedge \mathsf{E}(p\, \mathsf{U}\, (\neg p \wedge \neg q))))$ cannot be satisfied if s_7 cannot be reached.

3. $red(s_0) = a$, and for $s \neq s_0$ $red(s) = en(s)$ works.

5 Exercise 5

Note: The generalized stuttering principle is treated in the PhD thesis of Jan Strejček, Masaryk University Brno, and the theorems and proofs are taken from or inspired by the material in that thesis.

We saw in the last TD that there exists a unique (0-)stutter-free word which is (0-)stutter-equivalent to any given word. We use a similar concept here. We say that α_i is *n-redundant* in α (for $n \geq 0$) if $\alpha_i = \alpha_{i+1} = \cdots = \alpha_{i+n+1}$ and there is $j > i$ with $\alpha_j \neq \alpha_i$. The *n-canonical form* of α is obtained by deleting from it all n-redundant letters. Note that two words α, β are *n-stutter-equivalent* if and only if they have the same n-canonical form.

1. Let $\alpha \in \Sigma^\omega$. By $\alpha_{\geq i}$ we denote the suffix of α starting at α_i and by $(\alpha)_n$ the n-canonical form of α. We define the function g_n as $g_n(0) = 0$ and for all i, $g_n(i+1) = g_n(i)$ if α_i is n-redundant and $g_n(i+1) = g_n(i) + 1$ otherwise. Thus for all i, $\alpha_{\geq i}$ is n-stutter-equivalent to $((\alpha)_n)_{\geq g_n(i)}$.

   We now prove the claim by induction on n. The base case, $n = 0$, is already known to be true. So assuming that the claim holds for n, then for any sequence α and any LTL formula ϕ with X-depth $n+1$, we show that $\alpha \models \phi$ iff $(\alpha)_{n+1} \models \phi$.

Let us proceed by structural induction on ϕ. The cases where ϕ is an atomic proposition, a negation, or disjunction are trivial. Let $\phi = \phi_1 \,\mathsf{U}\, \phi_2$. Then there exists some i such that $\alpha_{\geq i} \models \phi_2$ and for all $k < i$, $\alpha_{\geq k} \models \phi_1$. By the previously mentioned property of g and structural induction w.r.t. ϕ_1 and ϕ_2, this is the case if and only if $((\alpha)_{n+1})_{\geq g_{n+1}(i)} \models \phi_2$ and for all $k < i$, $((\alpha)_{n+1})_{\geq g_{n+1}(k)} \models \phi_1$, thus $(\alpha)_{n+1} \models \phi$.

The interesting case is $\phi = X\,\phi_1$. Note that $\alpha_{\geq 1}$ is n-stuttering-equivalent to $((\alpha)_{n+1})_{\geq 1}$ and that ϕ_1 has X-depth n. So by the induction hypothesis, $\alpha_{\geq 1} \models \phi_1$ iff $((\alpha)_{n+1})_{\geq 1} \models \phi_1$, from which we conclude.

2. Let $\beta := uv^m\alpha$ and $\gamma := uv^{m+1}\alpha$. We show $\beta \models \phi$ by induction on m. In fact, the base case $m = 1$ and the induction step to $m+1$ are nearly identical. In both cases, we proceed by structural induction on ϕ. If ϕ is an atomic proposition, then the proof follows from $\beta_0 = \gamma_0$. If ϕ is a negation or disjunction, the proof follows trivially from the structural induction hypothesis. So let $\phi = \phi_1 \,\mathsf{U}\, \phi_2$. We first make two observations:

   Observation (i). For $j = 1, 2$ and $i < |uv|$, we have $\beta_{\geq i} \models \phi_j$ iff $\gamma_{\geq i} \models \phi_j$. Indeed, if $m = 1$, then this follows from the fact that ϕ_j can only be a boolean combination of atomic properties and from $\beta_i = \gamma_i$. If $m > 1$, then it follows from the induction hypothesis for $m-1$, considering that ϕ_j has U-depth $m-1$ and there exists u' such that $\beta_{\geq i} = u'v^{m-1}\alpha$ and $\gamma_{\geq i} = u'v^m\alpha$.

   Observation (ii). For $i \geq |uv|$, $\gamma_{\geq i} = \beta_{\geq i-|v|}$.

   Now suppose that $\beta \models \phi$. Then there exists i such that $\beta_{\geq i} \models \phi_2$ and for all $k < i$, $\beta_{\geq k} \models \phi_1$. Either $i < |uv|$, then $\gamma \models \phi$ follows automatically from (i). Otherwise let $i' = i + |v|$. Due to (ii) we have $\gamma_{\geq i'} \models \phi_2$. For all $k' < |uv|$ we have $\gamma_{\geq k'} \models \phi_1$ due to (i). For all $|uv| \leq k' < i'$ we have $\gamma_{\geq k'} \models \phi_1$ due to (ii). Therefore also in this case $\gamma \models \phi$ holds.

   The other direction, $\gamma \models \phi$ implies $\beta \models \phi$, follows in analogous fashion, by subtracting $|v|$ from the index.

3. Assume that the language is expressible in some LTL formula ϕ. Then let n be the X-depth of ϕ. According to (a), the language must be n-stutter-closed. That, however, is not true because $a^{2n+1}ba^\omega$ is in the language but the n-stutter-equivalent word $a^{2n+2}ba^\omega$ is not.