TD 5: Büchi Automata and LTL Model-Checking

Exercise 1 (Synchronous Büchi Transducers)**.** Give unambigous synchronous Büchi transducers for the following formulæ:

1. $\mathsf{SF}\, q$
2. $\mathsf{SG}\, q$
3. $\mathsf{G}(p \to \mathsf{F}\, q)$

Exercise 2 (Closure by Complementation)**.** The purpose of this exercise is to prove that $\mathrm{Rec}(\Sigma^\omega)$ is closed under complement. We consider for this a Büchi automaton $\mathcal{A} = (Q, \Sigma, T, I, F)$, and want to prove that its complement language $\overline{L(\mathcal{A})}$ is in $\mathrm{Rec}(\Sigma^\omega)$.

We write $q \xrightarrow{u} q'$ for q, q' in Q and $u = a_1 \cdots a_n$ in Σ^* if there exists a sequence of states $q_0, \ldots, q_n$ such that $q_0 = q$, $q_n = q'$ and for all $0 \leq i < n$, (q_i, a_{i+1}, q_{i+1}) is in T. We write in the same way $q \xrightarrow{u}_F q'$ if furthermore at least one of the states $q_0, \ldots, q_n$ belongs to F.

We define the *congruence* $\sim_\mathcal{A}$ over Σ^* by

$$u \sim_\mathcal{A} v \text{ iff } \forall q, q' \in Q,\ (q \xrightarrow{u} q' \Leftrightarrow q \xrightarrow{v} q') \text{ and } (q \xrightarrow{u}_F q' \Leftrightarrow q \xrightarrow{v}_F q')\ .$$

1. Show that $\sim_\mathcal{A}$ has finitely many congruence classes $[u]$, for u in Σ^*.
2. Show that each $[u]$ for u in Σ^* is in $\mathrm{Rec}(\Sigma^*)$, i.e. is a regular language of finite words.
3. Consider the language $K(L)$ for $L \subseteq \Sigma^\omega$

$$K(L) = \bigcup_{\substack{u,v \in \Sigma^* \\ [u][v]^\omega \cap L \neq \emptyset}} [u][v]^\omega$$

   Show that $K(L)$ is in $\mathrm{Rec}(\Sigma^\omega)$ for any $L \subseteq \Sigma^\omega$.

4. Show that $K(L(\mathcal{A})) \subseteq L(\mathcal{A})$ and $K(\overline{L(A)}) \subseteq \overline{L(\mathcal{A})}$.
5. Prove that for any infinite word σ in Σ^ω there exist u and v in Σ^* such that σ belongs to $[u][v]^\omega$. The following theorem might come in handy when applied to couples of positions (i, j) inside σ:

   Theorem 1 (Ramsey, infinite version)**.** *Let $E = \{(i,j) \in \mathbb{N}^2 \mid i < j\}$, and $c : E \to \{1, \ldots, k\}$ a k-coloring of E. There exists an infinite set $A \subseteq \mathbb{N}$ and a color $i \in \{1, \ldots, k\}$ such that for all $(n, m) \in A^2$ with $n < m$, $c(n, m) = i$.*

6. Conclude.

Exercise 3 (Model Checking a Path)**.** Consider the time flow $(\mathbb{N}, <)$. We want to verify a model which is an ultimately periodic word $w = uv^\omega$ with u in Σ^* and v in Σ^+, where $\Sigma = 2^{\mathrm{AP}}$.

Give an algorithm for checking whether $w, 0 \models \varphi$ holds, where φ is a LTL$(\mathsf{AP}, \mathsf{X}, \mathsf{U})$ formula, in time bounded by $O(|uv| \cdot |\varphi|)$. *Hint: reduce this to a CTL model-checking problem.*

Exercise 4 (Complexity of LTL(F))**.** Fix $\Sigma = 2^{\mathrm{AP}}$ and let $w = w_0 w_1 w_2 \cdots$ be an infinite word in Σ^ω. Let

$$\mathsf{alph}(w) = \{a \in \Sigma \mid |w|_a \geq 1\}$$

be the set of letters appearing in w and

$$\mathsf{inf}(w) = \{a \in \Sigma \mid |w|_a = \infty\}$$

be the set of letters appearing infinitely often in w. We consider *decompositions* $u \cdot v$ in $\Sigma^* \times \Sigma^\infty$ (where $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$) such that $\mathsf{alph}(v) = \mathsf{inf}(v)$; this definition enforces that either $v = \varepsilon$ or v is in Σ^ω. Given an infinite word w there exists a unique decomposition $w = u \cdot v$ with $u \in \Sigma^*$, $v \in (\mathsf{inf}(w))^\omega$, and u of minimal length.

Define the *size* $\|u \cdot v\|$ of a decomposition pair $u \cdot v$ as $\|u \cdot v\| = |u| + |\mathsf{inf}(v)|$. Our goal is, for any satisfiable φ in LTL(F), to prove the existence of a model $w = u \cdot v$ with $\|u \cdot v\| \leq |\varphi|$.

1. Consider an infinite word w decomposed as $u \cdot v$ and two indices $i, j \geq |u|$ with $w_i = w_j$; show that for all φ in LTL(F), $w, i \models \varphi$ iff $w, j \models \varphi$.

2. Let w, w' be two infinite words decomposed as $u \cdot v$ and $u \cdot v'$ (thus with a shared initial prefix) with $\mathsf{inf}(w) = \mathsf{inf}(w')$ and $w_0 = w'_0$ (necessary in case $u = \varepsilon$). Show that for all φ in LTL(F), $w, 0 \models \varphi$ iff $w', 0 \models \varphi$.

Let $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$. For a word $\sigma \in \Sigma^\infty$, denote by $\mathbb{T}_\sigma$ the set of positions of σ: $\mathbb{T}_\sigma = \mathbb{N}$ if $\sigma \in \Sigma^\omega$, and $\mathbb{T}_\sigma = \{0, \ldots, |\sigma| - 1\}$ if $\sigma \in \Sigma^*$.

Let σ, σ' be words in Σ^∞; σ' is a *subword* of σ, noted $\sigma' \preceq \sigma$, if there exists a monotone injection $f_{\sigma'} : \mathbb{T}_{\sigma'} \to \mathbb{T}_\sigma$ s.t. for all $i \in \mathbb{T}_{\sigma'}$, $\sigma'_i = \sigma_{f_{\sigma'}(i)}$. We denote by $R_{\sigma'} = f_{\sigma'}(\mathbb{T}_{\sigma'})$ the set of *preserved positions*. Note that for every $R \subseteq \mathbb{T}_\sigma$, there exists a unique $\sigma' \preceq \sigma$ and $f_{\sigma'}$ such that $R_{\sigma'} = R$.

Given a decomposition $u \cdot v$, a *subdecomposition* $u' \cdot v'$ is a decomposition such that $u' \preceq u$ and $v' \preceq v$ (by definition this enforces $\mathsf{alph}(v') = \mathsf{inf}(v')$). We write $R_{u' \cdot v'}$ for $R_{u'} \cup \{|u'| + i \mid i \in R_{v'}\}$; this is compatible with the notion of subwords on the words $w' = u' \cdot v'$ and $w = u \cdot v$.

3. Given two subdecompositions $u_1 \cdot v_1$ and $u_2 \cdot v_2$ of some decomposition $u \cdot v$, show that $u' \cdot v'$ with $R_{u'} = R_{u_1} \cup R_{u_2}$ and $R_{v'} = R_{v_1} \cup R_{v_2}$ is a subdecomposition of $u \cdot v$ that verifies $\|u' \cdot v'\| \leq \|u_1 \cdot v_1\| + \|u_2 \cdot v_2\|$.

4. Consider a formula φ in LTL(F). We denote by $m(\varphi)$ the number of F modalities in φ. Show that φ can be transformed into an equivalent formula $\psi \in \text{NNF}(\mathsf{F}, \mathsf{G})$ such that $m(\psi) \leq m(\varphi)$, where NNF(F, G) is the set of formulæ in negative normal form (where negations only occur in front of atomic fomulæ) using only F and G modalities:
$$\psi ::= p \mid \neg p \mid \psi \vee \psi \mid \psi \wedge \psi \mid \mathsf{F}\,\psi \mid \mathsf{G}\,\psi$$

5. Let w be an infinite word in Σ^ω decomposed as $w = u \cdot v$ and let ψ in NNF(F, G). Show by induction on ψ that, for all subdecompositions $u' \cdot v'$ of $u \cdot v$ s.t. for all $i \in R_{u' \cdot v'}$, $w, i \models \psi$, there exists a subdecomposition $\sigma \cdot \tau$ of $u \cdot v$ of size $\|\sigma \cdot \tau\| \leq m(\psi)$ such that, for all subdecompositions $\sigma' \cdot \tau'$ of $u \cdot v$ for which $\sigma \cdot \tau$ is a sub-subdecomposition, and for all $i \in R_{u' \cdot v'} \cap R_{\sigma' \cdot \tau'}$, $\sigma' \cdot \tau', f^{-1}_{\sigma' \cdot \tau'}(i) \models \psi$.

6. Show that for all satisfiable φ in LTL(F), there exists $w = u \cdot v$ with $\|u \cdot v\| \leq |\varphi|$ such that $w, 0 \models \varphi$.

7. Show that SAT(LTL(F)) and $\mathsf{MC}^\exists$(LTL(F)) are in NP.

8. Show that SAT(LTL(F)) and $\mathsf{MC}^\exists$(LTL(F)) are NP-hard.