TD 4: Complexity of LTL Fragments

Exercises 1–3 (marked with an asterisk in the margin) are to be prepared at home before the session.

1 LTL(X)

Exercise 1 (Model Checking a Path). We want to verify a model with a single run \( w \), (\( \ast \)) which is an ultimately periodic word \( uv^\omega \) with \( u \) in \( \Sigma^* \) and \( v \) in \( \Sigma^+ \).

Give an algorithm for checking whether \( w,0 \models \varphi \) holds, where \( \varphi \) is a LTL(X,U) formula, in time bounded by \( O(|uv| \cdot |\varphi|) \).

Exercise 2 (Complexity of LTL(X)). We want to show that LTL(X) existential model (\( \ast \)) checking is NP-complete (instead of PSPACE-complete for the full LTL(X,U)).

1. Show that MC\(^3\)(X) is in NP.
2. Reduce 3SAT to MC\(^3\)(X) in order to prove NP-hardness.

2 LTL(U)

Exercise 3 (Stuttering and LTL(U)). In the context of a word \( \sigma \) in \( \Sigma^\omega \), stuttering (\( \ast \)) denotes the existence of consecutive symbols, like \( aaaa \) and \( bb \) in \( baaaabb \). Concrete systems tend to stutter, and thus some argue that verification properties should be stutter invariant.

A stuttering function \( f : \mathbb{N} \to \mathbb{N}_+ \) from the positive integers to the strictly positive integers. Let \( \sigma = a_0a_1 \cdots \) be an infinite word of \( \Sigma^\omega \) and \( f \) a stuttering function, we denote by \( \sigma[f] \) the infinite word \( a_0^{f(0)} a_1^{f(1)} \cdots \), i.e. where the \( i \)-th symbol of \( \sigma \) is repeated \( f(i) \) times. A language \( L \subseteq \Sigma^\omega \) is stutter invariant if, for all words \( \sigma \) in \( \Sigma^\omega \) and all stuttering functions \( f \),

\[
\sigma \in L \text{ iff } \sigma[f] \in L.
\]

1. Prove that if \( \varphi \) is a LTL(U) formula, then \( L(\varphi) \) is stutter-invariant.
2. A word \( \sigma = a_0a_1 \cdots \) in \( \Sigma^\omega \) is stutter-free if, for all \( i \) in \( \mathbb{N} \), either \( a_i \neq a_{i+1} \), or \( a_i = a_j \) for all \( j \geq i \). We note sf(L) for the set of stutter-free words in a language \( L \).

Show that, if \( L \) and \( L' \) are two stutter invariant languages, then \( \text{sf}(L) = \text{sf}(L') \) iff \( L = L' \).
3. Let \( \varphi \) be a LTL(X,U) formula such that \( L(\varphi) \) is stutter invariant. Construct inductively a formula \( \tau(\varphi) \) of LTL(U) such that \( \text{sf}(L(\varphi)) = \text{sf}(L(\tau(\varphi))) \), and thus such that \( L(\varphi) = L(\tau(\varphi)) \) according to the previous question. What is the size of \( \tau(\varphi) \) (there exists a solution of size \( O(|\varphi| \cdot 2^{|\varphi|}) \))?
Exercise 4 (Complexity of LTL($U$)). We want to prove that the model checking and satisfiability problems for LTL($U$) formulae are both PSPACE-complete.

1. Prove that MC$^\exists$(X,$U$) can be reduced to MC$^\exists$(U): given an instance $(M,\varphi)$ of MC$^\exists$(X,$U$), construct a stutter-free Kripke structure $M'$ and an LTL($U$) formula $\tau'(\varphi)$. Beware: the $\tau$ construction of the previous exercise does not yield a polynomial reduction!

2. Show that MC$^\exists$(X,$U$) can be reduced to SAT(U).

3  LTL(F)

Exercise 5 (Small Model Property for LTL(F)). Fix $\Sigma = 2^{\text{AP}}$ and let $w = w_0w_1w_2\cdots$ be an infinite word in $\Sigma^\omega$. Let

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

be the set of letters appearing in $w$ and

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

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

Define the size $|u \cdot v|$ of a decomposition pair $u \cdot v$ as $|u \cdot v| = |u| + |\inf(v)|$. Our goal is, for any satisfiable $\varphi$ 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 $\varphi$ 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 $\inf(w) = \inf(w')$ and $w_0 = w'_0$ (necessary in case $u = \varepsilon$). Show that for all $\varphi$ in LTL($F$), $w, 0 \models \varphi$ iff $w', 0 \models \varphi$.

Let $\sigma, \sigma'$ be words in $\Sigma^\infty$; $\sigma'$ is a subsequence of $\sigma$, noted $\sigma' \preceq \sigma$, if there exists a monotone injection $f_{\sigma'}: \{0, \ldots, |\sigma'| - 1\} \rightarrow \{0, \ldots, |\sigma| - 1\}$ s.t. for all $i \in \{0, \ldots, |\sigma'| - 1\}$, $\sigma'_i = \sigma_{f_{\sigma'}(i)}$. Alternatively, given a subset $R_{\sigma'}$ of $\{0, \ldots, |\sigma| - 1\}$ with cardinal $|R_{\sigma'}| = |\sigma'|$, define $f_{\sigma'}$ as the unique monotone bijection mapping $\{0, \ldots, |\sigma'| - 1\}$ to $R_{\sigma'}$. If $\sigma \neq \varepsilon$ and $\sigma' \preceq \sigma$, define the sequence $s(\sigma') \preceq \sigma$ by $R_{s(\sigma')}(i) = \{0\} \cup R_{\sigma'}$.

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 $\text{alph}(v') = \inf(v')$). We write $R_{u',v'}$ for $R_{u'} \cup \{|u'| + i \mid i \in R_{v'}\}$; this is compatible with the notion of subsequence on the words $w' = u' \cdot v'$ and $w = u \cdot v$. 

2
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 $u \cdot v$ and s.t. $\|u' \cdot v'\| \leq \|u_1 \cdot v_1\| + \|u_2 \cdot v_2\|$.

Consider a formula $\varphi$ in LTL($F$). By the standard “push negations using dualities” argument, it can be transformed into an equivalent formula $\psi$ in negative normal form, where negations only occur in front of atomic formulae, using only $F$ and $G$ modalities, i.e. $\psi$ is in NNF($F, G$). Let us note $m(\varphi)$ the number of $F$ modalities in a LTL formula $\varphi$; we have $m(\psi) \leq m(\varphi) \leq |\varphi|$.

4. Let $w$ be an infinite word in $\Sigma^\omega$ decomposed as $w = u \cdot v$ and let $\psi$ in NNF($F, G$).
   Show by induction on $\psi$ that, if there exists a subdecomposition $u' \cdot v'$ of $u \cdot v$, s.t. for all $i \in R_{u' \cdot v'}$, $w, i \models \psi$, then 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 subdecomposition, and for all $i \in R_{\sigma' \cdot \tau'} \cap R_{\sigma \cdot \tau}$, $i \models \psi$.

5. Conclude.

Exercise 6 (Complexity of LTL($F$)).

1. Show that $MC_3^\exists(F)$ and $SAT(F)$ are NPTIME-hard.

2. Show that $MC_3^\exists(F)$ and $SAT(F)$ are in NPTIME.