TD 6: LTL Model-Checking

Exercise 1 (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 2 (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 if for all satisfiabel 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)) is in NP.

Exercise 3 (Stuttering and LTL(U))**.** In the time flow $(\mathbb{N}, <)$, i.e. when working with words σ in Σ^ω, *stuttering* 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* $f : \mathbb{N} \to \mathbb{N}_{>0}$ from the positive integers to the positive integers. Let $\sigma = a_0 a_1 \cdots$ be an infinite word of Σ^ω 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 σ is repeated $f(i)$ times. A language $L \subseteq \Sigma^\omega$ is *stutter invariant* if, for all words σ in Σ^ω and all stuttering functions f,
$$\sigma \in L \text{ iff } \sigma[f] \in L\ .$$

1. Prove that if φ is a TL(AP, U) formula, then $L(\varphi)$ is stutter-invariant.

2. A word $\sigma = a_0 a_1 \cdots$ in Σ^ω 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 sf$(L) = $ sf(L') iff $L = L'$.

3. Let φ be a TL(AP, X, U) formula such that $L(\varphi)$ is stutter invariant. Construct inductively a formula $\tau(\varphi)$ of TL(AP, U) such that sf$(L(\varphi)) = $ 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) formulæ are both PSPACE-complete.

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

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