TD 3: Model-Checking and Büchi Automata

1 CTL Model Checking

Exercise 1 (Fair CTL)**.** We consider *strong* fairness constraints, which are conjunctions of formulæ of form

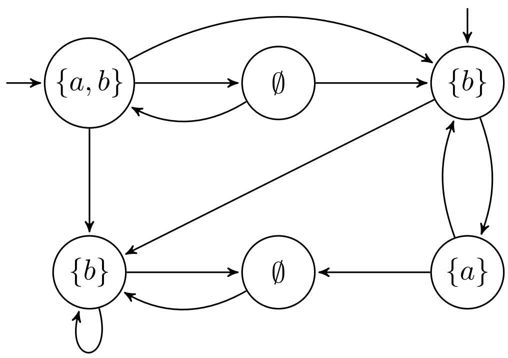
$$\mathsf{GF}\psi_1 \Rightarrow \mathsf{GF}\psi_2\ .$$

We want to check whether the following Kripke structure fairly verifies

$$\varphi = \mathsf{A}_e\mathsf{G}\,\mathsf{A}_e\mathsf{F}\,a$$

under the fairness requirement e defined by

$$\begin{aligned}\psi_1 &= b \wedge \neg a\\ \psi_2 &= \mathsf{E}(b\,\mathsf{U}\,(a \wedge \neg b))\\ e &= \mathsf{GF}\,\psi_1 \Rightarrow \mathsf{GF}\,\psi_2\ .\end{aligned}$$



1. Compute $[\![\psi_1]\!]$ and $[\![\psi_2]\!]$.
2. Compute $[\![\mathsf{E}_e\,\mathsf{G}\,\top]\!]$.
3. Compute $[\![\varphi]\!]$.

Exercise 2 (Horn Satisfiability)**.** Given a finite total Kripke structure $M = (S, T, I, \mathrm{AP}, \ell)$ and a "smallest fixed-point" CTL formula φ over AP, we want to reduce the model-checking problem $M, s \models \varphi$ with $s \in S$ to a Horn satisfiability instance, where smallest fixed-point CTL formulæ are defined by the syntax:

$$\varphi ::= \top \mid p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathsf{EX}\,\varphi \mid \mathsf{E}(\varphi\,\mathsf{U}\,\varphi) \mid \mathsf{AF}\,\varphi$$

1. Reduce the model-checking problem $M, s \models \varphi$ where φ is a smallest fixed-point CTL formula and s is a state in S to a Horn satisfiability instance.

2. What complexity can you obtain through to this reduction for *full* CTL model-checking?

Exercise 3 (Even and Odd Positions)**.** We saw in Exercise 2 of TD 2 that the set $(\{p\}\Sigma)^\omega$ is not expressible in LTL$(\{p\}, \mathsf{X}, \mathsf{U})$ over $(\mathbb{N}, <)$. We define two new temporal modalities U_0 and U_1 to fill this void:

$$w, i \models \varphi \,\mathsf{U}_b\, \psi \text{ if } \exists k \geq i, (k - i) \equiv b \bmod 2 \text{ and } w, k \models \psi \text{ and } \forall j . i \leq j < k \rightarrow w, j \models \varphi$$

for $b = 0$ (resp. 1), i.e. restrictions of U to even (resp. odd) choices of positions.

1. Show that $(\{p\}\Sigma)^\omega$ can be expressed in TL$(\{p\}, \mathsf{U}_0)$.

2. Complete the reduction from the previous exercise to handle the new modality U_0 in CTL model-checking. What complexity can you derive on the model-checking problem for CTL when U_0 is allowed?

Exercise 4 (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$(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ formula, in time bounded by $O(|uv| \cdot |\varphi|)$.

2 Büchi Automata

Recall from the course that a language L of infinite words in Σ^ω is *recognizable* iff there exists a Büchi automaton $\mathcal{B}$ with $L = L(\mathcal{B})$.

Exercise 5 (Generalized Acceptance Condition)**.** A *generalized* Büchi automaton $\mathcal{B} = (Q, \Sigma, I, T, (F_i)_{0 \leq i < n})$ has a finite set of accepting sets F_i. An infinite run σ in Q^ω satisfies this generalized acceptance condition if

$$\bigwedge_{0 \leq i < n} \mathsf{Inf}(\sigma) \cap F_i \neq \emptyset \,.$$

i.e. if each set F_i is visited infinitely often.

Show that for any generalized Büchi automaton, one can construct an equivalent Büchi automaton.

Exercise 6 (Basic Closure Properties of Recognizable Languages)**.** Show that $\mathsf{Rec}(\Sigma^\omega)$ is closed under

1. finite union, and
2. finite intersection.

Exercise 7 (Prophetic Automata)**.** A Büchi automaton $\mathcal{B} = (Q, \Sigma, I, T, F)$ over an alphabet Σ is *prophetic* if any infinite string w in Σ^ω has exactly one final (but not necessarily initial) run in $\mathcal{B}$.

1. The *residual language* $L(\mathcal{B}_q)$ of a state q in Q is the language accepted by $\mathcal{B}_q = (Q, \Sigma, \{q\}, T, F)$, i.e. the set of words with a final run in $\mathcal{B}$ that starts with state q.

   Show that $\mathcal{B}$ is prophetic if and only if Σ^ω can be partitioned as $\biguplus_{q \in Q} L(\mathcal{B}_q)$.

2. An automaton $\mathcal{B}$ is *trim* if every $L(\mathcal{B}_q) \neq \emptyset$ for every q in Q. It is *co-deterministic* if, for every state q' in Q and a in Σ, there is at most one state q in Q such that (q, a, q') belongs to T. It is *co-complete* if, for every state q' in Q and a in Σ, there is at least one state q in Q such that (q, a, q') belongs to T.

   Show that, if $\mathcal{B}$ is trim and prophetic, then $\mathcal{B}$ is co-deterministic and co-complete.

3. Let $\Sigma = \{a, b\}$. Construct a prophetic automaton for the language $(a\Sigma)^\omega$.

Exercise 8 (Ultimately Periodic Words)**.** An *ultimately periodic word* over Σ is a word of form $u \cdot v^\omega$ with u in Σ^* and v in Σ^+.

Prove that any nonempty recognizable language in $\mathsf{Rec}(\Sigma^\omega)$ contains an ultimately periodic word.

Exercise 9 (Rational Languages)**.** A *rational language* L of infinite words over Σ is a finite union

$$L = \bigcup X \cdot Y^\omega$$

where X is in $\mathsf{Rat}(\Sigma^*)$ and Y in $\mathsf{Rat}(\Sigma^+)$. We denote the set of *rational* languages of infinite words by $\mathsf{Rat}(\Sigma^\omega)$.

Show that $\mathsf{Rec}(\Sigma^\omega) = \mathsf{Rat}(\Sigma^\omega)$.

Exercise 10 (Deterministic Büchi Automata)**.** A Büchi automaton is *deterministic* if $|I| \leq 1$, and for each state q in Q and symbol a in Σ, $|\{(q, a, q') \in T \mid q' \in Q\}| \leq 1$.

1. Give a nondeterministic Büchi automaton for the language in $\{a, b\}^\omega$ described by the expression $(a + b)^* a^\omega$.

2. Show that there does not exist any deterministic Büchi automaton for this language.

3. Let $\mathcal{A} = (Q, \Sigma, q_0, T, F)$ be a finite deterministic automaton that recognizes the language of finite words $L \subseteq \Sigma^*$. We can also interpret $\mathcal{A}$ as a deterministic Büchi automaton with a language $L' \subseteq \Sigma^\omega$; our goal here is to relate the languages of finite and infinite words defined by $\mathcal{A}$.

   Let the *limit* of a language $L \subseteq \Sigma^*$ be

   $$\overrightarrow{L} = \{w \in \Sigma^\omega \mid w \text{ has infinitely many prefixes in } L\} .$$

   Characterize the language L' of infinite words of $\mathcal{A}$ in terms of its language of finite words L and of the limit operation.

Exercise 11 (Closure by Complementation)**.** The purpose of this exercise is to prove that $\text{Rec}(\Sigma^\omega)$ is closed under complement. We consider for this a Büchi automaton $A = (Q, \Sigma, T, I, F)$, and want to prove that its complement language $\overline{L(A)}$ is in $\text{Rec}(\Sigma^\omega)$.

We note $q \xrightarrow{u} q'$ 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 note 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* $\sim_A$ over Σ^* by

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

1. Show that $\sim_A$ has finitely many congruence classes $[u]$, for u in Σ^*.

2. Show that each $[u]$ for u in Σ^* is in $\text{Rec}(\Sigma^*)$, i.e. is a regular language of finite words.

3. Consider the language $K(L)$ for $L \subseteq \Sigma^\omega$

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

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

4. Show that $K(L(A)) \subseteq L(A)$ and $K(\overline{L(A)}) \subseteq \overline{L(A)}$.

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 X be some countably infinite set, n an integer, and $c : X^{(n)} \to \{1, \ldots, k\}$ a k-*coloring *of the n-tuples of X. Then there exists some infinite* monochromatic *subset M of X such that all the n-tuples of M have the same image by c.*

6. Conclude.