TD 3: Büchi Automata

Exercises 1–5 (marked with an asterisk in the margin) are to be prepared at home *before* the session.

1 LTL and Büchi Automata

Exercise 1 (Specification)**.** We would like to verify the properties of a boolean circuit with input x, output y, and two registers r_1 and r_2. We define accordingly $\mathrm{AP} = \{x, y, r_1, r_2\}$ as our set of atomic propositions, and model check infinite runs $\sigma = s_0 s_1 s_2 \cdots$ from $(2^{\mathrm{AP}})^\omega$. (∗)

Provide a Büchi automaton for each of the following properties:

1. "it is impossible to get two consecutive 1 as output"
2. "each time the input is 1, at most two ticks later the output will be 1"
3. "each time the input is 1, the register contents remains the same over the next tick"
4. "register r_1 is infinitely often 1"

Note that there might be several, non-equivalent formal specifications matching these informal descriptions—that's the whole point of writing specifications!

Exercise 2 (Büchi Automaton Construction)**.** Use the LTL to Büchi algorithm seen during the last lecture to construct another Büchi automaton for the LTL formula $\varphi = \mathsf{G}(\neg p \vee \neg \mathsf{X} p)$. (∗)

2 Recognizable Languages

Recall from the course that a language of infinite words in Σ^ω is *recognizable* iff there exists a Büchi automaton for it.

Exercise 3 (Basic Closure Properties)**.** Show that $\mathsf{Rec}(\Sigma^\omega)$ is closed under (∗)

1. finite union, and
2. finite intersection.

Exercise 4 (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 5 (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 6 (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 $A = (Q, \Sigma, T, q_0, F)$ 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

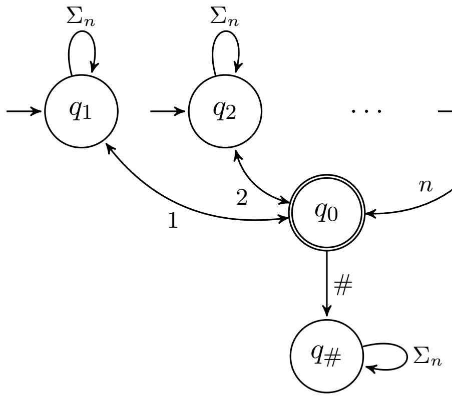
   $$\overrightarrow{L} = \{w \in \Sigma^\omega \mid w \text{ has infinitely many prefixes in } L\} .$$

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

3 Büchi Complementation

Exercise 7 (Lower Bound on Büchi Complementation)**.** The best known lower bound on the size of a Büchi automaton for the complement $\overline{L}$ of a language, compared to that of the Büchi automaton for L, is $\Omega\big((0.76\,n)^n\big)$ [Yan, LMCS 4(1:5), 2008], with a matching upper bound modulo a quadratic factor [Schewe, STACS 2009]. We see in this exercise an easier to obtain lower bound of $\Omega(n!)$.

Let $\Sigma_n = \{\#, 1, 2, \ldots, n\}$ be our alphabet, and L_n the language of the following Büchi automaton (note the two-ways transitions):



1. Let $a_1 \cdots a_k$ be a fixed, finite word in $\{1, \dots, n\}^*$. Prove that any infinite word in

$$(\Sigma_n^* a_1 a_2 \Sigma_n^* a_2 a_3 \Sigma_n^* \cdots \Sigma_n^* a_{k-1} a_k \Sigma_n^* a_k a_1)^\omega$$

is also a word of L_n.

2. Let $(i_1, \dots, i_n)$ be a permutation of $\{1, \dots, n\}$. Show that the infinite word

$$(i_1 \cdots i_n \#)^\omega$$

is not in L_n.

3. Consider two different permutations $(i_1, \dots, i_n)$ and $(j_1, \dots, j_n)$ of $\{1, \dots, n\}$. As shown in the previous question, the two infinite words $\rho = (i_1 \cdots i_n \#)^\omega$ and $\sigma = (j_1 \cdots j_n \#)^\omega$ are in $\overline{L_n}$.

   Suppose that $\mathcal{B}$ is a Büchi automaton that recognizes $\overline{L_n}$; show that if ρ eventually loops forever in a subset R of the states of $\mathcal{B}$, and σ does the same in a subset S, then R and S are disjoint sets.

4. Conclude.

Exercise 8 (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 $A = (Q, \Sigma, T, I, F)$, and want to prove that its complement language $\overline{L(A)}$ is in $\mathrm{Rec}(\Sigma^\omega)$.

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 $q_0, \dots, q_n$ such that $q_0 = q$, $q_n = q'$ and for all $0 \le i < n$, (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 $q_0, \dots, q_n$ belongs to F.

We define a *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 $\mathrm{Rec}(\Sigma^*)$, i.e. is a regular language of finite words.

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

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

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