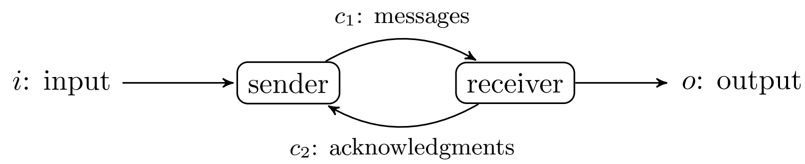
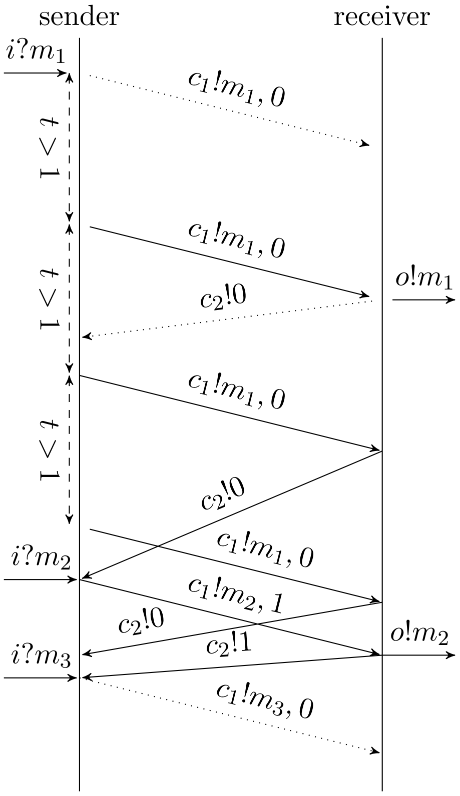
TD 2

1 Models

Exercise 1 (Alternating Bit Protocol)**.** The alternating bit protocol allows to exchange messages over a lossy channel, and to ensure that no messages are lost. The protocol employs two processes, a *sender* and a *receiver*, that communicate through two lossy channels c_1 and c_2 as depicted below:



The gist of the protocol is that both the sender and the receiver will retransmit data over the lossy channels, until they receive proof that at least one of their messages has gone through. For this, an *alternating bit* is attached to all their communications, and is changed whenever the processes know that their previous message has been received. Here is an example of message exchange between the processes:

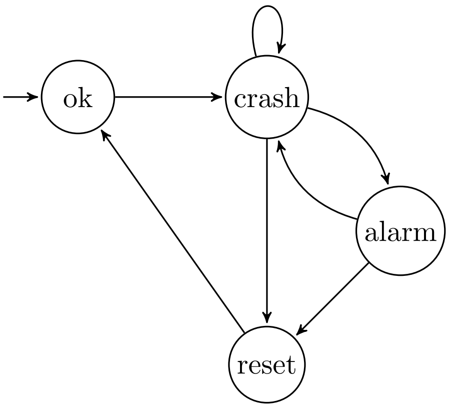


Lost messages are represented with dotted arrows, and we endow the sender with a timer t that triggers resending the message if the acknowledgment with the appropriate bit value has not been received.

1. Propose two models, one for the sender and one for the receiver.
2. Label some of your states with the atomic propositions sent_1, sent_2, rec_1, and rec_2. How can you express the following fairness constraints on the two channels: "if infinitely many messages are sent, then infinitely many are received"?
3. Let $m_1, \ldots, m_n$ be the sequence of messages to send. How can one specify that exactly the same sequence will be received, in the same order, and without duplicates?

2 LTL with Past

Exercise 2 (Specifying with Past)**.** Consider the following alarm system:



Provide LTL formulæ with and without past modalities for the following properties:

1. "Whenever the alarm rings, there has been a crash immediately before."
2. "Whenever the alarm rings, there has been a crash some time before, and no reset since."

Exercise 3 (History Variables)**.** One means of getting rid of past modalities is to tweak both the model and the formula, by adding *history variables* to the model and by replacing the past subformulæ by atomic propositions on these variables. For instance, a subformula $\mathsf{Y}\varphi$ will be replaced by a variable $h_{\mathsf{Y}\varphi}$ in the specification, and the model will update this variable according to whether or not φ holds in the previous state.

1. Apply this technique to the specification and model of the previous exercise.

2. What is the cost of the model transformation?

Exercise 4 (Succinctness of Past Formulæ)**.** Let $\mathrm{AP}_{n+1} = \{p_0, \ldots, p_n\} = \mathrm{AP}_n \cup \{p_n\}$ be a set of atomic proositions, defining the alphabet $\Sigma_{n+1} = 2^{\mathrm{AP}_{n+1}}$. We want to show the existence of an $O(n)$-sized LTL formula with past such that any equivalent pure future LTL formula is of size $\Omega(2^n)$.

First consider the following LTL formula of exponential size:

$$\bigwedge_{S\subseteq \mathrm{AP}_n} \left(\begin{aligned} &(\bigwedge_{p_i\in S} p_i \wedge \bigwedge_{p_j\notin S} \neg p_j \wedge p_n) \Rightarrow \mathsf{G}((\bigwedge_{p_i\in S} p_i \wedge \bigwedge_{p_j\notin S} \neg p_j) \Rightarrow p_n) \\ \wedge &(\bigwedge_{p_i\in S} p_i \wedge \bigwedge_{p_j\notin S} \neg p_j \wedge \neg p_n) \Rightarrow \mathsf{G}((\bigwedge_{p_i\in S} p_i \wedge \bigwedge_{p_j\notin S} \neg p_j) \Rightarrow \neg p_n) \end{aligned} \right) \qquad (\varphi_n)$$

1. Describe which words of Σ^ω_{n+1} are the models of φ_n.

2. Can an LTL formula with past modalities check whether it is at the initial position of a word?

3. Provide an LTL formula with past ψ_n of size $O(n)$ initially equivalent to φ_n.

4. Consider the language $L_n = \{\sigma \in \Sigma^\omega_{n+1} \mid \sigma \models \mathsf{G}\varphi_n\}$. We want to prove that any generalized Büchi automaton that recognizes L_n requires at least 2^{2^n} states.

   For this we fix a permutation $a_0 \cdots a_{2^n-1}$ of the symbols in Σ_n and we consider all the different subsets $K \subseteq \{0, \ldots, 2^n - 1\}$. For each K we consider the word

   $$w_K = b_0 \cdots b_{2^n-1}$$

   in $\Sigma^{2^n}_{n+1}$, defined for each i in $\{0, \ldots, 2^n - 1\}$ by

   $$\begin{aligned} b_i &= a_i && \text{if } i \in K \\ b_i &= a_i \cup \{p_n\} && \text{otherwise.} \end{aligned}$$

   Thus K is the set of positions of w_K where p_n holds.

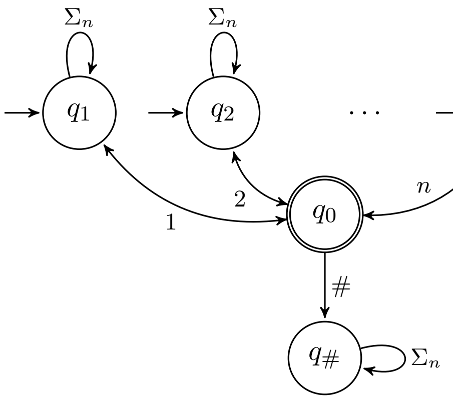
   Using the w_K for different values of K, prove that any generalized Büchi automaton for $\mathsf{G}\varphi_n$ requires at least 2^{2^n} states.

5. Conclude using the fact that any pure future LTL formula φ can be given a generalized Büchi automaton with at most $2^{|\varphi|}$ states.

3 Büchi Complementation

Exercise 5 (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 $\{1, \ldots, n\}^*$. 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 $(i_1, \ldots, i_n)$ be a permutation of $\{1, \ldots, n\}$. Show that the infinite word
$$(i_1 \cdots i_n \#)^\omega$$
is not in L_n.

3. Consider two different permutations $(i_1, \ldots, i_n)$ and $(j_1, \ldots, j_n)$ of $\{1, \ldots, n\}$. 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 6 (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 $q_0, \ldots, q_n$ 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 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.