TD 2: LTL

1 Specification

Exercise 1. 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 $\text{AP} = \{x, y, r_1, r_2\}$ as our set of atomic propositions and consider the time flow $(\mathbb{N}, <)$ where the runs of the circuit can be seen as temporal structures.

Translate the following properties (a) in $\text{TL(\text{AP})}$ and (b) in $\text{FO(<)}$:

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!—but your (a) and (b) should be equivalent.

2 LTL

Exercise 2. We fix a set $\text{AP}$ of atomic propositions including $\{p, q, r\}$ and some discrete linear time flow $(T, <)$.

1. Consider the formulæ $\varphi_1 = G(p \rightarrow Xq)$ and $\varphi_2 = G(p \rightarrow ((\neg q) R q))$.
   (a) Does $\varphi_2$ imply $\varphi_1$?
   (b) Does $\varphi_1$ imply $\varphi_2$?
2. Simplify the following formula:

$$F(((Gr \ U' p) \land (\neg q \ U' p)) \lor F(\neg p \lor F'q)).$$

Exercise 3 (Expressiveness). We fix the set $\text{AP} = \{p\}$ of atomic propositions, with an associated alphabet $\Sigma = \{\{p\}, \emptyset\}$, and consider the $(\mathbb{N}, <)$ flow of time, where temporal structures can be seen as infinite words over $\Sigma$, i.e. words in $\Sigma^\omega$.

1. Show that the following subsets of $\Sigma^\omega$ are expressible in $\text{TL(\text{AP}, U', X)}$:
(a) \( \{p\}^* \cdot \emptyset^\omega \), and
(b) \( \{p\}^n \cdot \emptyset^\omega \) for each fixed \( n \geq 0 \).

2. Is the language \( (\{p\} \cdot \emptyset)^\omega \) expressible in \( \text{TL}(\text{AP}, \mathcal{U}', X) \)?

3. Consider the infinite sequence \( \sigma_i = \{p\}^i \cdot \emptyset \cdot \{p\}^\omega \) for \( i \geq 0 \). Show by induction on TL(\( \text{AP}, \mathcal{U}', X \)) formulæ \( \varphi \) that, for all \( n \geq 0 \), if \( \varphi \) has less than \( n \) \( X \) modalities, then for all \( i, i' > n \), \( \sigma_i \models \varphi \) iff \( \sigma_{i'} \models \varphi \). (Hint: For the case of \( \mathcal{U}' \), show that \( \sigma_i \models \varphi \) iff \( \sigma_{n+1} \models \varphi \).)

4. Using the previous question, show that the set \( (\{p\} \cdot \Sigma)^\omega \) is not expressible in \( \text{TL}(\text{AP}) \) over \( (N, <) \).

3 LTL with Past

Exercise 4 (Specifying with Past). Provide TL formulæ over \( \text{AP} = \{\text{ok}, \text{crash}, \text{alarm}, \text{reset}\} \) 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 in the meantime.”

Exercise 5 (History Variables). Consider the time flow \( (N, <) \). One way of getting rid of pure past modalities is to tweak both the model and the formula, by adding history variables to the model and by replacing pure past subformulae by atomic propositions on these variables, i.e. from a pair \( \langle M, \varphi \rangle \) where \( M \) is a Kripke model and \( \varphi \) a LTL formula with past modalities, construct \( \langle M', \varphi' \rangle \) where \( M' \) is a modified version of \( M \) with extra atomic propositions, and \( \varphi' \) is a pure future LTL formula, such that \( M \models \varphi \) iff \( M' \models \varphi' \).

For instance, a subformula \( Y\psi \) will be replaced by a boolean variable \( h_{Y\psi} \) in the specification, and the model will update this variable according to whether or not \( \psi \) holds in the previous state. Two new atomic propositions are introduced, corresponding to \( h_{Y\psi} = \text{true} \) and \( h_{Y\psi} = \text{false} \).

1. Apply this technique to the specification of the previous exercise and the following alarm system:
2. What is the cost of the model transformation?

Exercise 6 (Succinctness of Past Formulae). Consider the time flow \((\mathbb{N}, <)\). Let \(\text{AP}_{n+1} = \{p_0, \ldots, p_n\} = \text{AP}_n \cup \{p_n\}\) be a set of atomic propositions, defining the alphabet \(\Sigma_{n+1} = 2^{\text{AP}_{n+1}}\). 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:

\[
\bigwedge_{S \subseteq \text{AP}_n} \left( (\bigwedge_{p_i \in S} p_i \land \bigwedge_{p_j \notin S} \lnot p_j \land p_n) \Rightarrow G((\bigwedge_{p_i \in S} p_i \land \bigwedge_{p_j \notin S} \lnot p_j) \Rightarrow p_n) \right)
\]

\(\& (\bigwedge_{p_i \in S} p_i \land \bigwedge_{p_j \notin S} \lnot p_j \land \lnot p_n) \Rightarrow G((\bigwedge_{p_i \in S} p_i \land \bigwedge_{p_j \notin S} \lnot p_j) \Rightarrow \lnot p_n) \right) \tag{\varphi_n}

1. Describe which words of \(\Sigma_{n+1}^\omega\) are the models of \(\varphi_n\).

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 \(\psi_n\) of size \(O(n)\) initially equivalent to \(\varphi_n\).

4. Consider the language \(L_n = \{\sigma \in \Sigma_{n+1}^\omega \mid \sigma \models G' \varphi_n\}\). 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 \(\Sigma_n\) 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 \(\Sigma_{n+1}^{2^n}\), defined for each \(i\) in \(\{0, \ldots, 2^n - 1\}\) by

\[
\begin{align*}
    b_i &= a_i & \text{if } i \in K \\
    b_i &= a_i \cup \{p_n\} & \text{otherwise.}
\end{align*}
\]
Thus $K$ is the set of positions of $w_K$ where $p_n$ does not hold.

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

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