TD 1: Temporal Logics

Note: As in the course, we will interpret LTL on discrete linear time. This means that every execution of a Kripke structure can be seen as an infinite word, i.e. an element of Σ^ω, where $\Sigma = 2^{AP}$.

Moreover, in the following, only future modalities are needed.

Exercise 1 (Specification)**.** We would like to verify the properties of a boolean circuit with input x, output y, and a register r. We define accordingly $\mathrm{AP} = \{x = 0, x = 1, y = 0, y = 1, r = 0, r = 1\}$ as our set of atomic propositions and consider the linear time flow $(\mathbb{N}, <)$ where the runs of the circuit can be seen as temporal structures.

Translate the following properties into LTL.

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 remain the same over the next tick"
4. "The register is infinitely often 1"

Note that there might be several, non-equivalent formal specifications matching these informal descriptions. Indeed, fixing one precise formal specification is the whole point of writing them! equivalent.

Exercise 2 (Equivalences)**.** We fix a set AP of atomic propositions including $\{p, q, r\}$.

1. For the following pairs of formulae, determine whether ϕ_1 implies ϕ_2 and vice versa.
   (a) $\phi_1 = \mathsf{F}\,\mathsf{G}(p \,\mathsf{U}\, q)$ et $\phi_2 = \mathsf{F}\,\mathsf{G}(\neg p \to q)$;
   (b) $\phi_1 = \mathsf{G}((\mathsf{F}\,p) \to q)$ et $\phi_2 = \mathsf{G}(q \,\mathsf{U}\, p)$;
2. Simplify the following formula:
$$\mathsf{F}(((\mathsf{G}\,r) \,\mathsf{U}\, p) \wedge (\neg q \,\mathsf{U}\, p)) \vee \mathsf{F}(\neg p \vee \mathsf{F}\,q)\ .$$
3. Consider the formula $\psi := (p \,\mathsf{U}\, q) \,\mathsf{U}\, r$. Show that ψ is not equivalent to $p \,\mathsf{U}\, (q \,\mathsf{U}\, r)$.
4. For ψ from the previous question, give an equivalent LTL formula ψ', where the only allowed temporal modality is U, and for any subformula $\phi \,\mathsf{U}\, \phi'$ of ψ', ϕ does not contain U.

Exercise 3 (Expressiveness)**.** We fix $\mathrm{AP} = \{p\}$, so $\Sigma = \{\emptyset, \{p\}\}$.

1. Show that the following subsets of Σ^ω are expressible in LTL.
   (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 LTL?
3. Consider the infinite sequence $\sigma_i = \{p\}^i \cdot \emptyset \cdot \{p\}^\omega$ for $i \geq 0$. Show by induction on LTL formulæ φ that, for all $n \geq 0$, if φ 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* 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 LTL.