TD 2: Temporal Logics

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 consider the linear time flow $(\mathbb{N}, <)$ where the runs of the circuit can be seen as temporal structures.

Translate the following properties (a) in $\mathrm{TL}(\mathrm{AP}, \mathsf{SU})$ and (b) in $\mathrm{FO}(\mathrm{AP}, <)$:

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. "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.

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

1. Consider the formulæ $\varphi_1 = \mathsf{G}(p \to \mathsf{X}\, q)$ and $\varphi_2 = \mathsf{G}(p \to ((\neg q)\ \mathsf{R}\ q))$
   (a) Does φ_2 imply φ_1?
   (b) Does φ_1 imply φ_2?
2. Simplify the following formula:
$$\mathsf{SF}(((\mathsf{G}\, r)\ \mathsf{U}\ p) \wedge (\neg q\ \mathsf{U}\ p)) \vee \mathsf{SF}(\neg p \vee \mathsf{F}\, q)\ .$$
3. Give a $\mathrm{TL}(\mathrm{AP}, \mathsf{U})$ formula φ equivalent to $(p\ \mathsf{U}\ q)\ \mathsf{U}\ r$ and such that for any sub-formula $\psi\ \mathsf{U}\ \psi'$ of φ, ψ is a boolean formula.

Exercise 3 (Expressiveness)**.** We fix the set $\mathrm{AP} = \{p\}$ 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 Σ, i.e. words in Σ^ω.

1. Show that the following subsets of Σ^ω are expressible in $\mathrm{LTL}(\mathrm{AP}, \mathsf{U}, \mathsf{X})$:
   (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 LTL(AP, U, X)?

3. Consider the infinite sequence $\sigma_i = \{p\}^i \cdot \emptyset \cdot \{p\}^\omega$ for $i \geq 0$. Show by induction on LTL(AP, U, X) 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(AP, U, X) over $(\mathbb{N}, <)$.

Exercise 4 (2017 Mid-term Exam)**.** The flow of time is $(\mathbb{N}, <)$, AP is the set of atomic propositions, and $\Sigma = 2^{\mathrm{AP}}$.

1. Given $p \in$ AP and $\varphi \in$ TL(AP, SU, SS), construct a formula $\widetilde{\varphi} \in$ TL(AP, SU, SS) such that

$$\forall u \in \Sigma_{\neg p}^* \Sigma_p,\ \forall v \in \Sigma^\omega,\ \forall i \geq 0 : \qquad v, i \models \varphi \quad \text{iff} \quad uv, |u| + i \models \widetilde{\varphi}\,.$$

2. Given $p \in$ AP and $\varphi \in$ TL(AP, SU, SS), construct a formula $\overline{\varphi} \in$ TL(AP, SU, SS) such that

$$\forall u \in \Sigma_{\neg p}^* \Sigma_p,\ \forall v \in \Sigma^\omega,\ \forall i \geq 0 : \qquad v, 0 \models \varphi \quad \text{iff} \quad uv, 0 \models \overline{\varphi}\,.$$

Exercise 5 (Linear Orders with Gaps)**.** In this exercise we assume $(\mathbb{T}, <)$ to be a linear time flow. Let us define a new unary "gap" modality gap:

$$\begin{aligned} w, i \models \mathsf{gap}\varphi \text{ iff } \forall k. k > i \to\ & (\exists \ell. k < \ell \wedge \forall j. i < j < \ell \to w, j \models \varphi) \\ & \vee (\exists j. i < j < k \wedge w, j \models \neg\varphi) \\ \wedge\ & \exists k_1. k_1 > i \wedge \forall j. i < j \leq k_1 \to w, j \models \varphi \\ \wedge\ & \exists k_2. k_2 > i \wedge w, k_2 \models \neg\varphi\,. \end{aligned}$$

The intuition behind gap is that φ should hold for some time until a gap occurs in the time flow, after which $\neg\varphi$ holds at points arbitrarily close to the gap.

1. Express $\mathsf{gap}\varphi$ using the standard SU modality.

2. Show that, if $(\mathbb{T}, <)$ is Dedekind-complete (i.e. every nonempty subset of $\mathbb{T}$ with an upper bound has a least upper bound), then $\mathsf{gap}p$ for $p \in$ AP cannot be satisfied.