TD 2: Temporal Logics

1 LTL

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 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 LTL(AP) and (b) in 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.

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:

$$\mathsf{SF}(((\mathsf{SG}\, r)\, \mathsf{U}\, p) \wedge (\neg q\, \mathsf{U}\, p)) \vee \mathsf{SF}(\neg p \vee \mathsf{F}\, q)\ .$$

Exercise 3 (Expressiveness)**.** We fix the set 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 LTL(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 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) over $(\mathbb{N}, <)$.

2 CTL*

We work throughout this section and the next with tree temporal flows.

Exercise 4 (Equivalences)**.** Are the following formulæ equivalent?

1. $\mathsf{A}\,\mathsf{X}\,\mathsf{A}\,\mathsf{G}\,\varphi$ and $\mathsf{A}\,\mathsf{X}\,\mathsf{G}\,\varphi$

2. $\mathsf{E}\,\mathsf{X}\,\mathsf{E}\,\mathsf{G}\,\varphi$ and $\mathsf{E}\,\mathsf{X}\,\mathsf{G}\,\varphi$

3. $\mathsf{A}(\varphi \wedge \psi)$ and $\mathsf{A}\,\varphi \wedge \mathsf{A}\,\psi$

4. $\mathsf{E}(\varphi \wedge \psi)$ and $\mathsf{E}\,\varphi \wedge \mathsf{E}\,\psi$

5. $\neg\,\mathsf{A}(\varphi \Rightarrow \psi)$ and $\mathsf{E}(\varphi \wedge \neg\psi)$

3 CTL and CTL$^+$

Exercise 5 (CTL Equivalences)**.**

1. Are the two formulæ $\varphi = \mathsf{A}\,\mathsf{G}(\mathsf{E}\,\mathsf{F}\,p)$ and $\psi = \mathsf{E}\,\mathsf{F}\,p$ equivalent? Does one imply the other?

2. Same questions for $\varphi = \mathsf{E}\,\mathsf{G}\,q \vee (\mathsf{E}\,\mathsf{G}\,p \wedge \mathsf{E}\,\mathsf{F}\,q)$ and $\psi = \mathsf{E}(p\,\mathsf{U}\,q)$.

Exercise 6 (CTL$^+$)**.** CTL$^+$ extends CTL by allowing boolean connectives on path formulæ, according to the following abstract syntax:

$$f ::= \top \mid a \mid f \wedge g \mid \neg f \mid \mathsf{E}\,\varphi \mid \mathsf{A}\,\varphi \qquad \text{(state formulæ } f, g)$$
$$\varphi ::= \varphi \wedge \psi \mid \neg\varphi \mid \mathsf{X}\,f \mid f\,\mathsf{U}\,g \qquad \text{(path formulæ } \varphi, \psi)$$

where a is an atomic proposition. The associated semantics is that of CTL*.

We want to prove that, for any CTL$^+$ formula, there exists an equivalent CTL formula.

1. Give an equivalent CTL formula for

$$\mathsf{E}((a_1 \mathbin{\mathsf{U}} b_1) \wedge (a_2 \mathbin{\mathsf{U}} b_2)) \ .$$

2. Generalize your translation for any formula of form

$$\mathsf{E}(\bigwedge_{i=1,\dots,n} (\psi_i \mathbin{\mathsf{U}} \psi'_i) \wedge \mathsf{G}\,\varphi) \ . \tag{1}$$

   What is the complexity of your translation?

3. Give an equivalent CTL formula for the following CTL$^+$ formula:

$$\mathsf{E}(\mathsf{X}\,a \wedge (b \mathbin{\mathsf{U}} c)) \ .$$

4. Using subformulæ of form (1) and E modalities, give an equivalent CTL formula to

$$\mathsf{E}(\mathsf{X}\,\varphi \wedge \bigwedge_{i=1,\dots,n} (\psi_i \mathbin{\mathsf{U}} \psi'_i) \wedge \mathsf{G}\,\varphi') \ . \tag{2}$$

   What is the complexity of your translation?

5. We only have to transform any CTL$^+$ formula into (nested) disjuncts of form (2). Detail this translation for the following formula:

$$\mathsf{A}((\mathsf{F}\,a \vee \mathsf{X}\,a \vee \mathsf{X}\,\neg b \vee \mathsf{F}\,\neg d) \wedge (d \mathbin{\mathsf{U}} \neg c)) \ .$$