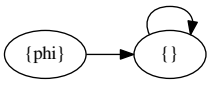
Exercise session 7: LTL and CTL

1 Check equivalence

Which of the following pairs of CTL formulas are equivalent? For those which are not, exhibit a model of one of the pair which is not a model of the other:

1. $\mathrm{EF}\ \phi$ and $\mathrm{EG}\ \phi$

   Solution: Not equivalent. $\mathrm{EG}\ \phi$ implies $\mathrm{EF}\ \phi$, but not the other way around. $\mathrm{EF}\ \phi$ allows for paths in which $\neg\phi$, and $\mathrm{EG}\ \phi$ does not.



2. $\mathrm{EF}\ \phi \vee \mathrm{EF}\ \psi$ and $\mathrm{EF}\ (\phi \vee \psi)$

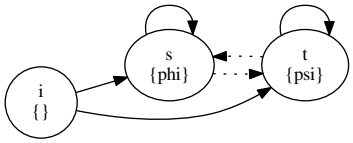
   Solution: Equivalent.

   - First, assume that $s \models \mathrm{EF}\ \phi \vee \mathrm{EF}\ \psi$. Then without loss of generality, we may assume that $s \models \mathrm{EF}\ \phi$ (the other case is shown in the same manner). This means that there is a future state s_n, reachable from s, such that $s_n \models \phi$, But then $s_n \models \phi \vee \psi$ follows. But this means that there is a state reachable from s which statisfies $\phi \vee \psi$. Thus, $s \models \mathrm{EF}\ (\phi \vee \psi)$ follows.
   - Second, assume that $s \models \mathrm{EF}\ (\phi \vee \psi)$. Then there exists a state s_m, reachable from s, such that $s_m \models \phi \vee \psi$. Without loss of generality, we may assume that $s_m \models \psi$. But then we can conclude that $s \models \mathrm{EF}\ \psi$, as s_m is reachable from s. Therefore, we also have $s \models \mathrm{EF}\ \psi \vee \mathrm{EF}\ \psi$.

3. $\mathrm{AF}\ \phi \vee \mathrm{AF}\ \psi$ and $\mathrm{AF}\ (\phi \vee \psi)$

   Solution: Not equivalent. While we have that $s \models (\mathrm{AF}\ \phi \vee \mathrm{AF}\ \phi)$ implies $s \models \mathrm{AF}\ (\phi \vee \psi)$, the converse is not true. Therefore, the formulas $\mathrm{AF}\ \phi \vee \mathrm{AF}\ \psi$ and $\mathrm{AF}\ (\phi \vee \psi)$ are not equivalent. To see that the converse fails, consider a model with three states i, s and t such that $i \to s$, $i \to t$, $s \to s$, ($s \to t$, $t \to s$), and $t \to t$ are the state transitions. If we think of ϕ and ψ to be atoms phi, respectively psi, we create labelings $L(i) = \emptyset$, $L(s) = \{phi\}$ and $L(t) = \{psi\}$. Since s and t satisfy $phi \vee psi$ we have $i \models \mathrm{AF}\ (phi \vee psi)$. However, we do not have $i \models \mathrm{AF}\ phi \vee \mathrm{AF}\ psi$:

   - To see $i \not\models \mathrm{AF}\ phi$ we can chose the path $i \to t \to t \to t \to t \to \ldots$.
   - To see $i \not\models \mathrm{AF}\ psi$ we symmetrically choose the path $i \to s \to s \to s \to \ldots$.



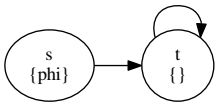
4. $\mathrm{AF}\ \neg\phi$ and $\neg\mathrm{EG}\ \phi$

   Solution: Equivalent. If there are no paths where ϕ holds throughout all, then for all paths somewhere $\neg\phi$ is true. If for all paths somewhere $\neg\phi$ is true, then there is not one path where ϕ holds throughout.

5. $\mathrm{EF}\ \neg\phi$ and $\neg\mathrm{AF}\ \phi$

   Solution: Not equivalent. **Solution:** This is not an equivalence (it would have to be $\neg\mathrm{AG}\ \phi$ instead of $\neg\mathrm{AF}\ \phi$). Consider the model from item 3 (repeated here). We have $s \models \mathrm{EF}\ \neg phi$ since we have the initial path segment $s \to t \to \ldots$ But we do not have $s \models \neg\mathrm{AF}\ phi$, for the present is part of the future in CTL (and $\neg\mathrm{AF}\ phi \equiv \mathrm{EG}\ \neg phi$).

   Or, $\mathcal{M}, s \models \mathrm{EF}\ \neg\phi$ and $\mathcal{M}, s \models \mathrm{AF}\ \phi$ and hence $\mathcal{M}, s \not\models \neg\mathrm{AF}\ \phi$



6. $\mathrm{A}\ (\phi_1\ \mathrm{U}\ \mathrm{A}\ (\phi_2\ \mathrm{U}\ \phi_3))$ and $\mathrm{A}\ (\mathrm{A}\ (\phi_1\ \mathrm{U}\ \phi_2)\ \mathrm{U}\ \phi_3)$, hint: it might make it simpler if you think first about models that have just one path

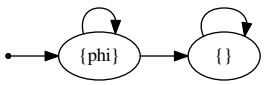
   Solution: Not equivalent.

7. $\top$ and $\mathrm{AG}\ \phi \Rightarrow \mathrm{EG}\ \phi$

   Solution: Equivalent (at least if we require that there is always one state. If there is one state, there is always at least one path – so much is made clear in the definition on page 178).

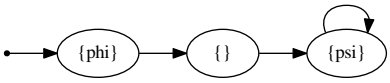
8. $\top$ and $\mathrm{EG}\ \phi \Rightarrow \mathrm{AG}\ \phi$

   Solution: Not equivalent. Saying that a CTL formula ϕ is equivalent to $\top$ is just paraphrasing that ϕ is true at all states in all models. (Why?) But this is not the case for $\mathrm{EG}\ \phi \Rightarrow \mathrm{AG}\ \phi$. Consider the model below. Clearly, we have $s \models \mathrm{EG}\ p$, but we certainly don't have $s \models \mathrm{AG}\ p$. (What about $\top$ and $\mathrm{AG}\ \phi \Rightarrow \mathrm{EG}\ \phi$, though?)



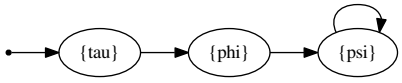
9. $\mathrm{A}\ [\phi\ \mathrm{U}\ \psi]$ and $\phi \wedge \mathrm{AF}\ \psi$

   Solution: Not equivalent.



10. $\mathrm{A}\ [\phi\ \mathrm{U}\ \psi] \vee \mathrm{A}\ [\tau\ \mathrm{U}\ \psi]$ and $\mathrm{A}\ [(\tau \vee \phi)\ \mathrm{U}\ \psi]$

    Solution: Not equivalent.



2 Express in CTL and LTL

Express the following properties in CTL and LTL whenever possible. If neither is possible, try to express the property in CTL*:

1. Whenever p is followed by q (after finitely many steps), then the system enters an 'interval' in which no r occurs until t.

   Solution: The process of translating informal requirements into formal specifications is subject to various pitfalls. One of them is simply ambiguity. For example, it is unclear whether "after some finite steps" means "at least one, but infinitely many steps", or whether zero steps are allowed as well. It may also be debatable what "then" exactly means in "... then the system enters ...". We chose to solve this problem for the case when zero steps are not admissible, mostly since "followed by" suggests a real state transition to take place. The CTL formula we came up with is

   $$\mathrm{AG}\ (p \Rightarrow \mathrm{AX}\ \mathrm{AG}\ (\neg q \vee \mathrm{A}\ [\neg r\ \mathrm{U}\ t]))$$

   which in LTL may be expressed as

   $$\mathrm{G}\ (p \Rightarrow \mathrm{X}\ \mathrm{G}\ (\neg q \vee \neg r\ \mathrm{U}\ t))$$

   It says: At any state, if p is true, then at any state which one can reach with at least one state transition from here, either q is false, or r is false until t becomes true (for continuations of the computation path). This is evidently the property we intent to model. Various other "equivalent" solutions can be given.

2. Event p precedes s and t on all computation paths. (You may find it easier to code the negation of that specification first)

   Solution: The negation: there exists in the future a state in which p follows s or t:

   $$\mathrm{EF}\ ((s \vee t) \Rightarrow \mathrm{EF}\ p)$$

   The real specification (and negation of the previous):

   $$\neg\mathrm{EF}\ ((s \vee t) \wedge \mathrm{EF}\ (p)) \equiv \mathrm{AG}\ (\neg((s \vee t) \wedge \mathrm{EF}\ (p))) \equiv AG((s \vee t) \Rightarrow \mathrm{AG}\ (\neg p))$$

   Alternative interpretation:

   $$\neg\mathrm{E}\ [\neg p\ \mathrm{U}\ s] \wedge \neg\mathrm{E}\ [\neg p\ \mathrm{U}\ t]$$

3. After p, q is never true. (Where this constraint is meant to apply on all computation paths.)

   Solution:

$$\mathrm{AG}\ (p \Rightarrow \neg \mathrm{EF}\ q) \ \text{ or } \ \mathrm{AG}\ (p \Rightarrow \neg \mathrm{EX}\ \mathrm{EF}\ q)$$

4. Between the events q and r, event p is never true.

   Solution: It is open to several interpretations. Please assume that what is meant is that on all paths, p is false throughout each closed interval $[q, r]$ where q holds at the beginning of the interval and r holds at the end of the interval and only at the end.) Because of ambiguity, it is often a non-trivial task to go from specifications in English to appropriate formal specifications. In this case, the question was did we mean the strict or inclusive meaning of "between"? I chose the inclusive meaning. The strict meaning would be that p is false in the open interval (q, r).)

$$[\mathrm{AG}\ (q \Rightarrow \neg \mathrm{EF}\ (p \wedge \mathrm{EF}\ r))] \wedge [\mathrm{AG}\ (r \Rightarrow \neg \mathrm{EF}\ (p \wedge \mathrm{EF}\ q))]$$

5. Transitions to states satisfying p occur at most twice.

   Solution: Transition to self is counted as a transition, otherwise you have to add $\neg p$ parts to the formula.

$$\neg(\mathrm{EF}\ (p \wedge \mathrm{EX}\ \mathrm{EF}\ (p \wedge \mathrm{EX}\ \mathrm{EF}\ p))) \equiv \mathrm{AG}\ (p \Rightarrow \mathrm{AX}\ \mathrm{AG}\ (p \Rightarrow \mathrm{AX}\ \mathrm{AG}\ \neg p))$$

6. Property p is true for every second state along a path.

   Solution:

$$\mathrm{X}\ \mathrm{X}\ p$$

$$\mathrm{AX}\ \mathrm{AX}\ p$$

3 Expressable in ...

1. Give example of an LTL-formula for which equivalent translation in CTL does not exist.

   Solution: $\mathrm{G}\ p \Rightarrow \mathrm{G}\ q$ or $\mathrm{F}\ \mathrm{G}\ p$

2. Give example of an CTL-formula for which equivalent translation in LTL does not exist.

   Solution: $\mathrm{EX}\ p$ or $\mathrm{AF}\ \mathrm{AG}\ p$

3. Give example of an CTL*-formula for which equivalent translation in LTL either in CTL does not exist.

   Solution: $\mathrm{A}\ (\mathrm{G}\ p \Rightarrow \mathrm{G}\ q) \vee \mathrm{EX}\ p$ or $(\mathrm{A}\ \mathrm{F}\ \mathrm{G}\ p) \wedge (\mathrm{AF}\ \mathrm{AG}\ q)$

4 Proof the equivalence

Given the definitions:

- $\pi \models \psi\ \mathrm{U}\ \phi$ iff there is some $i \geq 1$ such that $\pi^i \models \phi$ and for all $j = 1, \ldots, i-1$ we have $\pi^j \models \psi$
- $\pi \models \psi\ \mathrm{R}\ \phi$ iff either there is some $i \geq 1$ such that $\pi^i \models \psi$ and for all $j = 1, \ldots, i$ we have $\pi^j \models \phi$, or for all $k \geq 1$ we have $\pi^k \models \phi$

Proof the following theorem:

$$\neg(\psi \ \mathrm{U} \ \phi) \equiv \neg\psi \ \mathrm{R} \ \neg\phi \tag{1}$$

Solution: Proof. Let $\mathcal{M}$ be a transition structure, s a state of $\mathcal{M}$. We must show that for every path π of $\mathcal{M}$ starting in s, $\pi \models \neg(\psi \ \mathrm{U} \ \phi)$ iff $\pi \models \neg\psi \ \mathrm{R} \ \neg\phi$,
The trick of the proof is in first simplifying the definition of R :

$$\pi \models \psi \ \mathrm{R} \ \phi \text{ iff for all } i \geq 1 \text{ such that } \pi^i \models \neg\phi, \text{ there exists a } j < i \text{ such that } \pi^j \models \psi \tag{2}$$

Assume that $\pi \models \psi \ \mathrm{R} \ \phi$. Then either all $i \geq 1$ satisfy $\pi^i \models \phi$, or equivalently, there is no $i \geq 1$ such that $\pi^i \models \neg\phi$. In this case, the righthand of the equivalence is trivially satisfied. Or, there is an $i \geq 1$ such that $\pi^i \models \psi$ and $j \leq i$ implies $\pi^i \models \phi$. It follows for any $i' \geq 0$ such that $\pi^{i'} \models \neg\phi$, that $i < i'$ and $\pi^i \models \psi$. Again, the righthand is satisfied.

Assume that $\pi \not\models \psi \ \mathrm{R} \ \phi$. Hence, there is an $i \geq 1$ such that $\pi^i \models \neg\phi$ and ϕ has not been released, i.e., ψ is false in each of $\pi^1, \ldots, \pi^{j-1}$. Hence, for this i we have $\pi^i \models \neg\phi$ and there is no $j < i$ such that $\pi^j \models \psi$.

Given this equivalence, the theorem can no easily be proven:

$$\pi \models \neg(\psi \ \mathrm{U} \ \phi) \text{ iff for all } i \geq 1 \text{ such that } \pi^i \models \phi, \text{ there is a } j < i \text{ such that } \pi^j \models \neg\psi \text{ iff } \pi \models \neg\psi \ \mathrm{R} \ \neg\phi. \tag{3}$$

5 Nim game

If you have time left, and haven't made the Nim game yet last session, complete this exercise. The assignment from last week can still be found on Toledo.