CTL Tutorial Notes

CSC410

November 2023

1 Formalization

a) If the light is red (r) and at some point in the future switches to yellow (y), then there is a possibility that it will eventually turn to green (g).

$$\forall\Box(r \land \forall\Diamond y \implies \exists\Diamond g)$$

b) "The light can turn green (g) and, having done so, it will eventually turn yellow (y), but it will not turn red (r) before it turns yellow."

$$\exists\Diamond g \land \forall\Box(g \implies \forall(\neg r\,\mathcal{U}\,y))$$

Note. The original English specification used in the tutorial was slightly weaker. It was:

"The light can turn green (g) but, having done so, it will not turn red (r) before it turns yellow."

As pointed out during tutorial, there is nothing in this specification that *requires* the light to eventually turn yellow if it turns green.

It is a good exercise to try and think about how to translate this more faithfully.

Hint: this is a kind of safety property, i.e. there is something *bad* we want to prohibit from happening. That is, the formula will be of the form

$$\exists\Diamond g \wedge \forall\Box(g \implies \neg\texttt{Bad})$$

The bad thing, in this case, is the existence of a trace from the green state to a red state without any intermediate yellow states. In particular, a path which never encounters a red state is fine. You can consider defining `Bad` in a way which does a kind of "case analysis" on whether a red state is ever encountered along some path – since if a red state is never encountered along a path, we don't care about whether or not it turns yellow.

$$\exists\Diamond g \wedge \forall\Box(g \implies \forall))$$

c) "Should the light turn green, it will eventually be yellow for exactly one time-step, and will never be yellow again."

$$\forall\Box(g \implies \forall(\neg y\, \mathcal{U}\ (y \wedge \forall \bigcirc (\forall\Box\neg y))))$$

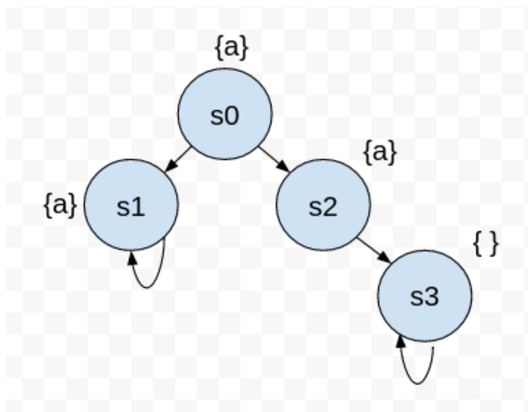
2 Satisfiability

Determine the satisfiability of the following CTL formulae. If it is satisfiable, provide a satisfying model. If it is unsatisfiable, provide a proof.

a)

$$\exists\Box\phi \wedge \exists\Diamond\neg\phi \wedge \forall \bigcirc \phi$$

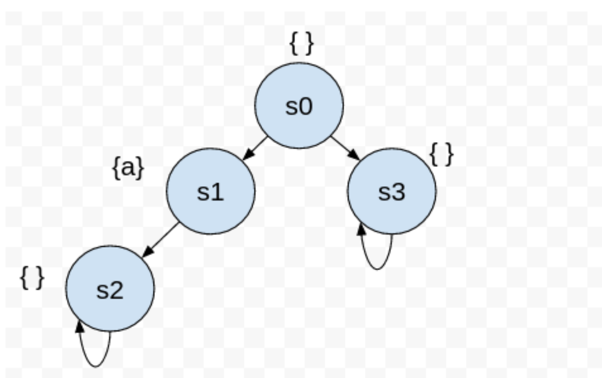
Satisfiable. Let $AP = \{a\}$, define $\phi = a$, and consider the following model:



b)

$$\forall\Diamond(\exists\Diamond\phi \wedge \exists\Box\neg\phi \wedge \forall(\phi\,\mathcal{U}\,\neg\phi))$$

Satisfiable.Let $AP = \{a\}$, define $\phi = a$, and consider the following model:



3 Equivalence Proofs

Prove or disprove the following equivalences. If it does not hold, provide a counterexample.

$$\exists(\phi\,\mathcal{U}\,\psi) \equiv \psi \vee (\phi \wedge \exists \bigcirc \exists\phi\,\mathcal{U}\,\psi)$$

Fix a state s in some model.

Forward Direction.
Assume $s \models \exists(\phi\,\mathcal{U}\,\psi)$.

Then there is a path π such that $\pi[0] = s$ and $\pi \models \phi\,\mathcal{U}\,\psi$. That is to say, there exist $k \in \mathbb{N}$ such that $\pi[k] \models \psi$ and, for all $j < k$, we have $\pi[j] \models \phi$.

We proceed by case analysis on $k = 0 \vee k = k' + 1$ for some k'.

Case 1. $k = 0$. Then $\pi[0] \models \psi$, which is to say $s \models \psi$. And since $s \models \psi$, we have $s \models \psi \vee (\phi \wedge \exists \bigcirc \exists(\phi\,\mathcal{U}\,\psi))$, so we are done.

Case 2. $k = k' + 1$. Then $\pi[k' + 1] \models \psi$ and for all $j \leq k$, we have $\pi[j] \models \phi$.

We will try to prove the right disjunct, which is to say $s \models \phi \wedge \exists \bigcirc \exists(\phi\,\mathcal{U}\,\psi)$

To prove $s \models \phi$, we use the above assumption with the fact that $0 \leq k$, which gives us $\pi[0] \models \phi$, and so $s \models \phi$.

We now need to prove $s \models \exists \bigcirc \exists\phi\,\mathcal{U}\,\psi$. We begin by unfolding the semantics of $\exists$:

$$\exists\pi' \in \texttt{Paths}(s).\ \pi' \models \bigcirc\exists(\phi\,\mathcal{U}\,\psi)$$

unfolding the semantics of $\bigcirc$, we have

$$\exists\pi' \in \texttt{Paths}(s).\ \pi'[1] \models \exists(\phi\,\mathcal{U}\,\psi)$$

which then becomes

$$\exists\pi' \in \texttt{Paths}(s).\ \exists\pi'' \in \texttt{Paths}(\pi'[1]).\ \pi'' \models \phi\,\mathcal{U}\,\psi$$

So we need a path π from whose second state there is a path satisfying $\phi\,\mathcal{U}\,\psi$. The only path from s we know about is our path π from our assumption, so we'll use it as the witness for the outer quantifier. We now need to prove

$$\exists\pi'' \in \texttt{Paths}(\pi[1]).\ \pi'' \models \phi\,\mathcal{U}\,\psi$$

Let's define the witness $\pi'' = \pi[1...]$. Then $\pi'' \in \mathtt{Paths}(\pi[1])$ by construction.

We need to prove $\pi'' \vDash \phi\,\mathcal{U}\,\psi$. Using the construction of π'', we get

$$\begin{aligned}
&\pi'' \vDash \phi\,\mathcal{U}\,\psi \\
\iff &\pi[1..] \vDash \phi\,\mathcal{U}\,\psi \\
\iff &\exists m \in \mathbb{N}.\, \pi[m+1] \vDash \psi \wedge \forall j < m.\, \pi[j+1] \vDash \phi \\
&\hfill \text{(Semantics of } \mathcal{U} \text{ and algebra of paths)}
\end{aligned}$$

Recall our assumption that we have a k' such that $\pi[k'+1] \vDash \psi$, so we use k' as our witness to the existential. We then need to prove that $\forall j < k'$ we have $\pi[j+1] \vDash \phi$. But this is the same as saying that for all $j < k'+1$, we have $\pi[j] \vDash \phi$, which is exactly our other assumption. So we are done.

Reverse Direction.

Assume $s \vDash \psi \vee (\phi \wedge \exists \bigcirc \exists(\phi\,\mathcal{U}\,\psi))$.

We want to show that $s \vDash \phi\,\mathcal{U}\,\psi$, which is to say

$$\exists \pi \in \mathtt{Paths}(s).\, \exists k.\, \pi[k] \vDash \psi \wedge \forall j < k.\, \pi[j] \vDash \phi$$

We proceed by case analysis on the disjunction in our assumption.

Case 1. Assume $s \vDash \psi$. Then fix any path $\pi \in \mathtt{Paths}(s)$ as the witness for the first existential, and use $k = 0$ as the witness for the second. existential. The conjunct $\pi[k] \vDash \psi$ is handled by our assumption, since $\pi[0] = s$ and $s \vDash \psi$. The other conjunct holds vacuously, for there is no $j \in \mathbb{N}$ such that $j < 0$. So we are done

Case 2. Assume $s \vDash \phi \wedge \exists \bigcirc \exists \phi\,\mathcal{U}\,\psi$. That is to say,

a) $s \vDash \phi$, and

b) there is a path π beginning from s such that $\pi[1] \vDash \phi\,\mathcal{U}\,\psi$

which is to say

c) there is a path $\pi' \in \mathtt{Paths}(\pi[1])$ and $k \in \mathbb{N}$ such that $\pi'[k] \vDash \psi$ and for every $j < k$, we have $\pi'[j] \vDash \phi$.

The proof obligation, of course, is to produce a path beginning from s which eventually satisfies ψ and satisfies ϕ until then. Based on what we have, it should be clear how to construct this path: we just take the first state of π and append to it the path π'. More formally, we define the path

$$\pi'' = \pi[0] \cdot \pi'$$

By construction, we have that for any i, we have $\pi'[i] = \pi''[i + 11]$. We then use π'' as the witness for the outer existential, and use $k + 1$ as our witness for the inner existential. The rest follows from our assumption c).