Computation Tree Logic

Syntax and Semantics, Equivalences, Specification, CTL*

Ranald Clouston

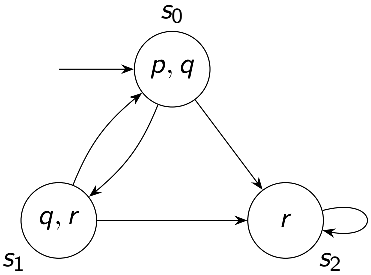
May 9, 2025

Australian National University

Branching Transition Systems

Transition systems often branch (evolve in different ways), perhaps because of:

- Interaction with users, external processes, environment
- Randomness
- Parallelism creating unpredictable ordering of operations



Beyond LTL

LTL propositions only talk about a single path of a transition system

- Sometimes in practice LTL propositions are analysed with respect to all possible paths.

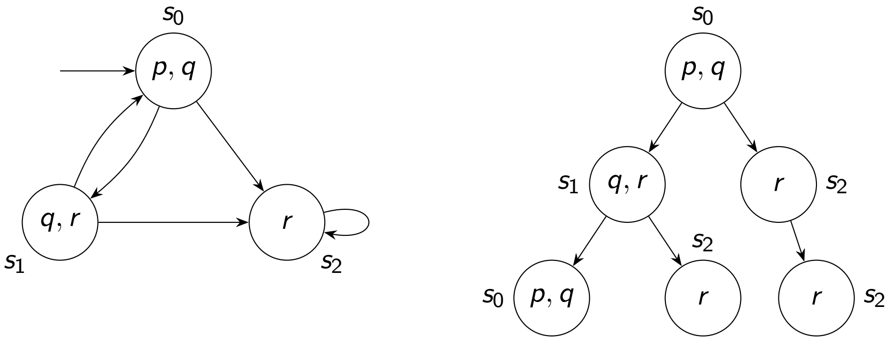
We often want to talk about all or some possible paths, and to mix these existential and universal statements in a single proposition

- It is possible to get to state where a certain property holds;
- From any point on any path through the system, it is possible to get to state where a certain property holds;
- There exists a situation from which all paths will lead to a certain proposition.

This capability is provided by branching temporal logic, better known as Computation Tree Logic (CTL).

Computation Trees

Computation Tree Logic takes its name from a visualisation of all paths through a system as an infinite tree of branching possibilities:



CTL Syntax and Semantics

Extending LTL Syntax

If we consider of multiple paths, even a connective as simple as X becomes ambiguous:

- By $X\varphi$, do I mean that all possible next states satisfy φ, or only that some possible next state does?
- If there is exactly one possible next state, as in LTL, there is no distinction here!

We resolve this ambiguity by splitting X into two connectives:

- AX means 'All neXt'
- EX means 'Exists a neXt'
- X on its own is no longer a valid unary connective; we must specify which X we mean by putting A or E on top, every time.
- A and E on their own are also not valid unary connectives.

We perform the same doubling to all the temporal connectives.

CTL Syntax

Definition of a CTL proposition:

$$\varphi \quad := \quad p \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid AX\varphi \mid EX\varphi$$
$$\mid AF\varphi \mid EF\varphi \mid AG\varphi \mid EG\varphi \mid A[\varphi U \varphi] \mid E[\varphi U \varphi]$$

where p is any propositional variable.

The unary connectives bind as tightly as $\neg$. Where AU and EU need disambiguation, we will use parentheses.

Semantics of Propositional Connectives

A CTL proposition holds, or fails to hold, for a particular transition system $\mathcal{M}$ and state s (usually, we are interested in a start state).

- Write $\vDash_{\mathcal{M},s} \varphi$ to say that φ is satisfied by all paths whose first state is s.
- If we want a proposition to hold for all states in the model, write $\vDash_{\mathcal{M}}$. If we want to express that it holds for all transition systems, write $\vDash$.

Semantics for the propositional connectives are mostly familiar from LTL:

- $\vDash_{\mathcal{M},s} p$ if $p \in L(s)$
- $\vDash_{\mathcal{M},s} \bot$ never
- $\vDash_{\mathcal{M},s} \neg\varphi$ if it is not the case that $\vDash_{\mathcal{M},s} \varphi$
- $\vDash_{\mathcal{M},s} \varphi \wedge \psi$ if $\vDash_{\mathcal{M},s} \varphi$ and $\vDash_{\mathcal{M},s} \psi$
- $\vDash_{\mathcal{M},s} \varphi \vee \psi$ if $\vDash_{\mathcal{M},s} \varphi$ or $\vDash_{\mathcal{M},s} \psi$ (or both)
- $\vDash_{\mathcal{M},s} \varphi \rightarrow \psi$ if $\vDash_{\mathcal{M},s} \varphi$ implies $\vDash_{\mathcal{M},s} \psi$

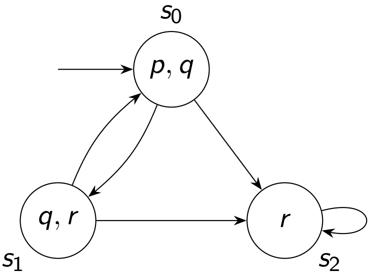
Semantics of Temporal Connectives, via LTL

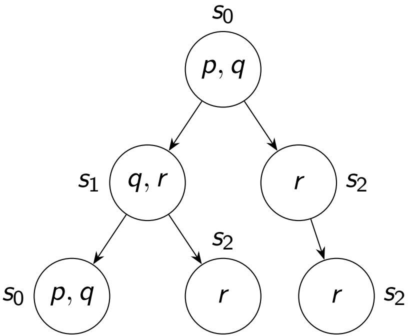
- $\models_{\mathcal{M},s} AX\varphi$ if for all paths $\sigma = s \to s_1 \to s_2 \to \cdots$ in $\mathcal{M}$, we have $\models_{\mathcal{M},\sigma} X\varphi$ in LTL.
- $\models_{\mathcal{M},s} EX\varphi$ if there exists a path $s \to \cdots$ satisfying $X\varphi$
- $\models_{\mathcal{M},s} AG\varphi$ if all paths $s \to \cdots$ satisfy $G\varphi$
- $\models_{\mathcal{M},s} EG\varphi$ if there exists a path $s \to \cdots$ satisfying $G\varphi$
- $\models_{\mathcal{M},s} AF\varphi$ if all paths $s \to \cdots$ satisfy $F\varphi$
- $\models_{\mathcal{M},s} EF\varphi$ if there exists a path $s \to \cdots$ satisfying $F\varphi$
- $\models_{\mathcal{M},s} A[\varphi\, U\, \psi]$ if all paths $s \to \cdots$ satisfy $\varphi\, U\, \psi$
- $\models_{\mathcal{M},s} E[\varphi\, U\, \psi]$ if there exists a path $s \to \cdots$ satisfying $\varphi\, U\, \psi$

Semantics of Temporal Connectives, Directly

- $\models_{\mathcal{M},s} AX\varphi$ if for all transitions $s \to s'$ in $\mathcal{M}$, we have $\models_{\mathcal{M},s'} \varphi$.
- $\models_{\mathcal{M},s} EX\varphi$ if there exists a transition $s \to s'$ such that $\models_{\mathcal{M},s'} \varphi$
- $\models_{\mathcal{M},s} AG\varphi$ if all paths $s \to \cdots$ and all states s' in such a path, $\models_{\mathcal{M},s'} \varphi$
- $\models_{\mathcal{M},s} EG\varphi$ if there exists a path $s \to \cdots$ such that for all states s' in that path, $\models_{\mathcal{M},s'} \varphi$
- $\models_{\mathcal{M},s} AF\varphi$ if all for paths $s \to \cdots$ there exists a state s' in that path such that $\models_{\mathcal{M},s'} \varphi$
- $\models_{\mathcal{M},s} EF\varphi$ if there exists a path $s \to \cdots$ such that there exists a state s' in that path such that $\models_{\mathcal{M},s'} \varphi$
- $\models_{\mathcal{M},s} A[\varphi\, U\, \psi]$ if for all paths $s \to \cdots$ there exists a state s' in that path such that $\models_{\mathcal{M},s'} \psi$, and for all strictly earlier states s'' in that path, $\models_{\mathcal{M},s''} \varphi$
- $\models_{\mathcal{M},s} E[\varphi\, U\, \psi]$ if there exists a path $s \to \cdots$ such that there exists a state s' in that path such that $\models_{\mathcal{M},s'} \psi$, and for all strictly earlier states s'' in that path, $\models_{\mathcal{M},s''} \varphi$

Examples

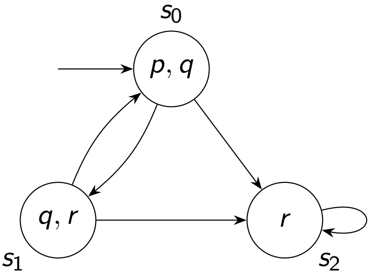


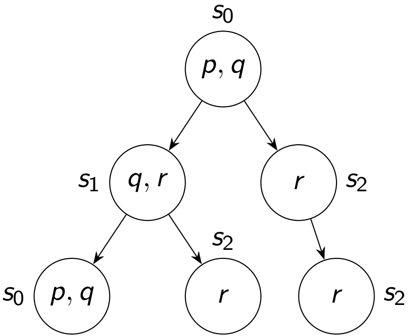


In this transition system starting at s_0 / induced computation tree:

- $AX(q \wedge r)$ or $EX(q \wedge r)$?
- If either of the above fail, what is a true statement involving AX or EX?

Examples





- AFr or EFr? What can we say in general about $A\heartsuit$ and $E\heartsuit$ for any LTL connective $\heartsuit$?
- $A[p \wedge q\, U\, AGr]$ or $E[p \wedge q\, U\, AGr]$?

Equivalences

Duality

We are now used to pairs of 'dual connectives' that are related to each other by $\neg$:

- $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ and $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$
- $\neg\forall x\, \varphi \equiv \exists x \neg\varphi$ and $\neg\exists x\, \varphi \equiv \forall x \neg\varphi$
- $\neg G\varphi \equiv F\neg\varphi$ and $\neg F\varphi \equiv G\neg\varphi$

In all the above, $\equiv$ means 'is satisfied by exactly the same models'.

Hence either of these pairs of connectives are definable in terms of their dual:

- e.g. $\varphi \vee \psi \;\equiv\; \neg\neg\varphi \vee \neg\neg\psi \;\equiv\; \neg(\neg\varphi \wedge \neg\psi)$

What dualities does CTL exhibit?

Duality in CTL

Each A and G is defined universally, and each E and F is existential, so:

- $\neg AG\varphi \equiv EF\neg\varphi$ and $\neg EF\varphi \equiv AG\neg\varphi$
- $\neg AF\varphi \equiv EG\neg\varphi$ and $\neg EG\varphi \equiv AF\neg\varphi$

X was self dual in LTL, so

- $\neg AX\varphi \equiv EX\neg\varphi$ and $\neg EX\varphi \equiv AX\neg\varphi$

But what about U?

- $\neg A[\varphi\, U\, \psi]$ cannot be $E\neg[\varphi\, U\, \psi]$ because this is not valid syntax!

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

Hence $\vDash_{\mathcal{M},s} A[\varphi \, U \, \psi]$ iff...

- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \varphi \, U \, \psi$ in LTL, iff
- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

Hence $\vDash_{\mathcal{M},s} A[\varphi \, U \, \psi]$ iff...

- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \varphi \, U \, \psi$ in LTL, iff
- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s for which it is not the case that $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

Hence $\vDash_{\mathcal{M},s} A[\varphi \, U \, \psi]$ iff...

- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \varphi \, U \, \psi$ in LTL, iff
- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s for which it is not the case that $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s such that $\vDash_{\mathcal{M},\sigma} \neg(\neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi)$, iff

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

Hence $\models_{\mathcal{M},s} A[\varphi \, U \, \psi]$ iff...

- for all paths σ from s, $\models_{\mathcal{M},\sigma} \varphi \, U \, \psi$ in LTL, iff
- for all paths σ from s, $\models_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s for which it is not the case that $\models_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s such that $\models_{\mathcal{M},\sigma} \neg(\neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi)$, iff
- there does not exist a path σ from s for which $\models_{\mathcal{M},\sigma} (\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \vee G\neg\psi$
- it is neither the case that there exists a path σ from s for which $\models_{\mathcal{M},\sigma} \neg\psi \, U \, (\neg\varphi \wedge \neg\psi)$, nor that there exists a path σ from s for which $\models_{\mathcal{M},\sigma} G\neg\psi$, iff
- it is not the case that $\models_{\mathcal{M},s} E[\neg\varphi \, U \, \neg\varphi \wedge \neg\psi]$, nor $\models_{\mathcal{M},s} EG\neg\psi$, iff

AU via EU

In LTL it is a fact (don't believe me? Prove the two sequents with tableaux!) that

$$\varphi \, U \, \psi \quad \equiv \quad \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$$

Hence $\vDash_{\mathcal{M},s} A[\varphi \, U \, \psi]$ iff...

- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \varphi \, U \, \psi$ in LTL, iff
- for all paths σ from s, $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s for which it is not the case that $\vDash_{\mathcal{M},\sigma} \neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi$, iff
- there does not exist a path σ from s such that $\vDash_{\mathcal{M},\sigma} \neg(\neg(\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \wedge F\psi)$, iff
- there does not exist a path σ from s for which $\vDash_{\mathcal{M},\sigma} (\neg\psi \, U \, (\neg\varphi \wedge \neg\psi)) \vee G\neg\psi$
- it is neither the case that there exists a path σ from s for which $\vDash_{\mathcal{M},\sigma} \neg\psi \, U \, (\neg\varphi \wedge \neg\psi)$, nor that there exists a path σ from s for which $\vDash_{\mathcal{M},\sigma} G\neg\psi$, iff
- it is not the case that $\vDash_{\mathcal{M},s} E[\neg\varphi \, U \, \neg\varphi \wedge \neg\psi]$, nor $\vDash_{\mathcal{M},s} EG\neg\psi$, iff
- $\vDash_{\mathcal{M},s} \neg(E[\neg\varphi \, U \, \neg\varphi \wedge \neg\psi] \vee EG\neg\psi)$

A Minimal Set of Connectives

So we get the far from obvious fact that AU can be defined via $\neg$, EU, $\wedge$, and EG:

$$A[\varphi\, U\, \psi] \quad \equiv \quad \neg(E[\neg\varphi\, U\, \neg\varphi \wedge \neg\psi] \vee EG\neg\psi)$$

(essentially the same argument would define EU in terms of AU)

As with LTL, we can define our F connectives in terms of our U connectives:

$$AF\varphi \quad \equiv \quad A[\top\, U\, \varphi] \qquad \text{and} \qquad EF\varphi \quad \equiv \quad E[\top\, U\, \varphi]$$

We will continue to use all our connectives because it is more convenient

- But when we get to model checking next week we will simplify our algorithm by assuming that our only connectives are $\bot$, $\neg$, $\wedge$, EX, EG, and EU.

Specification with CTL

A Two-Player Alternating Game

Suppose we are design a game with two players strictly alternating turns (like chess, tic-tac-toe). What would some desirable properties be?

- Let f be ‘first player’s move’, and e be ‘game is ended’

The property that the game starts with the first player, and is not already ended, can be expressed without temporal connectives, as $f \wedge \neg e$.

Some desirable properties are expressible, for an arbitrary game (path), in LTL:

- The game eventually ends: Fe
- The game eventually ends, and turns alternate until then: $((f \wedge X\neg f) \vee (\neg f \wedge Xf))\ U\ e$
- Whenever the game ends, it stays ended: $G(e \rightarrow Ge)$

A Two-Player Alternating Game

We can sometimes say an LTL proposition holds of an arbitrary path by prefixing A:

- 'The game eventually ends: Fe' becomes 'all games eventually end: AFe'

But $A[(f \wedge X\neg f) \vee (\neg f \wedge Xf)\ U\ e]$ and $AG(e \rightarrow Ge)$ are not CTL propositions.

- In fact, we can convert these to CTL without changing the intended meaning by adding some more As: $A[(f \wedge AX\neg f) \vee (\neg f \wedge AXf)\ U\ e]$ and $AG(e \rightarrow AGe)$

But here is a CTL proposition that seems to have no LTL counterpart:

- Introducing w for 'first player wins', we probably want to rule out a first move so powerful that they are guaranteed a win from it: $\neg EX\ AFw$.

CTL* : Beyond LTL and CTL

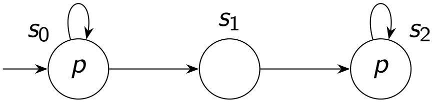
LTL vs CTL

Because CTL can talk about branching time, in particular mixing universals and existentials, it is obvious that it can express things than LTL cannot.

But what about the other way around? Can we always translate an LTL proposition (considered as a statement about an aribtrary path from the start state) into a CTL proposition by sprinkling in As?

Surprisingly perhaps, the answer is no.

LTL but not CTL: An Example



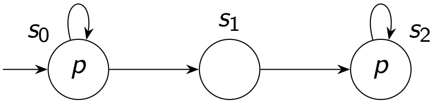
There are two kinds of paths through this system:

- Loop forever at s_0;
- Loop some finite number (maybe 0) times on s_0, then proceed to s_2

Both these sorts of paths obey the LTL proposition FGp: eventually they affirm p forever.

But the system does not satisfy $AF\,AGp$: there is a path (looping on s_0) in which there is no point from which the only paths always satisfy p (because we can always proceed to s_1).

LTL but not CTL: Another Example



Another example: all paths through this system obey the LTL proposition FXp, but the system does not satisfy $AF\ AXp$.

In fact, in LTL FXp is equivalent to XFp; but while we have just shown these propositions do not match $AF\ AXp$, they in fact do match $AX\ AFp$!

- So a lot of care is needed when trying to translate from LTL to CTL
- In fact (not proved in this course) there are LTL propositions with meanings that cannot be captured by any CTL proposition. The logics are formally incomparable.

Introducing CTL*

CTL* is a logic powerful enough to include all statements of LTL and CTL.

This is achieved by keeping the LTL connectives, but letting A and E be unary connectives on their own as well.

- Complication: $X\varphi$ and similar propositions on their own are still ambiguous.
- Solution: $X\varphi$ etc. must have an A or E above it in the syntax tree, but not necessarily immediately above.

So all CTL propositions are CTL* propositions, but we can now also express tricky LTL propositions like FGp, by writing $AFGp$.

- More precisely, we use square brackets and write $A[FG\varphi]$
- In fact any LTL proposition φ becomes the CTL* proposition $A[\varphi]$.

CTL* Syntax

Definition of a CTL* proposition φ involves the ancillary notion of a path propositions α:

$$\varphi \quad := \quad p \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid A[\alpha] \mid E[\alpha]$$

$$\alpha \quad := \quad \varphi \mid \neg\alpha \mid \alpha \wedge \alpha \mid \alpha \vee \alpha \mid \alpha \rightarrow \alpha \mid X\alpha \mid F\alpha \mid G\alpha \mid \alpha\, U\, \alpha$$

where p is any propositional variable.

This is complex to read, but the effect is simply to ensure that any occurrence of an LTL operator has at least one A or E above it.

CTL* Path Proposition Semantics, via LTL

The path propositions:

$$\alpha \quad := \quad \varphi \mid \neg\alpha \mid \alpha \wedge \alpha \mid \alpha \vee \alpha \mid \alpha \rightarrow \alpha \mid X\alpha \mid F\alpha \mid G\alpha \mid \alpha\, U\, \alpha$$

satisfy, or fail to satisfy, a model and a path though it, so we write $\vDash_{\mathcal{M},\sigma} \alpha$.

The semantics are defined exactly as for LTL, with the exception of the φ case (a CTL* proposition considered as a path proposition):

- $\vDash_{\mathcal{M},\sigma} \varphi$ if $\vDash_{\mathcal{M},\sigma_0} \varphi$

CTL* Semantics

CTL* propositions:

$$\varphi \quad := \quad p \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid A[\alpha] \mid E[\alpha]$$

satisfy, or fail to satisfy, a model and a state in it, so we write $\vDash_{\mathcal{M},s} \alpha$.

The semantics are defined exactly as for CTL, except for:

- $\vDash_{\mathcal{M},s} A[\alpha]$ if for all paths $\sigma = s \rightarrow \cdots$, $\vDash_{\mathcal{M},\sigma} \alpha$
- $\vDash_{\mathcal{M},s} E[\alpha]$ if there exists a path $\sigma = s \rightarrow \cdots$ such that $\vDash_{\mathcal{M},\sigma} \alpha$

The Power of CTL*

Clearly CTL* lets us say everything that LTL and CTL can (including the many things that both those logics can say).

In fact, it can also say some things which *neither* of these logics can say.

There exists a path with infinitely many p:

- In CTL*, $E[GFp]$
- Obviously not expressible in LTL, which has no existentials over possible futures;
- Not at all obvious it cannot be expressed in CTL, but the obvious candidates $EG\ EFp$ and $EG\ AFp$ fail (counter-examples on whiteboard).

Why Not Stick with CTL*?

CTL* expresses all of LTL, CTL, and a few other properties as well.

Why not jettison the earlier systems and spend all our time with CTL*?

We have seen this issue earlier with propositional logic and first order logic

- Yes, first order order logic is more expressive...
- but proof methods are more complex, and computation (much) more expensive.

Similarly:

- Yes, CTL* is the most expressive of our three temporal logics...
- but LTL is much simpler for humans to prove in (our tableaux method)...
- and it is in fact CTL that is computationally superior, at least for model checking, the topic of our final set of lectures (apart from exam revision).