Tecniche di Specifica e di Verifica

CTL*, CTL and LTL

CTL* language I

Syntax Let **AP** a finite set of ***atomic propositions***. We define by mutual induction the following set of formulae:

(*state formulae*)

0 If $\mathbf{p} \in \mathbf{AP}$, then $\mathbf{p}$ is a ***state*** formula.

1 If ϕ and ϕ' are ***state*** formulae, then so are $\neg \phi$ and $\phi \vee \phi'$, $\phi \wedge \phi'$.

2 If ψ is a ***path*** formula, then $\mathbf{E}\psi$ and $\mathbf{A}\psi$ are ***state*** formulae .

CTL* language I

Syntax ...

(***path formulae***)

3 if ϕ is a ***state*** formula, then ϕ is a ***path*** formula.

4 if ψ and ψ' are ***path*** formulae, then so are $\neg\psi$ and $\psi \vee \psi'$, $\psi \wedge \psi'$.

5 if ψ and ψ' are ***path*** formulae, then so are $\mathbf{X}\psi$ and $\psi\mathbf{U}\psi'$.

CTL* semantics I

Semantics Given the standard definitions

$K = (S, S_0, R, AP, L)$, $s \in S$, $L: S \to 2^{AP}$ and

path of K: $\pi = s_0\, s_1\, s_2 \dots$ where $(s_i\, s_{i+1}) \in R$:

0 $K, s \models p$ iff $p \in L(s)$.

1 for ***propositional formulae***

- $K, s \models \neg \phi$ iff ***not*** $K, s \models \phi$
- $K, s \models \phi_1 \vee \phi_2$ iff $K, s \models \phi_1$ or $K, s \models \phi_2$.
- $K, s \models \phi_1 \wedge \phi_2$ iff $K, s \models \phi_1$ and $K, s \models \phi_2$.

2 $K,s \models E\phi$ ($K,s \models A\phi$) iff for some (for all) path

$\pi = s\, s_1\, s_2 \dots$, it holds that $K,\pi \models \phi$

CTL* semantics II

Semantics ...

3 $\mathbf{K}, \pi \models p$ iff $\mathbf{K}, s_0 \models p$.

4 for propositional combination of path formulae

- $\mathbf{K}, \pi \models \neg\psi$ iff ***not*** $\mathbf{K}, \pi \models \psi$
- $\mathbf{K}, \pi \models \psi_1 \vee \psi_2$ iff $\mathbf{K}, \pi \models \psi_1$ or $\mathbf{K}, \pi \models \psi_2$.
- $\mathbf{K}, \pi \models \psi_1 \wedge \psi_2$ iff $\mathbf{K}, \pi \models \psi_1$ and $\mathbf{K}, \pi \models \psi_2$.

5 ***temporal operators***

- $\mathbf{K},\pi \models \mathbf{X}\psi$ iff $\mathbf{K},\pi^1 \models \psi$
- $\mathbf{K},\pi \models \psi_1 \mathbf{U} \psi_2$ iff for some j, $\mathbf{K},\pi^j \models \psi_2$, and for all $k<j$, $\mathbf{K},\pi^k \models \psi_1$

CTL language definition

CTL can be defined as the ***sub-labguage*** of **CTL*** by replacing items 3-5 of the above definition, by the following:

3' if ϕ and ϕ' are ***state*** formulae, then $\mathbf{X}\phi$ and $\phi \mathbf{U} \phi'$ are ***path*** formulae.

0 If $\mathbf{p} \in \mathbf{AP}$, then **p** is a ***state*** formula.

1 If ϕ and ϕ' are ***state*** formulae, then so are $\neg \phi$ and $\phi \vee \phi'$, $\phi \wedge \phi'$.

2 If ψ is a ***path*** formula, then $\mathbf{E}\psi$ and $\mathbf{A}\psi$ are ***state*** formulae.

LTL, CTL and CTL*

LTL (state): $\varphi ::= \mathbf{A}\,\psi$

(path): $\psi ::= p \mid \neg\,\psi \mid \psi_1 \lor \psi_2 \mid \mathbf{X}\,\psi \mid \psi_1\,\mathbf{U}\,\psi_2$

CTL (state): $\varphi ::= p \mid \neg\,\varphi \mid \varphi_1 \lor \varphi_2 \mid \mathbf{E}\,\psi$

(path): $\psi ::= \mathbf{X}\,\varphi \mid \varphi_1\,\mathbf{U}\,\varphi_2$

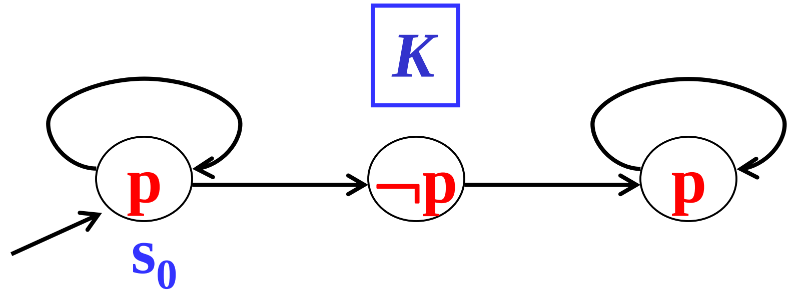
CTL* (state): $\varphi ::= p \mid \neg\,\varphi \mid \varphi_1 \lor \varphi_2 \mid \mathbf{E}\,\psi$

(path): $\psi ::= \varphi \mid \neg\,\psi \mid \psi_1 \lor \psi_2 \mid \mathbf{X}\,\psi \mid \psi_1\,\mathbf{U}\,\psi_2$

LTL and CTL*

Theorem:**[**Clarke**]** For every **CTL*** formula **ψ**, an equivalent **LTL** (it it exists) must be of the form **A*f*(ψ)** where ***f*(ψ)** is equal to **ψ** with all the path quantifiers eliminated.

LTL vs CTL

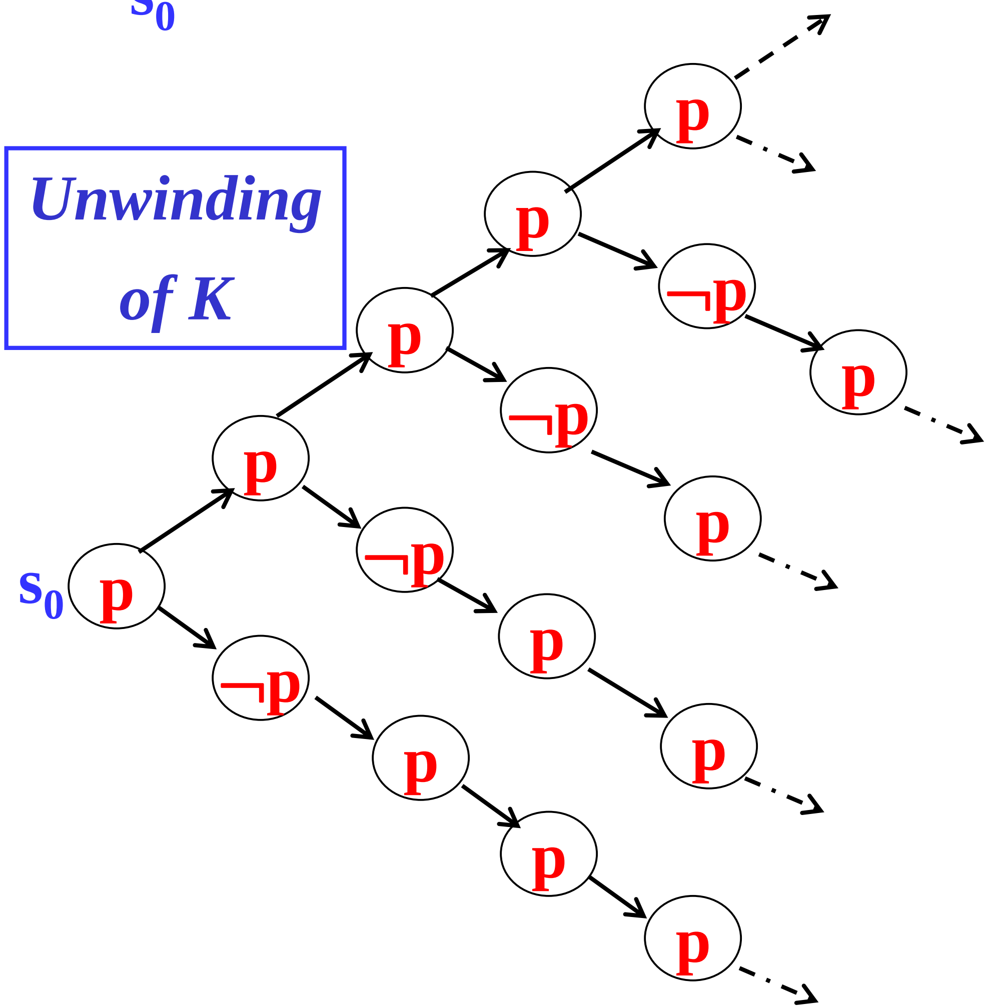


In LTL, we could write:
A FG *p* , which means "on all paths, there is some state from which *p* will forever hold" (i.e. ¬ *p* holds finitely often). `

There is no equivalent of this LTL formula in CTL.

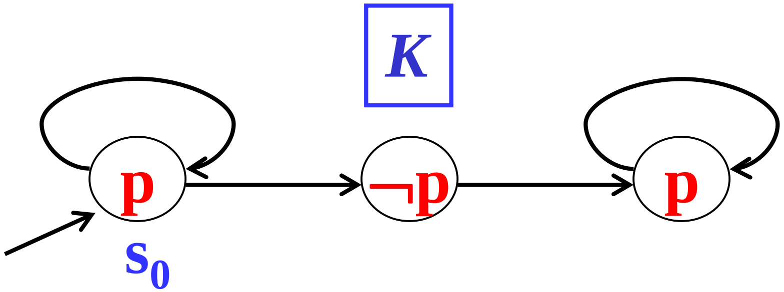
For example, in the following model, **A FG *p*** holds, but the formula **AF AG *p*** does not.

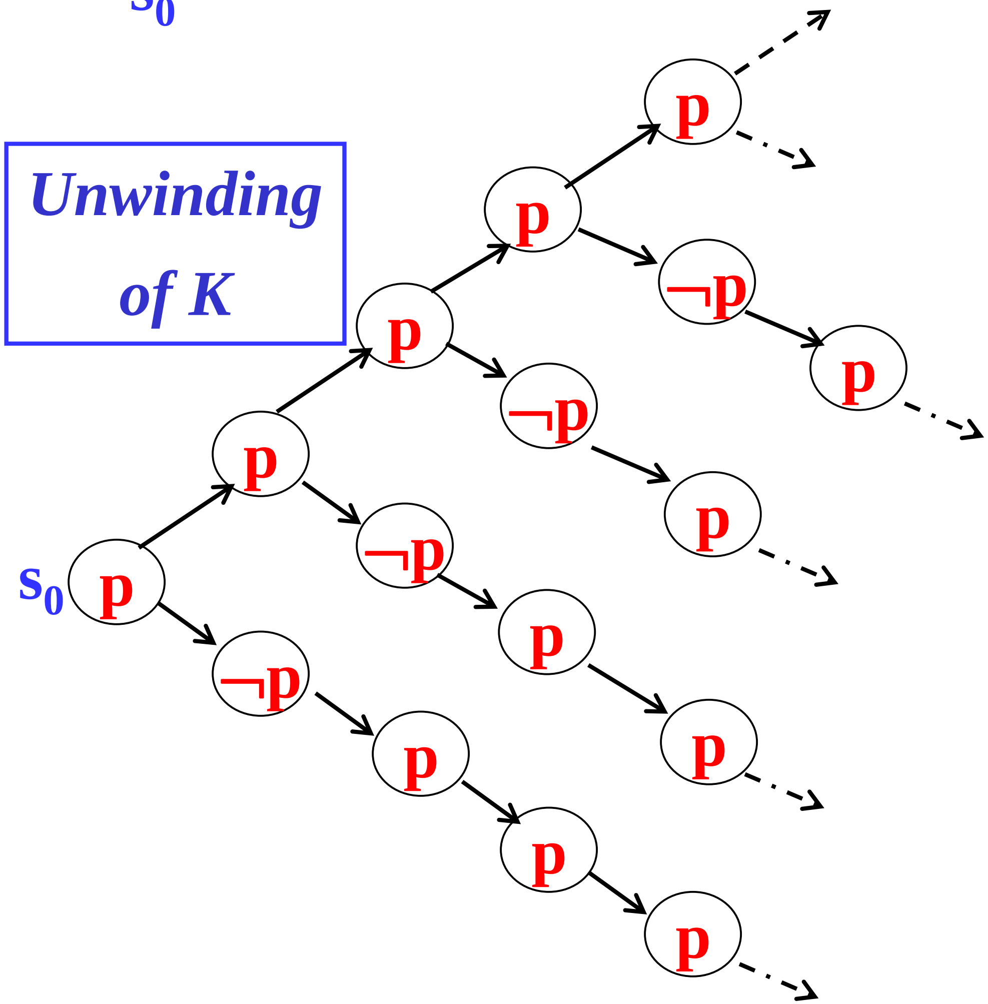
Unwinding of K



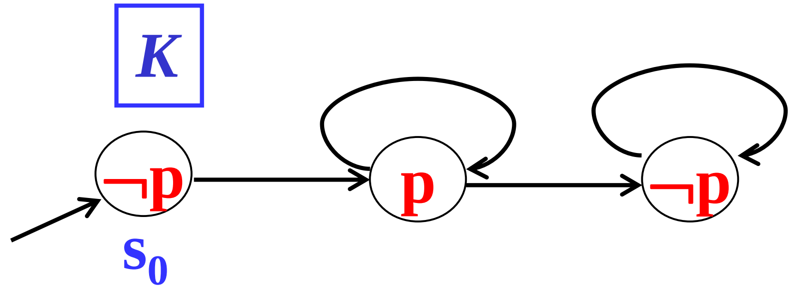
LTL vs CTL

Similarly the LTL formula **AF(*p* ∧ X *p*)** has no equivalent in CTL.
Two attempts are:
AF(*p* ∧ AX *p*)
But in the model on the right, the LTL formula is true while the CTL formula is false

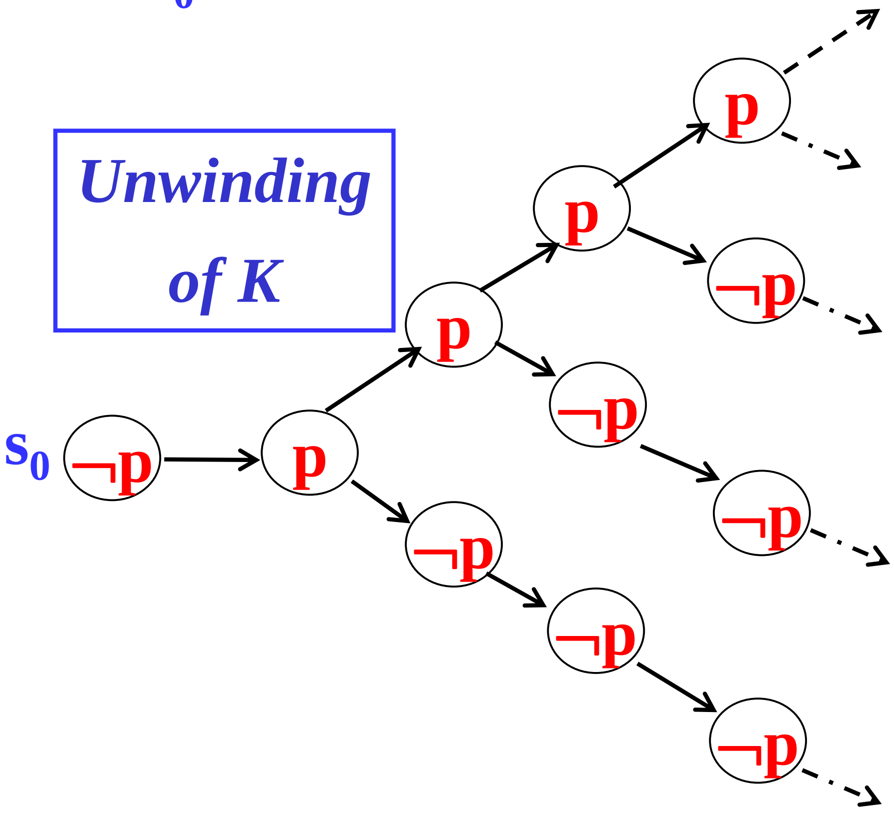




LTL vs CTL



Similarly the LTL formula **AF(p ∧ X p)** has no equivalent in CTL.
Two attempts are:
AF(p ∧ AX p)
and
AF(p ∧ EX p)
But in the model on the right, the LTL formula is false while the second CTL formula is true.



LTL vs CTL

The LTL formula **A GF *p*** means "on all paths and for all states, a state is reachable where ***p*** holds" (i.e. ***p*** holds infinitely often).

There is an equivalent CTL formula for this LTL formula.

The equivalent CTL formula is **AGAF *p*** which holds in all and only the models where **A GF *p*** holds.

Proof: It suffices to show that for any kripke structure ***K***, ***K*** $\models$ **AGAF *p*** iff ***K*** $\models$ **A GF *p***.

LTL vs CTL

The LTL formula φ = $\mathbf{A(GF}p \rightarrow \mathbf{F}q)$ (meaning that $\mathbf{F}q$ holds on all fair paths satisfying p infinitely often) cannot be expressed in CTL.

Proof: It suffices to show that for any candidate CTL formula ψ, there is at least a kripke structure K, with either

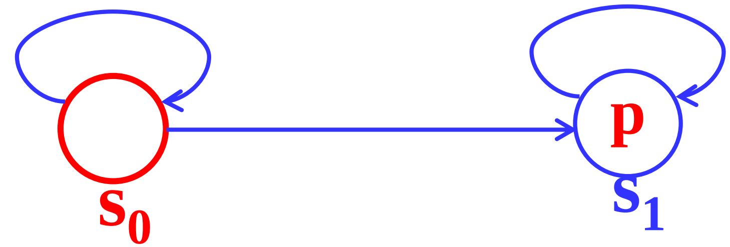
$K \models \varphi$ and $K \not\models \psi$

or

$K \not\models \varphi$ and $K \models \psi$.

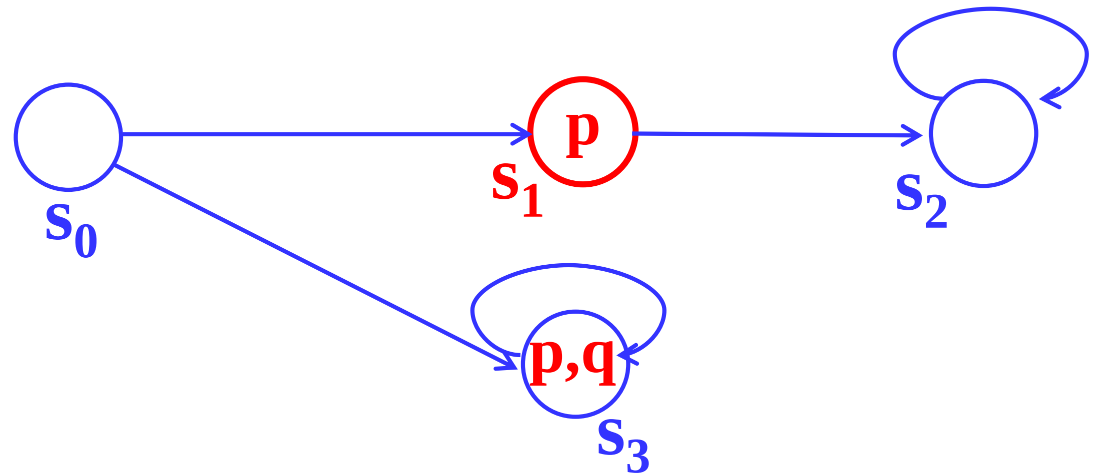
$$\varphi = \mathbf{A}(\mathbf{GF}p \rightarrow \mathbf{F}q)$$

$\psi = \mathbf{AGAF}\ p \rightarrow \mathbf{AF}q$



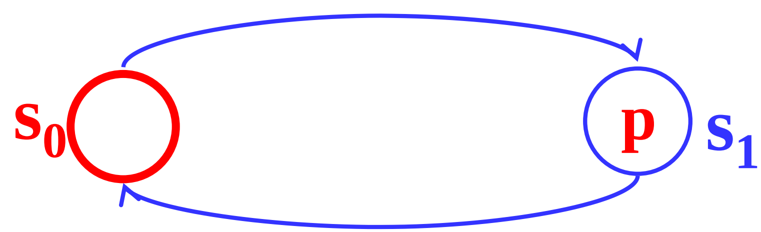
$\boxed{K \not\models \varphi \text{ and } K \models \psi}$

$\psi = \mathbf{AG}(\mathbf{AF}\ p \rightarrow \mathbf{AF}q)$



$\boxed{K \models \varphi \text{ and } K \not\models \psi}$

$\psi = \mathbf{AGAF}\ (p \rightarrow \mathbf{AF}q)$



$\boxed{K \not\models \varphi \text{ and } K \models \psi}$

CTL vs LTL

Let us consider the **CTL** formula **AGEF** α. Clearly:

$$K \models AG(EF\ \alpha)$$

Suppose β is a **LTL** formula which is ***equivalent*** to **AGEF** α. If this where true, then:

$$K \models \beta$$

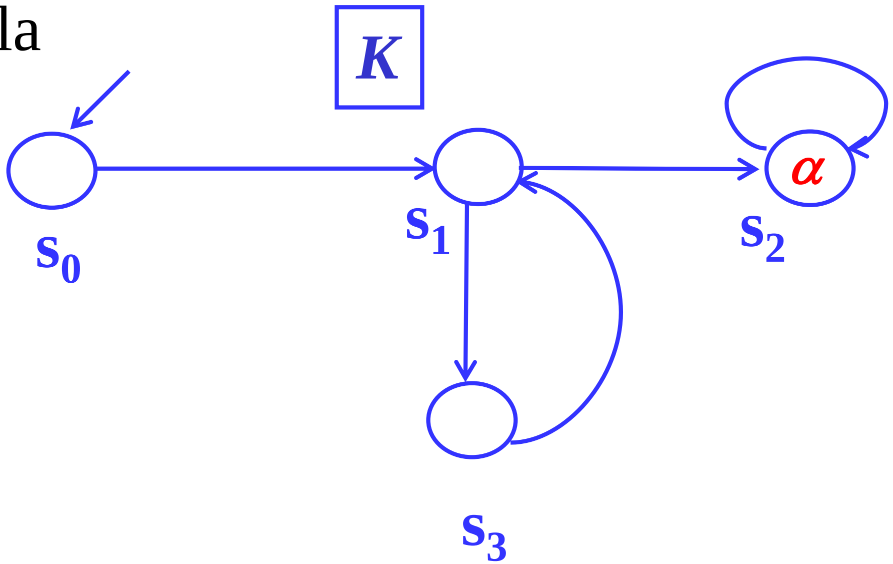
But $K \models \beta$ if and only if for every path π of K

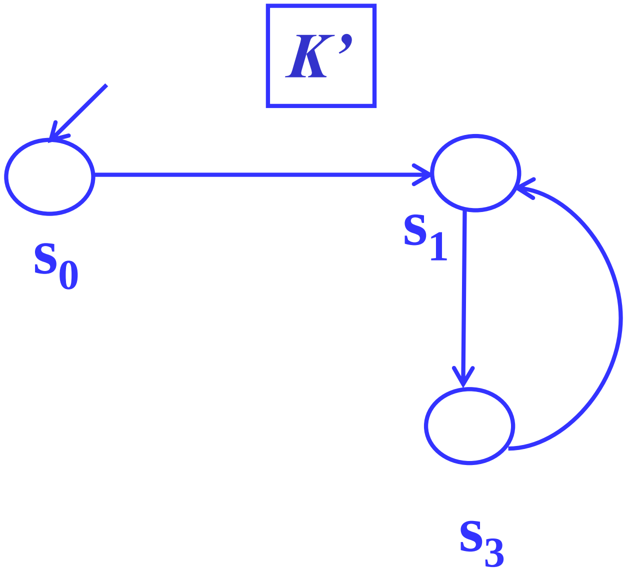
$$K, \pi \models \beta$$

Since any path π in K' is also in K, this would imply that for every path π of K'

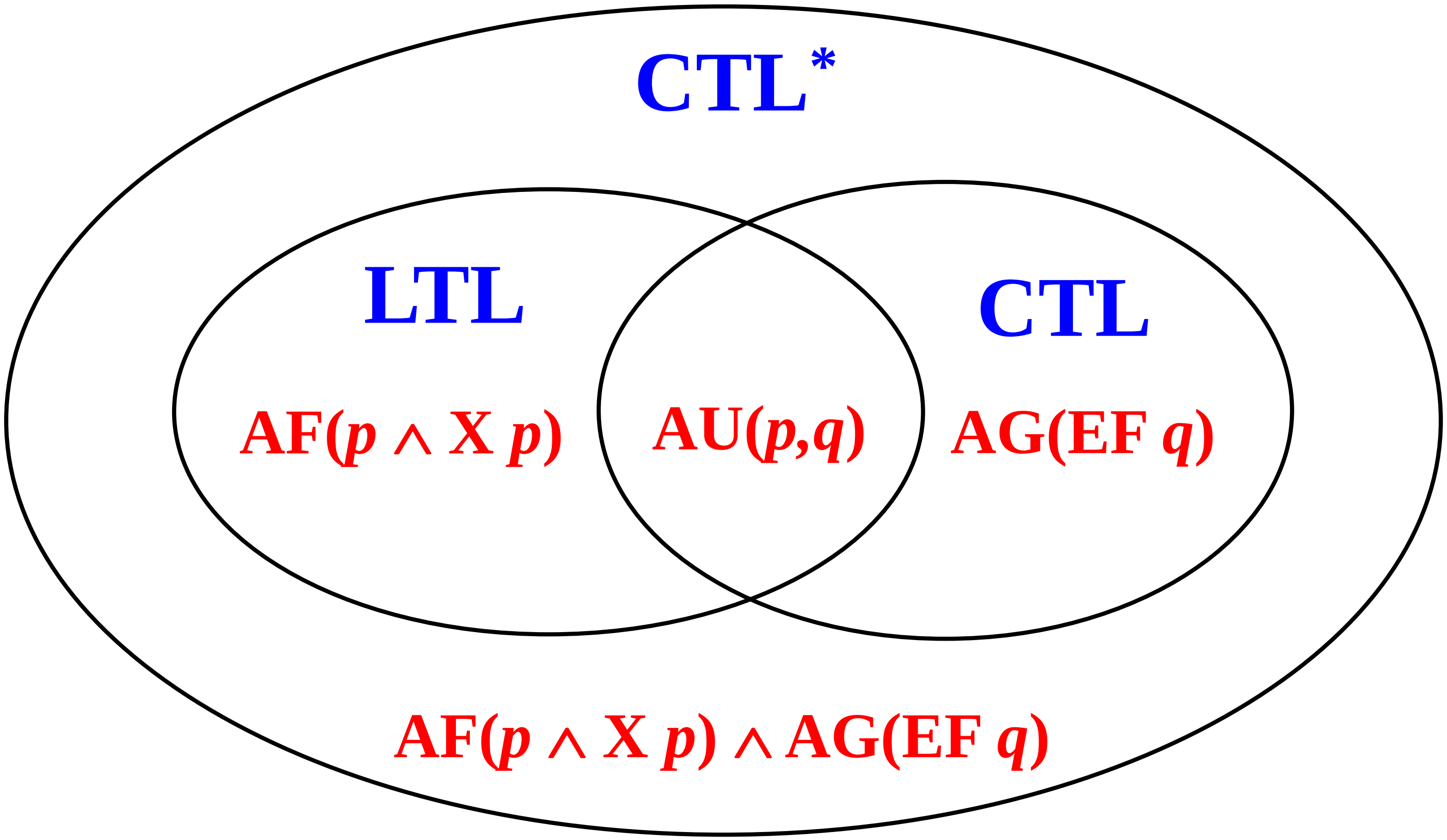
$$K', \pi \models \beta$$

But $K' \models AG(EF\ \alpha)$, therefore the **LTL** formula β cannot be equivalent to **AGEF** α.





LTL vs CTL vs CTL*



LTL vs CTL vs CTL*

- **A GF φ is a LTL formula which *can be expressed* in CTL by the *equivalent* formula AG AF φ.**
- **For any φ and ψ the LTL formula A(GF φ → ψ) is *not expressible* in CTL, in particular it is *not equivalent to* ((AG AF φ) → ψ).**
- **In other words, *fairness constraints cannot be expressed* directly in CTL.**