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 **p** ∈ **AP**, then **p** is a ***state*** formula.

1 If ψ and ψ' are ***state*** formulae, then so are ¬ψ and ψ ∨ ψ', ψ ∧ ψ'.

2 If ψ and ψ' are ***path*** formulae, then **E**ψ and **A**ψ are ***state*** formulae .

CTL* language I

Syntax ...

(*path formulae*)

3 if ψ is a ***state*** formula, then ψ 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 **X**ψ and ψ**U**ψ'.

CTL* semantics I

Semantics Given the standard definitions

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

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

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

1 for ***propositional formulae***

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

2 $\mathbf{K,s \models E\psi}$ [$\mathbf{K,s \models A\psi}$] iff for some [for all] path

$\pi = s\, s_1\, s_2 \ldots$, it holds $\mathbf{K,\pi \models \psi}$

CTL* semantics II

Semantics ...

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

4 for propositional formulare

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

5 ***temporal operators***

- $K,\pi \models X\psi$ iff $K,\pi^1 \models \psi$
- $K,\pi \models \psi U \psi'$ iff for some $j \geq 0$, $K,\pi^j \models \psi'$, and for all $0 \leq k < j$, $K,\pi^k \models \psi$

CTL language definition

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

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

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

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

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

LTL, CTL and CTL*

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

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

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

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

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

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

LTL and CTL*

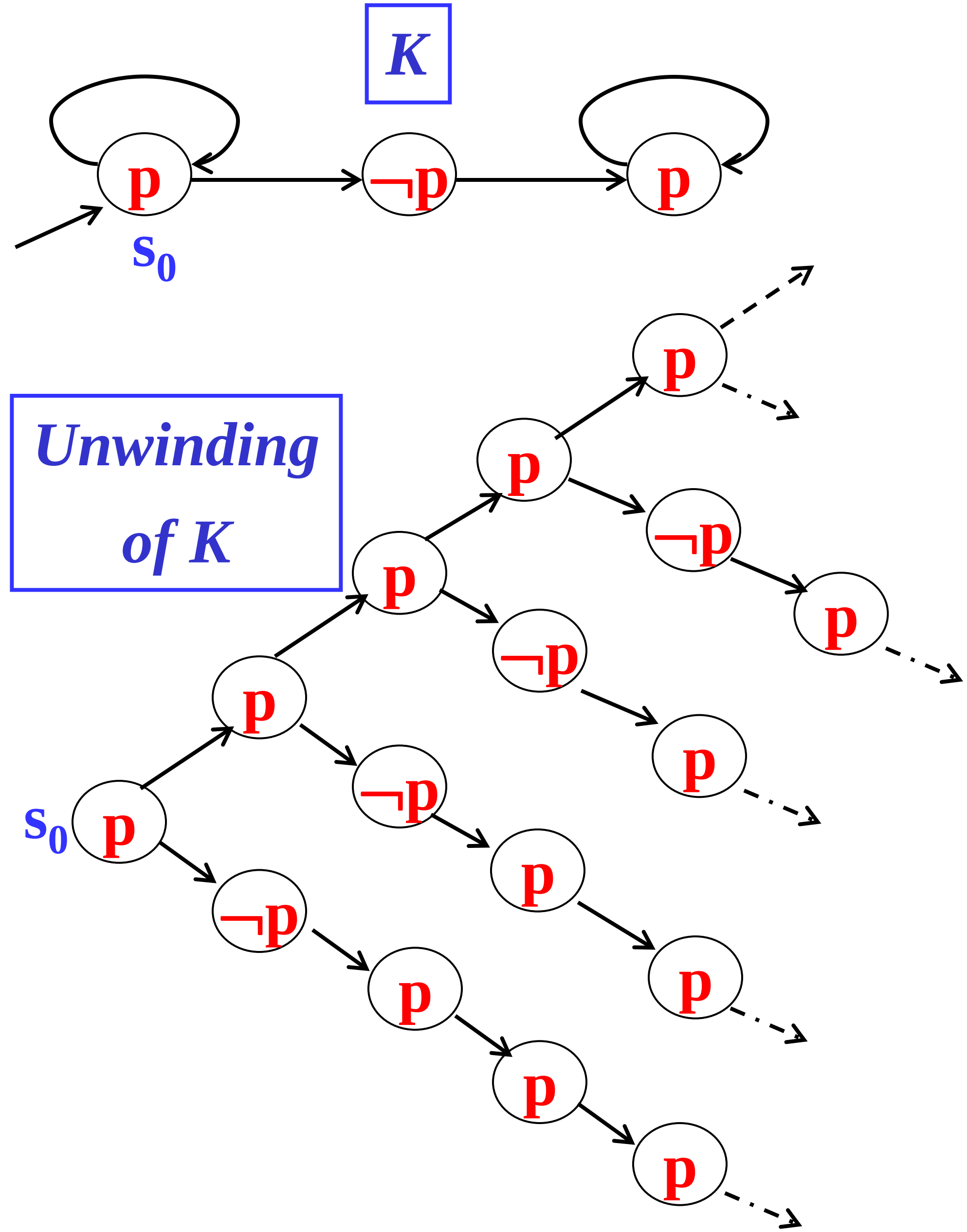
Theorem:*[**Clarke**]** For every **CTL formula **ψ**, an equivalent **LTL** (if it exists) must be of the form **A *f*(ψ)**, where ***f*(ψ)** is equal to **ψ** with all the path quantifiers eliminated.

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).

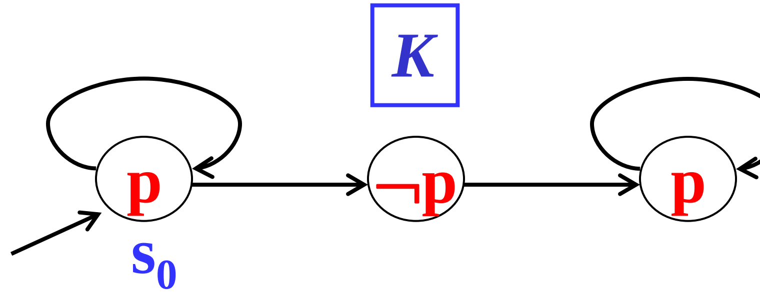
There is no equivalent of this LTL formula in CTL.

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



LTL vs CTL

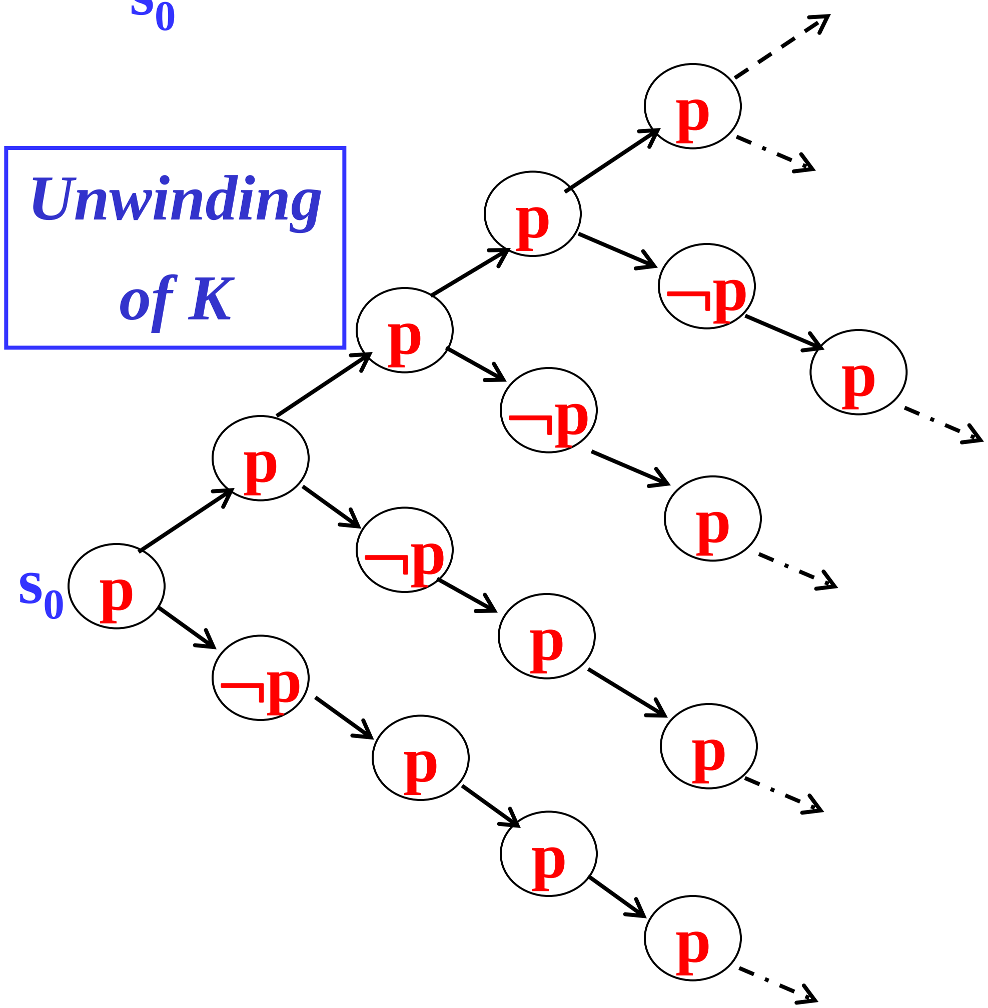
Similarly the **LTL** formula **AF(*p* ∧ X *p*)** has no equivalent in CTL.



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 **$AF(p \wedge X\, p)$** has no equivalent in CTL.

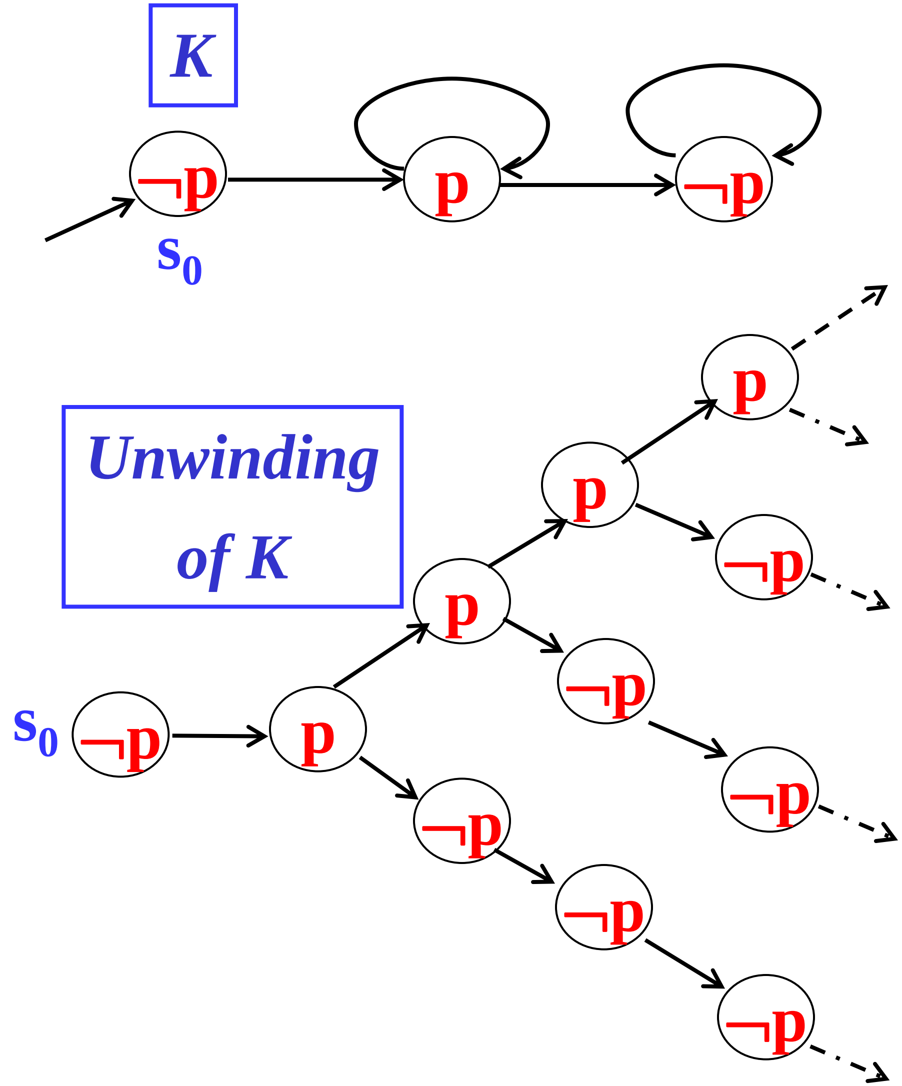
Two attempts are:

$AF(p \wedge AX\, p)$

and

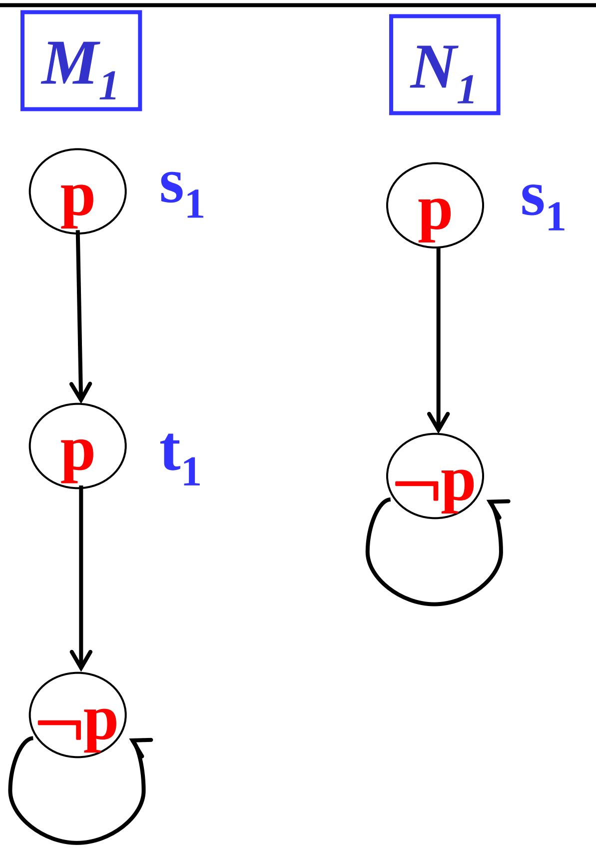
$AF(p \wedge EX\, p)$

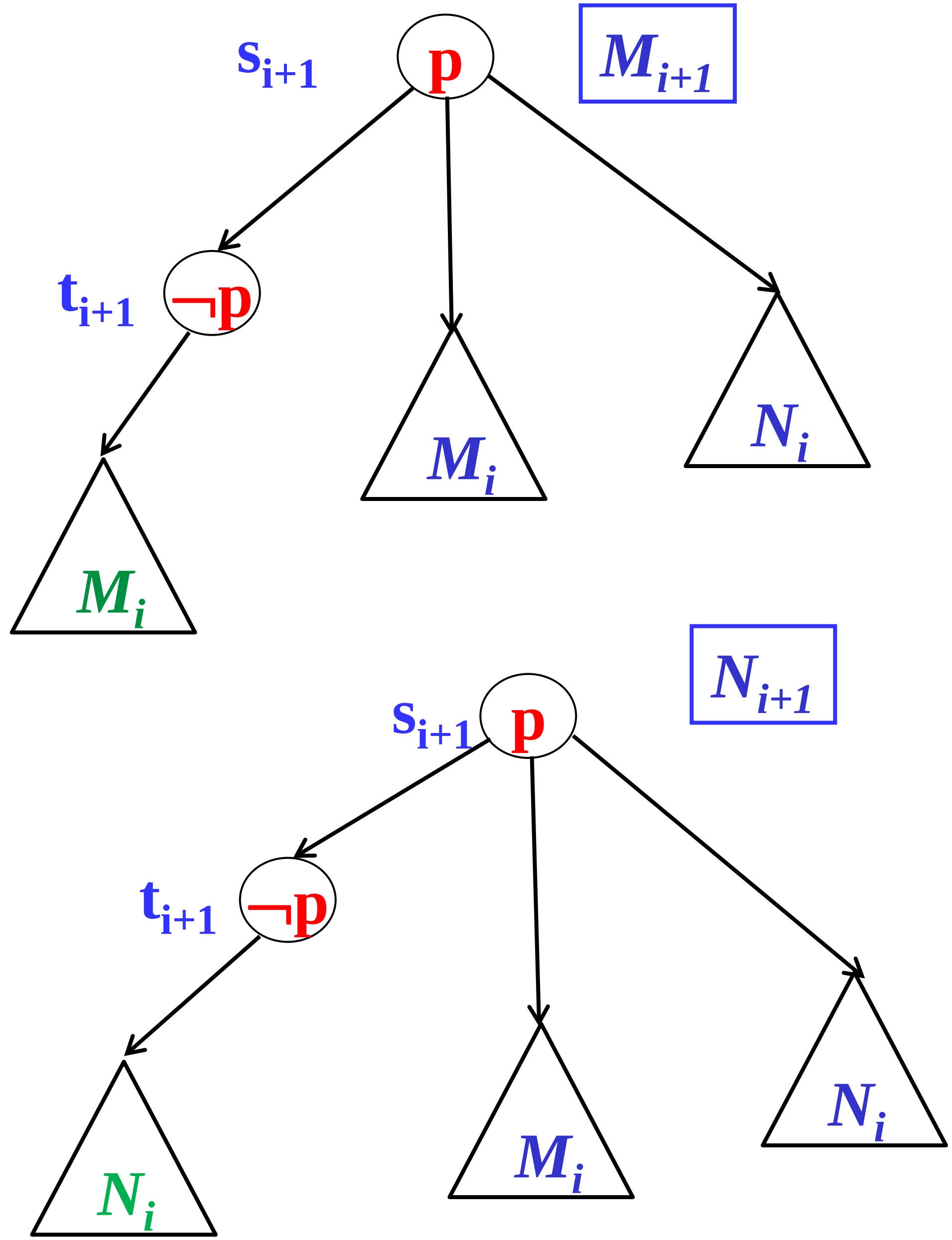
But in the model on the right, the LTL formula is false while the second CTL formula is true.



LTL vs CTL: AF($p \wedge$ X p)

Let us build ***two sequences of Kripke structures***, **M_1, M_2**, … and **N_1, N_2**, … defined inductively as follows.



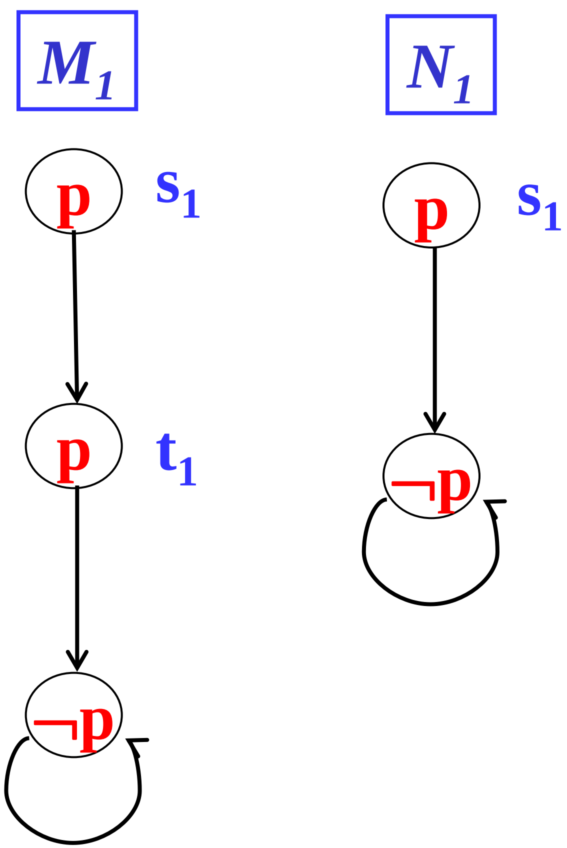


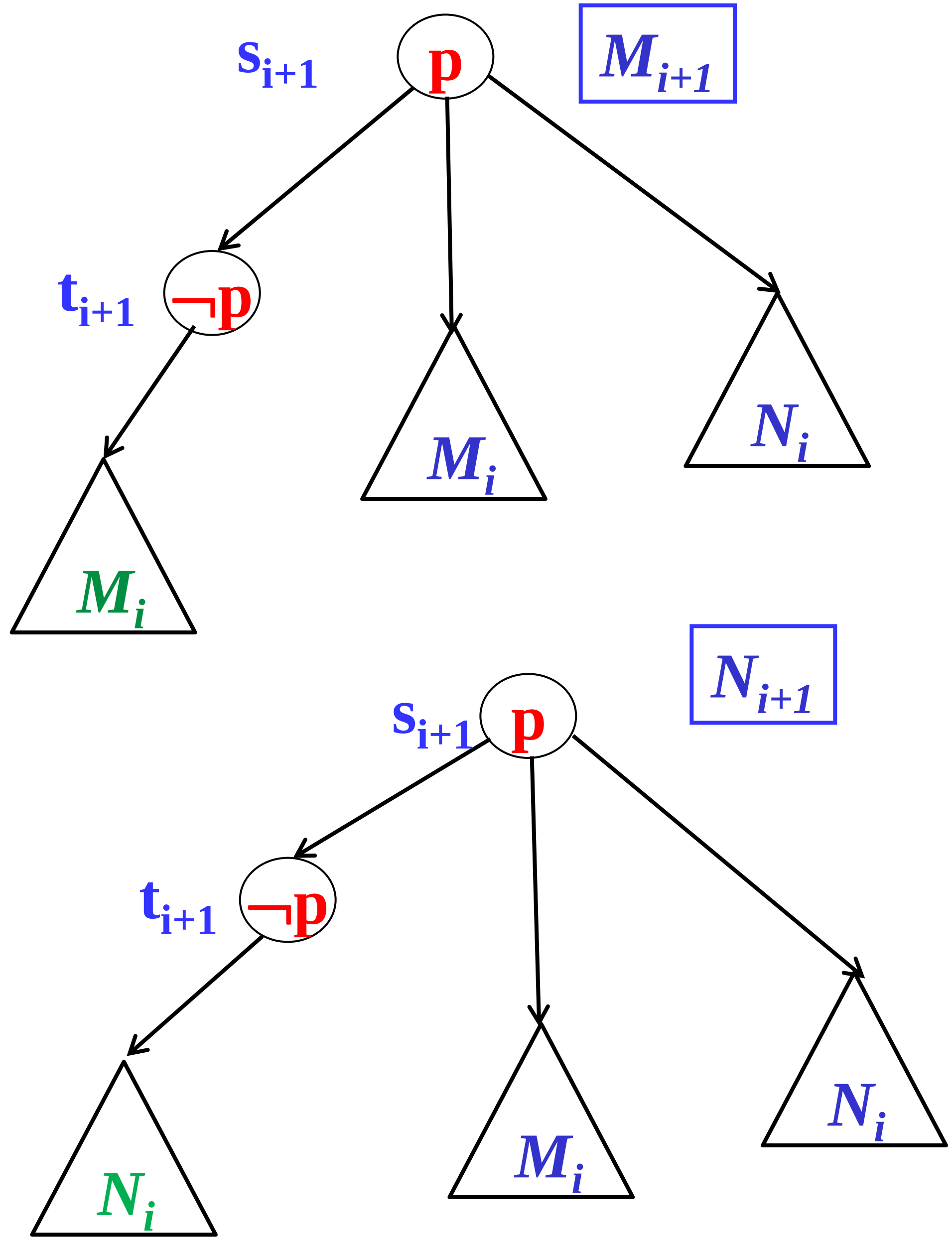
LTL vs CTL: AF($p \wedge X\, p$)

For all $i \geq 1$ it holds that:

$M_i, s_i \models AF(p \wedge X\, p)$

$N_i, s_i \models \neg\, AF(p \wedge X\, p)$

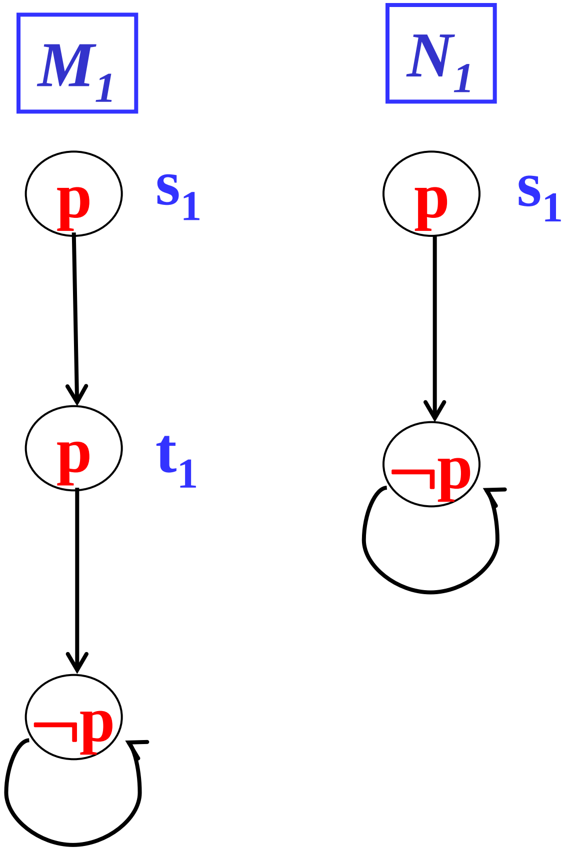


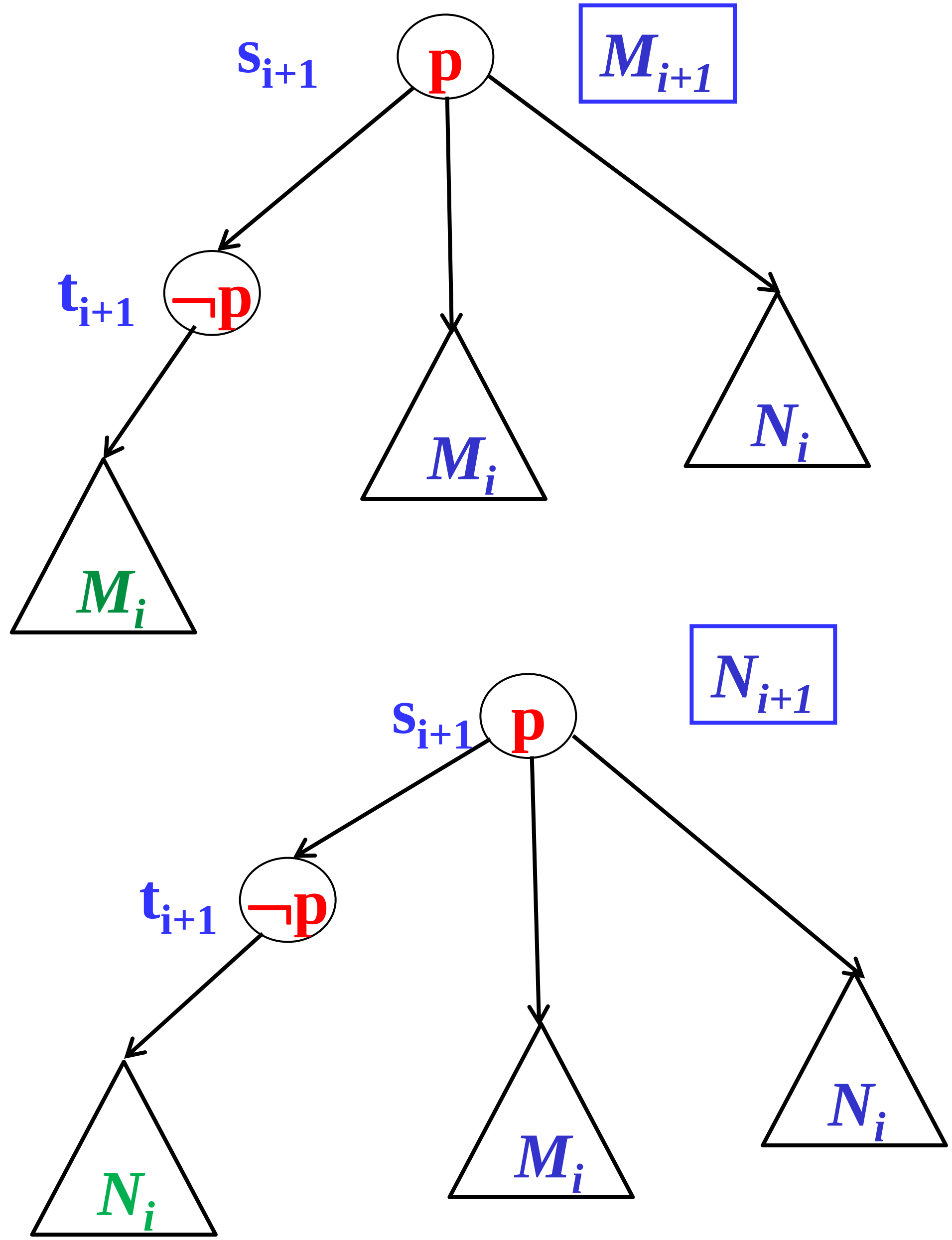


LTL vs CTL: AF($p \wedge X\, p$)

For all $i \geq 1$ and all CTL formula ψ with $|\psi| \leq i$ it holds that:

$$M_i, s_i \models \psi \quad \textit{iff} \quad N_i, s_i \models \psi$$

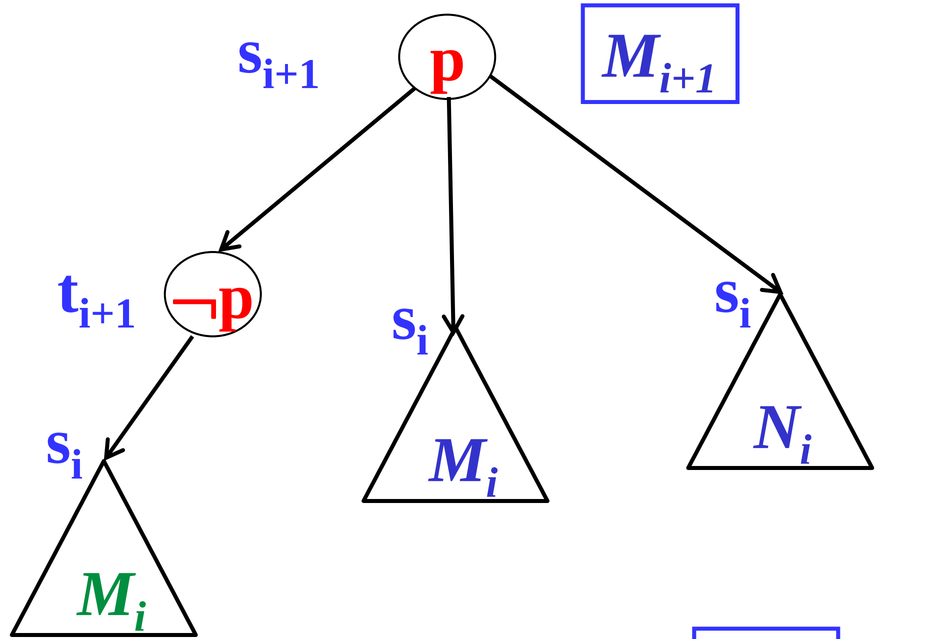




LTL vs CTL: AF($p \wedge$ X p)

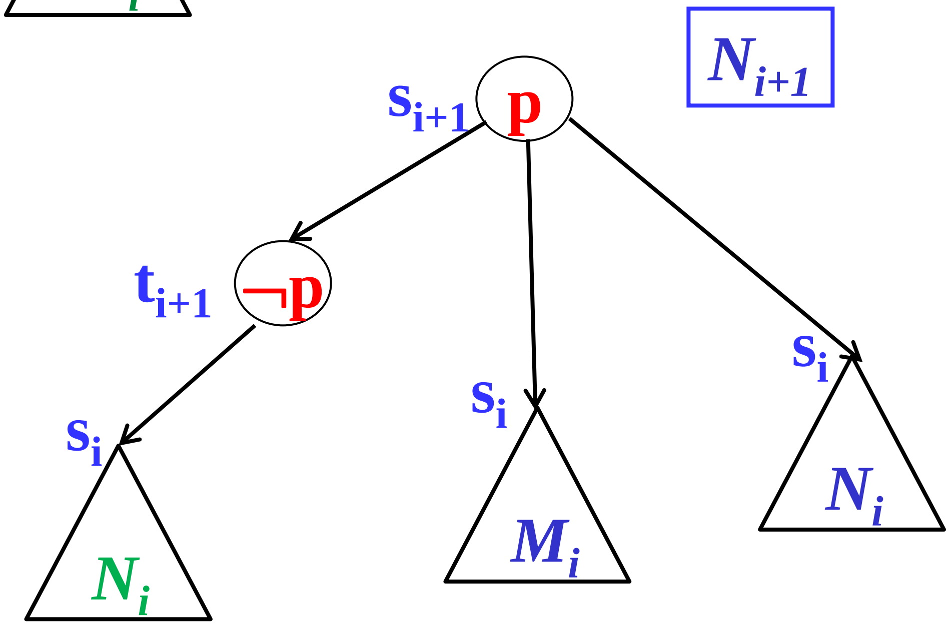
For all $\mathbf{i \geq 1}$ and for all **CTL** formula ψ with $|\psi| \leq \mathbf{i}$ it holds that:

$$M_i, s_i \models \psi \quad \textit{iff} \quad N_i, s_i \models \psi$$



Note 1: For any given $\mathbf{i \geq 1}$, it the above holds then for all **CTL** formula ϕ with $|\phi| \leq \mathbf{i}$:

$$M_{i+1}, s_i \models \phi \quad \textit{iff} \quad N_{i+1}, s_i \models \phi$$



Note 2: Which, in turn, implies that if $|\phi| \leq \mathbf{i}$ then it holds that:

$$M_{i+1}, t_{i+1} \models \phi \quad \textit{iff} \quad N_{i+1}, t_{i+1} \models \phi$$

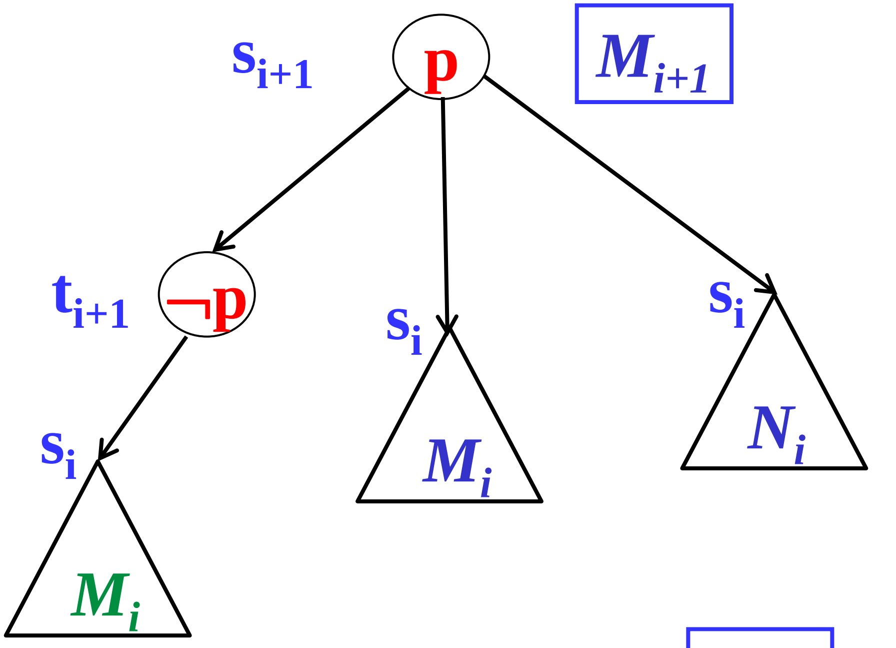
LTL vs CTL: $AF(p \wedge X\, p)$

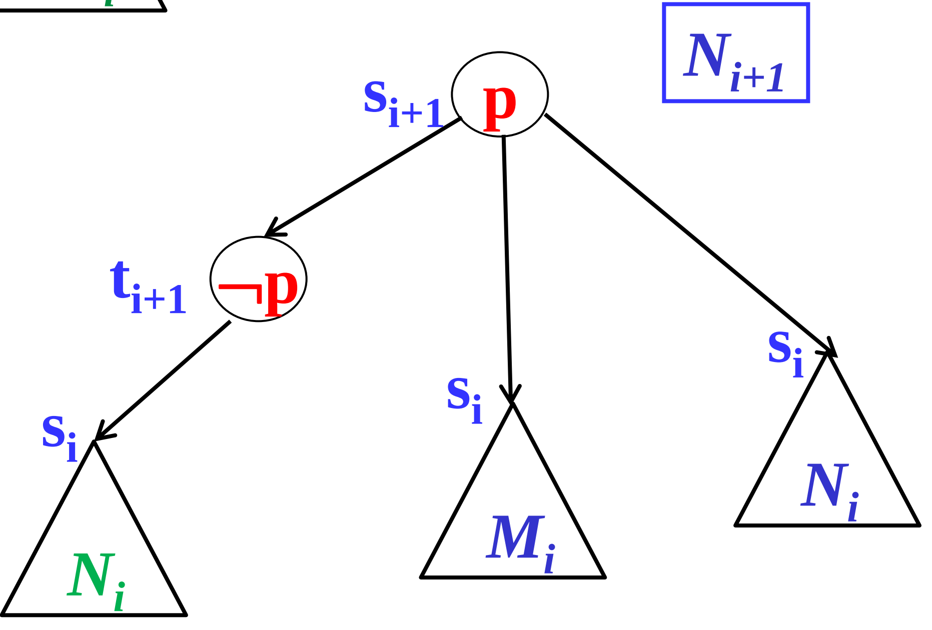
For all $i \geq 1$ and all **CTL** formula ψ with $|\psi| \leq i$ it holds that:

$$M_i, s_i \models \psi \quad \textit{iff} \quad N_i, s_i \models \psi$$

Can be proved by induction on **i**.

The base case is immediate as for **i=1** it must be that the CTL formila ψ is an atomic proposition M_1 and N_1 clearly satisfy the same atoms in s_1.





LTL vs CTL: $AF(p \wedge X\, p)$

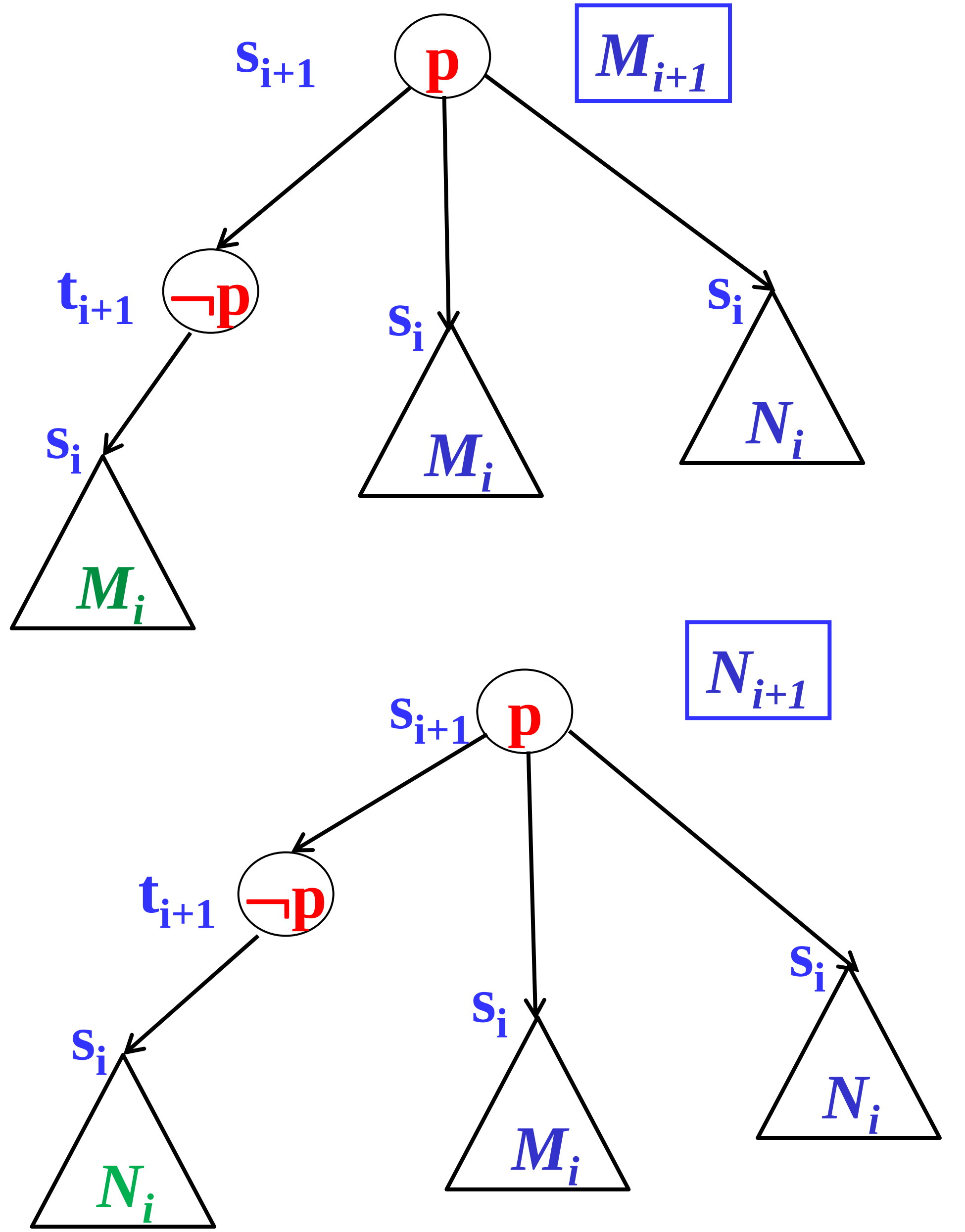
For all $i \geq 1$ and all CTL formula ψ with $|\psi| \leq i$ it holds that:

$$M_i, s_i \models \psi \quad \textit{iff} \quad N_i, s_i \models \psi$$

Can be proved by induction on **i**.

For **i>1**, ψ must be of one of the following forms:

- $\psi_1 \wedge \psi_2$
- $\neg\psi$
- $EX\ \psi_1$
- $EU(\psi_1, \psi_2)$
- $AU(\psi_1, \psi_2)$



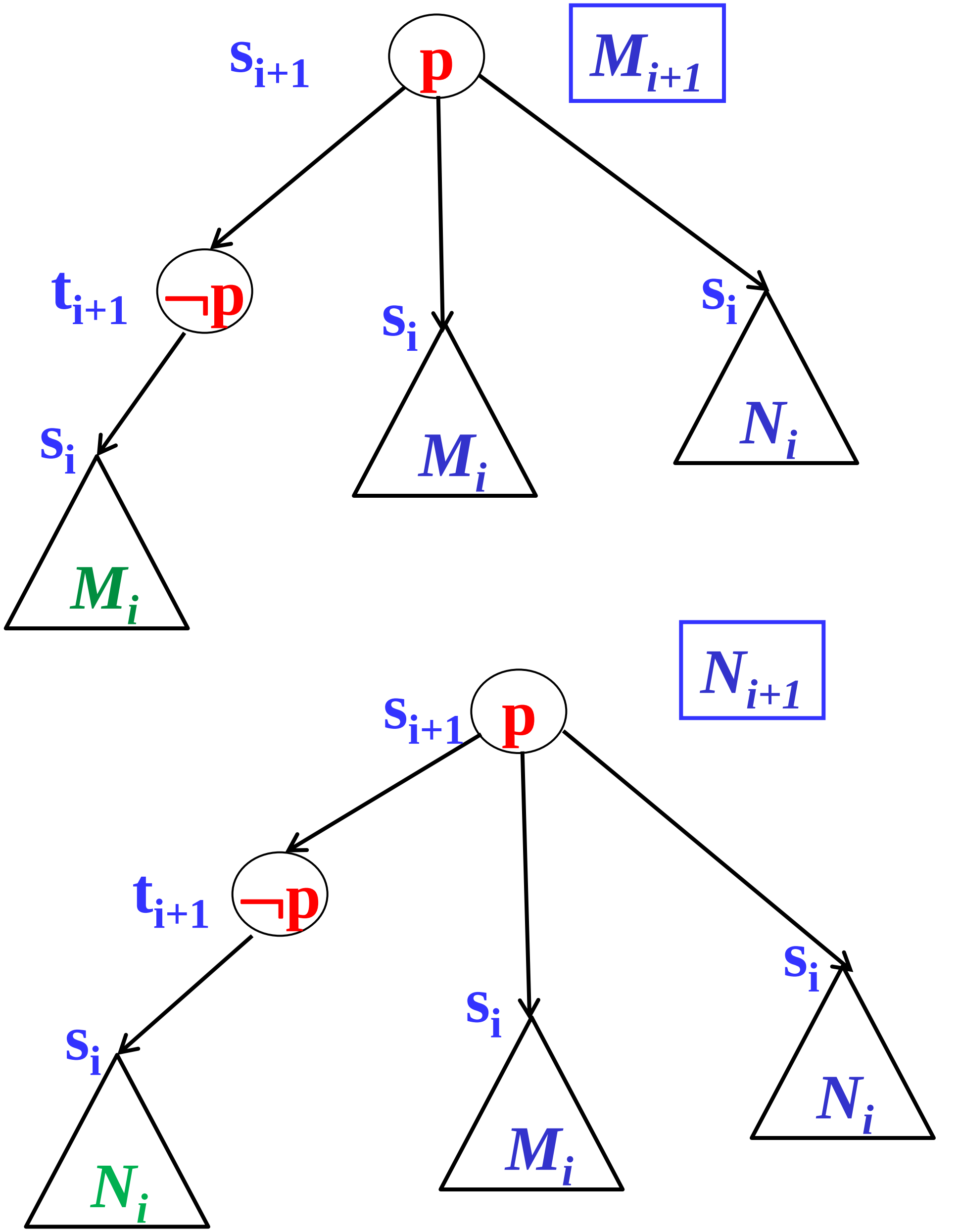
LTL vs CTL: AF($p \wedge X\, p$)

For all $i \geq 1$ and all CTL formula ψ with $|\psi| \leq i$ it holds that:

$$M_i, s_i \models \psi \quad \textit{iff} \quad N_i, s_i \models \psi$$

- $\psi = \psi_1 \wedge \psi_2$ of length $\leq i+1$

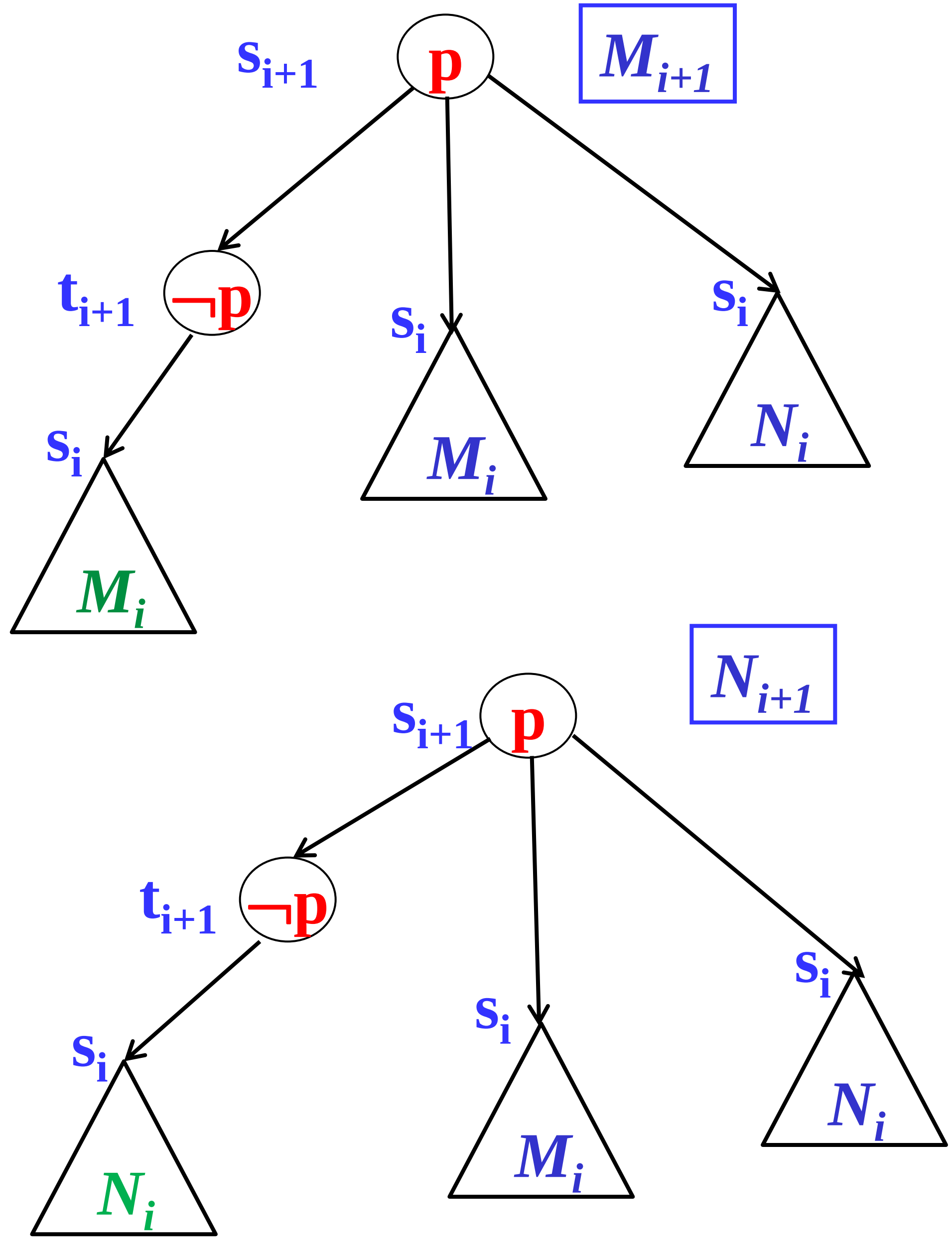
In this case, ψ_1 and ψ_2 have length $\leq i$. By the inductive hypothesis, then $M_i, s_i \models \psi'$ *iff* $N_i, s_i \models \psi'$ for all ψ' of length $\leq i$. Since M_{i+1} and N_{i+1} only differ on the leftmost subtree which cannot distinguish between formulas of length $\leq i$, we conclude that $M_{i+1}, s_{i+1} \models \psi_k$ *iff* $N_{i+1}, s_{i+1} \models \psi_k$ (with k=1,2), and the conclusion follows.



LTL vs CTL: AF($p \wedge X\, p$)

- ψ = EX ψ_1 of length $\leq$ i+1 with ψ_1 of length $\leq$ i. Then, $M_{i+1}, s_{i+1} \models \psi$ *iff*
- $M_{i+1}, t_{i+1} \models \psi_1$ or $M_i, s_i \models \psi_1$ or
- $N_i, s_i \models \psi_1$.

Consider the first case. By the inductive hypothesis, we have $M_i, s_i \models \psi_1$ *iff* $N_i, s_i \models \psi_1$, which implies (see **Note 2**) $M_{i+1}, t_{i+1} \models \psi_1$ *iff* $N_{i+1}, t_i \models \psi_1$, and the conclusion follows. The other cases are even easer.



LTL vs CTL: AF($p \wedge X\, p$)

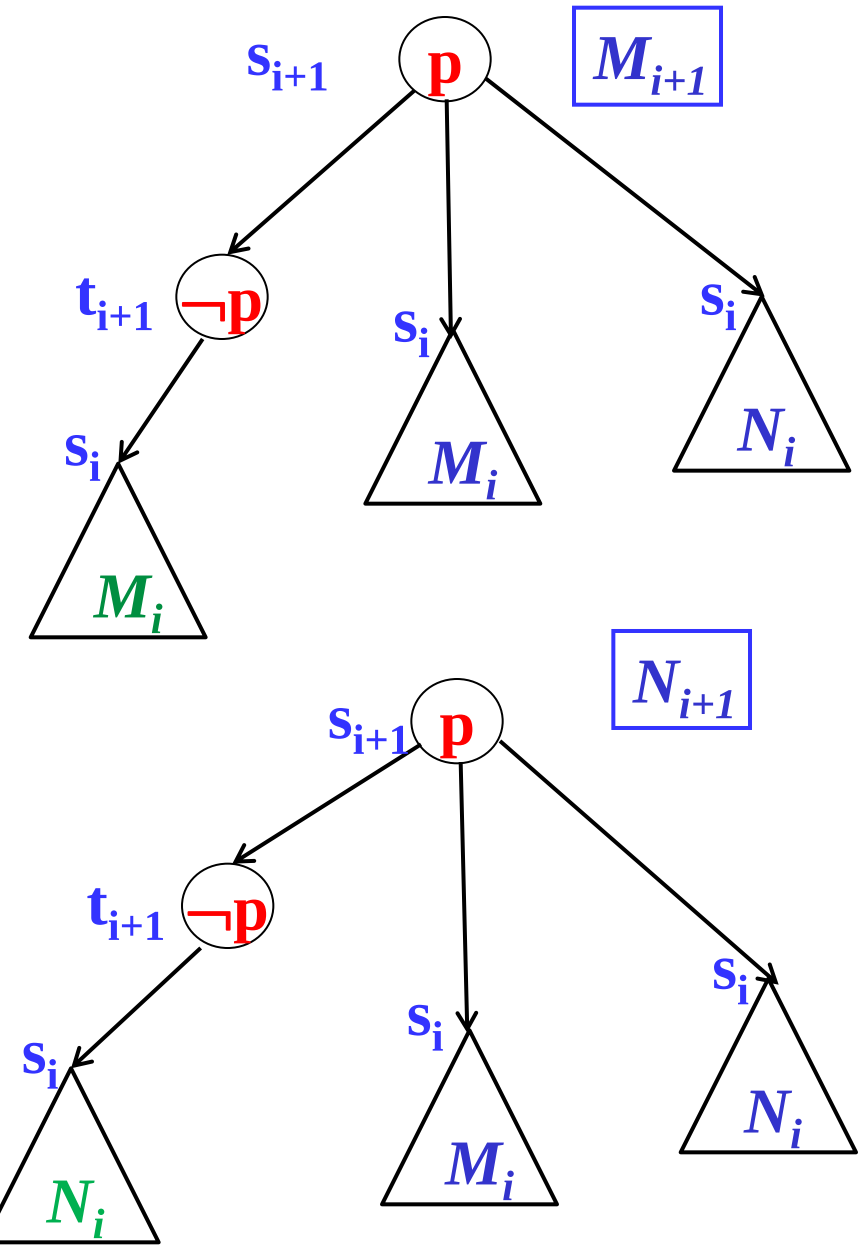
- $\psi = EU(\psi_1,\psi_2)$ of length $\leq$ **i+1**

with ψ_1,ψ_2 of length $\leq$ **i**. Then, we have that $M_{i+1}, s_{i+1} \models \psi$ *iff*

- $M_{i+1}, s_{i+1} \models \psi_2$
- or $M_{i+1}, s_{i+1} \models \psi_1$ and $M_{i+1}, t_{i+1} \models \psi_2$
- or $M_{i+1}, s_{i+1} \models \psi_1$ and $M_i, s_i \models EU(\psi_1,\psi_2)$
- or $M_{i+1}, s_{i+1} \models \psi_1$ and $N_i, s_i \models EU(\psi_1,\psi_2)$.

The *latter two cases* immediately imply the conclusion.

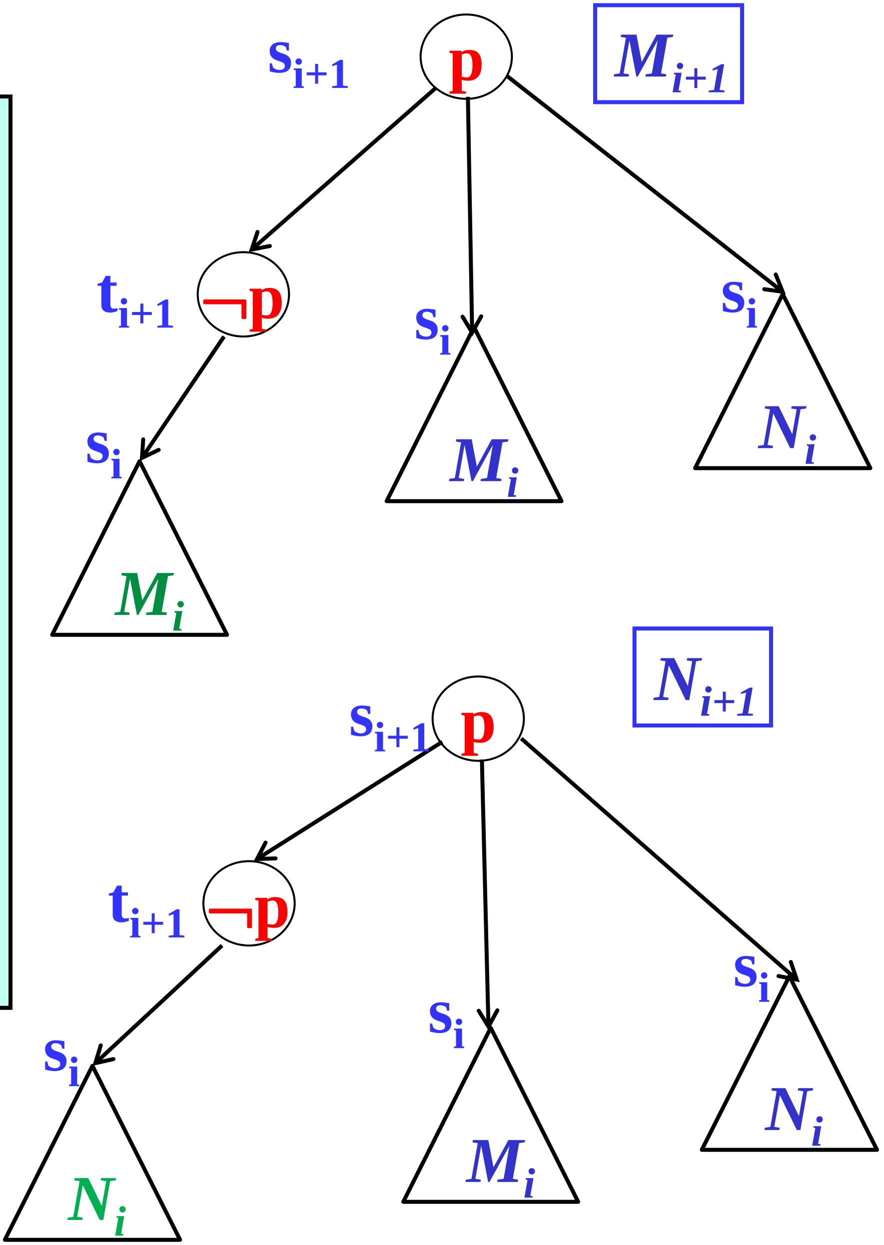
The *first case* follows immediately from the inductive hypothesis, while the *second case* follows by using the inductive hypothesis together with **Note 1** and **Note 2**.



LTL vs CTL: AF($p \wedge X\, p$)

- $\psi = AU(\psi_1,\psi_2)$ of length $\leq i+1$ with ψ_1,ψ_2 of length $\leq i$. Then, we have that $M_{i+1}, s_{i+1} \models \psi$ *iff*
- $M_{i+1}, s_{i+1} \models \psi_2$
- or $M_{i+1},s_{i+1} \models \psi_1$ and $M_{i+1},t_{i+1} \models \psi_1$ and $M_i,s_i \models AU(\psi_1,\psi_2)$ and $N_i, s_i \models AU(\psi_1,\psi_2)$
- or $M_{i+1},s_{i+1} \models \psi_1$ and $M_{i+1},t_{i+1} \models \psi_2$ and $M_i,s_i \models AU(\psi_1,\psi_2)$ and $N_i, s_i \models AU(\psi_1,\psi_2)$.

The reasoning is similar to the previous case and the conclusion follows.



LTL vs CTL: $AF(p \wedge X\, p)$

- Assume now that there exists a **CTL** formula ψ which is equivalent to the **LTL** formula $AF\,(p \wedge X\, p)$ and let $i = |\psi|$.

- Then, by the above property, $M_i, s_i \models \psi$ ***iff*** $N_i, s_i \models \psi$

- However, $M_i, s_i \models AF(p \wedge X\, p)$ but $N_i, s_i \not\models AF(p \wedge X\, p)$.

- This contradicts the equivalence between ψ and $AF(p \wedge X\, p)$.

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, it holds $K \models \mathbf{AGAF}\ p$ iff $K \models \mathbf{A\ GF}\ p$.

LTL vs CTL

The LTL formula φ = $\mathbf{A}(\mathbf{GF}p \rightarrow \mathbf{F}q)$ (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

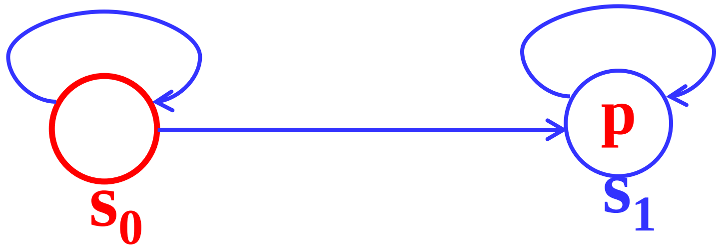
$$K \models \varphi \text{ and } K \not\models \psi$$

or

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

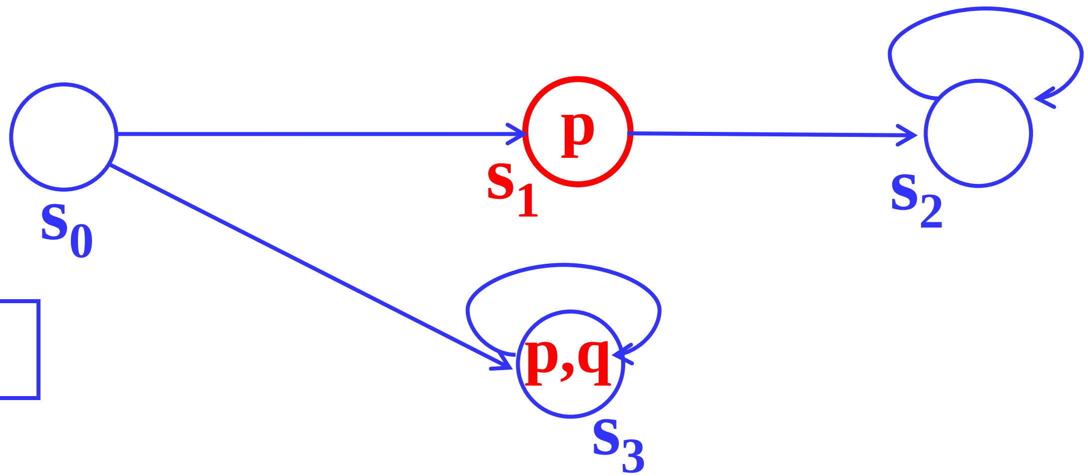
$$\varphi = \mathbf{A}(\mathbf{GF}p \rightarrow \mathbf{F}q)$$

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



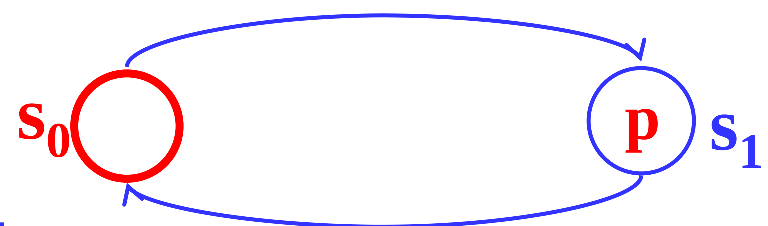
$K \not\models \varphi$ and $K \models \psi$

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



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

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



$K \not\models \varphi$ 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 were true, then:

$$K \models \beta$$

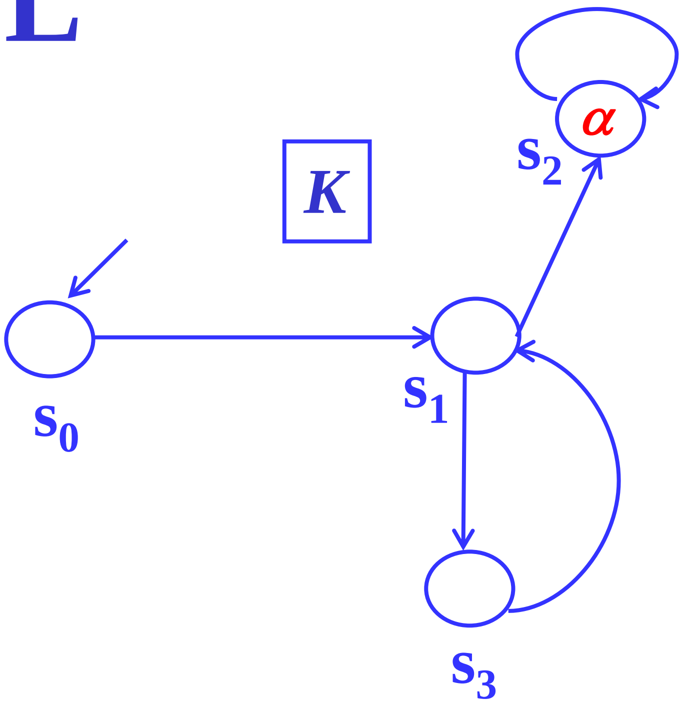
But $K \models \beta$ if and only if for every path π of K

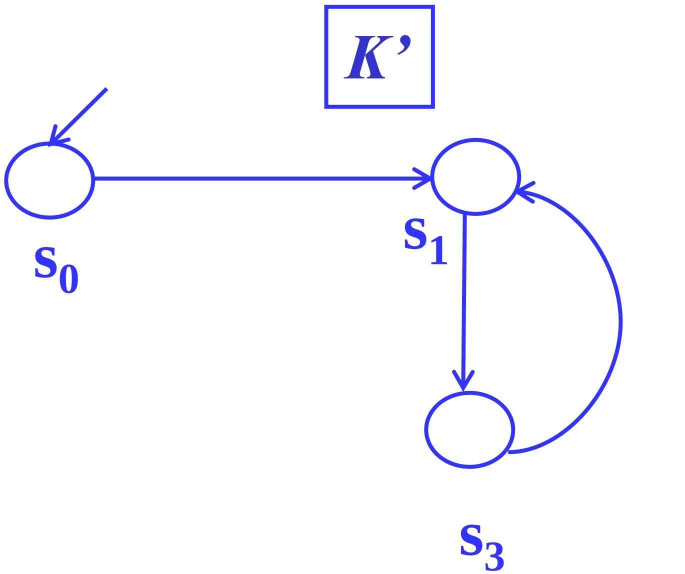
$$K, \pi \models \beta$$

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

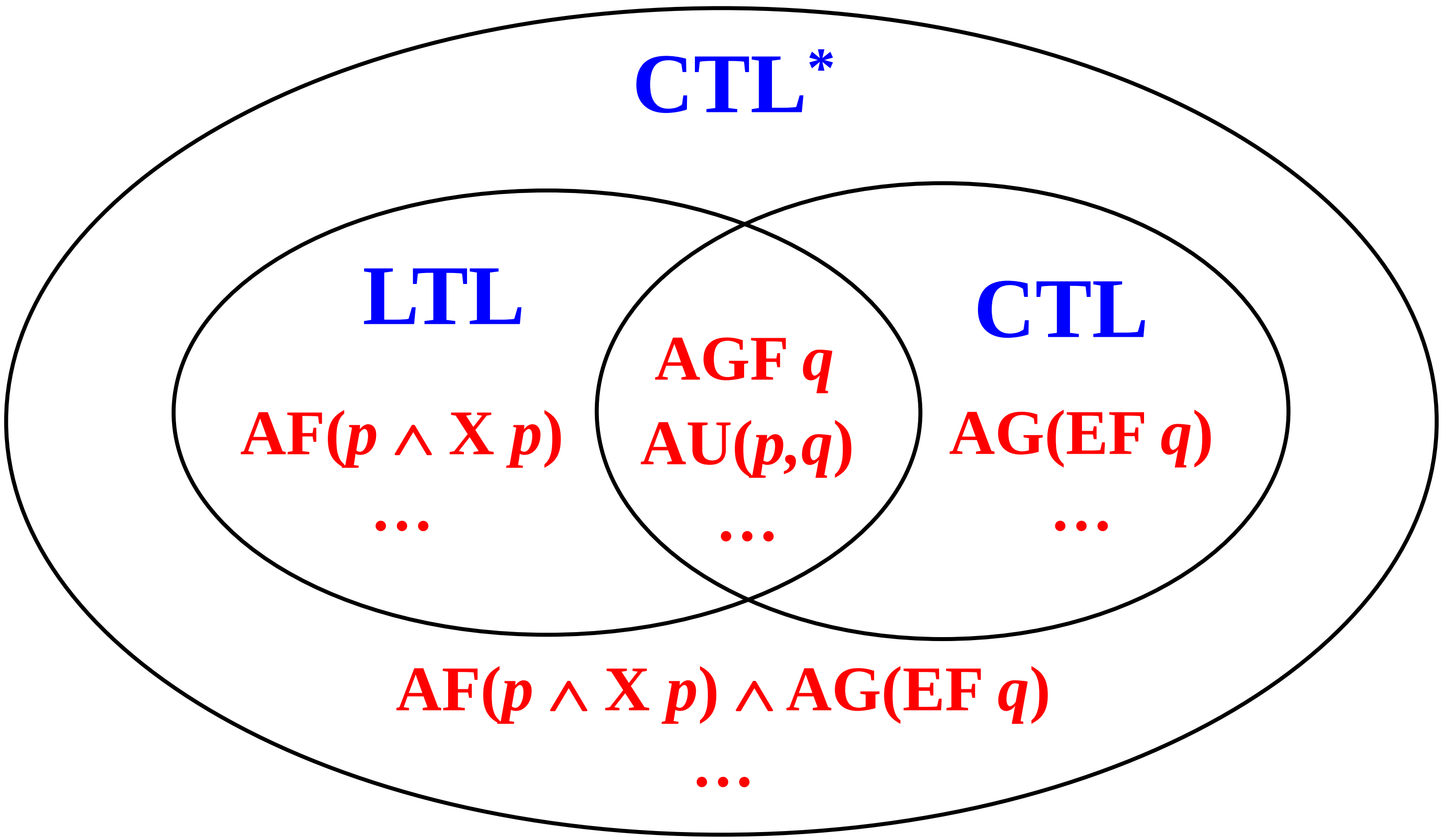
$$K', \pi \models \beta$$

But $K' \not\models AG(EF\ \alpha)$, 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.**