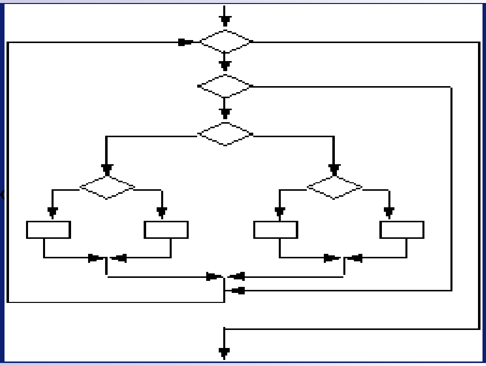
Spring 2007



# Program correctness

## Branching-time temporal logics

*Marcello Bonsangue*

Leiden Institute of Advanced Computer Science
Research & Education

# CTL

- CTL = Computational Tree Logic
  - the temporal combinators are under the immediate scope of the path quantifiers

- Why CTL? The truth of CTL formulas depends only on the current state and not on the current execution!

⇓

Benefit: easy and efficient model checking

Disadvantages: hard for describing individual path

# The language

- Path quantifiers allows to speaks about sets of executions.
  - The model of time is tree-like: many futures are possible from a given state
- Inevitably $A\phi$

  from the current state all executions satisfy $\phi$
- Possibly $E\phi$

  from the current state there exists an execution satisfying $\phi$

# CTL - Syntax

- $\phi ::= p_1 \mid p_2 \mid \ldots$

  $\top \mid \bot \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \Rightarrow \phi \mid$

  $AX\phi \mid AF\phi \mid AG\phi \mid A[\phi \; U \; \phi] \mid$

  $EX\phi \mid EF\phi \mid EG\phi \mid E[\phi \; U \; \phi]$ .

# CTL - Priorities

- Unary connectives bind most tightly
  - $\neg$, AG, EG, AF, EF, AX, and EX
- Next come $\wedge$, and $\vee$
- Finally come, AU and EU

- Example:

  $AGp_1 \Rightarrow EGp_2$ is not the same as $AG(p_1 \Rightarrow EGp_2)$

# CTL - yes or no?

- Yes
  - EFE[p U q]
  - A[p U EF q]
- No
  - EF(p U q)
  - FG p
- Yes or no?
  - $AG(p \Rightarrow A[p\ U\ (\neg p \wedge A[\neg p\ U\ q])])$
  - $AF[(p\ U\ q) \wedge (q\ U\ p)]$

# A is not G

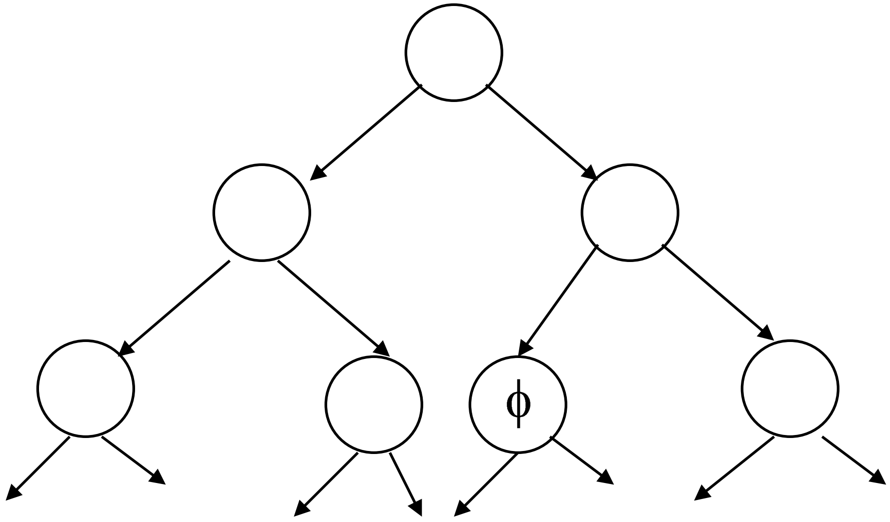
- A$\phi$ states that all the executions starting from the current state will satisfy $\phi$
- G$\phi$ state that $\phi$ holds at every state of the execution considered

- A and E quantify over paths in a tree
- G and F quantify over positions along a given path in a tree

# Combining E and F (I)

- EF$\phi$

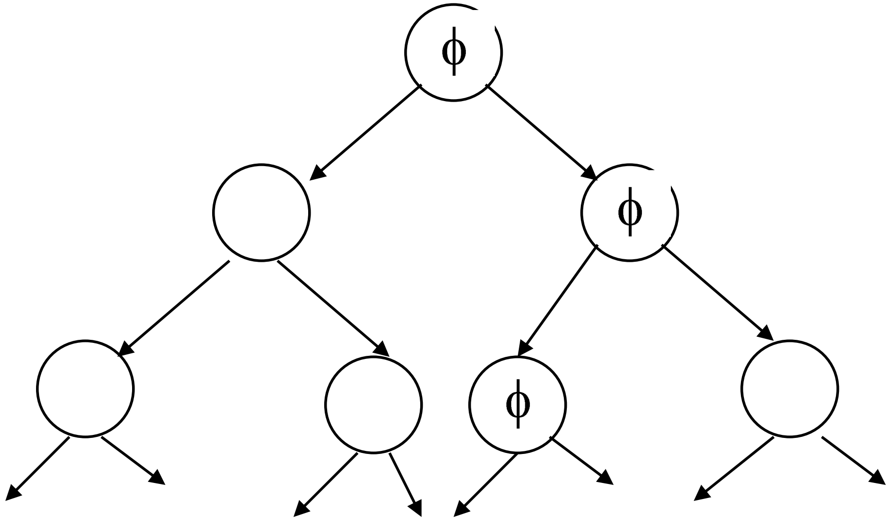
  "it is possible that $\phi$ will hold in the future"



# Combining E and F (II)

- $EG\phi = E\neg F\neg\phi$

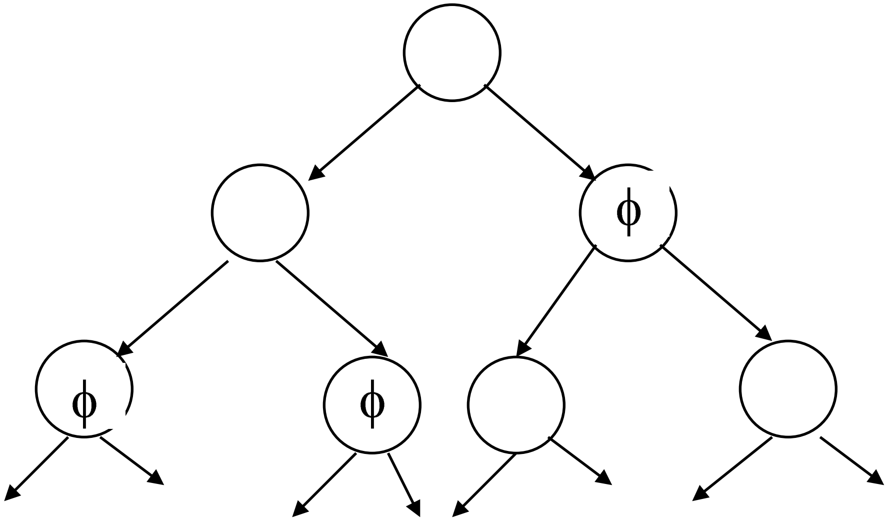
  "it is possible that $\phi$ will always hold"



# Combining E and F (III)

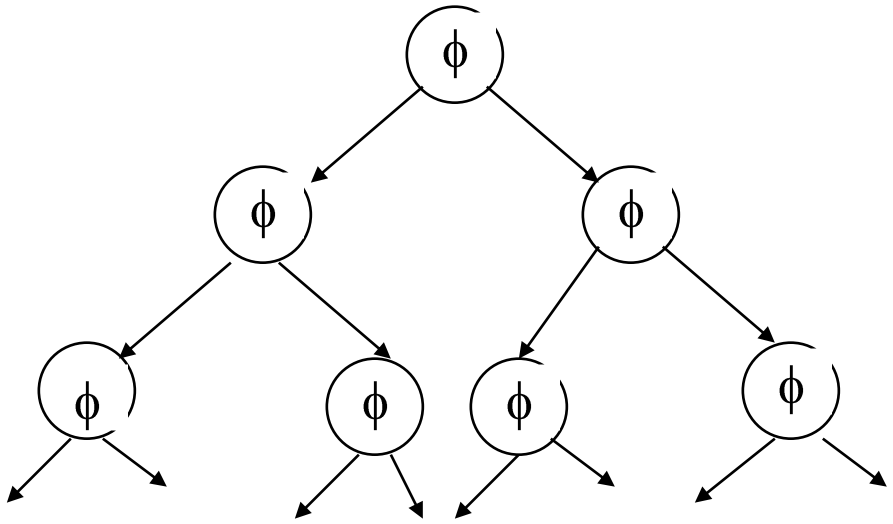
- $AF\phi = \neg E \neg F \phi$

  "it is inevitable that $\phi$ will hold in the future"



# Combining E and F (IV)

- $AG\phi = \neg EF \neg \phi$
  "$\phi$ is always true"



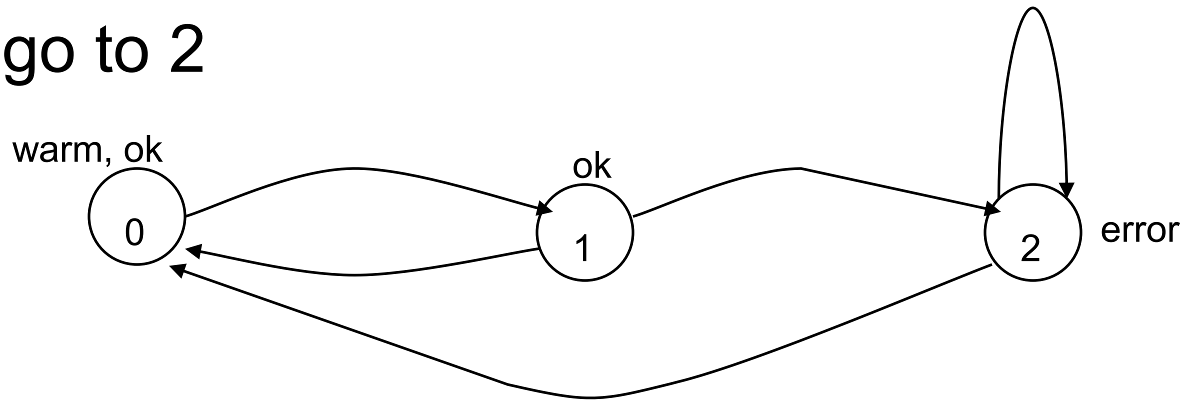

- In this case $\phi$ is an invariant, that is, a property that is true continuously

# Example

- All executions starting from 0 satisfy

$$AFEXerror$$

Why? Because from 0 all executions traverse 1 and may go to 2




- There exists an execution which does not satisfy AFAXerror. Which one?

# Examples

- AGEF$\phi$

Along every execution (A)
from every state (G)
it is possible (E)
that we will encounter a state (F)
satisfying $\phi$

that is, $\phi$ is always reachable

# CTL - Satisfaction

- Let M = <S,→,I> be a transition system with I(s) the set of atomic propositions satisfied by a state s ∈S.
- Idea for a model: A CTL formula refers to a given state of a given transition system
  - $M,s \vDash \phi$ means "$\phi$ is true at state s"

We will define it by induction on the structure of $\phi$

# CTL - Semantics (I)

- $M,s \models T$ for all s in S
- $M,s \models p$ iff $p \in I(s)$
- $M,s \models \neg\phi$ iff not $M,s \models \phi$
- $M,s \models \phi_1 \wedge \phi_2$ iff $M,s \models \phi_1$ and $M,s \models \phi_2$

  :

  :

# CTL - Semantics (II)

- $M,s \models AX\phi$ iff for all s' such that $s \rightarrow s'$ we have $M,s' \models \phi$
- $M,s \models EX\phi$ iff there exists s' such that $s \rightarrow s'$ and $M,s' \models \phi$

# CTL - Semantics (III)

- $M,s \vDash AG\phi$ iff for all executions $s_0 \to s_1 \to s_2 \to s_3 \ldots$ with $s = s_0$ we have $M,s_i \vDash \phi$
- $M,s \vDash EG\phi$ iff there exists an execution $s_0 \to s_1 \to s_2 \to s_3 \ldots$ with $s = s_0$ and such that $M,s_i \vDash \phi$

# CTL - Semantics (IV)

- $M,s \vDash AF\phi$ iff for all executions $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with $s = s_0$ there is i such that $M,s_i \vDash \phi$
- $M,s \vDash EF\phi$ iff there exists an execution $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with $s=s_0$ and there is i such that $M,s_i \vDash \phi$

# CTL - Semantics (V)

- $M,s \vDash A[\phi_1 U \phi_2]$ iff for all executions $s \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ there is i such that $M,s_i \vDash \phi_2$ and for each $j < i$ $M,s_j \vDash \phi_1$

- $M,s \vDash E[\phi_1 U \phi_2]$ iff there exists an execution $s \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ and there is i such that $M,s_i \vDash \phi_2$ and for each $j < i$ $M,s_j \vDash \phi_1$

# CTL equivalences

- De Morgan-based
  - $\neg AF\phi \equiv EG\neg\phi$
  - $\neg EF\phi \equiv AG\neg\phi$
  - $\neg AX\phi \equiv EX\neg\phi$

X-self duality: on a path each state has a unique successor

- Until reduction
  - $AF\phi \equiv A[T\ U\ \phi]$
  - $EF\phi \equiv E[T\ U\ \phi]$

# CTL: Adequate sets of connectives

- Theorem: The set of operators

  $\top, \neg, \wedge$, {AX or EX}, {EG,AF or AU}, and EU

  is adequate for CTL.

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

# CTL: Weak until and release

- Use LTL equivalence to define:
  - $A[\phi R \psi] \equiv \neg E[\neg\phi U \neg\psi]$
  - $E[\phi R \psi] \equiv \neg A[\neg\phi U \neg\psi]$

  - $A[\phi W \psi] \equiv A[\psi R(\phi \vee \psi)]$
  - $E[\phi W \psi] \equiv E[\psi R(\phi \vee \psi)]$

# Other CTL equivalences

- $EG\phi \equiv \phi \wedge EX\ EG\phi$
- $AG\phi \equiv \phi \wedge AX\ AG\phi$

- $AF\phi \equiv \phi \vee AX\ AF\phi$
- $EF\phi \equiv \phi \vee EX\ EF\phi$

- $A[\phi U \psi] \equiv \psi \vee (\phi \wedge AXA[\phi U \psi])$
- $E[\phi U \psi] \equiv \psi \vee (\phi \wedge EXE[\phi U \psi])$

# CTL* - Syntax

- State formulas (evaluated in states)

$$\phi ::= T \mid p \mid \neg\phi \mid \phi \wedge \phi \mid A\psi \mid E\psi$$

- Path formulas (evaluated along paths)

$$\psi ::= \phi \mid \neg \psi \mid \psi \wedge \psi \mid X\psi \mid F\psi \mid G\psi \mid \psi \, U\psi$$

# Examples

- AGF$\phi$

Along every execution (A)
from every state (G)
we will encounter a state (F)
satisfying $\phi$

that is, $\phi$ is satisfied infinitely often

# Model

- Let $M = <S,\rightarrow,l>$ be a transition system with $l(s)$ the set of atomic propositions satisfied by a state $s \in S$.
- Idea for a model: A formula of temporal logic refers to an instant $i$ of an execution $\pi$ of a transition system M
- $M,\pi,i \vDash \phi$ means

  "$\phi$ is true at position $i$ of path $\pi$ of M"

# Semantics (I)

- $M,\pi,i \vDash T$ always
- $M,\pi,i \vDash p$ iff $p \in l(\pi(i))$
- $M,\pi,i \vDash \neg\phi$ iff not $M,\pi,i \vDash \phi$
- $M,\pi,i \vDash \phi_1 \wedge \phi_2$ iff $M,\pi,i \vDash \phi_1$ and $M,\pi,i \vDash \phi_2$

# Semantics (II)

- $M,\pi,i \vDash X\phi$ iff $M,\pi,i+1 \vDash \phi$
- $M,\pi,i \vDash F\phi$ iff there exists $i \leq j$ such that $M,\pi,j \vDash \phi$
- $M,\pi,i \vDash G\phi$ iff $M,\pi,j \vDash \phi$ for all $i \leq j$
- $M,\pi,i \vDash \phi_1 U \phi_2$ iff there exists $i \leq j$ such that $M,\pi,j \vDash \phi_2$ and for all $i \leq k < j$ we have $M,\pi,k \vDash \phi_1$

# Semantics (III)

- $M,\pi,i \models E\phi$ iff there exists $\pi'$ such that $\pi(0)\ldots \pi(i) = \pi'(0)\ldots \pi'(i)$ and $M,\pi',i \models \phi$

- $M,\pi,i \models A\phi$ iff for all $\pi'$ such that $\pi(0)\ldots \pi(i) = \pi'(0)\ldots \pi'(i)$ we have $M,\pi',i \models \phi$

# LTL and CTL $\subseteq$ CTL*

- Semantically, an LTL formula $\phi$ is equivalent to the CTL* formula $A\phi$

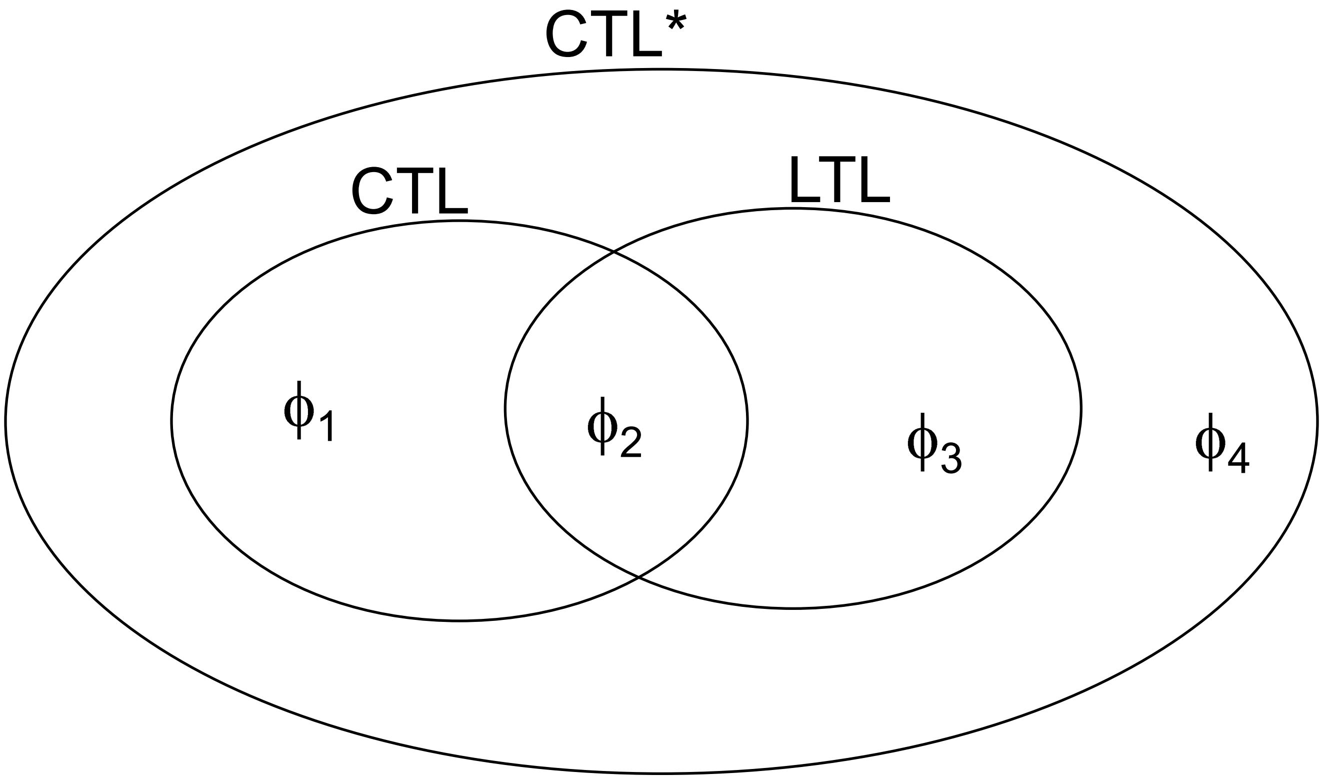
- CTL is a restricted fragment of CTL* with path formulas

$$\psi ::= X\phi \mid F\phi \mid G\phi \mid \phi\ U\ \phi$$

and the same state formulas as CTL*, i.e.

$$\phi ::= T \mid p \mid \neg\phi \mid \phi \wedge \phi \mid A\psi \mid E\psi$$

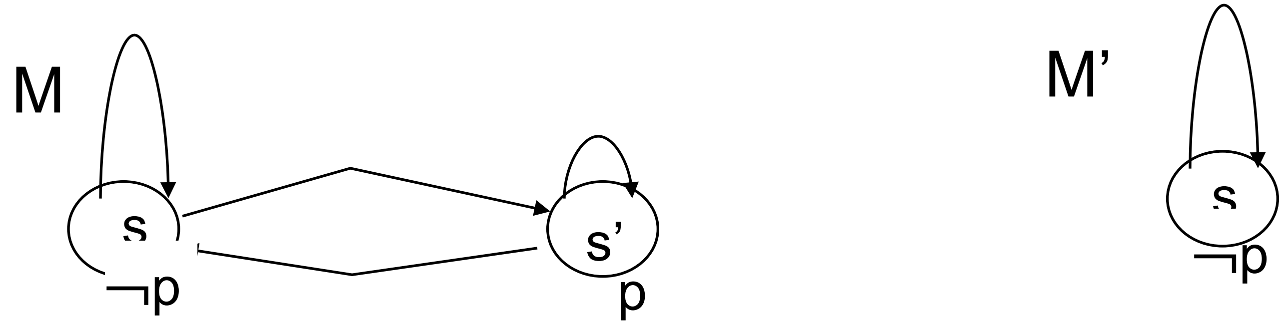
# Expressivity



# In CTL but not in LTL

$\phi_1$ = AG EF p        in CTL

From any state we can always get to a state in which p holds




- It cannot be expressed as LTL formula $\phi$ because
  - All executions starting from s in M' are also executions starting from s in M
  - In CTL M,s $\models \phi_1$ but M',s $\not\models \phi_1$

# In CTL and in LTL

$\phi_2 = AG(p \Rightarrow AFq)$ in CTL

and

$\phi_2 = G(p \Rightarrow Fq)$ in LTL

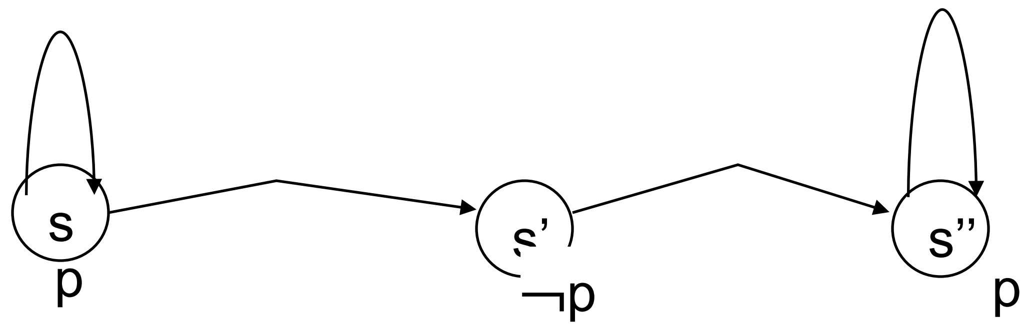
"Any p is eventually followed by a q"

# In LTL but not in CTL

$\phi_3$ = GFp $\Rightarrow$ Fq in LTL

"If p holds infinitely often along a path, then there is a state in which q holds"

Note: FGp is different from AFAGp since the first is satisfied in




whereas the latter is not (starting from s).

# Neither in CTL nor in LTL

$\phi_4$ = E(GFp) in CTL*

"There is a path with infinitely many state in which p holds"

- Not expressible in LTL: Trivial
- Not expressible in CTL: very complex

# Boolean combination of path in CTL

- CTL = CTL* but
  - Without boolean combination of path formulas
  - Without nesting of path formulas

- The first restriction is not real …
  - $E[Fp \wedge Fq] \equiv EF[p \wedge EFq] \vee EF[q \wedge EFp]$
    - First p and then q or viceversa

# More generally …

- $E[\neg(pUq)] \equiv E[\neg qU(\neg p \wedge \neg q)] \vee EG \neg q$
- $E[(p_1Uq_1) \wedge (p_2Uq_2)] \equiv E[(p_1 \wedge p_2)U(q_1 \wedge E[p_2Uq_2])] \vee E[(p_1 \wedge p_2)U(q_2 \wedge E[p_1Uq_1])]$
- $E[Fp \wedge Gq] \equiv E[q\ U\ (p \wedge EG\ q)]$

- $E[\neg Xp] \equiv EX\neg p$
- $E[Xp \wedge Xq] \equiv EX(p \wedge q)$
- $E[Fp \wedge Xq] \equiv EX(q \wedge EFp)$

- $A[\phi] \equiv \neg E[\neg \phi]$

# Past operators

| | | analogues of | |
|---|---|---|---|
| ■ Previous | P | X | neXt |
| ■ Since | S | U | Until |
| ■ Once | O | F | Future |
| ■ Historically | H | G | Globally |

- In LTL they do not add expressive power, but CTL they do!