Computation Tree Logic (CTL)

Slides by Alessandro Artale
`http://www.inf.unibz.it/~artale/`

Some material (text, figures) displayed in these slides is courtesy of: M. Benerecetti, A. Cimatti, M. Fisher, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani.

Computation Tree logic Vs. LTL

- LTL implicitly quantifies universally over paths.

$$\langle \mathscr{T}, s \rangle \models \phi \quad \text{iff} \quad \text{for every path } \pi \text{ starting at } s,\ \langle \mathscr{T}, \pi \rangle \models \phi$$

- Properties that assert the existence of a path cannot be expressed in plain LTL. In particular, properties mixing existential and universal path quantifiers cannot be expressed.
- The Computation Tree Logic, CTL, solves these problems!
  - CTL explicitly introduces path quantifiers
  - CTL is the natural temporal logic interpreted over branching time structures.

CTL at a glance

- CTL is evaluated over branching-time structures (trees).
- CTL explicitly introduces path quantifiers:
  All Paths: A
  Exists a Path: E
- Every temporal operator ($\Box$/G, $\Diamond$/F, $\bigcirc$/X, U/U) is preceded by a path quantifier (A or E).
- **Universal modalities:** AF, AG, AX, AU — true in **all** paths from current state.
- **Existential modalities:** EF, EG, EX, EU — true in **some** path from current state.

CTL: Syntax

Given a set Σ of atomic propositions $p, q, \ldots$, CTL formulas are obtained through the following syntax:

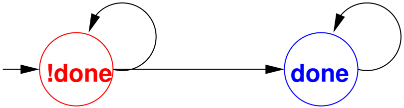
$$\begin{array}{rcl} \varphi, \psi & \rightarrow & p \mid \top \mid \bot \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \\ & & \mathrm{AX}\varphi \mid \mathrm{AG}\varphi \mid \mathrm{AF}\varphi \mid (\varphi \mathrm{AU} \psi) \\ & & \mathrm{EX}\varphi \mid \mathrm{EG}\varphi \mid \mathrm{EF}\varphi \mid (\varphi \mathrm{EU} \psi) \end{array}$$

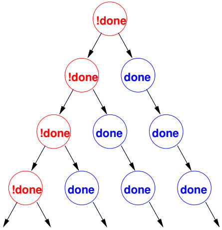
Intuition:

E	there Exists a path
A	in All paths
F	sometime in the Future
G	Globally in the future
X	neXtime

CTL: Semantics

We interpret CTL formulas directly over transition systems (expanded to infinite trees).





- Universal modalities (AF, AG, AX, AU): true in **all** paths from the current state.
- Existential modalities (EF, EG, EX, EU): true in**some** path from the current state.

CTL: Semantics (formal)

Let $\mathscr{T}$ a transition system.

The semantics of a CTL temporal formula is provided by the **satisfaction relation**:

$$\models : (\mathscr{T} \times S \times \text{Formula}) \rightarrow \{\text{true}, \text{false}\}$$

CTL Semantics: The Propositional Aspect

We start by defining when an atomic proposition is true at a state/time s_i

$$\mathscr{T}, s_i \models p \iff p \in L(s_i) \quad (p \in \Sigma)$$

Classical boolean connectives:

$$\begin{aligned}
\mathscr{T}, s_i \models \neg\varphi &\iff \mathscr{T}, s_i \not\models \varphi \\
\mathscr{T}, s_i \models \varphi \wedge \psi &\iff \mathscr{T}, s_i \models \varphi \text{ and } \mathscr{T}, s_i \models \psi \\
\mathscr{T}, s_i \models \varphi \vee \psi &\iff \mathscr{T}, s_i \models \varphi \text{ or } \mathscr{T}, s_i \models \psi \\
\mathscr{T}, s_i \models \varphi \to \psi &\iff \text{if } \mathscr{T}, s_i \models \varphi \text{ then } \mathscr{T}, s_i \models \psi
\end{aligned}$$

CTL Semantics: The Temporal Aspect

Let $\pi = (s_i, s_{i+1}, \ldots)$ be a path from s_i. Then:

$$
\begin{array}{lcl}
\mathscr{T}, s_i \models \mathrm{AX}\varphi & \iff & \forall \pi = (s_i, s_{i+1}, \ldots) : \ \mathscr{T}, s_{i+1} \models \varphi \\
\mathscr{T}, s_i \models \mathrm{EX}\varphi & \iff & \exists \pi = (s_i, s_{i+1}, \ldots) : \ \mathscr{T}, s_{i+1} \models \varphi \\
\mathscr{T}, s_i \models \mathrm{AG}\varphi & \iff & \forall \pi = (s_i, \ldots) : \ \forall j \geq i. \ \mathscr{T}, s_j \models \varphi \\
\mathscr{T}, s_i \models \mathrm{EG}\varphi & \iff & \exists \pi = (s_i, \ldots) : \ \forall j \geq i. \ \mathscr{T}, s_j \models \varphi \\
\mathscr{T}, s_i \models \mathrm{AF}\varphi & \iff & \forall \pi = (s_i, \ldots) : \ \exists j \geq i. \ \mathscr{T}, s_j \models \varphi \\
\mathscr{T}, s_i \models \mathrm{EF}\varphi & \iff & \exists \pi = (s_i, \ldots) : \ \exists j \geq i. \ \mathscr{T}, s_j \models \varphi \\
\mathscr{T}, s_i \models (\varphi \mathrm{AU} \psi) & \iff & \forall \pi = (s_i, \ldots) : \ \exists j \geq i. \ \mathscr{T}, s_j \models \psi \ \wedge \\
& & \qquad \forall i \leq k < j : \ \mathscr{T}, s_k \models \varphi \\
\mathscr{T}, s_i \models (\varphi \mathrm{EU} \psi) & \iff & \exists \pi = (s_i, \ldots) : \ \exists j \geq i. \ \mathscr{T}, s_j \models \psi \ \wedge \\
& & \qquad \forall i \leq k < j : \ \mathscr{T}, s_k \models \varphi
\end{array}
$$

CTL Semantics: Intuitions

- "Necessarily Next": $AX\varphi$ holds in s_t iff φ holds in every successor s_{t+1}.
- "Possibly Next": $EX\varphi$ holds in s_t iff φ holds in some successor s_{t+1}.

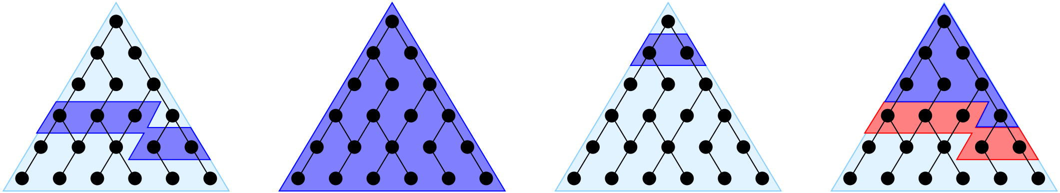
- "Necessarily in the future": $AF\varphi$ iff on all paths eventually φ occurs.
- "Possibly in the future": $EF\varphi$ iff on some path eventually φ occurs.

- "Globally": $AG\varphi$ iff φ holds on all future states on all paths.
- "Possibly henceforth": $EG\varphi$ iff there exists a path where φ holds forever.

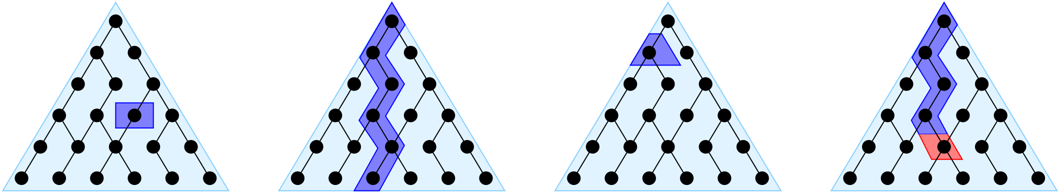
- "Necessarily Until": $\varphi AU \psi$ iff on all paths φ holds until ψ.
- "Possibly Until": $\varphi EU \psi$ iff there exists a path where φ holds until ψ.

CTL Semantics: illustration

finally p   globally p   next p   p until q



AF p   **AG p**   **AX p**   **A[p U q]**



EF p   **EG p**   **EX p**   **E[p U q]**

A Complete Set of CTL Operators

All CTL operators can be expressed via: $\mathsf{EX}, \mathsf{EG}, \mathsf{EU}$.

- $\mathsf{AX}\varphi \equiv \neg\mathsf{EX}\neg\varphi$
- $\mathsf{AF}\varphi \equiv \neg\mathsf{EG}\neg\varphi$
- $\mathsf{EF}\varphi \equiv (\top\mathsf{EU}\varphi)$
- $\mathsf{AG}\varphi \equiv \neg\mathsf{EF}\neg\varphi \equiv \neg(\top\mathsf{EU}\neg\varphi)$
- $(\varphi\mathsf{AU}\psi) \equiv \neg\mathsf{EG}\neg\psi \wedge \neg(\neg\psi\mathsf{EU}(\neg\varphi \wedge \neg\psi))$

Safety Properties

Safety: "something bad will not happen"

Typical examples:

$$\mathrm{AG}\neg(\mathit{reactor\_temp} > 1000)$$

$$\mathrm{AG}\neg(\mathit{one\_way} \wedge \mathrm{AX}\mathit{other\_way})$$

$$\mathrm{AG}\neg((x = 0) \wedge \mathrm{AXAXAX}(y = z/x))$$

Usually: $\mathrm{AG}\neg\ldots$

Liveness Properties

Liveness: "something good will happen"

Typical examples:

$$\mathsf{AF}\,\mathit{rich}, \quad \mathsf{AF}(x > 5), \quad \mathsf{AG}(\mathit{start} \rightarrow \mathsf{AF}\,\mathit{terminate})$$

Usually: $\mathsf{AF}\ldots$

Fairness Properties

Fairness: "something is successful/allocated infinitely often"

Typical example:

$$\mathrm{AG}(\mathrm{AF}\,\mathit{enabled})$$

Usually: AGAF...

The CTL Model Checking Problem

he CTL Model Checking Problem is formulated as:

$$\mathscr{T} \models \phi$$

Check if $\mathscr{T}, s_0 \models \phi$ for every initial state s_0 of $\mathscr{T}$.

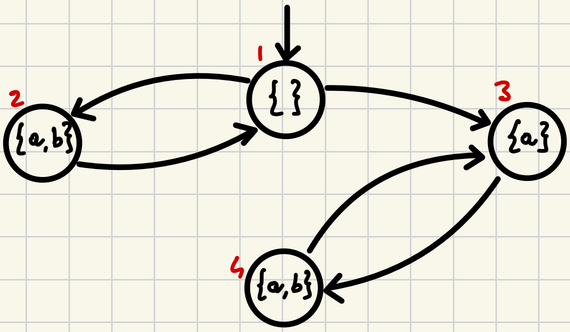
CTL	μ-CALC		
$EX\, p$	$\langle NEXT \rangle\, p$		
$AX\, p$	$[NEXT]\, p$		
$EF\, p$	$\mu Z.\, p \vee \langle NEXT \rangle Z$	$\leftarrow Z \equiv p \vee \langle NEXT \rangle Z$	$LFP = \mu Z.\, p \vee \langle NEXT \rangle Z$
$AF\, p$	$\mu Z.\, p \vee [NEXT] Z$	$\leftarrow Z \equiv p \vee [NEXT] Z$	$LFP = \mu Z.\, p \vee [NEXT] Z$
$EG\, p$	$\nu Z.\, p \wedge \langle NEXT \rangle Z$	$\leftarrow Z \equiv p \wedge \langle NEXT \rangle Z$	$GFP = \nu Z.\, p \wedge \langle NEXT \rangle Z$
$AG\, p$	$\nu Z.\, p \wedge [NEXT] Z$	$\leftarrow Z \equiv p \wedge [NEXT] Z$	$GFP = \nu Z.\, p \wedge [NEXT] Z$
$p\, EU\, q$	$\mu Z.\, q \vee (p \wedge \langle NEXT \rangle Z)$	$\leftarrow Z \equiv q \vee (p \wedge \langle NEXT \rangle Z)$	$LFP = \mu Z.\, q \vee (p \wedge \langle NEXT \rangle Z)$
$p\, AU\, q$	$\mu Z.\, q \vee (p \wedge [NEXT] Z)$	$\leftarrow Z \equiv q \vee (p \wedge [NEXT] Z)$	$LFP = \mu Z.\, q \vee (p \wedge [NEXT] Z)$

TS CTL

$$\mathcal{T} \models \phi \longrightarrow \mathcal{T} \models \phi_\mu$$

$$\mathcal{T}_{s_0} \models \phi \longrightarrow \mathcal{T}_{s_0} \models \phi_\mu$$

Ex:



$$\underbrace{EG(\underbrace{b \supset \underbrace{EX\,\underbrace{AF\,a}_{\alpha}}_{\beta}}_{\gamma})}_{\delta}$$

$[\alpha] = [AF\,a] = [\mu Z.\ a \vee [NEXT]\, Z]$

$[Z_0] = \emptyset$

$[Z_1] = [a \vee [NEXT]\, Z_0] =$
$= [a] \cup PREA(NEXT, Z_0) =$
$= \{2,3,4\} \cup \emptyset = \{2,3,4\}$

$[Z_2] = [a \vee [NEXT]\, Z_1] =$
$= [a] \cup PREA(NEXT, Z_1) =$
$= \{2,3,4\} \cup \{1,3,4\} = \{1,2,3,4\}$

$[Z_3] = [a \vee [NEXT]\, Z_2] =$
$= [a] \cup PREA(NEXT, Z_2) =$
$= \{2,3,4\} \cup \{1,2,3,4\} = \{1,2,3,4\}$

$[Z_2] = [Z_3] = \{1,2,3,4\} = [a]$

$[\beta] = [EX\,\alpha] = [\langle NEXT \rangle \alpha] = PREE(NEXT, \alpha) = \{1,2,3,4\} = [\beta]$

$[\gamma] = [b \supset \beta] = [\neg b] \cup [\beta] = \{1,3\} \cup \{1,2,3,4\} = \{1,2,3,4\} = [\gamma]$

$[\delta] = [EG\,\gamma] = \nu Z.\ \gamma \wedge \langle NEXT \rangle Z$

$[Z_0] = \{1,2,3,4\}$

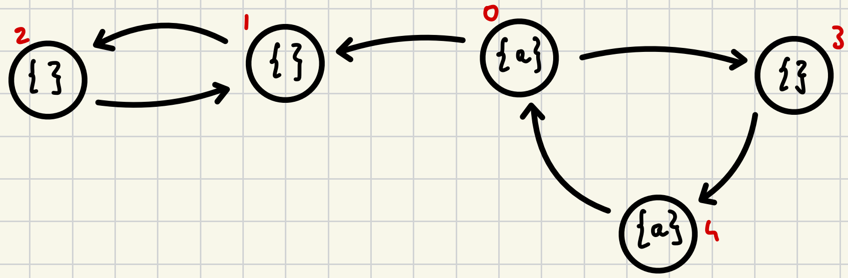
$[Z_1] = [\gamma \wedge \langle NEXT \rangle Z_0] =$
$= [\gamma] \cap PREE(NEXT, Z_0) =$
$= \{1,2,3,4\} \cap \{1,2,3,4\} = \{1,2,3,4\}$

$[Z_0] = [Z_1] = \{1,2,3,4\} = [\delta]$

$T \models \phi \Rightarrow T_{s_0} \models \phi \Rightarrow T_1 \models \phi$

$1 \in [\phi] = [\delta] = \{1,2,3,4\}$? YES

Ex:



$$\underbrace{EF\,(\overbrace{\underbrace{EX\,\underbrace{AF\,a}_{\gamma}}_{\varepsilon} \wedge \underbrace{AX\,\underbrace{EG\,a}_{\alpha}}_{\beta}}^{\delta})}_{\eta}$$

$[\alpha] = [EG\, a] = [\nu Z.\ a \wedge \langle NEXT\rangle Z]$

$[Z_0] = \{0,1,2,3,4\}$

$[Z_1] = [a] \cap PREE(NEXT, Z_0) =$
$= \{0,4\} \cap \{0,1,2,3,4\} = \{0,4\}$

$[Z_2] = [a] \cap PREE(NEXT, Z_1) =$
$= \{0,4\} \cap \{3,4\} = \{4\}$

$[Z_3] = [a] \cap PREE(NEXT, Z_2) =$
$= \{0,4\} \cap \{3\} = \phi$

$[Z_4] = [a] \cap PREE(NEXT, Z_3) =$
$= \{0,4\} \cap \phi = \phi$

$[Z_3] = [Z_4] = \phi = [\alpha]$

$[\beta] = [AX\, \alpha] = [[NEXT]\alpha] = PREA(NEXT, \alpha) = \phi = [\beta]$

$[\gamma] = [AF\, a] = [\mu Z.\ a \vee [NEXT] Z] =$

$[Z_0] = \phi$

$[Z_1] = [a] \cup PREA(NEXT, Z_0) =$
$= \{0,4\} \cup \phi = \{0,4\}$

$[Z_2] = [a] \cup PREA(NEXT, Z_1) =$
$= \{0,4\} \cup \{3,4\} = \{0,3,4\}$

$[Z_3] = [a] \cup PREA(NEXT, Z_2) =$
$= \{0,4\} \cup \{3,4\} = \{0,3,4\}$

$[Z_2] = [Z_3] = \{0,3,4\} = [\gamma]$

$[\varepsilon] = [EX\, \gamma] = [\langle NEXT\rangle \gamma] = PREE(NEXT, \gamma) = \{0,3,4\} = [\varepsilon]$

$[\delta] = [\varepsilon \wedge \beta] = \{0,3,4\} \cap \phi = \phi = [\delta]$

$[\eta] = [EF\, \delta] = [\mu Z.\ \delta \vee \langle NEXT\rangle Z] =$

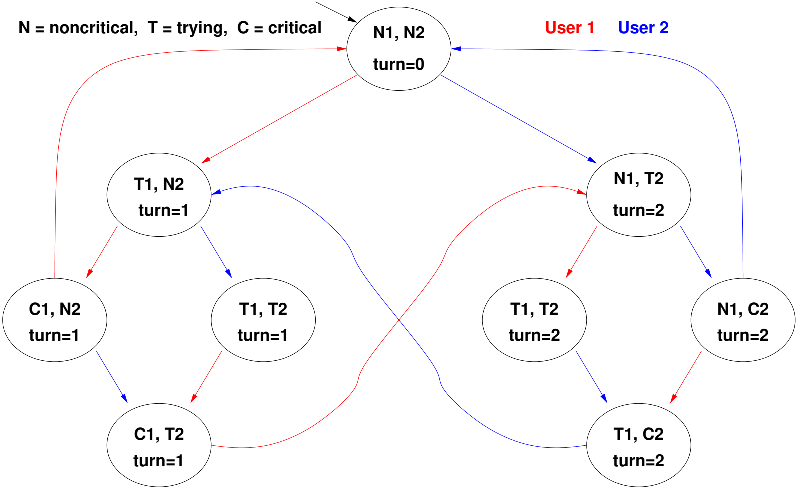
$[Z_0] = \phi$

$[Z_1] = [\delta] \cup PREE(NEXT, Z_0) =$
$= \phi \cup \phi = \phi$

$[Z_0] = [Z_1] = \phi = [\eta]$

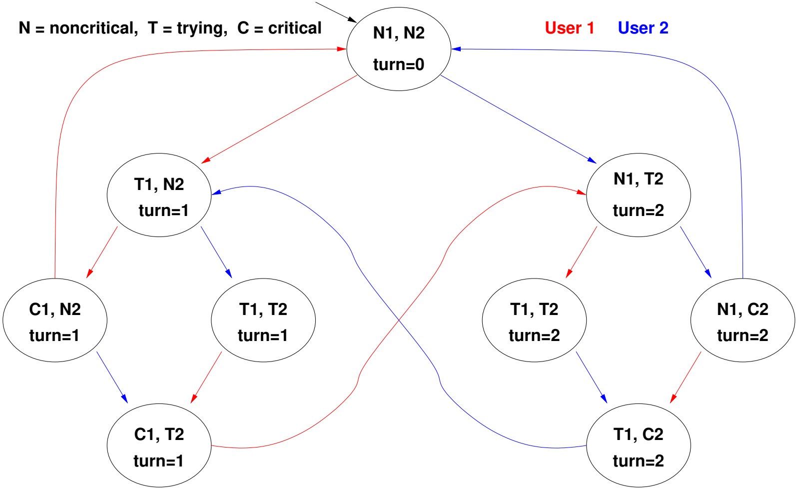
$\mathcal{T} \models \phi \Rightarrow \mathcal{T}_{s_0} \models \phi \Rightarrow \mathcal{T}_0 \models \phi \qquad 0 \in [\eta] = \phi\ ?$ NO

Example 1: Mutual Exclusion (Safety)



$\mathscr{T} \models \mathrm{AG}\neg(C_1 \wedge C_2)$?

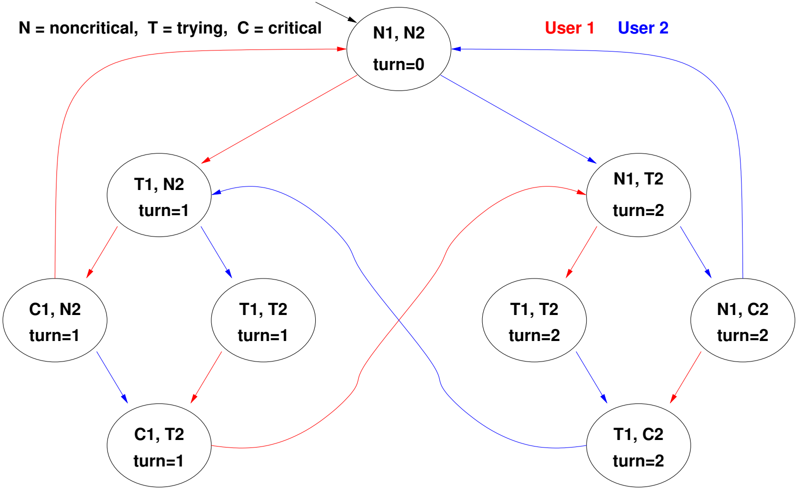
Example 1: Mutual Exclusion (Safety)



$\mathscr{T} \models \mathrm{AG}\neg(C_1 \wedge C_2)$?

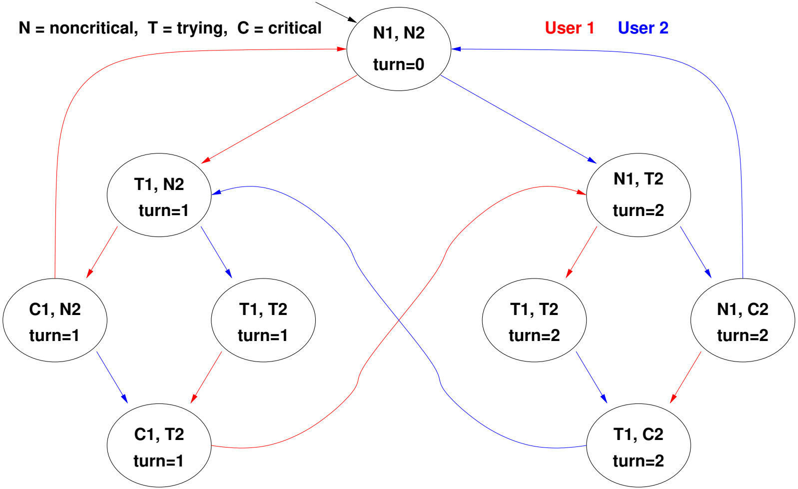
YES: There is no reachable state in which $(C_1 \wedge C_2)$ holds!
(Same as $\square\neg(C_1 \wedge C_2)$ in LTL.)

Example 2: Liveness



$$\mathscr{T} \models \mathsf{AG}(T_1 \rightarrow \mathsf{AF}\, C_1)\ ?$$

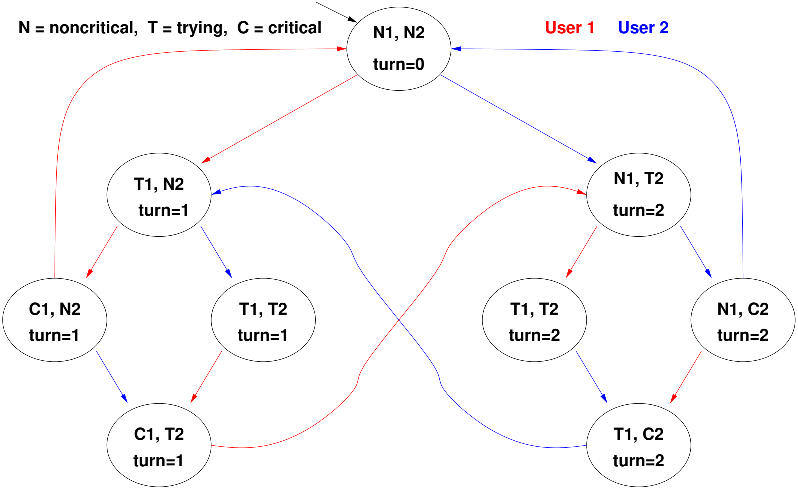
Example 2: Liveness



$$\mathscr{T} \models \mathrm{AG}(T_1 \rightarrow \mathrm{AF}\, C_1)\ ?$$

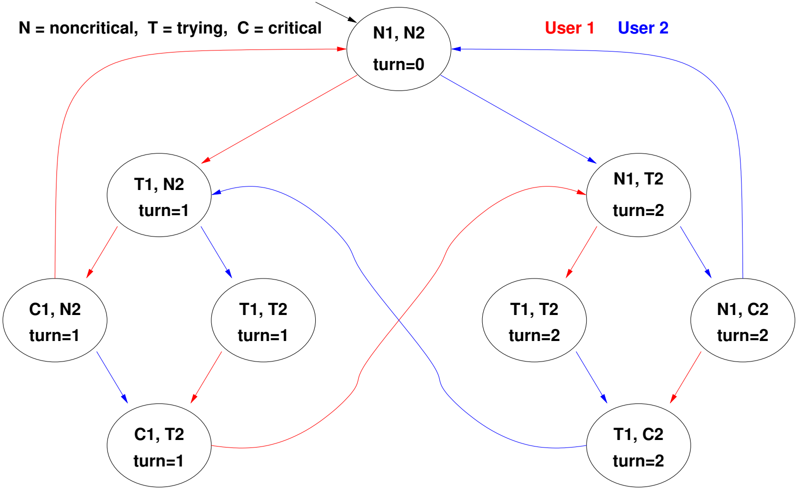
YES: every path from each state where T_1 holds passes through a state where C_1 holds.
(Same as $\Box(T_1 \rightarrow \Diamond C_1)$ in LTL.)

Example 3: Fairness



$\mathscr{T} \models \mathrm{AGAF}\, C_1$?

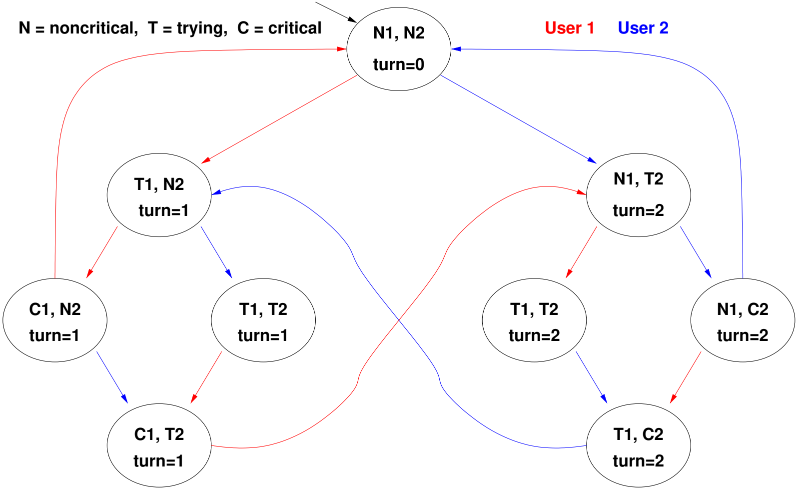
Example 3: Fairness



$\mathcal{T} \models \mathrm{AGAF}\, C_1$?

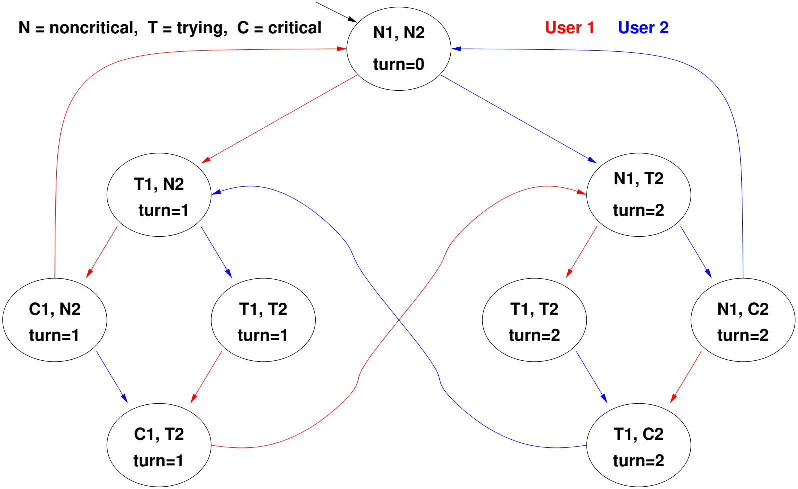
NO: in the initial state there is a blue cyclic path where C_1 never holds.
(Same as $\Box\Diamond C_1$ in LTL.)

Example 4: Non-Blocking



$$\mathcal{T} \models \mathrm{AG}(N_1 \rightarrow \mathrm{EF}\, T_1) \ ?$$

Example 4: Non-Blocking

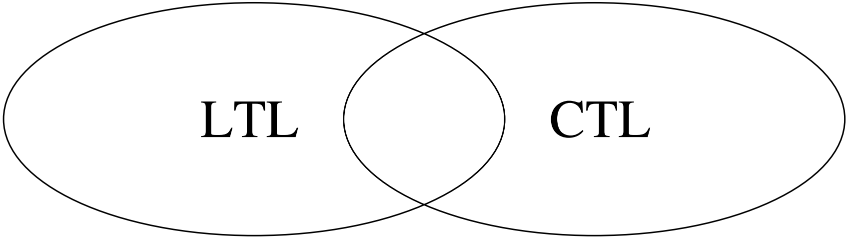


$$\mathcal{T} \models \mathrm{AG}(N_1 \rightarrow \mathrm{EF}\, T_1) \ ?$$

YES: from each state where N_1 holds there is a path leading to a state where T_1 holds. (No corresponding LTL formula.)

LTL Vs. CTL: Expressiveness

- Many CTL formulas cannot be expressed in LTL (e.g., those with existential path quantifiers): e.g. $\mathsf{AG}(N_1 \rightarrow \mathsf{EF}\, T_1)$.
- Many LTL formulas cannot be expressed in CTL (e.g., strong fairness): $\Box\Diamond\, T_1 \rightarrow \Box\Diamond\, C_1$.
- Some formulas are expressible in both (typically depth-1 LTL): e.g. $\Box\neg(C_1 \wedge C_2)$, $\Diamond\, C_1$, $\Box(T_1 \rightarrow \Diamond\, C_1)$, $\Box\Diamond\, C_1$.



The Computation Tree Logic CTL*

- CTL* combines the expressive power of LTL and CTL.
- Temporal operators can be applied freely in the context of path quantifiers.
- Examples:
  - $\mathsf{A}(\mathsf{X}\varphi \vee \mathsf{XX}\varphi)$
  - $\mathsf{E}(\mathsf{GF}\varphi)$

CTL*: Syntax

IF I REMOVE Eα I HAVE LTL

State formulas:

$$\varphi, \psi \quad \rightarrow \quad p \mid \top \mid \perp \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \mathsf{A}\alpha \mid \mathsf{E}\alpha$$

Path formulas:

$$\alpha, \beta \quad \rightarrow \quad \varphi \mid \neg\alpha \mid \alpha \wedge \beta \mid \alpha \vee \beta \mid \mathsf{X}\alpha \mid \mathsf{G}\alpha \mid \mathsf{F}\alpha \mid (\alpha \mathsf{U} \beta)$$

CTL* Semantics: State Formulas

$$\mathscr{T}, s_0 \models p \iff p \in L(s_0)$$

$$\begin{aligned}
\mathscr{T}, s_0 \models \neg\varphi &\iff \mathscr{T}, s_0 \not\models \varphi \\
\mathscr{T}, s_0 \models \varphi \wedge \psi &\iff \mathscr{T}, s_0 \models \varphi \text{ and } \mathscr{T}, s_0 \models \psi \\
\mathscr{T}, s_0 \models \mathsf{E}\alpha &\iff \exists \pi = (s_0, s_1, \ldots) :\ \mathscr{T}, \pi \models \alpha \\
\mathscr{T}, s_0 \models \mathsf{A}\alpha &\iff \forall \pi = (s_0, s_1, \ldots) :\ \mathscr{T}, \pi \models \alpha
\end{aligned}$$

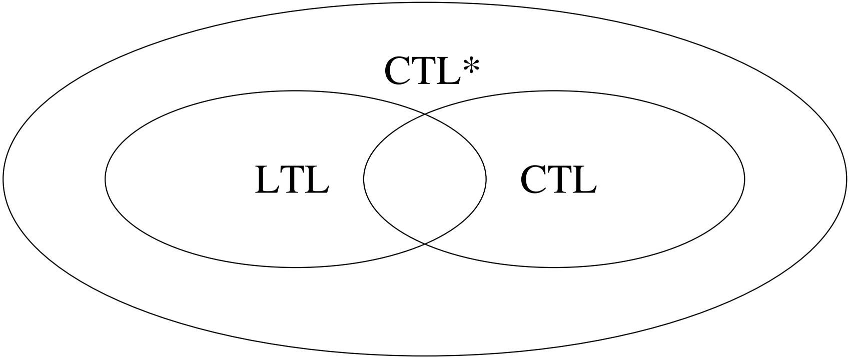
CTL* Semantics: Path Formulas

Let $\pi = (s_0, s_1, \ldots)$ and $\pi^i = (s_i, s_{i+1}, \ldots)$.

$$
\begin{aligned}
\mathscr{T}, \pi \models \varphi \quad & \iff \mathscr{T}, s_0 \models \varphi \\
\mathscr{T}, \pi \models \neg\alpha \quad & \iff \mathscr{T}, \pi \not\models \alpha \\
\mathscr{T}, \pi \models \mathsf{F}\alpha \quad & \iff \exists i \geq 0 : \ \mathscr{T}, \pi^i \models \alpha \\
\mathscr{T}, \pi \models \mathsf{G}\alpha \quad & \iff \forall i \geq 0 : \ \mathscr{T}, \pi^i \models \alpha \\
\mathscr{T}, \pi \models \mathsf{X}\alpha \quad & \iff \mathscr{T}, \pi^1 \models \alpha \\
\mathscr{T}, \pi \models \alpha \mathsf{U} \beta & \iff \exists i \geq 0 : \ \mathscr{T}, \pi^i \models \beta \ \wedge \ \forall 0 \leq j < i : \ \mathscr{T}, \pi^j \models \alpha
\end{aligned}
$$

CTL* Vs LTL Vs CTL: Expressiveness

- CTL* subsumes both CTL and LTL.
- If φ is in CTL then φ is in CTL*.
- If φ is in LTL then $A\varphi$ is in CTL*.



CTL* Vs LTL Vs CTL: Complexity

Satisfiability complexity:

Logic	Complexity
LTL	PSpace-Complete
CTL	ExpTime-Complete
CTL*	2ExpTime-Complete

CTL* Vs LTL Vs CTL: Complexity (cont.)

Model checking complexity (two measures):

Logic	Complexity wrt $|\varphi|$	Complexity wrt $|\mathscr{M}|$
LTL	PSpace-Complete	P (linear)
CTL	P-Complete	P (linear)
CTL*	PSpace-Complete	P (linear)