

## LINEAR TEMPORAL LOGIC (LTL)

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.

## Summary of Lecture III

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

## An Introduction to Temporal Logics

In classical logic, formulae are evaluated within a single fixed world.

For example, a proposition such as “it is Monday” must be either *true* or *false*.

Propositions are then combined using constructs such as ‘ $\wedge$ ’, ‘ $\neg$ ’, etc.

But, most (not just computational) systems are **dynamic**.

In temporal logics, evaluation takes place within a **set of worlds**. Thus, “it is Monday” may be satisfied in some worlds, but not in others.

– p. 1/??

## An Introduction to Temporal Logics (Cont.)

The set of worlds correspond to **moments in time**.

How we navigate between these worlds depends on our particular view of time.

The particular model of time is captured by a temporal **accessibility relation** between worlds.

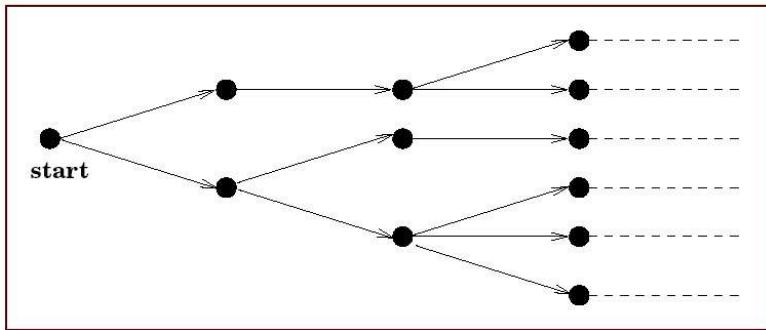
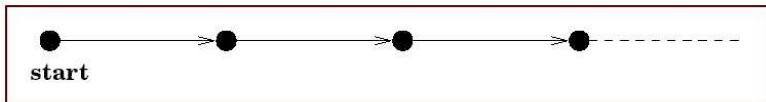
Essentially, temporal logic extends classical propositional logic with a set of **temporal operators** that navigate between worlds using this accessibility relation.

– p. 3/??

– p. 2/??

– p. 4/??

## Typical Models of Time



- 0. 5/??

## Linear Temporal Logic (LTL): Intuitions

Consider a simple temporal logic (LTL) where the accessibility relation characterises a discrete, linear model isomorphic to the Natural Numbers.

Typical temporal operators used are

$\bigcirc\varphi$	$\varphi$ is true in the <i>next</i> moment in time
$\Box\varphi$	$\varphi$ is true in <i>all</i> future moments
$\Diamond\varphi$	$\varphi$ is true in <i>some</i> future moment
$\varphi \wedge \psi$	$\varphi$ is true <i>until</i> $\psi$ is true

Examples:

$$\Box((\neg\text{passport} \vee \neg\text{ticket}) \Rightarrow \bigcirc\neg\text{board\_flight})$$

- 0. 7/??

## Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

- 0. 6/??

## Computational Example

$$\Box(\text{requested} \Rightarrow \Diamond\text{received})$$

$$\Box(\text{received} \Rightarrow \bigcirc\text{processed})$$

$$\Box(\text{processed} \Rightarrow \Diamond\Box\text{done})$$

From the above we should be able to infer that it is *not* the case that the system continually re-sends a request, but never sees it completed ( $\Box\neg\text{done}$ ); i.e. the statement

$$\Box\text{requested} \wedge \Box\neg\text{done}$$

should be inconsistent.

- 0. 8/??

## Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- [LTL: Syntax and Semantics](#).
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

- 0. 9/??

## LTL: Syntax

Countable set  $\Sigma$  of *atomic propositions*:  $p, q, \dots$  the set FORM of formulas is:

$\varphi, \psi$	$\rightarrow$	$p \mid$	(atomic proposition)
		$\top \mid$	(true)
		$\perp \mid$	(false)
		$\neg \varphi \mid$	(complement)
		$\varphi \wedge \psi \mid$	(conjunction)
		$\varphi \vee \psi \mid$	(disjunction)
		$\bigcirc \varphi \mid$	(next time)
		$\Box \varphi \mid$	(always)
		$\Diamond \varphi \mid$	(sometime)
		$\varphi \text{ } U \text{ } \psi \mid$	(until)

- 0. 10/??

## Temporal Semantics

We interpret our temporal formulae in a discrete, linear model of time. Formally, this structure is represented by

$$\mathcal{M} = \langle \mathbb{N}, I \rangle$$

where

- $I : \mathbb{N} \mapsto 2^\Sigma$   
maps each Natural number (representing a moment in time) to a set of propositions.

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

$$\models : (\mathcal{M} \times \mathbb{N} \times \text{FORM}) \rightarrow \{\text{true, false}\}$$

- 0. 11/??

## Semantics: The Propositional Aspect

We start by defining when an atomic proposition is true at a time point " $i$ "

$$\langle \mathcal{M}, i \rangle \models p \quad \text{iff} \quad p \in I(i) \quad (\text{for } p \in \Sigma)$$

The semantics for the classical operators is as expected:

$\langle \mathcal{M}, i \rangle \models \neg \varphi$	$\text{iff}$	$\langle \mathcal{M}, i \rangle \not\models \varphi$
$\langle \mathcal{M}, i \rangle \models \varphi \wedge \psi$	$\text{iff}$	$\langle \mathcal{M}, i \rangle \models \varphi \text{ and } \langle \mathcal{M}, i \rangle \models \psi$
$\langle \mathcal{M}, i \rangle \models \varphi \vee \psi$	$\text{iff}$	$\langle \mathcal{M}, i \rangle \models \varphi \text{ or } \langle \mathcal{M}, i \rangle \models \psi$
$\langle \mathcal{M}, i \rangle \models \varphi \Rightarrow \psi$	$\text{iff}$	if $\langle \mathcal{M}, i \rangle \models \varphi$ then $\langle \mathcal{M}, i \rangle \models \psi$

$$\langle \mathcal{M}, i \rangle \models \top$$

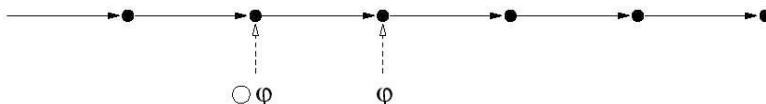
$$\langle \mathcal{M}, i \rangle \not\models \perp$$

- 0. 12/??

## Temporal Operators: ‘next’

$$\langle \mathcal{M}, i \rangle \models \bigcirc \varphi \quad \text{iff} \quad \langle \mathcal{M}, i+1 \rangle \models \varphi$$

This operator provides a constraint on the next moment in time.



Examples:

$$(sad \wedge \neg rich) \Rightarrow \bigcirc sad$$

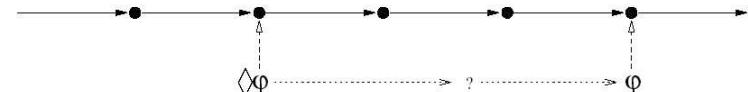
$$((x=0) \wedge add3) \Rightarrow \bigcirc (x=3)$$

- 0. 13/??

## Temporal Operators: ‘sometime’

$$\langle \mathcal{M}, i \rangle \models \lozenge \varphi \quad \text{iff} \quad \text{there exists } j. (j \geq i) \wedge \langle \mathcal{M}, j \rangle \models \varphi$$

**N.B.** while we can be sure that  $\varphi$  *will* be true either now or in the future, we can not be sure exactly *when* it will be true.



Examples:

$$(\neg resigned \wedge sad) \Rightarrow \lozenge famous$$

$$sad \Rightarrow \lozenge happy$$

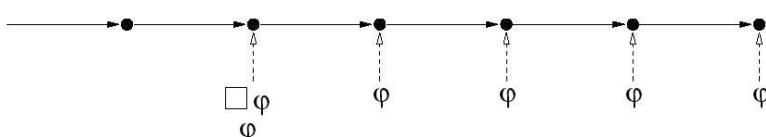
$$send \Rightarrow \lozenge receive$$

- 0. 14/??

## Temporal Operators: ‘always’

$$\langle \mathcal{M}, i \rangle \models \Box \varphi \quad \text{iff} \quad \text{for all } j. \text{ if } (j \geq i) \text{ then } \langle \mathcal{M}, j \rangle \models \varphi$$

This can represent invariant properties.



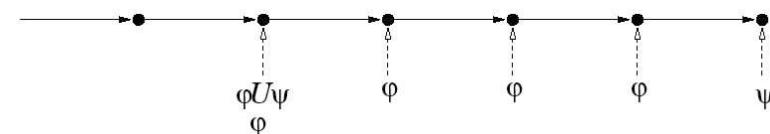
Examples:

$$lottery-win \Rightarrow \Box rich$$

- 0. 15/??

## Temporal Operators: ‘until’

$$\langle \mathcal{M}, i \rangle \models \varphi U \psi \quad \text{iff} \quad \text{there exists } j. (j \geq i) \wedge \langle \mathcal{M}, j \rangle \models \psi \wedge \text{for all } k. (i \leq k < j) \Rightarrow \langle \mathcal{M}, k \rangle \models \varphi$$



Examples:

$$start\_lecture \Rightarrow talk U end\_lecture$$

$$born \Rightarrow alive U dead$$

$$request \Rightarrow reply U acknowledgement$$

- 0. 16/??

A structure  $\mathcal{M} = \langle \mathbb{N}, I \rangle$  is a **model** of  $\phi$ , if

$\langle \mathcal{M}, i \rangle \models \phi$ , for some  $i \in \mathbb{N}$ .

Similarly as in classical logic, an LTL formula  $\phi$  can be **satisfiable**, **unsatisfiable** or **valid**. A formula  $\phi$  is:

- **Satisfiable**, if there is model for  $\phi$ .
- **Unsatisfiable**, if  $\phi$  is not satisfiable.
- **Valid** (i.e., a Tautology):  
 $\models \phi$  iff  $\forall \mathcal{M}, \forall i \in \mathbb{N}. \langle \mathcal{M}, i \rangle \models \phi$ .

- P. 17/??

## Equivalences in LTL

The temporal operators  $\Box$  and  $\Diamond$  are duals

$$\neg \Box \varphi \equiv \Diamond \neg \varphi$$

$\diamond$  (and then  $\Box$ ) can be rewritten in terms of  $\Diamond$

$$\Diamond \varphi \equiv \top \vee \varphi$$

All the temporal operators can be rewritten using the “Until” and “Next” operators

- p. 19/22

## Entailment and Equivalence

Similarly as in classical logic we can define the notions of **entailment** and **equivalence** between two LTL formulas

- **Entailment.**  
 $\phi \models \psi$  iff  $\forall \mathcal{M}, \forall i \in \mathbb{N}. \langle \mathcal{M}, i \rangle \models \phi \Rightarrow \langle \mathcal{M}, i \rangle \models \psi$
- **Equivalence.**  
 $\phi \equiv \psi$  iff  $\forall \mathcal{M}, \forall i \in \mathbb{N}. \langle \mathcal{M}, i \rangle \models \phi \Leftrightarrow \langle \mathcal{M}, i \rangle \models \psi$

- p. 18/23

## Equivalences in LTL (Cont.)

$\diamond$  distributes over  $\vee$  while  $\Box$  distributes over  $\wedge$

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

$$\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$$

The following equivalences are useful for generating formulas in Negated Normal Form

$$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$$

$$\neg(\varphi \vee \psi) \equiv (\neg \psi \vee (\neg \varphi \wedge \neg \psi)) \vee \square \neg \psi$$

- p. 20/22

## LTL Vs. FOL

Linear Temporal Logic can be thought of as

*a specific decidable (PSPACE-complete) fragment  
of classical first-order logic*

We just map each proposition to a unary predicate in FOL.  
In general, the following satisfiability preserving mapping  
( $\rightsquigarrow$ ) holds:

$$\begin{array}{lll} p & \rightsquigarrow & p(t) \\ \bigcirc p & \rightsquigarrow & p(t+1) \\ \lozenge p & \rightsquigarrow & \exists t'. (t' \geq t) \wedge p(t') \\ \square p & \rightsquigarrow & \forall t'. (t' \geq t) \Rightarrow p(t') \end{array}$$

- p. 21/??

## Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- [LTL in Computer Science](#).
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

## Temporal Logic in Computer Science

Temporal logic was originally developed in order to represent tense in natural language.

Within Computer Science, it has achieved a significant role in the formal specification and verification of concurrent reactive systems.

Much of this popularity has been achieved as a number of useful concepts can be formally, and concisely, specified using temporal logics, e.g.

- *safety properties*
- *liveness properties*
- *fairness properties*

- p. 23/??

## Safety Properties

**Safety:**

*“something bad will not happen”*

Typical examples:

$$\begin{aligned} & \square \neg (reactor\_temp > 1000) \\ & \square \neg ((x = 0) \wedge \bigcirc \bigcirc \bigcirc (y = z/x)) \\ & \text{and so on....} \end{aligned}$$

Usually:  $\square \neg \dots$

- p. 22/??

- p. 24/??

## Liveness Properties

Liveness:

“something good will happen”

Typical examples:

$\diamondsuit \text{rich}$

$\diamondsuit(x > 5)$

$\square(\text{start} \Rightarrow \diamondsuit\text{terminate})$

$\square(\text{Trying} \Rightarrow \diamondsuit\text{Critical})$

and so on.....

Usually:  $\diamondsuit \dots$

- p. 25/??

## Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- **LTL Interpreted over Kripke Models.**
- LTL and Model Checking: Intuitions.

- p. 27/??

## Fairness Properties

Often only really useful when scheduling processes, responding to messages, etc.

Strong Fairness:

“if something is attempted/requested infinitely often, then it will be successful/allocated infinitely often”

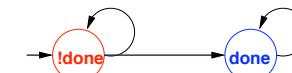
Typical example:

$\square\diamondsuit\text{ready} \Rightarrow \square\diamondsuit\text{run}$

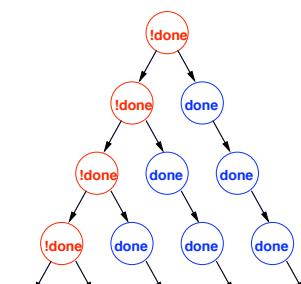
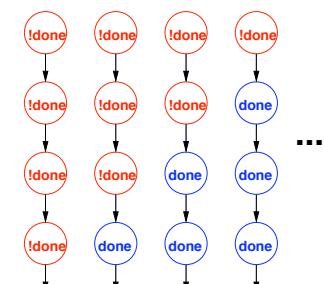
- p. 26/??

## Kripke Models and Linear Structures

Consider the following Kripke structure:



Its paths/computations can be seen as a set of linear structures (computation tree):



- p. 28/??

## Path-Semantics for LTL

- LTL formulae are evaluated over the set  $\mathbb{N}$  of Natural Numbers.
- Paths in Kripke structures are infinite and linear sequences of states. Thus, they are isomorphic to the Natural Numbers:

$$\pi = s_0 \rightarrow s_1 \rightarrow \dots \rightarrow s_i \rightarrow s_{i+1} \rightarrow \dots$$

- We want to interpret LTL formulas over Kripke structures.
- Given a Kripke structure,  $\mathcal{KM} = (S, I, R, AP, L)$ , a path  $\pi$  in  $\mathcal{KM}$ , a state  $s \in S$ , and an LTL formula  $\phi$ , we define:
  1.  $\langle \mathcal{KM}, \pi \rangle \models \phi$ , and then
  2.  $\langle \mathcal{KM}, s \rangle \models \phi$

Based on the LTL semantics over the Natural Numbers.

- d. 29/??

## LTL Model Checking Definition

Given a Kripke structure,  $\mathcal{KM} = (S, I, R, AP, L)$ , the LTL model checking problem  $\mathcal{KM} \models \phi$ :

Check if  $\langle \mathcal{KM}, s_0 \rangle \models \phi$ , for every  $s_0 \in I$  initial state of the Kripke structure  $\mathcal{KM}$

- d. 31/??

## Path-Semantics for LTL (Cont.)

- We first extract an LTL model,  $\mathcal{M}_\pi = (\pi, I_\pi)$ , from the Kripke structure  $\mathcal{KM}$ .  $\mathcal{M}_\pi = (\pi, I_\pi)$  is such that:
  - $\pi$  is a path in  $\mathcal{KM}$
  - $I_\pi$  is the restriction of  $L$  to states in  $\pi$ :

$$\forall s \in \pi \text{ and } \forall p \in AP, p \in I_\pi(s) \text{ iff } p \in L(s)$$

- Given a Kripke structure,  $\mathcal{KM} = (S, I, R, AP, L)$ , a path  $\pi$  in  $\mathcal{KM}$ , a state  $s \in S$ , and an LTL formula  $\phi$ :
  1.  $\langle \mathcal{KM}, \pi \rangle \models \phi$  iff  $\langle \mathcal{M}_\pi, s_0 \rangle \models \phi$  with  $s_0$  initial state of  $\pi$
  2.  $\langle \mathcal{KM}, s \rangle \models \phi$  iff  $\langle \mathcal{KM}, \pi \rangle \models \phi$  for all paths  $\pi$  starting at  $s$ .

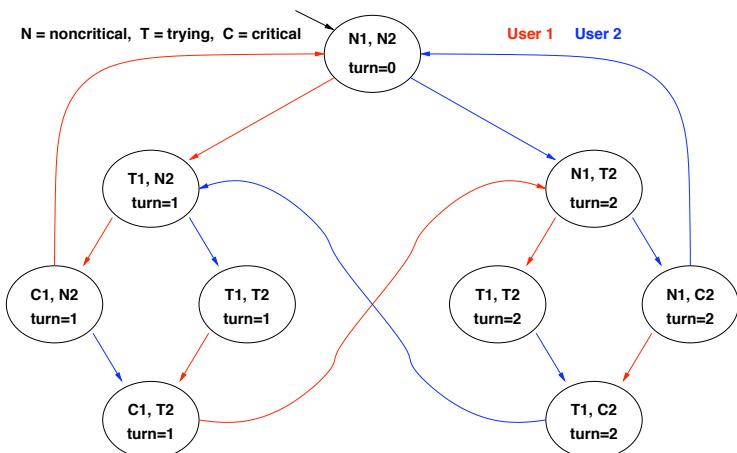
- d. 30/??

## Summary

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

- d. 32/??

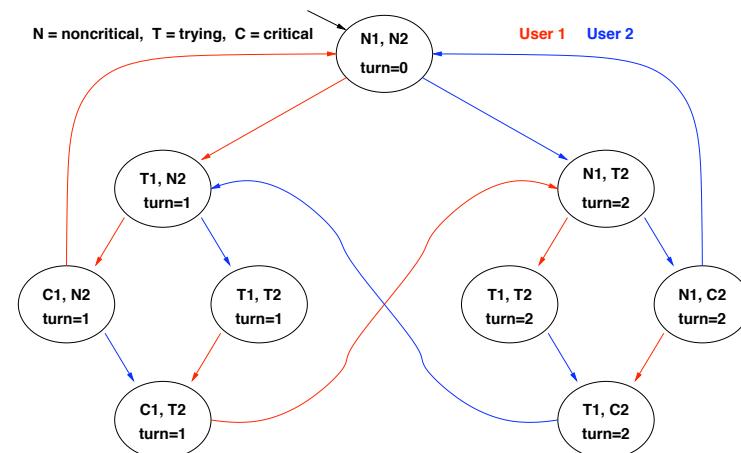
## Example 1: mutual exclusion (safety)



$$\mathcal{KM} \models \Box \neg(C_1 \wedge C_2) ?$$

- 0. 33/??

## Example 1: mutual exclusion (safety)

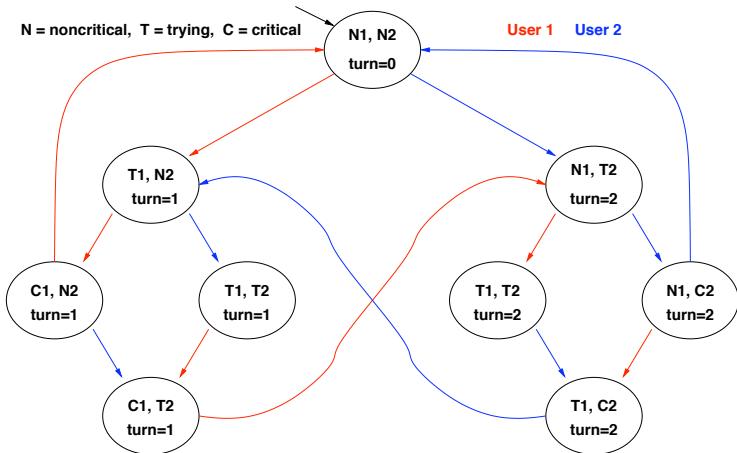


$$\mathcal{KM} \models \Box \neg(C_1 \wedge C_2) ?$$

YES: There is no reachable state in which  $(C_1 \wedge C_2)$  holds!

- 0. 33/??

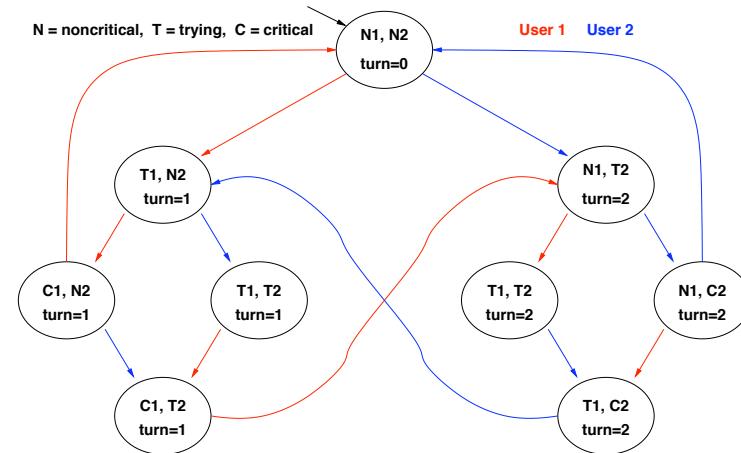
## Example 2: mutual exclusion (liveness)



$$\mathcal{KM} \models \Diamond C_1 ?$$

- 0. 34/??

## Example 2: mutual exclusion (liveness)

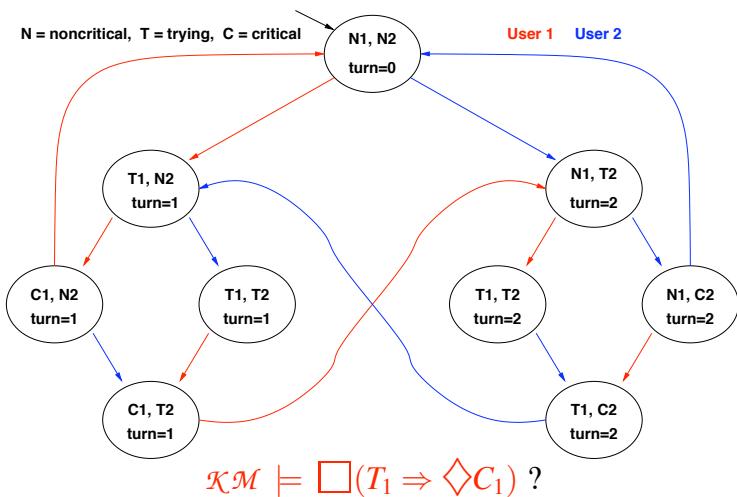


$$\mathcal{KM} \models \Diamond C_1 ?$$

NO: the blue cyclic path is a counterexample!

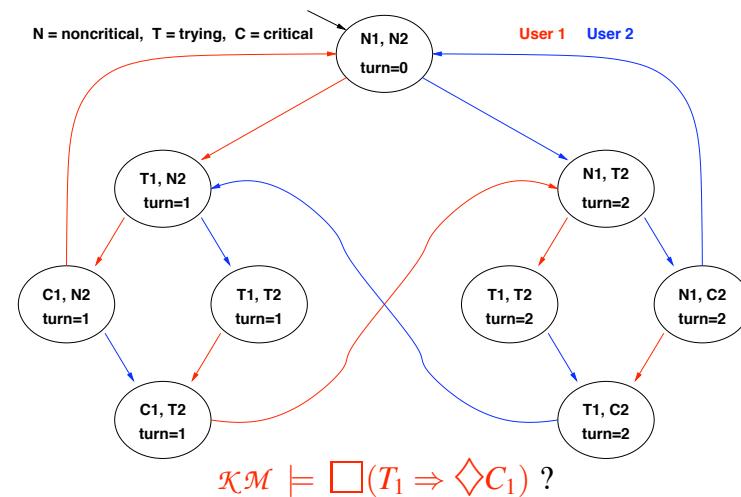
- 0. 34/??

## Example 3: mutual exclusion (liveness)



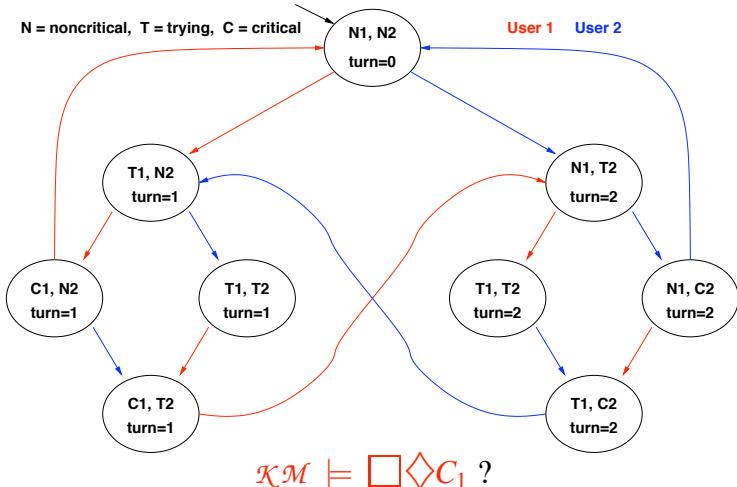
- 0. 35/??

## Example 3: mutual exclusion (liveness)



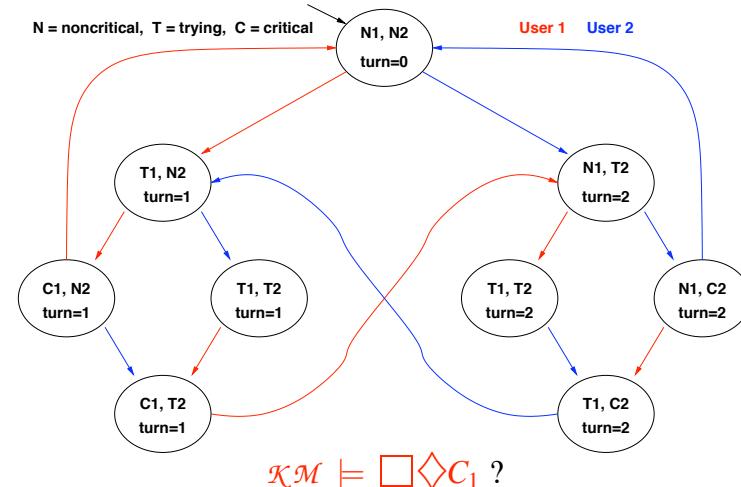
- 0. 35/??

## Example 4: mutual exclusion (fairness)



- 0. 36/??

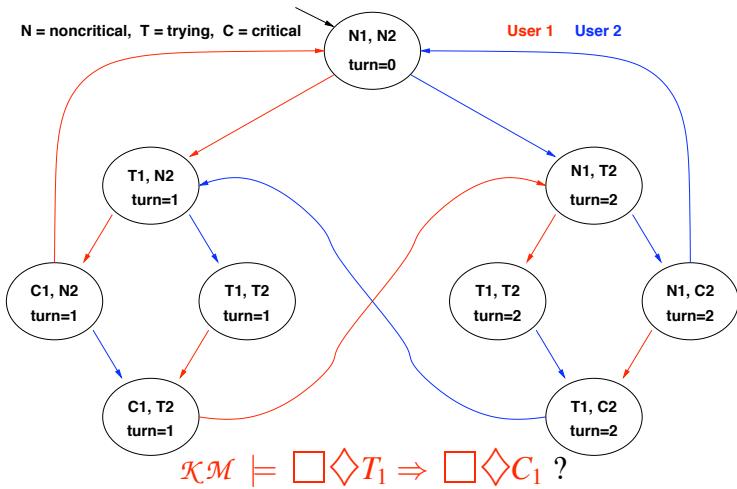
## Example 4: mutual exclusion (fairness)



- 0. 36/??

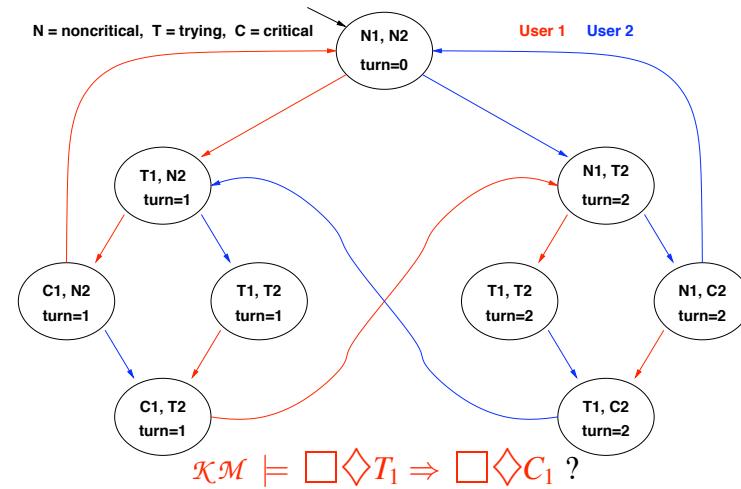
NO: the blue cyclic path is a counterexample!

## Example 4: mutual exclusion (strong fairness)



- 37/??

## Example 4: mutual exclusion (strong fairness)



YES: every path which visits  $T_1$  infinitely often also visits  $C_1$  infinitely often!

- 37/??

## LTL Alternative Notation

Alternative notations are used for temporal operators.

- $\Diamond \sim F$  sometime in the Future
- $\Box \sim G$  Globally in the future
- $\circlearrowleft \sim X$  neXtime

- 38/??

## Summary of Lecture III

- Introducing Temporal Logics.
- Intuitions beyond Linear Temporal Logic.
- LTL: Syntax and Semantics.
- LTL in Computer Science.
- LTL Interpreted over Kripke Models.
- LTL and Model Checking: Intuitions.

- 39/??