

**FORMAL METHODS**  
**LECTURE V – PART II**  
**CTL MODEL CHECKING WITH**  
**FAIRNESS CONSTRAINTS**

**Alessandro Artale**

*Faculty of Computer Science – Free University of Bolzano*

artale@inf.unibz.it

<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.

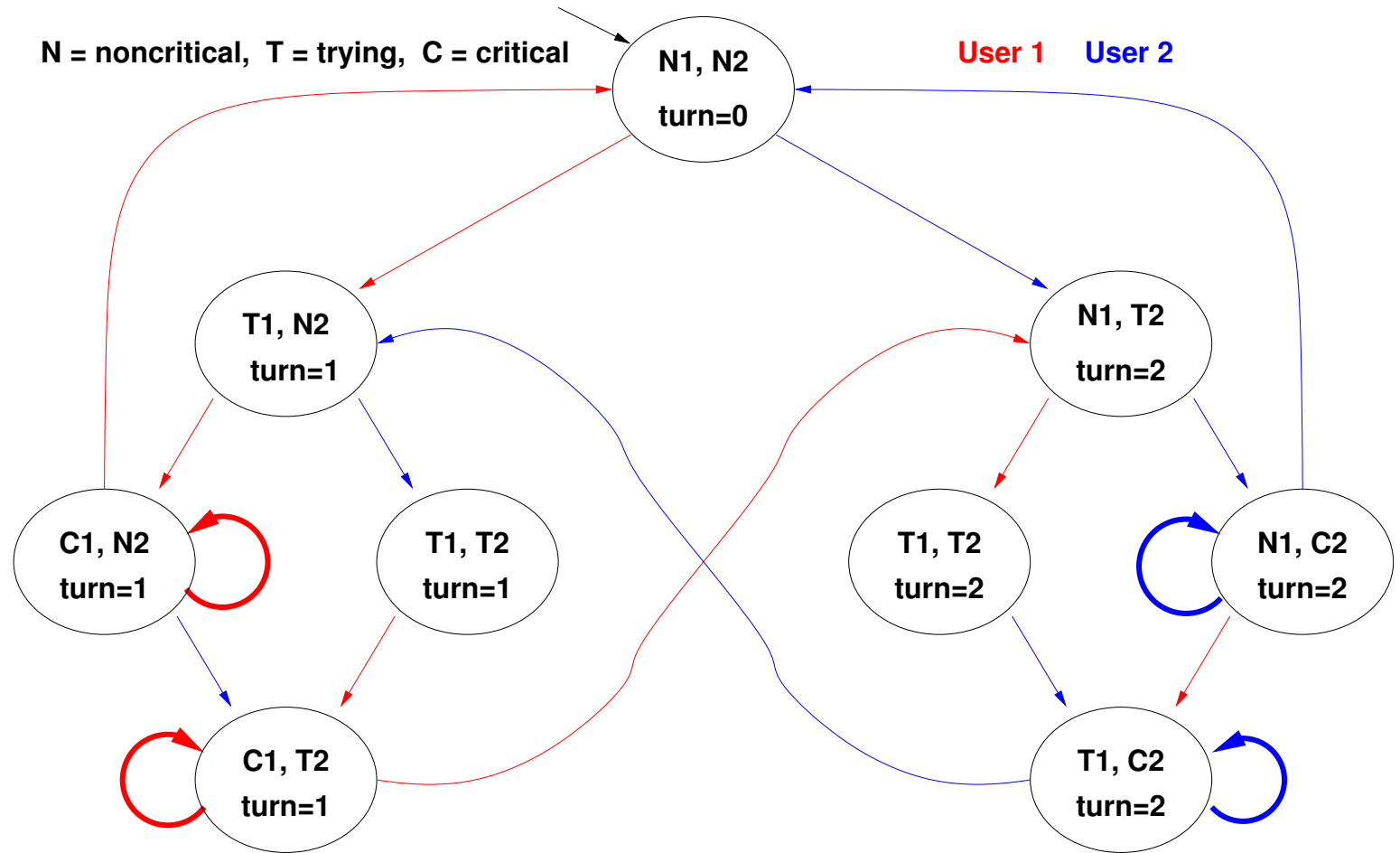
# Fair Kripke Models: An Example

- Consider a variant of the mutual exclusion protocol in which one process can stay in the critical section as long as it likes.
- Do the Liveness conditions still hold?

$$\mathcal{M} \models \boxed{P} \square (T_1 \Rightarrow \boxed{P} \blacklozenge C_1);$$

$$\mathcal{M} \models \boxed{P} \square (T_2 \Rightarrow \boxed{P} \blacklozenge C_2).$$

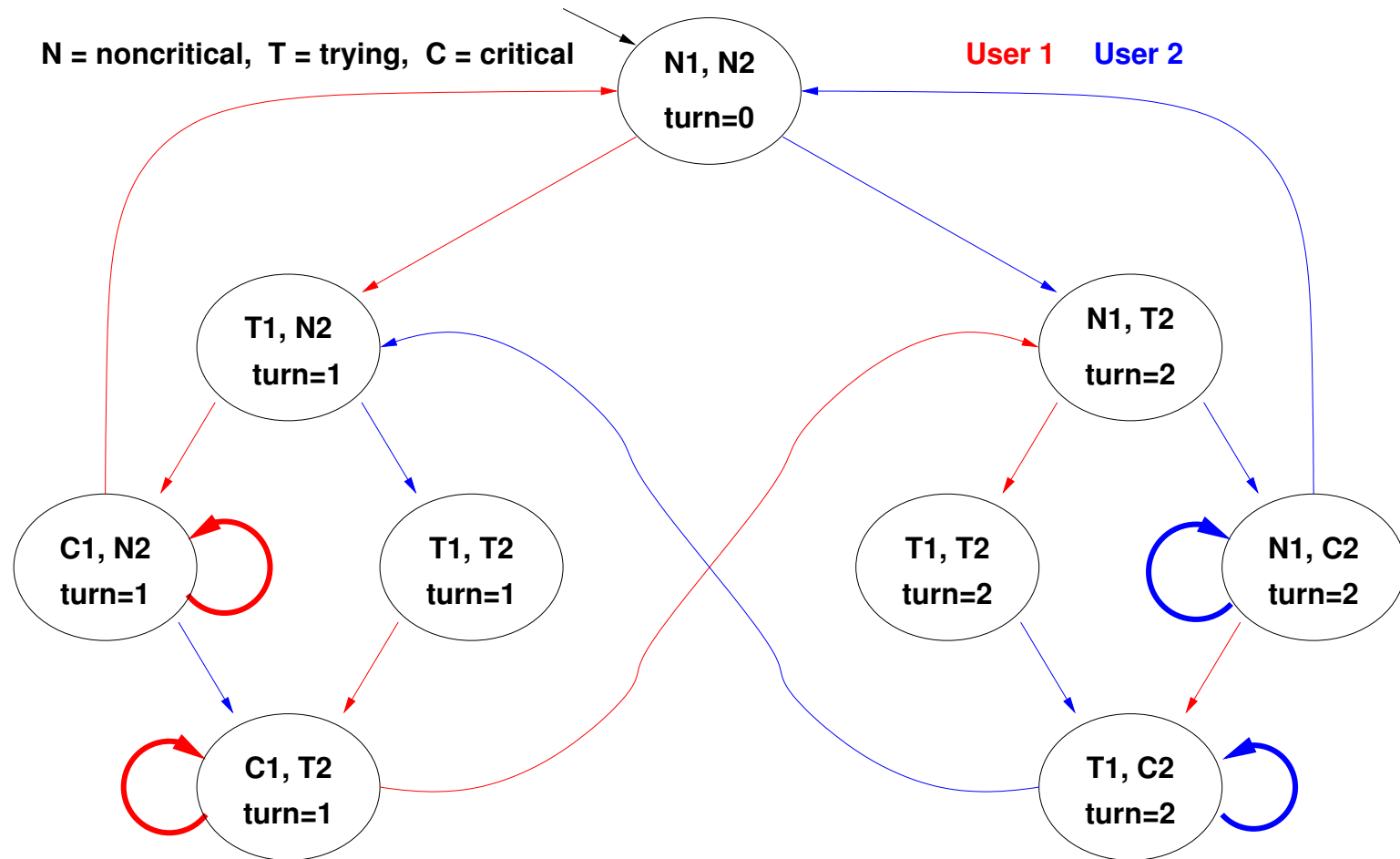
# Fair Kripke Models: An Example (Cont.)



$$\mathcal{M} \models \text{P} \square (T_2 \Rightarrow \text{P} \diamond C_2)?$$

$$\mathcal{M} \models \text{P} \square (T_1 \Rightarrow \text{P} \diamond C_1)?$$

# Fair Kripke Models: An Example (Cont.)



$$\mathcal{M} \models \Box (T_2 \Rightarrow \Box \Diamond C_2)?$$

$$\mathcal{M} \models \Box (T_1 \Rightarrow \Box \Diamond C_1)?$$

**NO:** E.g., it can cycle forever in  $\{C_1, T_2, turn = 1\}$

**Unfair Protocol:** one process might never be served!

# Fairness Conditions in LTL

**Fairness Conditions in LTL.**  $\Box \Diamond \varphi \Rightarrow \psi$ , where  $\psi$  is the formula to be verified.

- Using LTL the fairness conditions of the example can be expressed as:

$$\mathcal{M} \models \Box \Diamond \neg C_2 \Rightarrow \Box (T_1 \Rightarrow \Box \Diamond C_1)$$

$$\mathcal{M} \models \Box \Diamond \neg C_1 \Rightarrow \Box (T_2 \Rightarrow \Box \Diamond C_2)$$

# Fairness Conditions in CTL

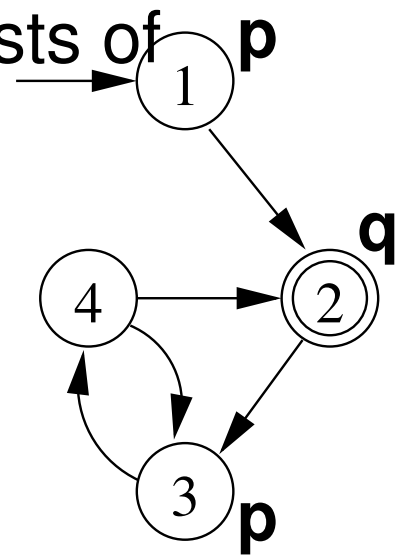
**Fairness Conditions in CTL.** In CTL fairness constraints cannot be expressed!

**Solution.** Impose **Fairness Constraints** on top of the Kripke Model.

- We call **Fair Computation Paths** those paths verifying a fairness constraint **infinitely often**;
- We call **Fair Kripke Models** those models restricted to fair paths.

# Fair Kripke Models

- A Fair Kripke model  $\mathcal{M}_F := \langle S, R, I, AP, L, F \rangle$  consists of
- a set of states  $S$ ;
  - a set of initial states  $I \subseteq S$ ;
  - a set of transitions  $R \subseteq S \times S$ ;
  - a set of atomic propositions  $AP$ ;
  - a labeling  $L : S \mapsto 2^{AP}$ ;
  - a set of fairness conditions  $F = \{f_1, \dots, f_n\}$ , with  $f_i \subseteq S$ .
- E.g.,  $\{\{2\}\} := \{\{s \mid \mathcal{M}, s \models q\}\}$  can be a set of fair conditions of the Kripke model above.
- **Fair path  $\pi$** : At least one state for each  $f_i$  must occur *infinitely often* in  $\pi$ .
- E.g., every path visiting *infinitely often* state 2 is a fair path.



# M.C. with Fair Kripke Models

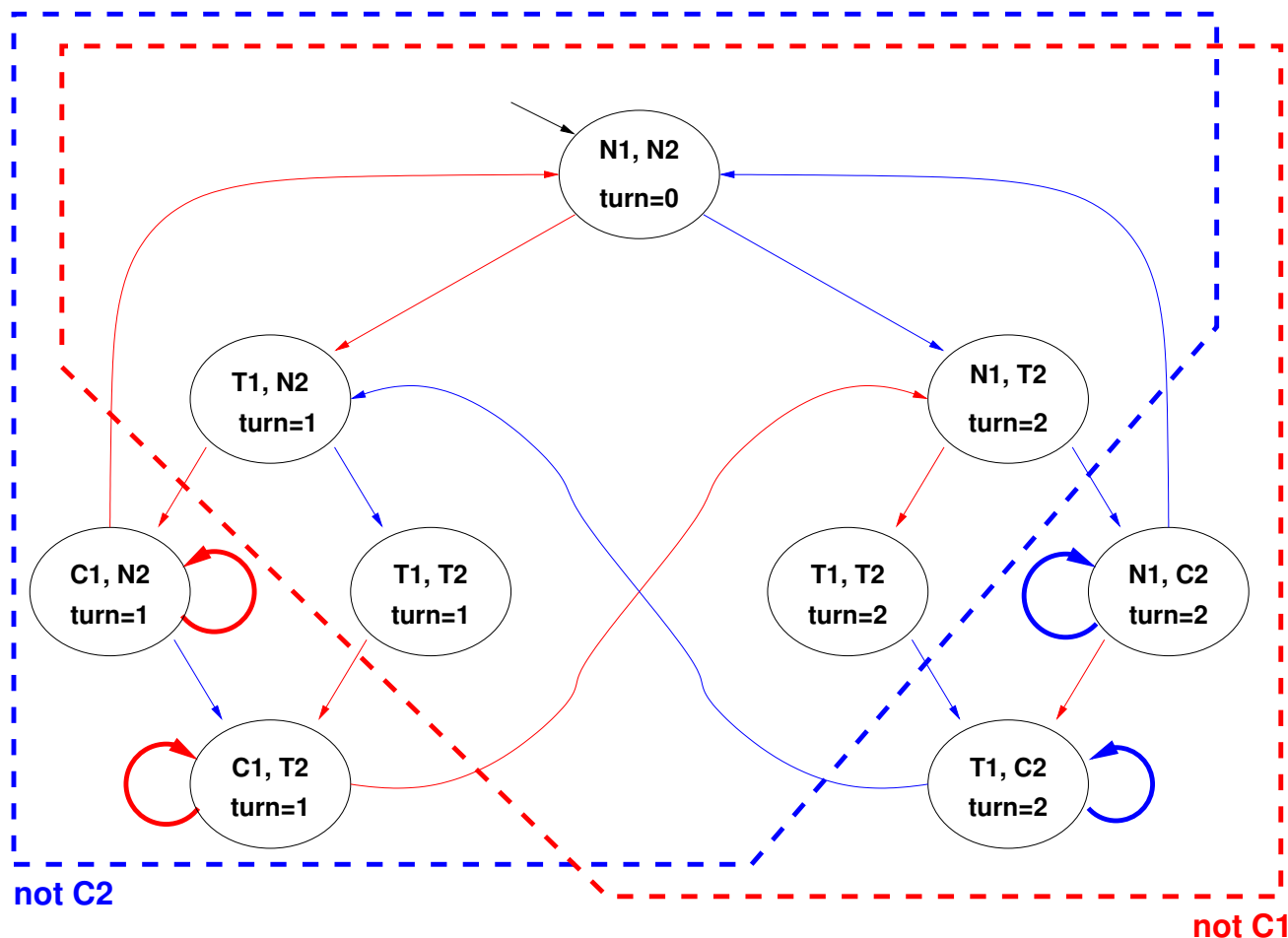
Fair Kripke Models restrict the CTL Model Checking process to fair paths:

> Path quantifiers apply only to fair paths:

- $\mathcal{M}_F, s_i \models \boxed{P} \square \varphi$  iff for every **fair path**  $\pi = (s_i, s_{i+1}, \dots), \forall j \geq i. \mathcal{M}, s_j \models \varphi$ .
- $\mathcal{M}_F, s_i \models \diamond \boxed{P} \square \varphi$  iff for some **fair path**  $\pi = (s_i, s_{i+1}, \dots), \forall j \geq i. \mathcal{M}, s_j \models \varphi$ .

# Fairness Constraints: An Example

$$F := \{ \{s \mid \mathcal{M}, s \models \neg C1\}, \{s \mid \mathcal{M}, s \models \neg C2\} \}$$

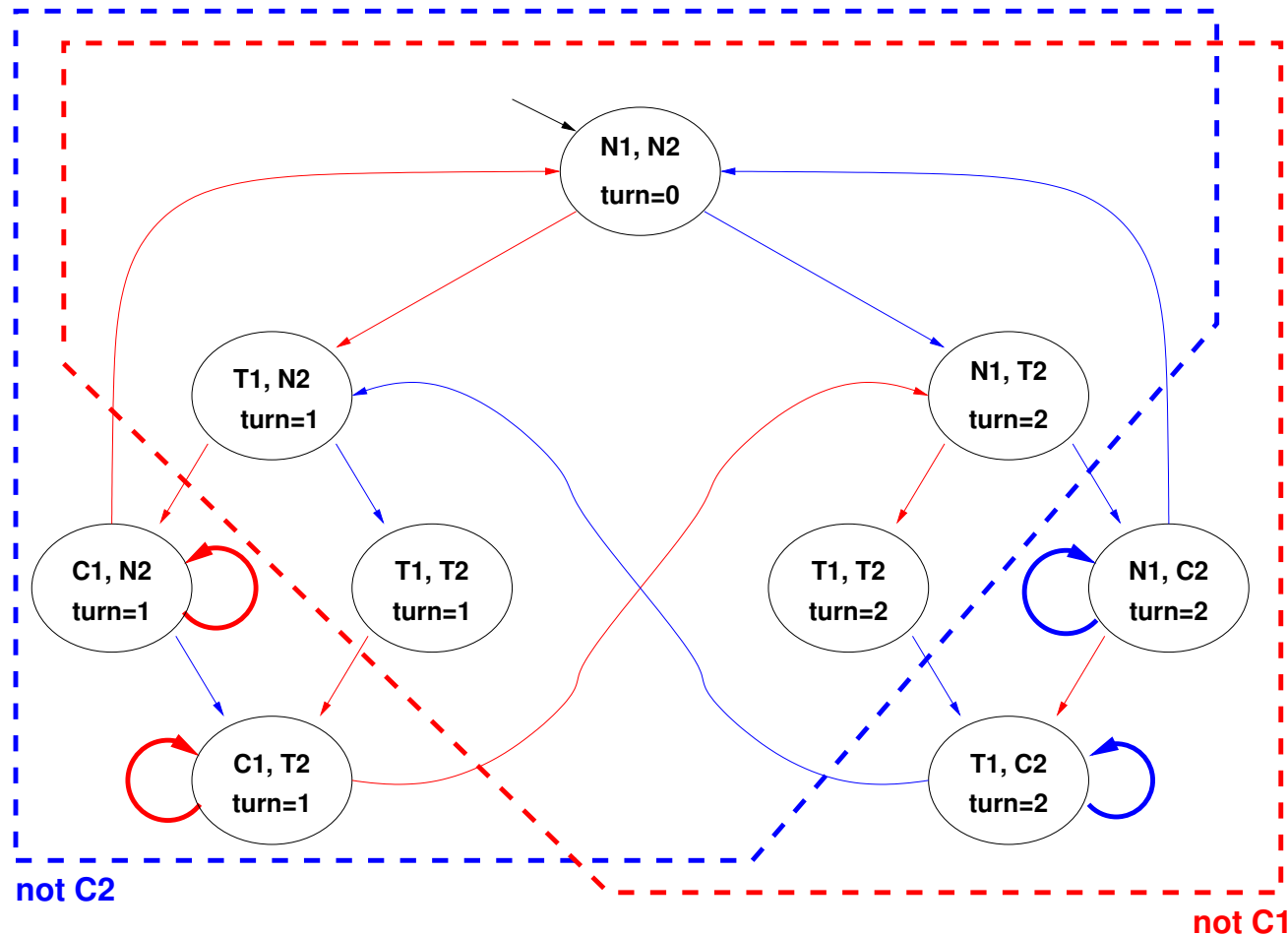


$$\mathcal{M}_F \models \Box (T_1 \Rightarrow \Box \Diamond C_1)?$$

$$\mathcal{M}_F \models \Box (T_2 \Rightarrow \Box \Diamond C_2)?$$

# Fairness Constraints: An Example

$$F := \{ \{s \mid \mathcal{M}, s \models \neg C1\}, \{s \mid \mathcal{M}, s \models \neg C2\} \}$$



$$\mathcal{M}_F \models \Box (T_1 \Rightarrow \Box \Diamond C_1)?$$

$$\mathcal{M}_F \models \Box (T_2 \Rightarrow \Box \Diamond C_2)?$$

**YES:** every **fair path** satisfies the conditions.