CTL Model Checking

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.

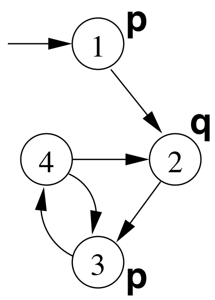
Summary

- CTL Model Checking: General Ideas.
- CTL Model Checking: The Labeling Algorithm.
- Labeling Algorithm in Details.
- CTL Model Checking: Theoretical Issues.

CTL Model Checking

CTL Model Checking is a formal verification technique s.t.

- The system is represented as a Kripke Model $\mathcal{KM}$:



- The property is expressed as a CTL formula φ, e.g.:

$$\mathbf{AG}(p \Rightarrow \mathbf{AF}q)$$

- The algorithm checks whether **all** the initial states, s_0, of the Kripke model satisfy the formula ($\mathcal{KM}, s_0 \models \varphi$).

CTL M.C. Algorithm: General Ideas

The algorithm proceeds along two macro-steps:

1. Construct the set of states where the formula holds:
   $[\![\varphi]\!] := \{s \in S : \mathcal{KM}, s \models \varphi\}$
   ($[\![\varphi]\!]$ is called the denotation of φ);

2. Then compare the denotation with the set of initial states:
   $I \subseteq [\![\varphi]\!]$?

CTL M.C. Algorithm: General Ideas

To compute $[\![\varphi]\!]$ proceed "bottom-up" on the structure of the formula, computing $[\![\varphi_i]\!]$ for each subformula φ_i of φ.

For example, to compute $[\![\mathbf{AG}(p \Rightarrow \mathbf{AF}q)]\!]$ we need to compute:

- $[\![q]\!]$,
- $[\![\mathbf{AF}q]\!]$,
- $[\![p]\!]$,
- $[\![p \Rightarrow \mathbf{AF}q]\!]$,
- $[\![\mathbf{AG}(p \Rightarrow \mathbf{AF}q)]\!]$

CTL M.C. Algorithm: General Ideas

To compute each $[\![\varphi_i]\!]$ for generic subformulas:

- Handle boolean operators by standard set operations;
- Handle temporal operators $\mathbf{AX}$, $\mathbf{EX}$ by computing pre-images;
- Handle temporal operators $\mathbf{AG}$, $\mathbf{EG}$, $\mathbf{AF}$, $\mathbf{EF}$, $\mathbf{AU}$, $\mathbf{EU}$, by applying fixpoint operators.

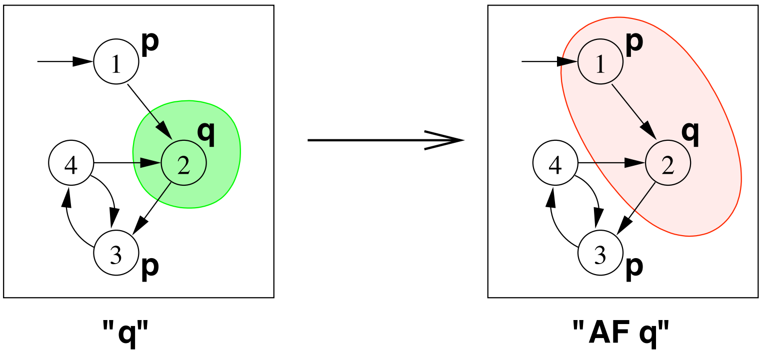
Summary

- CTL Model Checking: General Ideas.
- CTL Model Checking: The Labeling Algorithm.
- Labeling Algorithm in Details.
- CTL Model Checking: Theoretical Issues.

The Labeling Algorithm: General Idea

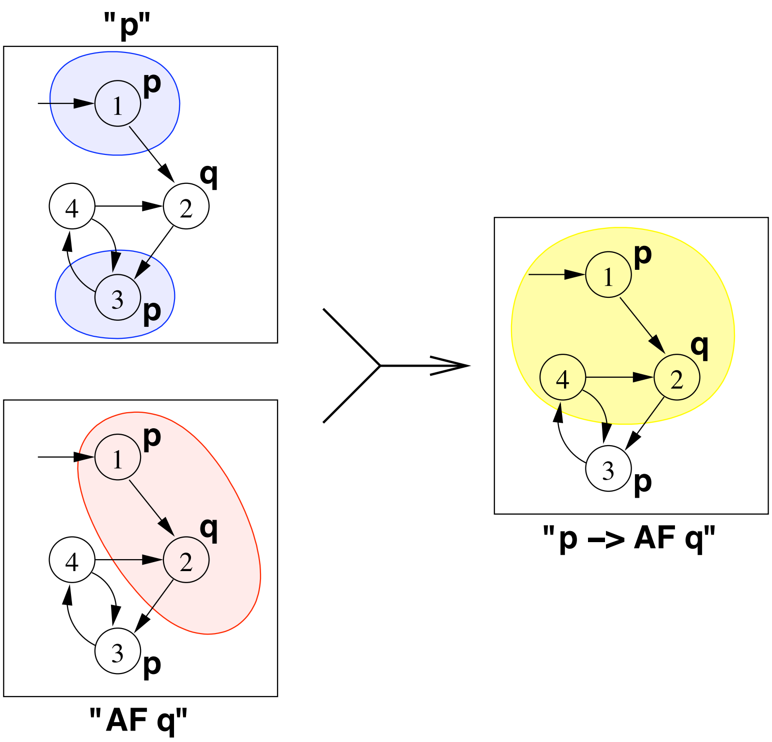
- The Labeling Algorithm given a Kripke Model and a CTL formula outputs the set of states satisfying the formula.
- Main Idea: Label the states of the Kripke Model with the subformulas of φ satisfied there.

The Labeling Algorithm: An Example

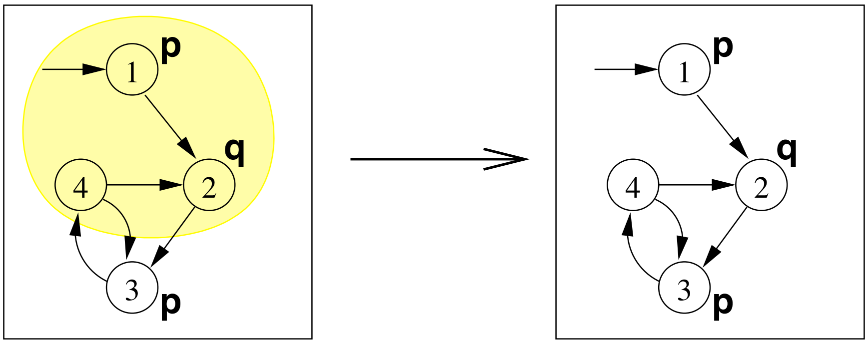


- ▷ $\mathbf{AF}q \equiv (q \vee \mathbf{AX}(\mathbf{AF}q))$
- ▷ $[\![\mathbf{AF}q]\!]$ can be computed as the union of:
  - $[\![q]\!] = \{2\}$
  - $[\![q \vee \mathbf{AX}q]\!] = \{2\} \cup \{1\} = \{1,2\}$
  - $[\![q \vee \mathbf{AX}(q \vee \mathbf{AX}q)]\!] = \{2\} \cup \{1\} = \{1,2\}$ (fixpoint).

The Labeling Algorithm: An Example



The Labeling Algorithm: An Example



"p –> AF q" "AG(p –> AF q)"

- ▷ $\mathbf{AG}\varphi \equiv (\varphi \wedge \mathbf{AX}(\mathbf{AG}\varphi))$
- ▷ $[\![\mathbf{AG}\varphi]\!]$ can be computed as the intersection of:
  - $[\![\varphi]\!] = \{1,2,4\}$
  - $[\![\varphi \wedge \mathbf{AX}\varphi]\!] = \{1,2,4\} \cap \{1,3\} = \{1\}$
  - $[\![\varphi \wedge \mathbf{AX}(\varphi \wedge \mathbf{AX}\varphi)]\!] = \{1,2,4\} \cap \{\} = \{\}$ (fixpoint)

The Labeling Algorithm: An Example

- ▷ The set of states where the formula holds is empty, thus:
  - The initial state does not satisfy the property;
  - $\mathcal{KM} \not\models \mathbf{AG}(p \Rightarrow \mathbf{AF}q)$.
- ▷ Counterexample: A lazo-shaped path: $1,2,\{3,4\}^{\omega}$ (satisfying $\mathbf{EF}(p \wedge \mathbf{EG}\neg q)$)

Summary

- CTL Model Checking: General Ideas.
- CTL Model Checking: The Labeling Algorithm.
- Labeling Algorithm in Details.
- CTL Model Checking: Theoretical Issues.

The Labeling Algorithm: General Schema

▷ Assume φ written in terms of $\neg$, $\wedge$, $\mathbf{EX}$, $\mathbf{EU}$, $\mathbf{EG}$ – minimal set of CTL operators

▷ The Labeling algorithm takes a CTL formula and a Kripke Model as input and returns the set of states satisfying the formula (i.e., the *denotation* of φ):

1. For every $\varphi_i \in Sub(\varphi)$, find $[[\varphi_i]]$;
2. Compute $[[\varphi]]$ starting from $[[\varphi_i]]$;
3. Check if $I \subseteq [[\varphi]]$.

▷ Subformulas $Sub(\varphi)$ of φ are checked bottom-up

▷ To compute each $[[\varphi_i]]$: if the main operator of φ_i is a
- *Boolean Operator*: apply standard set operations;
- *Temporal Operator*: apply recursive rules until a fixpoint is reached.

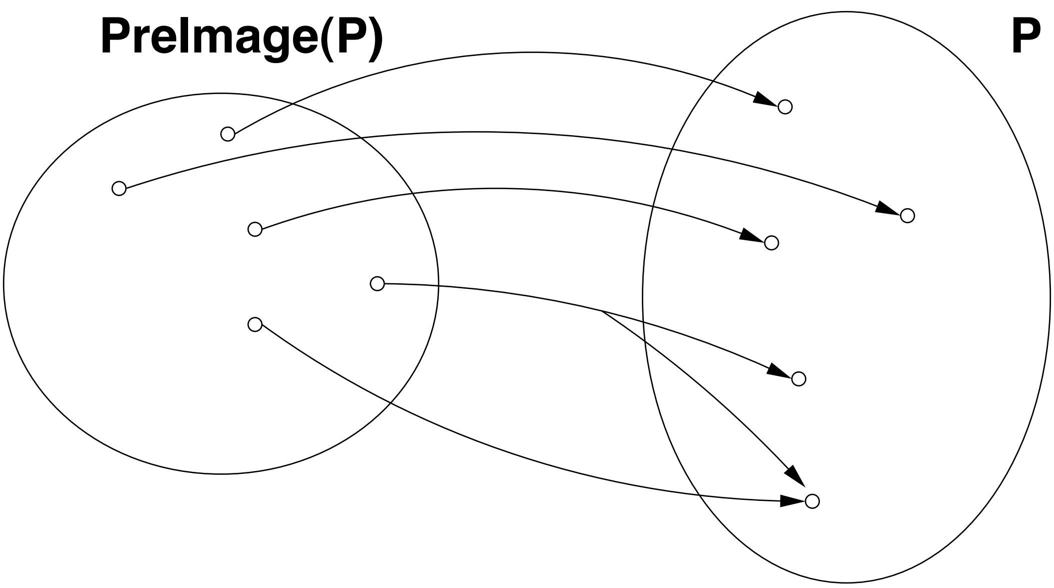
Denotation of Formulas: The Boolean Case

Let $\mathcal{KM} = \langle S, I, R, L, \Sigma \rangle$ be a Kripke Model.

$$
\begin{array}{lcl}
[\![false]\!] & = & \{\} \\
[\![true]\!] & = & S \\
[\![p]\!] & = & \{s \mid p \in L(s)\} \\
[\![\neg\varphi_1]\!] & = & S \setminus [\![\varphi_1]\!] \\
[\![\varphi_1 \wedge \varphi_2]\!] & = & [\![\varphi_1]\!] \cap [\![\varphi_2]\!]
\end{array}
$$

Denotation of Formulas: The EX Case

- ▷ $[\![\mathbf{EX}\varphi]\!] = \{s \in S \mid \exists s'.\langle s, s'\rangle \in R \text{ and } s' \in [\![\varphi]\!]\}$
- ▷ $[\![\mathbf{EX}\varphi]\!]$ is said to be the Pre-image of $[\![\varphi]\!]$ ($\textsc{Pre}([\![\varphi]\!])$).
- ▷ Key step of every CTL M.C. operation.



Denotation of Formulas: The EG Case

- From the semantics of the $\Box$ temporal operator:

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

- Then, the following equivalence holds:

  $$\mathbf{EG}\varphi \equiv \varphi \wedge \mathbf{EX}(\mathbf{EG}\varphi)$$

- To compute $[\![\mathbf{EG}\varphi]\!]$ we can apply the following recursive definition:

  $$[\![\mathbf{EG}\varphi]\!] = [\![\varphi]\!] \cap \textsc{Pre}([\![\mathbf{EG}\varphi]\!])$$

Denotation of Formulas: The EG Case

- We can compute $X := [\![\mathbf{EG}\varphi]\!]$ inductively as follows:

  $$\begin{array}{lcl} X_1 & := & [\![\varphi]\!] \\ X_2 & := & X_1 \cap \textsc{Pre}(X_1) \\ \ldots & & \\ X_{j+1} & := & X_j \cap \textsc{Pre}(X_j) \end{array}$$

- When $X_n = X_{n+1}$ we reach a fixpoint and we stop.
- **Termination.** Since $X_{j+1} \subseteq X_j$ for every $j \geq 0$, thus a fixed point always exists (Knaster-Tarski's theorem).

Denotation of Formulas: The EU Case

- From the semantics of the $\mathcal{U}$ temporal operator:

  $\varphi\,\mathcal{U}\,\psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi\,\mathcal{U}\,\psi))$
- Then, the following equivalence holds:

  $(\varphi \mathbf{EU} \psi) \equiv \psi \vee (\varphi \wedge \mathbf{EX}(\varphi \mathbf{EU} \psi))$
- To compute $[\![(\varphi \mathbf{EU} \psi)]\!]$ we can apply the following recursive definition:

  $[\![(\varphi \mathbf{EU} \psi)]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \textsc{Pre}([\![(\varphi \mathbf{EU} \psi)]\!]))$

Denotation of Formulas: The EU Case

- We can compute $X := [\![(\varphi \mathbf{EU} \psi)]\!]$ inductively as follows:

$$
\begin{aligned}
X_1 &:= [\![\psi]\!] \\
X_2 &:= X_1 \cup ([\![\varphi]\!] \cap \textsc{Pre}(X_1)) \\
\dots & \\
X_{j+1} &:= X_j \cup ([\![\varphi]\!] \cap \textsc{Pre}(X_j))
\end{aligned}
$$

- When $X_n = X_{n+1}$ we reach a fixpoint and we stop.
- **Termination.** Since $X_{j+1} \supseteq X_j$ for every $j \geq 0$, thus a fixed point always exists (Knaster-Tarski's theorem).

The Pseudo-Code

We assume the Kripke Model to be a global variable:

FUNCTION Label(φ) {
  case φ **of**
    $true$: **return** S;
    $false$: **return** $\{\}$;
    an atom p: **return** $\{s \in S \mid p \in L(s)\}$;
    $\neg\varphi_1$: **return** $S \backslash$Label(φ_1);
    $\varphi_1 \wedge \varphi_2$: **return** Label($\varphi_1$)$\cap$Label($\varphi_2$);
    $\mathbf{EX}\varphi_1$: **return** PRE(Label(φ_1));
    $(\varphi_1 \mathbf{EU} \varphi_2)$: **return** Label_EU(Label(φ_1),Label(φ_2));
    $\mathbf{EG}\varphi_1$: **return** Label_EG(Label(φ_1));
  end case
}

PreImage

$[\![\mathbf{EX}\varphi]\!] = \text{PRE}([\![\varphi]\!]) = \{s \in S \mid \exists s'.\langle s, s'\rangle \in R \text{ and } s' \in [\![\varphi]\!]\}$

FUNCTION PRE($[\![\varphi]\!]$){
  var X;
  $X := \{\}$;
  for each $s' \in [\![\varphi]\!]$ **do**
    for each $s \in S$ **such that** $\langle s, s'\rangle \in R$ **do**
      $X := X \cup \{s\}$;
  return X
}

Label_EG

$[\![\mathbf{EG}\varphi]\!] = [\![\varphi]\!] \cap \textsc{Pre}([\![\mathbf{EG}\varphi]\!])$

```
FUNCTION LABEL_EG([[φ]]){
    var X, OLD-X;
    X := [[φ]];
    OLD-X := ∅;
    while X ≠ OLD-X
    begin
        OLD-X := X;
        X := X ∩ PRE(X)
    end
    return X
}
```


Label_EU

$[\![(\varphi\mathbf{EU}\psi)]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \textsc{Pre}([\![(\varphi\mathbf{EU}\psi)]\!]))$

```
FUNCTION LABEL_EU([[φ]],[[ψ]]){
    var X, OLD-X;
    X := [[ψ]];
    OLD-X := S;
    while X ≠ OLD-X
    begin
        OLD-X := X;
        X := X ∪ ([[φ]] ∩ PRE(X))
    end
    return X
}
```

Summary

- CTL Model Checking: General Ideas.
- CTL Model Checking: The Labeling Algorithm.
- Labeling Algorithm in Details.
- CTL Model Checking: Theoretical Issues.

Correctness and Termination

- The Labeling algorithm works recursively on the structure φ.
- For most of the logical constructors the algorithm does the correct things according to the semantics of CTL.
- To prove that the algorithm is *Correct* and *Terminating* we need to prove the correctness and termination of both **EG** and **EU** operators.

Monotone Functions and Fixpoints

Definition. Let S be a set and F a function, $F : 2^S \to 2^S$, then:

1. F is monotone iff $X \subseteq Y$ then $F(X) \subseteq F(Y)$;
2. A subset X of S is called a fixpoint of F iff $F(X) = X$;
3. X is a least fixpoint (LFP) of F, written $\mu X.F(X)$, iff, for every other fixpoint Y of F, $X \subseteq Y$
4. X is a greatest fixpoint (GFP) of F, written $\nu X.F(X)$, iff, for every other fixpoint Y of F, $Y \subseteq X$

Example. Let $S = \{s_0, s_1\}$ and $F(X) = X \cup \{s_0\}$.

Knaster-Tarski Theorem

Notation: $F^i(X)$ means applying F i-times, i.e., $F(F(\ldots F(X)\ldots))$.

Theorem[Knaster-Tarski]. Let S be a finite set with $n+1$ elements. If $F : 2^S \to 2^S$ is a monotone function then:

1. $\mu X.F(X) \equiv F^{n+1}(\emptyset)$;
2. $\nu X.F(X) \equiv F^{n+1}(S)$.

Correctness and Termination: EG Case

The function LABEL_EG computes:

$$[\![\mathbf{EG}\varphi]\!] = [\![\varphi]\!] \cap \text{PRE}([\![\mathbf{EG}\varphi]\!])$$

applying the semantic equivalence:

$$\mathbf{EG}\varphi \equiv \varphi \wedge \mathbf{EX}(\mathbf{EG}\varphi)$$

Thus, $[\![\mathbf{EG}\varphi]\!]$ is the fixpoint of the function:

$$F(X) = [\![\varphi]\!] \cap \text{PRE}(X)$$

Correctness and Termination: EG Case

Theorem. Let $F(X) = [\![\varphi]\!] \cap \text{PRE}(X)$, and let S have $n+1$ elements. Then:

1. F is monotone;
2. $[\![\mathbf{EG}\varphi]\!]$ is the greatest fixpoint of F.

Correctness and Terminationpr: EU Case

The function LABEL_EU computes:

$$[\![(\varphi \mathbf{EU} \psi)]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \textsc{Pre}([\![(\varphi \mathbf{EU} \psi)]\!]))$$

applying the semantic equivalence:

$$(\varphi \mathbf{EU} \psi) \equiv \psi \vee (\varphi \wedge \mathbf{EX}(\varphi \mathbf{EU} \psi))$$

Thus, $[\![(\varphi \mathbf{EU} \psi)]\!]$ is the fixpoint of the function:

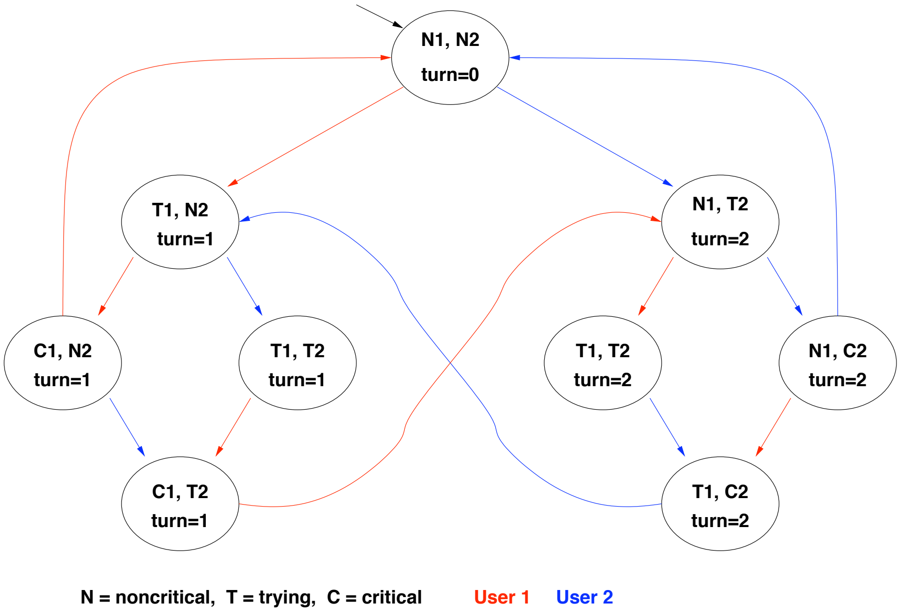
$$F(X) = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \textsc{Pre}(X))$$

Correctness and Termination: EU Case

Theorem. Let $F(X) = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \textsc{Pre}(X))$, and let S have $n+1$ elements. Then:

1. F is monotone;
2. $[\![(\varphi \mathbf{EU} \psi)]\!]$ is the least fixpoint of F.

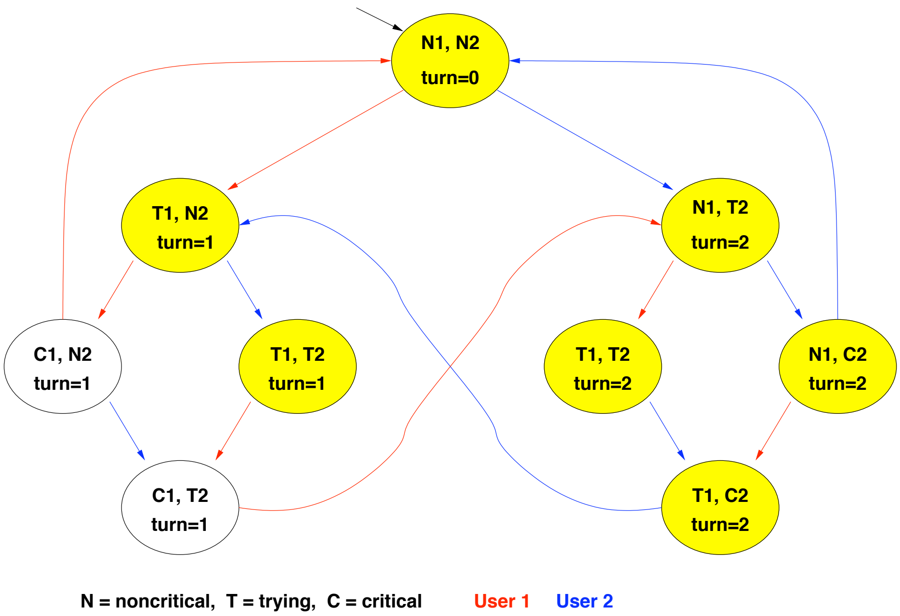
Example 1: fairness



$M \models \mathbf{AGAF}C_1$? $\Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1$?

Example 1: fairness

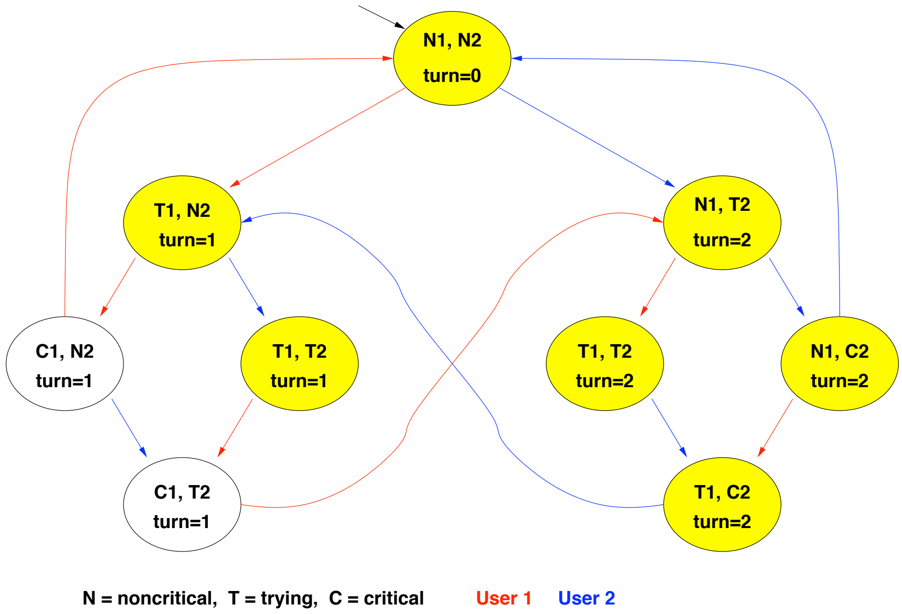
$[\neg C_1]$



$M \models \mathbf{AGAF}C_1$? $\Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1$?

Example 1: fairness

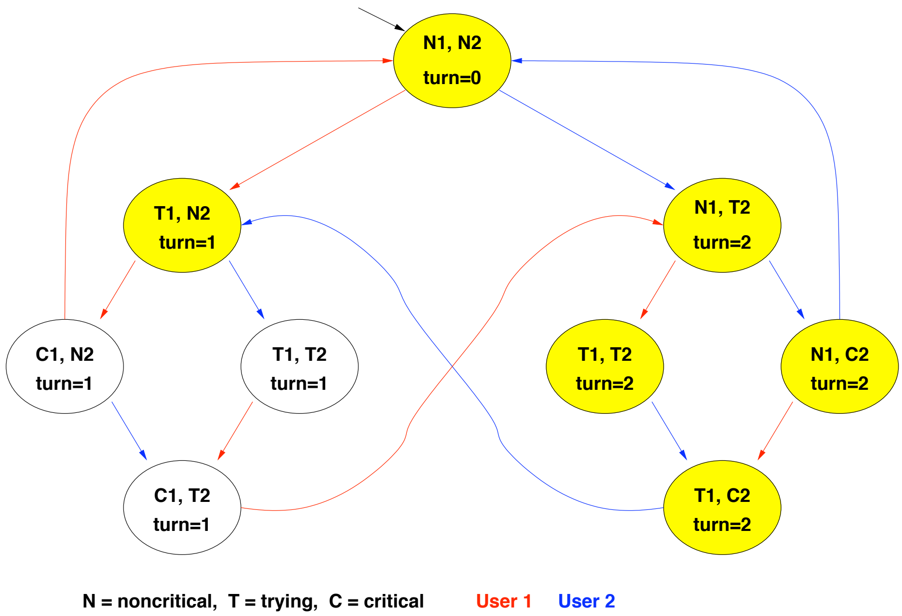
$[\mathbf{EG}\neg C_1]$, step 0:



$M \models \mathbf{AGAF}C_1\ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1\ ?$

Example 1: fairness

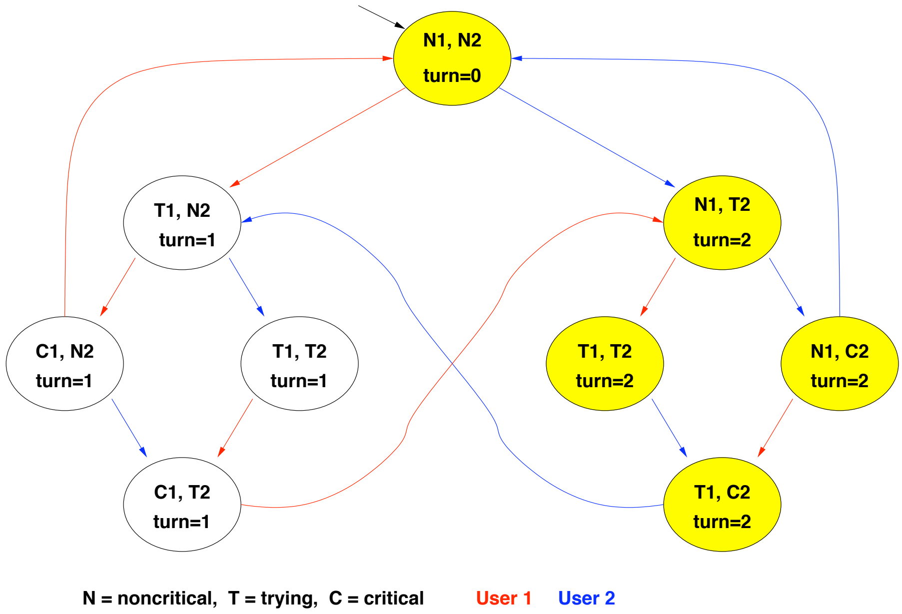
$[\mathbf{EG}\neg C_1]$, step 1:



$M \models \mathbf{AGAF}C_1\ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1\ ?$

Example 1: fairness

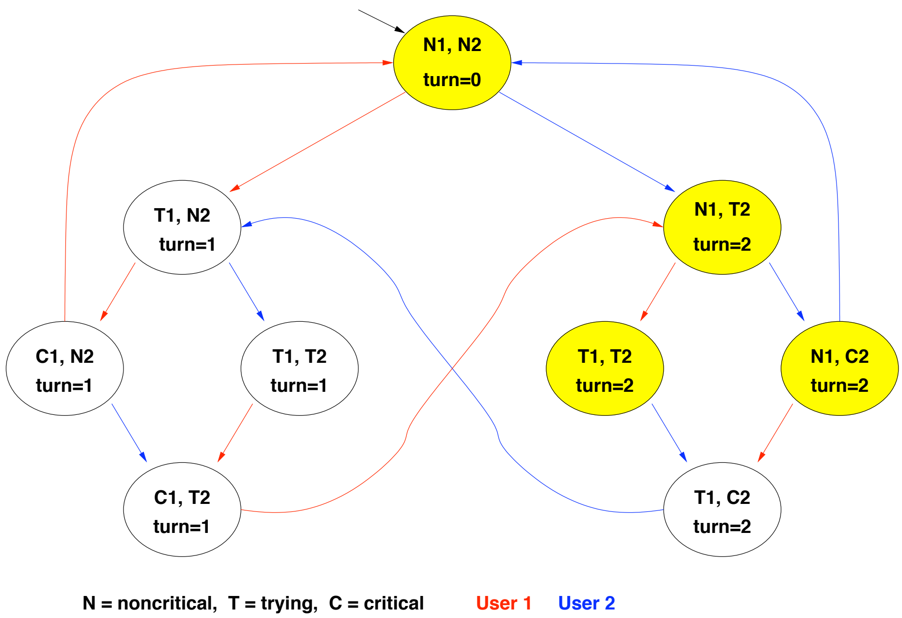
$[\mathbf{EG}\neg C_1]$, step 2:



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

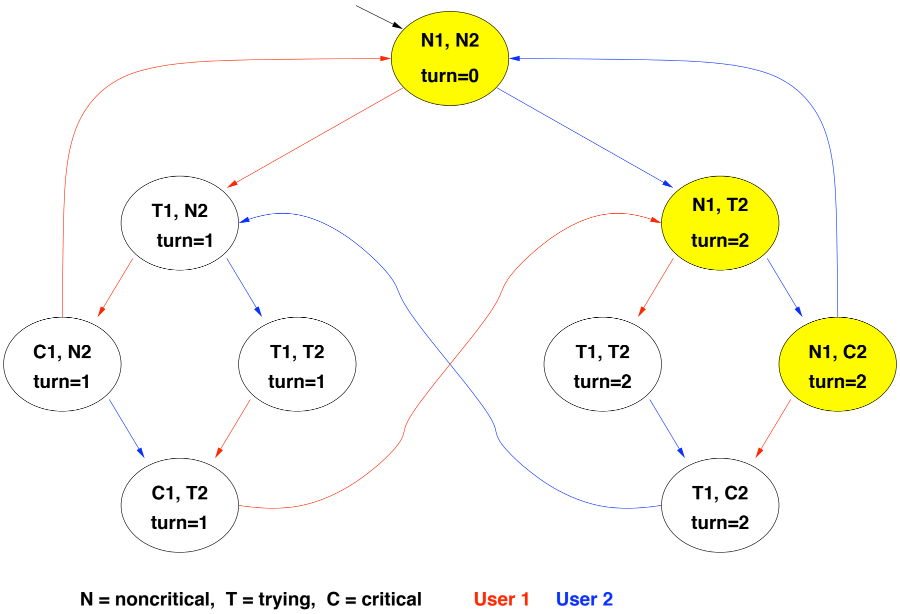
$[\mathbf{EG}\neg C_1]$, step 3:



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

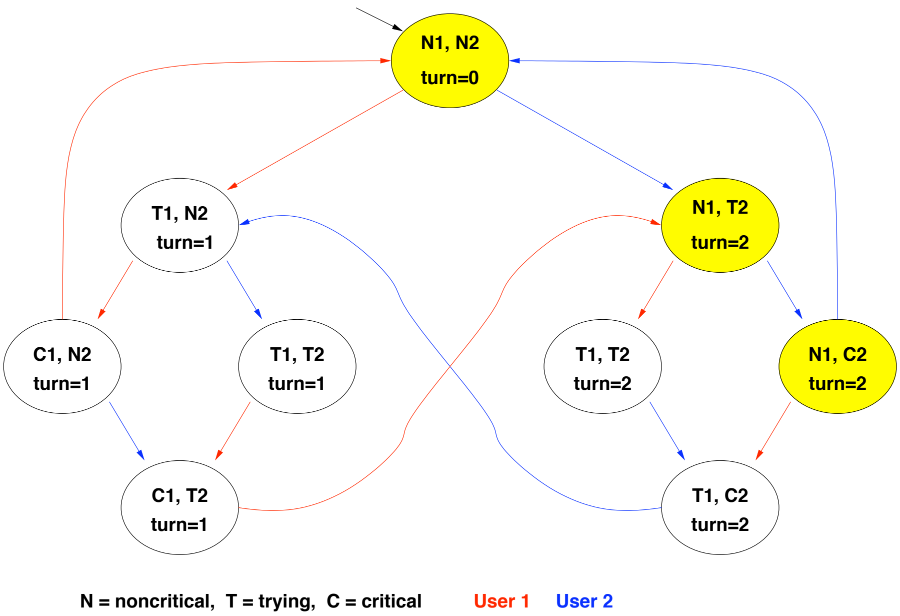
$[\mathbf{EG}\neg C_1]$, step 4:



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

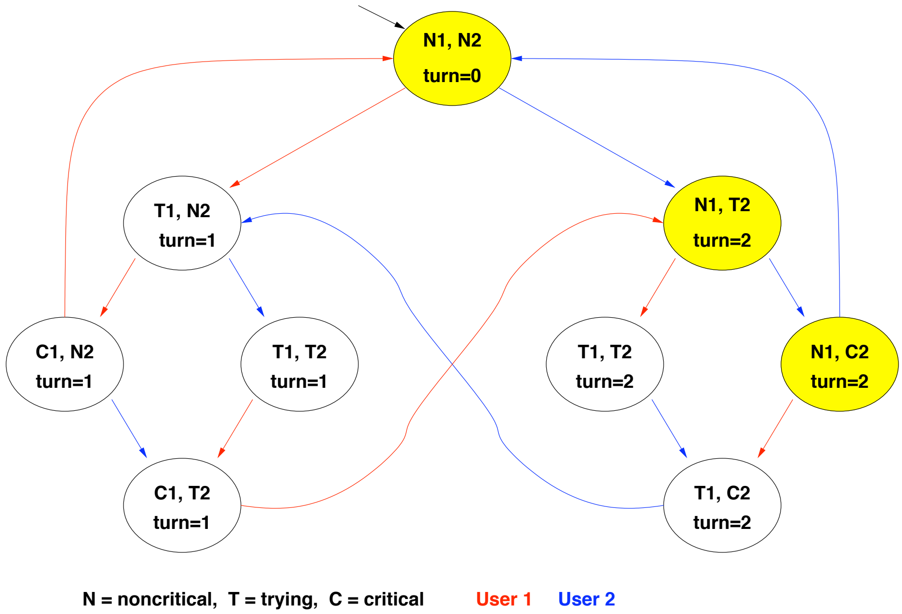
$[\mathbf{EG}\neg C_1]$, FIXPOINT!



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

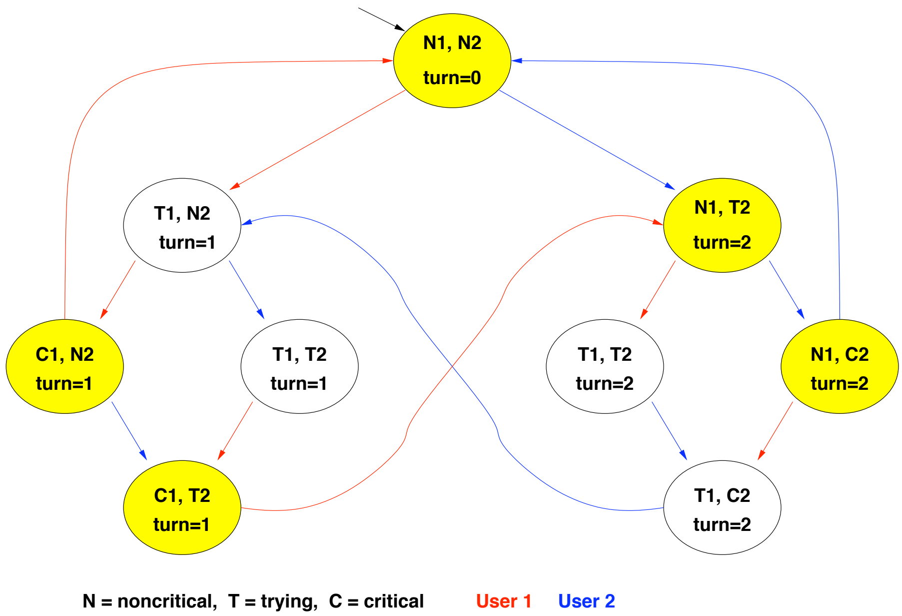
$[\mathbf{EFEG}\neg C_1]$, STEP 0



$$M \models \mathbf{AGAF}C_1 \;? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \;?$$

Example 1: fairness

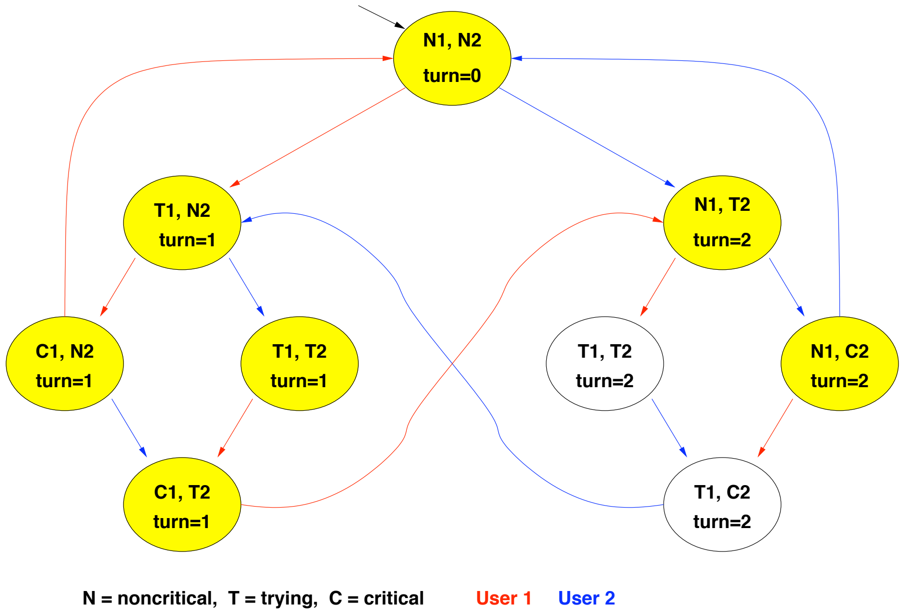
$[\mathbf{EFEG}\neg C_1]$, STEP 1



$$M \models \mathbf{AGAF}C_1 \;? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \;?$$

Example 1: fairness

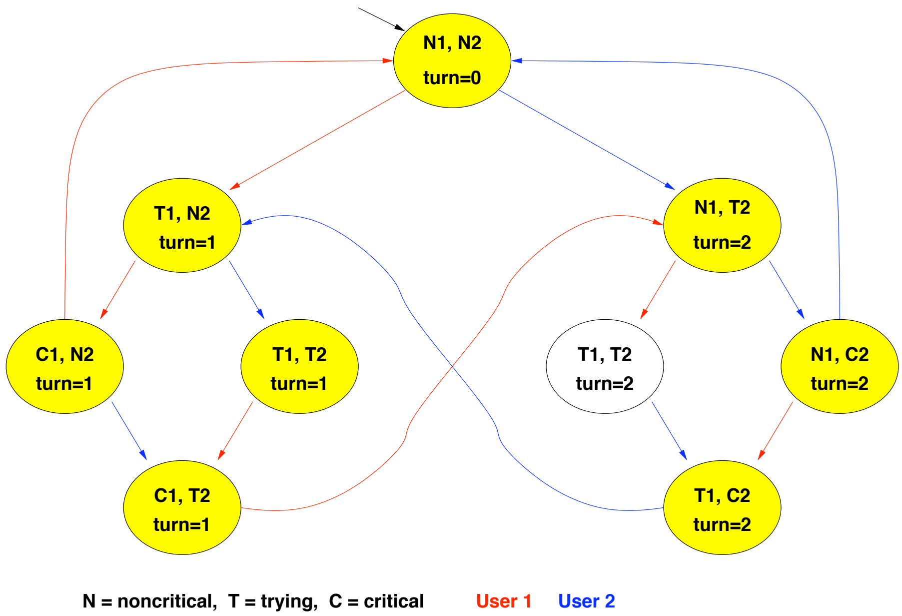
$[\mathbf{EFEG}\neg C_1]$, STEP 2



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

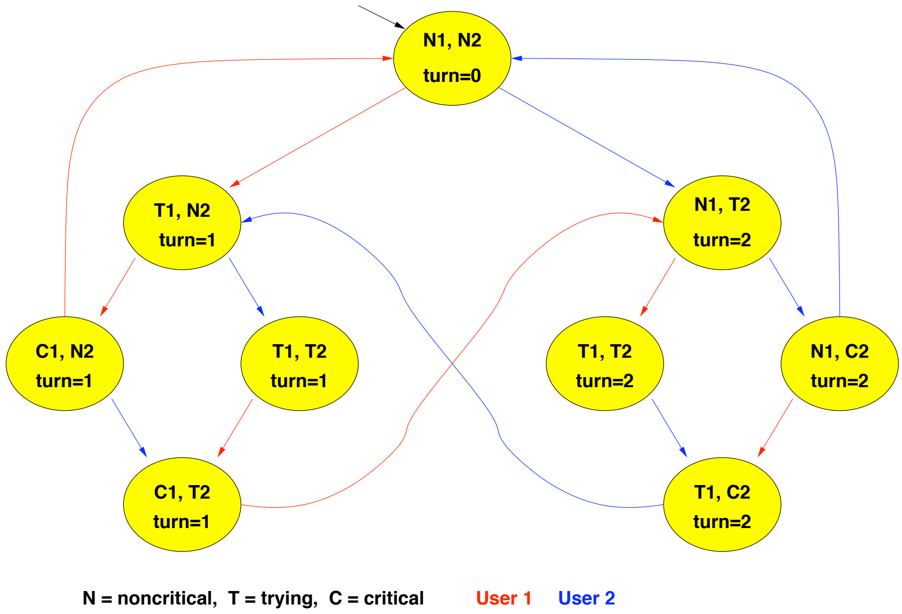
$[\mathbf{EFEG}\neg C_1]$, STEP 3



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

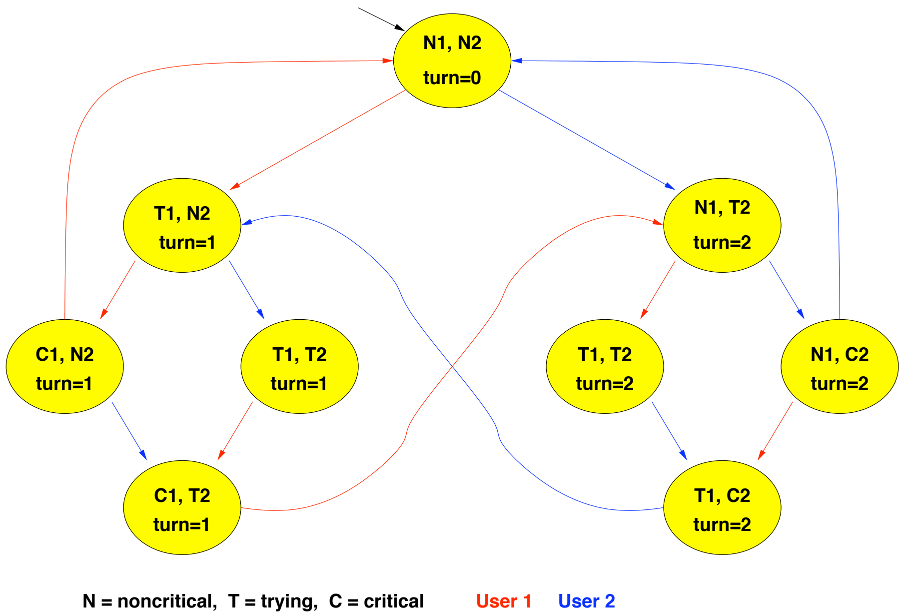
$[\mathbf{EFEG}\neg C_1]$, STEP 4



$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

Example 1: fairness

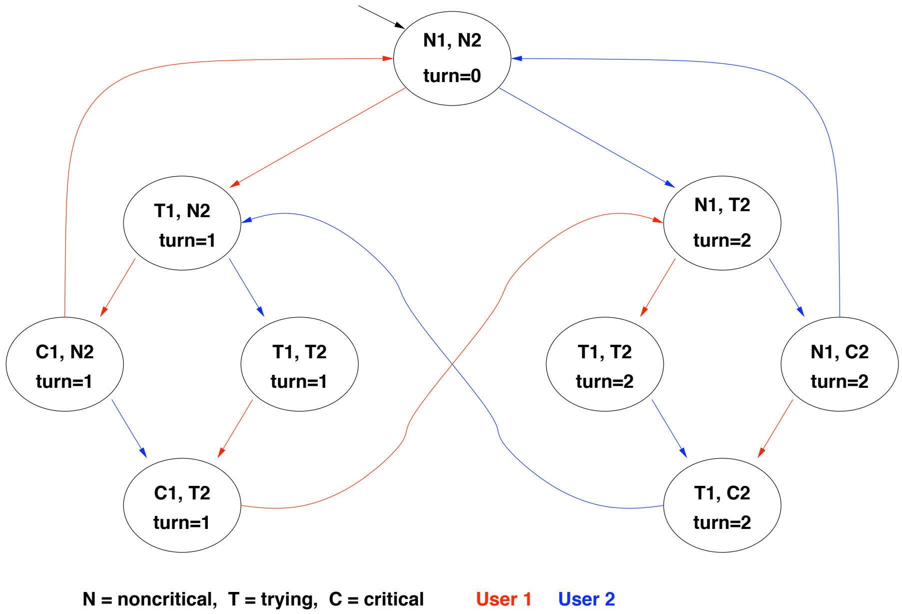
$[\mathbf{EFEG}\neg C_1]$, FIXPOINT!



$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

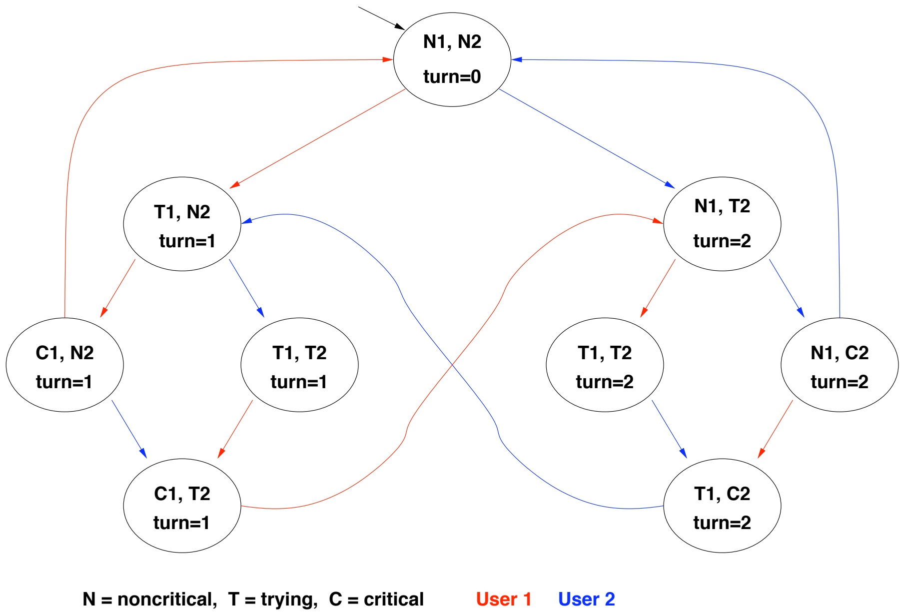
Example 1: fairness

$[\neg \mathbf{EFEG} \neg C_1]$



$M \models \mathbf{AGAF} C_1 \ ? \Longrightarrow M \models \neg \mathbf{EFEG} \neg C_1 \ ? \Longrightarrow$ NO!

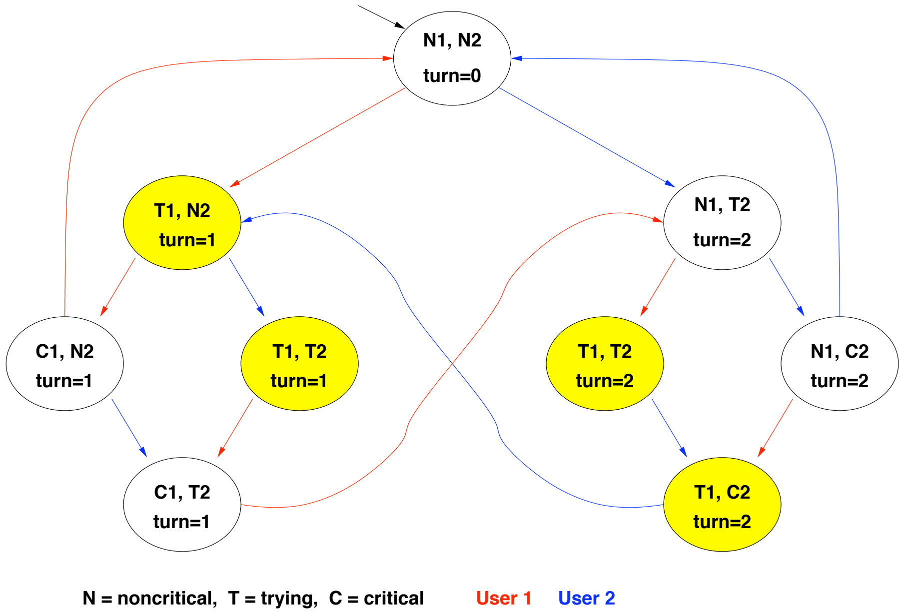
Example 2: liveness



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF} C_1) \ ? \Longrightarrow M \models \neg \mathbf{EF}(T_1 \wedge \mathbf{EG} \neg C_1) \ ?$

Example 2: liveness

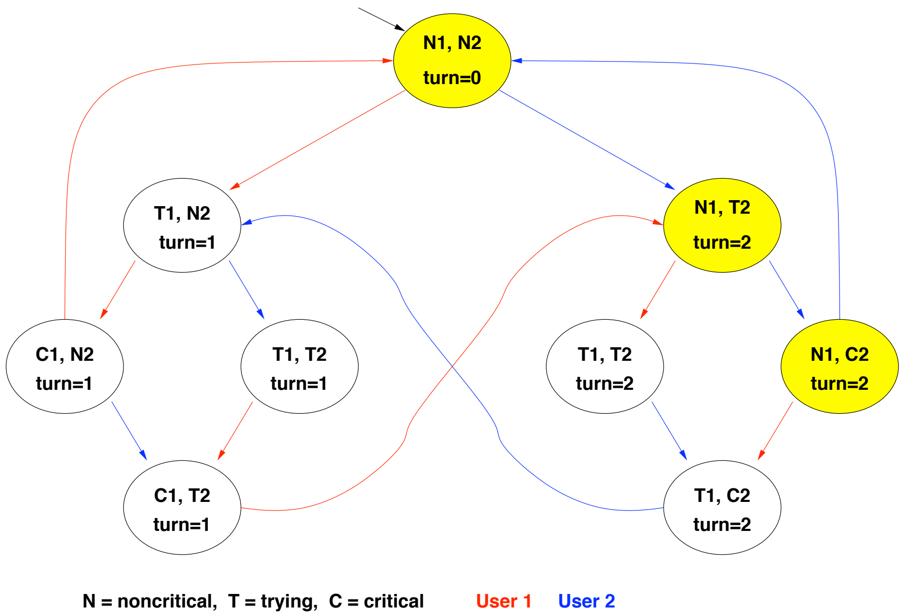
$[T_1]$:



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)$? $\Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)$?

Example 2: liveness

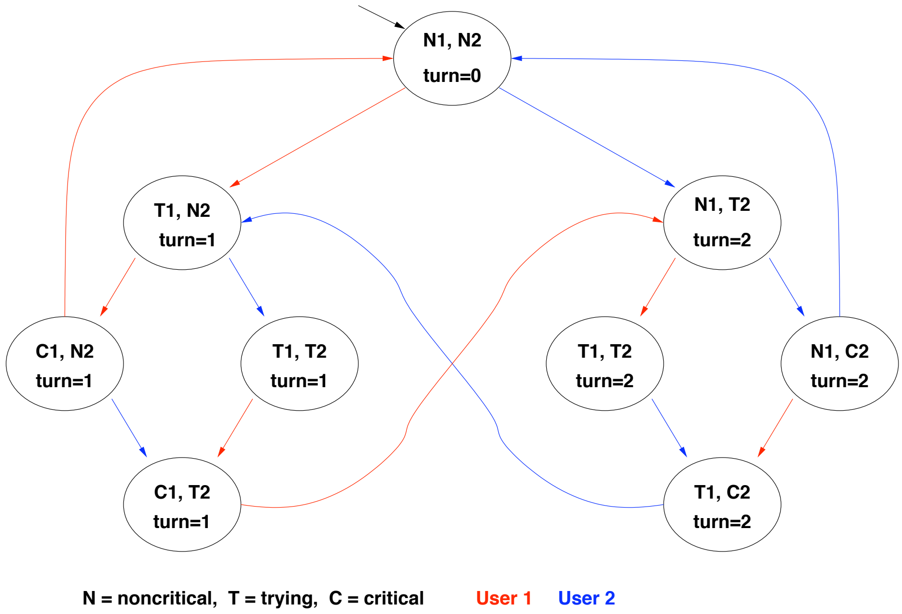
$[\mathbf{EG}\neg C_1]$, STEPS 0-4: (see previous example)



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)$? $\Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)$?

Example 2: liveness

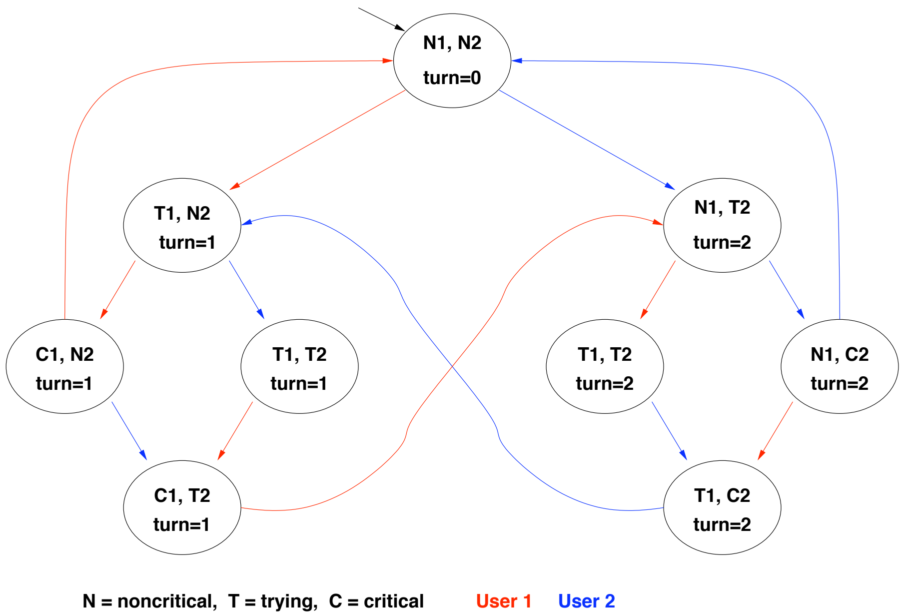
$[T_1 \wedge \mathbf{EG}\neg C_1]$:



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$

Example 2: liveness

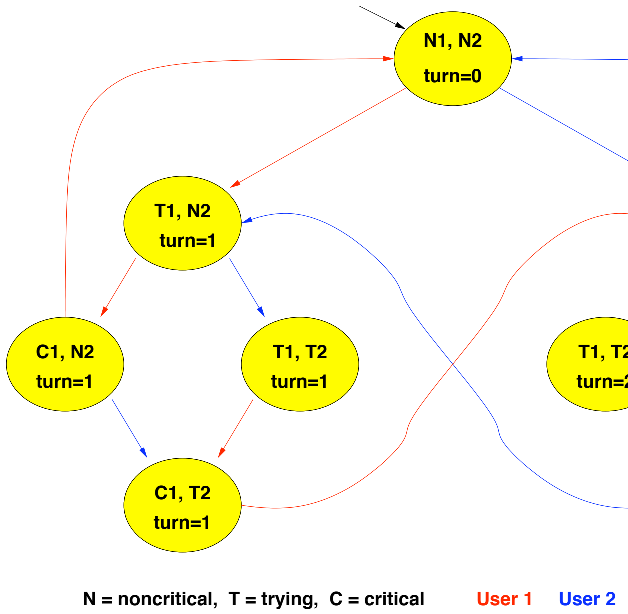
$[\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)]$:



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$

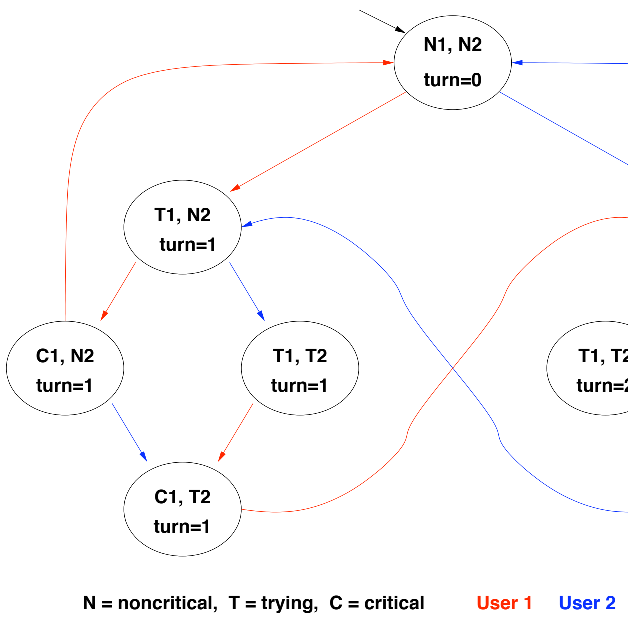
Example 2: liveness

$[\neg \mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)]$:



$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)$? $\Longrightarrow M \models \neg \mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)$? YES!

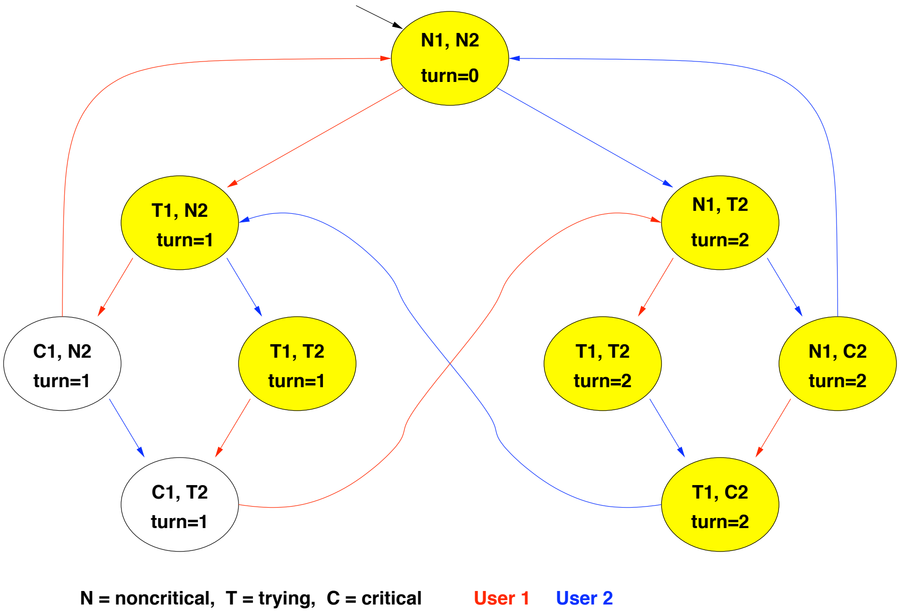
Example 1: fairness



$M \models \mathbf{AGAF}C_1$? $\Longrightarrow M \models \neg \mathbf{EFEG}\neg C_1$?

Example 1: fairness

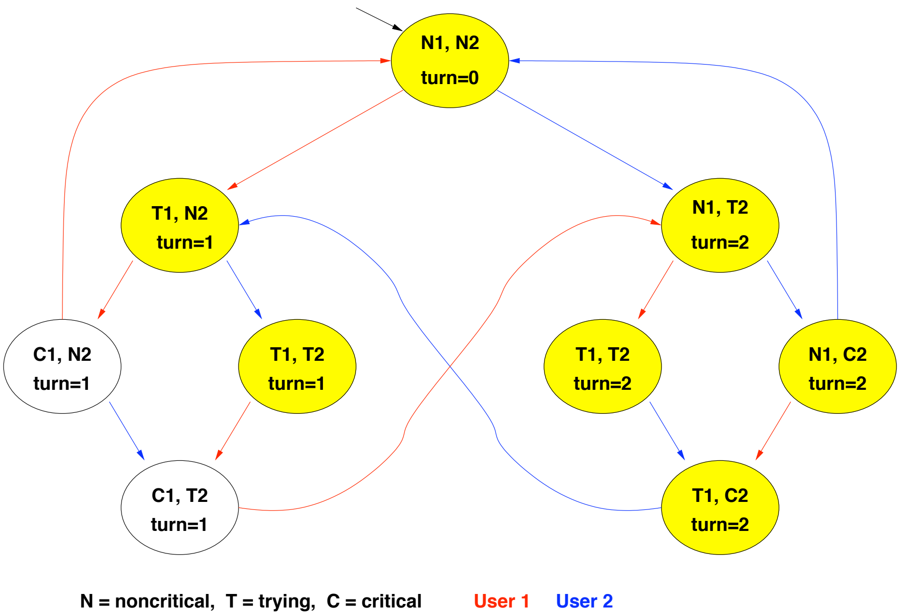
$[\neg C_1]$



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

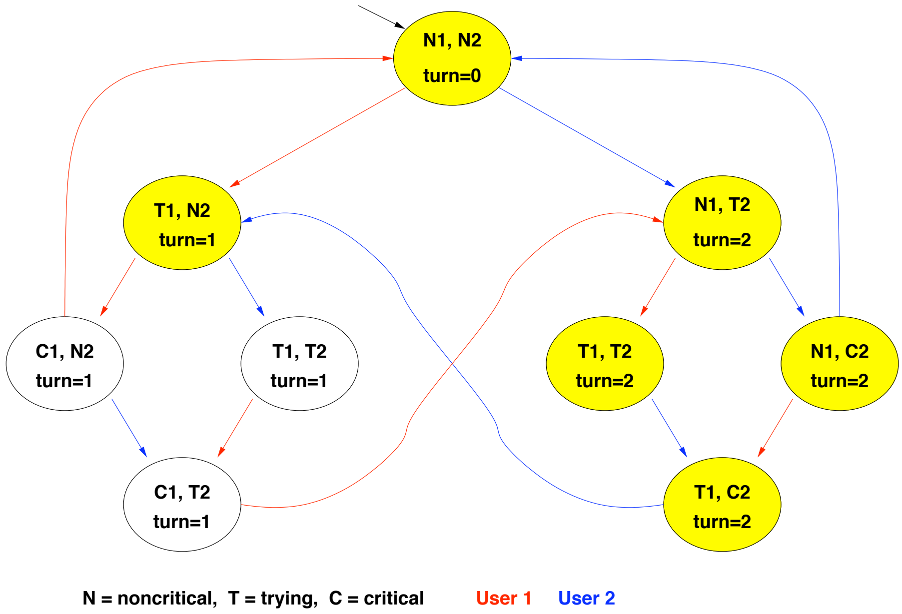
$[\mathbf{EG}\neg C_1]$, step 0:



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

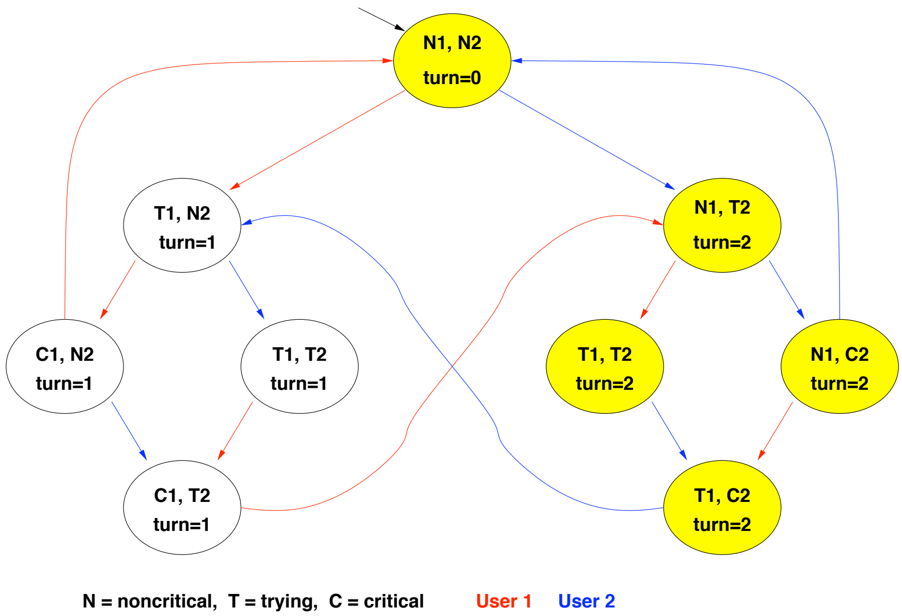
$[\mathbf{EG}\neg C_1]$, step 1:



$M \models \mathbf{AGAF}C_1$? $\Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1$?

Example 1: fairness

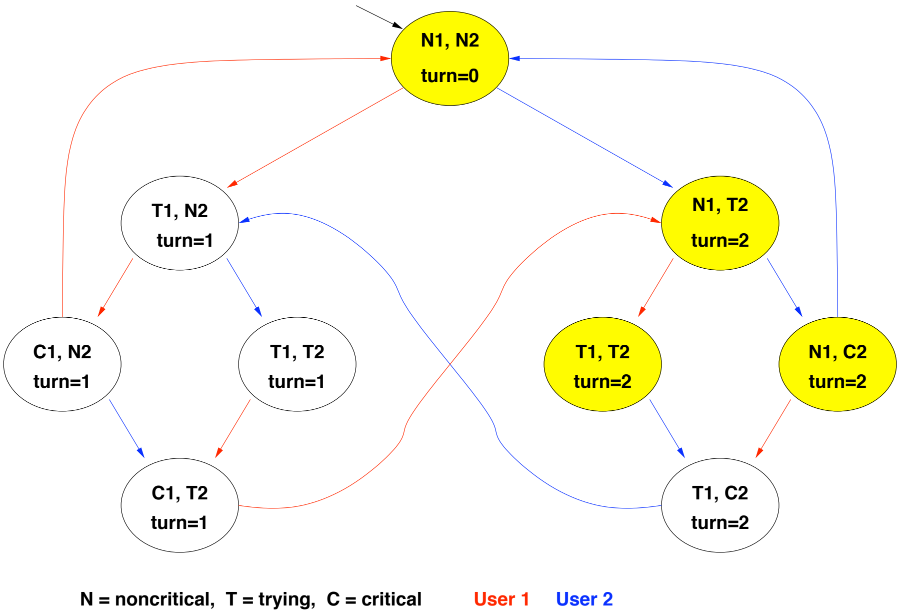
$[\mathbf{EG}\neg C_1]$, step 2:



$M \models \mathbf{AGAF}C_1$? $\Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1$?

Example 1: fairness

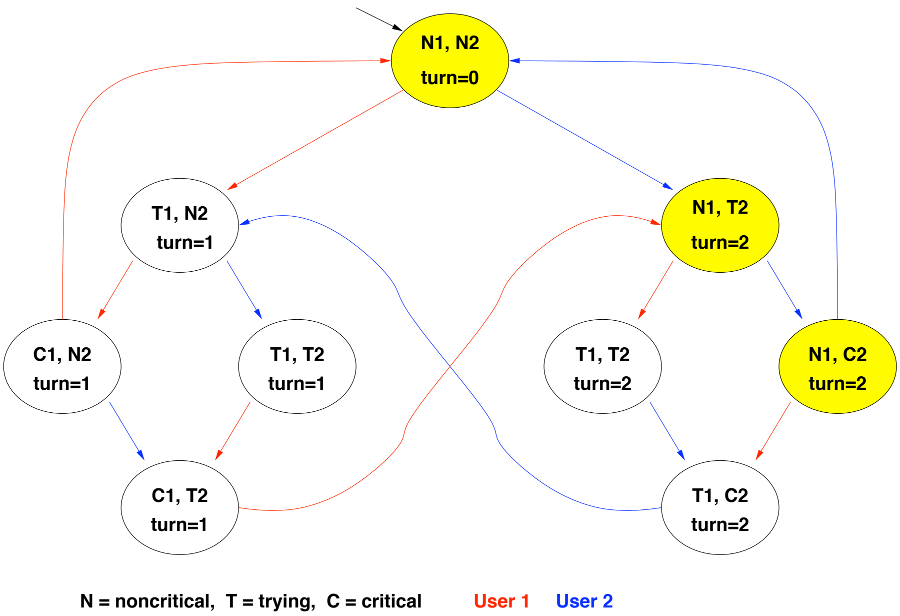
$[\mathbf{EG}\neg C_1]$, step 3:



$M \models \mathbf{AGAF}C_1\ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1\ ?$

Example 1: fairness

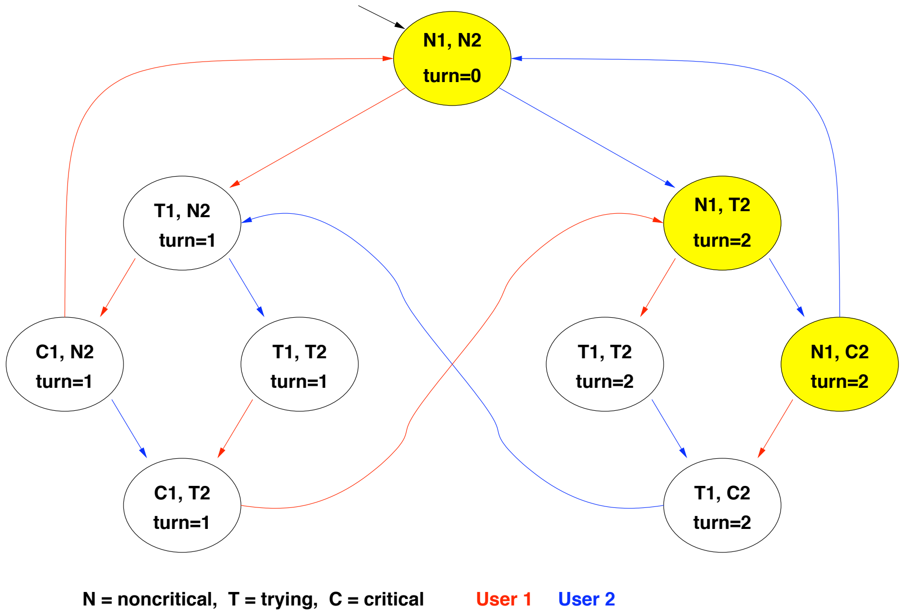
$[\mathbf{EG}\neg C_1]$, step 4:



$M \models \mathbf{AGAF}C_1\ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1\ ?$

Example 1: fairness

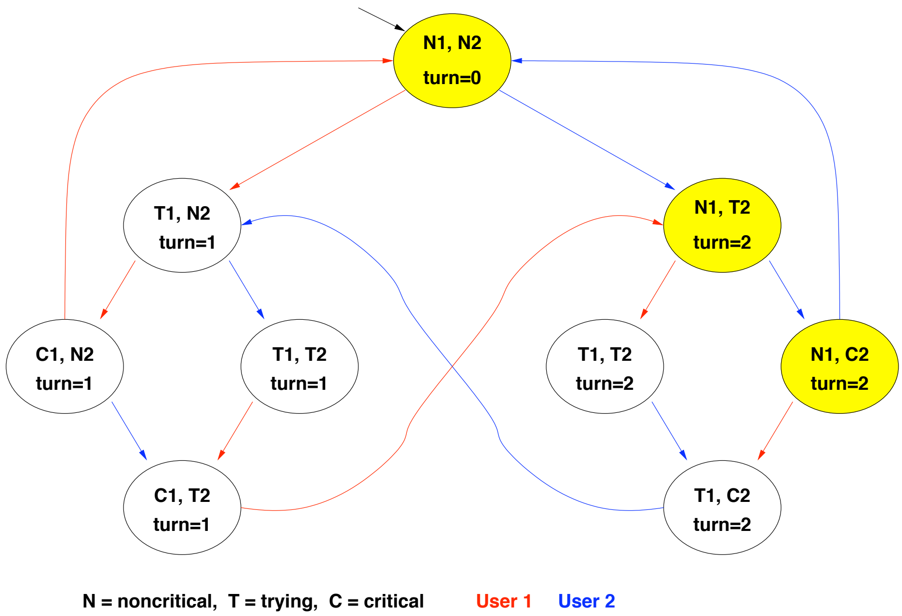
$[\mathbf{EG}\neg C_1]$, FIXPOINT!



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

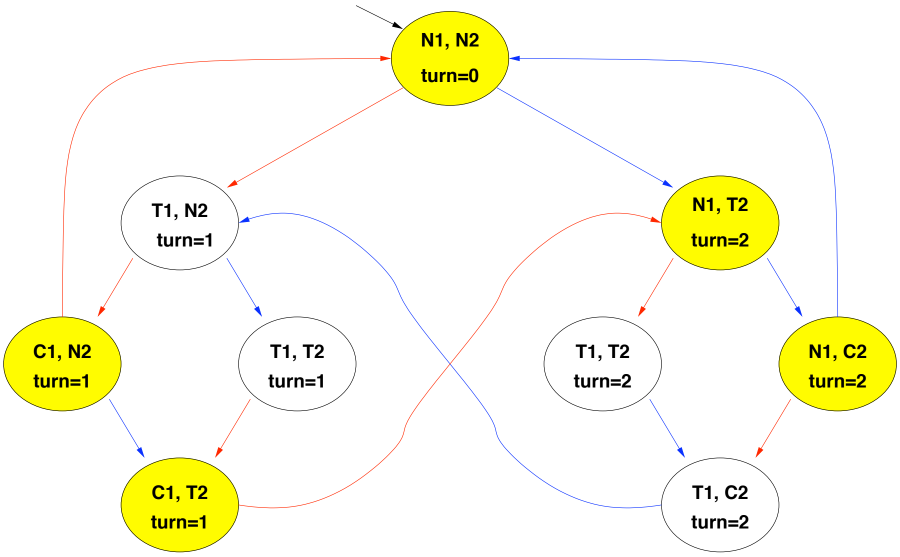
$[\mathbf{EFEG}\neg C_1]$, STEP 0



$M \models \mathbf{AGAF}C_1 \; ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \; ?$

Example 1: fairness

$[\mathbf{EFEG}\neg C_1]$, STEP 1

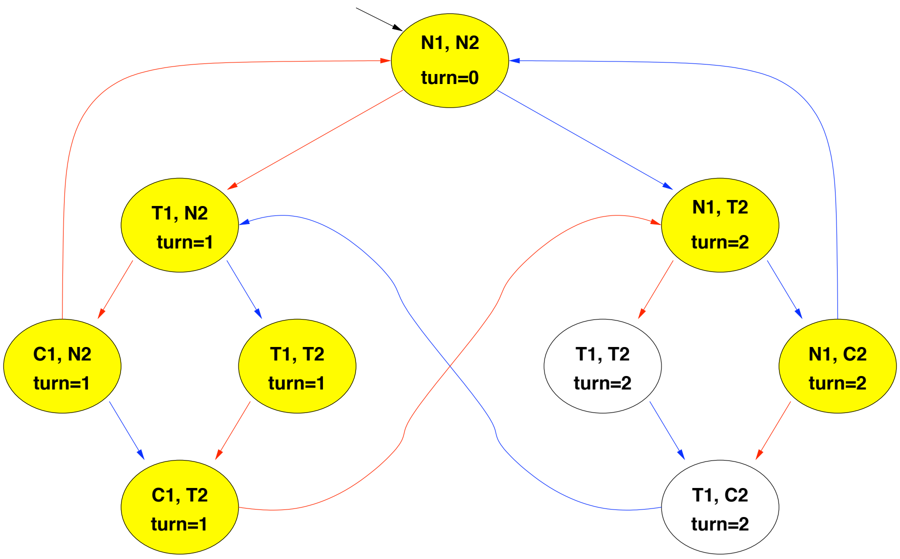


N = noncritical, T = trying, C = critical User 1 User 2

$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

Example 1: fairness

$[\mathbf{EFEG}\neg C_1]$, STEP 2

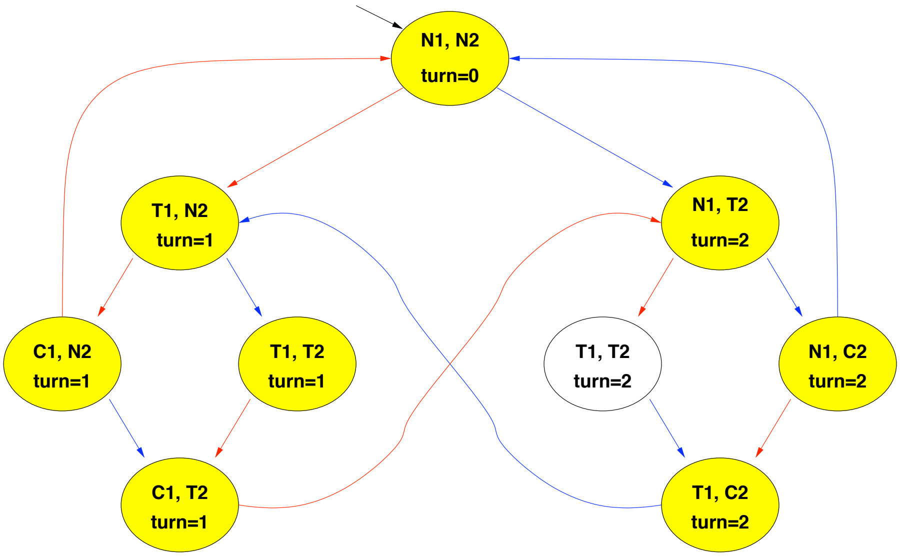


N = noncritical, T = trying, C = critical User 1 User 2

$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

Example 1: fairness

$[\mathbf{EFEG}\neg C_1]$, STEP 3

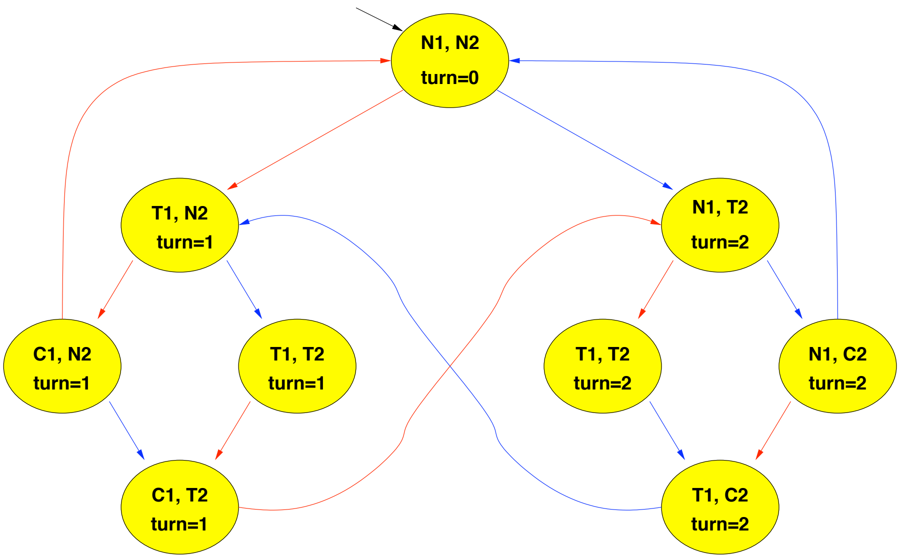


N = noncritical, T = trying, C = critical User 1 User 2

$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

Example 1: fairness

$[\mathbf{EFEG}\neg C_1]$, STEP 4

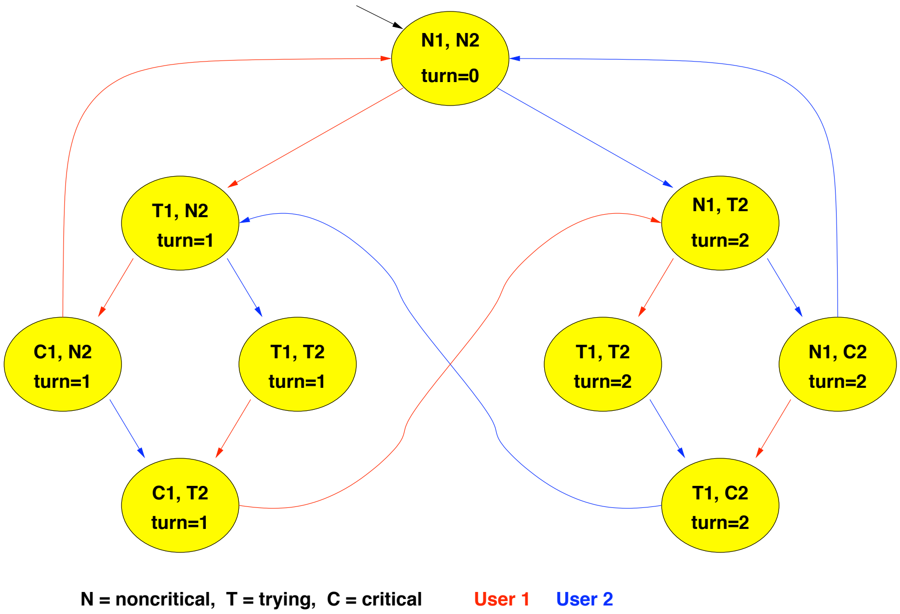


N = noncritical, T = trying, C = critical User 1 User 2

$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

Example 1: fairness

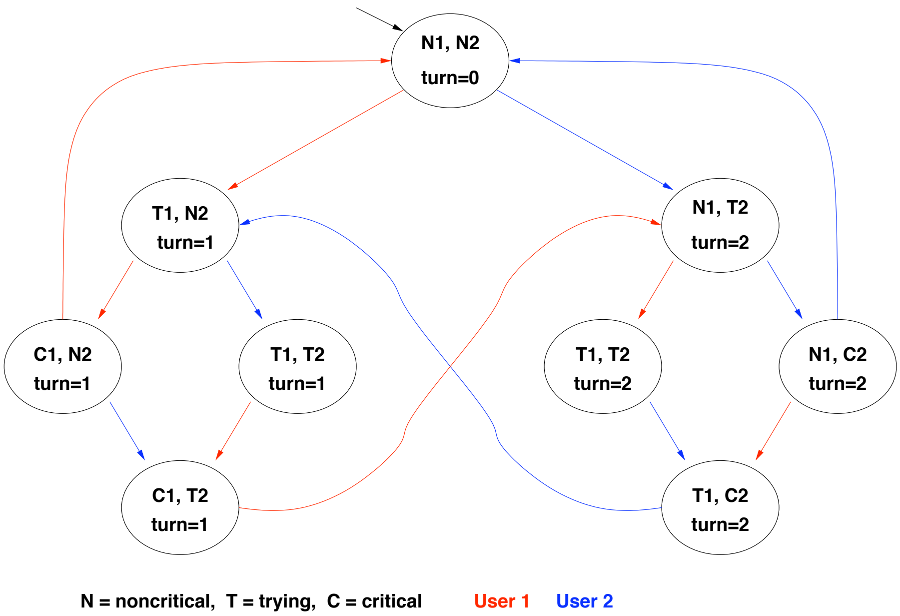
$[\mathbf{EFEG}\neg C_1]$, FIXPOINT!



$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ?$$

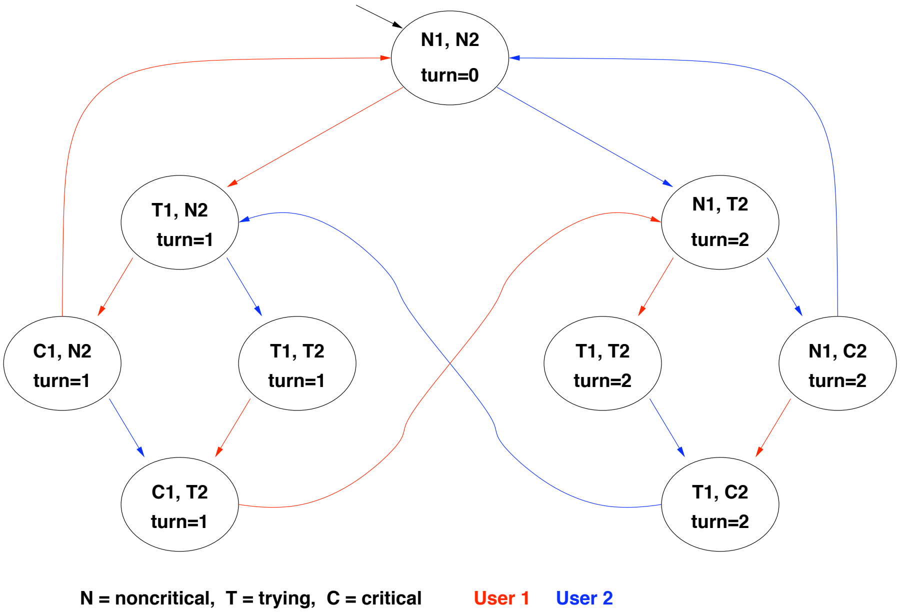
Example 1: fairness

$[\neg\mathbf{EFEG}\neg C_1]$



$$M \models \mathbf{AGAF}C_1 \ ? \Longrightarrow M \models \neg\mathbf{EFEG}\neg C_1 \ ? \Longrightarrow \text{NO!}$$

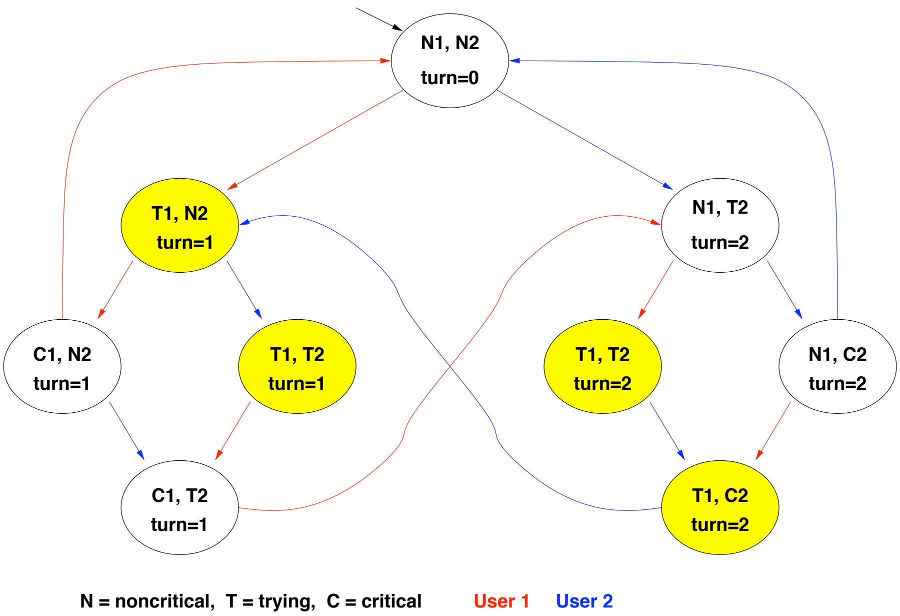
Example 2: liveness



$$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$$

Example 2: liveness

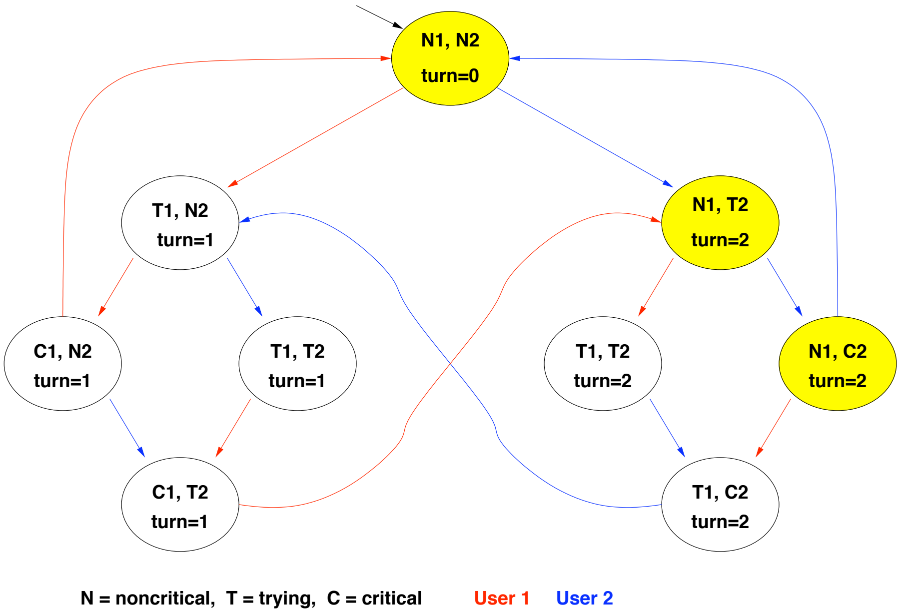
$[T_1]$:



$$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$$

Example 2: liveness

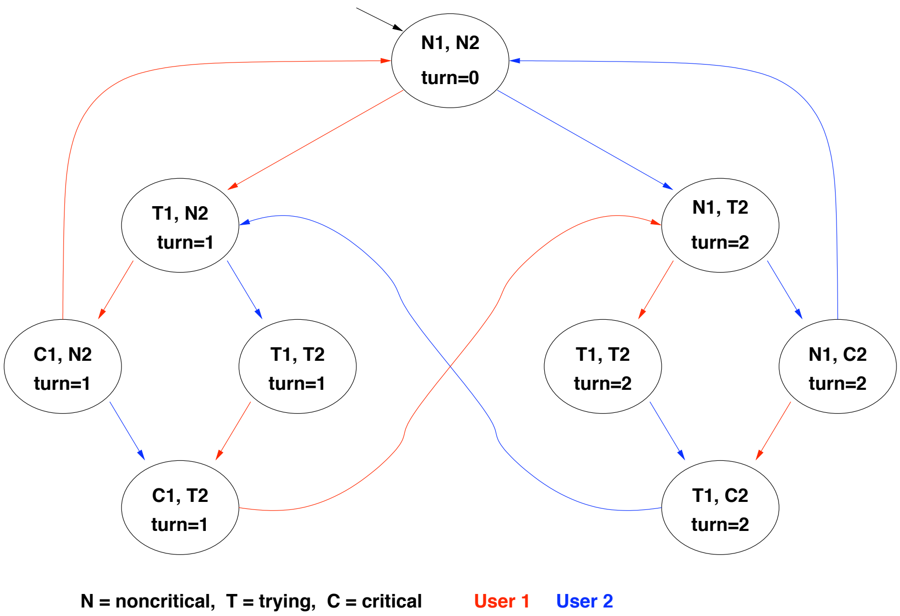
$[\mathbf{EG}\neg C_1]$, STEPS 0-4: (see previous example)



$$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1) \ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1) \ ?$$

Example 2: liveness

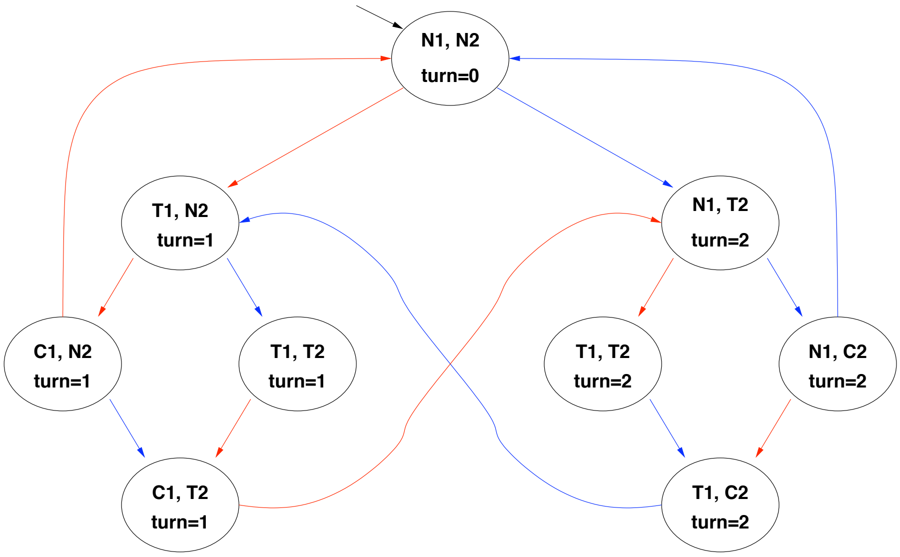
$[T_1 \wedge \mathbf{EG}\neg C_1]$:



$$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1) \ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1) \ ?$$

Example 2: liveness

$[\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)]$:

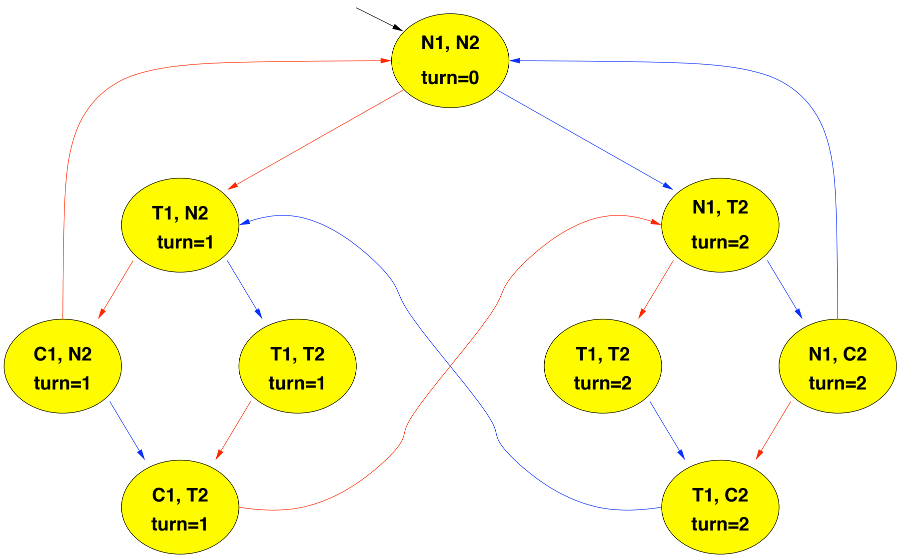


N = noncritical, T = trying, C = critical User 1 User 2

$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$

Example 2: liveness

$[\neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)]$:



N = noncritical, T = trying, C = critical User 1 User 2

$M \models \mathbf{AG}(T_1 \rightarrow \mathbf{AF}C_1)\ ? \Longrightarrow M \models \neg\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)\ ?$ YES!