Introduction to Formal Methods
Chapter 04: CTL Model Checking

Roberto Sebastiani

DISI, Università di Trento, Italy – roberto.sebastiani@unitn.it
URL: http://disi.unitn.it/rseba/DIDATTICA/fm2020/
Teaching assistant: Enrico Magnago – enrico.magnago@unitn.it

CDLM in Informatica, academic year 2019-2020

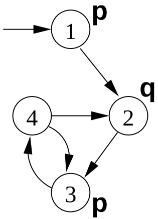
last update: Monday 18th May, 2020, 14:48

Outline

CTL Model Checking

CTL Model Checking is a formal verification technique where...

- ...the system is represented as a Finite State Machine M:



- ...the property is expressed a CTL formula φ:

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

- ...the model checking algorithm checks whether in all initial states of M all the executions of the model satisfy the formula ($M \models \varphi$).

CTL Model Checking: General Idea

Two macro-steps:

1. construct the set of states where the formula holds:
   $[\varphi] := \{s \in S : M, s \models \varphi\}$
   ($[\varphi]$ is called the denotation of φ)
2. then compare with the set of initial states:
   $I \subseteq [\varphi]$?

CTL Model Checking: General Idea [cont.]

In order to compute $[\varphi]$:

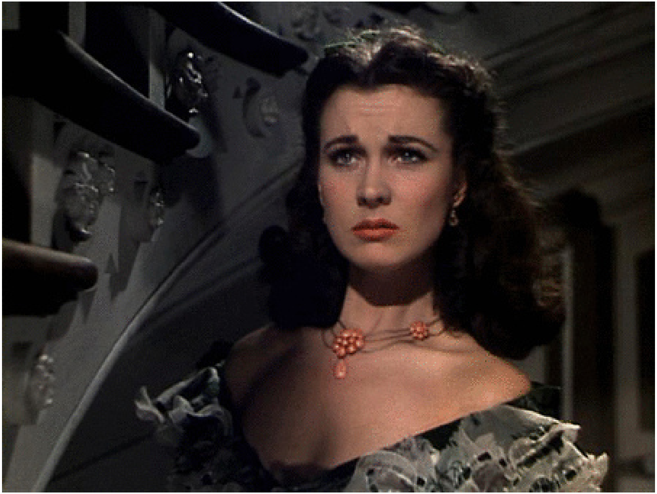
- proceed "bottom-up" on the structure of the formula, computing $[\varphi_i]$ for each subformula φ_i of $\mathbf{AG}(p \rightarrow \mathbf{AF}q)$:
  - $[q]$,
  - $[\mathbf{AF}q]$,
  - $[p]$,
  - $[p \rightarrow \mathbf{AF}q]$,
  - $[\mathbf{AG}(p \rightarrow \mathbf{AF}q)]$

CTL Model Checking: General Idea [cont.]

In order to compute each $[\varphi_i]$:

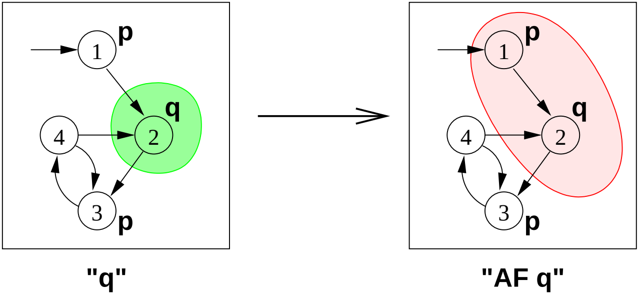
- assign Propositional atoms by labeling function
- handle Boolean operators by standard set operations
- handle temporal operators **AX**, **EX** by computing pre-images
- handle temporal operators **AG**, **EG**, **AF**, **EF**, **AU**, **EU**, by (implicitly) applying tableaux rules, until a fixpoint is reached

Tableaux rules: a quote



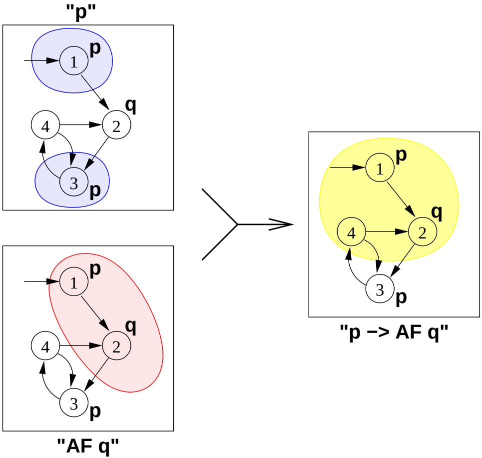
“After all... tomorrow is another day."
[Scarlett O’Hara, “Gone with the Wind”]

CTL Model Checking: Example: $\mathbf{AG}(p \rightarrow \mathbf{AF}q)$

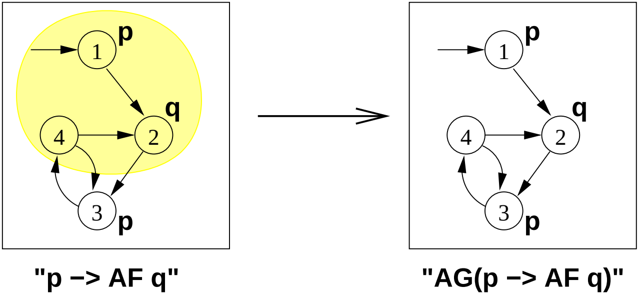


- Recall the **AF** tableau rule: $\mathbf{AF}q \leftrightarrow (q \vee \mathbf{AXAF}q)$
- Iteration: $[\mathbf{AF}q]^{(1)} = [q]$; $\quad [\mathbf{AF}q]^{(i+1)} = [q] \cup \mathbf{AX}[\mathbf{AF}q]^{(i)}$
  - $[\mathbf{AF}q]^{(1)} = [q] = \{2\}$
  - $[\mathbf{AF}q]^{(2)} = [q \vee \mathbf{AX}q] = \{2\} \cup \{1\} = \{1, 2\}$
  - $[\mathbf{AF}q]^{(3)} = [q \vee \mathbf{AX}(q \vee \mathbf{AX}q)] = \{2\} \cup \{1\} = \{1, 2\}$
    $\Longrightarrow$ (fix point reached)

CTL Model Checking: Example: $\mathbf{AG}(p \rightarrow \mathbf{AF}q)$ [cont.]



CTL Model Checking: Example: $\mathbf{AG}(p \rightarrow \mathbf{AF}q)$ [cont.]



- Recall the **AG** tableau rule: $\mathbf{AG}\varphi \leftrightarrow (\varphi \wedge \mathbf{AXAG}\varphi)$
- Iteration: $[\mathbf{AG}\varphi^{(1)}] = [\varphi]$; $[\mathbf{AG}\varphi]^{(i+1)} = [\varphi] \cap \mathbf{AX}[\mathbf{AG}\varphi]^{(i)}$
  1. $[\mathbf{AG}\varphi]^{(1)} = [\varphi] = \{1, 2, 4\}$
  2. $[\mathbf{AG}\varphi]^{(2)} = [\varphi] \cap \mathbf{AX}[\mathbf{AG}\varphi]^{(1)} = \{1, 2, 4\} \cap \{1, 3\} = \{1\}$
  3. $[\mathbf{AG}\varphi]^{(3)} = [\varphi] \cap \mathbf{AX}[\mathbf{AG}\varphi]^{(2)} = \{1, 2, 4\} \cap \{\} = \{\}$

     $\Longrightarrow$ (fix point reached)

CTL Model Checking: Example: $\mathbf{AG}(p \rightarrow \mathbf{AF}q)$ [cont.]

- The set of states where the formula holds is empty
  $\Longrightarrow$ the initial state does not satisfy the property
  $\Longrightarrow M \not\models \mathbf{AG}(p \rightarrow \mathbf{AF}q)$
- Counterexample: a lazo-shaped path: $1, 2, \{3, 4\}^{\omega}$ (satisfying $\mathbf{EF}(p \wedge \mathbf{EG}\neg q)$)

Note

Counter-example reconstruction in general is not trivial, based on intermediate sets.

The fixed-point theory of lattice of sets

Definition

- For any finite set S, the structure $(2^S, \subseteq)$ forms a complete lattice with $\cup$ as join and $\cap$ as meet operations.
- A function $F : 2^S \longmapsto 2^S$ is monotonic provided $S_1 \subseteq S_2 \;\Rightarrow\; F(S_1) \subseteq F(S_2)$.

Fixed Points

Definition

Let $\langle 2^S, \subseteq \rangle$ be a complete lattice, S finite.

- Given a function $F : 2^S \longmapsto 2^S$, $a \subseteq S$ is a fixed point of F iff

$$F(a) = a$$

- a is a least fixed point (LFP) of F, written $\mu x.F(x)$, iff, for every other fixed point a' of F, $a \subseteq a'$
- a is a greatest fixed point (GFP) of F, written $\nu x.F(x)$, iff, for every other fixed point a' of F, $a' \subseteq a$

Iteratively computing fixed points

Tarski's Theorem

A monotonic function over a complete finite lattice has a least and a greatest fixed point.

(A corollary of) Kleene's Theorem

A monotonic function F over a complete finite lattice has a least and a greatest fixed point, which can be computed as follows:

- the least fixed point of F is the limit of the chain $\emptyset \subseteq F(\emptyset) \subseteq F(F(\emptyset)) \ldots$,
- the greatest fixed point of F is the limit of chain $S \supseteq F(S) \supseteq F(F(S)) \ldots$

Since 2^S is finite, convergence is obtained in a finite number of steps.

CTL Model Checking and Lattices

- If $M = \langle S, I, R, L, AP \rangle$ is a Kripke structure, then $\langle 2^S, \subseteq \rangle$ is a complete lattice
- We identify φ with its denotation $[\varphi]$

$\Longrightarrow$ we can see logical operators as functions $F : 2^S \longmapsto 2^S$ on the complete lattice $\langle 2^S, \subseteq \rangle$

Denotation of a CTL formula φ: $[\varphi]$

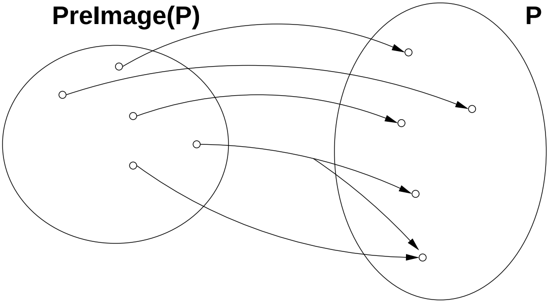
Definition of $[\varphi]$

$[\varphi] := \{s \in S : M, s \models \varphi\}$

Recursive definition of $[\varphi]$

$$
\begin{array}{lcl}
[true] & = & S \\
[false] & = & \{\} \\
[p] & = & \{s | p \in L(s)\} \\
[\neg\varphi_1] & = & S/[\varphi_1] \\
[\varphi_1 \wedge \varphi_2] & = & [\varphi_1] \cap [\varphi_2] \\
[\mathbf{EX}\varphi] & = & \{s \mid \exists s' \in [\varphi] \ s.t. \ \langle s, s' \rangle \in R\} \\
[\mathbf{EG}\beta] & = & \nu Z.(\ [\beta] \cap [\mathbf{EX}Z]\ ) \\
[\mathbf{E}(\beta_1 \mathbf{U} \beta_2)] & = & \mu Z.(\ [\beta_2] \cup ([\beta_1] \cap [\mathbf{EX}Z])\ )
\end{array}
$$

Case **EX**



- $[\mathbf{EX}\varphi] = \{s \mid \exists s' \in [\varphi] \; s.t. \; \langle s, s' \rangle \in R\}$
- $[\mathbf{EX}\varphi]$ is said to be the Pre-image of $[\varphi]$ ($Preimage([\varphi])$)
- Key step of every CTL M.C. operation

Note

Preimage() is monotonic: $X \subseteq X' \Longrightarrow Preimage(X) \subseteq Preimage(X')$

Case **EG**

- $\nu Z.(\ [\beta] \cap [\mathbf{EX}Z]\ )$: greatest fixed point of the function $F_\beta : 2^S \longmapsto 2^S$, s.t.

$$F_\beta([\varphi]) = ([\beta] \cap Preimage([\varphi])) = ([\beta] \cap \{s \mid \exists s' \in [\varphi]\ s.t.\ \langle s, s' \rangle \in R\})$$

- F_β Monotonic: $a \subseteq a' \Longrightarrow F_\beta(a) \subseteq F_\beta(a')$
  - (Tarski's theorem): $\nu x.F_\beta(x)$ always exists
  - (Kleene's theorem): $\nu x.F_\beta(x)$ can be computed as the limit $S \supseteq F_\beta(S) \supseteq F_\beta(F_\beta(S)) \supseteq \ldots$, in a finite number of steps.

Theorem (Clarke & Emerson)

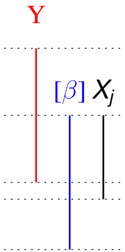
$[\mathbf{EG}\beta] = \nu Z.(\ [\beta] \cap [\mathbf{EX}Z]\ )$

Case **EG** [cont.]

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

$$
\begin{array}{lllll}
X_0 & := & S & & \\
X_1 & := & F_\beta(S) & = & [\beta] \\
X_2 & := & F_\beta(F_\beta(S)) & = & [\beta] \cap Preimage(X_1) \\
\ldots & & & & \\
X_{j+1} & := & F_\beta^{j+1}(S) & = & [\beta] \cap Preimage(X_j)
\end{array}
$$

- Noticing that $X_1 = [\beta]$ and $X_{j+1} \subseteq X_j$ for every $j \geq 0$, and that
  $([\beta] \cap Y) \subseteq X_j \subseteq [\beta] \Longrightarrow ([\beta] \cap Y) = (X_j \cap Y)$,
  we can use instead the following inductive schema:
  - $X_1 \quad := [\beta]$
  - $X_{j+1} := X_j \cap Preimage(X_j)$



Case **EU**

- $\mu Z.(\ [\beta_2] \cup ([\beta_1] \cap [\mathbf{EX}Z])\ )$: least fixed point of the function $F_{\beta_1,\beta_2} : 2^S \longmapsto 2^S$, s.t.

$$\begin{array}{rcl} F_{\beta_1,\beta_2}([\varphi]) & = & [\beta_2] \cup ([\beta_1] \cap \mathit{Preimage}([\varphi])) \\ & = & [\beta_2] \cup ([\beta_1] \cap \{s \mid \exists s' \in [\varphi]\ s.t.\ \langle s, s' \rangle \in R\}) \end{array}$$

- F_{β_1,β_2} Monotonic: $a \subseteq a' \Longrightarrow F_{\beta_1,\beta_2}(a) \subseteq F_{\beta_1,\beta_2}(a')$
  - (Tarski's theorem): $\mu x.F_{\beta_1,\beta_2}(x)$ always exists
  - (Kleene's theorem): $\mu x.F_{\beta_1,\beta_2}(x)$ can be computed as the limit $\emptyset \subseteq F_{\beta_1,\beta_2}(\emptyset) \subseteq F_{\beta_1,\beta_2}(F_{\beta_1,\beta_2}(\emptyset)) \subseteq \ldots$, in a finite number of steps.

Theorem (Clarke & Emerson)

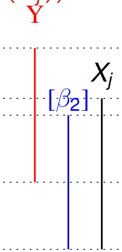
$[\mathbf{E}(\beta_1 \mathbf{U} \beta_2)] = \mu Z.(\ [\beta_2] \cup ([\beta_1] \cap [\mathbf{EX}Z])\ )$

Case **EU** [cont.]

- We can compute $X := [\mathbf{E}(\beta_1 \mathbf{U} \beta_2)]$ inductively as follows:

$$\begin{array}{lcl}
X_0 & := & \emptyset \\
X_1 & := & F_{\beta_1,\beta_2}(\emptyset) = [\beta_2] \\
X_2 & := & F_{\beta_1,\beta_2}(F_{\beta_1,\beta_2}(\emptyset)) = [\beta_2] \cup ([\beta_1] \cap Preimage(X_1)) \\
\ldots & & \\
X_{j+1} & := & F^{j+1}_{\beta_1,\beta_2}(\emptyset)) = [\beta_2] \cup ([\beta_1] \cap Preimage(X_j))
\end{array}$$

- Noticing that $X_1 = [\beta_2]$ and $X_{j+1} \supseteq X_j$ for every $j \geq 0$, and that $([\beta_2] \cup Y) \supseteq X_j \supseteq [\beta_2] \Longrightarrow ([\beta_2] \cup Y) = (X_j \cup Y)$, we can use instead the following inductive schema:
  - $X_1 := [\beta_2]$
  - $X_{j+1} := X_j \cup ([\beta_1] \cap Preimage(X_j))$



A relevant subcase: EF

- $\mathbf{EF}\beta = \mathbf{E}(\top \mathbf{U} \beta)$
- $[\top] = S \Longrightarrow [\top] \cap Preimage(X_j) = Preimage(X_j)$
- We can compute $X := [\mathbf{EF}\beta]$ inductively as follows:
  - $X_1 \quad := [\beta]$
  - $X_{j+1} := X_j \cup Preimage(X_j)$

General Schema

- Assume φ written in terms of $\neg$, $\wedge$, **EX**, **EU**, **EG**
- A general M.C. algorithm (fix-point):
  1. for every $\varphi_i \in Sub(\varphi)$, find $[\varphi_i]$
  2. 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
  - Propositional atoms: apply labeling function
  - Boolean operator: apply standard set operations
  - temporal operator: appy recursively the tableaux rules, until a fixpoint is reached

General M.C. Procedure

state_set Check(CTL_formula β) {
    case β **of**
    true: **return** S;
    false: **return** $\{\}$;
    p: **return** $\{s \mid p \in L(s)\}$;
    $\neg\beta_1$: **return** S / Check(β_1);
    $\beta_1 \wedge \beta_2$: **return** Check(β_1) $\cap$ Check(β_2);
    EXβ_1: **return** PreImage(Check(β_1));
    EGβ_1: **return** Check_EG(Check(β_1));
    E(β_1**U**β_2): **return** Check_EU(Check(β_1),Check(β_2));
}

PreImage

```
state_set PreImage(state_set [β]) {
    X := {};
    for each s ∈ S do
        for each s' s.t. s' ∈ [β] and ⟨s, s'⟩ ∈ R do
            X := X ∪ {s};
return X;
}
```

Check_EG

```
state_set Check_EG(state_set [β]) {
    X' := [β]; j := 1;
    repeat
        X := X'; j := j + 1;
        X' := X ∩ PreImage(X);
    until (X' = X);
return X;
}
```

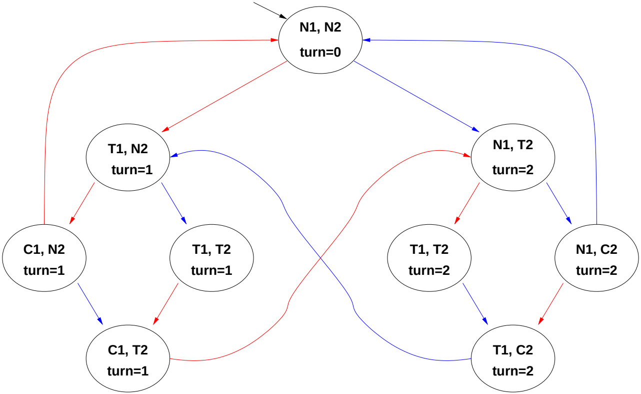
Check_EU

state_set Check_EU(**state_set** $[\beta_1]$,$[\beta_2]$) {
    $X' := [\beta_2]$; $j := 1$;
    repeat
        $X := X'$; $j := j + 1$;
        $X' := X \cup ([\beta_1] \cap PreImage(X))$;
    until $(X' = X)$;
return X;
}

A relevant subcase: Check_EF

state_set Check_EF(**state_set** $[\beta]$) $\{$
$\quad X' := [\beta];\ j := 1;$
$\quad$ **repeat**
$\quad\quad X := X';\ j := j + 1;$
$\quad\quad X' := X \cup PreImage(X);$
$\quad$ **until** $(X' = X)$;
return X;
$\}$

Example 1: fairness

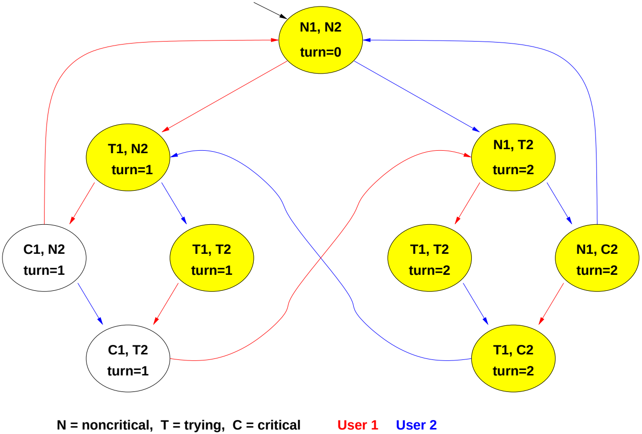


N = noncritical, T = trying, C = critical **User 1** **User 2**

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

Example 1: fairness

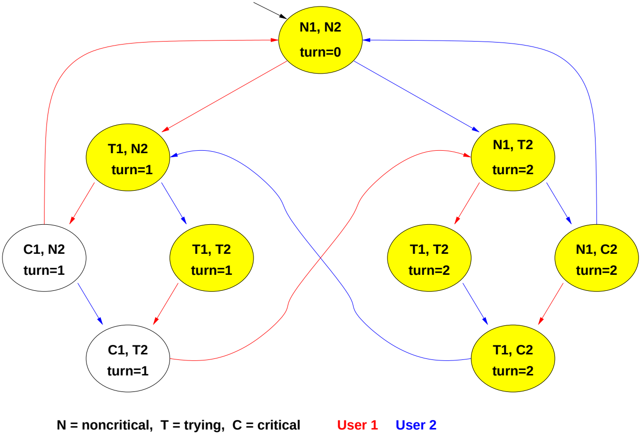
$[\neg C_1]$



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

Example 1: fairness

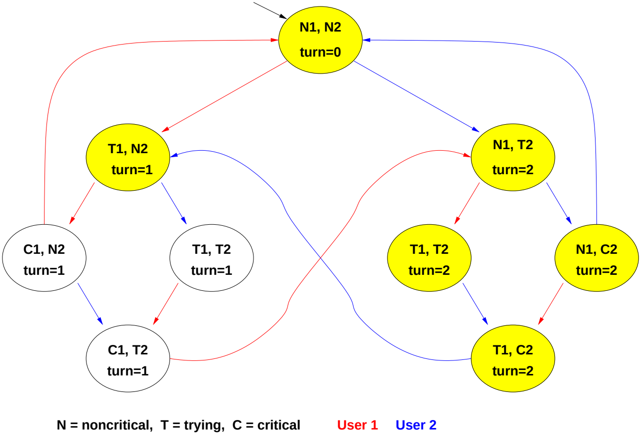
[**EG**$\neg C_1$], step 0:



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

Example 1: fairness

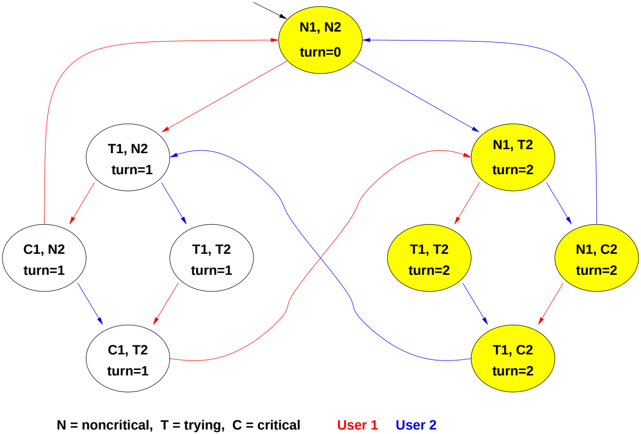
$[\mathbf{EG}\neg C_1]$, step 1:



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

Example 1: fairness

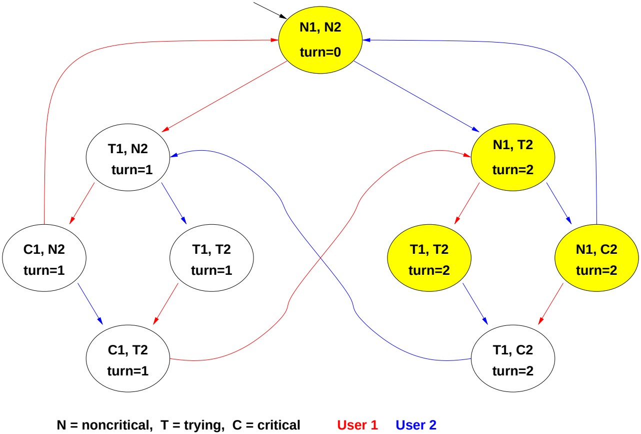
[$\mathbf{EG}\neg C_1$], step 2:



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

Example 1: fairness

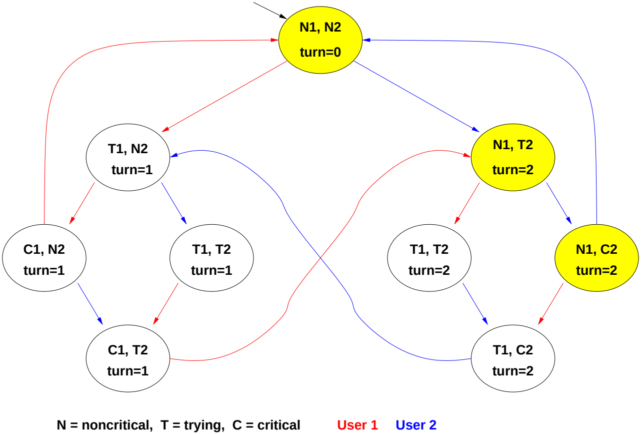
$[\mathbf{EG}\neg C_1]$, step 3:



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

Example 1: fairness

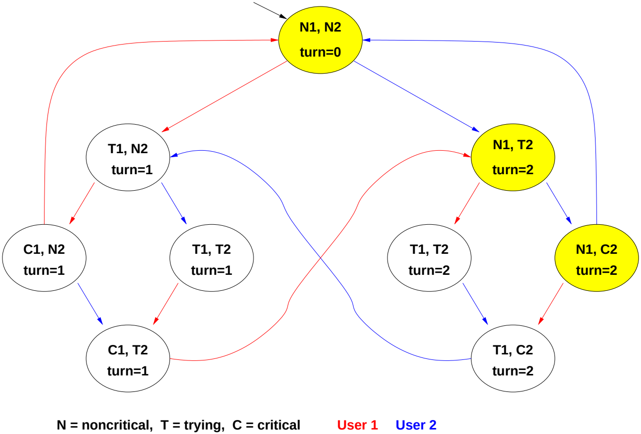
[**EG**$\neg C_1$], step 4:



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

Example 1: fairness

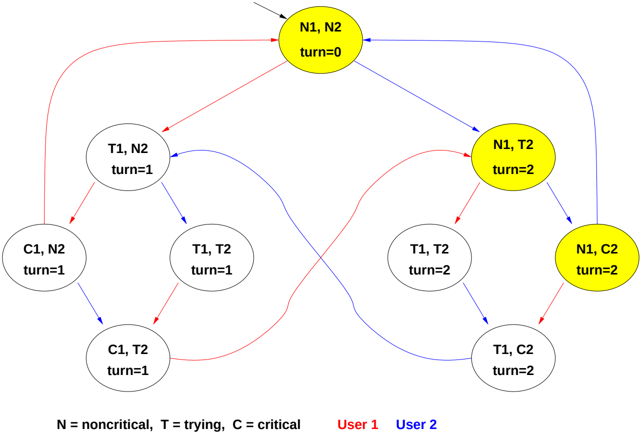
[**EG**$\neg C_1$], FIXPOINT!



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

Example 1: fairness

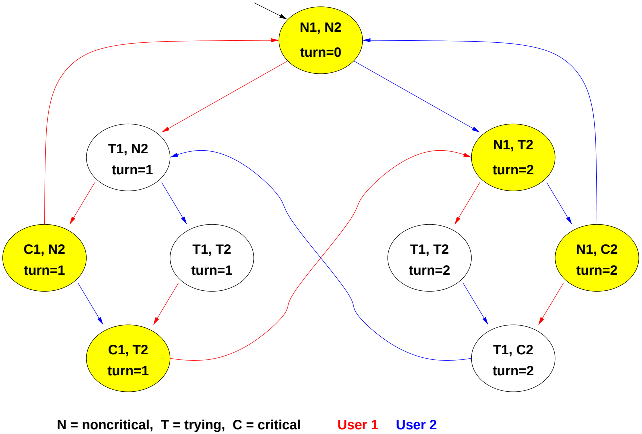
[**EFEG**$\neg C_1$], STEP 0



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

Example 1: fairness

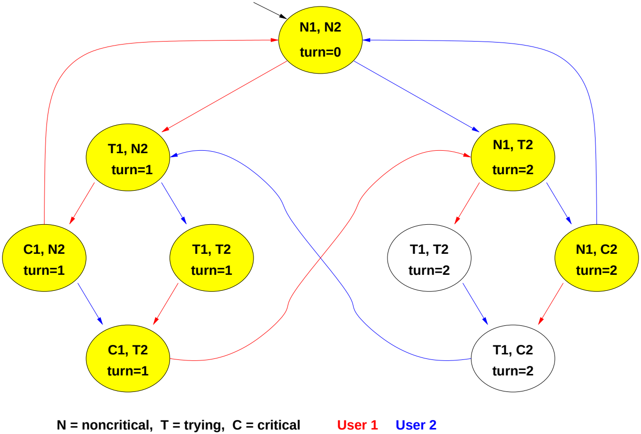
[**EFEG**$\neg C_1$], STEP 1



$M \models$ **AGAF**C_1 ? $\Longrightarrow M \models \neg$**EFEG**$\neg C_1$?

Example 1: fairness

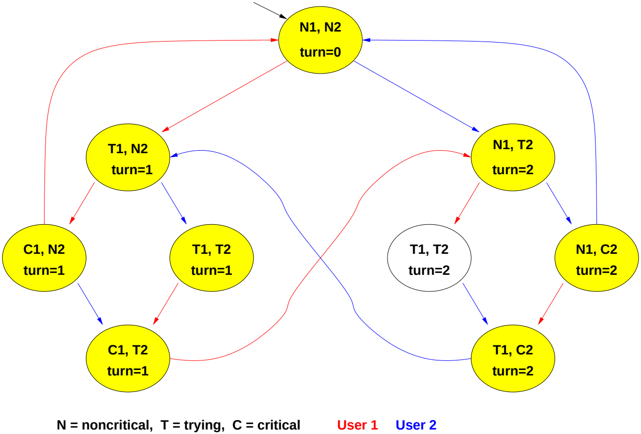
[$\mathbf{EFEG}\neg C_1$], STEP 2



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

Example 1: fairness

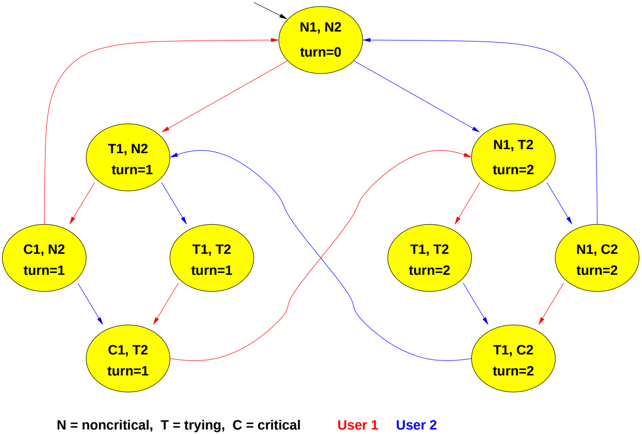
[**EFEG**$\neg C_1$], STEP 3



$M \models$ **AGAF**C_1 ? $\Longrightarrow M \models \neg$**EFEG**$\neg C_1$?

Example 1: fairness

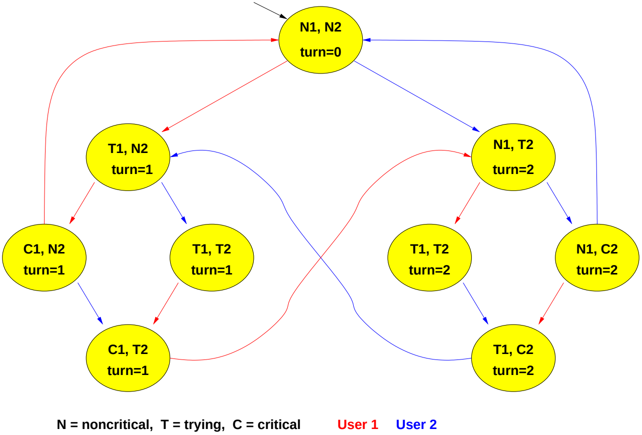
[**EFEG**$\neg C_1$], STEP 4



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

Example 1: fairness

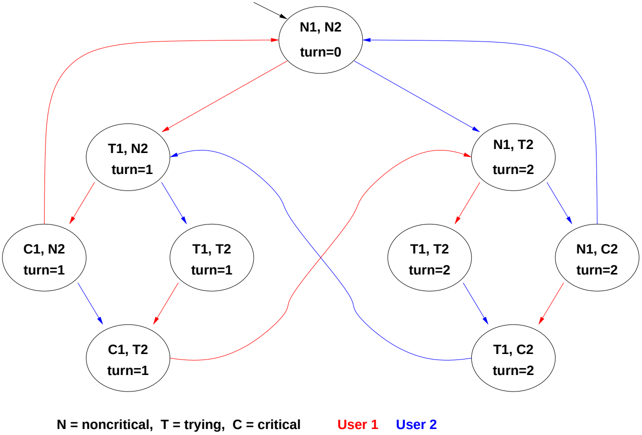
$[\mathbf{EFEG}\neg C_1]$, FIXPOINT!



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

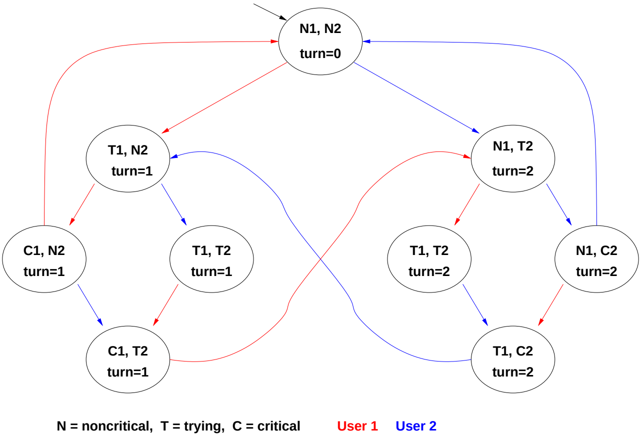
Example 1: fairness

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



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

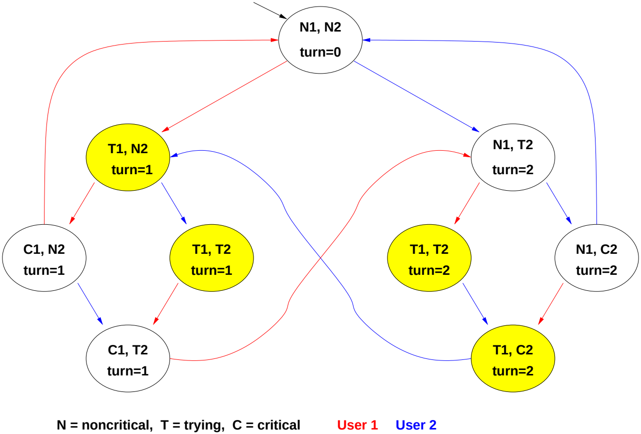
Example 2: liveness



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

Example 2: liveness

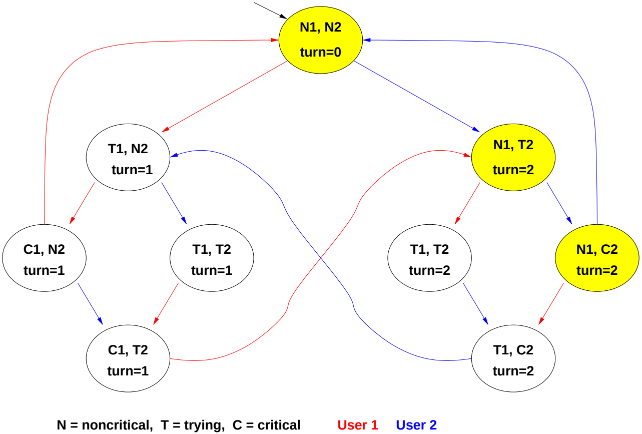
$[T_1]$:



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

Example 2: liveness

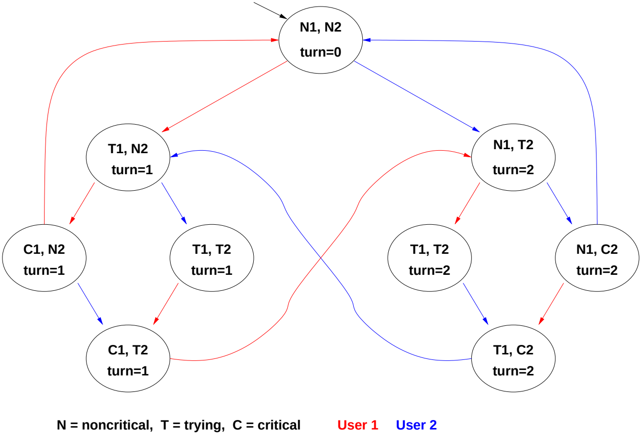
[$\mathbf{EG}\neg C_1$], STEPS 0-4: (see previous example)



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

Example 2: liveness

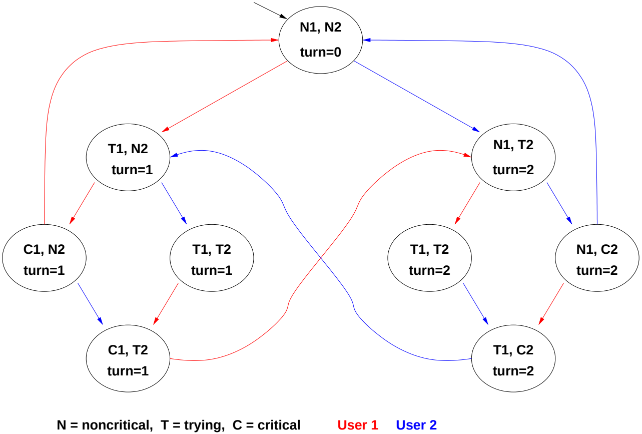
$[T_1 \wedge \mathbf{EG}\neg C_1]$:



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

Example 2: liveness

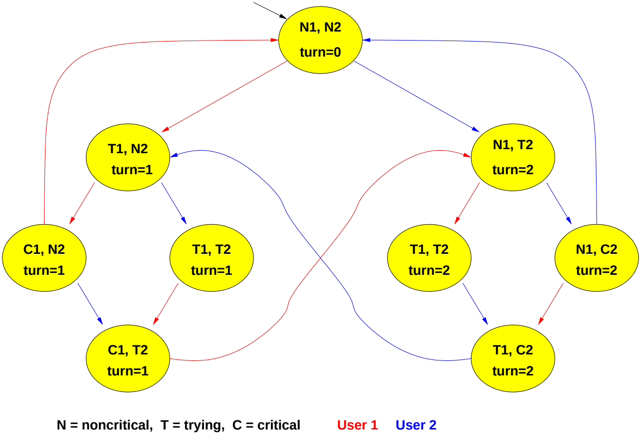
$[\mathbf{EF}(T_1 \wedge \mathbf{EG}\neg C_1)]$:



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

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!

The property verified is...

Homework

Apply the same process to all the CTL examples of Chapter 3.

Complexity of CTL Model Checking: $M \models \varphi$

- Step 1: compute $[\varphi]$
  - Compute $[\varphi]$ bottom-up on the $O(|\varphi|)$ sub-formulas of φ: $O(|\varphi|)$ steps...
  - ... each requiring at most exploring $O(|M|)$ states

  $\Longrightarrow O(|M| \cdot |\varphi|)$ steps
- Step 2: check $I \subseteq [\varphi]$: $O(|M|)$

$\Longrightarrow O(|M| \cdot |\varphi|)$

Model Checking of Invariants

- Invariant properties have the form **AG p** (e.g., **AG**$\neg$*bad*)
- Checking invariants is the negation of a reachability problem:
  - is there a reachable state that is also a bad state?
    (**AG**$\neg$*bad* $=$ $\neg$**EF***bad*)
- Standard M.C. algorithm reasons backward from the *bad* by iteratively applying PreImage computations:

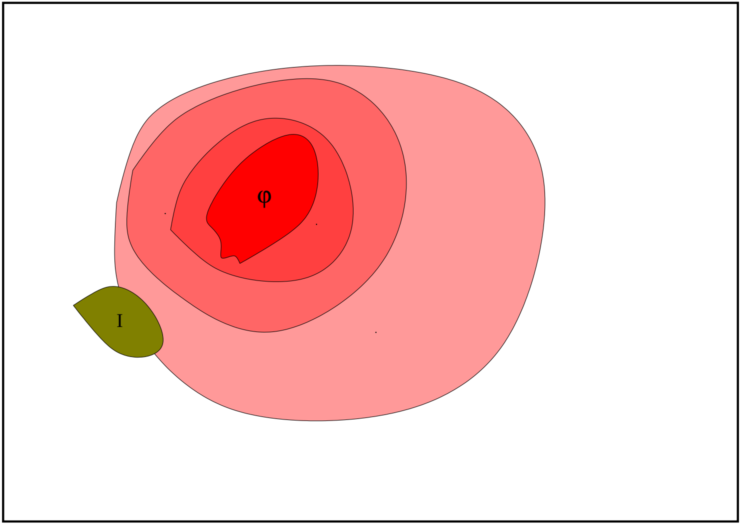
  $$Y' := Y \cup PreImage(Y)$$

  until a fixed point is reached. Then the complement is computed and I is checked for inclusion in the resulting set.
- Better algorithm: reasons backward from the *bad* by iteratively applying PreImage computations:

  $$Y' := Y \cup PreImage(Y)$$

  until (i) it intersect $[I]$ or (ii) a fixed point is reached

Model Checking of Invariants [cont.]



Symbolic Forward Model Checking of Invariants

Alternative algorithm (often more efficient): forward checking

- Compute the set of bad states $[bad]$
- Compute the set of initial states I
- Compute incrementally the set of reachable states from I until (i) it intersect $[bad]$ or (ii) a fixed point is reached
- Basic step is the (Forward) Image:

$$Image(Y) \stackrel{\text{def}}{=} \{s' \mid s \in Y \text{ and } R(s, s') \text{ holds}\}$$

- Simplest form: compute the set of reachable states.

Computing Reachable states: basic

State_Set Compute_reachable() {
    $Y' := I; Y := \emptyset; j := 1;$
    while $(Y' \neq Y)$
        $j := j + 1;$
        $Y := Y';$
        $Y' := Y \cup Image(Y);$
    }
return Y;
}

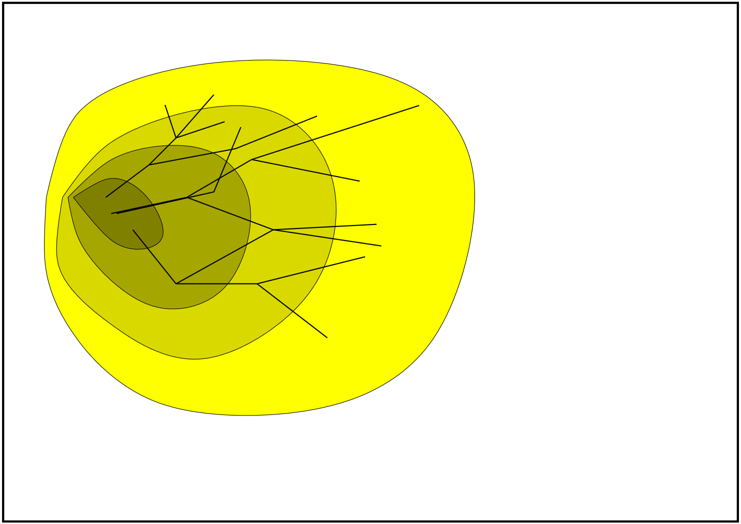
Y=reachable

Computing Reachable states: advanced

```
State_Set Compute_reachable() {
    Y := F := I; j := 1;
    while (F ≠ ∅)
        j := j + 1;
        F := Image(F) \ Y;
        Y := Y ∪ F;
    }
return Y;
}
```

Y=reachable;F=frontier (new)

Computing Reachable states [cont.]



Checking of Invariant Properties: basic

bool Forward_Check_EF(**State_Set** *BAD*) {
    $Y := I;\ Y' := \emptyset;\ j := 1;$
    while $(Y' \neq Y)$ **and** $(Y' \cap BAD) = \emptyset$
        $j := j + 1;$
        $Y := Y';$
        $Y' := Y \cup Image(Y);$
    }
    if $(Y' \cap BAD) \neq \emptyset$ // counter-example
        return *true*
    else // fixpoint reached
        return *false*
}

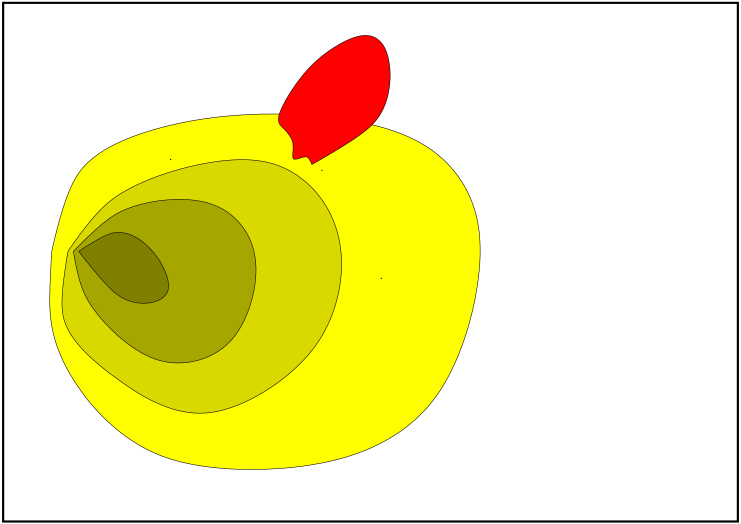
Y=reachable;

Checking of Invariant Properties: advanced

bool Forward_Check_EF(**State_Set** *BAD*) $\{$
    $Y := F := I;\ j := 1;$
    while $(F \neq \emptyset)$ **and** $(F \cap BAD) = \emptyset$
        $j := j + 1;$
        $F := Image(F) \setminus Y;$
        $Y := Y \cup F;$
    $\}$
    if $(F \cap BAD) \neq \emptyset$ // counter-example
        return *true*
    else // fixpoint reached
        return *false*
$\}$

Y=reachable;F=frontier (new)

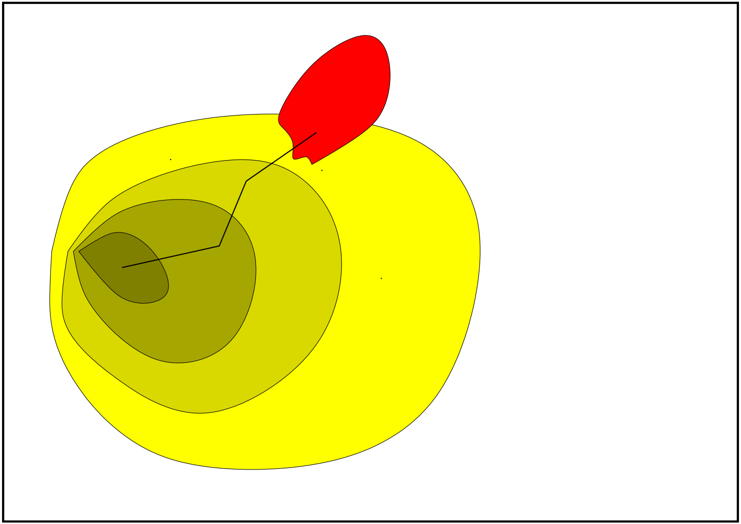
Checking of Invariant Properties [cont.]



Checking of Invariants: Counterexamples

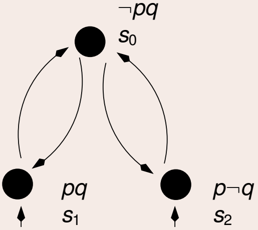
- if layer n intersects with the bad states, then the property is violated
- a counterexample can be reconstructed proceeding backwards
  (i) select any state of $BAD \cap F[n]$ (we know it is satisfiable), call it $t[n]$
  (ii) compute $Preimage(t[n])$, i.e. the states that can result in $t[n]$ in one step
  (iii) compute $Preimage(t[n]) \cap F[n-1]$, and select one state $t[n-1]$
- iterate (i)-(iii) until the initial states are reached
- $t[0], t[1], \ldots, t[n]$ is our counterexample

Checking of Invariants: Counterexamples [cont.]



Ex: CTL Model Checking

Consider the Kripke Model M below, and the CTL property $\varphi \stackrel{\text{def}}{=} \mathbf{AG}((p \wedge q) \rightarrow \mathbf{EG}q)$.



(a) Rewrite φ into an equivalent formula φ' expressed in terms of **EX**, **EG**, **EU**/**EF** only.
[Solution: $\varphi' = \neg\mathbf{EF}\neg((\neg p \vee \neg q) \vee \mathbf{EG}q) = \neg\mathbf{EF}((p \wedge q) \wedge \neg\mathbf{EG}q)$]

(b) Compute bottom-up the denotations of all subformulas of φ'. (Ex: $[p] = \{s_1, s_2\}$)
[Solution:

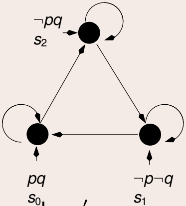
$[p]$	$=$	$\{s_1, s_2\}$	$[\neg\mathbf{EG}q]$	$=$	$\{s_2\}$
$[q]$	$=$	$\{s_0, s_1\}$	$[((p \wedge q) \wedge \neg\mathbf{EG}q)]$	$=$	$\{\}$
$[(p \wedge q)]$	$=$	$\{s_1\}$	$[\mathbf{EF}((p \wedge q) \wedge \neg\mathbf{EG}q)]$	$=$	$\{\}$
$[\mathbf{EG}q]$	$=$	$\{s_0, s_1\}$	$[\neg\mathbf{EF}((p \wedge q) \wedge \neg\mathbf{EG}q)]$	$=$	$\{s_0, s_1, s_2\}$

]

(c) As a consequence of point (b), say whether $M \models \varphi$ or not.
[Solution: Yes, $\{s_1, s_2\} \subseteq [\varphi']$.]

Ex: CTL Model Checking

Consider the Kripke Model M below, and the CTL property $\mathbf{AG}(\mathbf{AF}p \rightarrow \mathbf{AF}q)$.



(a) Rewrite φ into an equivalent formula φ' expressed in terms of **EX**, **EG**, **EU**/**EF** only.

[Solution:
$\varphi' = \mathbf{AG}(\mathbf{AF}p \rightarrow \mathbf{AF}q) = \neg\mathbf{EF}\neg(\neg\mathbf{EG}\neg p \rightarrow \neg\mathbf{EG}\neg q) = \neg\mathbf{EF}(\neg\mathbf{EG}\neg p \wedge \mathbf{EG}\neg q)$]

(b) Compute bottom-up the denotations of all subformulas of φ'. (Ex: $[p] = \{s_1, s_2\}$)

[Solution:

$$
\begin{array}{lll lll}
[p] & = & \{s_0\} & [\neg q] & = & \{s_1\} \\
[\neg p] & = & \{s_1, s_2\} & [\mathbf{EG}\neg q] & = & \{s_1\} \\
[\mathbf{EG}\neg p] & = & \{s_1, s_2\} & [\neg\mathbf{EG}\neg p \wedge \mathbf{EG}\neg q] & = & \{\} \\
[\neg\mathbf{EG}\neg p] & = & \{s_0\} & [\mathbf{EF}(\neg\mathbf{EG}\neg p \wedge \mathbf{EG}\neg q)] & = & \{\} \\
[q] & = & \{s_0, s_2\} & [\neg\mathbf{EF}(\neg\mathbf{EG}\neg p \wedge \mathbf{EG}\neg q)] & = & \{s_0, s_1, s_2\}
\end{array}
$$
]

(c) As a consequence of point (b), say whether $M \models \varphi$ or not.

[Solution: Yes, $\{s_0, s_1, s_2\} \subseteq [\varphi']$.]