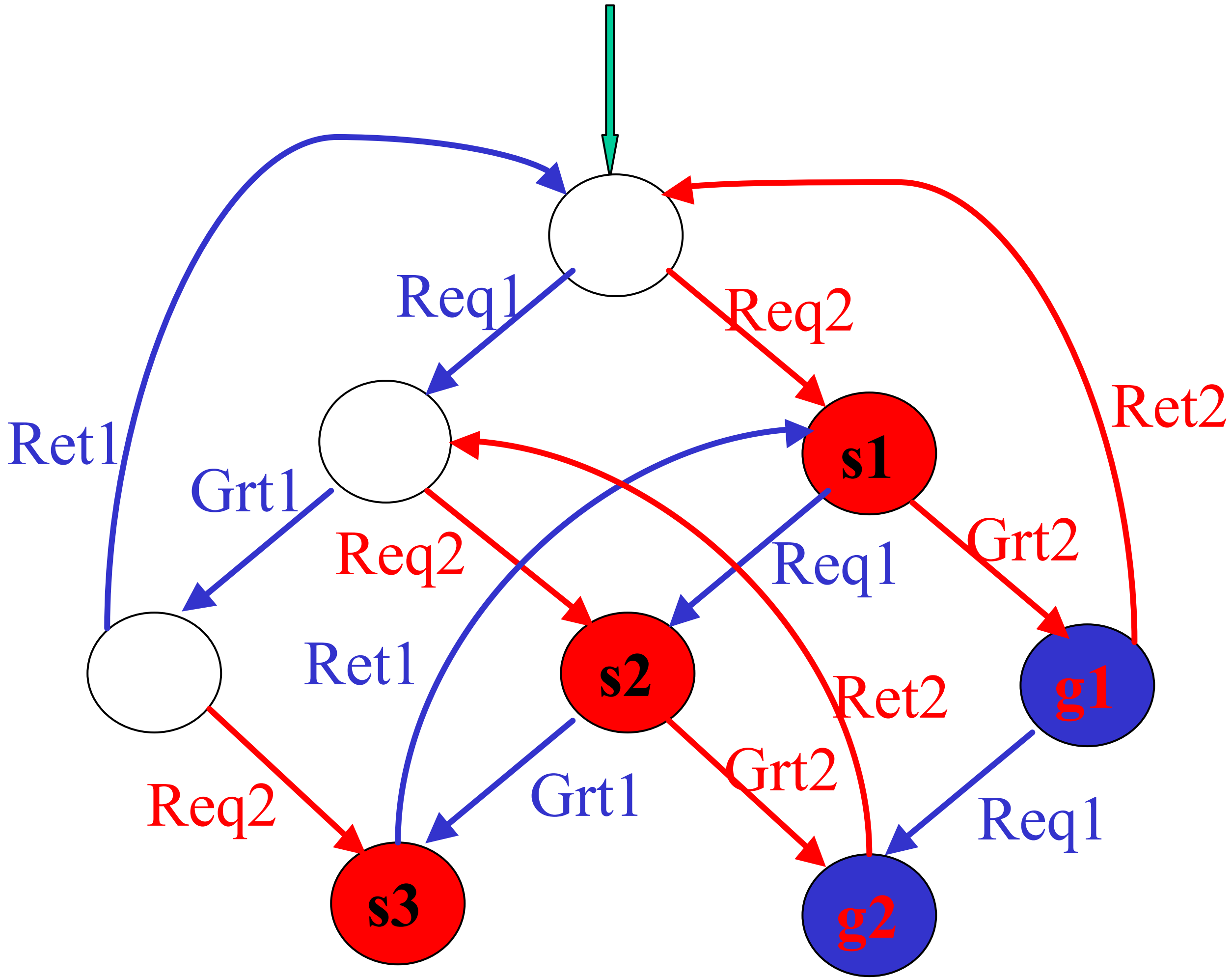
Tecniche di Specifica e di Verifica

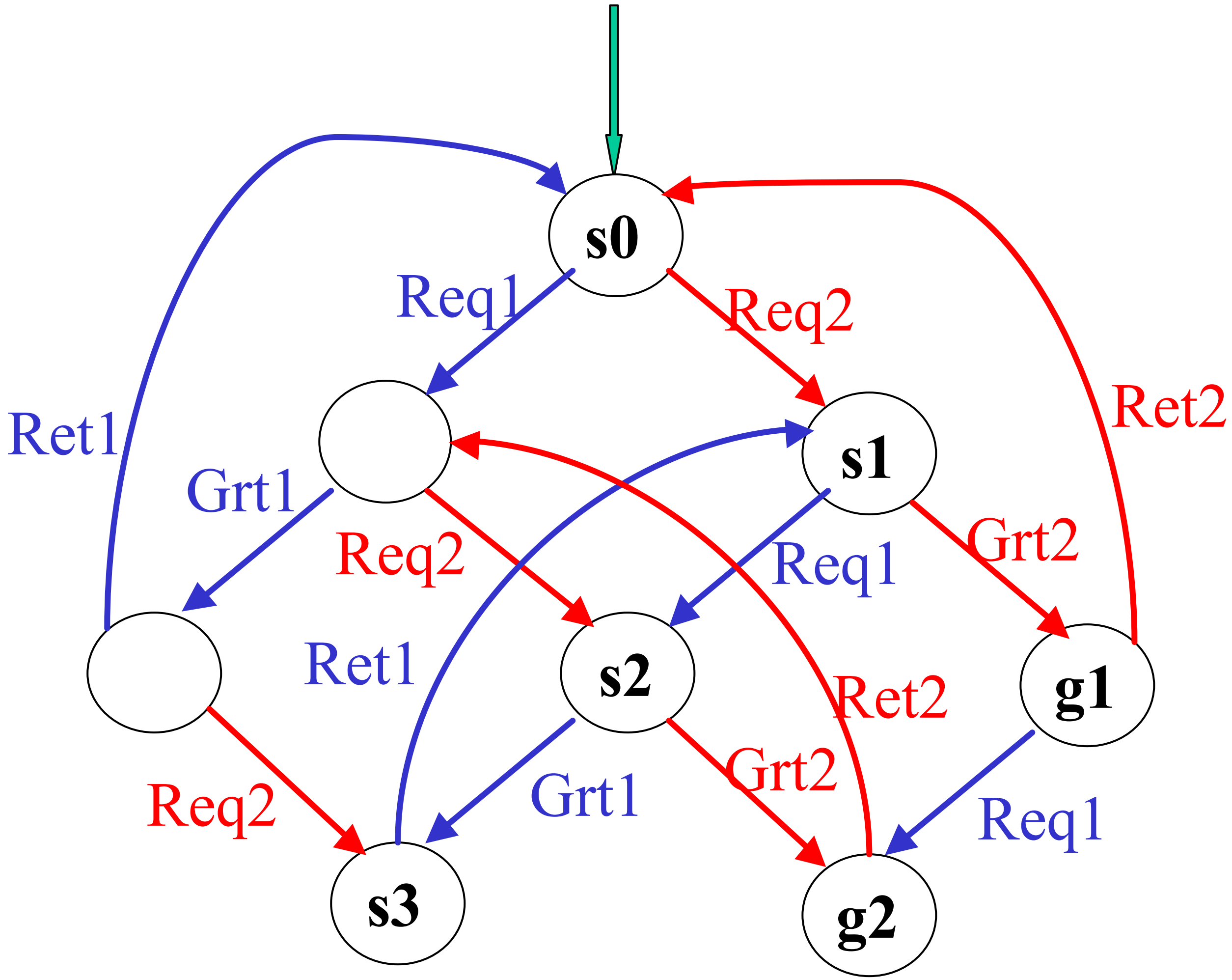
Model Checking under Fairness

Fairness

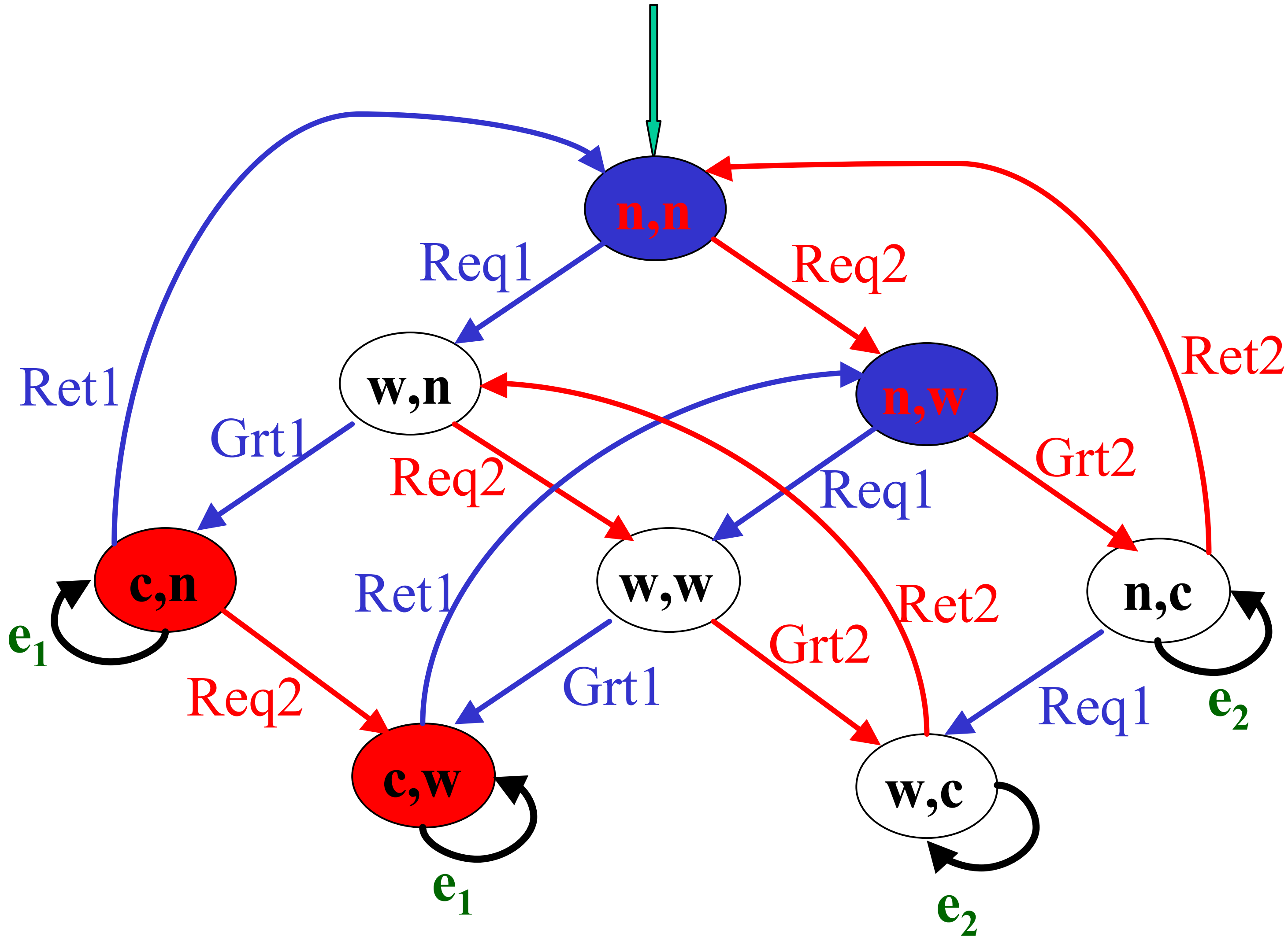
- **K =(S, S_0, R, AP, L)**
- **K** may ***not*** be able to capture ***exactly*** the desired executions.
  - Too generous.
- Use ***fairness constraints*** to rule out **undesired executions**.



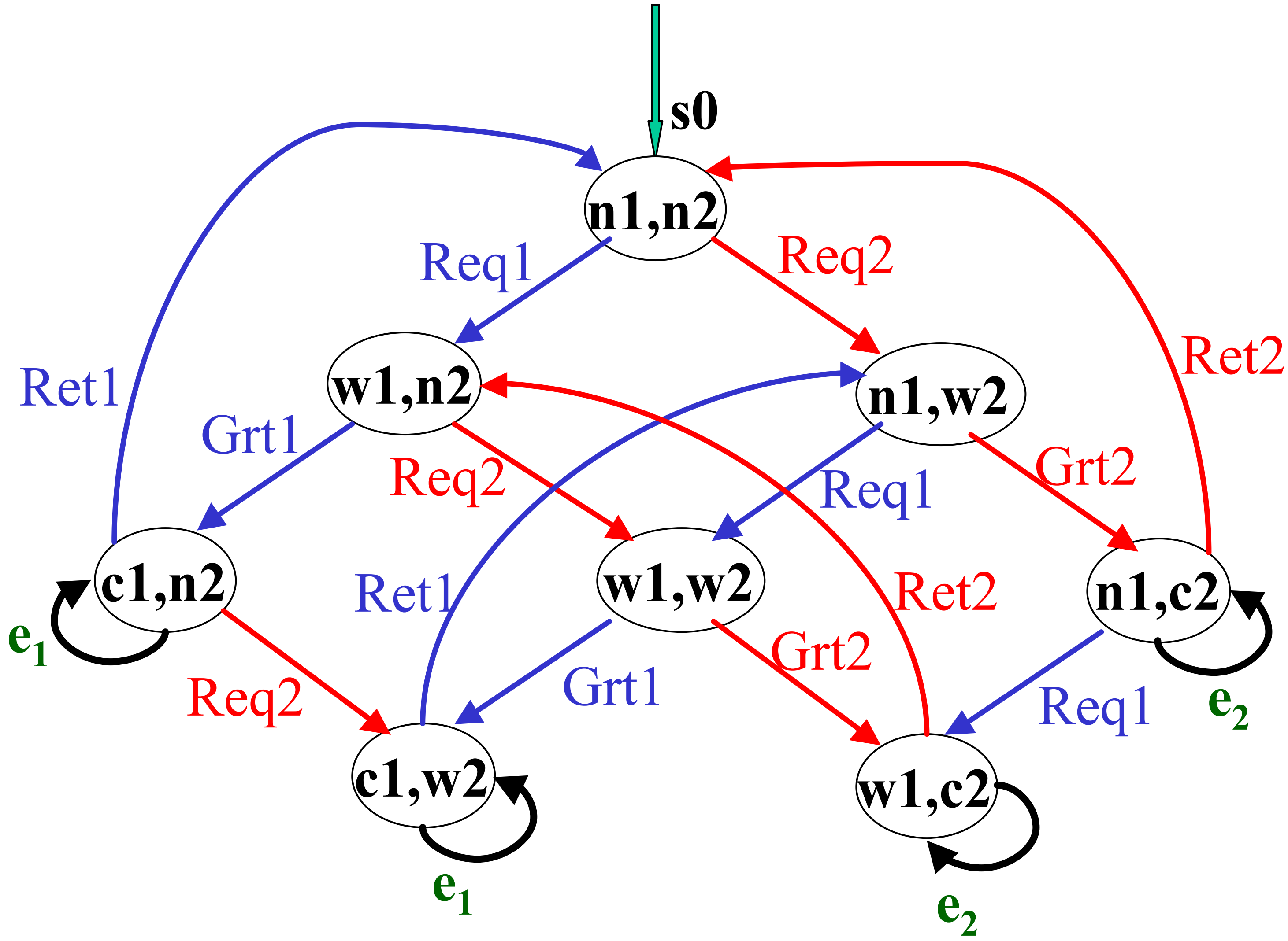
a **computation** in which **s1** or **s2** or **s3** is visited **infinitely** often but **g1** and **g2** are visited only **finitely often** is **unfair**.



K, s0 ⊭ AG (w2 ® AF grt2)



A computation in which **(c,n)** or **(c,w)** is visited infinitely often but **(n,n)** and **(n,w)** are visited only finitely often.


s0
n1,n2
Req1
Req2
Ret1
w1,n2
n1,w2
Ret2
Grt1
Req2
Grt2
Req1
c1,n2
w1,w2
n1,c2
e_1
Ret1
Ret2
Req2
Grt2
Grt1
Req1
e_2
c1,w2
w1,c2
e_1
e_2

K, s0 ⊨ EF EG c1 !

Fairness

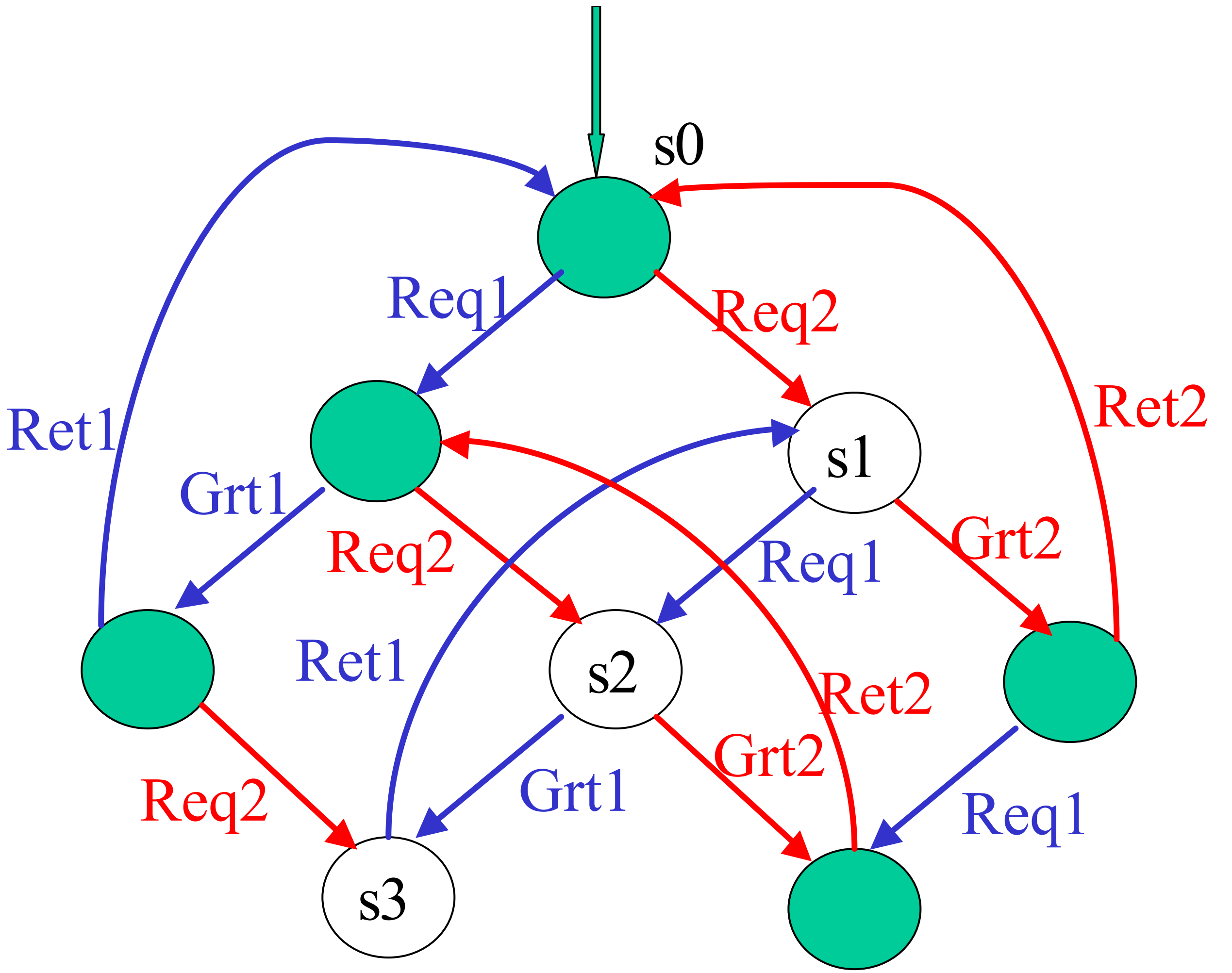
- The ***first kind of unfairness*** has to do with a ***bad scheduling policy***.
  - Find a better allocation scheme.
    - Turn-based.
- The ***second kind of unfairness*** is unavoidable.
- ***Solution***:
  - Consider only ***fair computations***.

Fairness

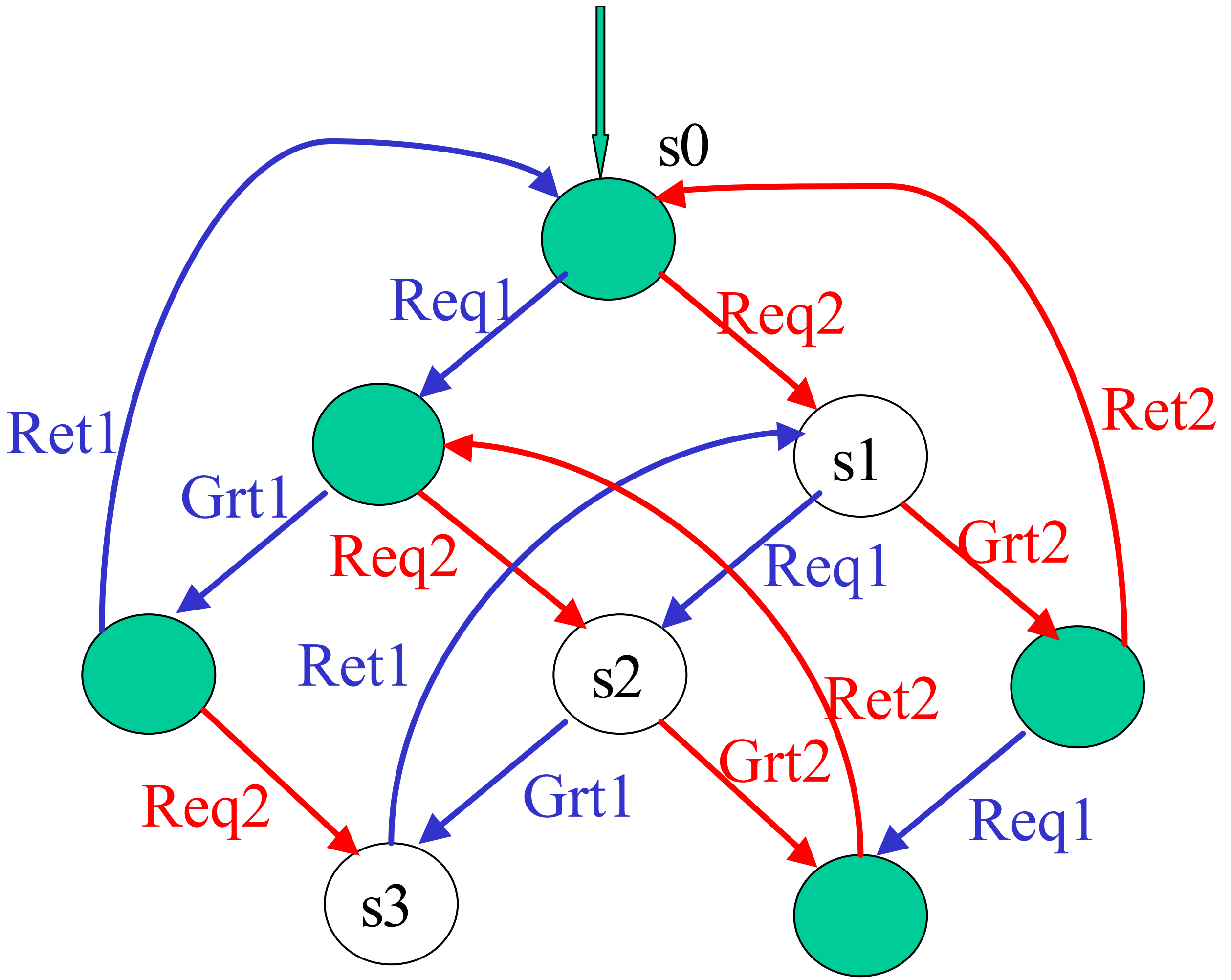
- ***Fair Kripke Structures***.
- First Attempt:
  - **K = (S, S_0, R, AP, L, F)**
  - F µ **S** (***fairness constraint***)
- π is a ***fair computation iff***:
  - It is a computation.
  - **inf**(p) Ç F ¹ Æ
  - **inf**(p) = {**s** : **s** appears infinitely often in p}

Fairness

- ***Fair Kripke Structures***.
- **K = (S, S_0, R, AP, L,** F_1, F_2,..,F_n**)**
  - F_i µ S (***fairness constraints***)
- p is a ***fair computation iff***:
  - It is a computation.
  - **inf(**p**)** Ç F_i ¹ Æ for each **i = 1, 2,..,n**
  - **inf(**p**) = {s : s** appears infinitely often in p}

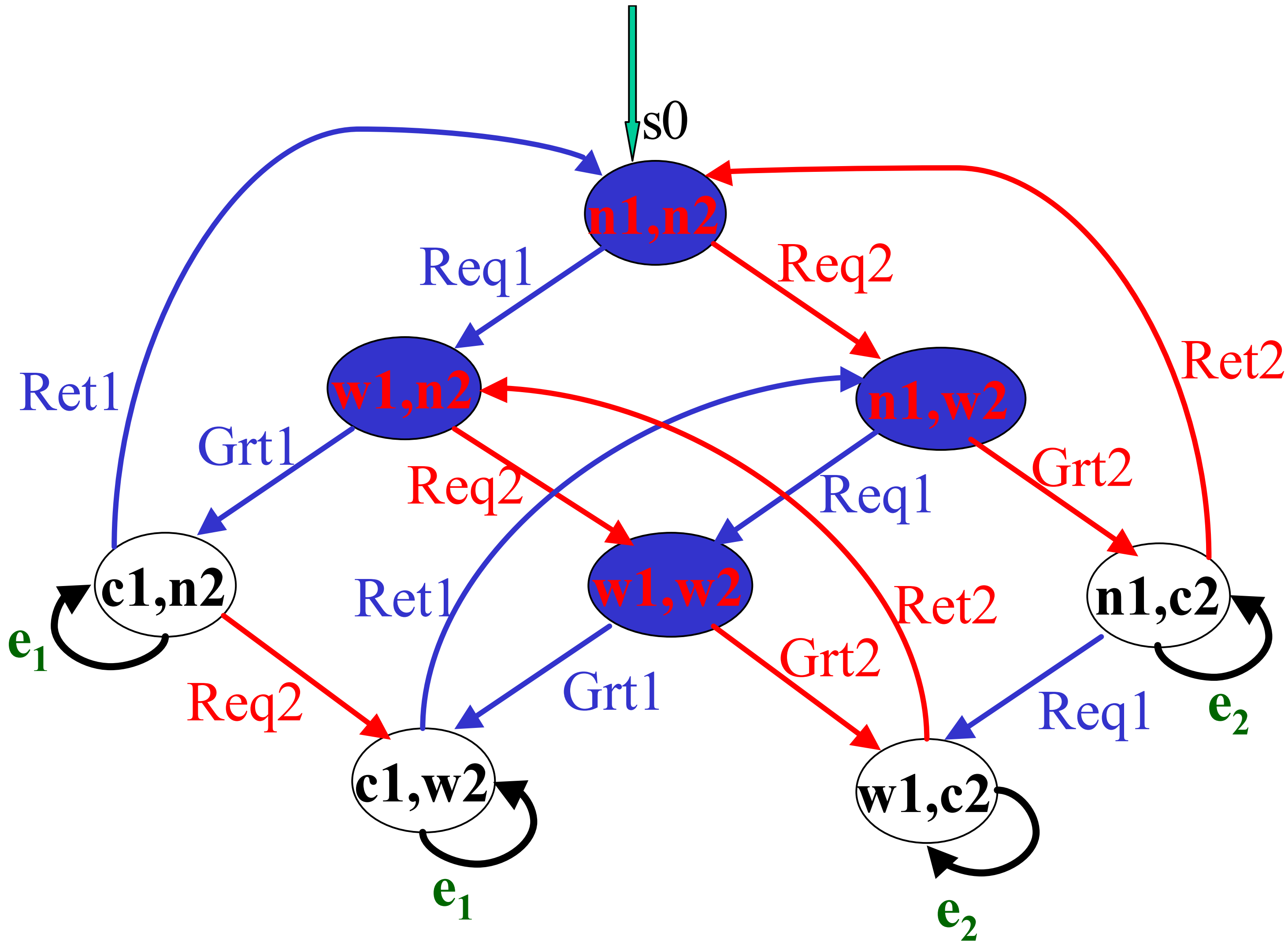


K, s0 ⊨ AG(w2 ® AF grt2) with above ***fairness constraint*** **!**



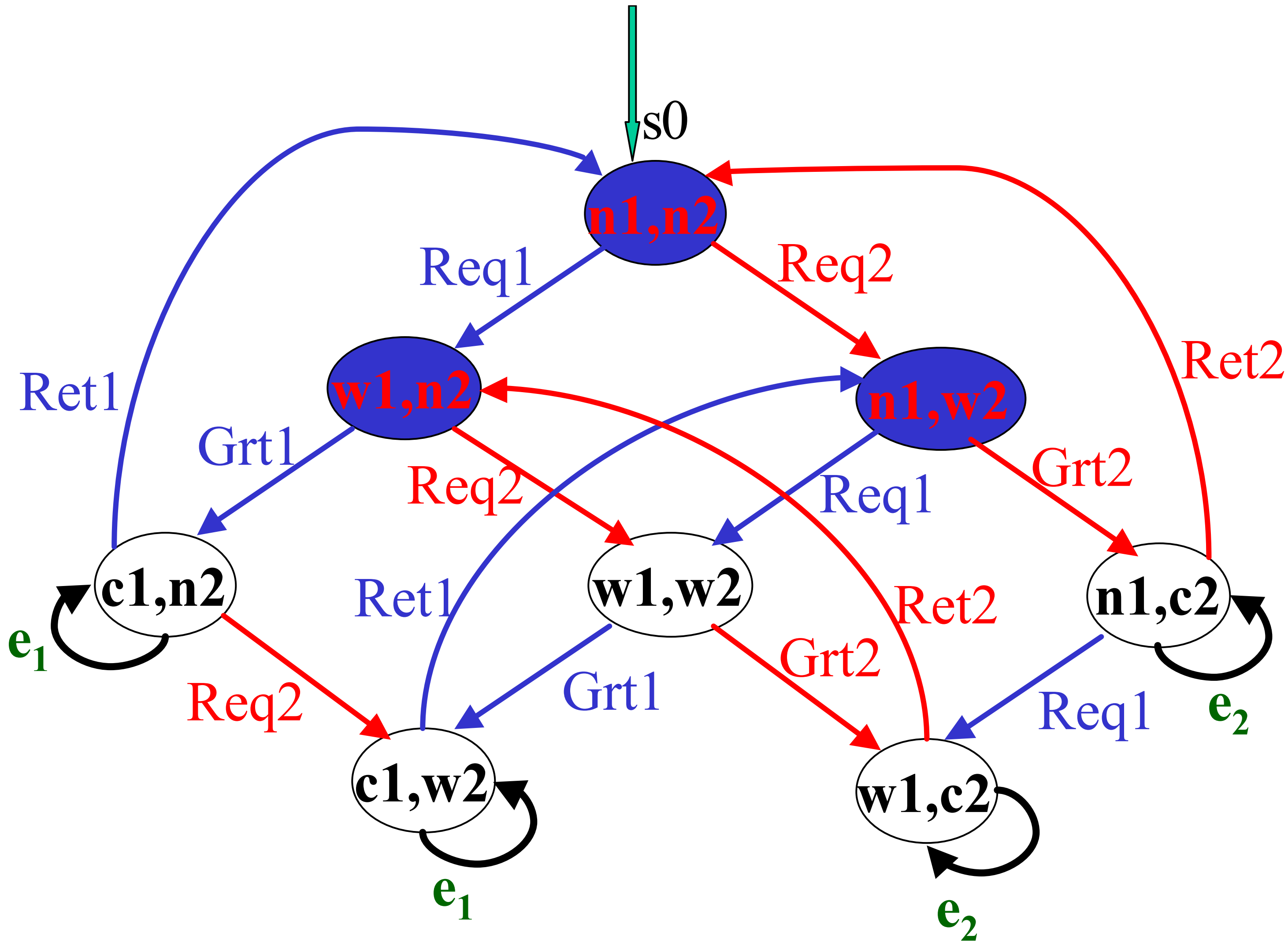
K, s0 ⊨ AG(w2 ® AF grt2)

F ---- Øw2 Ú grt2



K, s0 $\not\models$ EF (EG c1 Ú EG c2) with the above ***fairness constraint*** **!**

F ---- Øc1 Ù Øc2



K, s0 $\not\models$ **EF (EG c1 Ú EG c2)** with the above ***fairness constraint* !**

NuSMV Fairness

- Can't always use sets of states to specify fairness.
  - State space is often defined implicitly.
- Use formulas!
- f ---- Property f is true ***infinitely often***.
- ***Model check*** along only ***fair computation paths***.

NuSMV Fairness

- **$C = \{p_1, p_2, \ldots, p_n\}$**
  - Fairness constraints.
- **$K = (S, S_0, R, AP, L, C)$**
- **s0 s1 s2 …..** is a ***fair computation iff***:
  - ***It is a computation.***
  - ***For each i, there are infinitely many j such that***

$$K, s_j \models p_i$$

Model Checking with Fairness.

- $C = \{p_1, p_2, \ldots, p_n\}$
  - Fairness constraints.
- $K = (S, S_0, R, AP, L, C)$
- K, s ⊨$_C$ y ?
- K, s ⊨$_C$ p ***iff*** there exists a ***fair path*** from s and K, s ⊨ p (i.e. p Î L(s))
- K, s ⊨$_C$ y$_1$ Ù y$_2$ ***iff***

  K, s ⊨$_C$ y$_1$ and K, s ⊨$_C$ y$_2$

Model Checking with Fairness.

- $C = \{p_1, p_2, \ldots, p_n\}$
  - Fairness constraints.
- $K = (S, S_0, R, AP, L, C)$
- $K, s \models_C y$?
- $K, s \models_C EX y$ ***iff*** there exists a ***fair path*** from **s** and there exists **s'** along that path with **R(s, s')** and $K, s' \models_C y$.

Model Checking with Fairness.

- $C = \{p_1, p_2, \ldots, p_n\}$
  - Fairness constraints.
- $K = (S, S_0, R, AP, L, C)$
- $K, s \vDash_C y$?
- $K, s \vDash_C EU(y_1, y_2)$ ***iff*** there exists a ***fair path*** from **s** which satisfies $y_1 U y_2$.

Model Checking with Fairness.

- $C = \{p_1, p_2, \ldots, p_n\}$
  - Fairness constraints.
- $K = (S, S_0, R, AP, L, C)$
- $K, s \models_C y$?
- $K, s \models_C EG\, y$ ***iff*** there exists a ***fair path*** from **s** which satisfies y at every state along this fair path.

Model Checking with Fairness.

- $C = \{p_1, p_2, \ldots, p_n\}$
  - Fairness constraints.
- $K = (S, S_0, R, AP, L, C)$
- $K, s \models_C y$?
- It is possible to adapt the **NuSMV** model checking procedure:
  - $K, s \models y$

    to
  - $K, s \models_C y$.

Fair Strongly Connected Comp.

A non-trivial strongly connected component C of* K *is fair with respect to the fair set* C *=* {$\mathbf{p}_1$, $\mathbf{p}_2$,…, $\mathbf{p}_n$} *iff for each* $\mathbf{p}_i$ $\in$ C *there is a state s* $\in$ *C such that

$$K, s \models \mathbf{p}_i$$

M. C. with Fairness: EG(b)

Let **K' = (S',R',L', C)** be the sub-graph of **K** where

- **S' = { s | K, s $\models_C$ b }**
- **R' = R**$|_{S' \times S'}$ (the restriction of **R** to **S'**)
- **L' = L**$|_{S'}$ (the restriction of **L** to **S'**)

Lemma: K, s $\models_C$ EG(b) ***iff***

1. s $\in$ S' and

2. ***there exists a path*** in **K'** leading from **s** to a ***non-trivial fair strongly connected component*** **C** of the graph **(S',R')** *w.r.t.* C.

Computing the labeling for EG(β)

Complexity: O(|K||C|)

Algorithm Check_Fair_EG(β)

S' := {s | β Î Labels(s)};

SCC := {C | C is a *fair* non trivial SCC of S'};

T := È$_{C Î SCC}${s | s Î C};

for each s Î T do Labels(s) := Labels(s) È {**EG(β)**};

while T ¹ Æ do

chose s Î T;

T := T \{s};

for each t Î S' with t ® s do

if **EG(β)** Ï Lables(t) then

Labels(t) := Labels(t) È {**EG(β)**};

T := T È {t};

The Labels function

Let *fair* be a new *atomic proposition* and let us use the algorithm Check_Fair_EG(*true*) to label *K* with this new proposition (i.e. *fair* = *EG true*).

Then

- **K, s ⊨$_C$ p iff K, s ⊨ (p Ù *fair*)**
- **K, s ⊨$_C$ EX f iff K, s ⊨ EX (f Ù *fair*)**
- **K, s ⊨$_C$ EU(y , f) iff K, s ⊨ EU(y , f Ù *fair*)**

Symbolic MC for EG_f f

Let *Z* be the *largest set* of states with the following two properties:

1. **all of the states in Z satisfy f, and**
2. **for all p_k Î C and all states s Î Z**
   - **there is a *non-empty* sequence of states from s to a state in Z satisfying p_k, and**
   - **all states in the sequence satisfy the formula f.**

It can be shown that each state in Z is the beginning of a path on which f is *always true*,

and every formula in C holds *infinitely often* on this path.

Symbolic MC for EG_f f

It follows that $\mathbf{EG_f}\ \phi$ can be expressed as a greatest fixed point of the following function:

$$\mathbf{EG_f}\ \phi = \mathrm{n}\mathbf{Z.}\ \phi\ \text{Ù}\ \text{Ù}_{k=1\ldots n}\ \mathbf{EX\ EU}(\phi,\ Z\ \text{Ù}\ \mathbf{p_k})$$

This equation can be used to compute the set of states that satisfy $\mathbf{EG_f}\ \phi$ according to the ***fair semantics***.

Symbolic MC for $\mathbf{EX_f}\ \phi$ and $\mathrm{EU_f}(\phi,\psi)$

The set of all states which are the start of some ***fair computation*** is the set of states satisfying:

$$\textbf{\textit{fair}} = \mathbf{EG_f}\ \textbf{\textit{true}}$$

Hence,

$$\mathbf{EX_f}\ \phi = \mathbf{EX}(\phi \wedge \textbf{\textit{fair}});$$

$$\mathbf{EU_f}(\phi, \psi) = \mathbf{EU}(\phi, \psi \wedge \textbf{\textit{fair}})$$