Computer aided verification

Lecture 4: Model checking for LTL

(i) $M \mapsto \mathcal{A}_M$

(ii) $\neg\phi \mapsto \mathcal{A}_{\neg\phi}$ (not $\phi \mapsto \mathcal{A}_\phi \mapsto \bar{\mathcal{A}}_\phi$)

(iii) $L_\omega(\mathcal{A}_M) \cap L_\omega(\mathcal{A}_{\neg\phi}) = \emptyset$? (not $L_\omega(\mathcal{A}_M) \subseteq L_\omega(\mathcal{A}_\phi)$)

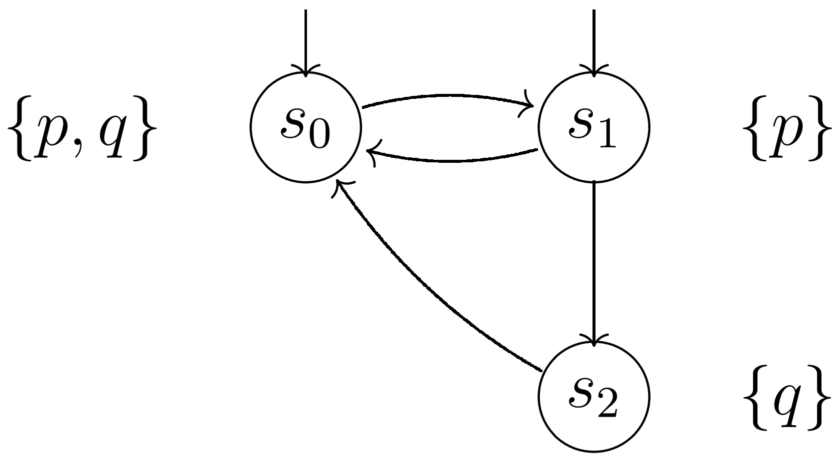
$L_\omega(\mathcal{A}_M \times \mathcal{A}_{\neg\phi}) = \emptyset$?

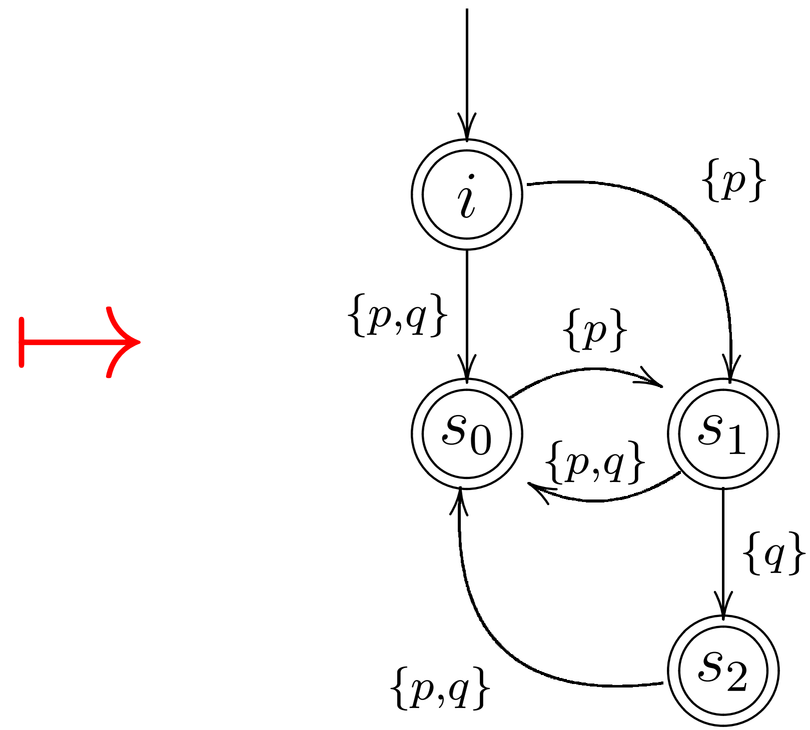
yes $\rightarrow M \models \phi$

no $\rightarrow \neg(M \models \phi)$, counterexample = a path in M

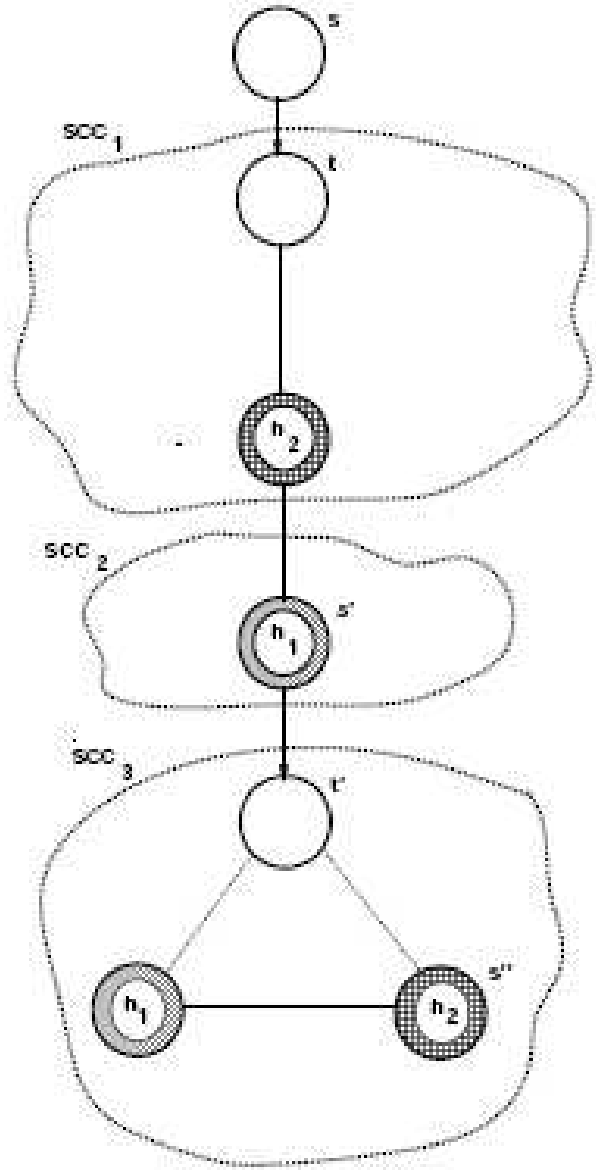
(i) $M \mapsto \mathcal{A}_M$

$M \mapsto \mathcal{A}_M$





(iii) $L_\omega(\mathcal{A}) \neq \emptyset$?

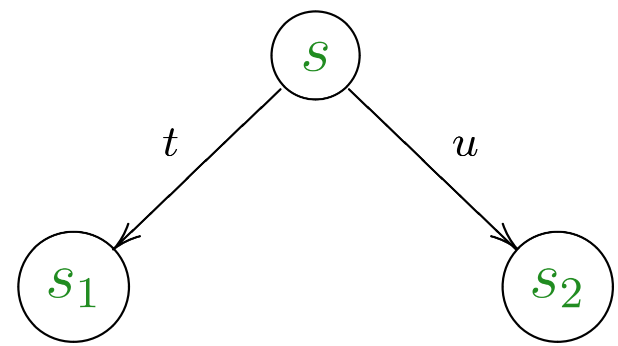


[Clarke, Grumberg, Peled 2000]

Restrictions

(1) On the fly verification

for each **successsor s_i of s do . . .**



. . .

Safety: DFS or BFS

```
proc dfs(s)
    if error(s) then report error fi
    add s to Statespace
    for each successor t of s do
      if t not in Statespace then dfs(t) fi
    od
end
```

[Holzmann,Peled,Yannakakis 1996]

Double DFS

```
proc dfs(s)
    if error(s) then report error fi
    add {s,0} to Statespace
    for each successor t of s do
       if {t,0} not in Statespace then dfs(t) fi
    od
    if accepting(s) then seed:=s; ndfs(s) fi
end
proc ndfs(s) /* the nested search */
    add {s,1} to Statespace
    for each successor t of s do
       if {t,1} not in Statespace then ndfs(t) fi
       else if t==seed then report cycle fi
    od
end
```

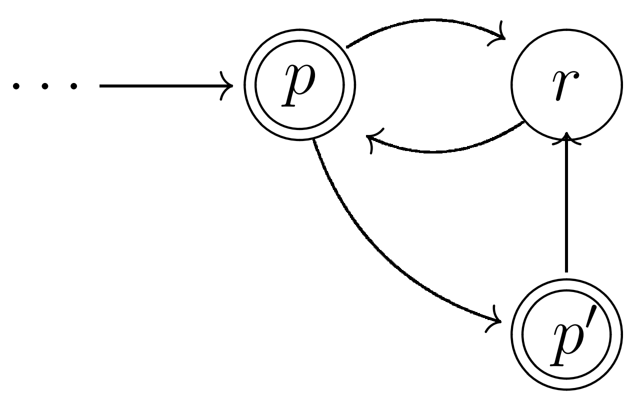
[Holzmann,Peled,Yannakakis 1996]

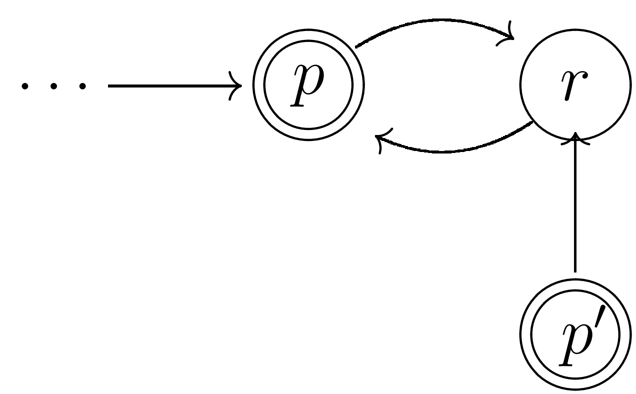
Proof of correctness

Assume an acceping state p with a cycle not detected by `ndfs(p)`. Let p – the first such state.

Let `r` – the first state inspected by `ndfs(p)` that is on a p-cycle and for which `{r,1}` in `Statespace`.

Let `p'` – the accepting state such that `r` visited by `ndfs(p')`.





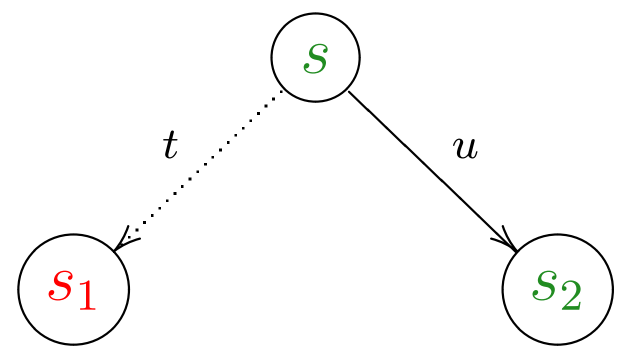
Restrictions (cont.)

(1) On the fly verification

for each **successsor** s_i **of** s **do . . .**

(2) Partial-order reductions

for each selected **successsor** s_i **of** s **do . . .**



selected – depends on states visited so far !

Solution

```
proc dfs(s)
    if error(s) then report error fi
    add {s,0} to Statespace
    add s to Stack
    for each (selected) successor t of s do
        if {t,0} not in Statespace then dfs(t) fi
    od
    if accepting(s) then ndfs(s) fi
    delete s from Stack
end
proc ndfs(s) /* the nested search */
    add {s,1} to Statespace
    for each (selected) successor t of s do
        if {t,1} not in Statespace then ndfs(t) fi
        else if t in Stack then report cycle fi
    od
end
```

[Holzmann,Peled,Yannakakis 1996]

np-cycles: FG ¬ progress

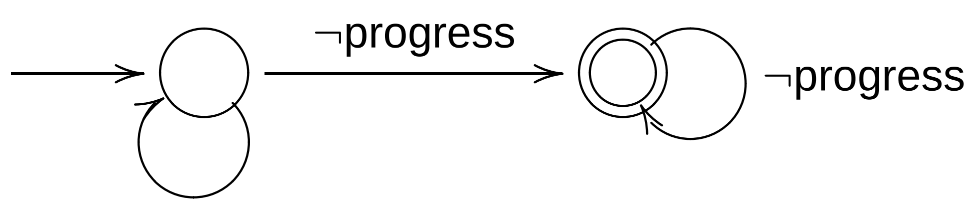
```
proc dfs(s)
    if error(s) then report error fi
    add {s,0} to Statespace
    for each successor t of s do
        if {t,0} not in Statespace then dfs(t) fi
    od
    ndfs(s) /* different */
end
proc ndfs(s) /* the nested search */
    if s is Progress State then return fi /* new */
    add {s,1} to Statespace
    add s to Stack /* new */
    for each successor t of s do
        if {t,1} not in Statespace then ndfs(t) fi
        else if t is in Stack then report cycle fi /* different */
    od
    delete s from Stack /* new */
end
```

[Holzmann,Peled,Yannakakis 1996]

np-cycles: automaton

```
never { /* non-progress: ◇□¬progress */
    do
    :: skip
    :: !progress -> break
    od;
accept: do
    :: !progress
    od
}
```

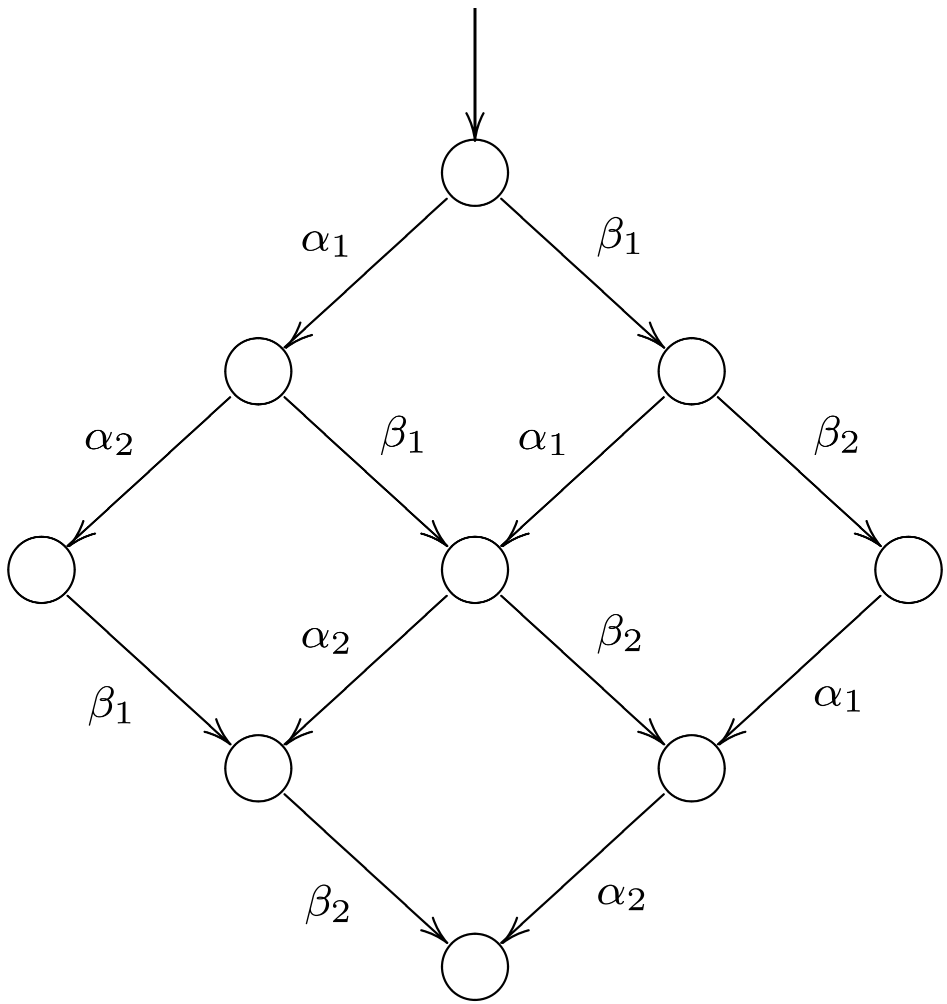
[Holzmann,Peled,Yannakakis 1996]



(co-Büchi $\subseteq$ Büchi)

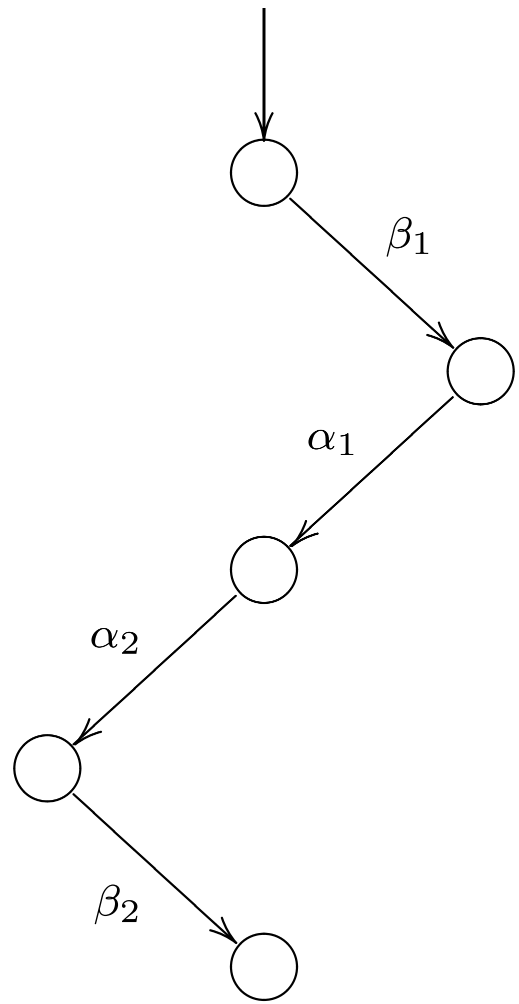
Partial-order reductions

Motivation

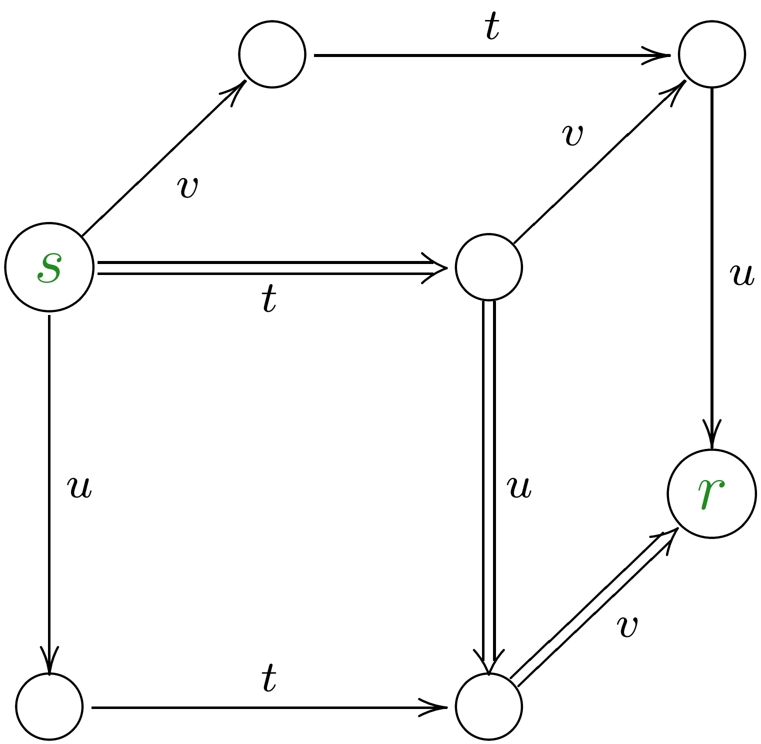


α_1
β_1
α_2
β_1
α_1
β_2
α_2
β_2
β_1
α_1
β_2
α_2

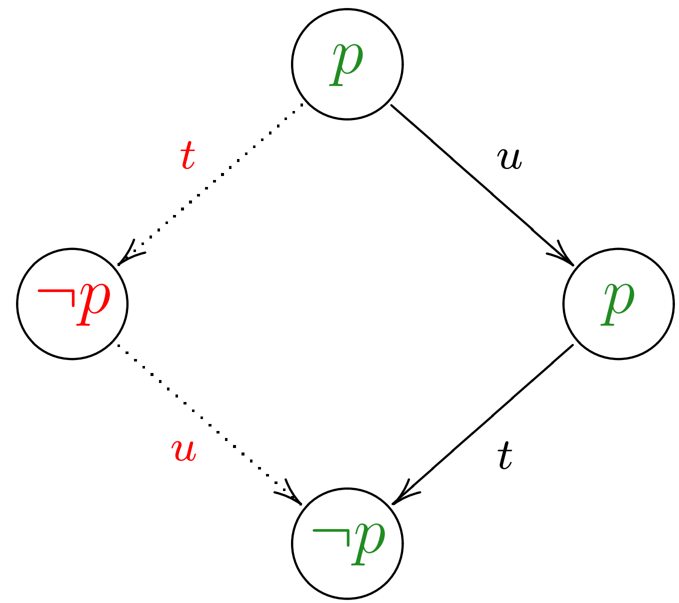
Motivation



Motivation



F $\neg p$



t, u niezależne

Model

Def.: $M = \langle S, S_{\text{init}}, T, L \rangle$ T – operations (transitions)

for $\alpha \in T$: $\mathrm{en}_\alpha \subseteq S$, $\alpha : \mathrm{en}_\alpha \to S$ (determinism)

path: $\Pi = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} s_2 \xrightarrow{\alpha_2} \ldots$ $s_0 = s_{\text{init}}$

$\alpha_i(s_i) = s_{i+1}$

$\mathrm{en}_s := \{\alpha \mid s \in \mathrm{en}_\alpha\}$ $(\alpha \in \mathrm{en}_s \iff s \in \mathrm{en}_\alpha)$

Idea: $\mathrm{ample}_s \subseteq \mathrm{en}_s$ instead of en_s in double DFS ?

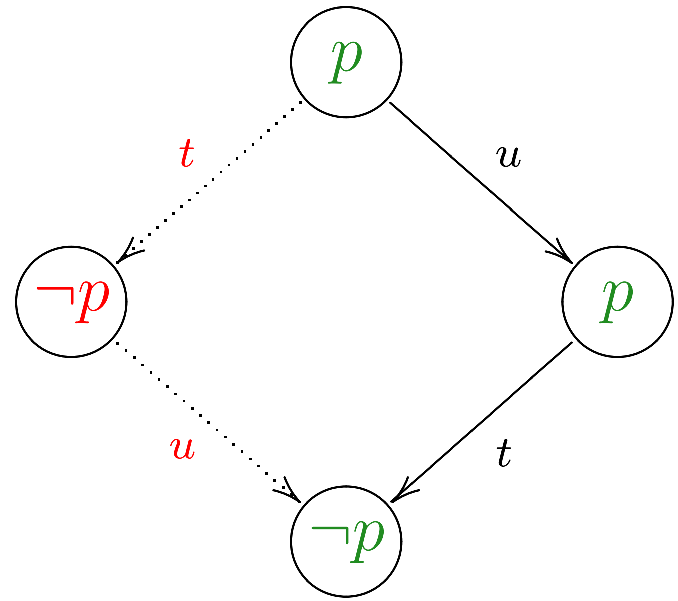
Idea: $\mathrm{ample}_s \subseteq \mathrm{en}_s$ instead of en_s in double DFS ?

This makes sense, when:

- the result of verification is the same (correctness)
- significantly less states visited
- time overhead reasonable (effectivity)

Problems?

When may we ignore t ?



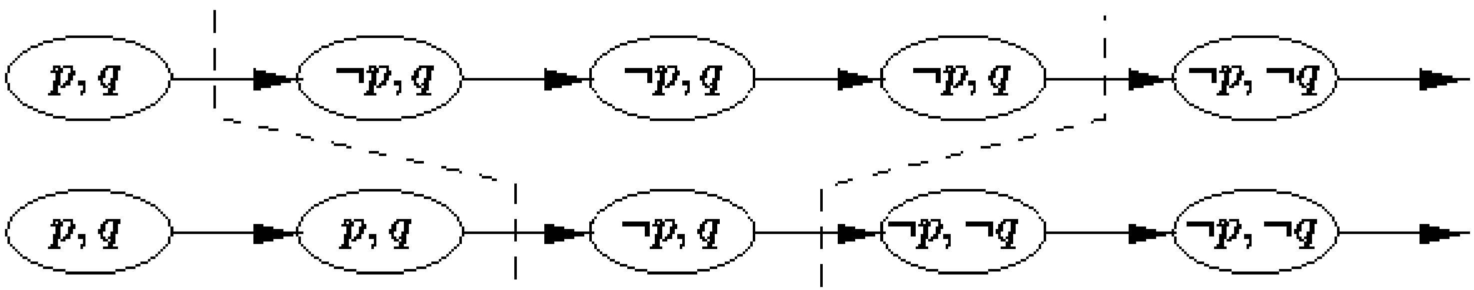
Problem 1: Property may depend on state $\neg p$.

Problem 2: $\neg p$ –successors unreachable otherwise.

Def.: $\Pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ i $\Pi' = s'_0 \rightarrow s'_1 \rightarrow s'_2 \rightarrow \ldots$ are stuttering equivalent, $\Pi \equiv \Pi'$, if sequences

$$L(s_0), L(s_1), L(s_2), \ldots \qquad L(s'_0), L(s'_1), L(s'_2), \ldots$$

become identical after grouping is done:



Def.: $M \equiv M'$ if and only if

– $\forall \Pi\ w\ M \quad \exists \Pi'\ w\ M' \quad \Pi \equiv \Pi'$

– $\forall \Pi'\ w\ M' \quad \exists \Pi\ w\ M \quad \Pi \equiv \Pi'$

LTL$_{-X}$ = LTL without X

Thm: If $\phi \in$ LTL$_{-X}$ and $\Pi \equiv \Pi'$, then $\Pi \models \phi \iff \Pi' \models \phi$

Thm: If $\phi \in$ LTL$_{-X}$ and $M \equiv M'$, then $M \models \phi \iff M' \models \phi$

Thm: LTL$_{-X}$ $=$ FO$_{\equiv}$

Correctness

$$M \xmapsto{\text{partial-order reduction}} M'$$

$$M \equiv M'$$

Sufficient condition for correctness

(C0) $\text{ample}_s = \emptyset \iff \text{en}_s = \emptyset$

(C1) ...

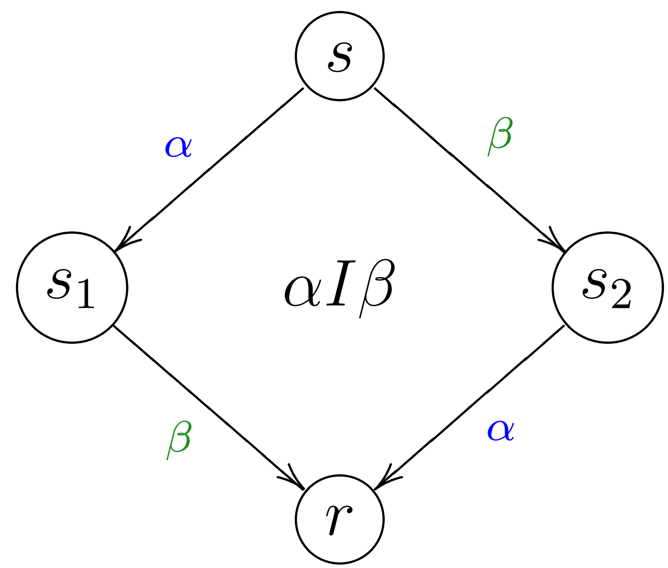
(C2) ...

(C3) ...

Def.: α is invisible if $L(s) = L(\alpha(s))$, $\forall\ s \in \mathrm{en}_\alpha$.

Przykład: If α invisible, then

$$ss_1r \equiv ss_2r$$



Sufficient condition for correctness

(C0) $\mathrm{ample}_s = \emptyset \iff \mathrm{en}_s = \emptyset$

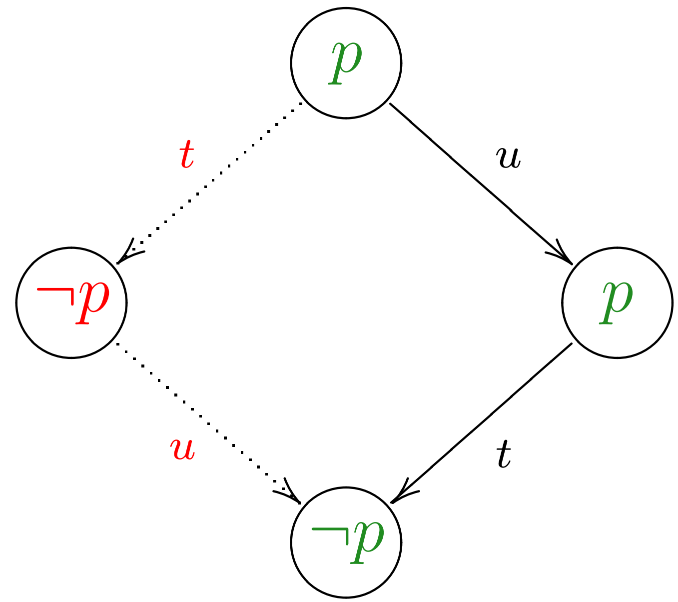
(C1) if $\mathrm{ample}_s \neq \mathrm{en}_s$ then every $\alpha \in \mathrm{ample}_s$ is invisible

(C2) ...

(C3) ...

Idea: Instead of doing sth now, do it in future!

Problem 1: Property may depend on state $\neg p$.

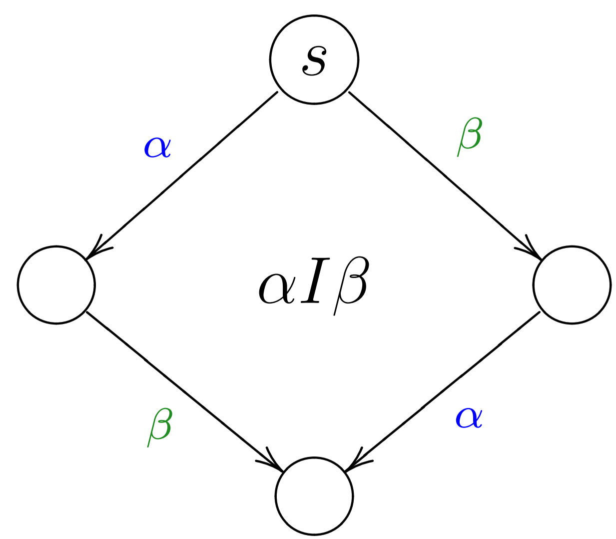


Solved due to **(C1)** !

(C1) if $\mathrm{ample}_s \neq \mathrm{en}_s$, then every $\alpha \in \mathrm{ample}_s$ is invisible

Def.: Relation of independence $I \subseteq T \times T$:

- irreflexive and antisymmetric
- if $\alpha I \beta$, $\alpha \in \mathrm{en}_s$, $\beta \in \mathrm{en}_s$, then ($s \in \mathrm{en}_\alpha \cap \mathrm{en}_\beta$)
  - $\beta(s) \in \mathrm{en}_\alpha$, $\alpha(s) \in \mathrm{en}_b$
  - $\beta(\alpha(s)) = \alpha(\beta(s))$



$D = T \times T \setminus I$ (dependency)

Example: Independent may be:

- 2 instructions of different processes operating on local variables
- 2 instructions of different processes that increment the same global variable
- 2 instructions of different processes writing to/reading from different buffers

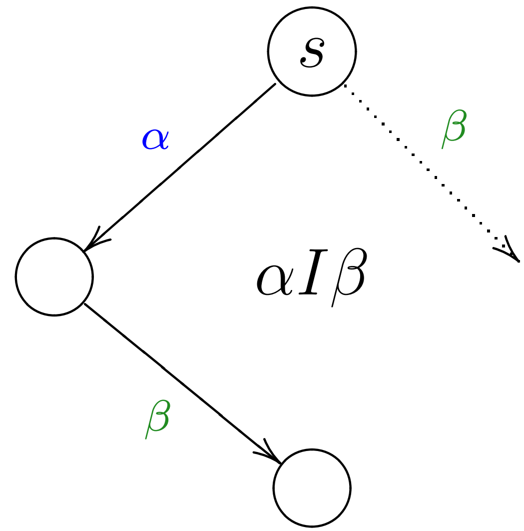
Example: Independent may be:

- 2 instructions of different processes operating on local variables
- 2 instructions of different processes that increment the same global variable
- 2 instructions of different processes writing to/reading from different buffers

- 2 instructions of the same process ?

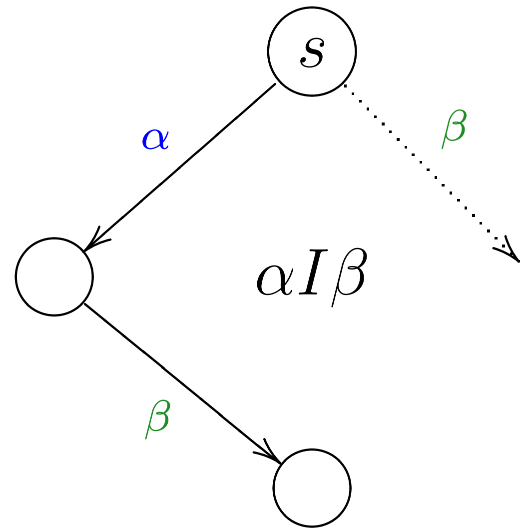
Question: Let $\alpha I \beta$. Is it possible that

$$s \in \mathrm{en}_\alpha \setminus \mathrm{en}_\beta \qquad \alpha(s) \in \mathrm{en}_\beta \ ?$$



Question: Let $\alpha I \beta$. Is it possible that

$$s \in \mathrm{en}_\alpha \setminus \mathrm{en}_\beta \qquad \alpha(s) \in \mathrm{en}_\beta \ ?$$



Yes! E.g. asynchronous reading and writing from/to the same buffer by two different processes.

Sufficient condition for correctness

(C0) $\mathrm{ample}_s = \emptyset \iff \mathrm{en}_s = \emptyset$

(C1) if $\mathrm{ample}_s \neq \mathrm{en}_s$ then every $\alpha \in \mathrm{ample}_s$ is invisible

(C2) ? $\left(\mathrm{en}_s \setminus \mathrm{ample}_s\right) \; I \; \mathrm{ample}_s$

(C3) ...

Idea: Instead of doing sth now, do it in future!

(C2) a transition dependent on some transition from ample_s

can not be executed

before some transition from ample_s is executed

(C2) a transition dependent on some transition from ample_s

can not be executed

before some transition from ample_s is executed

(C2) for every path Π starting in s:

if $\alpha \in \mathrm{ample}_s,\ \beta \notin \mathrm{ample}_s,\ \alpha D \beta$

then β can not be executed in Π

before some transition from ample_s is executed

Lemma: **(C2)** implies $(\mathrm{en}_s \setminus \mathrm{ample}_s)\ I\ \mathrm{ample}_s$.

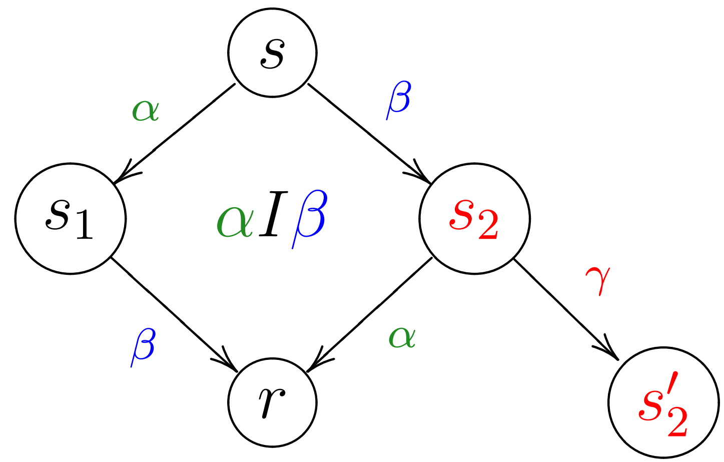
Proof: Let $\beta \in \mathrm{en}_s \setminus \mathrm{ample}_s$, $\alpha \in \mathrm{ample}_s$, $\alpha D \beta$.

$$s \xrightarrow{\beta} \beta(s) \rightarrow \ldots$$

contradiction with **(C2)** .

Problems?

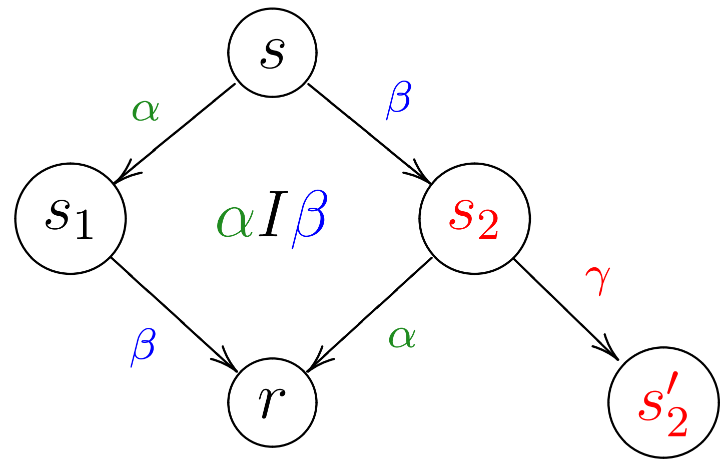
Problem 2: $\circled{s_2}$–successors unreachable otherwise.



e.g., let $\alpha \in \mathrm{ample}_s, \beta \notin \mathrm{ample}_s$

Problems?

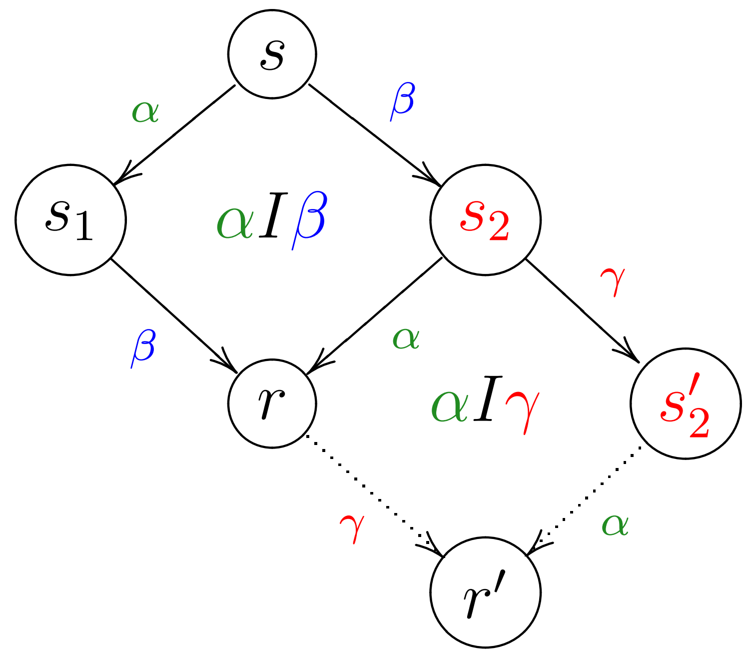
Problem 2: s_2–successors unreachable otherwise.



e.g., let $\alpha \in \text{ample}_s, \beta \notin \text{ample}_s$

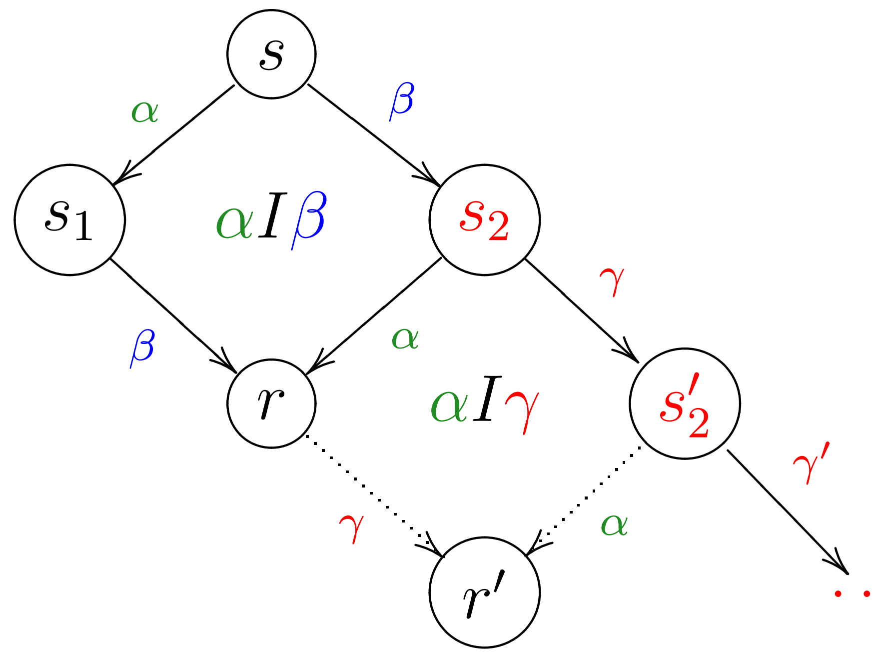
by **(C2)** applied to $\beta\gamma\ldots$, we deduce $\gamma I \alpha$

Problem 2: s_2–successors unreachable otherwise.



α invisible, thus $ss_1rr' \equiv ss_2s_2'$

Problem 2^{∞}: (s_2)–path unreachable otherwise.

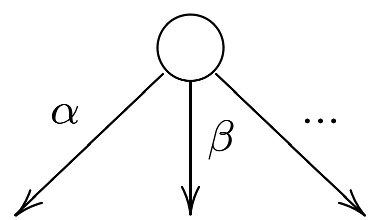


by **(C2)** we deduce $\gamma I \alpha$, $\gamma' I \alpha$, ...

α invisible, thus $s s_1 r r' \ldots \equiv s s_2 s'_2 \ldots$

Def. (weak fairness): if $\alpha \in \mathrm{en}_s$ almost always then α eventually executed.

Corollary: for every reachable state s, if $\alpha \in \mathrm{en}_s$ then eventually some β will be executed such that $\alpha D \beta$.



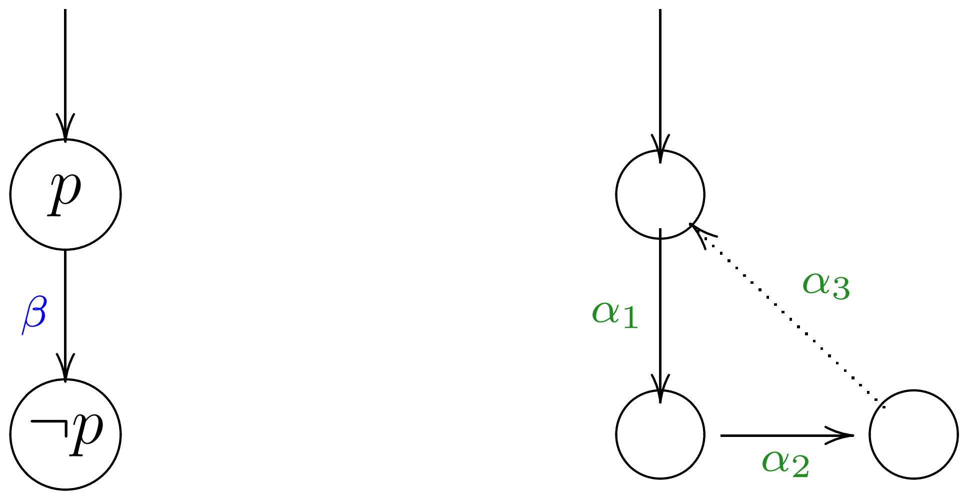
Problem 2^∞ does not appear under weak fairness

Enough?

Are **(C0)** – **(C2)** sufficient?

Are **(C0)** – **(C2)** sufficient?

No!



(C3) we forbid cycles C such that $\exists \beta \;\; \forall s \in C \;\; \beta \in \mathrm{en}_s \setminus \mathrm{ample}_s$

Sufficient condition for correctness

(C0) $\mathrm{ample}_s = \emptyset \iff \mathrm{en}_s = \emptyset$

(C1) if $\mathrm{ample}_s \neq \mathrm{en}_s$ then every $\alpha \in \mathrm{ample}_s$ is invisible

(C2) for every path Π starting in s:

if $\alpha \in \mathrm{ample}_s,\ \beta \notin \mathrm{ample}_s,\ \alpha D \beta$

then β can not be executed in Π

before some transition from ample_s is executed

(C3) we forbid cycles C such that $\exists \beta\ \ \forall s \in C\ \ \beta \in \mathrm{en}_s \setminus \mathrm{ample}_s$

How to implement this?

Sufficient condition for correctness

(C1) easy

(C2) hard, implemented in an approximate manner

- an over-approximation of D is computed
- condition **(C2)** is monotonic
- static analysis only

(C3) replaced by an easier but stronger:

(C3') if $\mathrm{ample}_s \neq \mathrm{en}_s$ then $\forall \alpha \in \mathrm{ample}_s \ \alpha(s) \notin$ stack

Implementation decision:

$\mathrm{ample}_s =$ all transitions of some process i enabled in s

Implementation decision:

$\mathrm{ample}_s =$ all transitions of some process i enabled in s

whenever

- they are independent from all operations of all other processes
- no operation of any other process may enable any other operation of process i

β enabling α (over-approximation)

– if β modifies pc so that α may be executed

– if Promela enabling condition for α depends on global variables, then any β that modifies these variables

– if α is reading from/writing to a buffer then any β that reads from/writes to this buffer

$\alpha D \beta$ (over-approximation)

– α i β refer to the same global variable

and at least one of them modifies the variable (over-appr.)

– α i β belong to the same process; synchronous communi-

-cation is understood as belonging to both processes

– α i β write to/read from the same buffer

However reading from and writing to the same buffer is independent!

What remains independent?

Example:

Operations independent from all operations of other processes:

- operating on local variables
- reading from a buffer with xr flag set
- writing to a bugger with xs flag set
- test `nempty(q)` if xr flad is set for q
- test `nfull(q)` if xs flaf is set for q

P.-o. reductions and on the fly verification

– in both DFS's the set ample_s should be the same

– condition **(C3')** is applied to $M \times \mathcal{A}_{\neg\phi}$ instead of M.

Is it correct?