# Property-Dependent Reductions for the Modal Mu-Calculus


Radu Mateescu

*INRIA Grenoble – Rhône-Alpes / LIG*

*VASY project-team*

*France*

http://vasy.inria.fr

Anton Wijs

*Technische Universiteit Eindhoven*

*Software Engineering & Technology*

*The Netherlands*

http://win.tue.nl

# Overview

- Motivation
- Background: PDL-$\Delta$ and modal mu-calculus
- Maximal hiding
- Mu-calculus fragment for ds-branching bisimulation
- Implementation and experiments
- Conclusion and future work

# Motivation

- Action-based setting:
  - Process algebras, $\mu$-calculi
  - Labeled transition system (LTS) models
  - Abstraction (hiding) and bisimulation minimization
- Objective:
  - Improve model checking performance
  - Reduce the LTS modulo the formula to be verified
- Approach:
  - Identify the maximum set of actions that can be hidden without disturbing the interpretation of the formula
  - Apply maximal hiding, then minimize the LTS modulo a bisimulation relation compatible with the formula

# Related work

- Selective $\mu$-calculus [Barbuti-et-al-99]
  - Syntactic criterion for hiding actions

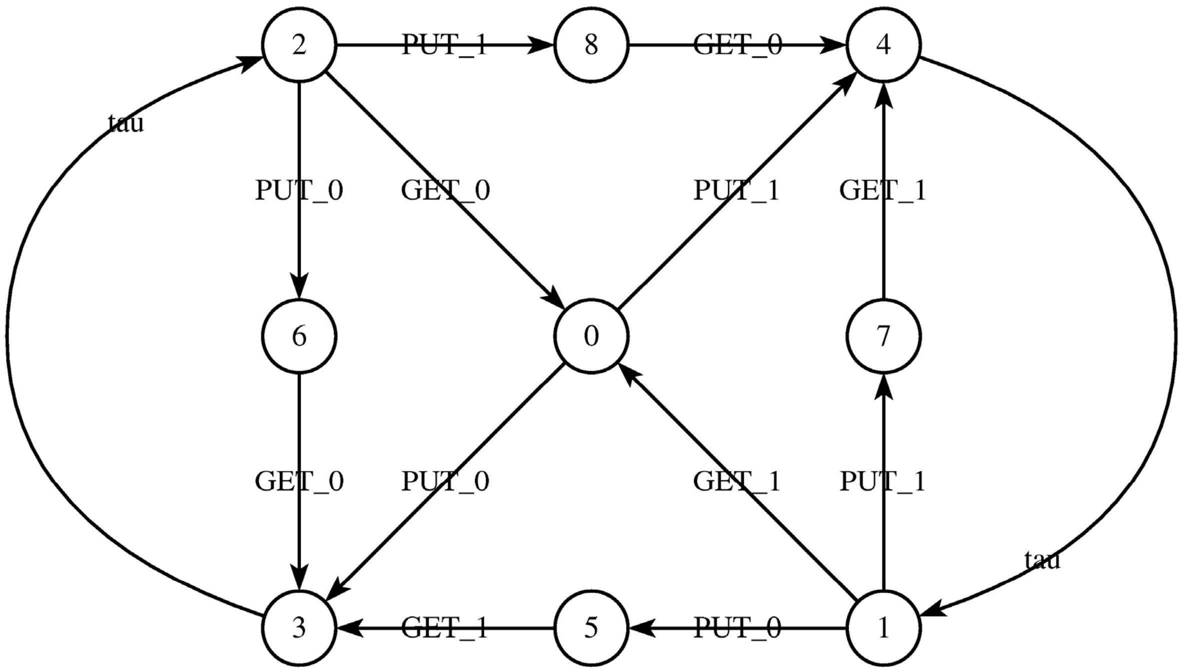
    ➔ *we use a semantic criterion (larger hiding sets)*
  - Reductions compatible with $\tau^*.a$ bisimulation

    ➔ *we use ds-branching bisimulation (stronger relation)*
- Adequacy between logics and bisimulations
  - $\mu$ACTL-X [Fantechi-Gnesi-et-al-92]
    - Adequate wrt ds-branching bisimulation
  - Weak $\mu$-calculus [Stirling-01]
    - Adequate wrt weak bisimulation

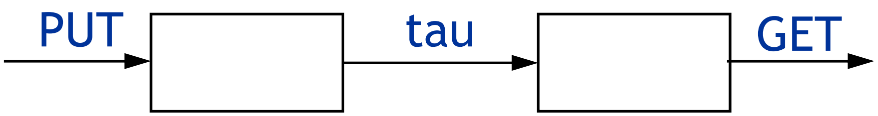
    ➔ *we define a $\mu$-calculus fragment subsuming these two logics*

# Background (1/5)

- Labeled transition system (LTS) $M = (S, A, T, s_0)$:




Two-place buffer:



# Background (2/5)

- Modal μ-calculus:

**Action formulas:**

| | |
|---|---|
| $\alpha ::= b$ | *action name* |
| $\quad \mid\ \text{false} \mid \neg\alpha_1 \mid \alpha_1 \vee \alpha_2$ | *boolean operators* |

**State formulas:**

| | |
|---|---|
| $\varphi ::= \text{false} \mid \neg\varphi_1 \mid \varphi_1 \vee \varphi_2$ | *boolean operators* |
| $\quad \mid\ <\alpha>\varphi \mid [\alpha]\varphi$ | *modal operators* |
| $\quad \mid\ X \mid \mu X.\varphi \mid \nu X.\varphi$ | *fixed point operators* |

# Background (3/5)

- Propositional Dynamic Logic with Looping (PDL-$\Delta$):

**Regular formulas:**

$\beta ::= \alpha$ — *one-step sequence*

$\quad | \ \varphi? \mid \beta_1.\beta_2 \mid \beta_1|\beta_2 \mid \beta_1^*$ — *regular operators*

**State formulas:**

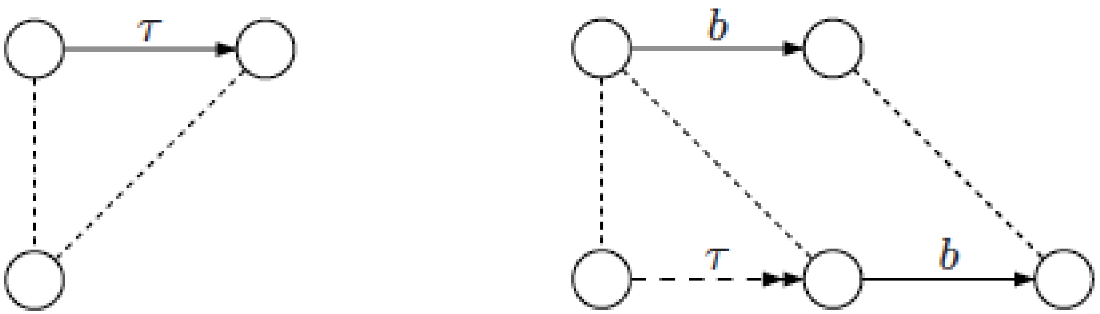
$\varphi ::= \text{false} \mid \neg\varphi_1 \mid \varphi_1 \vee \varphi_2$ — *boolean operators*

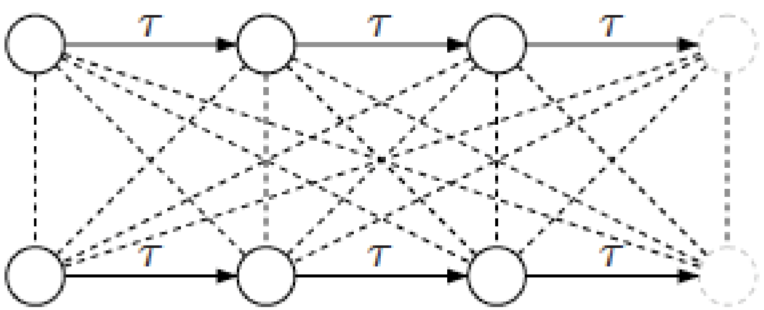
$\quad | \ < \beta > \varphi \mid [\ \beta\ ]\ \varphi$ — *modal operators*

$\quad | \ < \beta > @ \mid [\ \beta\ ]\ -|$ — *fairness operators*

# Background (4/5)

- Divergence-sensitive branching bisimulation [Van Glabbeek-Weijland-96]

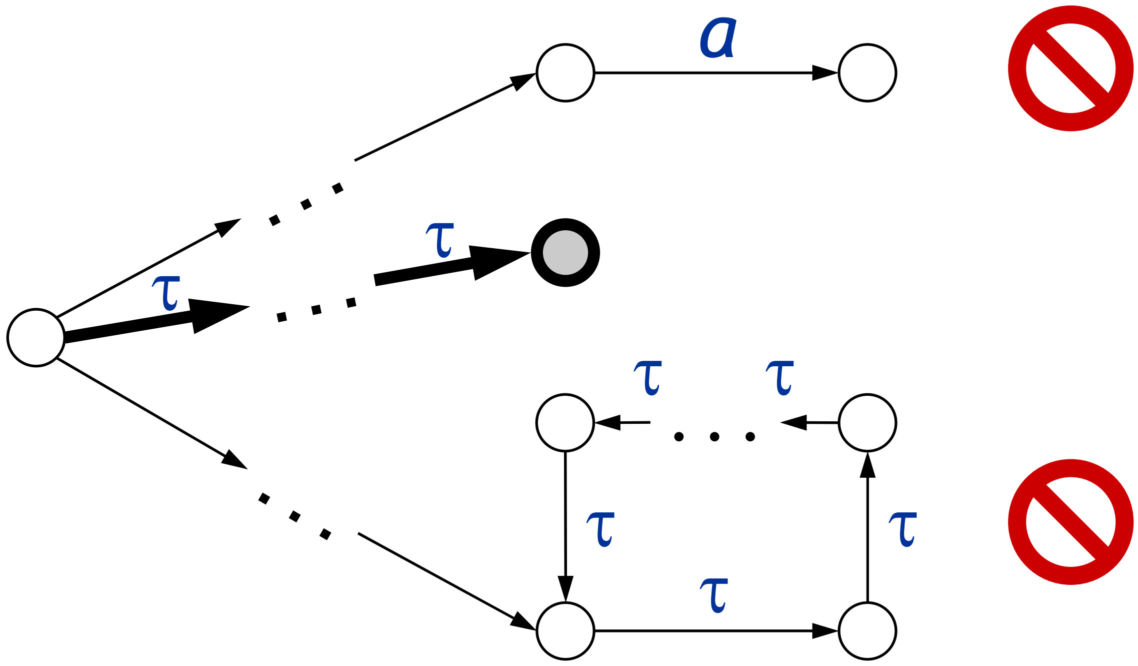


# Background (5/5)

- Deadlock states (modulo ds-bb):

$$deadlock = \underbrace{[\ true^* \ .\ \neg\tau\ ]\ \text{false}}_{\text{no visible actions reachable}} \wedge \underbrace{[\ \tau\ ]\ \text{-|}}_{\text{no } \tau\text{-cycles}}$$



# Maximal hiding (1/2)

- Hiding set of an action formula:

$$h_A(\alpha) = \begin{cases} [[\ \alpha\ ]] & \text{if } \tau \in [[\ \alpha\ ]] \\ A - [[\ \alpha\ ]] & \text{if } \tau \notin [[\ \alpha\ ]] \end{cases}$$

  Examples:

  $h_A(\neg \mathrm{GET}) = [[\ \neg \mathrm{GET}\ ]] = A - \{\ \mathrm{GET}\ \}$

  $h_A(\mathrm{PUT}) = A - [[\ \mathrm{PUT}\ ]] = A - \{\ \mathrm{PUT}\ \}$

- Hiding set of a state formula:

$$h_A(\varphi) = \cap \{\ h_A(\alpha) \mid \alpha \subset \varphi\ \}$$

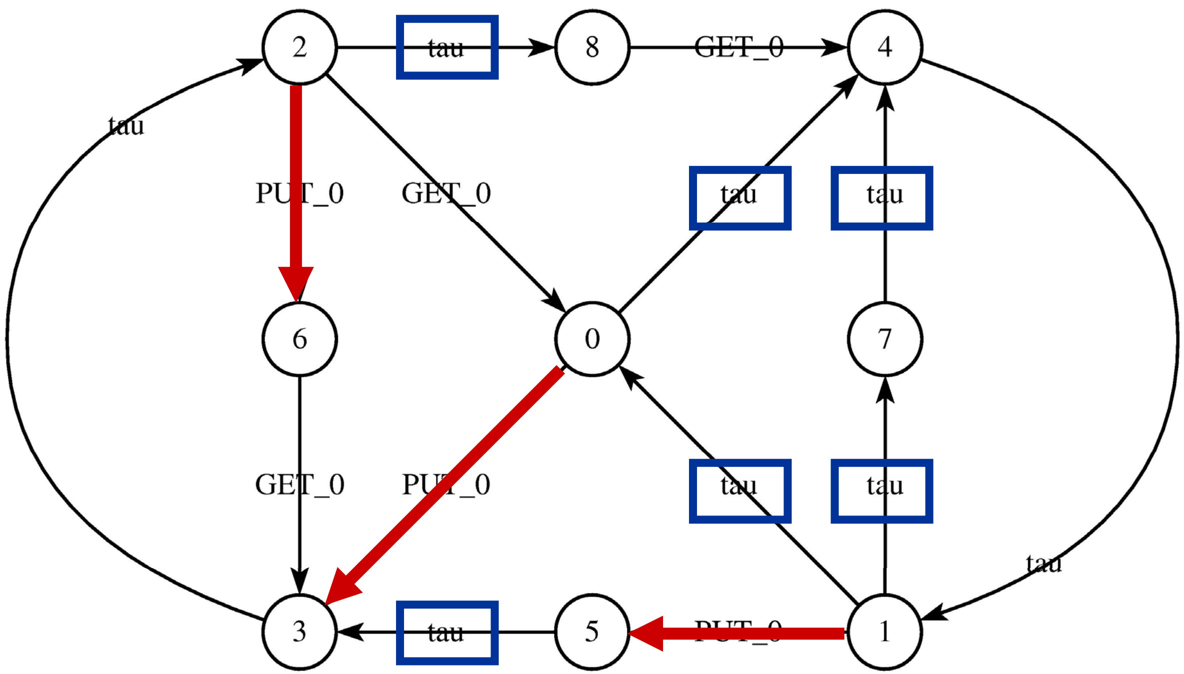
➔ *hiding all LTS actions belonging to $h_A(\varphi)$ does not change the interpretation of $\varphi$*

# Maximal hiding (2/2)

- Example:

  $\varphi$ = [ true* . PUT_0 ] $\mu X.(\neg \mathit{deadlock} \wedge$ [ $\neg$GET_0 ] $X)$

  $h_A(\varphi) = A -$ { PUT_0, GET_0 }



# Mu-calculus fragment compatible with ds-branching bisimulation

- Replace *strong* modalities by *weak* PDL-$\Delta$ modalities:

$$\varphi ::= \langle (\varphi_1? \,.\, \alpha_1)^* \rangle\, \psi$$

weak possibility

$(\tau \in [[\ \alpha_1\ ]])$

$$\quad |\ \langle \varphi_1? \,.\, \alpha_1 \rangle\, @$$

weak infinite looping

$$\psi ::= \varphi \mid \langle \alpha_2 \rangle\, \varphi \mid \neg\varphi \mid \varphi_1 \vee \varphi_2$$

strong possibility
$(\tau \notin [[\ \alpha_2\ ]])$

- Syntactic restriction:

*strong modalities must occur after a weak modality*

➔ *visible transitions matched by a strong modality will remain in the LTS after maximal hiding and ds-bb minimization*

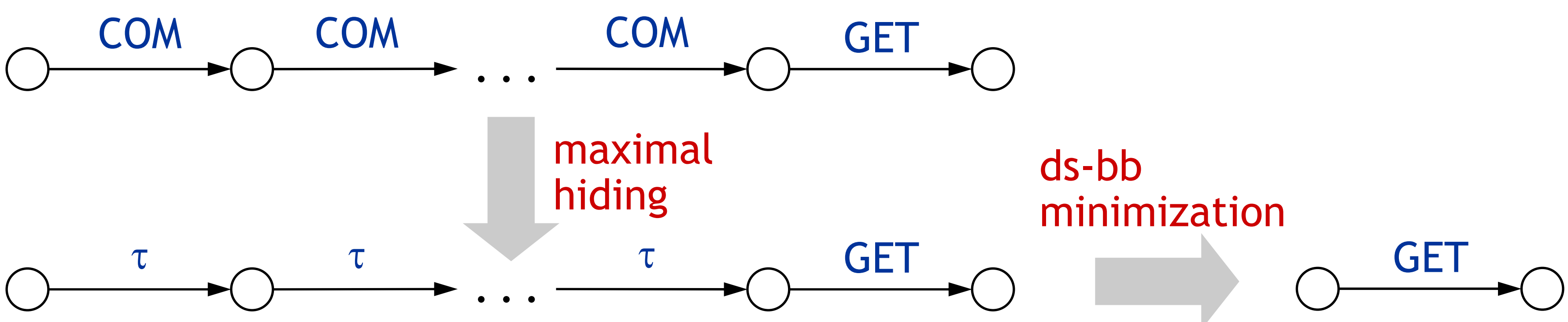
# Examples

- Deadlock (after expansion of '.' PDL operator):

$$\textit{deadlock} = [\ \underbrace{\text{true}^*}_{\text{weak necessity}}\ ]\ \underbrace{[\ \neg\tau\ ]\ \text{false}}_{\text{strong necessity}} \wedge \underbrace{[\ \tau\ ]\ \text{-|}}_{\text{weak saturation}}$$

- There is no reception before an emission:

$$[\ (\neg\text{PUT})^*\ ]\ [\ \text{GET}\ ]\ \text{false}$$

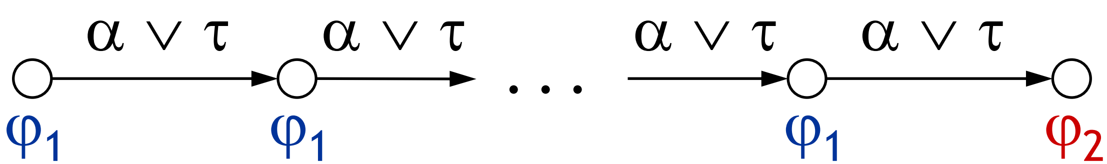


# Expressiveness of the ds-bb $\mu$-calculus fragment (1/3)

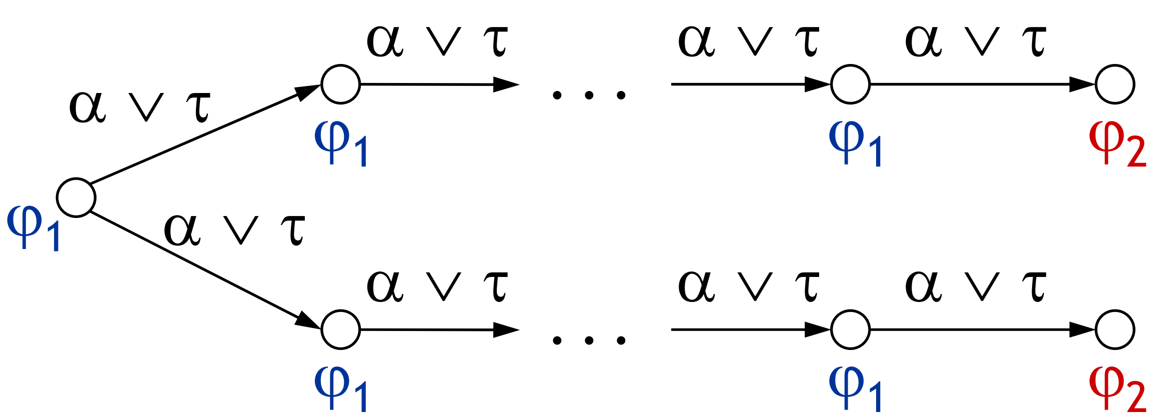
- Subsuming $\mu$ACTL-X [Fantechi-Gnesi-et-al-92]

$$E\,[\,\varphi_1\ U_\alpha\ \varphi_2\,] = \langle\,(\varphi_1?\,.\,(\alpha \vee \tau))^*\,\rangle\ \varphi_2$$

$\tau \notin [[\ \alpha\ ]]$



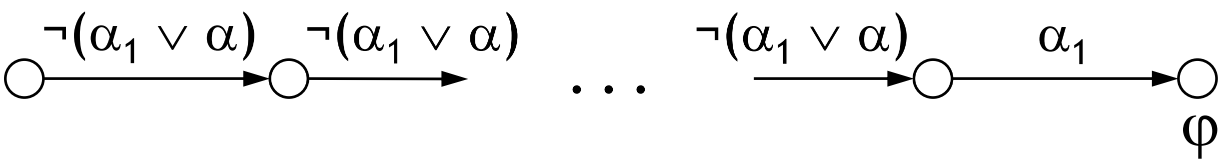

$$A\,[\,\varphi_1\ U_\alpha\ \varphi_2\,] = [\ (\neg\varphi_2?\,.\,(\alpha \vee \tau))^*\ ]\ (\varphi_2 \vee (\varphi_1 \wedge \neg \mathit{deadlock} \wedge [\ \neg(\alpha \vee \tau)\ ]\ \mathsf{false})) \wedge [\neg\varphi_2?\,.\,(\alpha \vee \tau)\ ] \dashv$$



# Expressiveness of the ds-bb $\mu$-calculus fragment (2/3)

- Subsuming selective $\mu$-calculus [Barbuti-et-al-98]

$$< \alpha_1 >_\alpha \varphi = < (\neg(\alpha_1 \vee \alpha))^* > < \alpha_1 > \varphi$$




$\tau \notin [[\ \alpha_1\ ]]$
$\tau \notin [[\ \alpha\ ]]$

- Enable to hide all actions but those occurring in $\alpha_1$ and $\alpha$, then to minimize modulo $\tau^*.a$ bisimulation
  - only weak safety/liveness properties
  - inevitability properties forbid any hiding:

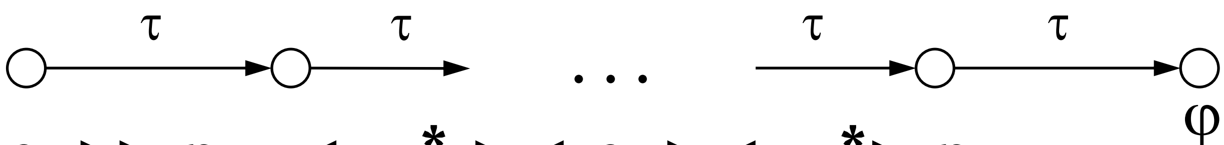
    $[\ \mathrm{PUT\_0}\ ]_{\mathrm{false}}\ \mu X.(\neg \mathit{deadlock} \wedge [\ \neg \mathrm{GET\_0}\ ]_{\mathrm{true}}\ X)$

    vs. hide all but PUT_0, GET_0 in ds-bb $\mu$-calculus

# Expressiveness of the ds-bb $\mu$-calculus fragment (3/3)

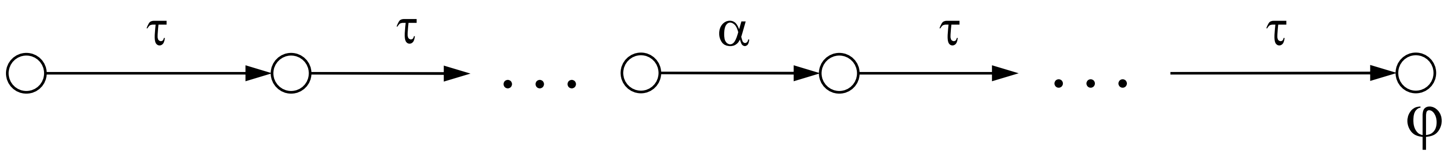
- Subsuming weak $\mu$-calculus [Stirling-et-al-01]

  $<<\ >>\ \varphi = <\tau^*>\ \varphi$



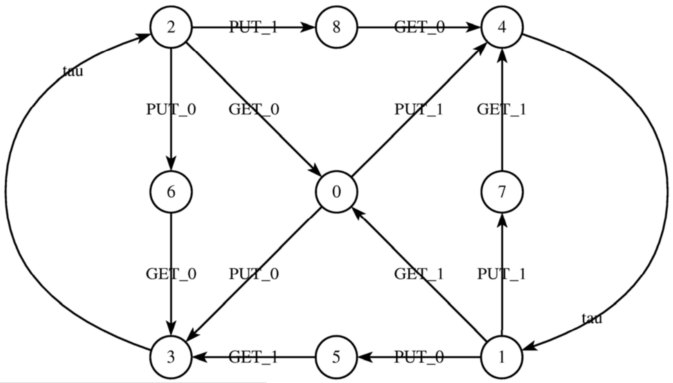

  $<<\alpha>>\ \varphi = <\tau^*>\ <\alpha>\ <\tau^*>\ \varphi$

  $\tau \notin [[\ \alpha\ ]]$




- Enable to hide all actions but those occurring in $\alpha$, then to minimize modulo weak bisimulation
  - only weak safety/liveness properties

# Property-dependent reduction
## (running example)



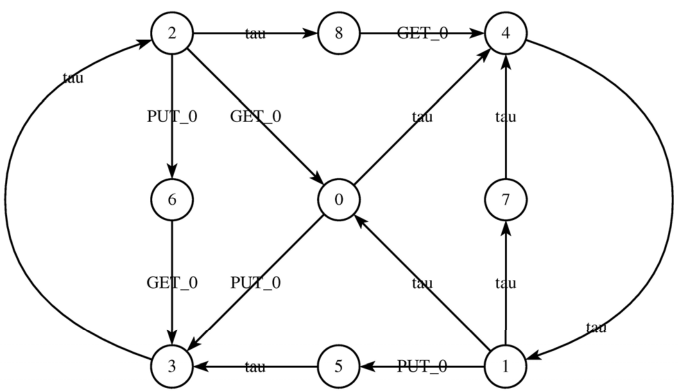

$\varphi$ = [ true* . PUT_0 ]

$\mu X.(\neg deadlock \wedge [\ \neg \text{GET\_0}\ ]\ X)$

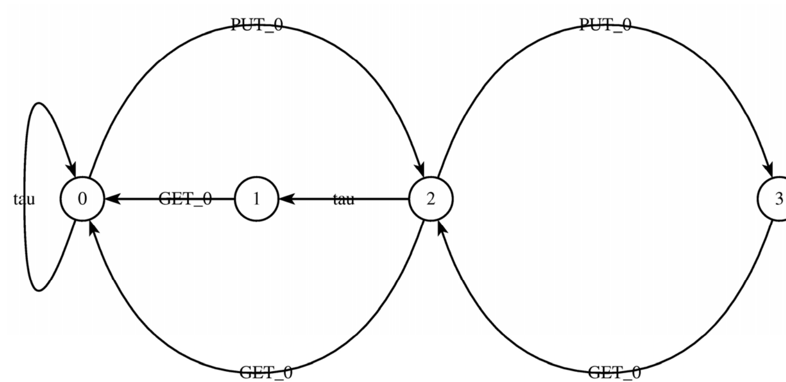
$h_A\ (\varphi) = A - \{$ PUT_0, GET_0 $\}$

9 states
14 transitions

maximal
hiding w.r.t. $h_A\ (\varphi)$

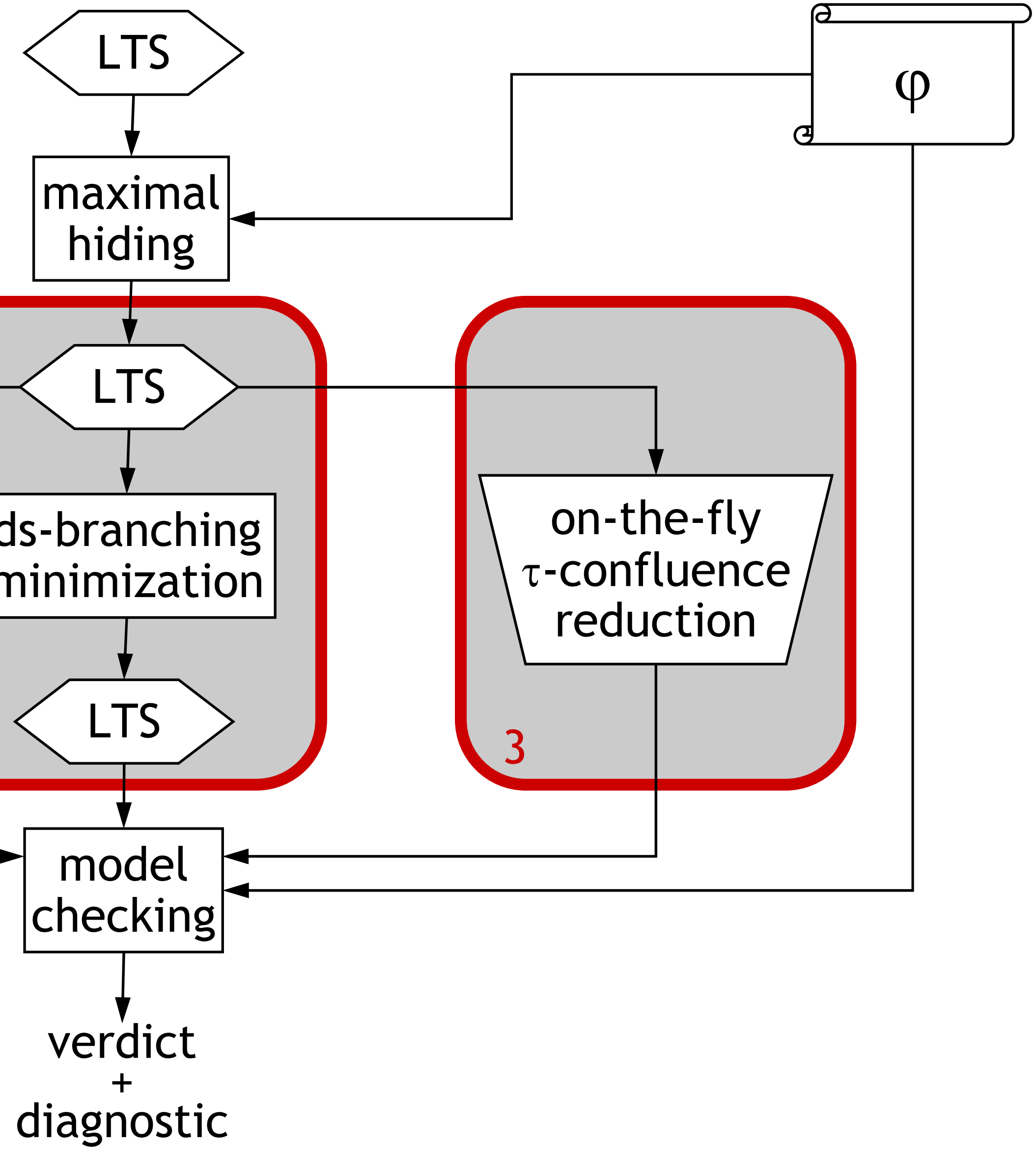



ds-bb
minimization



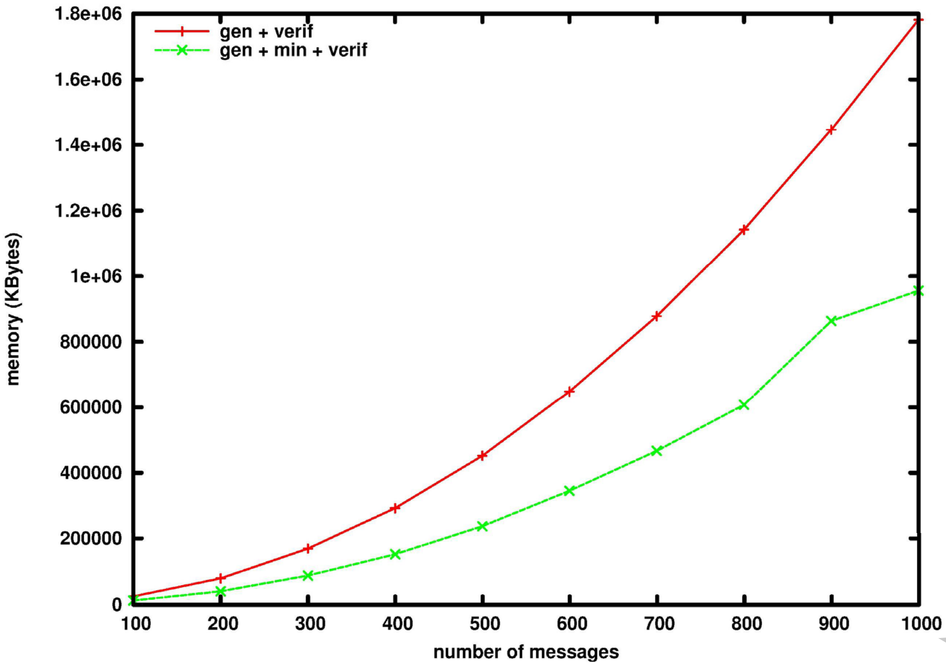

4 states, 7 transitions

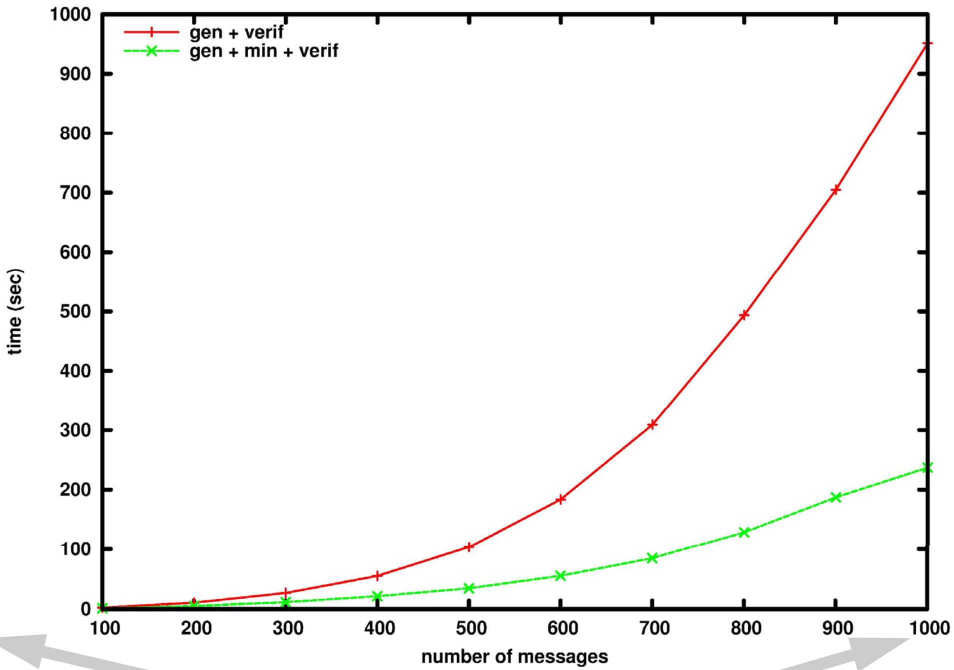
# Implementation and experiments




- **CADP** toolbox
  http://www.cadp.inria.fr
- **Bcg_Min** minimizer
- **Evaluator** model checker

# Strong bisimulation reduction
## (Alternating Bit Protocol)




12,196,201 states
46,639,612 transitions

Property checked:

[ true* ] (

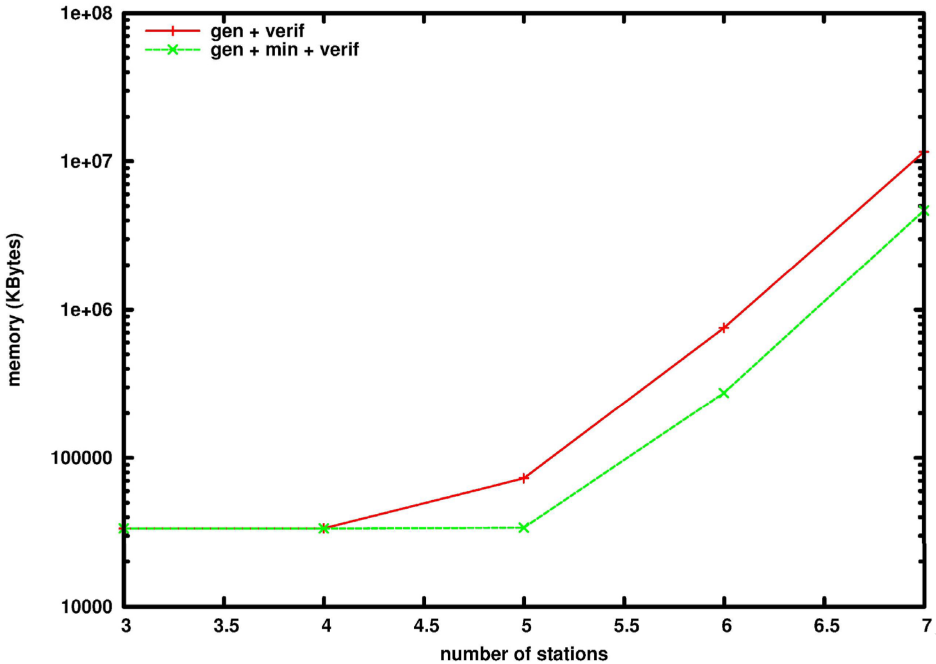
[ get ] (A [ $\text{true}_{\neg\text{put}}$ U < τ > @ ] ∧ [ (¬put)* . get ] false)

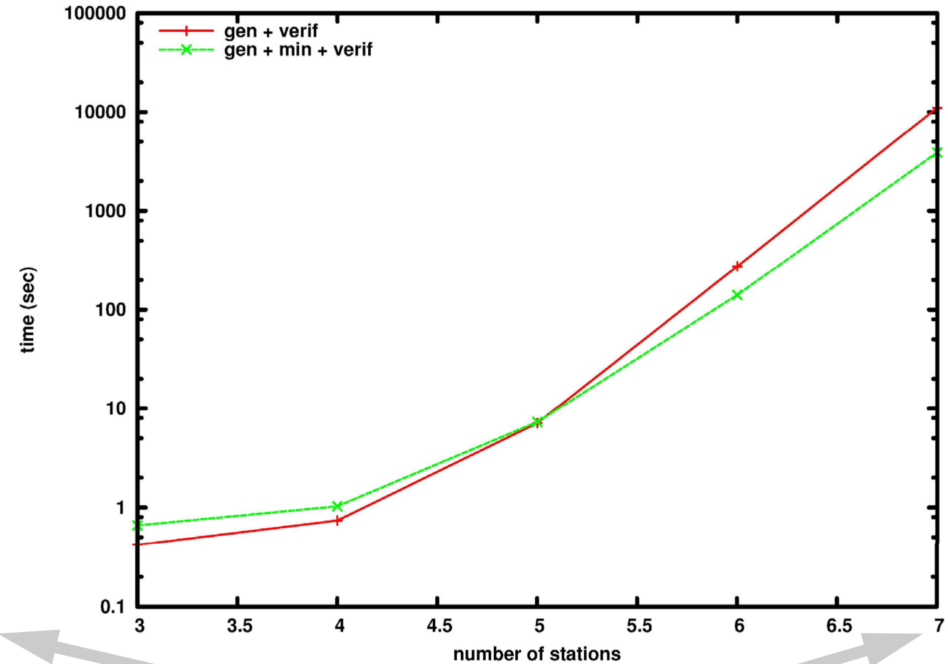
∧

[ put ] (A [ $\text{true}_{\neg\text{get}}$ U < τ > @ ] ∧ [ (¬get)* . put ] false)

)

# Strong bisimulation reduction
## (Token Ring Protocol)




53,848,492 states
214,528,176 transitions

Property checked:

$[\ \mathrm{true}^*\ ]\ ($

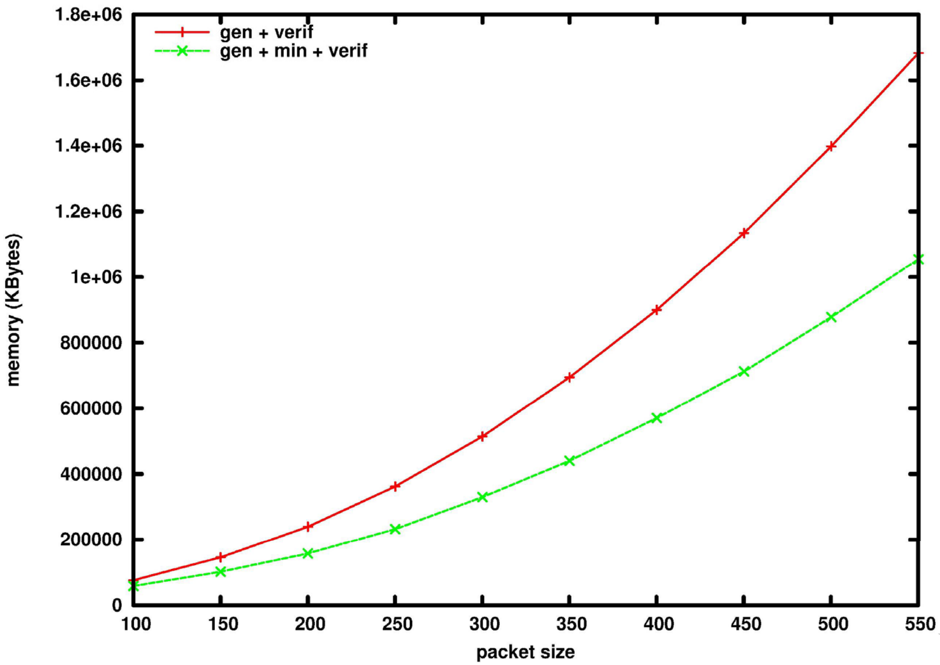
$\quad [\ \mathrm{open}_i\ .\ (\neg \mathrm{close}_i)^*\ .\ \mathrm{open}_j\ ]\ \mathrm{false}$

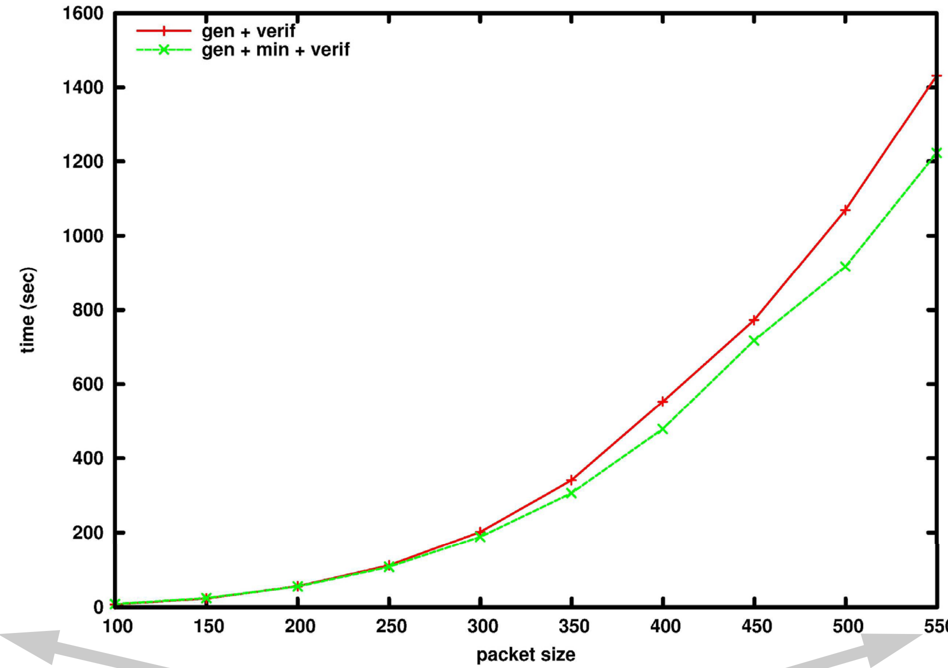
$\quad \wedge$

$\quad \mathrm{A}\ [\ \mathrm{true}_{\mathrm{true}}\ \mathrm{U} < (< \mathrm{true}^*\ .\ \mathrm{open}_i > \mathrm{true})?\ .\ \tau > @\ ]$

$)$

# ds-Branching bisimulation reduction
## (Bounded Retransmission Protocol)



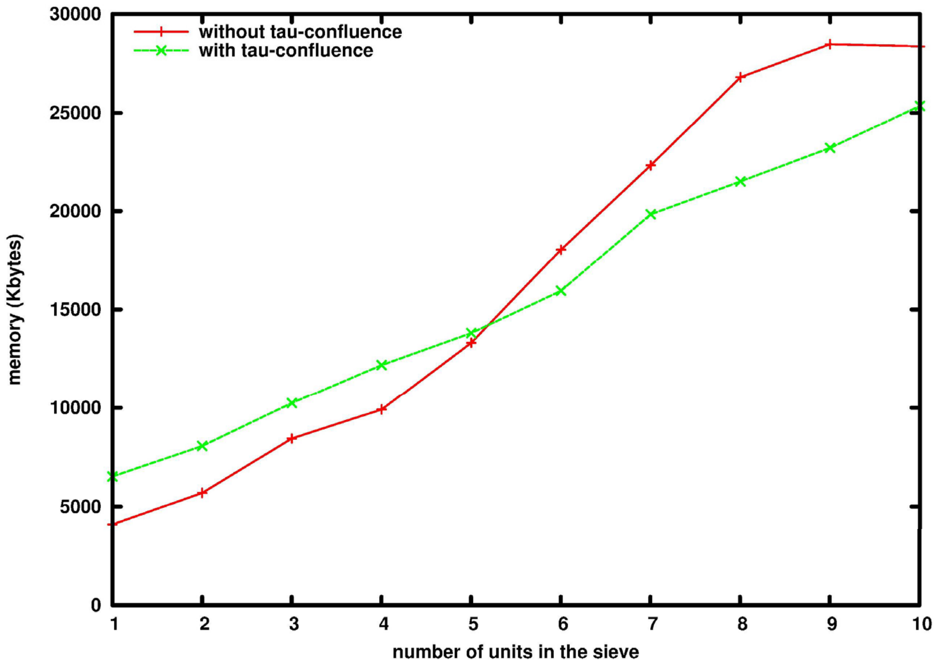

12,450,383 states
14,880,828 transitions

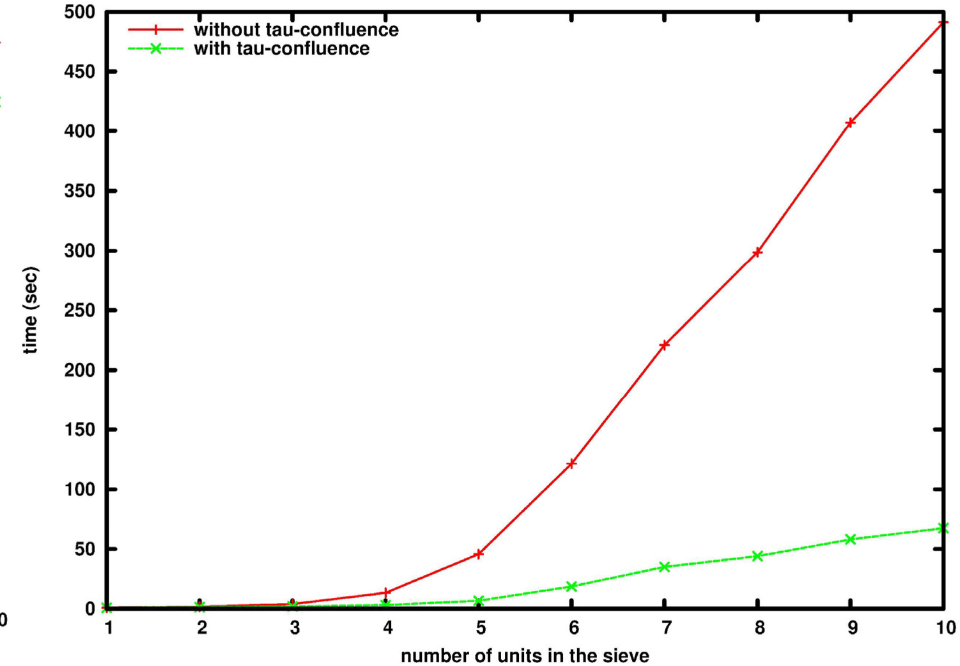
Property checked:

[ true* . in_data ]

A [ $\text{true}_{\neg \text{in\_data}}$ $\text{U}_{\text{in\_conf}}$ true ]

# On-the-fly τ-confluence reduction
## (Erathosthene's Sieve)




Property checked:

[ true* ] (

  [ $gen_p$ ] inev ($output_p$)

  $\wedge$

  [ $gen_q$ . true* . ¬$output_q$ ] false

)

inev (a) = [ (¬a)* ] ¬deadlock ∧ [ ¬a ] —|

# Conclusion and future work

- Summary:
  - Maximal hiding set derived from a $\mu$-calculus formula
    ➔ *non-intrusive approach*
  - Definition of an expressive $\mu$-calculus fragment compatible with ds-branching bisimulation
  - Reductions modulo strong and ds-branching bisimulation (global) and modulo divergence-sensitive $\tau$-confluence (on-the-fly)
- Future work:
  - Investigate the translations of property patterns [Dwyer-et-al-99] into the ds-bb $\mu$-calculus fragment
  - Experiment with on-the-fly reductions modulo *weak* divergence-sensitive $\tau$-confluence