# Project and Conquer

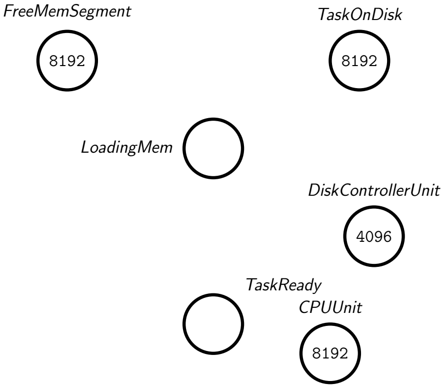
## Fast Quantifier Elimination for Checking Petri Net Reachability

**Nicolas Amat**, Silvano Dal Zilio, Didier Le Botlan

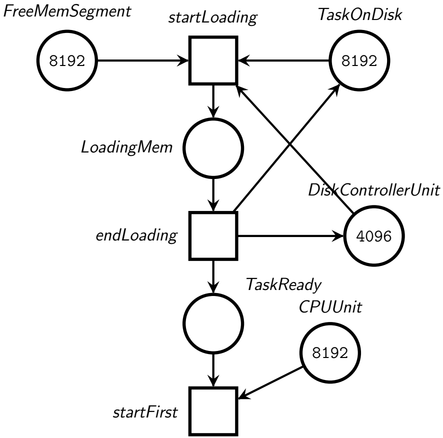
LAAS CNRS

# The SmallOperatingSystem example

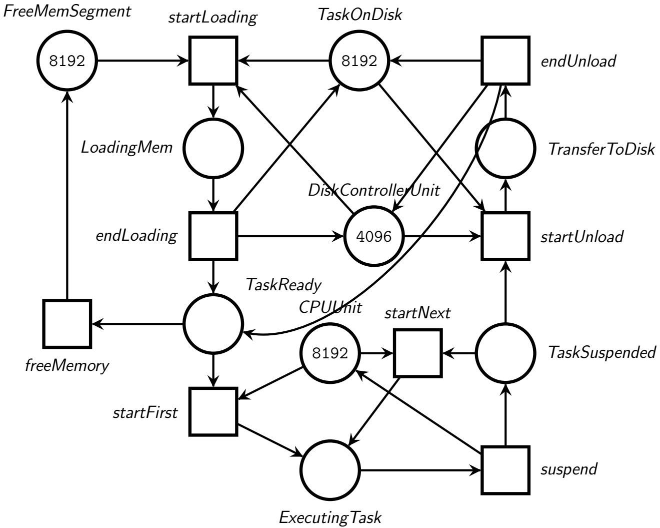
# The SmallOperatingSystem example



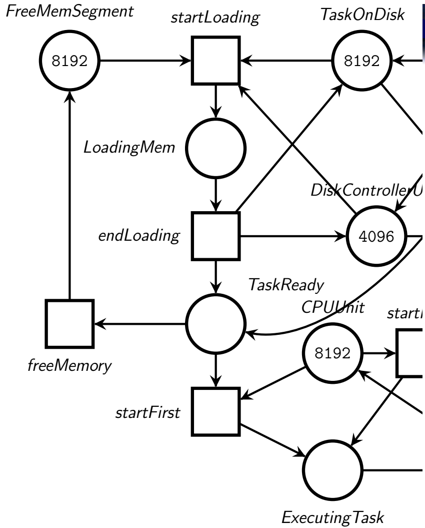
# The SmallOperatingSystem example



# The SmallOperatingSystem example



# The SmallOperatingSystem example







Fabrice Kordon
Fabrice.Kordon@lip6.fr


*This form is a summary description of the model entitled "SmallOperatingSystem" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.*

### Description

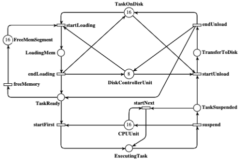
This Petri net models a simplified Operating System handling the execution of tasks on a machine with several so-called "memory segments", Disk controller units, and cores. The typical lifecycle of a task is the following:

1 A ask is loaded from disk to memory (requires a segment and a disk controller),

2 When the task is ready to execute, it can get a core, be suspended and get a core again as long as its execution is not finished. It can also be removed from the memory if some is needed otherwise

3 When the execution finishes, the task is saved back on the disk.

The system has several scaling parameters: $M$ (memory segments), $T$ (tasks), $D$ (Disk controllers) and $C$ (cores). However, to simplify this in the MCC, we reduce it to two parameters, $MT$ and $DC$ with the following correspondence: $M = T = MT$, $D = DC$ and $C = 2 \times DC$.

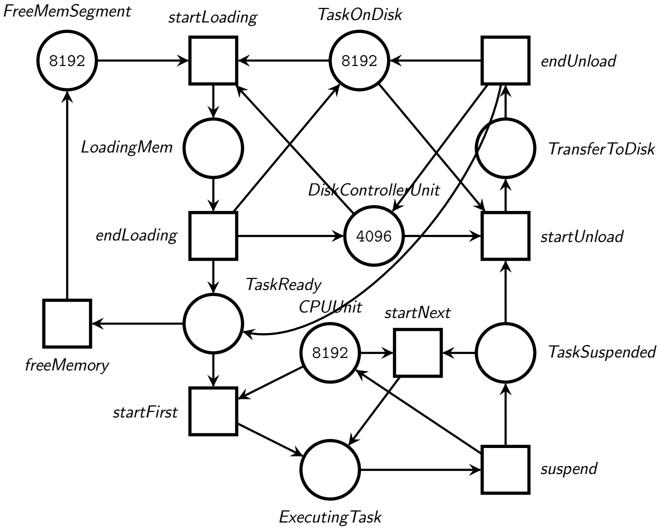



*Graphical representation for $MT16$ and $DC = 8$*

### Scaling parameter

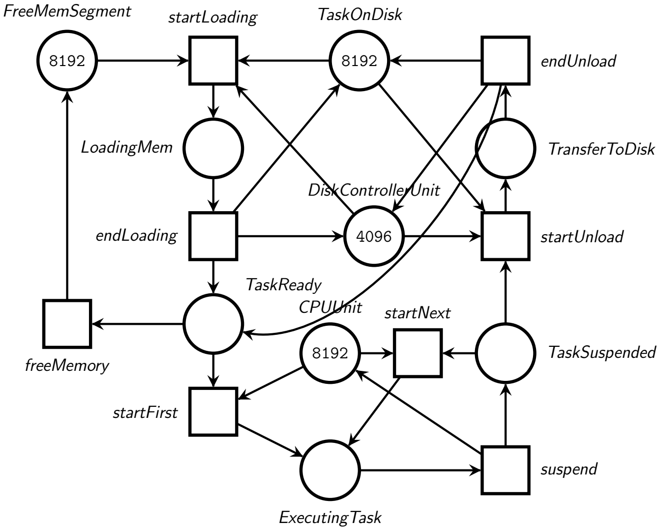
| Parameter name | Parameter description | Chosen parameter values |
|---|---|---|
| $MT$ and $DC$ | $MT$ to compute available tasks and memory and $DC$ to compute available disk controllers and cores | (MT=16, DC=8), (MT=32, DC=8), (MT=32, DC=16), (MT=64, DC=16), (MT=64, DC=32), (MT=128, DC=32), (MT=128, DC=64), (MT=256, DC=64), (MT=256, DC=128), (MT=512, DC=128), (MT=512, DC=256), (MT=1024, DC=256), (MT=1024, DC=512), (MT=2048, DC=512), (MT=2048, DC=1024), (MT=4096, DC=1024), (MT=4096, DC=2048), (MT=8192, DC=2048), (MT=8192, DC=4096) |

# The SmallOperatingSystem example




Is "*ExecutingTask* > *TaskOnDisk*" reachable from the initial marking?

# The SmallOperatingSystem example




State space $\approx 10^{17}$

# Reachability properties verification

- $F$ **reachable** if and only if $\exists m \in R(N, m_0)$ such that $m \models F$

# Reachability properties verification

- $F$ **reachable** if and only if $\exists m \in R(N, m_0)$ such that $m \models F$
- $F$ **invariant** if and only if $\forall m \in R(N, m_0)$ we have $m \models F$

# Some properties of interest

- **Coverability**: $\mathrm{COVER}(p, k) \;\equiv\; m(p) \geq k$
- **Reachability**: $\mathrm{REACH}(p, k) \;\equiv\; m(p) = k$
- **Quasi-liveness**: $\mathrm{QLIVE}(t) \;\equiv\; \bigwedge_{p \in {}^\bullet t} \mathrm{COVER}(p, \mathbf{pre}(t, p))$
- **Deadlock**: $\mathrm{DEAD} \;\equiv\; \bigwedge\limits_{t \in T} \neg \mathrm{QLIVE}(t)$

# Petri nets semantics

Same formalism for semantics and properties

Some transition $t$ enabled at $m$ when $m \models \mathrm{ENBL}_t(\boldsymbol{p})$:

$$\mathrm{ENBL}_t(\boldsymbol{p}) \triangleq \bigwedge_{i \in 1..n} (p_i \geqslant \mathrm{Pre}(t, p_i))$$

We have $m \to m'$ if and only if $m, m' \models \mathrm{T}(\boldsymbol{p}, \boldsymbol{p'})$:

$$\mathrm{T}(\boldsymbol{p}, \boldsymbol{p'}) \;\triangleq\; \bigvee\nolimits_{t \in T} \mathrm{ENBL}_t(\boldsymbol{p}) \wedge \Delta_t(\boldsymbol{p}, \boldsymbol{p'})$$

where the token displacement is defined as:

$$\Delta_t(\boldsymbol{p}, \boldsymbol{p'}) \;\triangleq\; \bigwedge\nolimits_{i \in 1..n} (p'_i = p_i + \mathrm{Post}(t)(p_i) - \mathrm{Pre}(t)(p_i))$$

# Outline

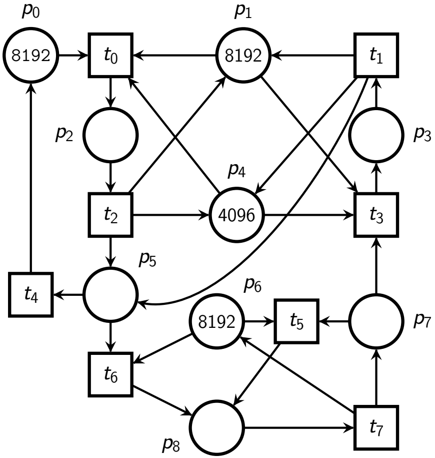
1. Polyhedral reduction
2. Token Flow Graphs
3. Quantifier elimination
4. Experimental evaluation

# Outline

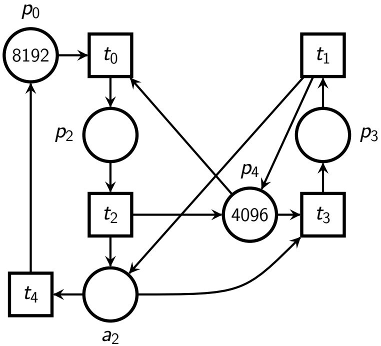
1. Polyhedral reduction
2. Token Flow Graphs
3. Quantifier elimination
4. Experimental evaluation

# SmallOperatingSystem

## Polyhedral Reduction




$\equiv_E$




$$E \triangleq \exists a_1. \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_6 \end{cases}$$

**Marking equivalence:** denote $m_1 \equiv_E m_2$ when: $E \wedge \underline{m_1} \wedge \underline{m_2}$ is satisfiable

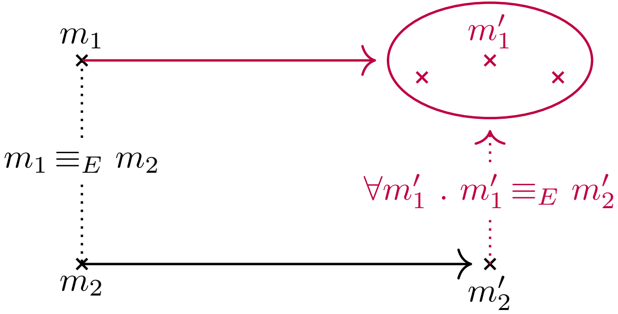
# Key results: reachability checking

## Polyhedral Reduction

**Lemma (Reachability checking)**

*For all pairs of markings $m'_1, m'_2$ of $N_1, N_2$ such that $m'_1 \equiv_E m'_2$:*

$$\textit{if } m'_2 \in R(N_2, m_2) \textit{ then } m'_1 \in R(N_1, m_1).$$

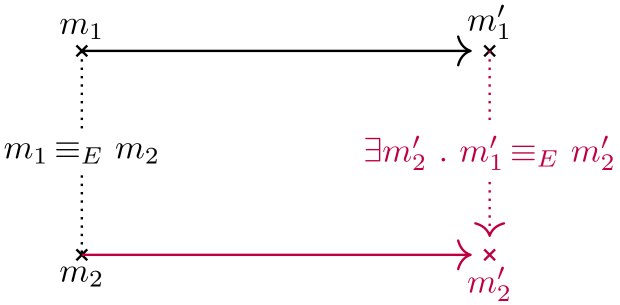


# Key results: invariance checking

## Polyhedral reduction

**Lemma (Invariance checking)**

*For all $m_1'$ in $R(N_1, m_1)$ there is $m_2'$ in $R(N_2, m_2)$ such that $m_1' \equiv_E m_2'$.*



# Polyhedral equivalence

## Polyhedral reduction

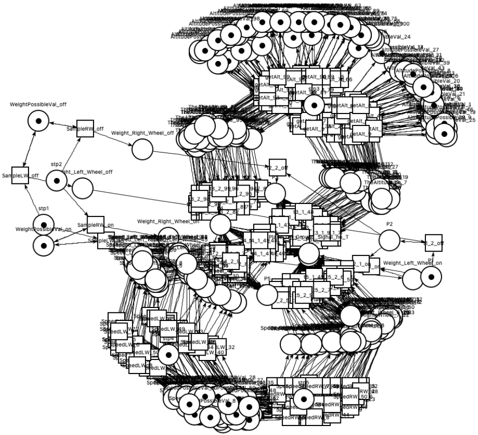
**Definition (Relaxed $E$-equivalence)**

$(N_1, m_1) \equiv_E (N_2, m_2)$ if and only if

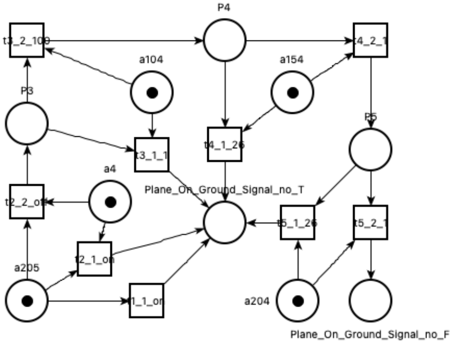
- **(A1)** initial markings are *realated up-to $E$*: $m_1 \equiv_E m_2$;
- **(A2a)** for all markings $m$ in $R(N_1, m_1)$ or $R(N_2, m_2)$: $E \wedge \underline{m}$ is satisfiable;
- **(A2b)** assume $m'_1, m'_2$ are markings of $N_1, N_2$ related up-to $E$, such that $m'_1 \equiv_E m'_2$, then $m'_1$ is reachable iff $m'_2$ is reachable.

# AirplaneLD-PT-0050

## Polyhedral reduction

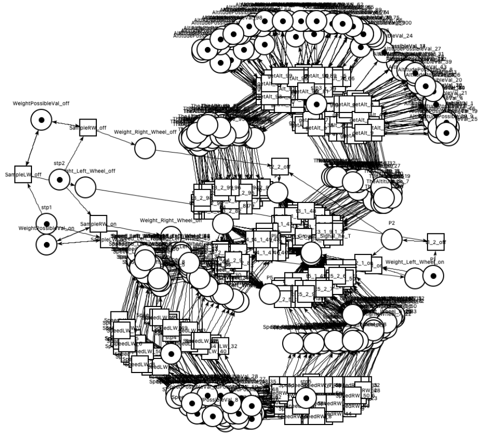



$\equiv_E$

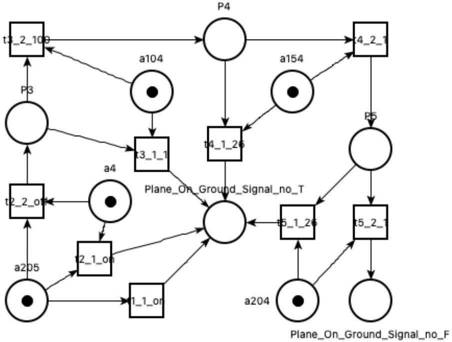


# AirplaneLD-PT-0050

## Polyhedral reduction



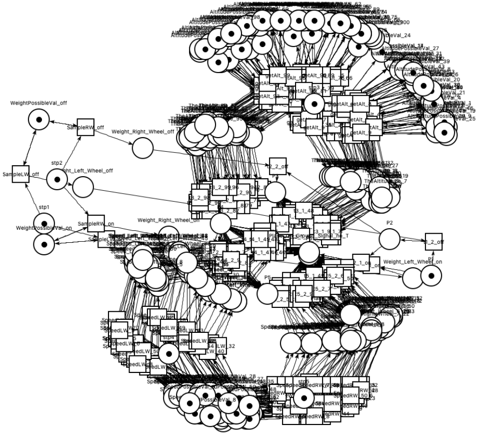

$\equiv_E$



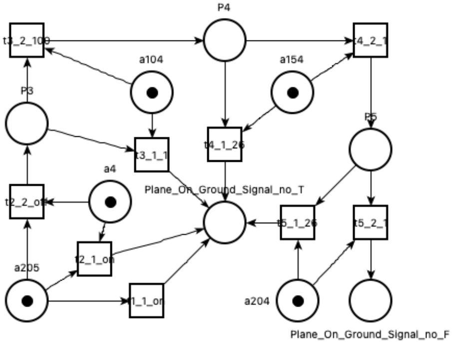

*E* contains about 400 variables and literals

# AirplaneLD-PT-0050

## Polyhedral reduction



$\equiv_E$




AirplaneLD-PT-**4000**: 30 000 variables and literals

# Combination with reachability

Polyhedral reduction

- Is $F_1$ reachable in $(N_1, m_1)$?

$$F_1 \triangleq \begin{cases} 3p_7 + 2p_8 & \geqslant p_6 \\ p_8 & \geqslant p_1 \end{cases}$$

# Combination with reachability

## Polyhedral reduction

- Is $F_1$ reachable in $(N_1, m_1)$?

$$F_1 \triangleq \begin{cases} 3p_7 + 2p_8 & \geqslant p_6 \\ p_8 & \geqslant p_1 \end{cases}$$

**Definition ($E$-Transform Formula)**

Formula $F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{p_1}.\, \tilde{E}(\boldsymbol{p_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{p_1})$ is the $E$-transform of $F_1$.

# Combination with reachability

## Polyhedral reduction

- Is $F_1$ reachable in $(N_1, m_1)$?

$$F_1 \triangleq \begin{cases} 3p_7 + 2p_8 & \geqslant p_6 \\ p_8 & \geqslant p_1 \end{cases}$$

**Definition ($E$-Transform Formula)**

Formula $F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{q_1}.\, \tilde{E}(\boldsymbol{q_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{q_1})$ is the $E$-transform of $F_1$.

$$F_2 \triangleq \exists q_0, .., q_8.\, \exists a_1. \begin{cases} q_1 = q_4 + 4096 \\ q_6 = q_0 + q_2 + q_3 + q_5 + q_7 \\ a_1 = q_7 + q_8 \\ a_2 = a_1 + q_6 \end{cases} \wedge \begin{cases} p_0 = q_0 \\ p_2 = q_2 \\ p_3 = q_3 \\ p_4 = q_4 \end{cases} \wedge \begin{cases} 3q_7 + 2q_8 & \geqslant q_6 \\ q_8 & \geqslant q_1 \end{cases}$$

# Combination with reachability

Polyhedral reduction

- Is $F_1$ reachable in $(N_1, m_1)$? $\qquad F_1 \triangleq \begin{cases} 3p_7 + 2p_8 & \geqslant p_6 \\ p_8 & \geqslant p_1 \end{cases}$

**Definition ($E$-Transform Formula)**

Formula $F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{q_1}.\, \tilde{E}(\boldsymbol{q_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{q_1})$ is the $E$-transform of $F_1$.

$$F_2 \triangleq \exists q_0, .., q_8.\, \exists a_1. \begin{cases} q_1 = q_4 + 4096 \\ q_6 = q_0 + q_2 + q_3 + q_5 + q_7 \\ a_1 = q_7 + q_8 \\ a_2 = a_1 + q_6 \end{cases} \wedge \begin{cases} p_0 = q_0 \\ p_2 = q_2 \\ p_3 = q_3 \\ p_4 = q_4 \end{cases} \wedge \begin{cases} 3q_7 + 2q_8 & \geqslant q_6 \\ q_8 & \geqslant q_1 \end{cases}$$

- Is the $E$-transform formula $F_2$ reachable in $(N_2, m_2)$?

# Fundamental results on $E$-transform formulas

## Polyhedral reduction

**Definition ($E$-Transform Formula)**

$F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{p_1}.\, \tilde{E}(\boldsymbol{p_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{p_1})$ is the $E$-transform of $F_1$

**Theorem (Reachability Conservation)**

*$F_1$ reachable in $N_1$ if and only if $F_2$ reachable in $N_2$*

# Fundamental results on $E$-transform formulas

## Polyhedral reduction

**Definition ($E$-Transform Formula)**

$F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{p_1}.\, \tilde{E}(\boldsymbol{p_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{p_1})$ is the $E$-transform of $F_1$

**Theorem (Reachability Conservation)**

*$F_1$ reachable in $N_1$ if and only if $F_2$ reachable in $N_2$*

- **Not suitable with random exploration**
  (need to evaluate a quantified formula for each visited state)
- **Not usable with standard model-checkers**
  (only support quantifier-free formulas on the set of places)

# Fundamental results on $E$-transform formulas

## Polyhedral reduction

**Definition ($E$-Transform Formula)**

$F_2(\boldsymbol{p_2}) \triangleq \exists \boldsymbol{p_1} . \tilde{E}(\boldsymbol{p_1}, \boldsymbol{p_2}) \wedge F_1(\boldsymbol{p_1})$ is the $E$-transform of $F_1$

**Theorem (Reachability Conservation)**

*$F_1$ reachable in $N_1$ if and only if $F_2$ reachable in $N_2$*

- **Not suitable with random exploration**
  (need to evaluate a quantified formula for each visited state)
- **Not usable with standard model-checkers**
  (only support quantifier-free formulas on the set of places)

We introduce a procedure to eliminate quantifiers in $F_2$ (EXPSPACE in general)

# Why not use standard elimination methods?

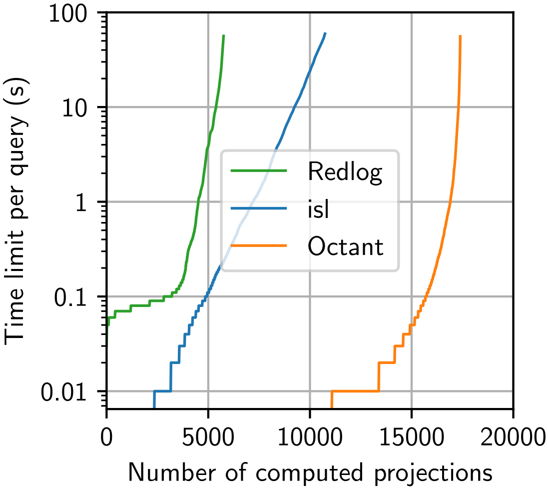
## Polyhedral reduction

Often requires the use of a divisibility operator (stride format)
⚠ Not part of the logic fragment that we target!

Formulas involves several hundreds and sometimes thousands of variables
⚠ Do not scale!

# Performance of fast elimination

## Polyhedral reduction



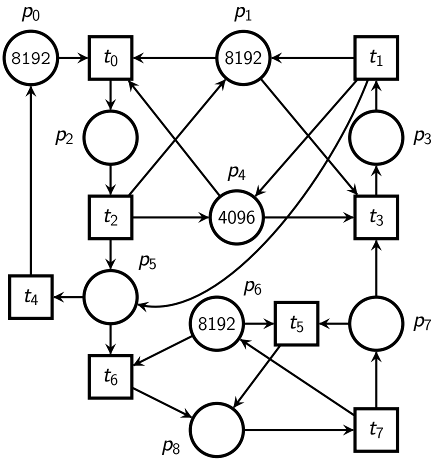

| | |
|---|---|
| Octant: | 99.5% |
| isl: | 61% |
| Redlog: | 33% |

# Outline

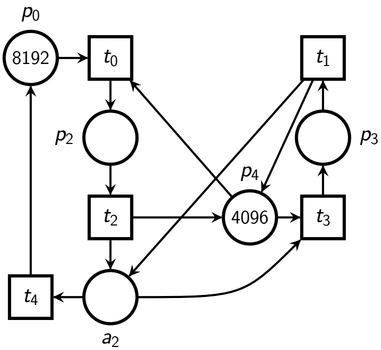
1. Polyhedral reduction
2. Token Flow Graphs
3. Quantifier elimination
4. Experimental evaluation

# SmallOperatingSystem

## Token Flow Graphs




$\equiv_E$




$$E \triangleq \exists a_1. \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$

# Motivation

## Token Flow Graphs

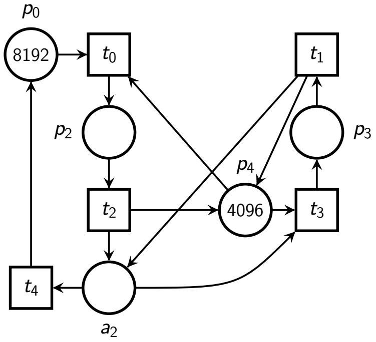
- Reason on **graphs** instead of solving **Presburger formulas**
- Capture the **particular structure** of constraints from polyhedral reductions
- Directed Acyclic Graph (**DAG**) with two kinds of arcs

$$E \triangleq \exists a_1.\ \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$

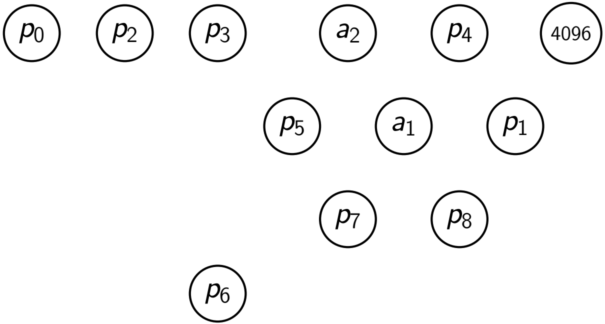
# Construction

## Token Flow Graphs

$$\exists a_1. \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$



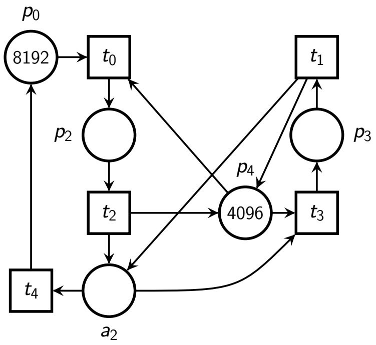

$(N_2, m_2)$



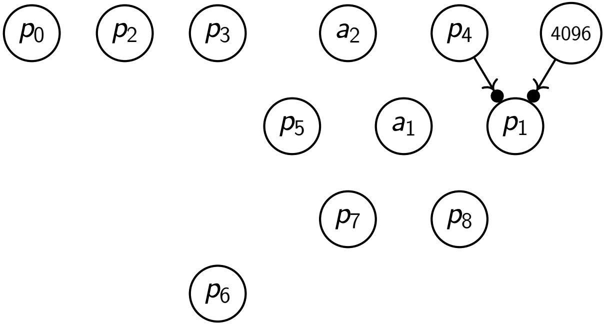
# Construction

## Token Flow Graphs

$$\exists a_1.\ \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$



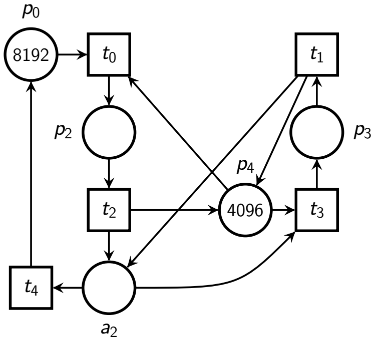

$(N_2, m_2)$



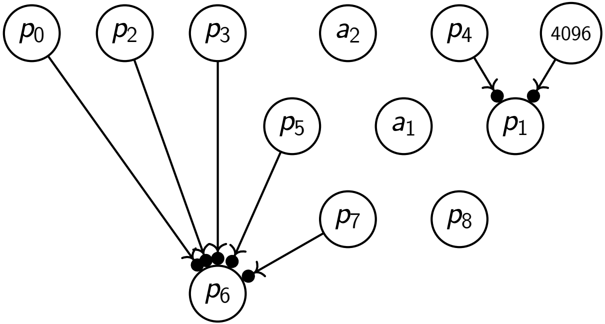
# Construction

## Token Flow Graphs

$$\exists a_1 . \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$



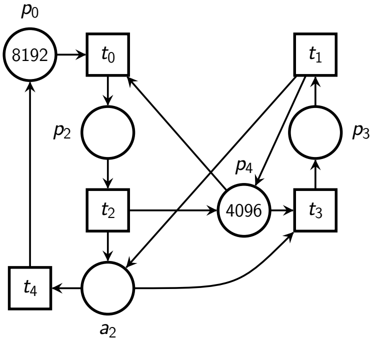

$(N_2, m_2)$



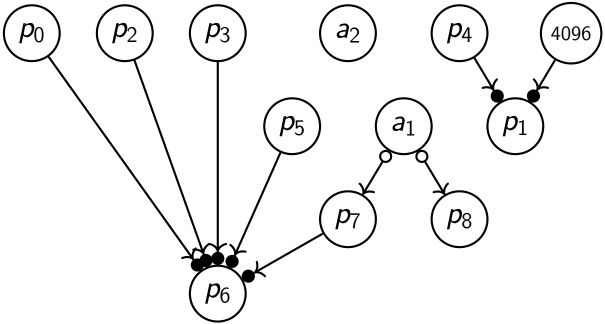
# Construction

## Token Flow Graphs

$$\exists a_1.\ \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$



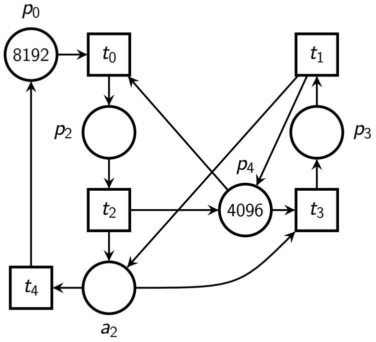

$(N_2, m_2)$



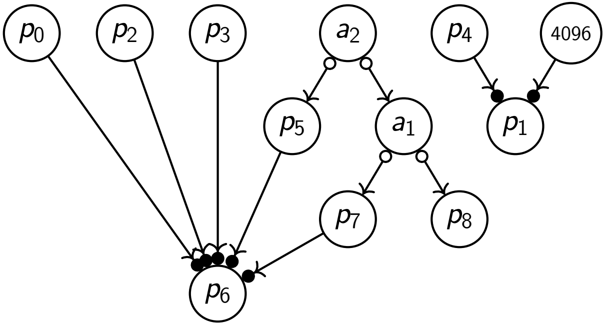
# Construction

## Token Flow Graphs

$$\exists a_1 . \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$



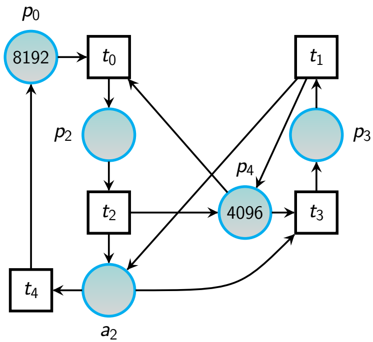

$(N_2, m_2)$



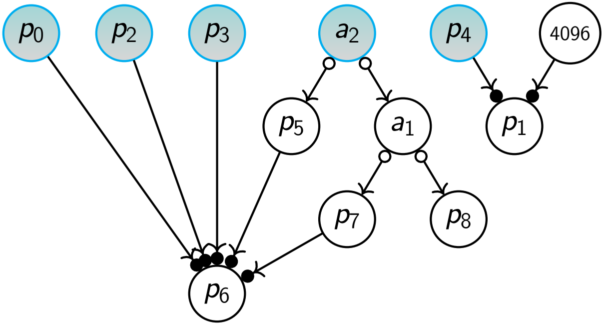
# Construction

## Token Flow Graphs

$$\exists a_1 . \begin{cases} p_1 = p_4 + 4096 \\ p_6 = p_0 + p_2 + p_3 + p_5 + p_7 \\ a_1 = p_7 + p_8 \\ a_2 = a_1 + p_5 \end{cases}$$




$(N_2, m_2)$

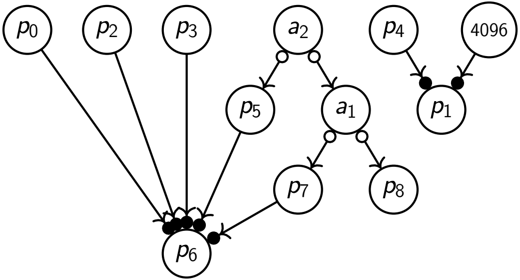


# Outline

1. Polyhedral reduction
2. Token Flow Graphs
3. Quantifier elimination
4. Experimental evaluation

# Running example

## Quantifier elimination




$$F_1 \triangleq (3p_7 + 2p_8 \geqslant p_6) \wedge (p_8 \geqslant p_1)$$

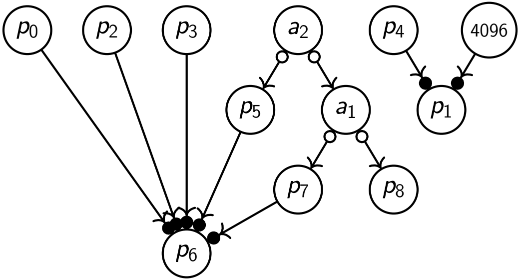
**Definition**

$F_1 \equiv_E F_2$, with $\mathrm{FV}(F_i) \subseteq P_i$ for all $i \in 1..2$ iff

$F_1$ is **reachable** in $N_1$ if and only if $F_2$ is **reachable** in $N_2$

# Running example

## Quantifier elimination

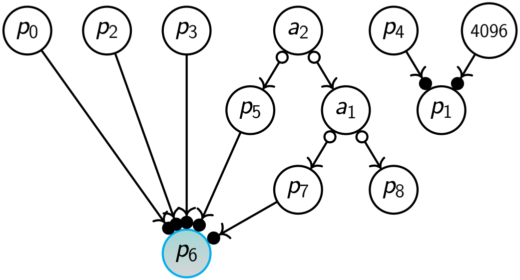



$$
\begin{array}{ccccccc}
3\,p_7 & + & 2\,p_8 & - & p_6 & \geqslant 0 \\
 & & p_8 & - & p_1 & \geqslant 0
\end{array}
$$

$$\Updownarrow$$

# Running example

## Quantifier elimination

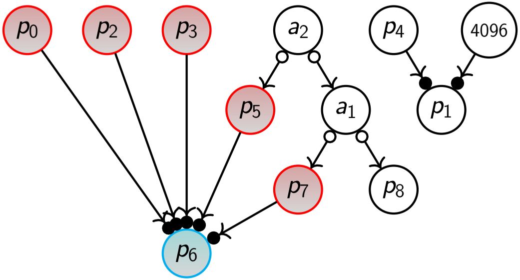



$$\begin{array}{rcrcrl} 3\,p_7 & + & 2\,p_8 & - & \color{blue}{p_6} & \geqslant 0 \\ & & p_8 & - & p_1 & \geqslant 0 \end{array}$$

$$\Updownarrow$$

# Running example

## Quantifier elimination



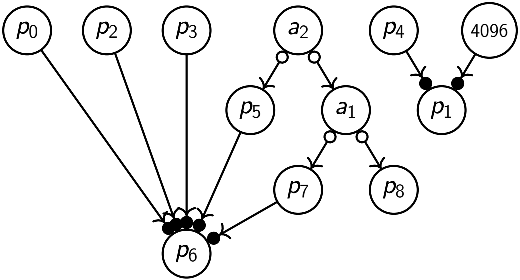

$$\begin{array}{rcrcrl} 3\,p_7 & + & 2\,p_8 & - & \color{blue}{p_6} & \geqslant 0 \\ & & p_8 & - & p_1 & \geqslant 0 \end{array}$$

$$\Updownarrow$$

$$\begin{array}{rcrcrl} 3\,p_7 & + & 2\,p_8 & - & \color{red}{(p_0 + p_2 + p_3 + p_5 + p_7)} & \geqslant 0 \\ & & p_8 & - & p_1 & \geqslant 0 \end{array}$$

# Running example

## Quantifier elimination



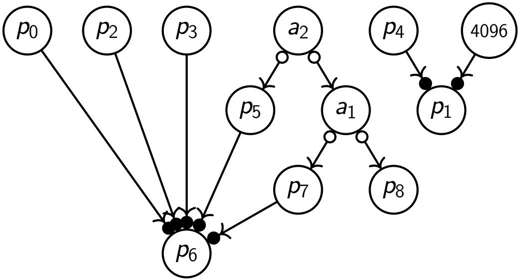

$$\begin{array}{ccccccc} 3\,p_7 & + & 2\,p_8 & - & p_6 & \geqslant 0 \\ p_8 & - & p_1 & & & \geqslant 0 \end{array}$$

$$\Updownarrow$$

$$\begin{array}{cccccccccccccc} 2\,p_7 & + & 2\,p_8 & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\ & & & & & & & & p_8 & - & p_1 & \geqslant 0 \end{array}$$

# Running example

## Quantifier elimination

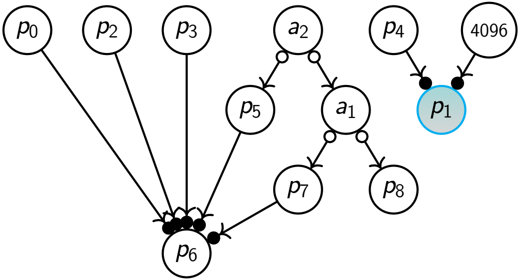



$$
\begin{array}{rcrcrcrcrcrcrl}
2\,p_7 & + & 2\,p_8 & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\
 & & & & & & & & p_8 & - & p_1 & \geqslant 0
\end{array}
$$

$$\Updownarrow$$

# Running example

## Quantifier elimination

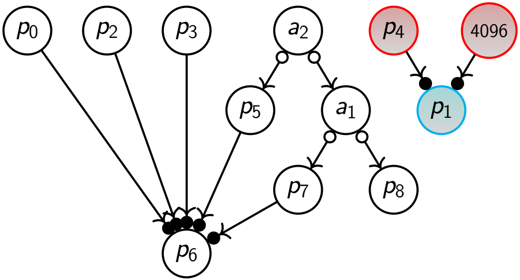



$$\begin{array}{rcl} 2\,p_7 + 2\,p_8 - p_0 - p_2 - p_3 - p_5 & \geqslant & 0 \\ p_8 - {\color{blue}p_1} & \geqslant & 0 \end{array}$$

$$\Updownarrow$$

# Running example

## Quantifier elimination



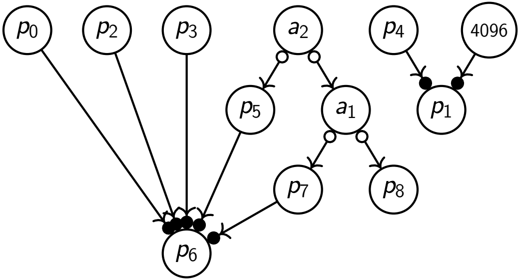

$$\begin{array}{rcrcrcrcrcr}
2\,p_7 + 2\,p_8 - p_0 - p_2 - p_3 - p_5 & \geqslant 0 \\
p_8 - {\color{blue}p_1} & \geqslant 0
\end{array}$$

$$\Updownarrow$$

$$\begin{array}{rl}
2\,p_7 + 2\,p_8 - p_0 - p_2 - p_3 - p_5 & \geqslant 0 \\
p_8 - {\color{red}(p_4 + 4096)} & \geqslant 0
\end{array}$$

# Running example

## Quantifier elimination



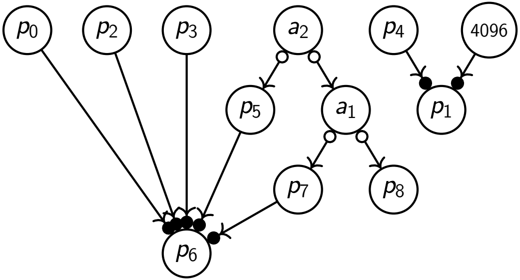

$$\begin{array}{lllllllllll} 2\,p_7 & + & 2\,p_8 & - & p_0 & - & p_3 & - & p_5 & \geqslant 0 \\ 1\,p_8 & - & p_1 & & & & & & & \geqslant 0 \end{array}$$

$$\Updownarrow$$

$$\begin{array}{llllllllllll} 2\,p_7 & + & 2\,p_8 & - & p_0 & - & p_2 & & p_3 & - & p_5 & \geqslant 0 \\ & & & & & & p_8 & - & p_4 & - & 4096 & \geqslant 0 \end{array}$$

# Running example

## Quantifier elimination

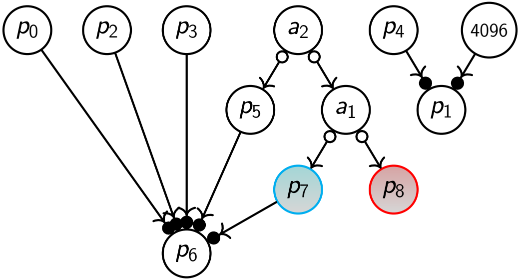



$$
\begin{array}{lllllllllllll}
2\,p_7 & + & 2\,p_8 & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\
0\,p_7 & + & 1\,p_8 & - & p_4 & - & 4096 & & & & & \geqslant 0
\end{array}
$$

$$\Updownarrow$$

# Running example

## Quantifier elimination



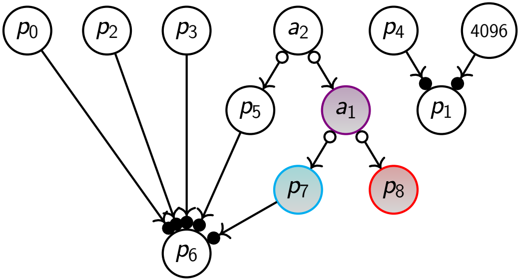

$$\begin{array}{cccccccccccccc}
{\color{blue}2\,p_7} & + & {\color{red}2\,p_8} & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\
{\color{blue}0\,p_7} & + & {\color{red}1\,p_8} & - & p_4 & - & 4096 & & & & & \geqslant 0
\end{array}$$

$$\Updownarrow$$

polarized: $p_8$ variable with the highest coefficient in both literals

# Running example

## Quantifier elimination




$$
\begin{array}{lllllllllllll}
{\color{blue}2\,p_7} & + & {\color{red}2\,p_8} & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\
{\color{blue}0\,p_7} & + & {\color{red}1\,p_8} & - & p_4 & - & 4096 & & & & & \geqslant 0
\end{array}
$$

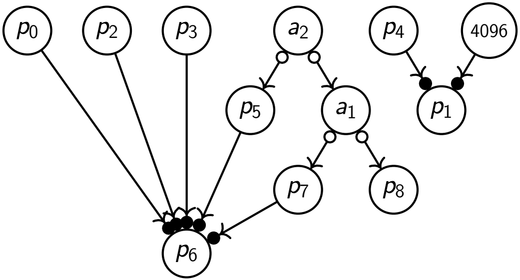
$$\Updownarrow$$

$$
\begin{array}{lllllllllll}
{\color{purple}2\,a_1} & - & p_0 & - & p_2 & - & p_3 & - & p_5 & \geqslant 0 \\
{\color{purple}1\,a_1} & - & p_4 & - & 4096 & & & & & \geqslant 0
\end{array}
$$

polarized: $p_8$ variable with the highest coefficient in both literals

# Running example

## Quantifier elimination

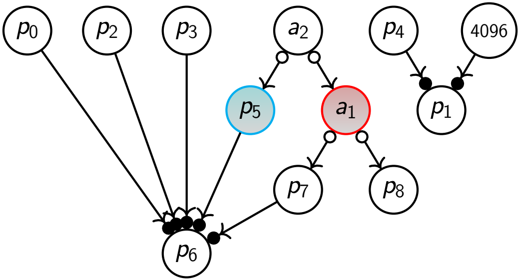



$$\begin{array}{ccccccccccc} 2\,a_1 & - & 1\,p_5 & - & p_0 & - & p_2 & - & p_3 & \geqslant 0 \\ 1\,a_1 & + & 0\,p_5 & - & p_4 & - & 4096 & & & \geqslant 0 \end{array}$$

$$\Updownarrow$$

# Running example

## Quantifier elimination



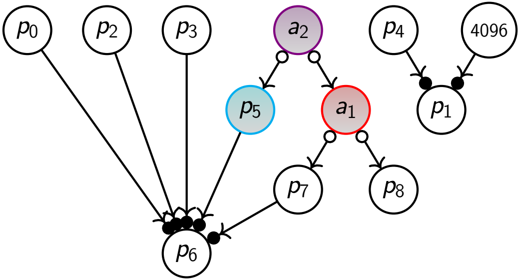

$$\begin{array}{cccccccccccc} 2\,a_1 & - & 1\,p_5 & - & p_0 & - & p_2 & - & p_3 & \geqslant 0 \\ 1\,a_1 & + & 0\,p_5 & - & p_4 & - & 4096 & & & \geqslant 0 \end{array}$$

$$\Updownarrow$$

polarized: $a_1$ variable with the highest coefficient in both literals

# Running example

## Quantifier elimination




$$\begin{array}{lclclclclcl} 2\,a_1 & - & 1\,p_5 & - & p_0 & - & p_2 & - & p_3 & \geqslant 0 \\ 1\,a_1 & + & 0\,p_5 & - & p_4 & - & 4096 & & & \geqslant 0 \end{array}$$

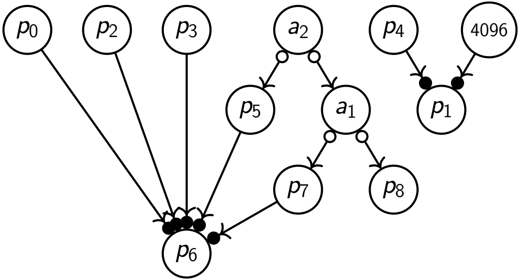
$$\Updownarrow$$

$$\begin{array}{lclclclcl} 2\,a_2 & - & p_0 & - & p_2 & - & p_3 & \geqslant 0 \\ 1\,a_2 & - & p_4 & - & 4096 & & & \geqslant 0 \end{array}$$

polarized: $a_1$ variable with the highest coefficient in both literals

# Running example

## Quantifier elimination




$$\begin{array}{rcrcrl} 3\,p_7 & + & 2\,p_8 & - & p_6 & \geqslant 0 \\ & & p_8 & - & p_1 & \geqslant 0 \end{array}$$

$$\Updownarrow$$

$$\begin{array}{rcrcrcrl} 2\,a_2 & - & p_0 & - & p_2 & - & p_3 & \geqslant 0 \\ a_2 & - & p_4 & - & 4096 & & & \geqslant 0 \end{array}$$

$$F_2 \triangleq (2a_2 \geqslant p_0 + p_2 + p_3) \wedge (a_2 \geqslant p_4 + 4096)$$

# If not polarized?

## Quantifier elimination

- **under-approximation**: If $m_2 \models F_2$ then $\exists m_1$ s.t. $m_1 \equiv_E m_2$ and $m_1 \models F_1$
- **over-approximation**: If $m_1 \models F_1$ then $\exists m_2$ s.t. $m_1 \equiv_E m_2$ and $m_2 \models F_2$

# If not polarized?

## Quantifier elimination

- **under-approximation**: If $m_2 \models F_2$ then $\exists m_1$ s.t. $m_1 \equiv_E m_2$ and $m_1 \models F_1$
- **over-approximation**: If $m_1 \models F_1$ then $\exists m_2$ s.t. $m_1 \equiv_E m_2$ and $m_2 \models F_2$

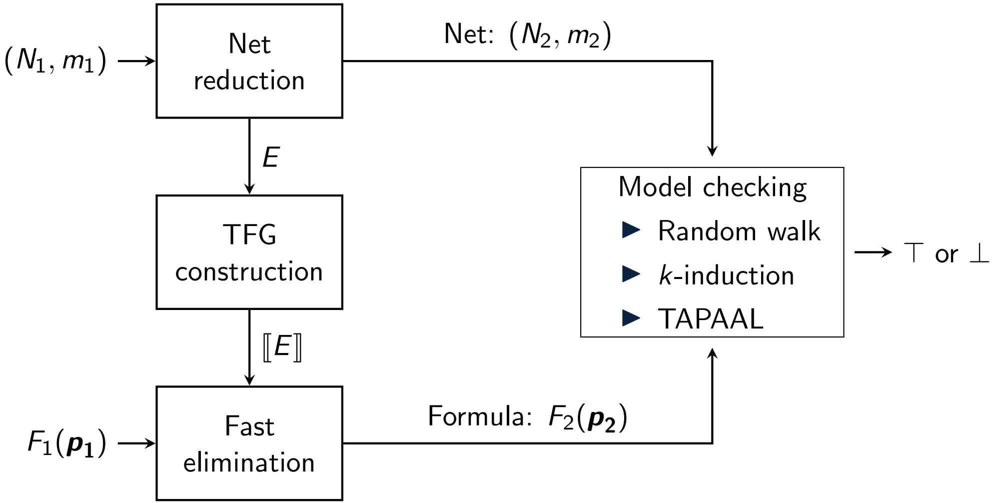
In practice, 80% of the formulas in the MCC benchmark are polarized!

# Outline

1. Polyhedral reduction
2. Token Flow Graphs
3. Quantifier elimination
4. Experimental evaluation

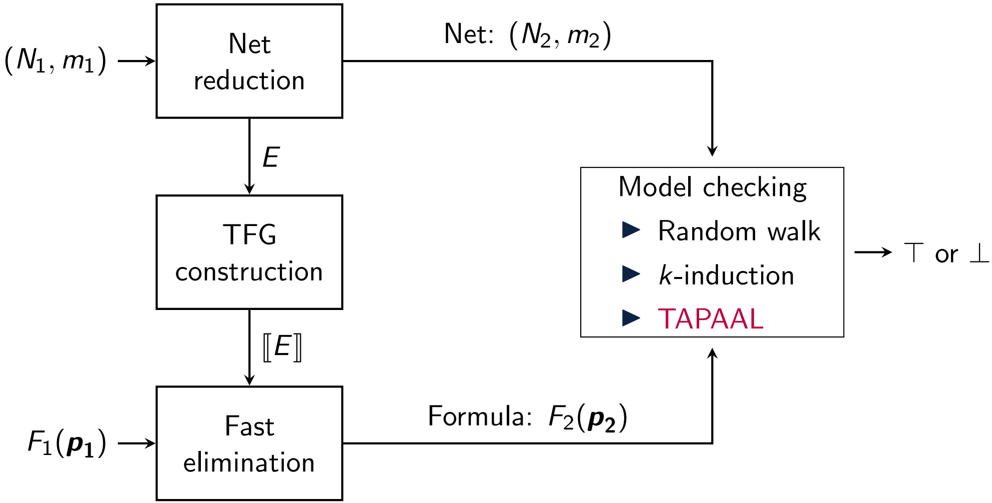
# Workflow

## Experimental evaluation



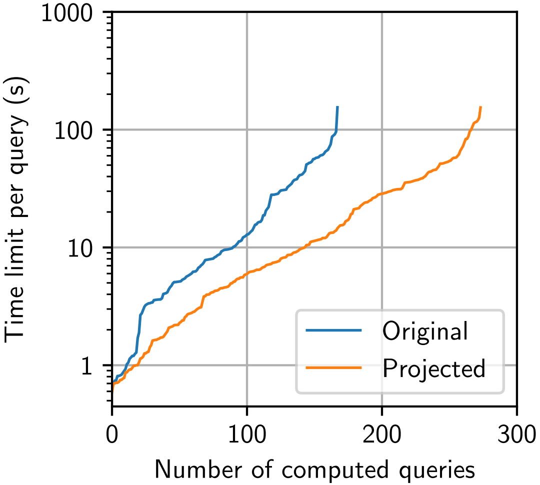
# Workflow

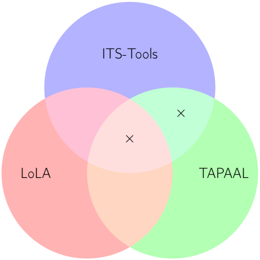
## Experimental evaluation



# Gains with TAPAAL: challenging queries

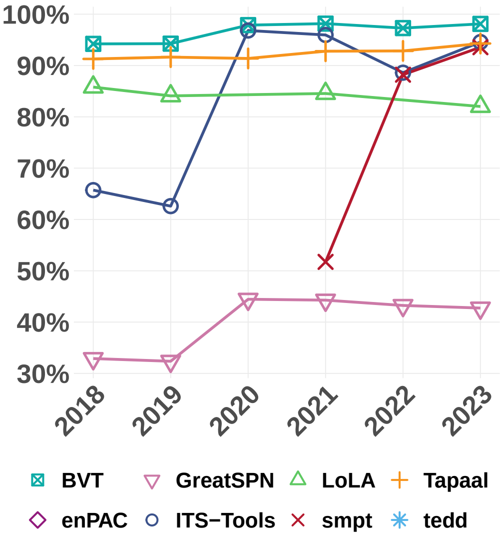
## Experimental evaluation



# Model Checking Contest: the tool SMPT

## Experimental evaluation




**2021**: BMC & PDR (coverability)

**2022**: Added standard methods

**2023**: Projection (+5.5%)

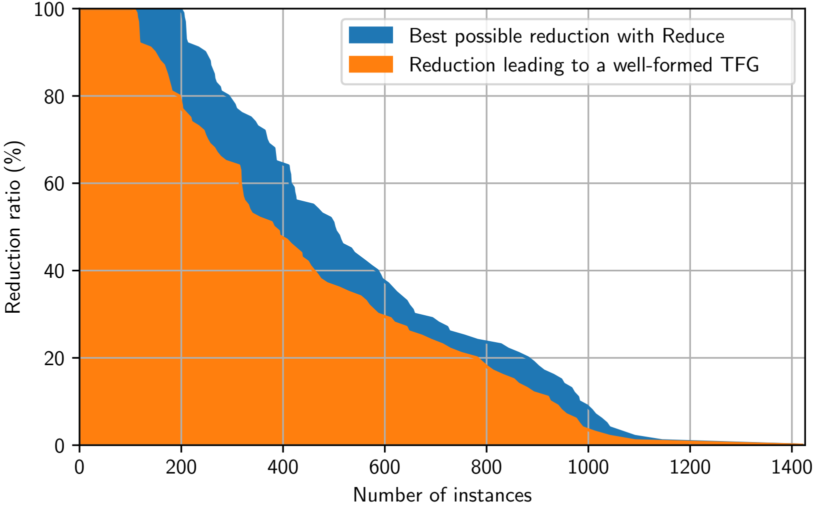
# Discussion

- Quantifier-elimination procedure tailored to the constraints we handle
- Combine polyhedral reduction with any model checking technique or tool
- Experimental results show the effectiveness of the approach
- Demonstrate it does not overlap other optimizations: slicing, symmetries, ...

# Prevalence of reductions over the MCC instances

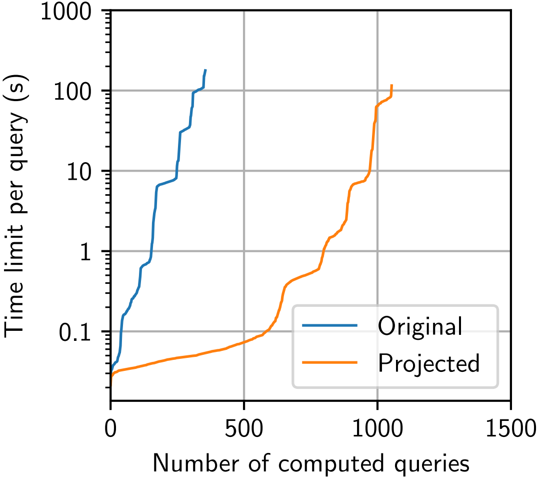
## Experimental evaluation

**Benchmark:** $\approx 1\,400$ nets and $\approx 25\,000$ reachability formulas



# Gains with $k$-induction: $50\% \leqslant$ reduction ratio $\leqslant 100\%$

Experimental evaluation



# Gains with $k$-induction: $1\% \leqslant$ reduction ratio $\leqslant 50\%$

Experimental evaluation