On the Combination of Polyhedral Abstraction and SMT-based Model Checking for Petri nets

Nicolas Amat, **Bernard Berthomieu**, **Silvano Dal Zilio**

LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France

Petri Nets, June 24 2021

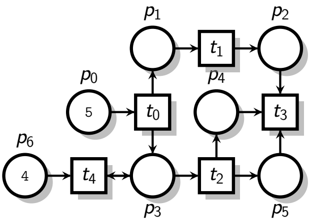
- Many results based on **linear algebra** and linear programming techniques [Murata, 1989] [Silva et al., 1996]
  - **Potentially reachable markings**
  - **Place invariants**
  - ...

- Many results based on **linear algebra** and linear programming techniques [Murata, 1989] [Silva et al., 1996]
  - **Potentially reachable markings**
  - **Place invariants**
  - ...
- **Structural reductions** [Berthelot, 1987]

- Many results based on **linear algebra** and linear programming techniques [Murata, 1989] [Silva et al., 1996]
  - **Potentially reachable markings**
  - **Place invariants**
  - ...
- **Structural reductions** [Berthelot, 1987]
- And 30 years after... [Berthomieu et al., 2019]
  Structural reductions with **linear equations**

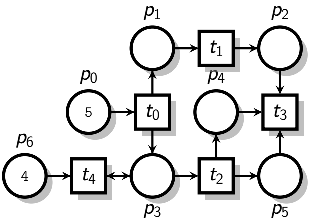
  Does it fit well with SMT-based methods?

A property ϕ is an **invariant** if for all reachable markings m in $R(N, m_0)$, m satisfies ϕ, denoted $m \models \phi$



$$\phi \equiv (p_1 + p_2 \leqslant 5) \wedge (p_4 = p_5)$$

We say that ϕ is **reachable** when there exists $m \in R(N, m_0)$ such that $m \models \phi$



$$\phi \equiv (p_1 \geqslant 1) \wedge (p_6 \leqslant 2)$$

- A marking is formula (**cube**) with variables in $\vec{x}$ that is only "satisfiable at marking m": $\underline{m}(\vec{x}) \equiv \bigwedge_{i \in 1..n}(x_i = m(p_i))$

$\underline{m_0}(\vec{p}) \equiv p_0 = 5 \wedge p_1 = 0 \wedge p_2 = 0 \wedge p_3 = 0 \wedge p_4 = 0 \wedge p_5 = 0 \wedge p_6 = 4$

- A marking is formula (**cube**) with variables in $\vec{x}$ that is only "satisfiable at marking m": $\underline{m}(\vec{x}) \equiv \bigwedge_{i \in 1..n}(x_i = m(p_i))$

  $\underline{m_0}(\vec{p}) \equiv p_0 = 5 \wedge p_1 = 0 \wedge p_2 = 0 \wedge p_3 = 0 \wedge p_4 = 0 \wedge p_5 = 0 \wedge p_6 = 4$

- ϕ **reachable** iff $\exists m \in R(N, m_0)$ s.t. $\phi(\vec{x}) \wedge \underline{m}(\vec{x})$ SAT

- A marking is formula (**cube**) with variables in $\vec{x}$ that is only "satisfiable at marking m": $\underline{m}(\vec{x}) \equiv \bigwedge_{i \in 1..n}(x_i = m(p_i))$

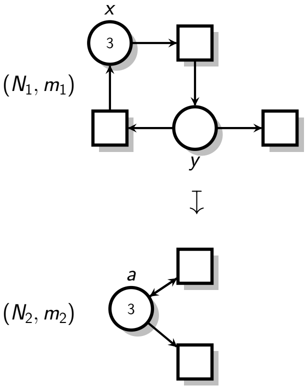
  $\underline{m_0}(\vec{p}) \equiv p_0 = 5 \land p_1 = 0 \land p_2 = 0 \land p_3 = 0 \land p_4 = 0 \land p_5 = 0 \land p_6 = 4$

- ϕ **reachable** iff $\exists m \in R(N, m_0)$ s.t. $\phi(\vec{x}) \land \underline{m}(\vec{x})$ SAT

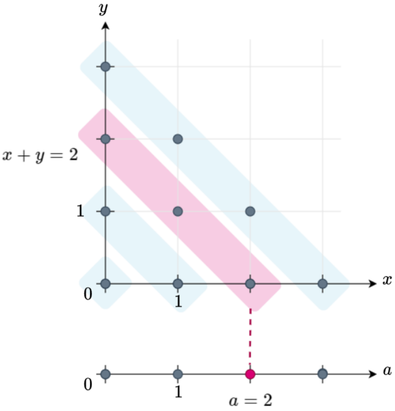
- ϕ **invariant** iff $\forall m \in R(N, m_0)$ we have $\neg\phi(\vec{x}) \land \underline{m}(\vec{x})$ $UNSAT$

- **Coverability**: $\mathrm{COVER}(p, k) \;\equiv\; m(p) \geq k$
- **Reachability**: $\mathrm{REACH}(p) \;\equiv\; m(p) \geq 1$
- **Quasi-liveness**: $\mathrm{LIVE}(t) \;\equiv\; \bigwedge_{p \in {}^{\bullet}t} \mathrm{COVER}(p, \mathbf{pre}(t, p))$
- **Deadlock**: $\mathrm{DEAD} \;\equiv\; \bigwedge_{t \in T} \neg \mathrm{LIVE}(t)$

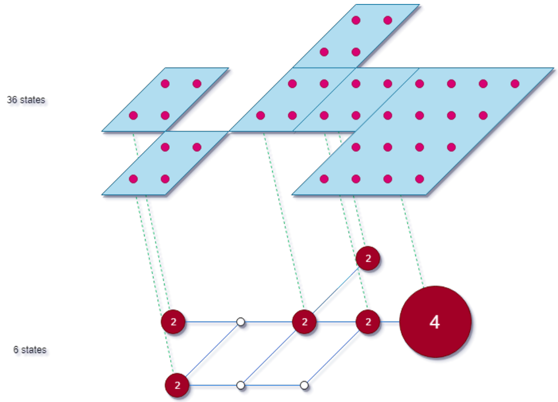
- **QF-LIA** theory
    - Unbounded Petri nets
    - Perfect fitting with properties of interest



Net reduction example, with equation $E : a = x + y$



Relation between state-spaces

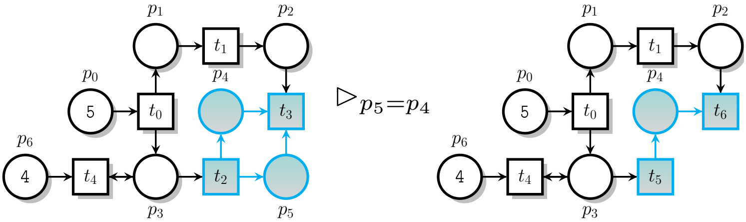


State-space abstraction by a "polyhedral approach"

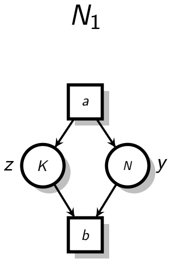
- **QF-LIA** theory
  - Unbounded Petri nets
  - Perfect fitting with properties of interest
  - \+ Perfect fitting with reduction equations

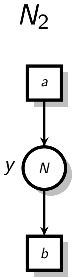
On the Combination of Polyhedral Abstraction and SMT-based Model Checking for Petri nets

Rule: RED


p1
p2
t1
p0
p4
5
t0
t3
p6
4
t4
t2
p3
p5
▷p5=p4
p1
p2
t1
p0
p4
5
t0
t6
p6
4
t4
t5
p3

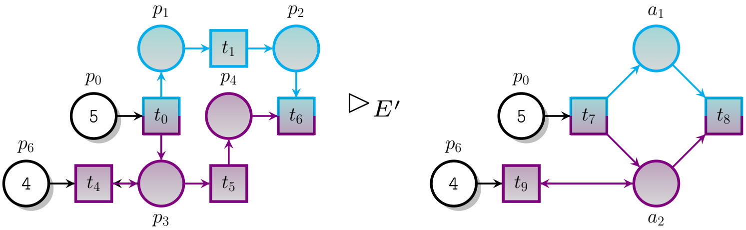
Condition: $K > N$





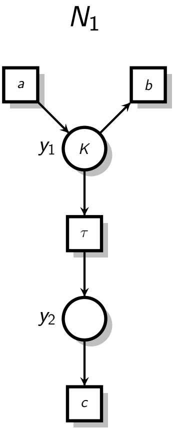
Equation: $z = y + K - N$

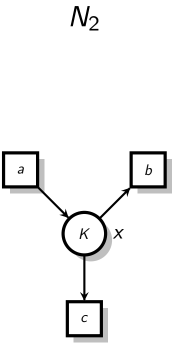
Rule: CONCAT



$$E' \triangleq (a_1 = p_1 + p_2) \wedge (a_2 = p_3 + p_4)$$

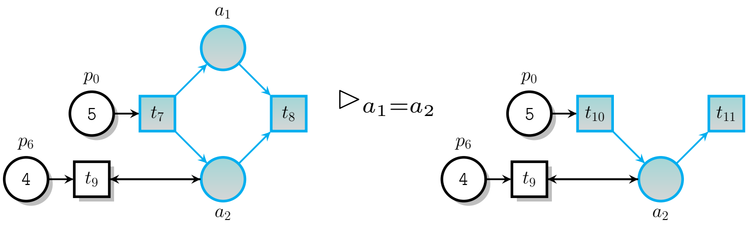
Reduction Rules: Concatenate (CONCAT)





Equation: $x = y_1 + y_2$

Rule: RED



- A marking m can be associated to **system of equations** $\underline{m}$ defined as, $p_1 = m(p_1), \ldots, p_k = m(p_k)$ where $P = \{p_1, \ldots, p_k\}$

- A marking m can be associated to **system of equations** $\underline{m}$ defined as, $p_1 = m(p_1), \ldots, p_k = m(p_k)$ where $P = \{p_1, \ldots, p_k\}$

- E is **satisfiable** for marking m if the system $E, \underline{m}$ has solutions

- A marking m can be associated to **system of equations** $\underline{m}$ defined as, $p_1 = m(p_1), \ldots, p_k = m(p_k)$ where $P = \{p_1, \ldots, p_k\}$

- E is **satisfiable** for marking m if the system $E, \underline{m}$ has solutions

- Two markings m_1 and m_2 are **compatible** when $m_1(p) = m_2(p)$ for all p in $P_1 \cap P_2$

  In that case we denote: $(m_1 \uplus m_2)(p) = \begin{cases} m_1(p) & \text{if } p \in P_1 \\ m_2(p) & \text{if } p \in P_2 \end{cases}$

Definition (E-abstraction)

$(N_1, m_1) \sqsupseteq_E (N_2, m_2)$ iff

(A1) initial markings are compatible with E, meaning $m_1 \uplus m_2 \models E$

(A2) for all observation sequences $\sigma \in \Sigma^\star$ such that $(N_1, m_1) \stackrel{\sigma}{\Rightarrow} (N_1, m_1')$

- there is at least one marking $m_2' \in R(N_2, m_2)$ such that $m_1' \uplus m_2' \models E$
- for all markings m_2' we have that $m_1' \uplus m_2' \models E$ implies $(N_2, m_2) \stackrel{\sigma}{\Rightarrow} (N_2, m_2')$

Definition (E-abstraction)

$(N_1, m_1) \sqsupseteq_E (N_2, m_2)$ iff

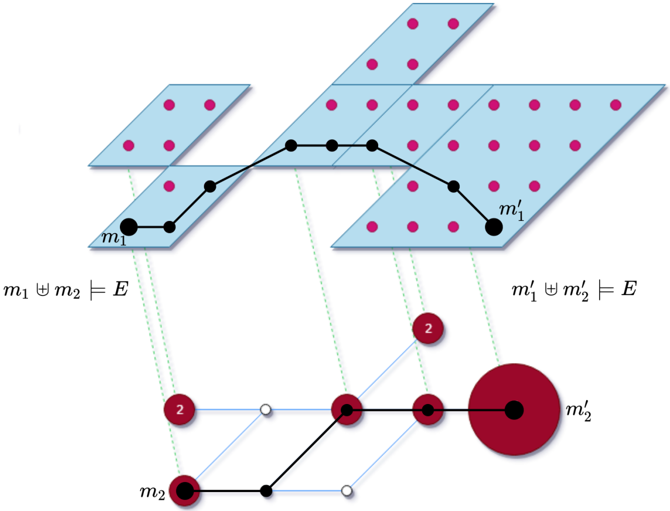
(A1) initial markings are compatible with E, meaning $m_1 \uplus m_2 \models E$

(A2) for all observation sequences $\sigma \in \Sigma^\star$ such that $(N_1, m_1) \stackrel{\sigma}{\Rightarrow} (N_1, m_1')$

- there is at least one marking $m_2' \in R(N_2, m_2)$ such that $m_1' \uplus m_2' \models E$
- for all markings m_2' we have that $m_1' \uplus m_2' \models E$ implies $(N_2, m_2) \stackrel{\sigma}{\Rightarrow} (N_2, m_2')$

E-abstraction equivalence

$(N_1, m_1) \rhd_E (N_2, m_2)$ iff $(N_1, m_1) \sqsupseteq_E (N_2, m_2)$ and $(N_2, m_2) \sqsupseteq_E (N_1, m_1)$



m_1
m'_1
$m_1 \uplus m_2 \models E$
$m'_1 \uplus m'_2 \models E$
2
2
m_2
m'_2

Axioms: Reduction Rules (RED, CONCAT, etc.)

Axioms: Reduction Rules (RED, CONCAT, etc.)

Laws:

- Composability
- Transitivity
- Relabeling

On the Combination of Polyhedral Abstraction and SMT-based Model Checking for Petri nets

- Is F_1 an invariant on (N_1, m_1)?

- Is F_1 an invariant on (N_1, m_1)?

Definition (E-transform Formula)

Formula $F_2(\vec{y}) \triangleq \tilde{E}(\vec{x}, \vec{y}) \wedge F_1(\vec{x})$ is the E-transform of F_1

- Is F_1 an invariant on (N_1, m_1)?

Definition (E-transform Formula)

Formula $F_2(\vec{y}) \triangleq \tilde{E}(\vec{x}, \vec{y}) \wedge F_1(\vec{x})$ is the E-transform of F_1

- Is the E-transform formula F_2 an invariant on (N_2, m_2)?

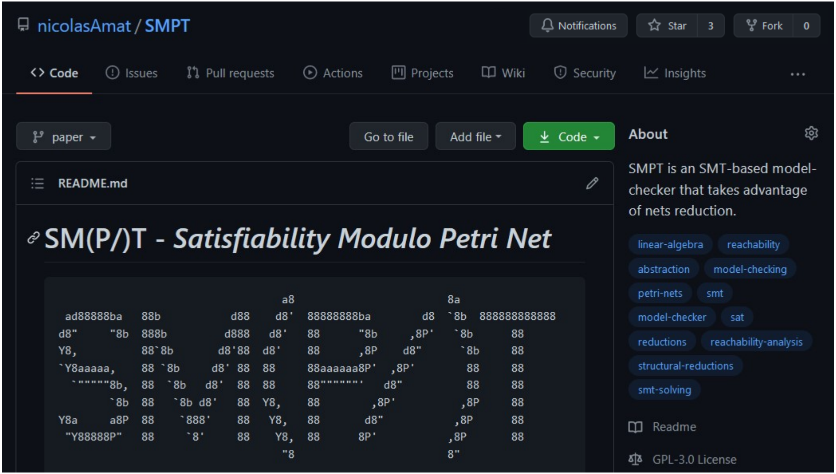
Theorem (Invariant Conservation)

F_1 is an invariant on N_1 if and only if its E-tranform formula is an invariant on N_2

Theorem (Reachability Conservation)

F_1 is reachable in N_1 if and only if its E-tranform formula is reachable in N_2

SMPT: Another Model-Checker



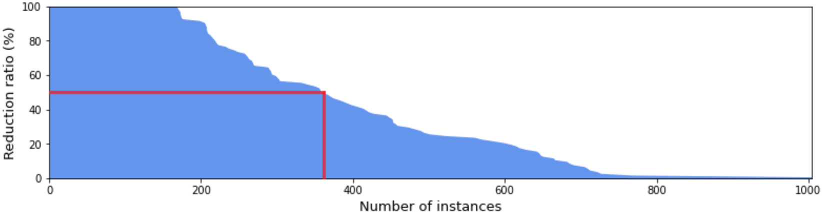
nicolasAmat / SMPT
Notifications
Star 3
Fork 0
Code
Issues
Pull requests
Actions
Projects
Wiki
Security
Insights
paper
Go to file
Add file
Code
README.md
SM(P/)T - Satisfiability Modulo Petri Net
About
SMPT is an SMT-based model-checker that takes advantage of nets reduction.
linear-algebra
reachability
abstraction
model-checking
petri-nets
smt
model-checker
sat
reductions
reachability-analysis
structural-reductions
smt-solving
Readme
GPL-3.0 License

- **Bounded Model Checking** (BMC): counterexample finder
- **Property Directed Reachability** (PDR): invariant prover

Experimental Results

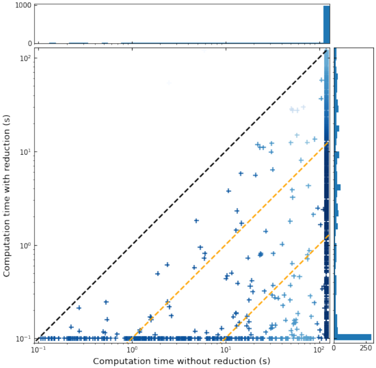
Prevalence of Reductions over the MCC Instances

Experimental Results



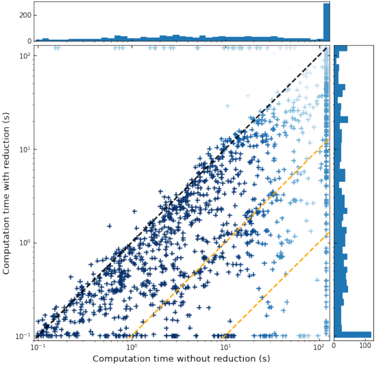
Computation Time
Experimental Results

Computation time with (y-axis) vs without (x-axis) reduction (s)

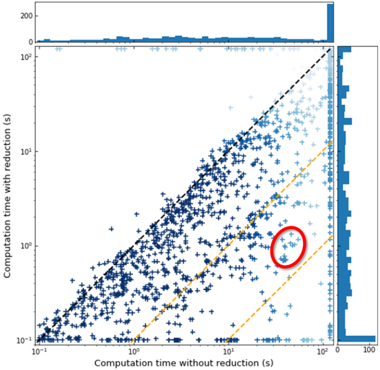


Reduction ratio $\in [0.5, 1[$

Computation time with (y-axis) vs without (x-axis) reduction (s)

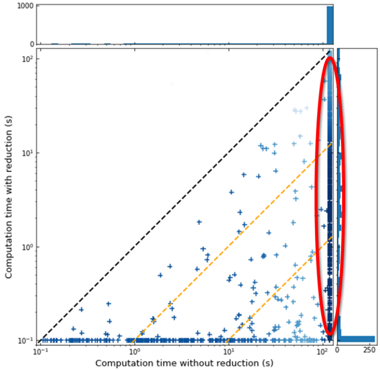


Reduction ratio $\in]0, 0.25[$



Reduction ratio $\in]0, 0.25[$

Instance	ARMCacheCoherence
State Space	3.206e+8
Red Ratio	17%
$\mathbb{E}_{red}(\theta)$	1 s
$\mathbb{E}_{\overline{red}}(\theta)$	20 s



Reduction ratio $\in [0.5, 1[$

Instance	AirplaneLD-1000
State Space	?
Red Ratio	99%
# Props with red	14
# Props without red	0

Conclusion and Perspectives

Conclusion

- New promising framework for the use of reductions with SMT-based methods
- New equivalence relation: *E-abstraction equivalence*
- Contributions for SMT-based algorithms

Perspectives

- New release of SMPT is coming
  - Adaptation of PDR for Reachability
- Automated proof of E-abstraction equivalences
- Accelerating the Computation of Dead and Concurrent Places using Reductions [SPIN2021]
- Participated to the MCC'2021

Thank you for your attention!