Hyper Partial Order Logic

B. Bérard[1], S. Haar[2], L. Hélouët[3]

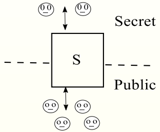
[1] LIP6, Paris,
[2] INRIA Paris-Saclay
[3] INRIA Rennes,

FSTTCS'18, December $10 - 14$, 2018

RAPS 2024, April, 24^{th} 2024

Motivations

<u>Non Interference</u>
$\Sigma = \Sigma_{low} \uplus \Sigma_h$



$$\mathcal{L}(\mathcal{O}_{low}(S)) \subseteq \mathcal{L}(\mathcal{O}_{low}(S \backslash \Sigma_h))$$

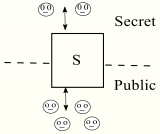
$$\forall \rho_1.h.\rho_1', \exists \rho_2 \in \sigma_{low}^*,$$
$$\mathcal{O}_{low}(\rho_1.h.\rho_1') = \mathcal{O}_{low}(\rho_2)$$

<u>Pb :</u> cannot be expressed with a LTL, CTL property.

Motivations

Non Interference

$\Sigma = \Sigma_{low} \uplus \Sigma_h$



$$\mathcal{L}(\mathcal{O}_{low}(S)) \subseteq \mathcal{L}(\mathcal{O}_{low}(S \backslash \Sigma_h))$$

$$\forall \rho_1.h.\rho_1', \exists \rho_2 \in \sigma_{low}^*, \\ \mathcal{O}_{low}(\rho_1.h.\rho_1') = \mathcal{O}_{low}(\rho_2)$$

Pb : cannot be expressed with a LTL, CTL property.

Mantel's framework

Comparison of language closures (projections, morphisms,...)
[Mantel00] [D'Souza11, 16]

$$\begin{array}{ll} & op_1(\mathcal{L}(S)) \subseteq op_2(\mathcal{L}(S)) \\ \wedge & op_3(\mathcal{L}(S)) \subseteq op_4(\mathcal{L}(S)) \\ \wedge & \ldots \end{array}$$

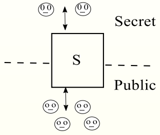
Hyperproperties

Properties of sets of traces
[Clarkson14, Schneider10]

Motivations

Non Interference

$\Sigma = \Sigma_{low} \uplus \Sigma_h$



$\mathcal{L}(\mathcal{O}_{low}(S)) \subseteq \mathcal{L}(\mathcal{O}_{low}(S \backslash \Sigma_h))$

$\forall \rho_1.h.\rho_1', \exists \rho_2 \in \sigma_{low}^*,$
$\mathcal{O}_{low}(\rho_1.h.\rho_1') = \mathcal{O}_{low}(\rho_2)$

Pb : cannot be expressed with a LTL, CTL property.

Mantel's framework

Comparison of language closures (projections, morphisms,...)

[*Mantel*00] [*D'Souza*11, 16]

Alur's framework : CTL∼ CTL

+ a relation on equivalent events

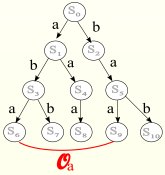
[*Alur*07]

$$\begin{array}{ll} & op_1(\mathcal{L}(S)) \subseteq op_2(\mathcal{L}(S)) \\ \wedge & op_3(\mathcal{L}(S)) \subseteq op_4(\mathcal{L}(S)) \\ \wedge & \ldots \end{array}$$

Hyperproperties

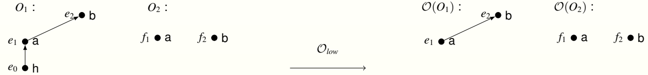
Properties of sets of traces

[*Clarkson*14, *Schneider*10]



Local Logics

$\mathcal{O}_{low}$ projection on events with label in $\{a, b\}$.



Interleaved setting :

Formula of the form $\phi ::= X(p_a \wedge Xp_b)$ does not characterize O_1

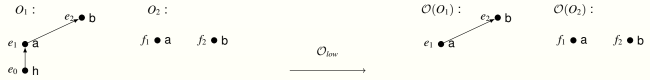
Partial order setting

$$O, e \models \lambda(e) = a \wedge \exists f, e \prec f, \lambda(f) = b$$

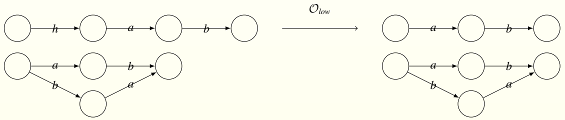
Address the shape of causal ordering among events in a single partial order !
LD_0 [*Meenakshi*04], TCL^- [*Peled*00],...

Local Logics

$\mathcal{O}_{low}$ projection on events with label in $\{a, b\}$.



Interleaved setting :



Formula of the form $\phi ::= X(p_a \wedge Xp_b)$ does not characterize O_1

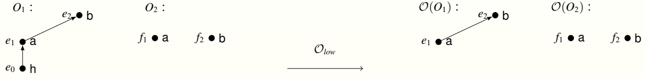
Partial order setting

$$O, e \models \lambda(e) = a \wedge \exists f, e \prec f, \lambda(f) = b$$

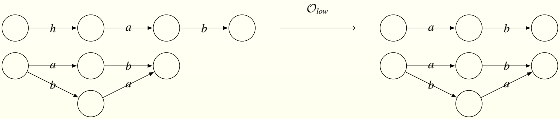
Address the shape of causal ordering among events in a single partial order !
LD_0 $[Meenakshi04]$, TCL^- $[Peled00]$,...

Local Logics

$\mathcal{O}_{low}$ projection on events with label in $\{a, b\}$.



Interleaved setting :



Formula of the form $\phi ::= X(p_a \wedge Xp_b)$ does not characterize O_1

Partial order setting

$$O, e \models \lambda(e) = a \wedge \exists f, e \prec f, \lambda(f) = b$$

Address the shape of causal ordering among events in a single partial order!
LD$_0$ [*Meenakshi*04], TCL$^-$ [*Peled*00],...

Outline

HYPOL : an Hyper Partial Order Logic

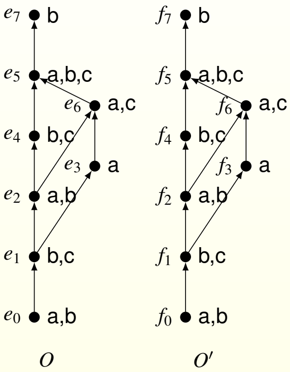
Part 1 : Hypol

- Partial orders, template
- Partial observations
- Hypol : Syntax & Semantics
- Satisfiability
- Example : causal non-interference

Part 2 : Model Checking on Petri nets processes

- Unfolding & processes
- A grammar for unfolding
- Execution graphs
- From Hypol to MSO
- Observable nets

Partial Orders, templates



LPO over Σ

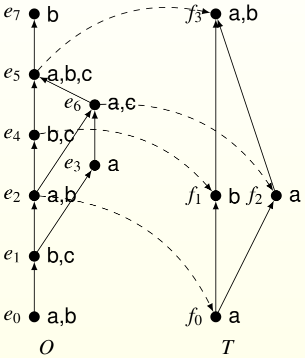
$O = (E, \leq, \lambda)$

- E is a set of events,
- $\leq \subseteq E \times E$ partial order,
- $\lambda : E \rightarrow 2^{\Sigma}$ labeling

Definition : Isomorphism

$O = (E, \leq, \lambda)$ and $O' = (E', \leq', \lambda')$ are *isomorphic* ($O \equiv O'$) iff $\exists h : E \rightarrow E'$ such that $e \leq e' \iff h(e) \leq' h(e')$ and $\lambda(e) = \lambda'(h(e))$.

Partial Orders, templates



LPO over Σ

$O = (E, \leq, \lambda)$

- E is a set of events,
- $\leq \subseteq E \times E$ partial order,
- $\lambda : E \to 2^{\Sigma}$ labeling

Template Matching

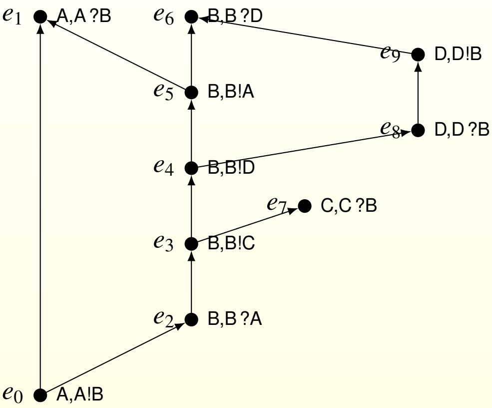
$O = (E, \leq, \lambda)$ and
$T = (E_T, \leq_T, \lambda_T)$
O *matches T* iff
$\exists h \subseteq E, h : H \to E_T$ such that :

- $\lambda_T(h(e)) \subseteq \lambda(e)$,
- $e <_T e'$ implies $h^{-1}(e) < h^{-1}(e')$.

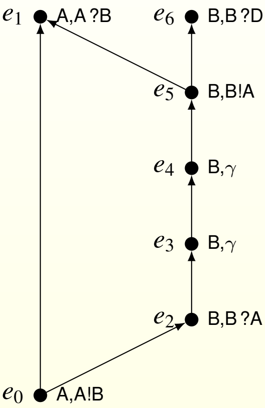
Partial Observations

Observation function

mapping $\mathcal{O} : \mathcal{L}PO(\Sigma) \rightarrow \mathcal{L}PO(\Sigma')$, representing the visible part of the system.

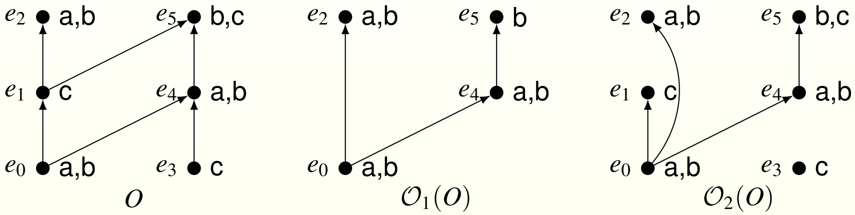


O



$\mathcal{O}_{a,b}(O)$

Observation : examples



$\mathcal{O}_1(O)$: projection on events that carry label a or b,

$\mathcal{O}_2(O)$: restriction of $\leq$ to events with an a

Main idea : model the observation power of an intruder.

Hypol : Syntax & Semantics

- A, Σ atomic propositions
- $\mathcal{T}$ finite set of templates over A,
- $\mathcal{O}bs$ finite set of observation functions

$$
\begin{aligned}
\phi ::= \quad & true \mid \neg\, \phi \mid \phi_1 \vee \phi_2 \\
& \mid match(\mathcal{O}, T, f) \\
& \mid EX_{D,\mathcal{O}}\ \phi \mid EX_{\equiv,\mathcal{O}}\ \phi \\
& \mid \phi_1\ EU_{D,\mathcal{O}}\ \phi_2 \mid EG_{D,\mathcal{O}}\ \phi
\end{aligned}
$$

where $D \subseteq A$, $T \in \mathcal{T}$, f is an event of T, and $\mathcal{O} \in \mathcal{O}bs$

Semantics

Evaluation of formulas

Formulas are evaluated over a set $\mathcal{W}$ of LPOs over Σ,
$\mathcal{W}$ satisfies ϕ iff $\exists O = (E, \leq, \lambda) \in W, e \in min(O)$,
$O, e \models \phi$

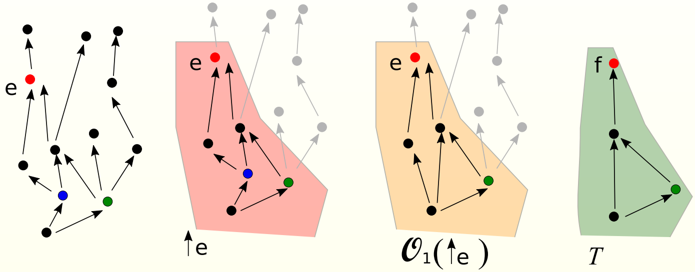
Satisfiability

A formula ϕ is satisfiable iff there exists an universe $\mathcal{W}$ such that
$\mathcal{W} \models \phi$
Satisfiability problem : Given ϕ, is it satisfiable by some universe $\mathcal{W}$?

Model checking

A model M satisfies a formula ϕ iff the universe $\mathcal{W}_M$ of its executions satisfies ϕ
Model checking problem : Given M, ϕ, does $\mathcal{W}_M \models \phi$?

Semantics : Matching

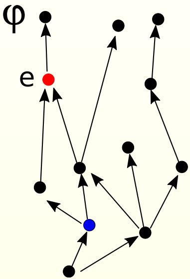


$O, e \models match(\mathcal{O}_1, T, f)$
iff

- one can match T in the observation $\mathcal{O}_1(\downarrow e)$ (causal past of e).
- with at least a witness mapping $h_{e,f}$ associating f with e

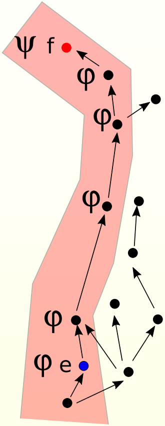
Semantics : $EX_{D,\mathcal{O}}$ and $EU_{D,\mathcal{O}}$

$O, e \models EX_{D,\mathcal{O}}\ \phi$



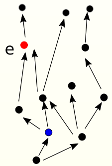
The next observed event satisfies ϕ

$O, e \models \phi EU_{D,\mathcal{O}}\ \psi$

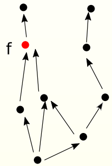


There exists an event in the future that satisfies ϕ

(D is a technicality allowing to select successors – e.g. next event on the same process–)



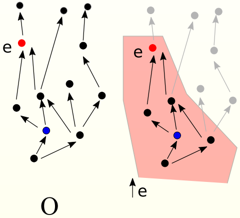
O

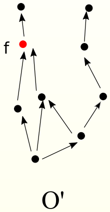


O'

$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

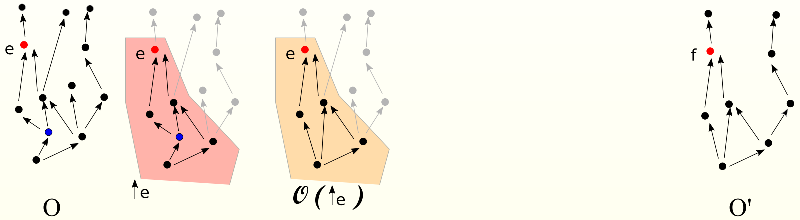
Semantics : $EX_{\equiv,\mathcal{O}}$ – The hyperlogic part –



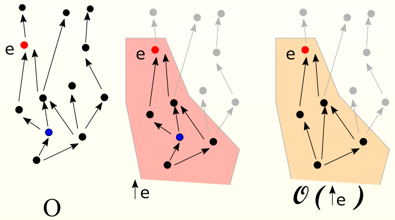


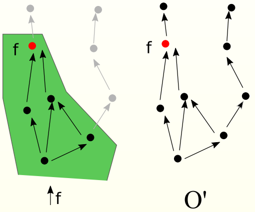
$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

Semantics : $EX_{\equiv,\mathcal{O}}$ – The hyperlogic part –

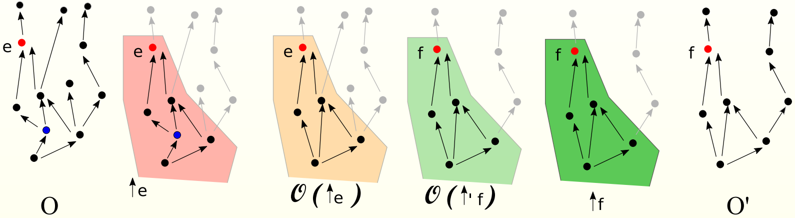


$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

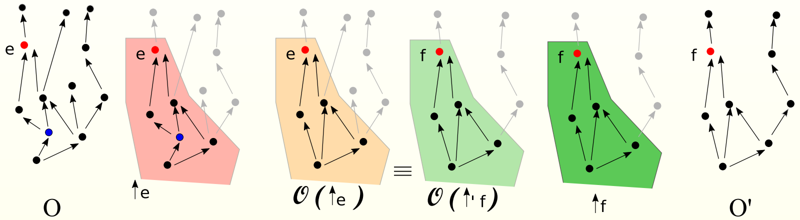




$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

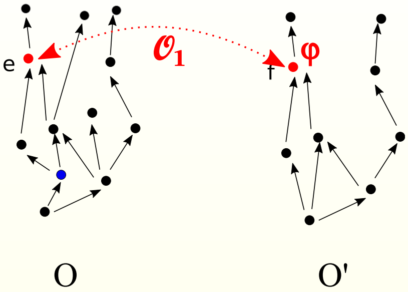


$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$



$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

Semantics : $EX_{\equiv,\mathcal{O}}$



$O, e \models EX_{\equiv,\mathcal{O}}\ \phi$

There exists another order O' in $\mathcal{W}$ and an event f such that

- $O', f \models \phi$
- $\mathcal{O}$ cannot distinguish the causal past of e and f

$$\mathcal{O}(\uparrow e) \equiv \mathcal{O}(\uparrow e)$$

An example : causal Non-Interference

Let $\Sigma = \Sigma_{high} \uplus \Sigma_{low}$ with $\Sigma_{high} = \{h\}$ and $\Sigma_{low} = \{a, b\}$

$\mathcal{O}_{low}$ projection of LPOs on events with label in Σ_{low}.

Causal Non-Interference

$$T_{\mathsf{h}\leq a} = \bullet^{h} \longrightarrow \bullet^{a}$$
$$Pred_h ::= \bigvee_{a\in\Sigma} match(\mathcal{O}_{\mathsf{h},a}, T_{\mathsf{h}\leq a})$$
$$\phi_{CNI} ::= AG_{\Sigma,id}\left(\lambda_{\in\Sigma_{high}} \vee Pred_h \implies EX_{\equiv,\mathcal{O}_{low}}(\lambda_{\notin\Sigma_{high}} \wedge \neg Pred_h)\right)$$

If a system satisfies ϕ_{CNI}, then an intruder with observation capacity $\mathcal{O}_{low}$ cannot differentiate runs with/without h.

In particular, a system with behaviors $\mathcal{W} = \{O_1, O_2\}$ does not satisfy ϕ_{CNI} and is not secure

Satisfiability

Theorem

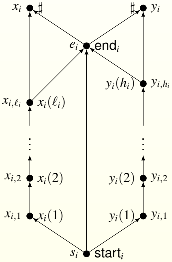
Satisfaibility of Hypol is undecidable

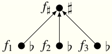
A PCP encoding :

$I = \{(x_1, y_1), \dots, (x_n, y_n)\}$

(x_i, y_i) pair of words in A^*.

$\exists i_1 \dots i_k$ such that
$x_{i_1} \dots x_{i_k} = y_{i_1} \dots y_{i_k}$?





two-pred♯ $::= AG_{P,id}(\lambda_{=\{\sharp\}} \implies \neg match(\mathcal{O}_\sharp, T_\sharp, f_\sharp))$
IsSeqIndex $::= EG_{S,\mathcal{O}_S}(\vee_{i=1}^n HoldsT_i) \wedge EF_{P,id} stop$
ϕ_I ::= *two-pred*♯ $\wedge$ *IsSeqIndex* $\wedge$ $(stop \implies EX_{\equiv,\mathcal{O}_{sol}} true)$

PCP instance I has a solution if $\exists O, e$ such that $O, e \models \phi_I$

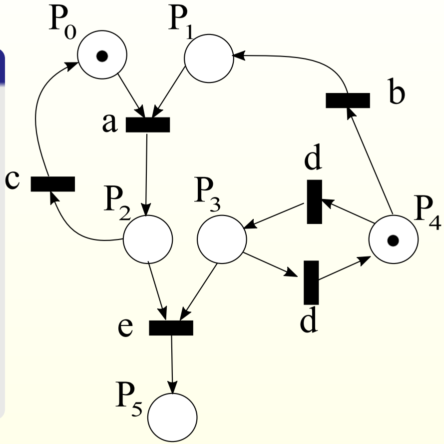
Part 2 : Model Checking on Petri nets Processes

Petri nets

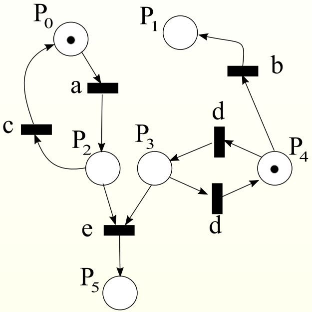
Definition

A *labeled Petri net* is a tuple $\mathcal{N} = (P, T, F, M_0)$

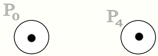
- P : set of places,
- T set of transitions
- $F \subseteq P \times T \cup T \times P$ flow relation,
- $M_0 \in \mathbb{N}^P$ is the initial marking.
- $\lambda : T \to \Sigma$



Process Semantics

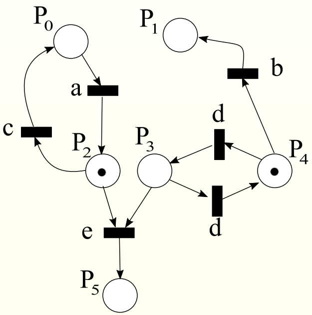


$\mathcal{N}$

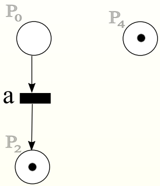


$W_1 \in PR(\mathcal{N})$

Process Semantics

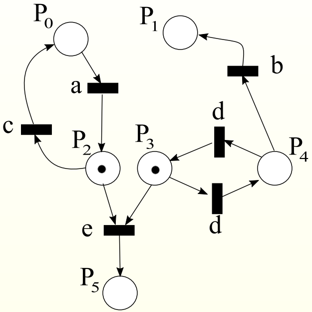


$\mathcal{N}$

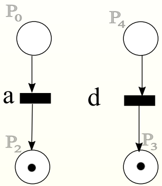


$W_1 \in Proc(\mathcal{N})$

Process Semantics

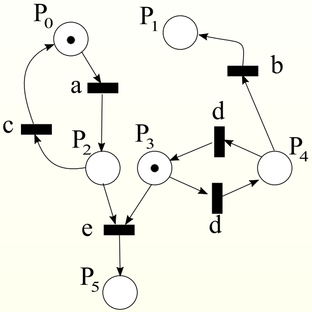


$\mathcal{N}$

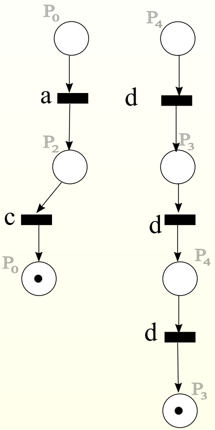


$W_1 \in Proc(\mathcal{N})$

Process Semantics

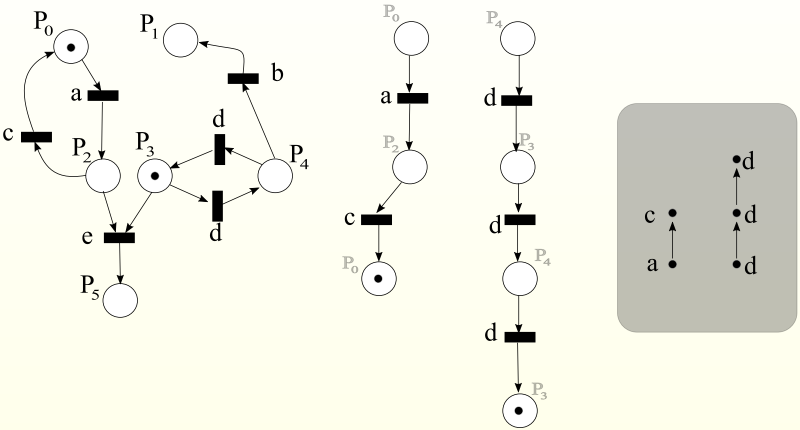


$\mathcal{N}$



$W_1 \in Proc(\mathcal{N})$

Process Semantics



$\mathcal{N}$ $\quad W_1 \in Proc(\mathcal{N})$ $\quad O_1 = Ord(W_1)$

Process Semantics : model checking

Model checking Hypol on Petri nets

Let $\mathcal{N}$ be a Petri net, *PR*$(\mathcal{N})$ its set of processes
Let ϕ be an hypol formula :
$\mathcal{N} \models \phi$ iff $\exists O \in Ord(PR(\mathcal{N})), e \in min(O)$ such that $O, e \models \phi$

Unfortunately ....

Undecidability

Model checking of Hypol properties for (safe) Petri nets is undecidable.

Why : PCP encoding. For every instance I of PCP, can build a net $\mathcal{N}_I$ such that $\mathcal{N}_I \models \phi_I$ iff this instance of PCP has a solution.

Definition

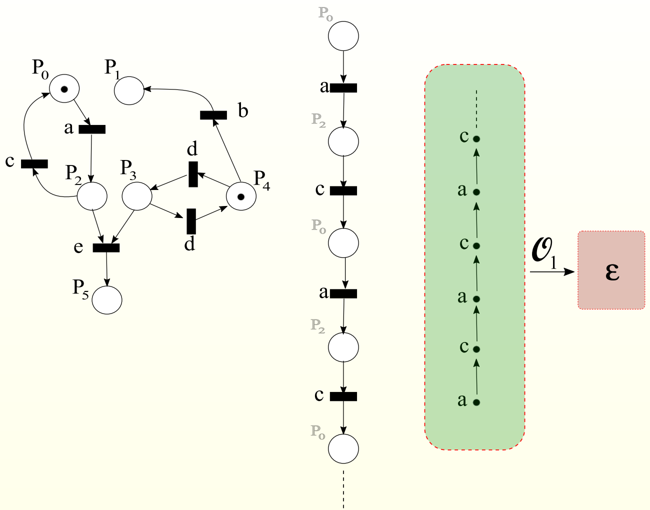
$\mathcal{N}$ is *observable* (wrt $\mathcal{O}_1, \ldots \mathcal{O}_k$) iff

i) $\forall \mathcal{O}_i$, every cyclic behavior produces something observable by $\mathcal{O}_i$ at every iteration,

ii) $\forall \mathcal{O}_i$, choices eventually appear in observation after k_c steps,

iii) $\forall \mathcal{O}_i$, there exists a bound on the size of parallel threads which have identical observation

Process Semantics : model checking

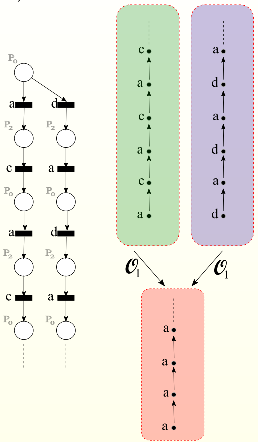


$\mathcal{O}_1$: projection on events with labels in $\{b, d, e\}$.

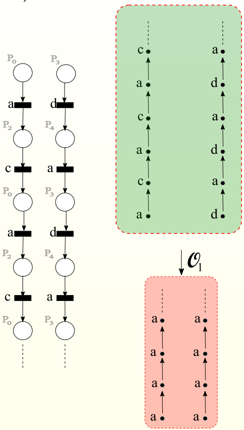
$i)$: $\mathcal{N}$ does not remain unobservable forever

Process Semantics : model checking

ii)



iii)



$\mathcal{O}_1$: projection on events with label a.

$i) + ii) + iii) \implies$ an event e is always equivalent to a bounded number of events in a bounded past / parallel part

Model checking of Hypol

Theorem

Hypol model-checking is decidable for observable nets.

- show that processes of a nets can be seen as a regular graph $\mathcal{G}^{\omega}_{\mathcal{N}}$
- isomorphism up to observation $\mathcal{O}_i$ can be encoded as an additional relation $\stackrel{i}{\longrightarrow}$:
  gives a new (non regular) graph $G_{\mathcal{N}}$
- Show that Hypol properties of safe nets can be encoded as MSO properties
- Identify a class of $K-$layered nets where $G_{\mathcal{N}}$ is regular
  Hypol decidable on this class !
- Show that observable nets belong to this class

Branching processes

Branching processes "unfold" Petri nets

Definition (Branching Process)

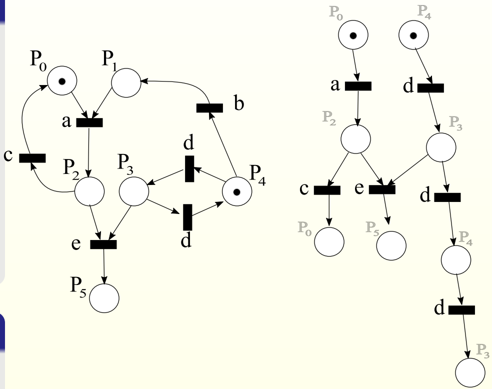
A *branching process* of $\mathcal{N} = (P, T, F, M_0, \lambda)$ is a triple $BR = (ON, \mu, \lambda')$

- $ON = (B, E, \hat{F}, Cut_0)$ is an occurrence net,
- μ is a homomorphism

and $\forall e \in E, \lambda'(e) = \lambda(\mu(e))$.

Definition (Unfolding)

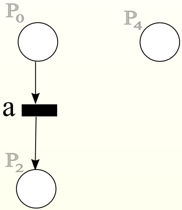
The *unfolding* of $\mathcal{N}$, $\mathcal{U}(\mathcal{N})$, is the maximal branching process.



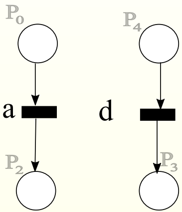
$\mathcal{U}(\mathcal{N})$ can be seen as the union of all processes of $\mathcal{N}$

Unfolding & processes

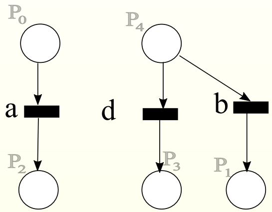
Unfolding & processes



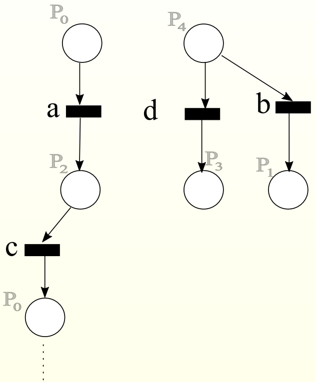
Unfolding & processes



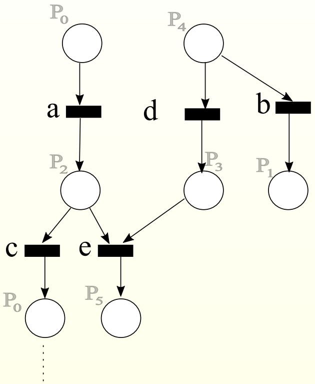
Unfolding & processes



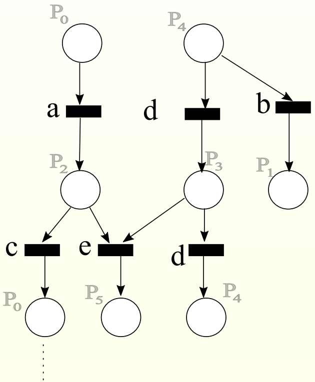
Unfolding & processes



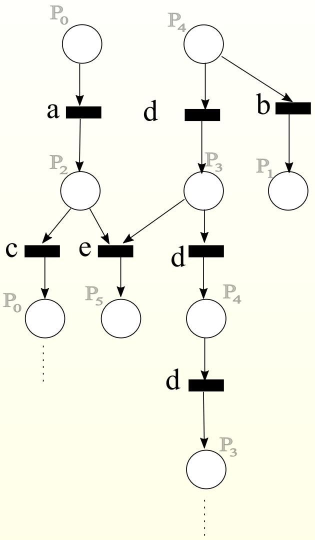
Unfolding & processes



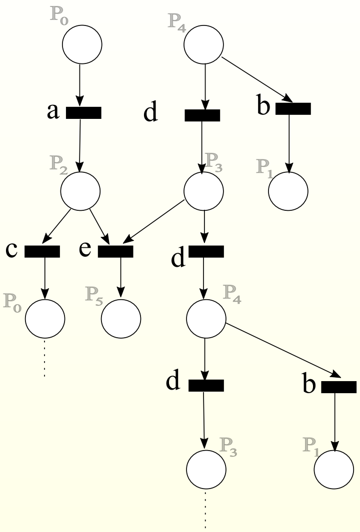
Unfolding & processes



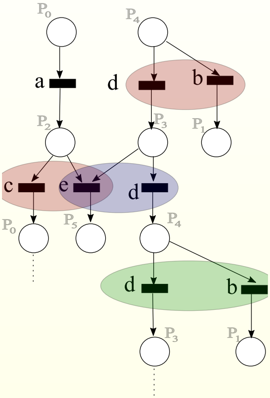
Unfolding & processes



Unfolding & processes



Unfolding & Processes



Conflicts

Two events e, f are conflicting if

- they are not causally related
- they have a common place in their past

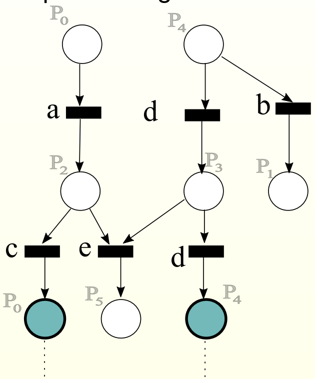
Processes in $\mathcal{U}_\mathcal{N}$

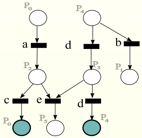
- $\mathcal{U}_\mathcal{N}$ is a graph
- Processes of $\mathcal{N}$ are projections of $\mathcal{U}_\mathcal{N}$ on maximal conflict-free sets of events & conditions

A grammar for unfolding

Idea of the construction :

Stop unfolding when reaching a marking already drawn





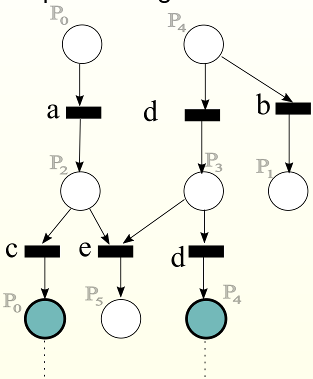
Close to Complete Finite Prefixes

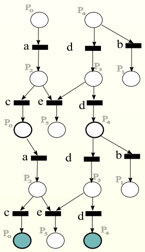
[*McMillan*95, *Esparza*02]

A grammar for unfolding

<u>Idea of the construction :</u>

Stop unfolding when reaching a marking already drawn



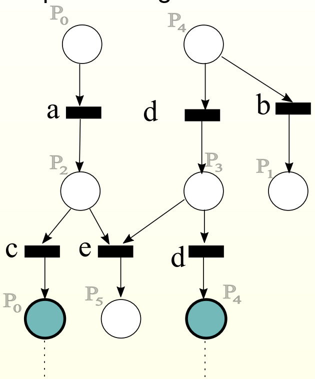


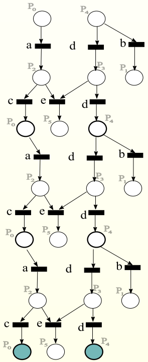
Close to Complete Finite Prefixes

$[McMillan95, Esparza02]$

A grammar for unfolding

<u>Idea of the construction :</u>
Stop unfolding when reaching a marking already drawn



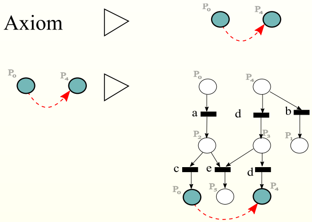


Close to Complete Finite Prefixes
[*McMillan*95, *Esparza*02]

Graph Grammars

Theorem

One can effectively build a graph grammar $\mathcal{G}_{\mathcal{N}}$ that generates $\mathcal{U}_{\mathcal{N}}$



Interesting...

Graphs generated by graph grammars have bounded treewidth

- size of the largest vertex set in a tree decomposition of the graph
- nb. colors needed to generate a graph with a simple graph algebra

MSO is decidable for graph grammars

Idea : translate ϕ to an equivalent MSO formula ... . but ...

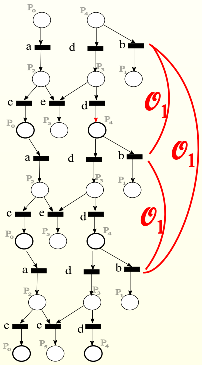
Isomorphism cannot be expressed in MSO.

Execution graph

Execution Graph

An unfolding, plus explicit representation of isomorphisms

$$G_{\mathcal{U}_{\mathcal{N}}} = \mathcal{U}_{\mathcal{N}} \uplus \{e \xrightarrow{i} f \mid \mathcal{O}_i(\downarrow e) \equiv \mathcal{O}_i(\downarrow f)\}$$



$\mathcal{O}_1$: erases occurrences of d

Proposition

There exist labeled safe Petri nets and observation functions whose execution graphs are not of bounded treewidth

From Hypol to MSO

Theorem

For every Hypol formula ϕ and every safe Petri net $\mathcal{N}$, there exists an MSO formula ψ such that $\mathcal{N} \models \phi$ iff $G_{\mathcal{U}_\mathcal{N}} \models \psi$

Proof idea :

- $e < f$, $e \leq f$, $x \leq_\mathcal{O} y$ expressible as an MSO property of $G_{\mathcal{U}_\mathcal{N}}$.
- $\mathcal{O}_i(\downarrow e) \equiv \mathcal{O}_i(\downarrow f)$ is a simple relation $e \xrightarrow{i} f$

Then inductive construction.

Example : $\phi = EX_{D,\mathcal{O}}\ \phi'$

Let x be a variable representing an event
C be a set of variable names already in use
$MSO(\phi, x, C) = \exists y, x \leq_\mathcal{O} y \wedge MSO(\phi, y, C')$
with

- y is a fresh variable name (w.r.t. C and to the set $C_{x \leq_\mathcal{O} y}$ of variables used to encode $x \leq_\mathcal{O} y$)
- $C' = C \cup \{y\} \cup C_{x \leq_\mathcal{O} y}$;

From Hypol to MSO

Immediate corollaries :

Corollary

Hypol $\setminus EX_{\equiv,\mathcal{O}_i}$ is decidable for safe Petri nets

Proof : Equivalence edges are not used. MSO decidable for graph grammars $[Courcelle90]$
Checking $\mathcal{N} \models \phi$ = checking $\mathcal{G}_{\mathcal{N}} \models MSO(\phi)$

Corollary

MSO is undecidable on execution graphs of safe Petri nets

Proof : Consistent with former theorems. Further $G_{\mathcal{U}_{\mathcal{N}}}$ may contain infinite grids minors (a condition for undecidability of MSO $[Robertson\&Seymour91]$)

Observable nets & Layeredness

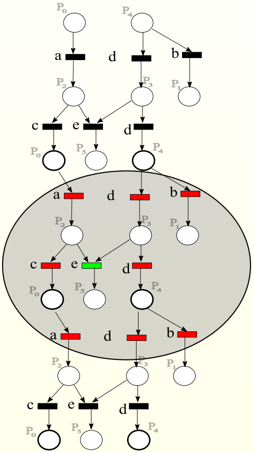
Distance between events

$dist(e,f)$ = maximal number of edges between $\{e,f\}$ and their common past

Balls

The $K - Ball$ of e in $\mathcal{U}_{\mathcal{N}}$ is the set

$$Ball_K(e) = \{f \in E \mid dist(e,f) \leq K\}$$

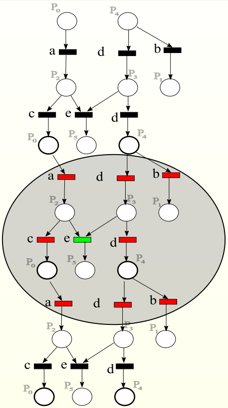


Equivalence decision on $K-$layered graphs

Definition : K-layeredness

$\mathcal{N}$ is $K-$layered for observations $\mathcal{O}_1, \ldots, \mathcal{O}_q$ iff :

- the $K-$ball of every event e of $\mathcal{U}_\mathcal{N}$ is finite
- $\forall \mathcal{O}_i, dist(e,f) > K$ implies $e \not\equiv_i f$
- $e \equiv_i f$ can be decided from the contents of $Ball_K(e)$ and $Ball_K(f)$



Proposition

Let $\mathcal{N}$ be a $K-$layered safe Petri net (w.r.t. $\mathcal{O}_1, \ldots, \mathcal{O}_g$). Then, one can effectively compute a graph grammar $\mathcal{G}_{K,\mathcal{N}}$ that recognizes $G_{\mathcal{U}_\mathcal{N}}$

<u>Proof idea :</u> Hyperedges memorize $K-$balls of maximal events.

Equivalence decision on K-layered graphs

Corollary

Hypol model checking is decidable for $K-$layered nets.

Open question

Is $K-$layeredness decidable ?

Theorem

Observable nets are $K-$layered for some $K \leq \max(2 \cdot k_c, 3 \cdot |T|)$

Corollary

Hypol model checking is decidable for Observable nets

Conclusion

Contributions

- A new partial order hyperlogic : Hypol
- Hypol Model checking decidable for $K-$Layered nets.
- A decidable subclass : Observable nets

Open questions

- Complexity ?
- Decidability of $K-$layeredness ?
- Unbounded Petri nets ?
- Other types of regular models ?

Bibliography

R. Alur, P. Cerný, and S. Chaudhuri.
Model checking on trees with path equivalences.
In *TACAS 2007*, volume 4424 of *LNCS*, pages 664–678. Springer, 2007.

B. Bérard, S. Haar, and L. Hélouët.
Hyper partial order logic.
Technical report, 2018.
https ://hal.inria.fr/hal-01884390.

B. Bérard, L. Hélouët, and J. Mullins.
Non-interference in partial order models.
ACM Trans. Embedded Comput. Syst., 16(2) :44 :1–44 :34, 2017.

M.R. Clarkson, B. Finkbeiner, M. Koleini, K.K. Micinski, M.N. Rabe, and C. Sánchez.
Temporal logics for hyperproperties.
In *POST*, pages 265–284, 2014.

M.R. Clarkson and F.B. Schneider.
Hyperproperties.
Journal of Computer Security, 18(6) :1157–1210, 2010.

B. Courcelle and J. Engelfriet.
Graph Structure and Monadic Second-Order Logic, a language theoretic approach.
Cambridge Univ. Press, 2012.

Bruno Courcelle.
The monadic second-order logic of graphs. i. recognizable sets of finite graphs.
Inf. Comput., 85(1) :12–75, 1990.

Bibliography

J. Engelfriet.
Branching processes of Petri nets.
Acta Inf., 28(6) :575–591, 1991.

J. Esparza, S. Römer, and W. Vogler.
An improvement of McMillan's unfolding algorithm.
Formal Methods in System Design, 20(3) :285–310, 2002.

J.A. Goguen and J. Meseguer.
Security policies and security models.
In *Proc. of IEEE Symposium on Security and Privacy*, pages 11–20, 1982.

A. Habel.
Hyperedge Replacement : Grammars and Languages, volume 643 of *LNCS*.
Springer, 1992.

P. Madhusudan and B. Meenakshi.
Beyond message sequence graphs.
In *FST TCS'01 : Foundations of Software Technology and Theoretical Computer Science*, volume 2245 of *LNCS*, pages 256–267. Springer, 2001.

H. Mantel.
Possibilistic definitions of security - an assembly kit.
In *Proc. of the 13th IEEE Computer Security Foundations Workshop, (CSFW'00)*, pages 185–199, 2000.

K.L. McMillan.
A technique of state space search based on unfolding.
Formal Methods in System Design, 6(1) :45–65, 1995.

Bibliography

B. Meenakshi and R. Ramanujam.
Reasoning about layered message passing systems.
Computer Languages, Systems & Structures, 30(3-4) :171–206, 2004.

D.A. Peled.
Specification and verification of message sequence charts.
In *FORTE/PSTV'00*, volume 183 of *IFIP Conference Proceedings*, pages 139–154. Kluwer, 2000.

N. Robertson and P.D. Seymour.
Graph minors. x. obstructions to tree-decomposition.
J. Comb. Theory, Ser. B, 52(2) :153–190, 1991.