TINA (Time Petri Net Analyser)
Vérification avec les outils TINA/Fiacre

Bernard Berthomieu Didier le Botlan
Silvano Dal Zilio François Vernadat

École d'été Temps Réel
Inria Rennes Bretagne Atlantique – Rennes 24-28 Août 2015

Processus de vérification

3 étapes :

Modélisation

$\Rightarrow$ modèle formel M de l'application
$\Rightarrow$ propriétés attendues P, dans la logique L

Abstraction

de M
préservant les formules de L
$\Rightarrow$ graphe d'états abstraits fini A

Vérification

des formules P sur A (Model-Checking)
$\Rightarrow$ VRAI ou un contre-exemple

Avec TINA

Modèles formels

- Réseaux de Petri Temporels + Priorités, Données, Chronomètres
- Descriptions de haut niveau en FIACRE (compilées)

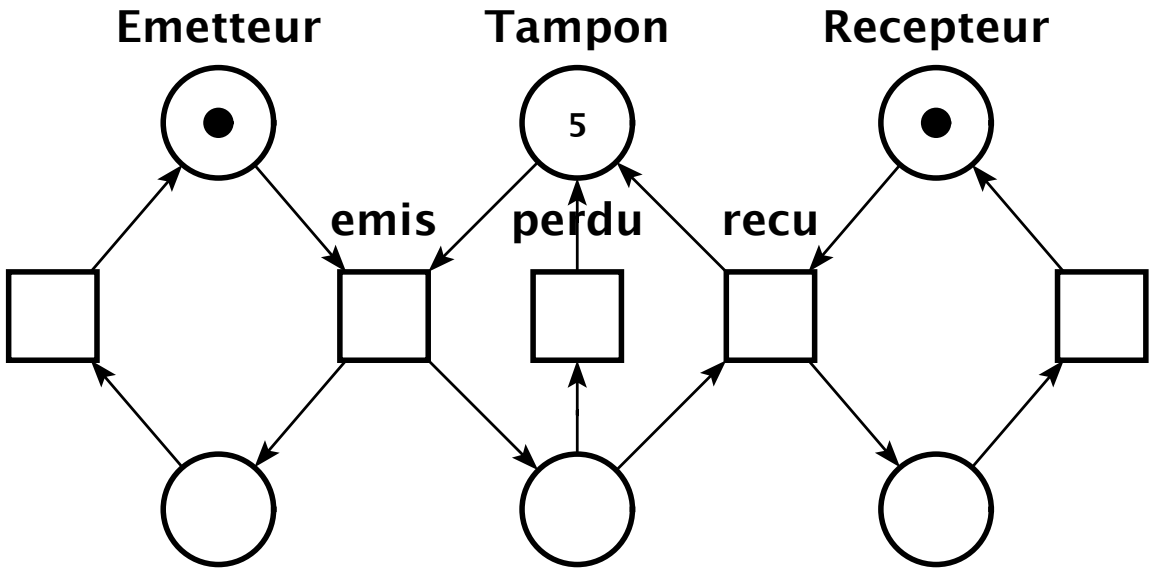
Abstractions

- Graphes de couverture
- Espaces d'états exacts
- Réductions ordre partiel
- Graphes de classes

Vérification

- State/Event LTL (natif)
- Mu-Calcul (natif)
- exportation abstraction vers outils CADP, MEC

Réseaux de Petri



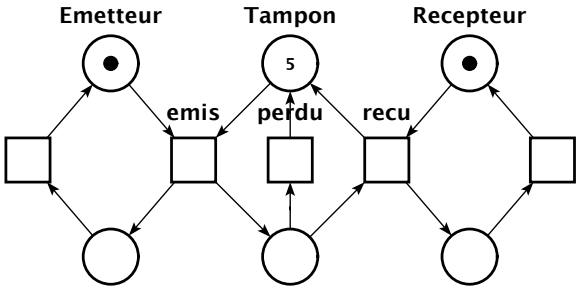
Places = conditions

Transitions = transforment les conditions

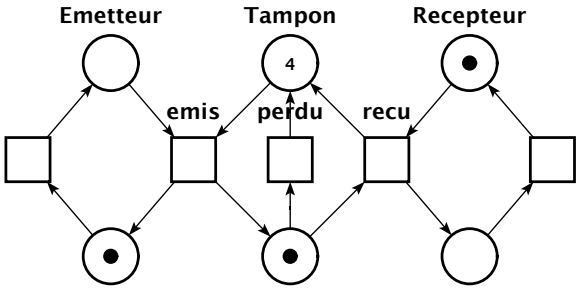
Si $Pre(t) \geq M$ alors $M \xrightarrow{t} M - Pre(t) + Post(t)$

Expriment nativement choix ET parallélisme

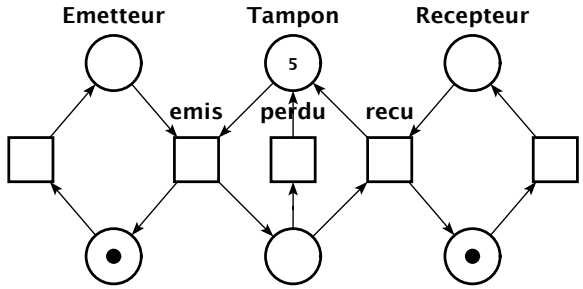
États (marquages) et transitions d'états



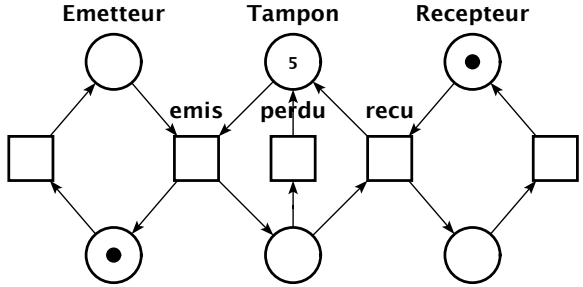
emis



recu



perdu



Propriétés des réseaux de Petri

Générales

borné : le marquage de toute place est borné

quasi-vivant : toute transition est tirable depuis un marquage atteignable

pseudo-vivant : absence de blocages

vivant : toute transition est quasi-vivante depuis tout marquage

reïnitialisable : on peut toujours retrouver le marquage initial

Spécifiques

Atteignabilité : est ce que m est atteignable ?

Propriétés plus riches exprimées en logiques temporelles

par ex. $\Box(t1 \Rightarrow \Diamond(p2 \geq p3 + p4 \vee p6))$

Réseaux de Petri – Abstractions

Abstractions

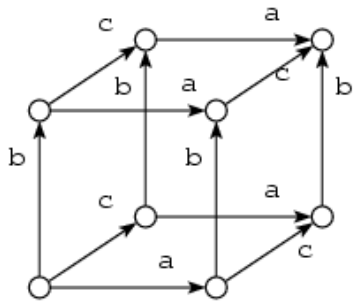
- Graphes de couverture (bornes sup, détectent places non bornées)
- Graphes des marquages (espace d'états exact)
- Réductions ordre partiel
  - Ensembles persistants (blocages)
  - Pas couvrants (blocages+)
  - Pas persistants (blocages+)
- Analyse structurelle
  - Surapproximations par ensembles semi-linéaires

Aussi ...

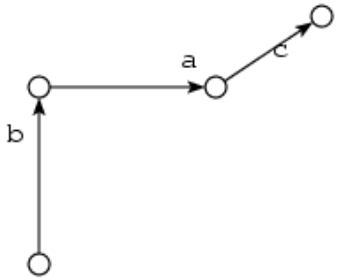
- Méthodes symboliques (SDD)

Réductions ordre partiel

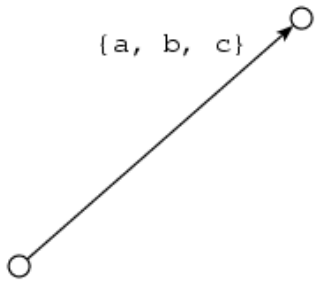
Explorations implicites



Exhaustif :
2^n états, $n \times 2^{n-1}$ transitions

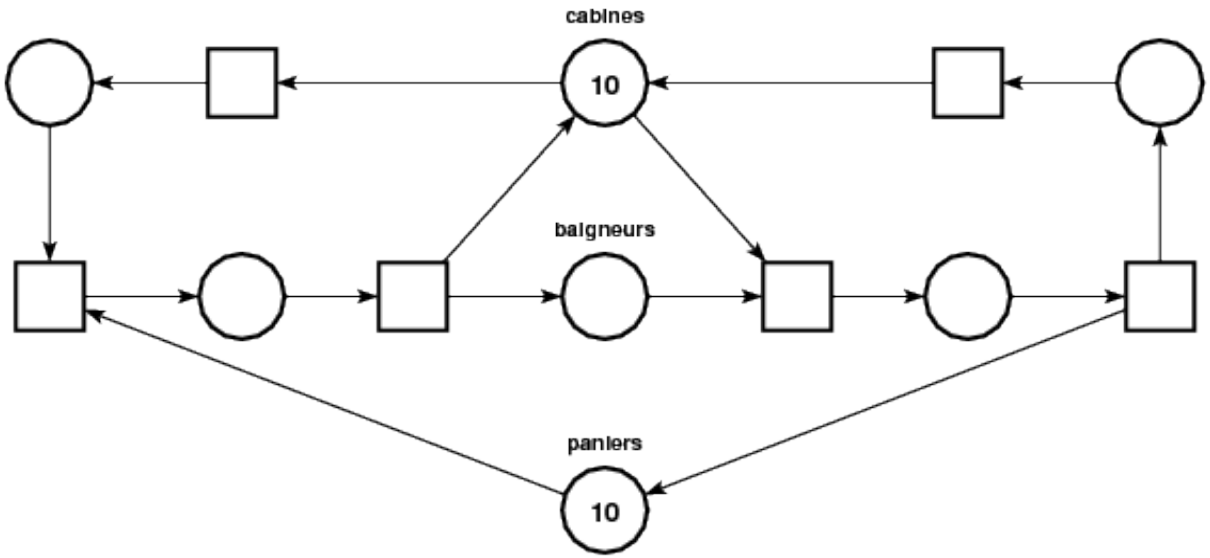


Ensembles persistants :
$(n+1)$ états, n transitions



Graphes de pas couvrants :
2 états, 1 transitions

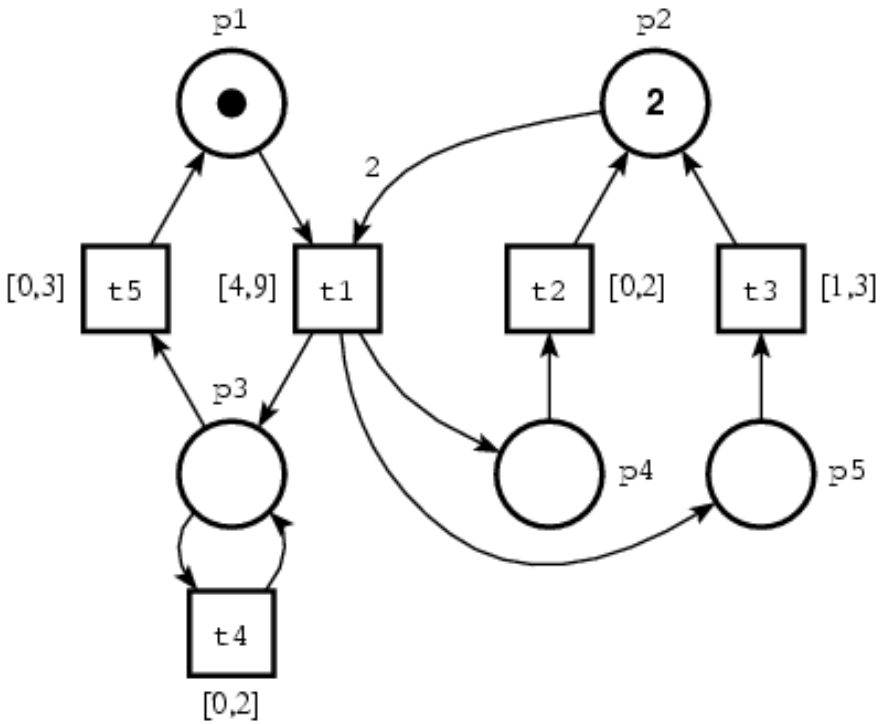
Piscine



		Exact tina -R	*Pas couvrants* tina -V	*Ens persistants* tina -P	*Pas persistants* tina -Q
$K = 10$	*Etats*	7006	367	97	87
	s	0	0	0	0
$K = 100$	*Etats*	$\sim 280M$	39517	997	897
	s	8800	0.3	0	0
$K = 1000$	*Etats*	?	$\sim 4M$	9997	8997
	s	?	30	0	0
$K = 10000$	*Etats*	?	$\sim 400M$	99997	89997
	s	?	4500	0.5	0.5

Réseaux Temporels (Merlin 74)

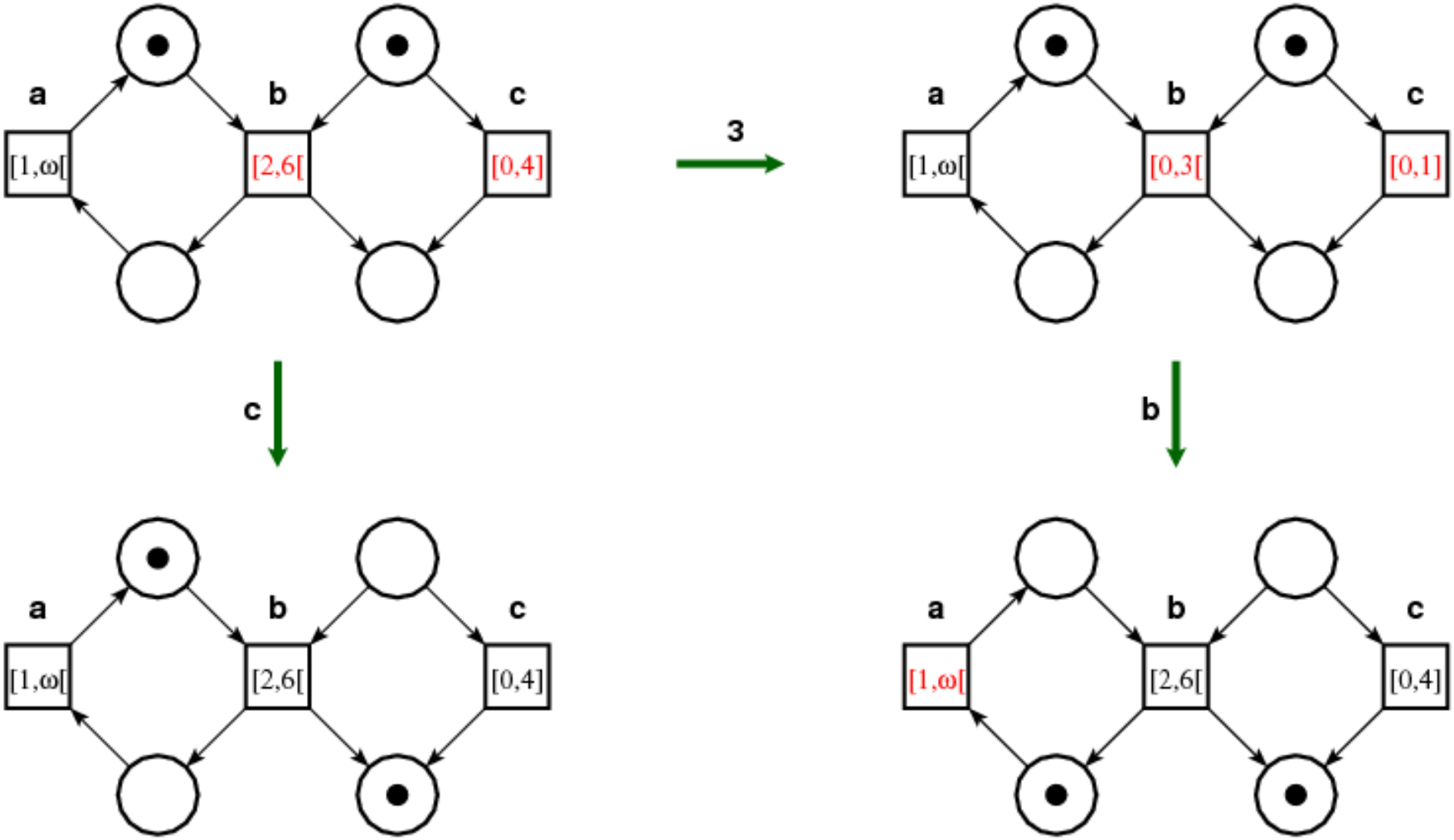
RdP + Intervalles temporels



Espaces d'états infinis (temps dense)

Caractère borné indécidable (mais conditions suffisantes)

États et transitions d'états



États et transitions d'états

$E_0 = (m_0, I_0)$

m_0 : $p_1, p_2(2)$
I_0 : *solutions en* t_1 *of*

$$4 \leq t_1 \leq 9$$

$E_0 \xrightarrow{t_1 @ \theta_1} E_1 = (m_1, I_1)$ avec $(\theta_1 \in [4, 9])$:
m_1 : p_3, p_4, p_5
I_1 : *solutions en* (t_2, t_3, t_4, t_5) *of*

$$0 \leq t_2 \leq 2$$
$$1 \leq t_3 \leq 3$$
$$0 \leq t_4 \leq 2$$
$$0 \leq t_5 \leq 3$$

$E_1 \xrightarrow{t_2 @ \theta_2} E_2 = (m_2, I_2)$ avec $(\theta_2 \in [0, 2])$:
m_2 : p_2, p_3, p_5
I_2 : *solutions en* (t_3, t_4, t_5) *of*

$$\max(0, 1 - \theta_2) \leq t_3 \leq 3 - \theta_2$$
$$0 \leq t_4 \leq 2 - \theta_2$$
$$0 \leq t_5 \leq 3 - \theta_2$$

L'échéancier $(t_1.t_2, 5.0)$ est tirable.

TPNs – Abstractions

Abstractions : Graphes de classes d'états

Classe d'état = ensemble d'états

classe = marquage (état discret) + polyèdre (information temporelle)

Differentes constructions, préservant :

Marquages + traces (LTL) (SCG [BM83] [BD91])

Marquages ($SCG_{\subset}$)

Marquages + états + traces (SSCG [BV03])

Marquages + états ($SSCG_{\subset}$)

Marquages + états + traces + branchements (CTL^*) (ASCG [BV03])

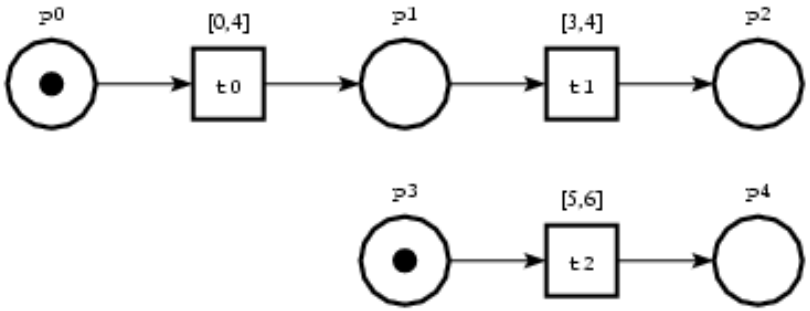
Aussi :

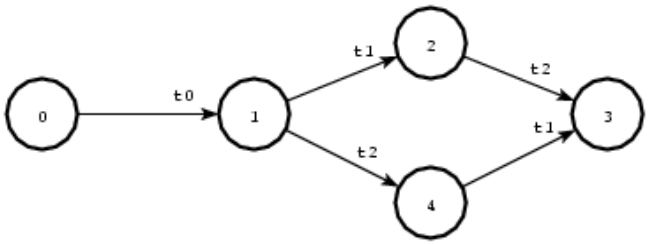
Espaces d'états en temps discret

Méthodes symboliques (BDD, préservent Marquages)

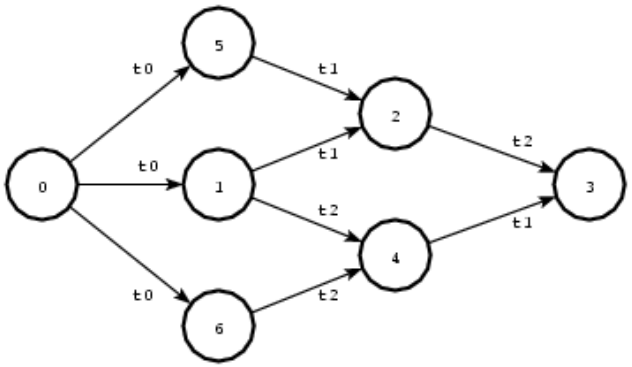
Théorème : Abstractions finies ssi réseau est borné

Exemples



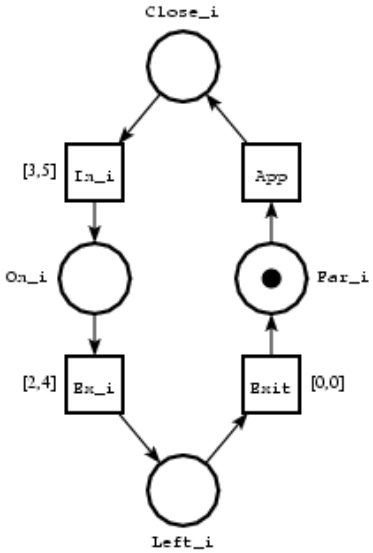


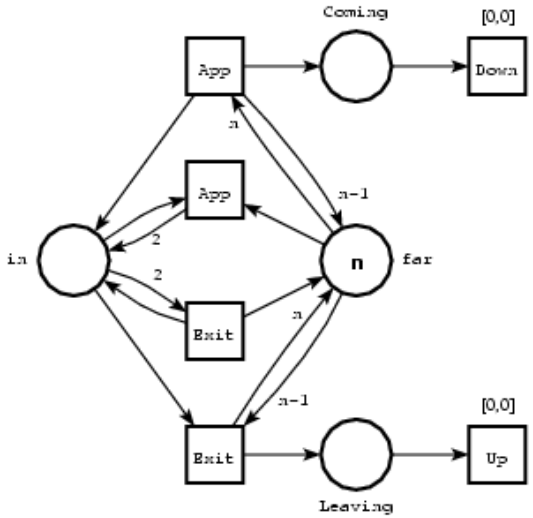
$C_0 = (p_0\ p_3, \{0 \leq t_0 \leq 4, 5 \leq t_2 \leq 6\})$
$C_1 = (p_1\ p_3, \{3 \leq t_1 \leq 4, 1 \leq t_2 \leq 6\})$
$C_2 = (p_2\ p_3, \{0 \leq t_2 \leq 3\})$
$C_3 = (p_2\ p_4, \{\})$
$C_4 = (p_1\ p_4, \{0 \leq t_1 \leq 3\})$

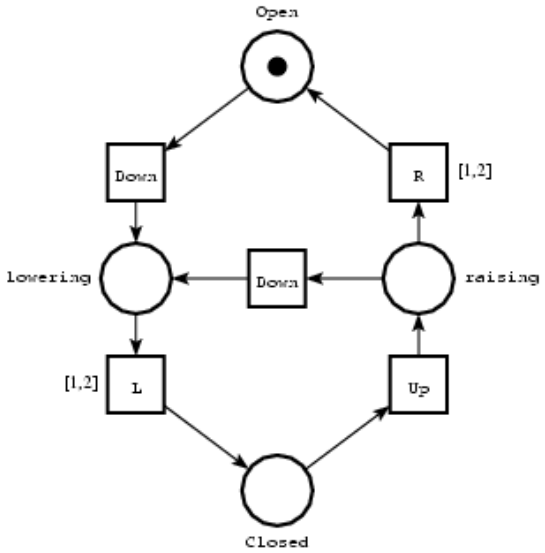


$C_0 = (p_0\ p_3, \{0 \leq t_0 \leq 0, 0 \leq t_2 \leq 0\})$
$C_1 = (p_1\ p_3, \{0 \leq t_1 \leq 0, 1 \leq t_2 \leq 3\})$
$C_2 = (p_2\ p_3, \{3 \leq t_2 \leq 6\})$
$C_3 = (p_2\ p_4, \{\})$
$C_4 = (p_1\ p_4, \{1 \leq t_1 \leq 4\})$
$C_5 = (p_1\ p_3, \{0 \leq t_1 \leq 0, 0 \leq t_2 < 1\})$
$C_6 = (p_1\ p_3, \{0 \leq t_1 \leq 0, 3 < t_2 \leq 4\})$

Passage à niveau



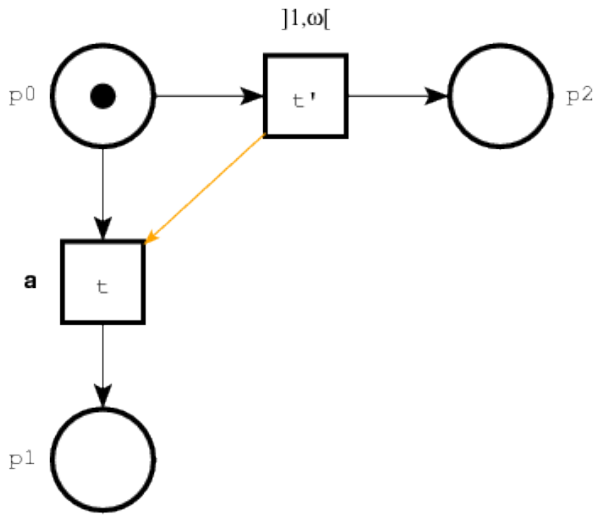




		M tina -M	*M* + *LTL* tina -W	*E* tina -E	*E* + *LTL* tina -S	*E* + *CTL* tina -A	*M* + *LTL* (*discret*) tina -D	*M* + *LTL* (*discret*) tina -F
(1 *train*)	*Classes*	10	11	10	11	12	13	23
	Transitions	13	14	13	14	16	27	36
(2 *trains*)	*Classes*	37	123	41	141	195	116	382
	Transitions	74	218	82	254	849	198	373
(3 *trains*)	*Classes*	172	3101	232	5051	6973	1550	2280
	Transitions	492	7754	672	13019	49818	5823	5275
(4 *trains*)	*Classes*	1175	134501	1807	351271	356940	22268	28830
	Transitions	4534	436896	7062	1193376	1447835	91256	81077
(5 *trains*)	*Classes*	10972	855762	18052	35945411	23081275	313214	372264
	Transitions	53766	34337748	89166	151908273	279572133	1397517	1245355
(6 *trains*)	*Classes*	128115	697913229	217647	?	?	4299116	4830558
	Transitions	760538	3334109864	1297730	?	?	20886774	18833697

Priorités

Réseaux Temporels + Priorités (PrTPN)



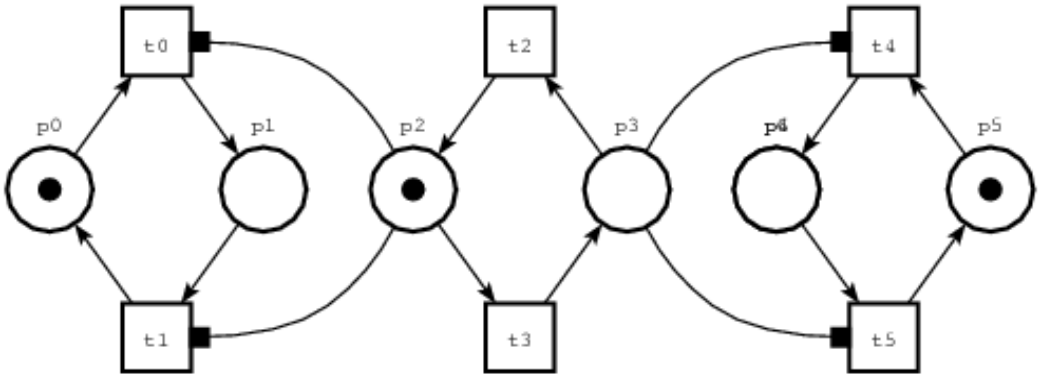
Priorités augmentent l'expressivité des TPN (PrTPN bornés $\approx$ TA)
Pour PrTPN, l'écoulement du temps peut rendre une transition non tirable

Abstractions

Classes d'états restent applicables (SSCG, ASCG, mais pas SCG)

Suspension et reprise de transitions

Réseaux Temporels à Chronomètres (SwTPN)



Une transition sensibilisée peut être *Active* ou *Suspendue*

Applications : systèmes ordonnancés, préemption temporelle

Abstractions

Graphes de classes adaptables, MAIS accessibilité indécidable ...

Surapproximations fournissent des conditions suffisantes ou nécessaires

Prise en compte des données

Time Transition System =

Systèmes de Keller

marquages $\Rightarrow$ états (vecteurs d'entiers)
transitions "additives" $\Rightarrow$ transitions arbitraires

\+ **contraintes temporelles à la TPN**

On perd : décidabilité du caractère borné

en Tina :

format tts = TPN + traitement de données synchronisé (en C)

Abstractions

Méthode des classes d'états reste applicable

Vérification – State/Event-LTL (CMU)

Propositions atomiques

d'états (marquages des places)

de transitions (transitions tirables)

Opérateurs logiques et temporels

Trace = suite alternée infinie d'états et de transitions

	(Pour toute trace)
P	P vraie dans le premier état (transition)
$\bigcirc P$	P vraie dans le prochain état (transition)
$\Box P$	P vraie dans tout état (transition)
$\Diamond P$	P vraie dans un état (transition) au moins
$\Box\Diamond P$	P vraie infiniment souvent
$\Box(P \Rightarrow \Diamond Q)$	Q "répond" à P

Specification patterns : http ://patterns.projects.cis.ksu.edu

Le vérificateur SELT

Formules

S/E-LTL + arithmétique, e.g.

$\Box(t1 \Rightarrow \Diamond(p2 \geq p3 + p4 \vee p6))$

Contre exemples Abrégés

```
- [] (t1 => <> t4);
FALSE
  state 0: p1 p2*2
  -t1 ... (preserving - t4 /\ t1)->
* [accepting] state 12: p3 p4 p5
  -t5 ... (preserving - t4)->
  state 12: p3 p4 p5
```

Peuvent être rejoués dans le simulateur Tina

TINA Toolbox (http ://www.laas.fr/tina)

nd (**n**et**d**raw)

- Graphic and textual editor
- Of Time Petri Net or Transition Systems
- Drawing, printing functions
- Interfaced with other tools

tina, sift (state space generators)

- Input : Petri nets + time, priorities, preemption, data (API)
- Builds : behavior abstractions, Preserving some classes of properties
- Output : in verbose form or in model-checkers formats

selt, muse

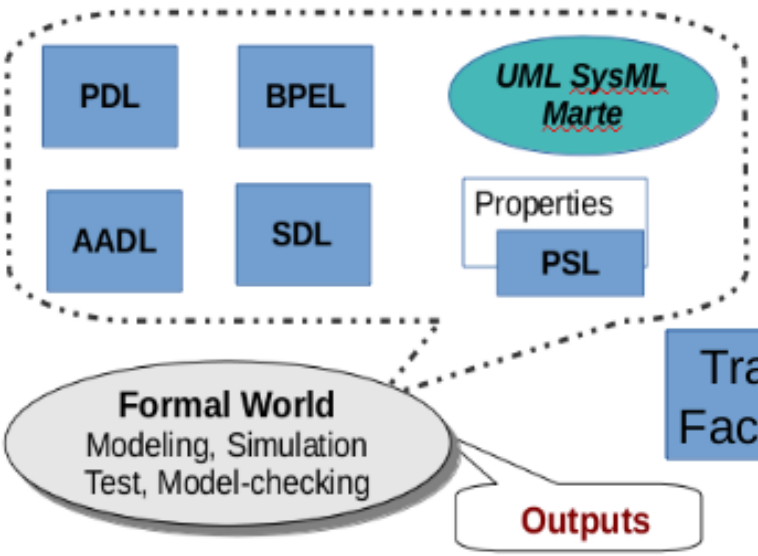
- Model checkers for State/Event-LTL temporal logic and modal mu-calculus

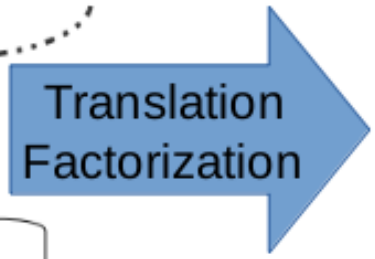
struct, plan, etc

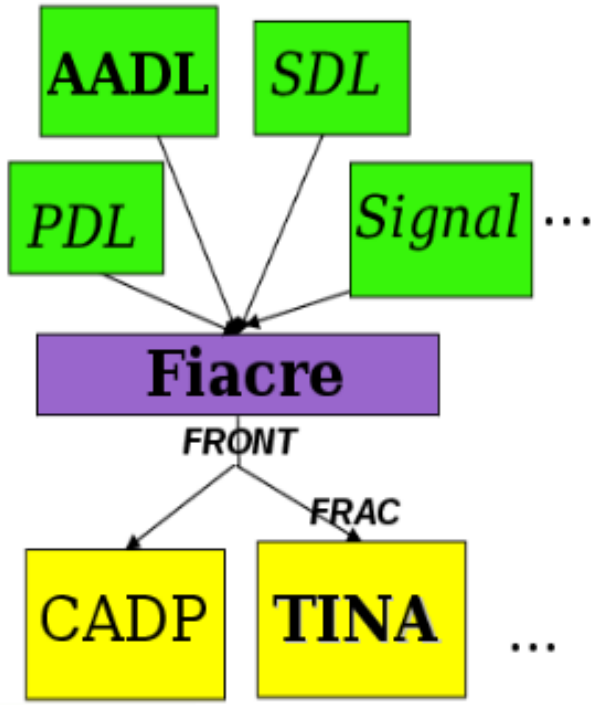
- Structural analysis, Path analysis, converters, etc

Descriptions de haut niveau — FIACRE

FIACRE "Intermediate Format for the Embedded Distributed Component Architectures"







Initiallement défini avec
IRIT/Acadie,
INRIA/Vasy-Convecs

Fiacre Features

Formally defined (semantics, compositional)

Strongly typed Rich set of primitive data types

Processes (basic components)

Parameterized labelled automata

State transitions expressed symbolically ; high-level constructions

Labels for communication and/or synchronization

May share variables with other components

Components

Hierarchically defined

Specify interactions between components or process instances

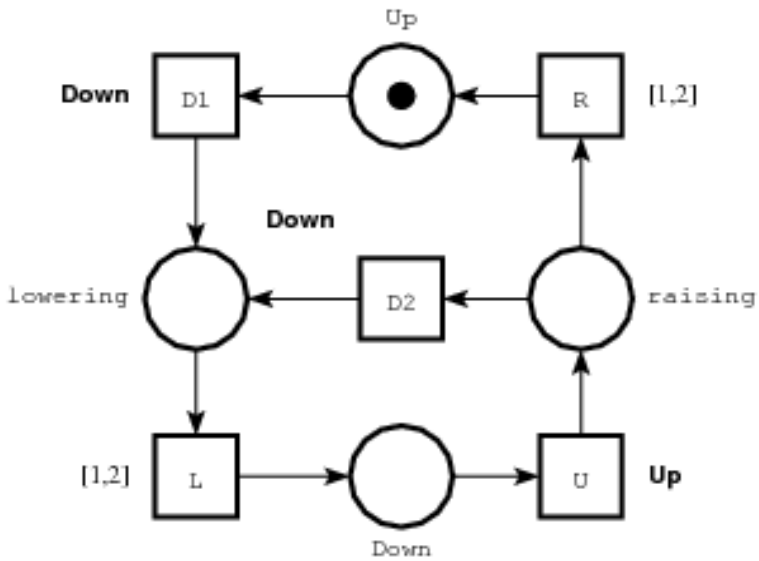
Constrain interactions (time, priorities)

Control scope of shared variables

FIACRE : exemple

```
process barrier_p [Down,Lower,Up,Raise: sync] is
  states up lowering down raising
  init up
  from up       Down; to lowering
  from lowering Lower; to down
  from down     Up; to raising
  from raising  select Raise; to up
                []     Down; to lowering
                end

component barrier [Down,Up: sync] is
  port Lower, Raise : none in [1,2]
  barrier_p [Down, Lower, Up, Raise]
```



Prospective

Fiacre

- Edition & Simulation
- Interprétation des résultats de vérification au niveau Fiacre
- Connexions amont : AADL, SysML, Mauve, . . .

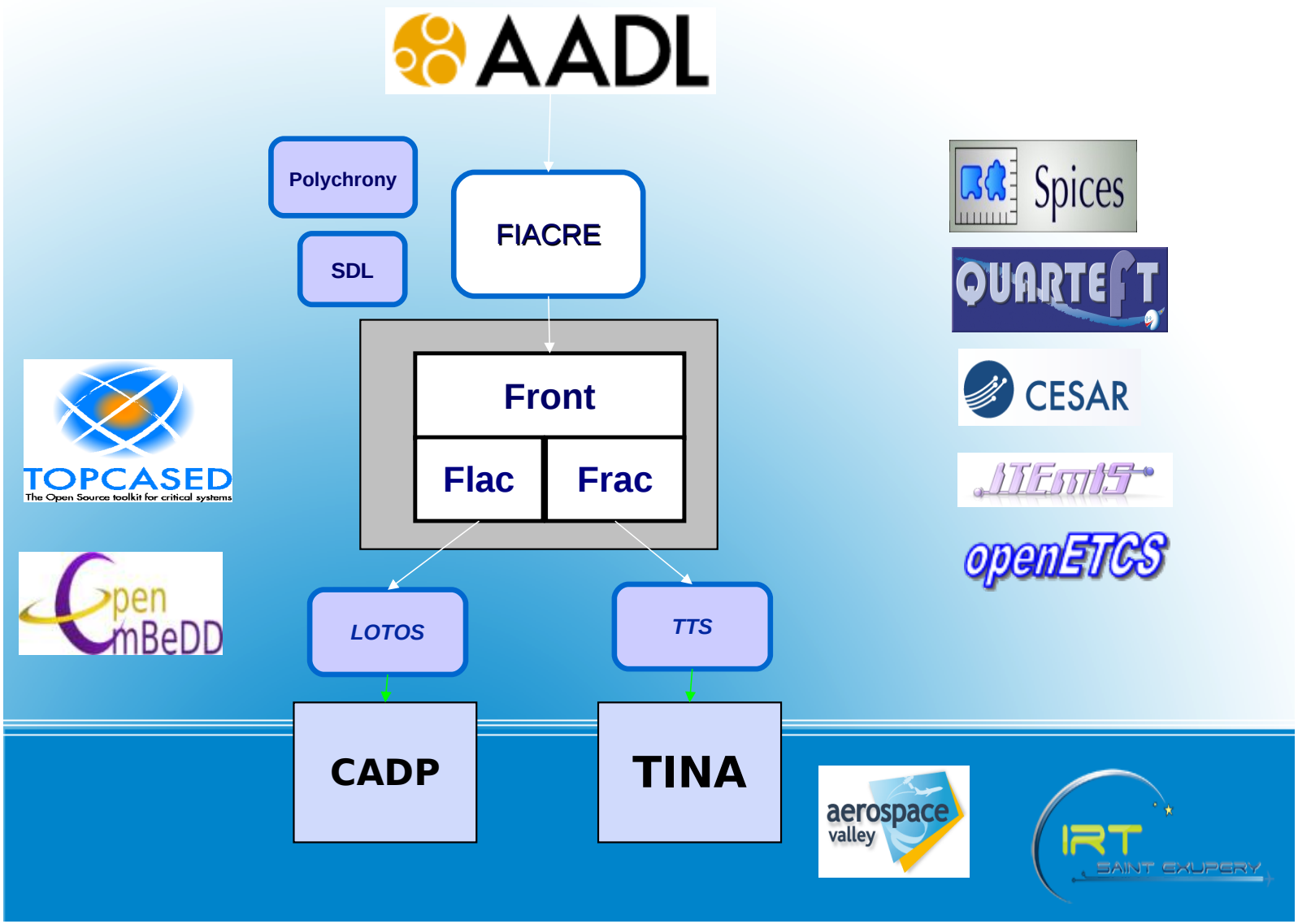
Passage à l'échelle

- Parallélisation : Exploration et vérification
- Représentation symbolique (diagrammes de décision)
- Vérification compositionnelle
- .../...

Optimisation de modèles

- Simplification de modèles (réductions, etc)
- Prise en compte informations spécifiques (symétries, invariants)
- Interprétation abstraite, pour systèmes infinis (Fiacre)

Projets


AADL
Polychrony
SDL
FIACRE
Front
Flac
Frac
LOTOS
TTS
CADP
TINA
Spices
QUARTEFT
CESAR
ITEmIS
openETCS
TOPCASED
The Open Source toolkit for critical systems
Open
mBeDD
aerospace
valley
IRT
SAINT EXUPERY

Liens

Outils

http://www.laas.fr/tina

http://www.laas.fr/fiacre

Projets

Topcased : www.topcased.org

Spices : www.spices-itea.org

OpenEmbeDD : openembedd.org

Itemis : itemis-anr.org

Quarteft : quarteft.loria.fr

CESAR : www.cesarproject.eu/

OpenETCS : openetcs.org/

INGEQUIP, MOISE : www.irt-saintexupery.com/