L'outil TINA

Construction d'espaces d'états abstraits
pour la vérification de systèmes critiques

B. Berthomieu, F. Peres, P-O. Ribet, F. Vernadat
CNRS/LAAS

Ecole d'Eté Temps Réel
Nancy /2005

Boite à outils Tina

tina (**TI**me petri **N**et **A**nalyser)

- Modèles décrits sous forme graphique ou textuelle
- Génère graphes de comportements
- Préservant certaines familles de propriétés
- Sortie en clair ou formats dédiés pour analyseurs

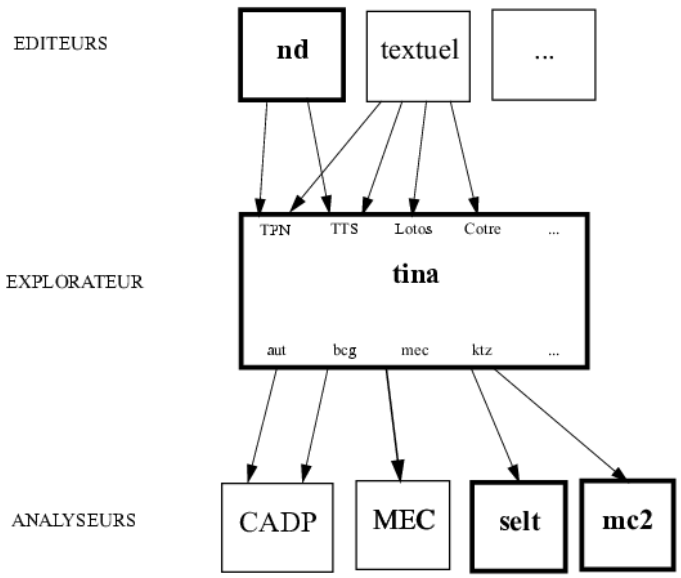
nd

- Editeur graphique et textuel
- De réseaux de Petri et d'automates
- Fonctions de dessin, d'impression
- Interfacé avec tina

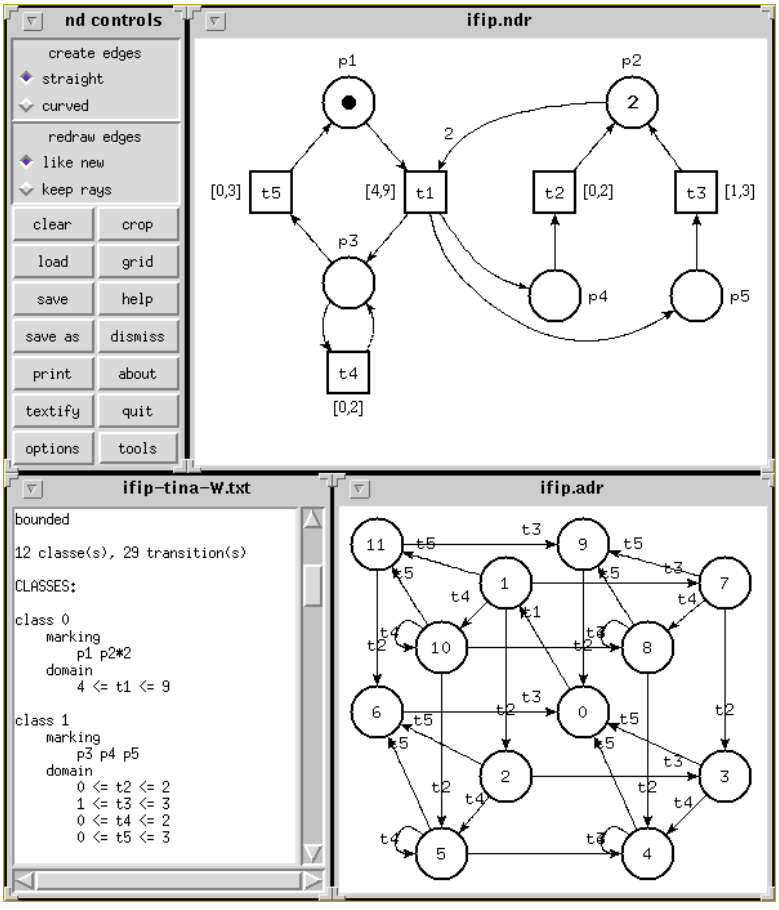
struct, setl, mc2, ktzio, bldio, ...

- Analyse structurelle, Model-checkers, convertisseurs, etc

Boite à outils Tina



nd



Module d'exploration tina

Modèles

Réseaux de Petri {Temporels {à Chronomètres}}

Réseaux Prédicats/Actions {Temporels {à Chronomètres}}

Systèmes de transitions temporisés : Cotre, RT-Lotos, etc

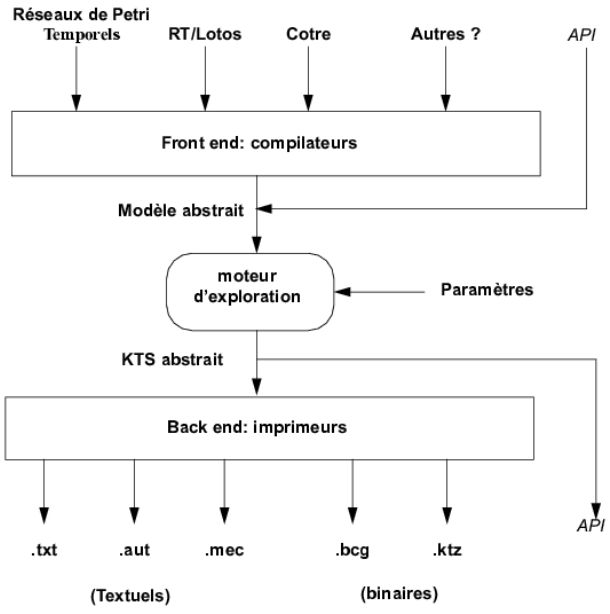
Constructions

Abstractions de graphes d'états discrets

Abstractions de graphes d'états temporisés

Abstraction = représentation finie, préservant certaines propriétés

Module d'exploration tina



Marquages, Couvertures

Graphes de couverture (Karp/Miller)

Détecte places non bornées

Si aucune, alors produit graphe des marquages

Sinon produit graphe (non unique) de couverture

Plusieurs heuristiques

Graphes des marquages

Diverses conditions d'arrêt

Construit simultanément graphe des CFCM

Diagnostic de vivacité

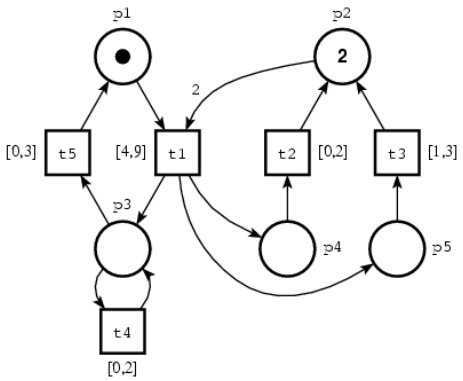
Limites : 10^6 à 10^7 marquages

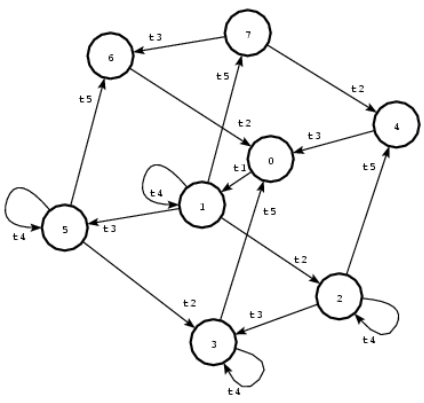
KTS, exemple

Graphes des marquages

```
MARKINGS:
0 : p1 p2*2
1 : p3 p4 p5
2 : p2 p3 p5
3 : p2*2 p3
4 : p1 p2 p5
5 : p2 p3 p4
6 : p1 p2 p4
7 : p1 p4 p5

REACHABILITY GRAPH:
0 -> t1/1
1 -> t2/2, t3/5, t4/1, t5/7
2 -> t3/3, t4/2, t5/4
3 -> t4/3, t5/0
4 -> t3/0
5 -> t2/3, t4/5, t5/6
6 -> t2/0
7 -> t2/4, t3/6
```

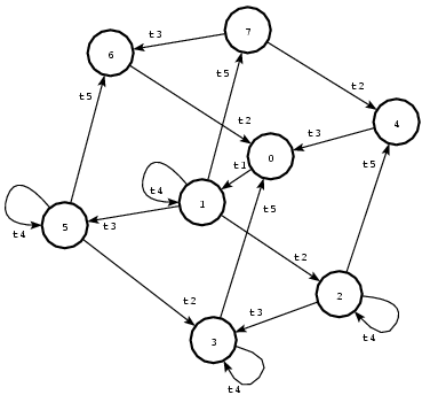




Ou au format Aldébaran (.aut)

(sans propriétés d'états)

```
des(0,17,8)
(0, "t1", 1)
(1, "t2", 2)
(1, "t3", 5)
(1, "t4", 1)
(1, "t5", 7)
(2, "t3", 3)
(2, "t4", 2)
(2, "t5", 4)
(3, "t4", 3)
(3, "t5", 0)
(4, "t3", 0)
(5, "t2", 3)
(5, "t4", 5)
(5, "t5", 6)
(6, "t2", 0)
(7, "t2", 4)
(7, "t3", 6)
```



Ou en formats binaires

Formats de stockage et d'échange

BCG (Outils CADP)

Accès aux outils CADP

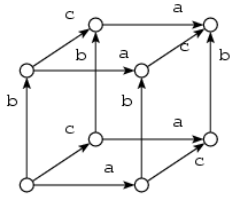
KTZ (Kripke Transition Systems compressés)

Code propriétés d'états ET de transitions

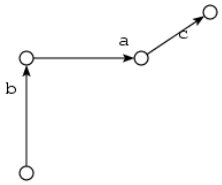
e.g. 135000 états, 450000 transitions, en 1Mo
avec 24 pa. d'états et 29 pa. de transitions

Explorations partielles

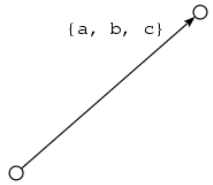
Idée : Ne pas explorer un chemin qui ne peut affecter les propriétés à préserver



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



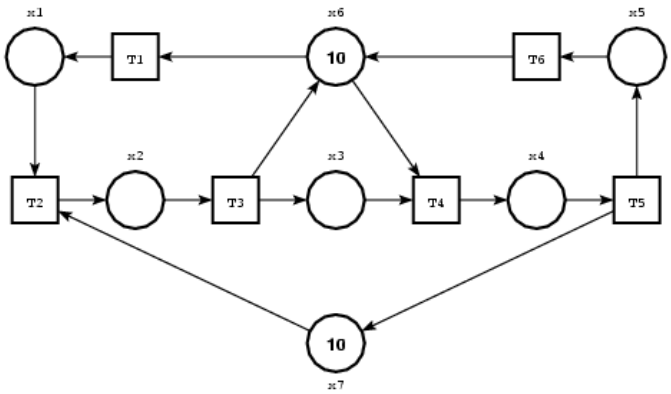
Ensembles persistants :
$(n+1)$ états, n transitions
(VALMARI, GODEFROID)



Graphes de pas couvrants :
2 états, 1 transitions
(VERNADAT)

Exemple

Piscine



Résultats

K	10		235		500	
Exhaustif	7006	0.6s	?	?	?	?
Persistants	857	0s	4.6M	9h	?	?
Pas couvrants	367	0s	220K	92s	1M	31s
Pas persistants	87	0s	2112	1s	4497	2s

Graphes de Pas Couvrant

Différentes abstractions:

ICATPN 1996 Graphes de Pas Couvrant

– Généraux: Blocage + Traces Maximales

–Bisimulation Faible

ICATPN 1997

– Equivalences de Refus

Thèse de P.O Ribet

– Graphes de Pas Persistants : Blocage [Forte 2002]

– Préservation de LTL

Graphes de classes d'états

Réseaux Temporels (Merlin 1974) **et extensions**

Avec suspension/Reprise des transitions (chronomètres)

Avec Données (Cotre, RT-Lotos, etc)

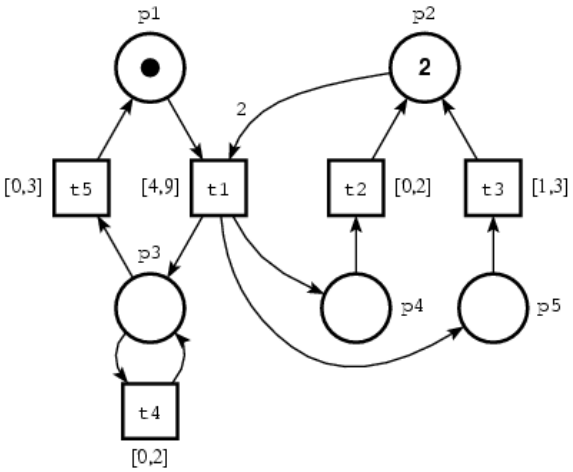
Abstractions préservant LTL (IFIP83, IEEE91)

Avec ou sans multi-sensibilisation (MSR01)

Abstractions préservant la bisimilarité (CTL^***)** (TACAS03)

Réseaux Temporels

(Time Petri Nets, Merlin 74)



$(P, T, \mathbf{Pre}, \mathbf{Post}, M_0, I_s)$, où

- $(P, T, \mathbf{Pre}, \mathbf{Post}, M_0)$ est un RdP
- I_s : application *Intervalle Statique*

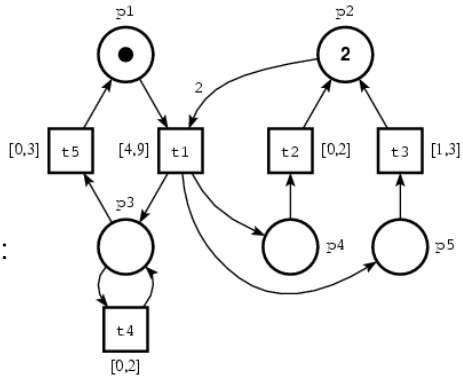
  $t \mapsto I_s(t) \subseteq R^+$, borne(s) rationnelle(s)

Exemples

$E_0 = (m_0, I_0)$

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

$4 \leq t_1 \leq 9$



$E_0 \xrightarrow{t_1@\theta_1} E_1 = (m_1, I_1)$ 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) de

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

$E_1 \xrightarrow{t_2@\theta_2} E_2 = (m_2, I_2)$ avec $(\theta_2 \in [0, 2])$:

m_2 : p_2, p_3, p_5
I_2 : solutions en (t_3, t_4, t_5) de

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

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

Espace d'états accessibles

Etats : $E = (m, I)$: marquage $\times$ vecteur d'intervalles

Espace des états accessibles : $SG = (S, \xrightarrow{t@\theta}, s_0)$, avec :

$S = \{s \mid s_0 \xrightarrow{*} s\}$, états accessibles depuis s_0

$s_0 = (m_0, I_0)$, état initial ($I_0(t) = I_s(t)$ pour toute t sensibilisée par m)

Graphes de classes d'états

Recouvrements de SG par ens. convexes d'états ayant même marquage

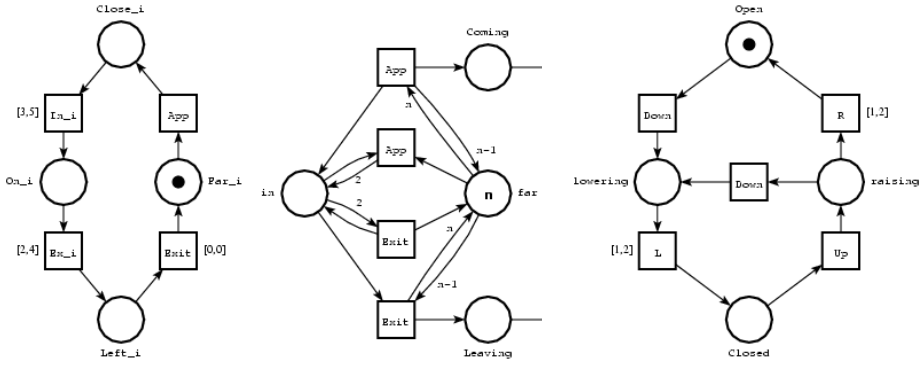
munis de $\xrightarrow{t}$: $c \xrightarrow{t} c'$ ssi $(\exists s \in c)(\exists s \in c')(\exists \theta)(s \xrightarrow{t@\theta} s')$

Plusieurs recouvrements possibles

Préservant propriétés LTL [BB & MM, IFIP 83]

Préservant propriétés CTL^* [BB & FV, TACAS 03]

Exemple : Passage à niveau



		$LSCG$	$SSCG$	$ASCG$
(1 *train*)	$Classes$	11	11	11
	$Edges$	14	14	15
	$CPU(s)$	0.00	0.00	0.00
(2 *trains*)	$Classes$	123	141	192
	$Edges$	218	254	844
	$CPU(s)$	0.00	0.01	0.02
(3 *trains*)	$Classes$	3101	5051	6966
	$Edges$	7754	13019	49802
	$CPU(s)$	0.13	0.29	2.95
(4 *trains*)	$Classes$	134501	351271	356940
	$Edges$	436896	1193376	3447624
	$CPU(s)$	10.99	42.34	458.36

Prise en compte des données

Des réseaux de Petri aux systèmes de transitions de Keller

marquages ⇒ états (vecteurs d'entiers)

transitions "additives" ⇒ transitions arbitraires

On perd : décidabilité du caractère borné et de la vivacité

Des systèmes de Keller aux TTS (Henzinger/Manna/Pnueli)

Timed Transition System = Keller + intervalles temporels

Méthode des classes d'états reste applicable

TTS abstraits

API

État initial

Ensemble fini de transitions, chacune avec :

- Un intervalle temporel
- Fonction Précondition
- Fonction de changement d'état
- Relation de Conflit

Fonctions auxiliaires (impression, etc)

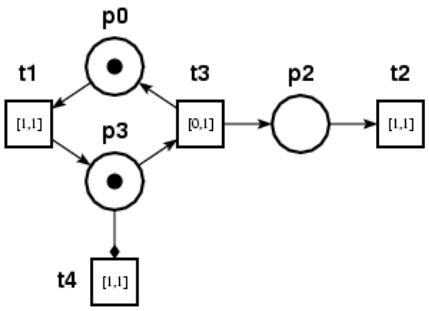
Mise en œuvre

Réseaux de Petri Prédicats/Actions :

Réseau de Petri + librairie conforme à l'API

Suspension et reprise de transitions

Réseaux Temporels à Chronomètres

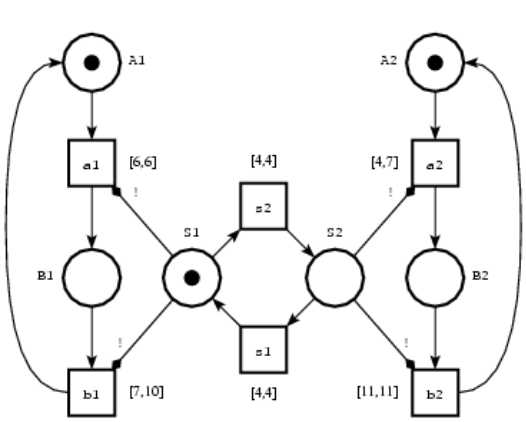


$(P, T, \mathbf{Pre}, \mathbf{Sw}, \mathbf{Post}, M_0, I_s)$, oú

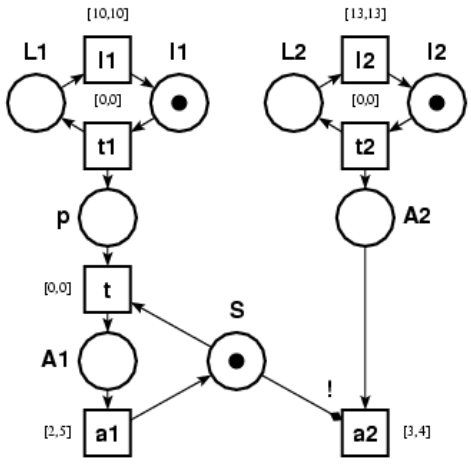
- $(P, T, \mathbf{Pre}, \mathbf{Post}, M_0)$: un réseau de Petri
- I_s : fonction *Intervalle statique*
- $\mathbf{Sw}$: fonction Chronomètre

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

Exemple, politiques d'ordonnancement



Round-Robin



Rate-monotonic

Méthodes d'analyse

Méthode des classes d'états adaptable

Termine souvent in pratique, MAIS graphes de classes peuvent être infinis

En fait : accessibilité d'état est indécidable, même si réseau borné !

Surapproximations de l'espace d'états

Caractérisent des espaces d'états contenant au moins les états accessibles

Graphes fini si le réseau est borné

Fournissent des conditions suffisantes ou nécessaires

SE-LTL Model-Checking (Shaki/Clarke/etc, CMU)

Propositions atomiques

d'états
de transitions

booléennes ($s34$, $t12$, $idle$, ...)
entières ($x \leq y + 2$, $s12 \geq 4.z$, ...)
autres ...

Opérateurs logiques et temporels

$\neg, \vee, \wedge, \Rightarrow$, ...
$\Box$ (always)
$\Diamond$ (eventually)
$\bigcirc$ (next)
U (until)

Interprétation

Systèmes de transitions de Kripke (kts)

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

$\Box(S \wedge \bigcirc\Diamond T \Rightarrow \bigcirc\Diamond(T \wedge \Diamond P))$ P "répond" à S, T

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

SELT, Commandes

Expressions SE-LTL

Propositions atomiques (trouvées dans le fichier ktz)

Opérateurs arithmétiques et logico arithmétiques

Opérateurs logiques et temporels

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

Commandes

évaluer une expression, retourne T ou contre exemple

déclarer un opérateur (prefixe, infixe ou fonctionnel)

traiter une directive (source, output, etc)

Exemple

Contre exemple

```
- output fullproof;
fullproof output set

- [] (t1 => <> t4);
FALSE
  state 0: p1 p2*2
  -t1->
* [accepting] state 12: p3 p4 p5
  -t5->
  state 13: p1 p4 p5
  -t3->
  state 14: p1 p2 p4
  -t2->
  state 15: p1 p2*2
  -t1->
  state 12: p3 p4 p5
```

Exemple . . .

Contre exemple Abrégé

```
- output proof;
proof output set

- [] (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
```

Conclusion

En résumé

Abstractions finies du comportement des PN ou TPNs

Préservant certaines classes de propriétés

Connexion avec vérificateurs de modèles

Libre accés à (http://www.laas.fr/tina)

Aussi

Composition de réseaux

Import/Export de modèles pour d'autres outils (PEP, Helena, etc)

Prospective

Techniques d'exploration partielles pour réseaux temporels

Simplification de réseaux (réductions)

D'autres front-ends

D'autres back-ends

References

B. Berthomieu, M. Menasche,
An Enumerative Approach for Analyzing Time Petri Nets,
IFIP Congress 1983, Paris, 1983.

B. Berthomieu, M. Diaz,
Modeling and verification of time dependent systems using time Petri nets.
IEEE Transactions on Software Engineering, 17(3), 1991.

B. Berthomieu, F. Vernadat,
State class constructions for branching analysis of time Petri nets.
TACAS 2003, Springer Verlag LNCS 2619, 2003.

B. Berthomieu, P-O. Ribet, F. Vernadat,
The tool TINA – Construction of Abstract State Spaces for Petri Nets and Time Petri Nets,
International Journal of Production Research, Vol 42, Number 14, July 2004.
(aussi MSR'03, Octobre 2003).

B. Berthomieu, D. Lime, O. H. Roux, F. Vernadat,
Problèmes d'Accessibilité et Espaces d'États Abstraits des Réseaux de Petri à Cl
Modélisation des Systèmes Réactifs (MSR'05), Octobre 2005.

Cotre project: http://www.laas.fr/COTRE

Tina tool: http://www.laas.fr/tina