Abstraction et accélération de systèmes infinis

Grégoire Sutre

LSV, ENS Cachan & CNRS UMR 8643

Directeur de Thèse : Alain Finkel

1– Plan

- Introduction
- Abstraction et accélération
- Analyse des automates à files FIFO
- Analyse des SAVE étendus
- Conclusion et perspectives

2– Cadre général

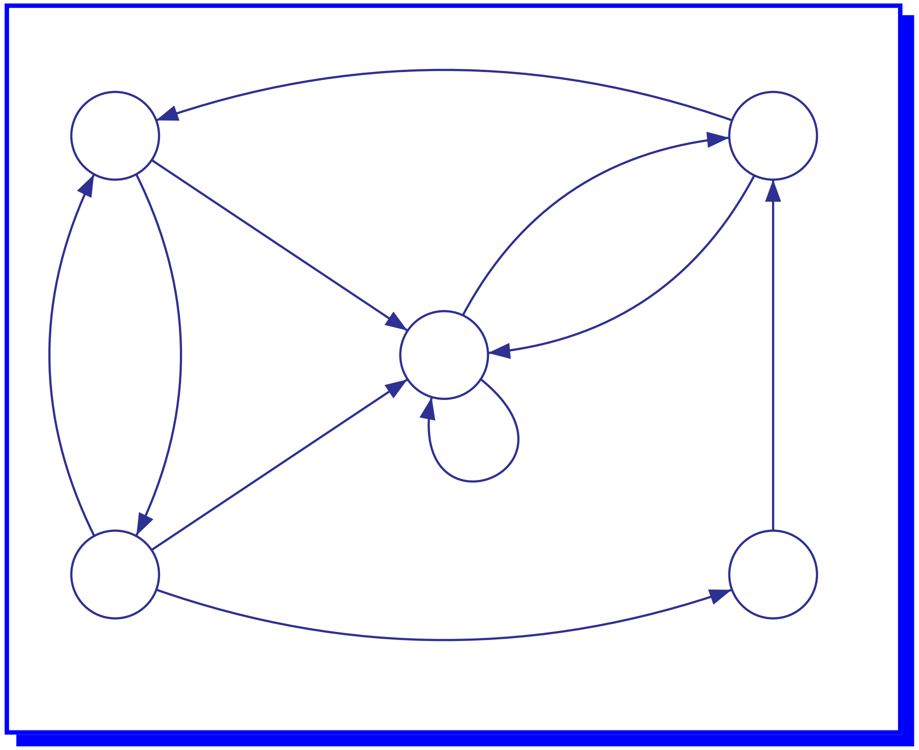
```
while (x > 1) {
   if (y == 0) {
     exit(1) ;
   }
   else {
     x = x - 1 ;
     ...
```

$\models$ Cahier des charges

$\Downarrow$ Modélisation

$$\mathcal{M} \models \varphi$$

3– Cadre général (2)



$$\models$$

$$
\begin{array}{ll}
 & \mathrm{AG}\,\neg(p \wedge q) \\
\wedge & \mathrm{AG}(p \Rightarrow \mathrm{AF}\,q) \\
\wedge & \ldots
\end{array}
$$

4– Vérification des propriétés de sûreté

- Propriété de sûreté : $\varphi = \mathrm{AG}\,\neg erreur$
- Calcul de l'ensemble $Erreur$ des états erronés
- Vérification :

$$
\begin{array}{llll}
Erreur & \cap & \mathrm{post}^*(Init) & \stackrel{?}{=} \emptyset \\
Init & \cap & \mathrm{pre}^*(Erreur) & \stackrel{?}{=} \emptyset
\end{array}
$$

$\Longrightarrow$ Parcours exhaustif des états accessibles pour les systèmes de transitions finis

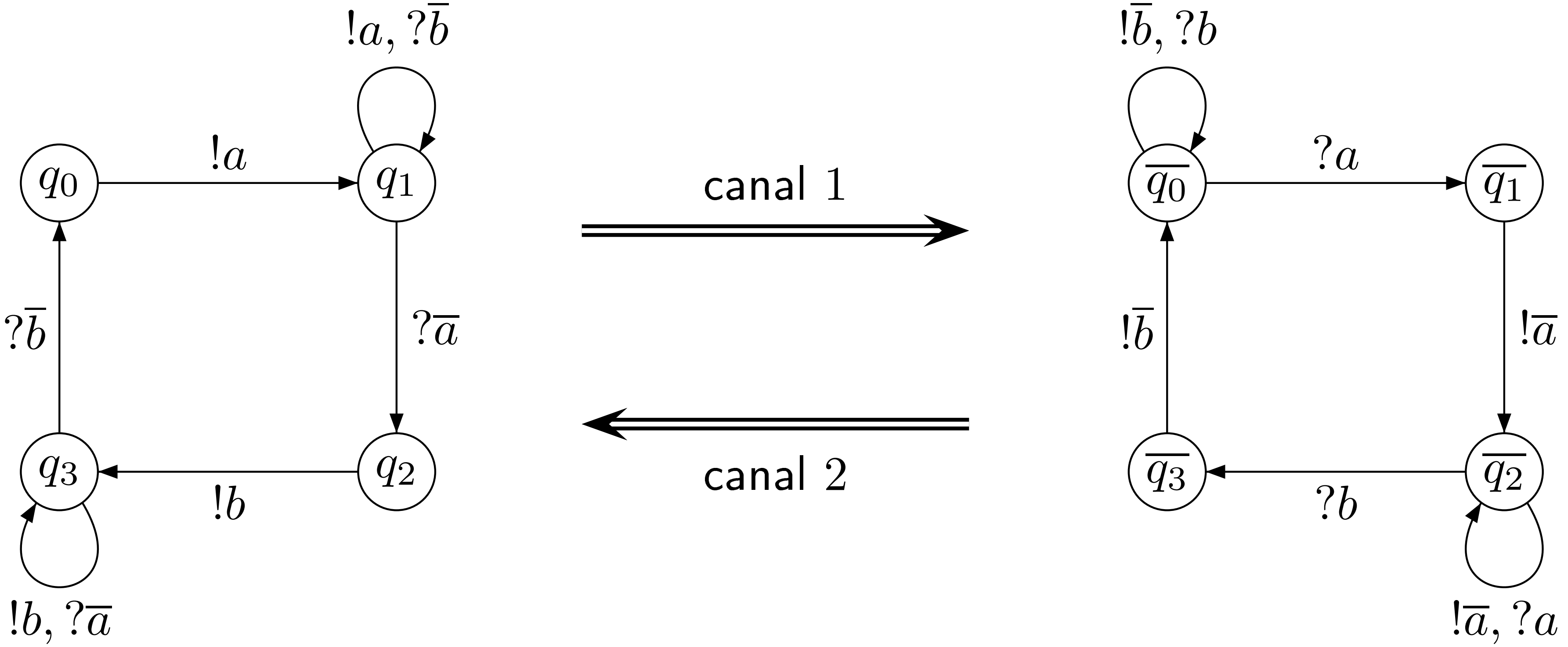
$\Longrightarrow$ Ne fonctionne pas dans le cas infini

5– Systèmes de transitions infinis

- Sources d'infini
  - ⋆ pile, file (canal de communication)
  - ⋆ variable entière (compteur)
  - ⋆ variable réelle (horloge, température)

- Pourquoi vérifier les systèmes de transitions infinis ?
  - ⋆ borner $\Longrightarrow$ explosion combinatoire du nombre d'états
  - ⋆ quelle borne ?
  - ⋆ vérification paramétrée

6– Exemple : le protocole du bit alterné



7– Exemple : le protocole du bit alterné (2)

Etats de contrôle : $Q = \{q_0, q_1, q_2, q_3\} \times \{\overline{q_0}, \overline{q_1}, \overline{q_2}, \overline{q_3}\}$

Alphabet des messages : $M = \{a, b, \overline{a}, \overline{b}\}$

Etats du système de transitions infini associé : $Q \times (M^*)^2$

Exemple d'exécution :

$$\begin{tikzcd}
(q_0, \overline{q_0}, \varepsilon, \varepsilon) \arrow[r, "!a"] & (q_1, \overline{q_0}, a, \varepsilon) \arrow[r, "!a"] & (q_1, \overline{q_0}, aa, \varepsilon) \arrow[r, "?a"] & (q_1, \overline{q_1}, a, \varepsilon) \arrow[d, "!\overline{a}"] \\
& (q_2, \overline{q_2}, a, \overline{a}) & (q_1, \overline{q_2}, a, \overline{aa}) \arrow[l, "?\overline{a}"'] & (q_1, \overline{q_2}, a, \overline{a}) \arrow[l, "!\overline{a}"']
\end{tikzcd}$$

8– Vérification des systèmes de transitions in

- Ne peut pas être automatisée dans le cas général
- Preuve

  $\Longrightarrow$ utilisation d'assitants de preuve, logiques très expressives

  $\Longrightarrow$ fortement interactive, demande une compréhension fine du système
- Vérification de modèles

  $\Longrightarrow$ entièrement automatique pour des classes restreintes

  $\Longrightarrow$ semi-algorithmes et vérification approchée pour des classes générales

9– Abstraction et accélération

- ✓ Introduction
- ⇒ Abstraction et accélération
- Analyse des automates à files FIFO
- Analyse des SAVE étendus
- Conclusion et perspectives

10– Représentations symboliqu

- Descriptions finies d'ensembles infinis de valeurs

  $\Longrightarrow$ clôture par $\mathrm{post}/\mathrm{pre}$ et par union

  $\Longrightarrow$ inclusion décidable

- Pile, file

  $\Longrightarrow$ expressions régulières, automates finis

  $\Longrightarrow$ QDD [BG96], CQDD [BH97]

- Variable entière

  $\Longrightarrow$ ensembles périodiques [BW94]

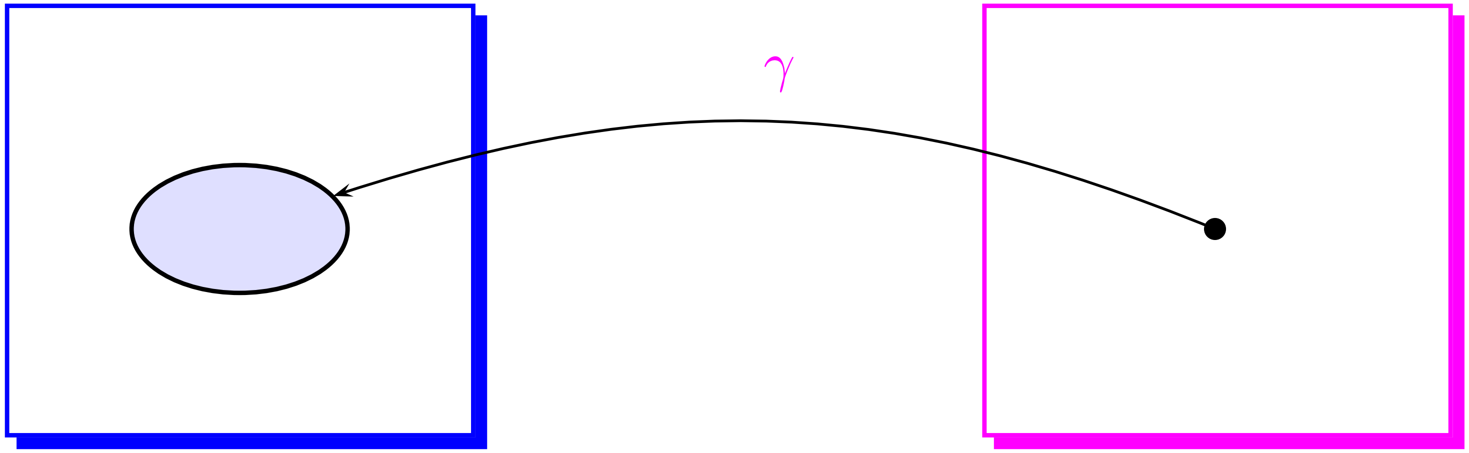
  $\Longrightarrow$ formules de Presburger [CJ98]

- Variable réelle

  $\Longrightarrow$ polyhèdres convexes [CH78]

  $\Longrightarrow$ régions [AD90]

11– Abstraction



$\mathcal{LTS} = (S, \Sigma, \rightarrow)$

$\mathcal{A}_{\mathcal{LTS}} = (A, \mathrm{post}_{\mathcal{A}}, \gamma, \sqcup, \Sigma)$

$$\mathrm{post}_{\mathcal{A}} : A \times \Sigma \rightarrow A$$
$$\gamma : A \rightarrow \mathcal{P}(S)$$
$$\sqcup : A \times A \rightarrow A$$

$$\begin{cases} \gamma(a \sqcup b) = \gamma(a) \cup \gamma(b) \\ \mathrm{post}(\gamma(a), \alpha) \subseteq \gamma(\mathrm{post}_{\mathcal{A}}(a, \alpha)) \subseteq \mathrm{post}^*(\gamma(a)) \end{cases}$$

12– Calcul abstrait de post^*

- Pré-ordre naturel : $a \sqsubseteq b$ si $\gamma(a) \subseteq \gamma(b)$

```
1 :  a ← a₀
2 :  répéter
3 :  a′ ← a
4 :  a ← a′ ⊔ post_A(a′)
5 :  jusqu'à ce que a ⊑ a′
6 :  retourner a
```

- Mais à chaque étape de la boucle, a peut ne représenter qu'une portion finie de $\mathrm{post}^*(\gamma(a_0))$

$\Longrightarrow$ Il faut accélérer le calcul

13– Accélération

- Itérer les circuits de contrôle

$$(q_3, \overline{q_2}, aaa, \overline{a}) \xrightarrow{(!b)^*} (q_3, \overline{q_2}, aaa\, b^*, \overline{a})$$

$\nabla : A \times \Sigma^+ \rightarrow A$ est une accélération pour $\mathcal{A}_{\mathcal{LTS}}$ si

$$\nabla(a, \sigma) \sqsupseteq a \tag{1}$$

∇ est correcte si

$$\gamma(\nabla(a, \sigma)) \subseteq \mathrm{post}^*(\gamma(a)) \tag{2}$$

∇ est complète si

$$\gamma(\nabla(a, \sigma)) \supseteq \bigcup_{i \in \mathbb{N}} \mathrm{post}(\gamma(a), \sigma^i) \tag{3}$$

- Arbre d'accessiblité symbolique avec accélération

14– Exemple : le protocole du bit alterné (3)

$$
\begin{array}{rlllll}
\mathrm{post}^*(q_0,\overline{q_0},\varepsilon,\varepsilon) = & & (q_0,\overline{q_0}) \times (b^*,\overline{b}^*) & \cup & (q_1,\overline{q_0}) \times (b^* a\, a^*, \overline{b}^* &) \\
& \cup & (q_1,\overline{q_1}) \times (a^*,\overline{b}^*) & \cup & (q_1,\overline{q_2}) \times (a^* & , \overline{b}^* \overline{a}\, \overline{a}^*) \\
& \cup & (q_2,\overline{q_2}) \times (a^*,\overline{a}^*) & \cup & (q_3,\overline{q_2}) \times (a^* b\, b^*, \overline{a}^* &) \\
& \cup & (q_3,\overline{q_3}) \times (b^*,\overline{a}^*) & \cup & (q_3,\overline{q_0}) \times (b^* & , \overline{a}^* \overline{b}\, \overline{b}^*)
\end{array}
$$

15– Comparaison avec l'interprétation abstra

$\boxed{\text{accélération} \neq \text{élargissement}}$

Car une accélération ∇ tient compte de $\mathcal{LTS}$ et de σ

- Abstraction exacte
- Aucune hypothèse de complétude, pas de borne inférieure
- Pas de fonction d'abstraction

16– Systèmes de transitions plats

- Expressions régulières semilinéraires (SLRE)

  LRE : $\boxed{x_0 {y_0}^* x_1 {y_1}^* \cdots x_{k-1} {y_{k-1}}^* x_k}$ avec $x_i \in \Sigma^*$ et $y_i \in \Sigma^+$

  SLRE : somme finie de LRE

- $(\mathcal{LTS}, Init)$ est plat si $Traces(\mathcal{LTS}, Init) \subseteq [\![\rho]\!]$ où $\rho \in SLRE$

- Calcul abstrait de post^* pour les systèmes de transitions plats
  - ⋆ abstraction $\mathcal{A}_{\mathcal{LTS}}$
  - ⋆ accélération ∇ correcte et complète

17– Systèmes de transitions bien structurés

- Système de transitions pré-ordonné : $(\mathcal{LTS}, \preceq)$ avec $\preceq$ pré-ordre sur S
- Ensemble de couverture : $\downarrow \mathrm{post}^*(Init)$
- Abstraction de $\downarrow(\mathcal{LTS}, \preceq)$ par ensembles clos inférieurement de base finie
- Accélération générique

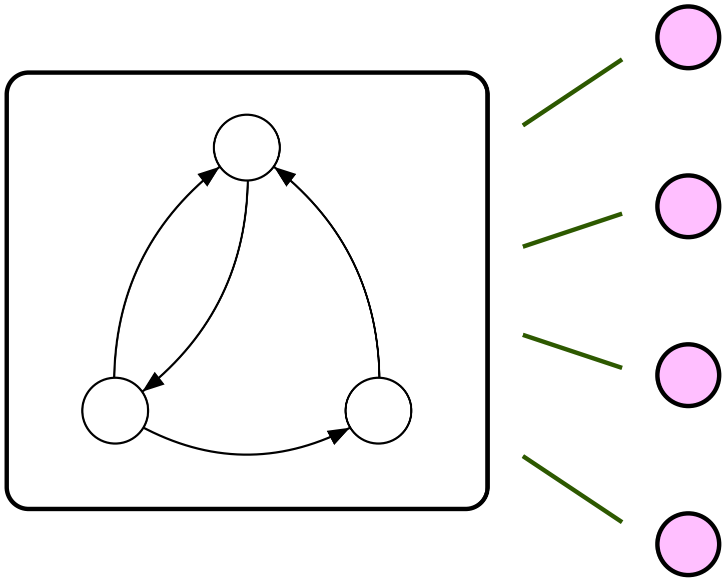
$\Longrightarrow$ Englobe [Fin90], [AČJT96], [EN98], [FS00]

$\Longrightarrow$ Sépare les hypothèses de correction des hypothèses de terminaison

18– Analyse des automates à files Fifo

- ✓ Introduction
- ✓ Abstraction et accélération
- ⇒ Analyse des automates à files Fifo
- • Analyse des SAVE étendus
- • Conclusion et perspectives

19– Automates à files Fifo



? – réception

! – émission

Les automates à files FIFO sont Turing-équivalents

20– Représentations symboliques Fifo

$$\mathcal{R}_{C,M} = (\underbrace{R, +, \perp}_{\text{monoïde}}, !!, ??, [\![\cdot]\!]) \qquad \text{avec} \qquad \begin{aligned} ?? &: C \times M \times R \to R \\ !! &: C \times M \times R \to R \\ [\![\cdot]\!] &: R \to 2^{(M^*)^C} \end{aligned}$$

- Accélération : itération des séquences d'opérations
- Caractérisation des séquences d'opérations σ tels que σ^* est $\mathcal{R}$–représentable

21– QDD

- Union finie de produits d'expressions régulières (langages reconnaissables)

- σ compte si

  $\star$ $|M| > 1$ et σ émet dans 2 canaux distincts, ou

  $\star$ $|M| = 1$ et σ fait croître 2 canaux distincts

Théorème [BGWW97] σ^* est $\mathcal{QDD}$–représentable ssi σ ne compte pas

22– CQDD

- Union finie de couples (r, φ) où
  - $\star$ r est un produit de LRE
  - $\star$ φ est une formule de Presburger reliant les occurrences de '$*$' dans r

Théorème [BH97] σ^* est $\mathcal{CQDD}$–représentable pour tout σ

23– SLRE

- Union finie de produits de SLRE

Théorème σ^* est $\mathcal{SLRE}$–représentable ssi σ ne compte pas

Corollaire σ^* est $\mathcal{SLRE}$–représentable ssi σ^* est $\mathcal{QDD}$–représentable

24– Comparaison des QDD, CQDD et SLRE

Théorème $\mathcal{SLRE} = \mathcal{QDD} \cap \mathcal{CQDD}$

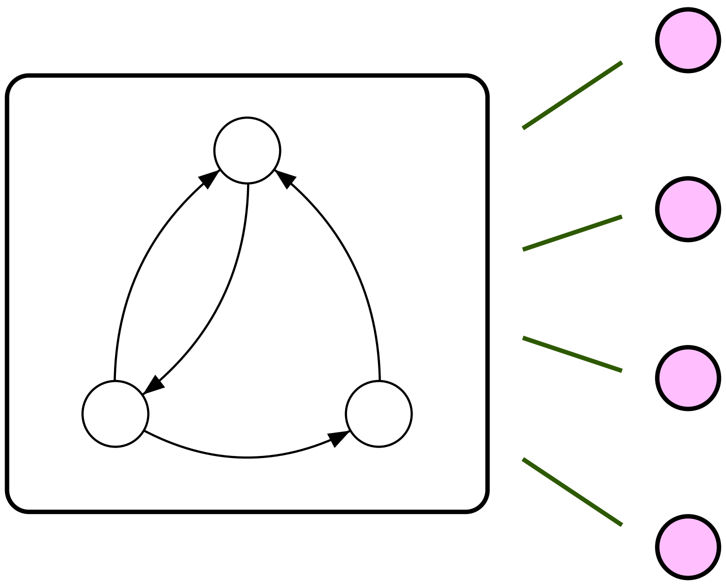
Théorème Les problèmes d'inclusion et d'équivalence pour les SLRE sont dans $NP \cap coNP$

- Partant d'un unique état initial,
  - $\star$ pour un seul canal, $\mathcal{SLRE} \cong \mathcal{QDD} \cong \mathcal{CQDD}$
  - $\star$ pour plusieurs canaux, $\mathcal{SLRE} \cong \mathcal{QDD}$

25– Analyse des SAVE étendus

26– SAVE étendus

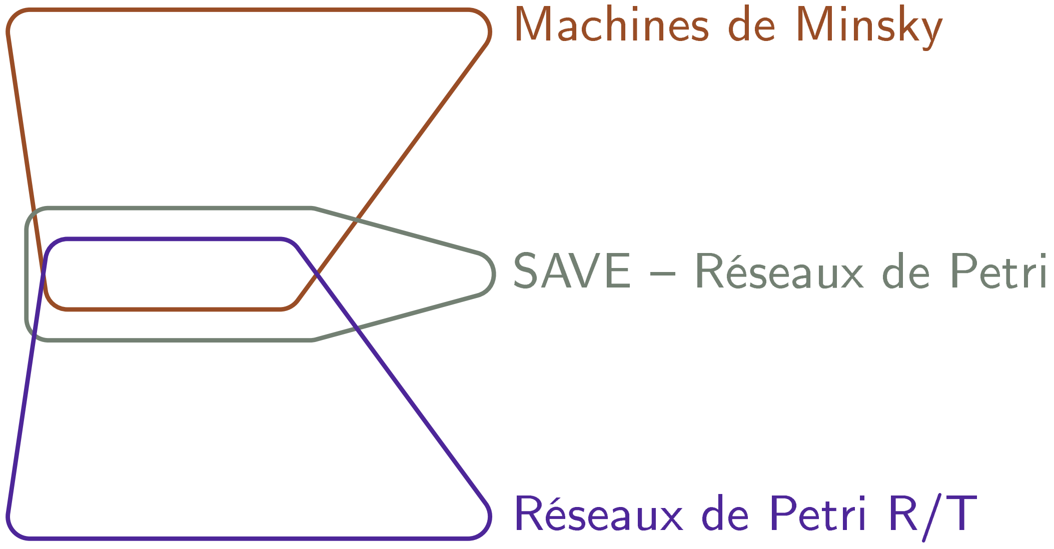
- variables — compteurs — à valeurs dans $\mathbb{N}$



test à zéro

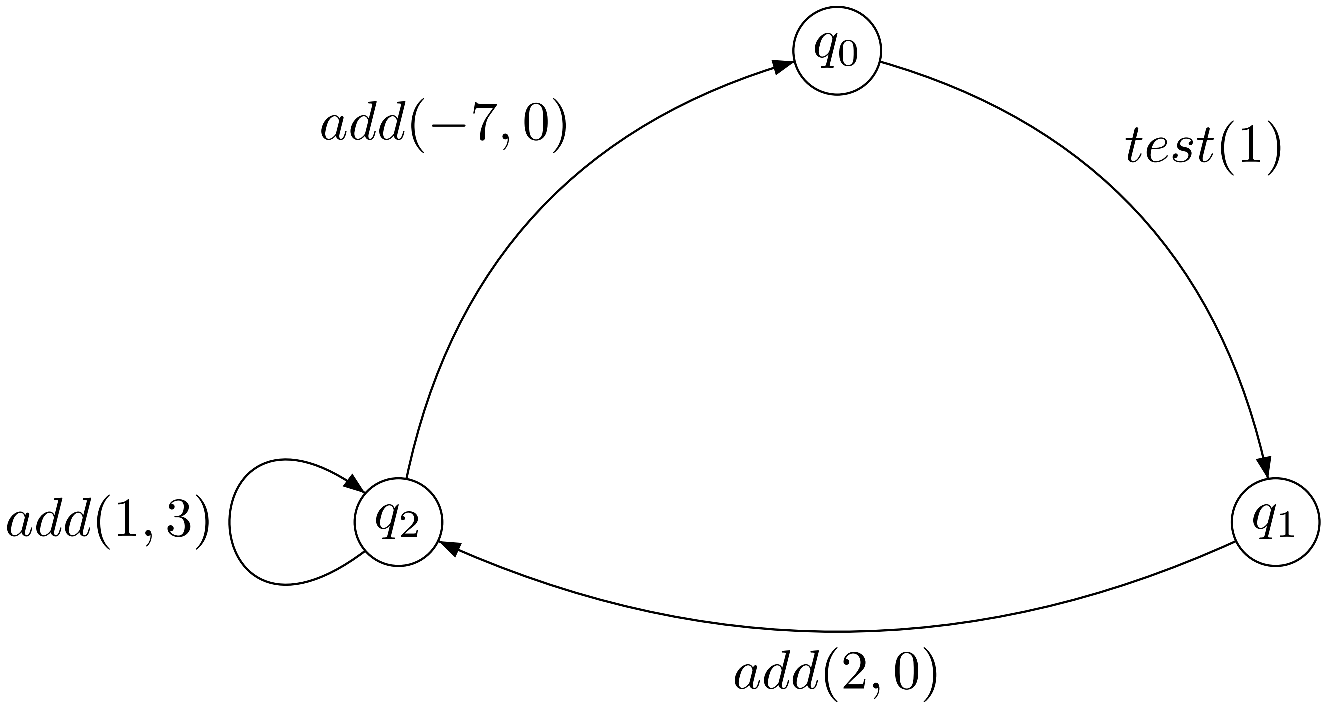
+1, -1

reset/transfert



Les SAVE étendus sont Turing-équivalents

27– Exemple de SAVE étendu à deux compte



28– Représentation symbolique par ensemble

$$\bigcup_{i \in I} (x_i + P_i{}^*) \quad \text{où} \quad \begin{cases} x_i \in \mathbb{N}^n \\ P_i = \{p_1, p_2, \cdots, p_k\} \subseteq \mathbb{N}^n \\ P_i{}^* = \{\sum_{i=1}^{k} \alpha_i p_i \ / \ \alpha_i \in \mathbb{N}\} \end{cases}$$

- Bonnes propriétés :

  $\Longrightarrow$ clôture effective par $\mathrm{post}/\mathrm{pre}$, $\cup$ et $\cap$

  $\Longrightarrow$ appartenance et inclusion sont décidables

29– Exemple de SAVE étendu à deux compte

$$
\begin{aligned}
\mathrm{post}^*(q_0,(0,0)) = & \quad \{(q_0,(0,0))\} \\
& \bigcup \quad \{q_0\} \times ((0,15) + \{(0,15),(1,3)\}^*) \\
& \bigcup \quad \{q_1\} \times ((0,0) + \{(0,15)\}^*) \\
& \bigcup \quad \{q_2\} \times ((2,0) + \{(0,15),(1,3)\}^*)
\end{aligned}
$$

30– Etat de l'art

compteurs	op. étendues	
1	$test, reset$	post^* et pre^* effectivement semilinéaires
2		post^* et pre^* effectivement semilinéaires [HP79]
2	$test(1,2)$	Turing–équivalent [Min61]
3		post^* et pre^* non semilinéaires [HP79]
3	$reset(1,2)$	accessibilité indécidable caractère borné décidable [DJS99]
3	$reset(1,2,3)$	caractère borné indécidable [DFS98]
3 avec perte	$reset(1,2,3)$	pre^* effectivement semilinéaire post^* semilinéaire mais non constructible [BM99] caractère borné indécidable

31– Etat de l'art pour 2 compteurs

op. étendues	
	post^* et pre^* effectivement semilinéaires
$reset(1,2)$	accessibilité indécidable caractère borné décidable
$test(1,2)$	Turing–équivalent

Calcul symbolique de post^* pour les SAVE étendus

- Abstraction des SAVE étendus basée sur les ensembles semilinéaires
- Accélération correcte et complète

Mais l'arbre d'accessibilité symbolique ne termine pas sur l'exemple, car :

- $\star$ séquence à itérer : $\sigma = add(2,0)(add(1,3))^5 add(-7,0) test(1)$
- $\star$ σ n'apparaît pas le long des branches de l'arbre

$\Longrightarrow$ Accélérer en tenant compte des accélérations précédentes

32– Calcul de $\mathrm{post}^*/\mathrm{pre}^*$ pour les SAVE étend

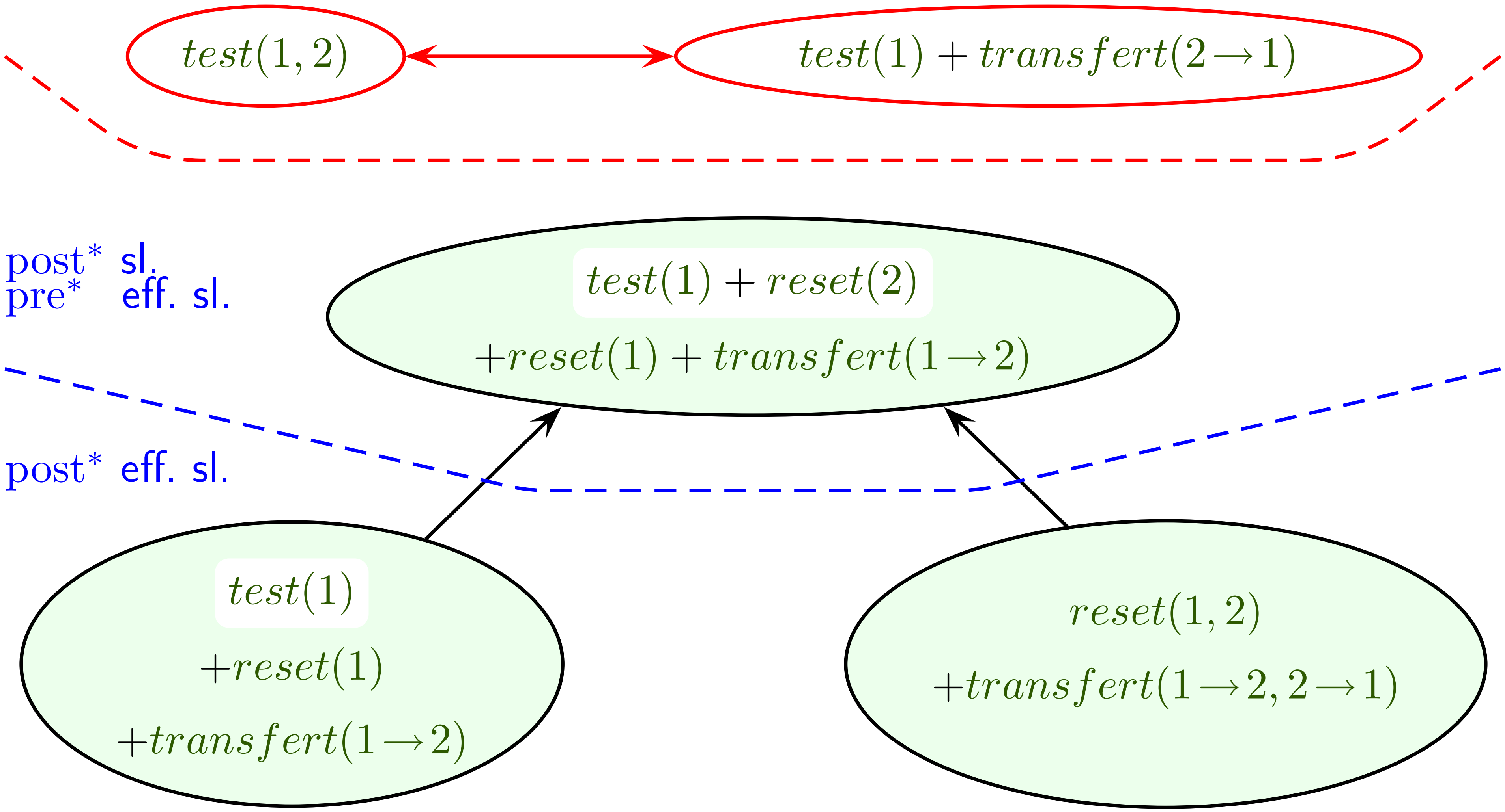


Schéma de preuve

- Définition d'un nouvel algorithme d'accessibilité symbolique
  - $\star$ étiquettes d'accélération sur les arcs
  - $\star$ accélération modulaire pouvant examiner la branche
- Obtention d'un beau pré-ordre sur l'ensemble des périodes
- Equivalence d'accélérations (simplification des preuves de terminaison)
- Simulations entre classes

Schéma de preuve (2)

- Conception d'accélérations correctes garantissant la terminaison pour
  - $\star$ aucune opération étendue [HP79]
  - $\star$ $test(1)$
  - $\star$ $test(1) + testfaible(2)$
  - $\star$ $test(1) + reset(2)$ (oracle $\cong$ couverture)
- Arbre de couverture pour $reset(1, 2) + transfert(1 \to 2, 2 \to 1)$
  - $\star$ schémas de chemins réguliers [DJS99]

33– Conclusion

- Cadre général d'abstraction et d'accélération qui capture
  - ⋆ représentations symboliques (QDD, CQDD, semilinéaires, ...)
  - ⋆ systèmes plats et systèmes bien structurés
- Nouvelle représentation symbolique FIFO basée sur les SLRE
  - ⋆ simple, au centre des QDD et des CQDD, suffisante
- Hiérarchie exhaustive des SAVE étendus à 2 compteurs
  - ⋆ complète vis-à-vis de la décidabilité de l'accessibilité
  - ⋆ presque complète vis-à-vis de l'effective semilinéarité de post^* et de pre^*
- Analyse des automates à file réactifs

34– Perspectives

- Programmation du cadre général d'abstraction et d'accélération
  - ⋆ représentations symboliques de files et de compteurs
  - ⋆ analyse des systèmes hybrides

- Algorithmique des représentations symboliques

- Composition des abstractions

- Problème ouverts :
  - ⋆ effective semilinéarité de post^* pour $test(1) + reset(2)$
  - ⋆ algorithme polynomial pour l'inclusion entre SLRE ?