Analyse d'espaces d'états par résolution distribuée de systèmes d'équations booléennes

Christophe Joubert

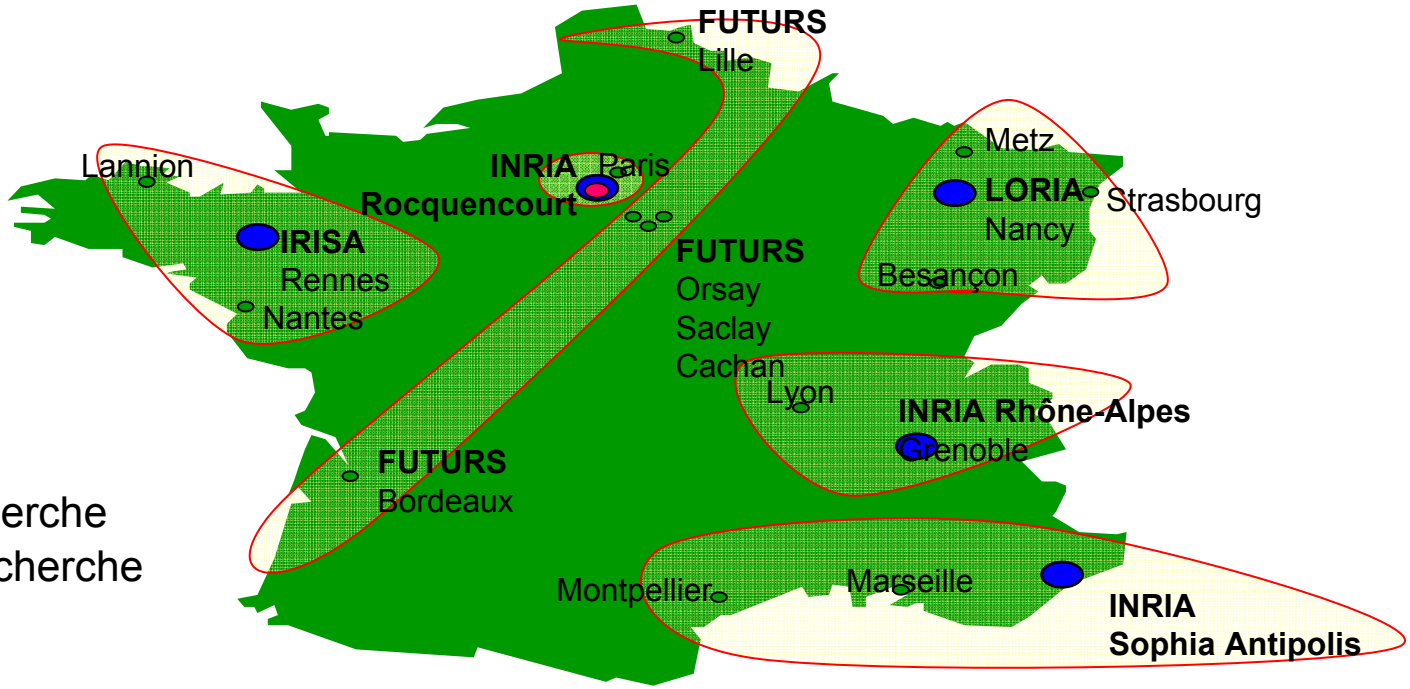
INRIA / VASY

http://www.inrialpes.fr/vasy

Sommaire

- L'INRIA et l'équipe de Validation de Systèmes (VASY)
- Vérification basée sur les modèles
- Traduction en termes de Systèmes d'Équations Booléennes (SEB)
- Résolution distribuée des SEB sur grappes de machines
- Applications à d'autres domaines

L'INRIA et l'équipe de Validation de Systèmes (VASY)



Thème : systèmes communicants
Systèmes distribués et architectures réparties, réseaux et télécommunications, systèmes embarqués et mobilité et architecture et compilation

Autres thèmes : systèmes cognitifs, systèmes symboliques, systèmes numériques et systèmes biologiques

Rhône-Alpes

Motivations pour les méthodes formelles

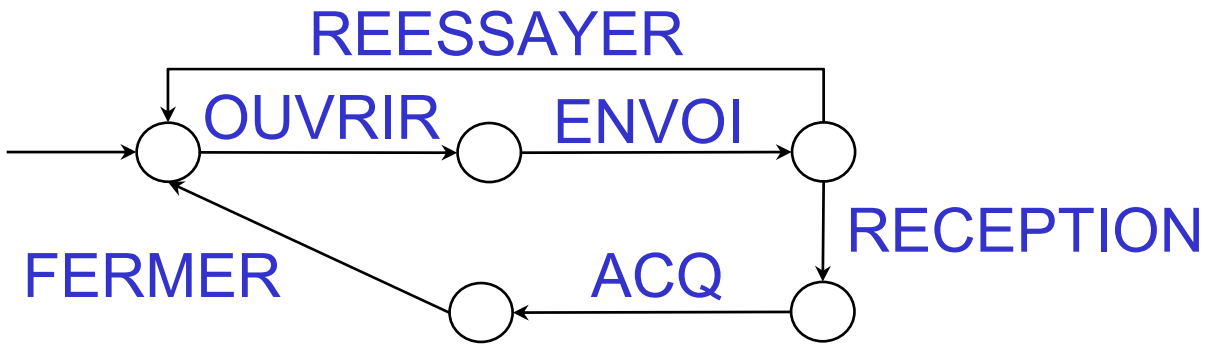
- Savoir produire des logiciels fiables, assurer leur maintenance et leur évolution sûre année après année
- Utiliser les ordinateurs pour raisonner sur le comportement d'autres ordinateurs!
- Méthodes déductives, d'analyse statique, de typage, d'analyse de syntaxe, de sémantique, d'interprétation abstraite

➔ méthodes de vérification basée sur les modèles

Explosion du lanceur Ariane 5 - Vol 501 Kourou, Guyane Française, 4 juin 1996 : erreur logicielle provenant de l'ordinateur de bord

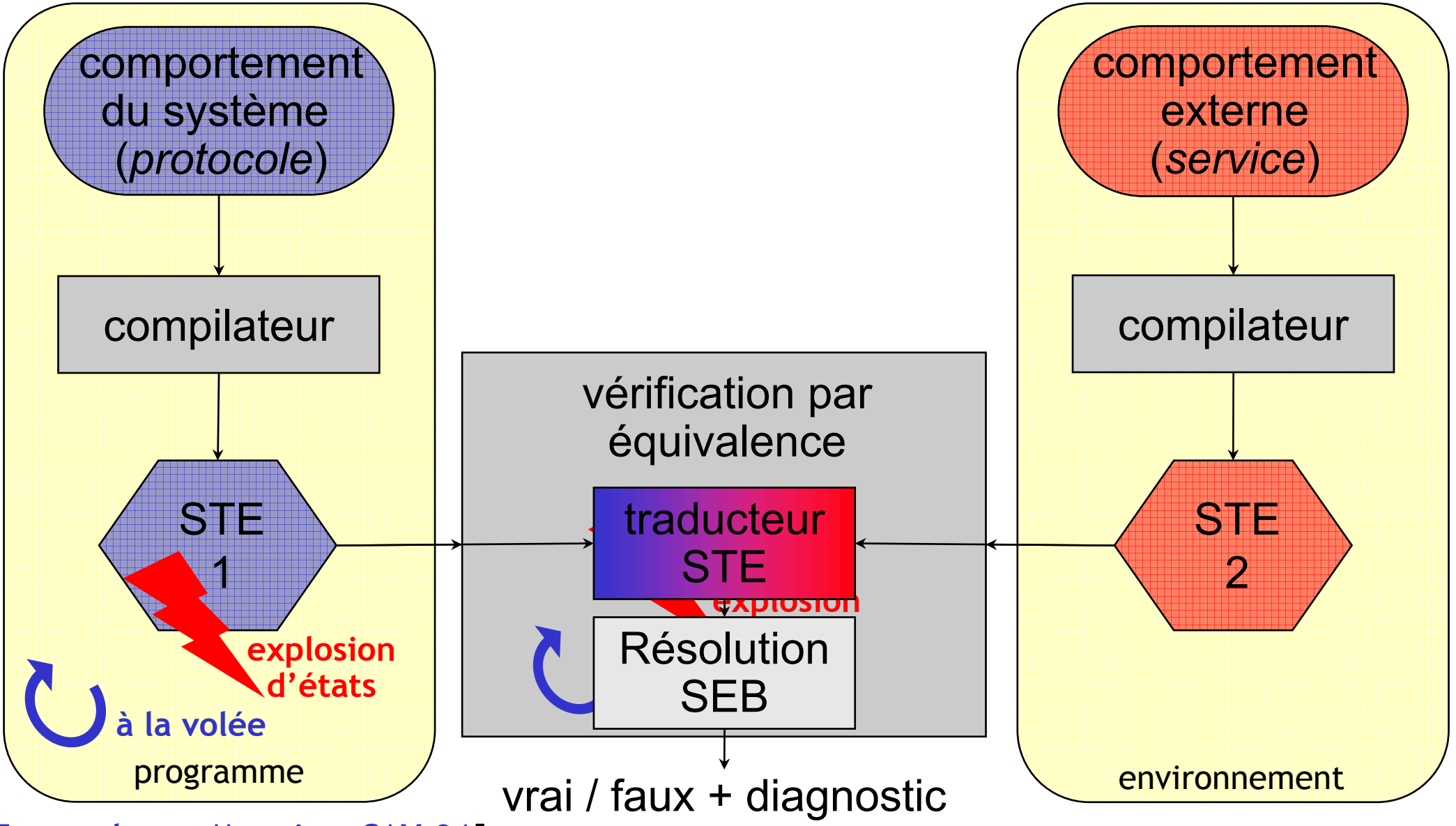
Systèmes de transitions étiquetées (STEs)

- STE : le modèle sémantique standard pour les langages à actions (y compris LOTOS)



- $M = (S, A, T, s_0)$, où :
  - S : ensemble d'états
  - A : ensemble d'actions (informations attachées aux transitions)
  - $T \in S \times A \times S$: relation de transition
  - $s_0 \in S$: état initial

Vérification par équivalence



- [Fernandez et Mounier, CAV-91]

Relations d'équivalence en terme de SEB

- $STE_1 = (Q_1, A, T_1, q_{01})$, $STE_2 = (Q_2, A, T_2, q_{02})$

  équivalence forte $\approx \subseteq Q_1 \times Q_2$ est la relation max t.q. $p \approx q$ ssi

$$\forall a \in A, \forall p \xrightarrow{a} p' \in T_1, \exists q \xrightarrow{a} q' \in T_2, p' \approx q'$$
$$\wedge$$
$$\forall a \in A, \forall q \xrightarrow{a} q' \in T_2, \exists p \xrightarrow{a} p' \in T_1, p' \approx q'$$

- $STE_1 \approx STE_2$ ssi $q_{01} \approx q_{02}$
- Principe : $p \approx q$ ssi $X_{p,q}$ est vrai
- Traduction en SEB :

$$X_{p,q} =_\nu (\wedge_{p \xrightarrow{b} p'} \vee_{q \xrightarrow{b} q'} X_{p',q'}) \wedge (\wedge_{q \xrightarrow{b} q'} \vee_{p \xrightarrow{b} p'} X_{p',q'})$$

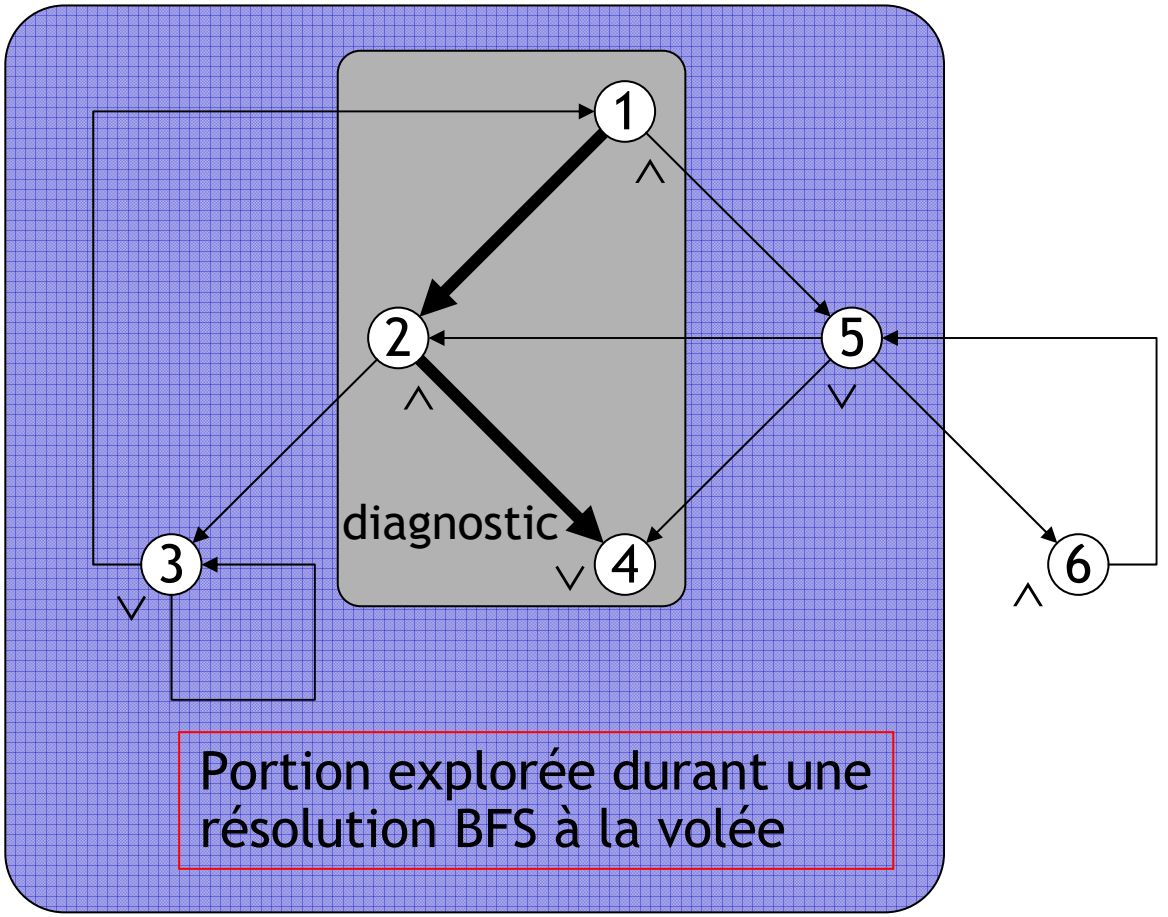
Résolution séquentielle de SEB / graphe booléen

SEB

$$\begin{cases} x_1 =_\nu x_2 \wedge x_5 \\ x_2 =_\nu x_3 \wedge x_4 \\ x_3 =_\nu x_1 \vee x_3 \\ x_4 =_\nu F \\ x_5 =_\nu x_2 \vee x_4 \vee x_6 \\ x_6 =_\nu x_5 \end{cases}$$

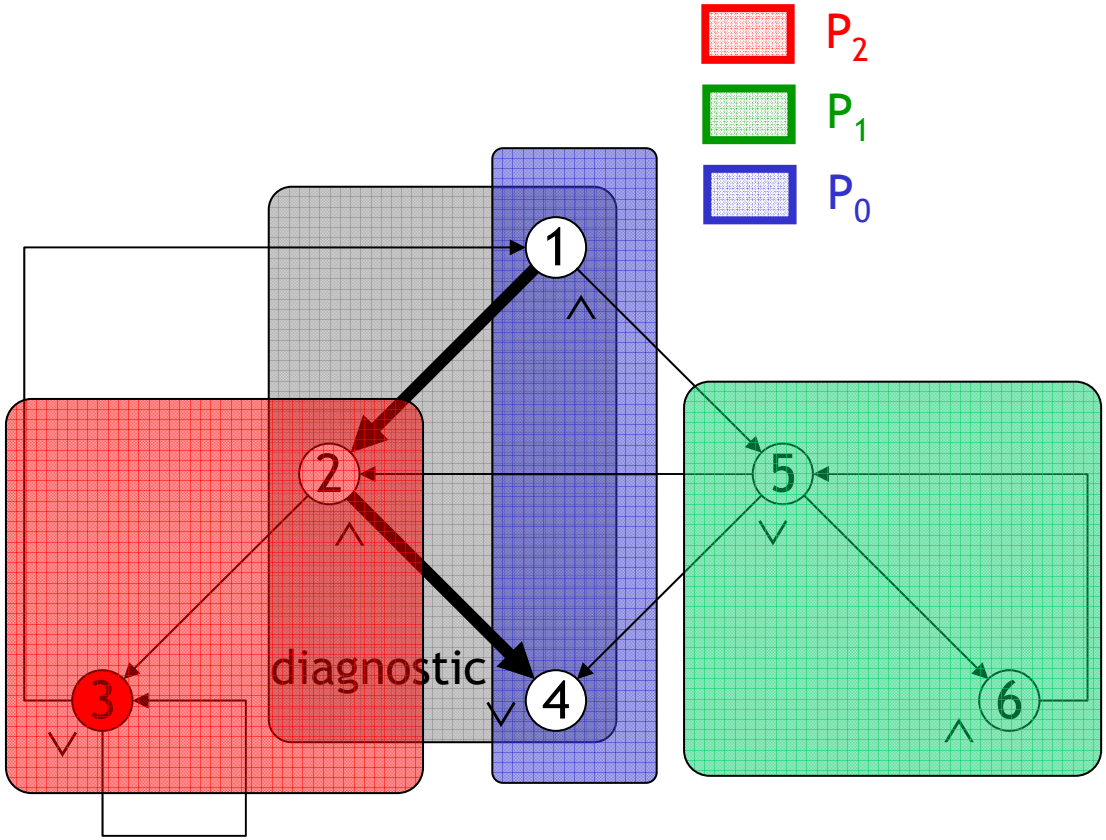
- Théorie des graphes booléens [Andersen, TCS-94][Vergauwen et Lewi, ICALP-94]
- Bibliothèque de résolution séquentielle CAESAR_SOLVE [Mateescu, TACAS-03]

graphe booléen



Résolution distribuée de SEB / graphe booléen

- Limitations de la résolution séquentielle :
  - Mémoire (SEB avec plus de 10^8 variables à résoudre)
  - Temps (parcours de SEB très larges)
- Raisons pour la distribution :
  - Problème régulier favorable à une distribution équilibrée des tâches et des données
  - Exécuter plus rapidement avec moins de mémoire utilisée par machine



Résolution BFS à la volée distribuée sur 3 processeurs

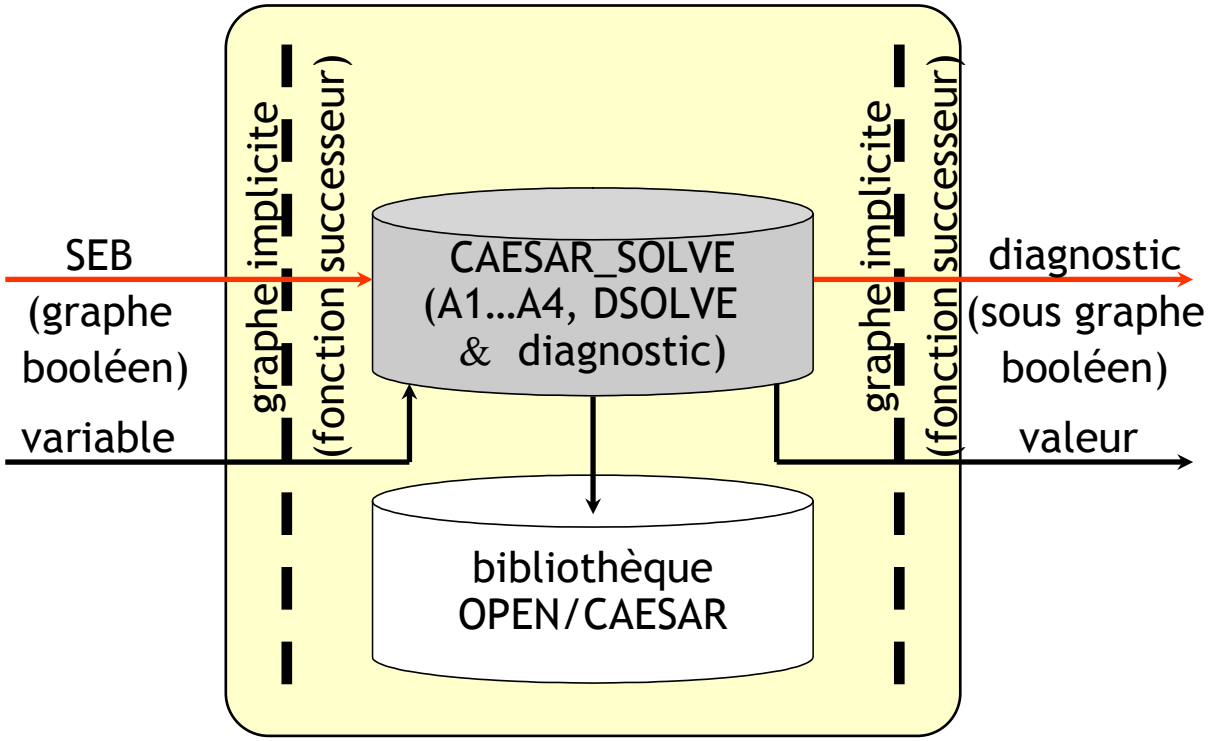
Algorithme distribué [Joubert et Mateescu, PDP-05]

- Architecture à mémoire distribuée (passage de messages) : NOW et grappes de PC
- Réseau faiblement couplé, topologie fortement connexe
- Modèle de programmation SPMD :
  - 2 parcours entrelacés (exploration et propagation arrière)
  - distribution des données par fonction de hachage
  - stabilisation de la variable d'intérêt et/ou détection distribuée de la terminaison
  - génération de diagnostic distribué
- Complexité en temps O (|V|+|E|), mémoire O (|V|+|E|), message O (2.|E|.(P-1)/P), et détection de terminaison O (|E|)

Contexte d'expérimentation (CADP)

- *Construction and Analysis of Distributed Processes*

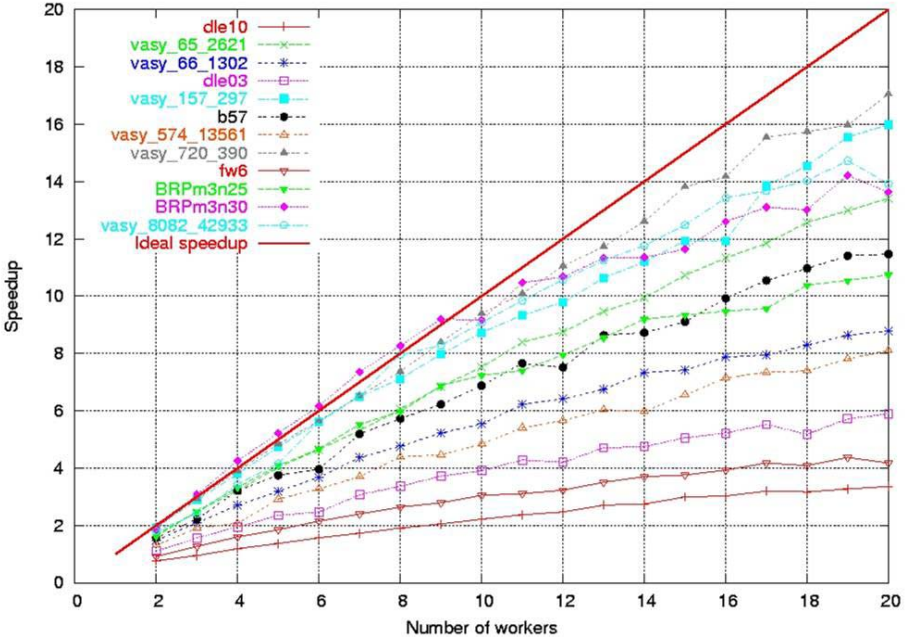
  http://www.inrialpes.fr/vasy/cadp
- Une boîte à outils pour l'ingénierie des protocoles et des systèmes répartis
- Caractéristiques essentielles :
  - modélisation par algèbres de processus (LOTOS)
  - vérification par logiques temporelles
  - vérification par équivalences
  - génération de tests



- Bibliothèque de résolution distribuée de SEB : 8500 lignes de code C
- Intégrée à la bibliothèque séquentielle existante CAESAR_SOLVE
- Développée en utilisant l'environnement OPEN/CAESAR [Garavel, TACAS-98]

Expérimentations sur grappes de PC Linux

- Grappe de 225 PC conçue par HP Laboratories Grenoble et l'INRIA Rhône-Alpes - TOP 500 des supercalculateurs



- Vérification distribuée à la volée par équivalence forte
- Benchmark VLTS http://www.inrialpes.fr/vasy/cadp/resources/benchmark_bcg.html
- Accélérations linéaires [Joubert et Mateescu, PDMC-04]

Applications à d'autres domaines

- Réalisées ou en cours :
  - Vérification par logique temporelle (mu-calcul modal) [Mateescu, TACAS-03]
  - Réduction par tau-confluence [Pace, Lang et Mateescu, CAV-03]
  - Résolution de clauses de Horn [Liu et Smolka, ICALP-98]
- Travaux futurs :
  - Bisimulation markovienne [Hermanns et Siegle, ARTS-99]
  - Génération de tests [Jéron et Morel, CAV-99]

Pour plus d'informations …

http://www.inrialpes.fr/vasy