Distributed On-the-Fly Equivalence Checking and Tau-Confluence Reduction

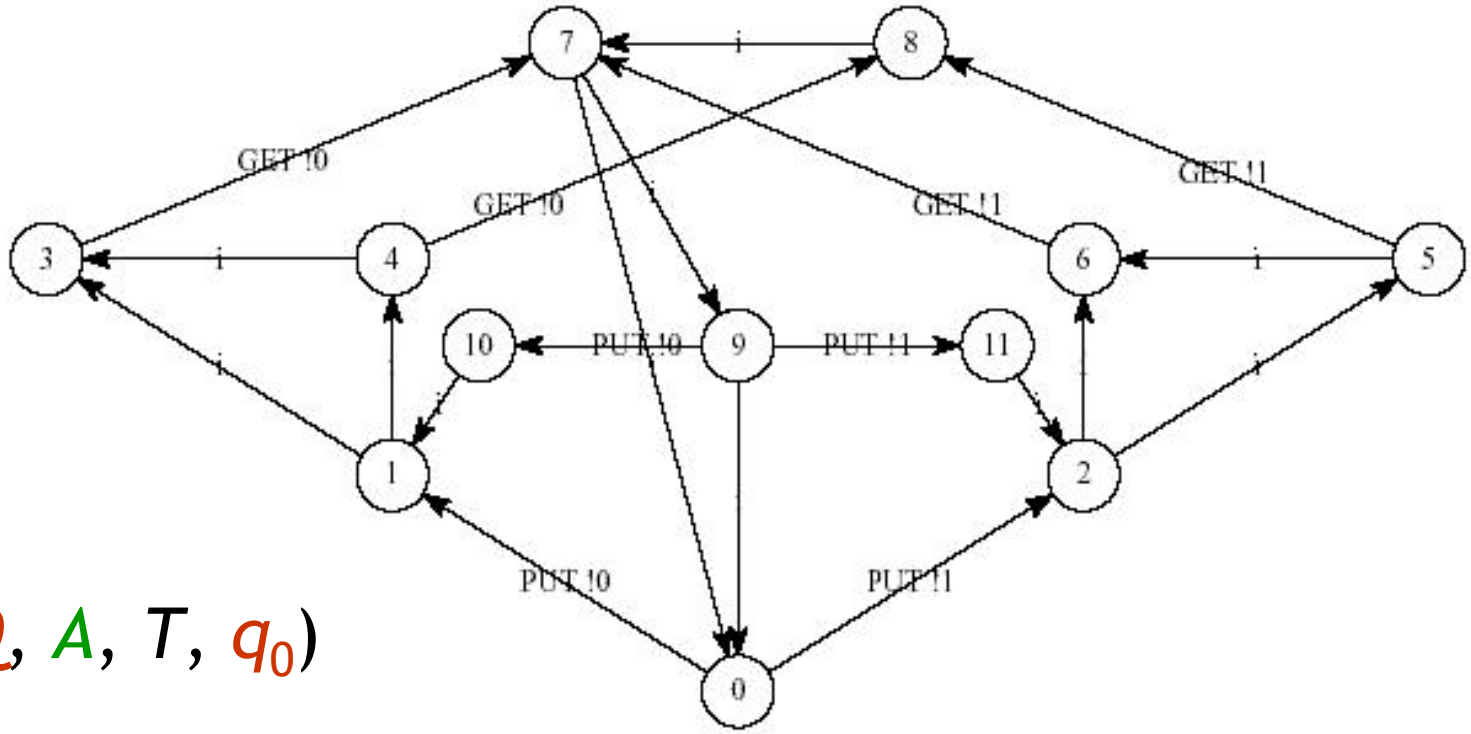
Christophe Joubert and Radu Mateescu

INRIA Rhône-Alpes / VASY
655, avenue de l'Europe
F-38330 Montbonnot Saint Martin, France
http://www.inrialpes.fr/vasy

Outline

- Introduction
- Boolean equation systems
- Equivalence relations
- Tau-confluence
- Tools architecture
- Demo
- Conclusion and future work

Labelled Transition Systems



$M = (Q, A, T, q_0)$

CADP toolbox (http://www.inrialpes.fr/vasy/cadp)

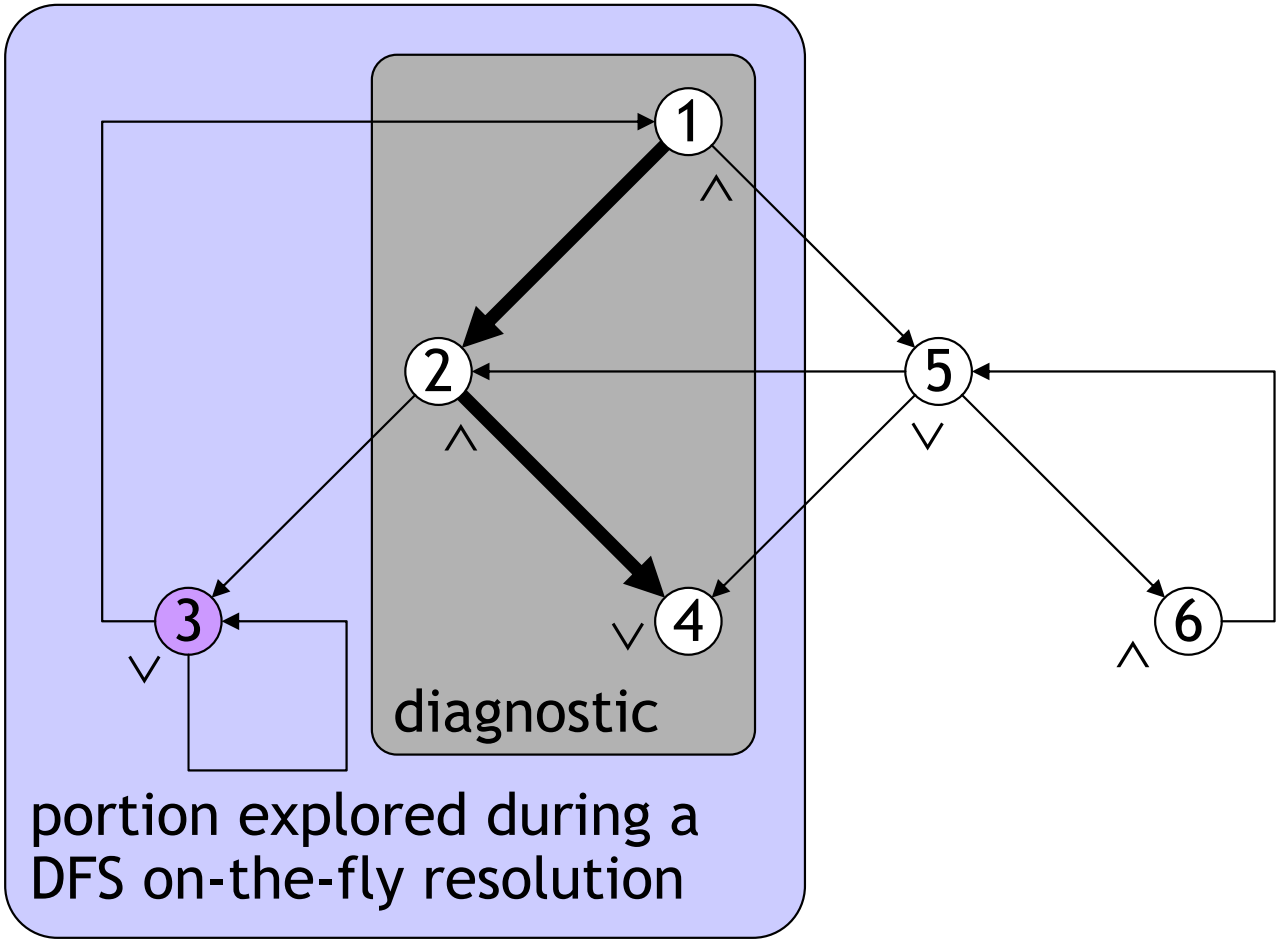
- Explicit representation (succ/pred function)
  - BCG (Binary Coded Graphs)
- Implicit representation (successor function)
  - OPEN/CAESAR [Garavel-98]

Alternation-free Boolean Equation Systems

BES

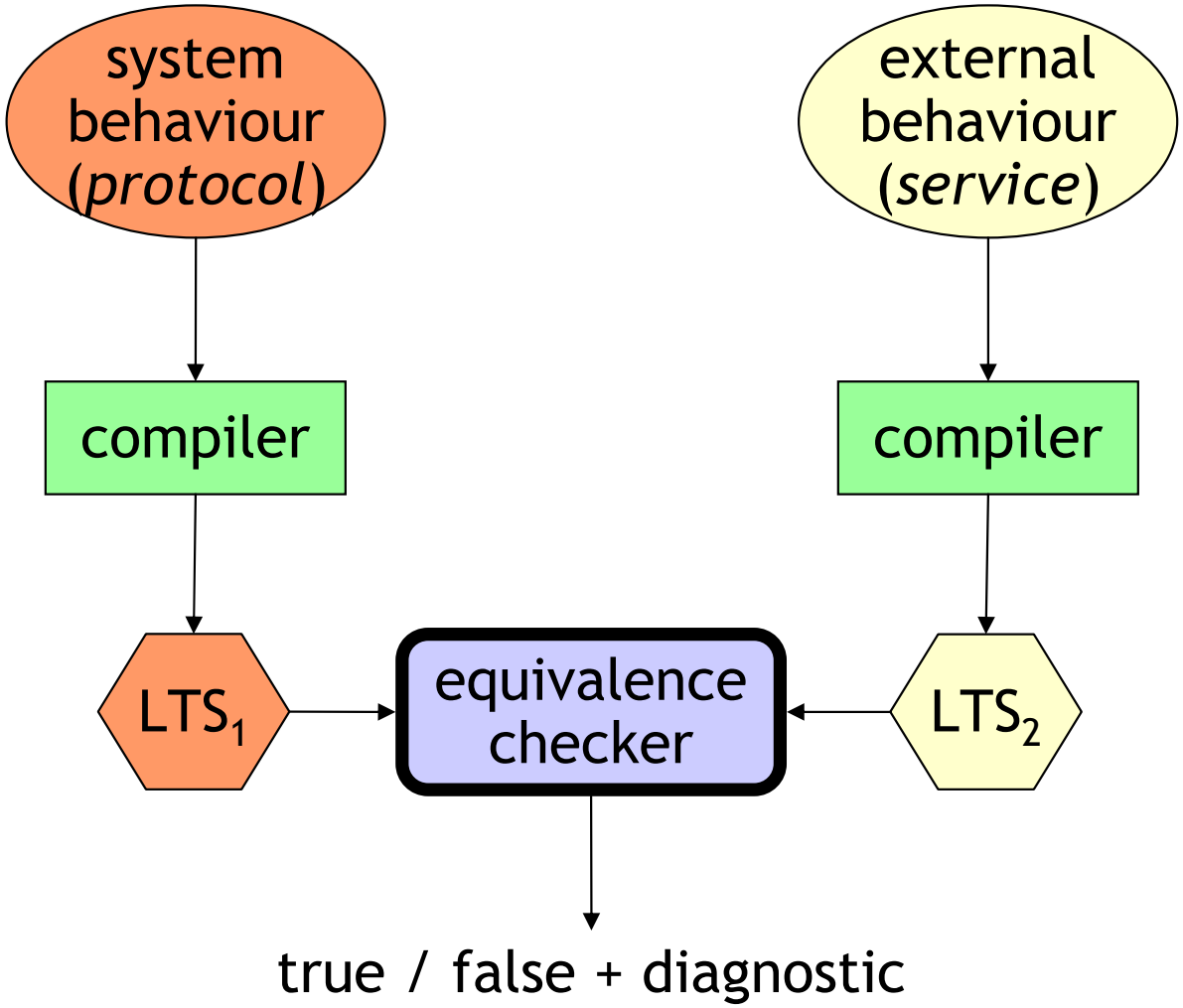
$$\begin{cases} x_1 =_\nu x_2 \wedge x_5 \\ x_2 =_\nu x_3 \wedge x_4 \\ x_3 =_\nu x_1 \vee x_3 \\ x_4 =_\nu F \\ x_5 =_\nu x_2 \vee x_4 \vee x_6 \\ x_6 =_\nu x_5 \end{cases}$$

boolean graph



[Andersen-94]
[Mader-97]

Equivalence checking



Global

- LTS built *before* check
- Partition refinement
- Better when check OK

On-the-fly

- LTS built *during* check
- Synchronous product
- Better when check KO

Strong equivalence

- $M_1 = (Q_1, A, T_1, q_{01})$, $M_2 = (Q_2, A, T_2, q_{02})$
  $\approx \subseteq Q_1 \times Q_2$ is the maximal relation s.t. $p \approx q$ iff

  $\forall a \in A. \forall p \rightarrow_a p' \in T_1. \exists q \rightarrow_a q' \in T_2. p' \approx q'$

  and

  $\forall a \in A. \forall q \rightarrow_a q' \in T_2. \exists p \rightarrow_a p' \in T_1. p' \approx q'$

- $M_1 \approx M_2$ iff $q_{01} \approx q_{02}$

Translation to BES

- Principle: $p \approx q$ iff $X_{p,q}$ is true
- General BES:

$$\begin{cases} X_{p,q} =_\nu (\wedge_{p \to a\, p'} \vee_{q \to a\, q'} X_{p',q'}) \\ \qquad \wedge \\ \qquad (\wedge_{q \to a\, q'} \vee_{p \to a\, p'} X_{p',q'}) \end{cases}$$

- Simple BES:

$$\begin{cases} X_{p,q} =_\nu (\wedge_{p \to a\, p'} Y_{a,p',q}) \wedge (\wedge_{q \to a\, q'} Z_{a,p,q'}) \\ Y_{a,p',q} =_\nu \vee_{q \to a\, q'} X_{p',q'} \\ Z_{a,p,q'} =_\nu \vee_{p \to a\, p'} X_{p',q'} \end{cases}$$

$p \leq q$ (preorder)

Tau*.a and safety equivalences

- $M_1 = (Q_1, A_\tau, T_1, q_{01})$, $M_2 = (Q_2, A_\tau, T_2, q_{02})$
  $A_\tau = A \cup \{ \tau \}$
- $\tau^*.a$ equivalence:

$$\begin{cases} X_{p,q} =_\nu (\wedge_{p \rightarrow \tau^*.a\ p'} \vee_{q \rightarrow \tau^*.a\ q'} X_{p',q'}) \\ \qquad\qquad \wedge \\ \qquad\qquad (\wedge_{q \rightarrow \tau^*.a\ q'} \vee_{p \rightarrow \tau^*.a\ p'} X_{p',q'}) \end{cases}$$

- Safety equivalence:

$$\begin{cases} X_{p,q} =_\nu Y_{p,q} \wedge Y_{q,p} \\ Y_{p,q} =_\nu \wedge_{p \rightarrow \tau^*.a\ p'} \vee_{q \rightarrow \tau^*.a\ q'} Y_{p',q'} \end{cases}$$

Observational and branching equivalences

- Observational equivalence:

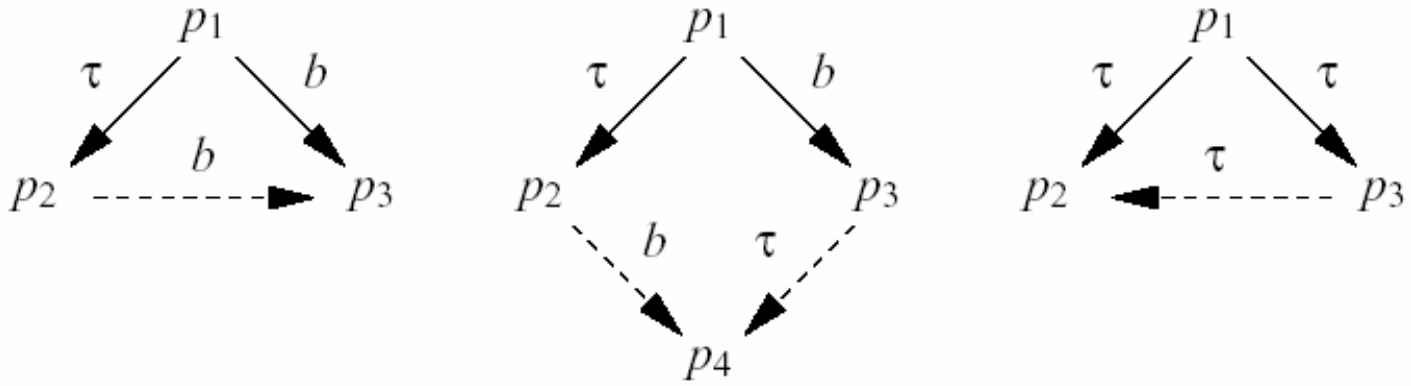
$$\begin{cases} X_{p,q} =_\nu (\wedge_{p \rightarrow\tau\, p'} \vee_{q \rightarrow\tau^*\, q'} X_{p',q'}) \wedge (\wedge_{p \rightarrow a\, p'} \vee_{q \rightarrow\tau^*.a.\tau^*\, q'} X_{p',q'}) \\ \qquad \wedge \\ \qquad (\wedge_{q \rightarrow\tau\, q'} \vee_{p \rightarrow\tau^*\, p'} X_{p',q'}) \wedge (\wedge_{q \rightarrow a\, q'} \vee_{p \rightarrow\tau^*.a.\tau^*\, p'} X_{p',q'}) \end{cases}$$

- Branching equivalence:

$$\begin{cases} X_{p,q} =_\nu \wedge_{p \rightarrow b\, p'} ((b{=}\tau \wedge X_{p',q}) \vee \vee_{q \rightarrow\tau^*\, q' \rightarrow b\, q''} (X_{p,q'} \wedge X_{p',q''}) \\ \qquad \wedge \\ \qquad \wedge_{q \rightarrow b\, q'} ((b{=}\tau \wedge X_{p,q'}) \vee \vee_{p \rightarrow\tau^*\, p' \rightarrow b\, p''} (X_{p',q} \wedge X_{p'',q'}) \end{cases}$$

Tau-confluence reduction
[Groote & van de Pol 00]

- Form of partial-order reduction preserving branching equivalence

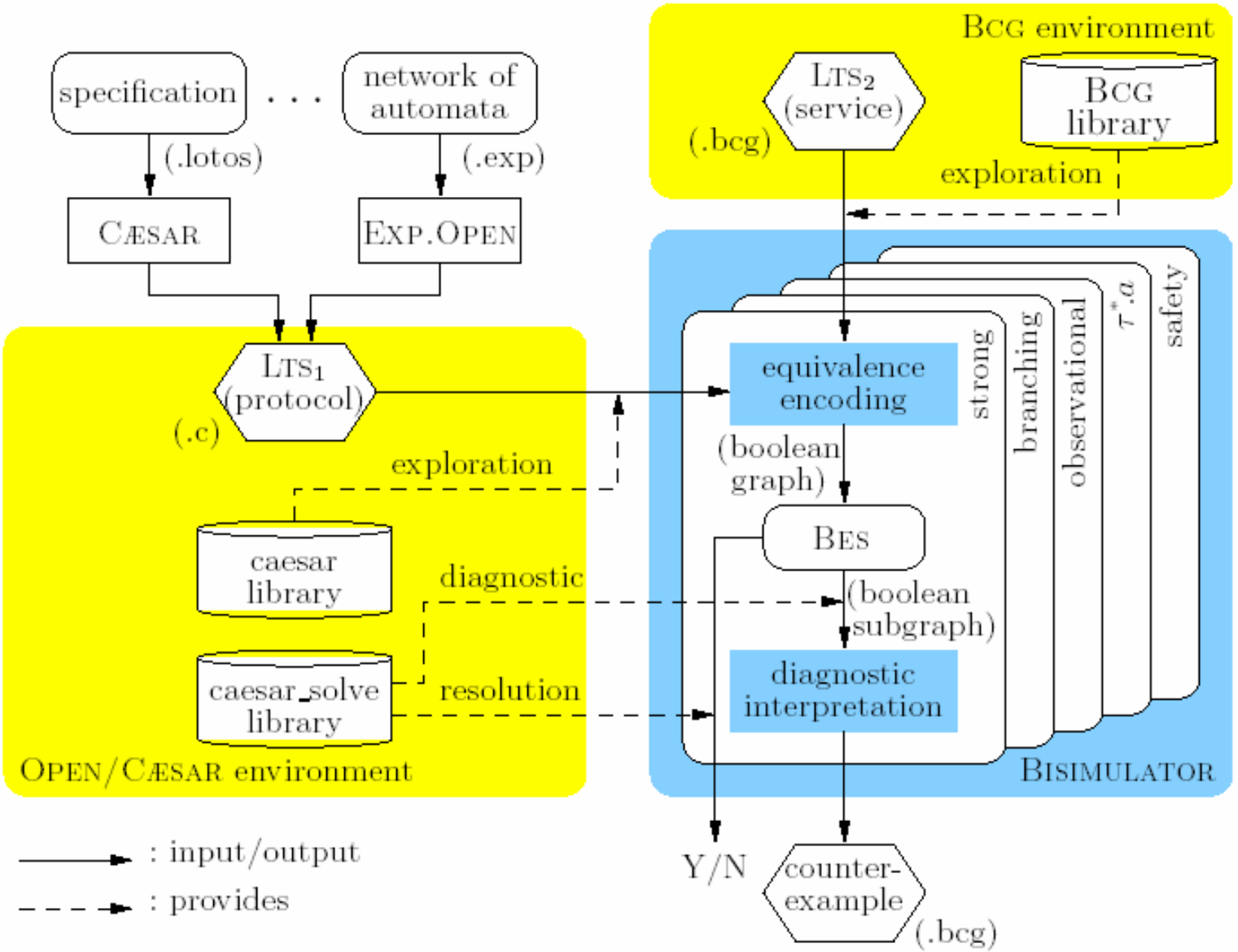


$$X_{p_1,p_2} = \bigwedge_{p_1 \xrightarrow{b} p_3} \left(p_2 \xrightarrow{b} p_3 \vee \bigvee_{p_2 \xrightarrow{b} p_4, p_3 \xrightarrow{\tau} p_4} X_{p_3,p_4} \vee \left((b = \tau) \wedge \bigvee_{p_3 \xrightarrow{\tau} p_2} X_{p_3,p_2} \right) \right)$$

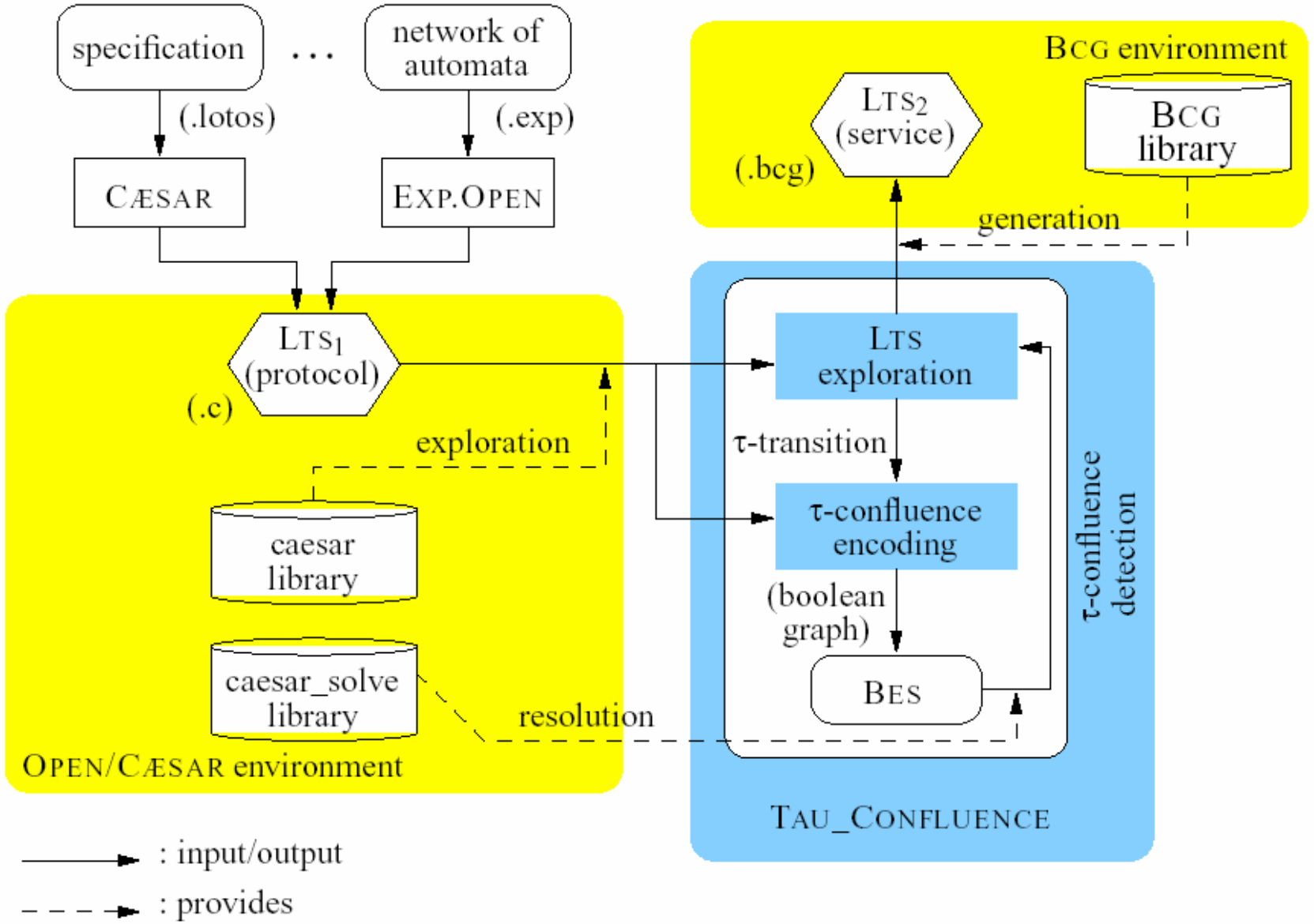
Caesar_Solve library

- On-the-fly resolution of alternation-free BESs [Mateescu-03]
- Developed in CADP using OPEN/CAESAR
- 5 linear-time sequential algorithms (12,000 lines of C)
  - DFS and BFS for general BESs
  - DFS memory-efficient for acyclic or conjunctive/disjunctive BESs
- 1 linear-time distributed algorithm (10,000 lines of C) [Joubert-Mateescu-04]
- Diagnostics (boolean subgraphs) [Mateescu-00]
- Generic, application-independent

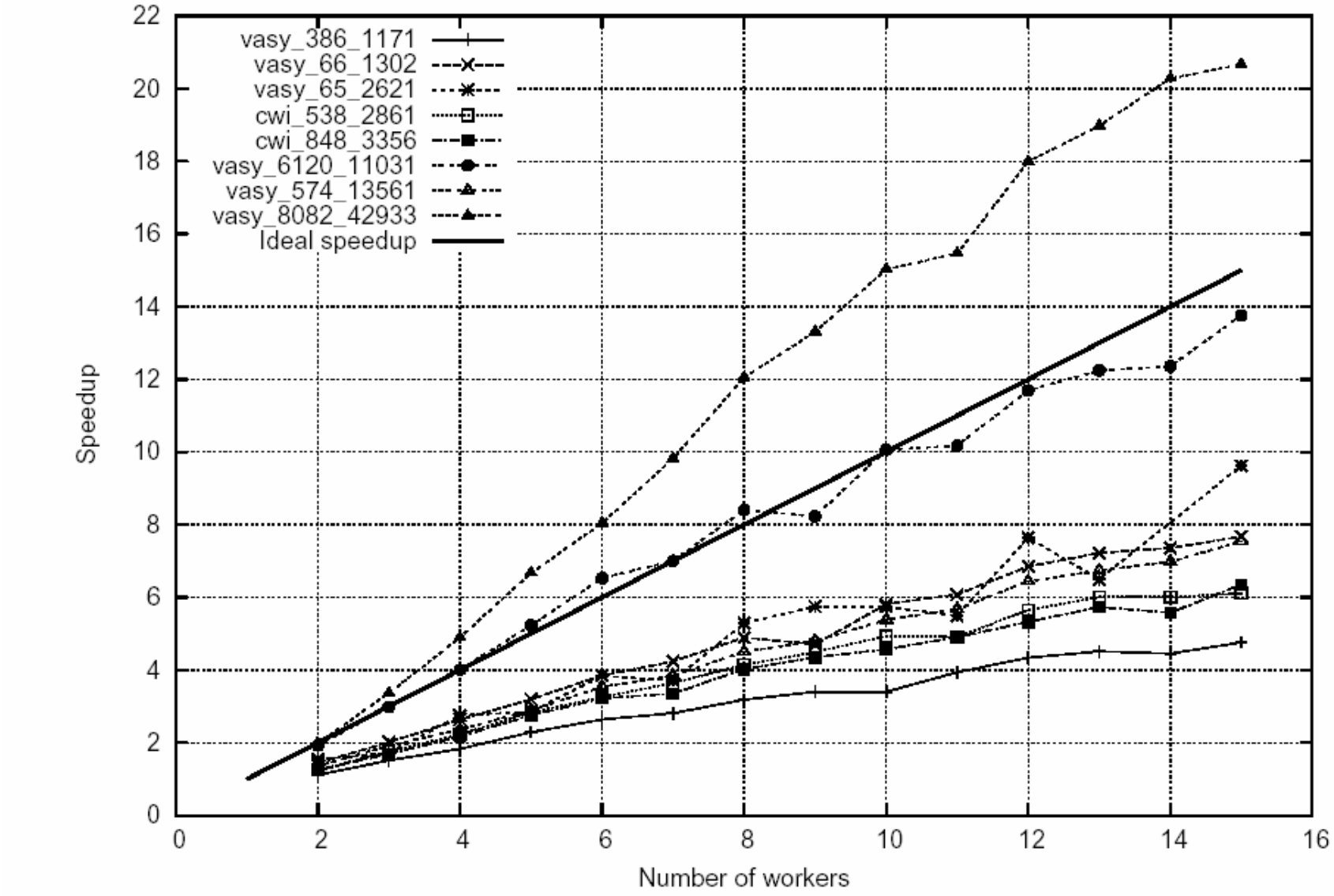
Architecture of Bisimulator



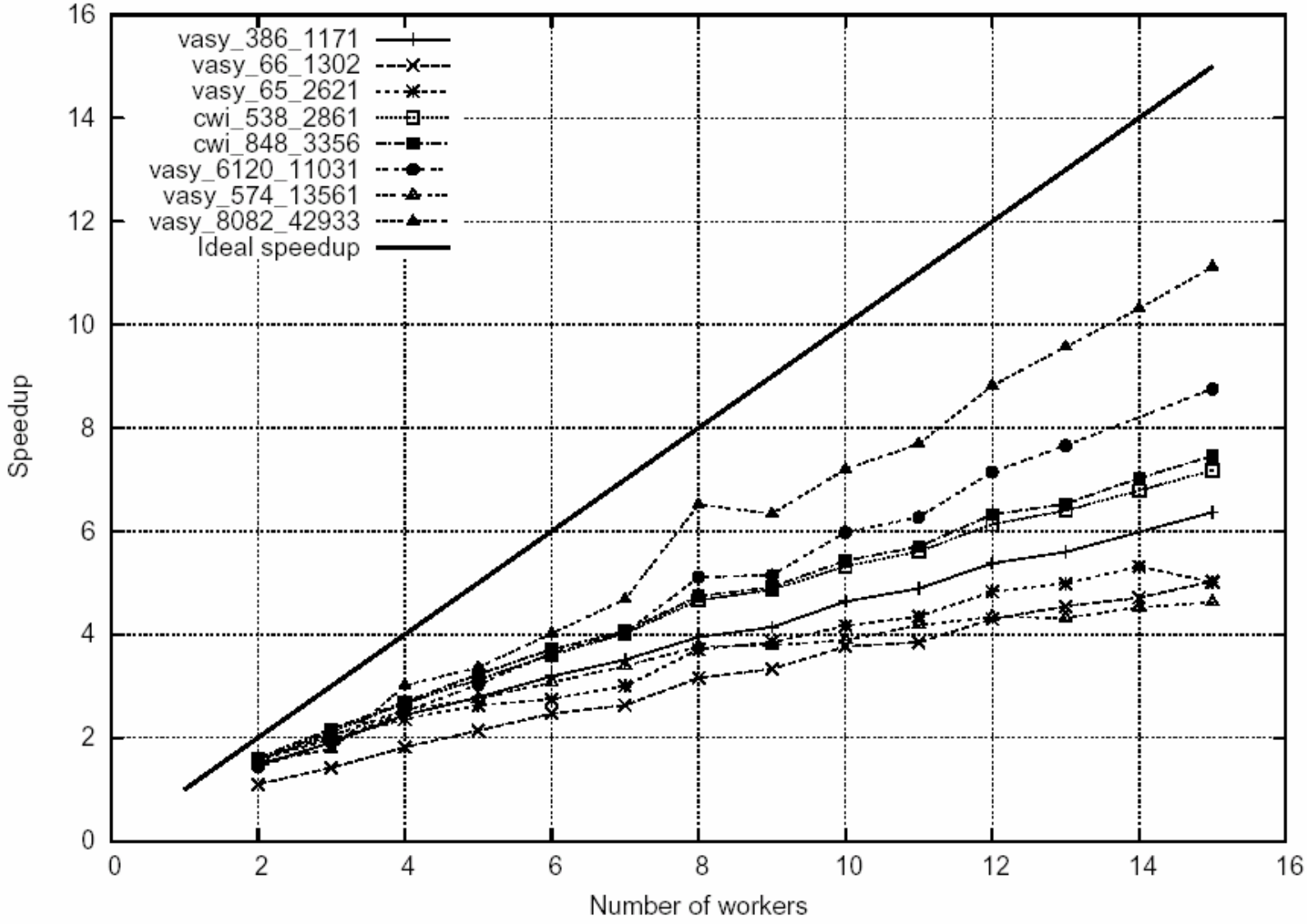
Architecture of Tau_Confluence



Distributed vs sequential Bisimulator (strong equivalence)



Distributed vs sequential Bisimulator (branching equivalence)



Reduction by tau-confluence

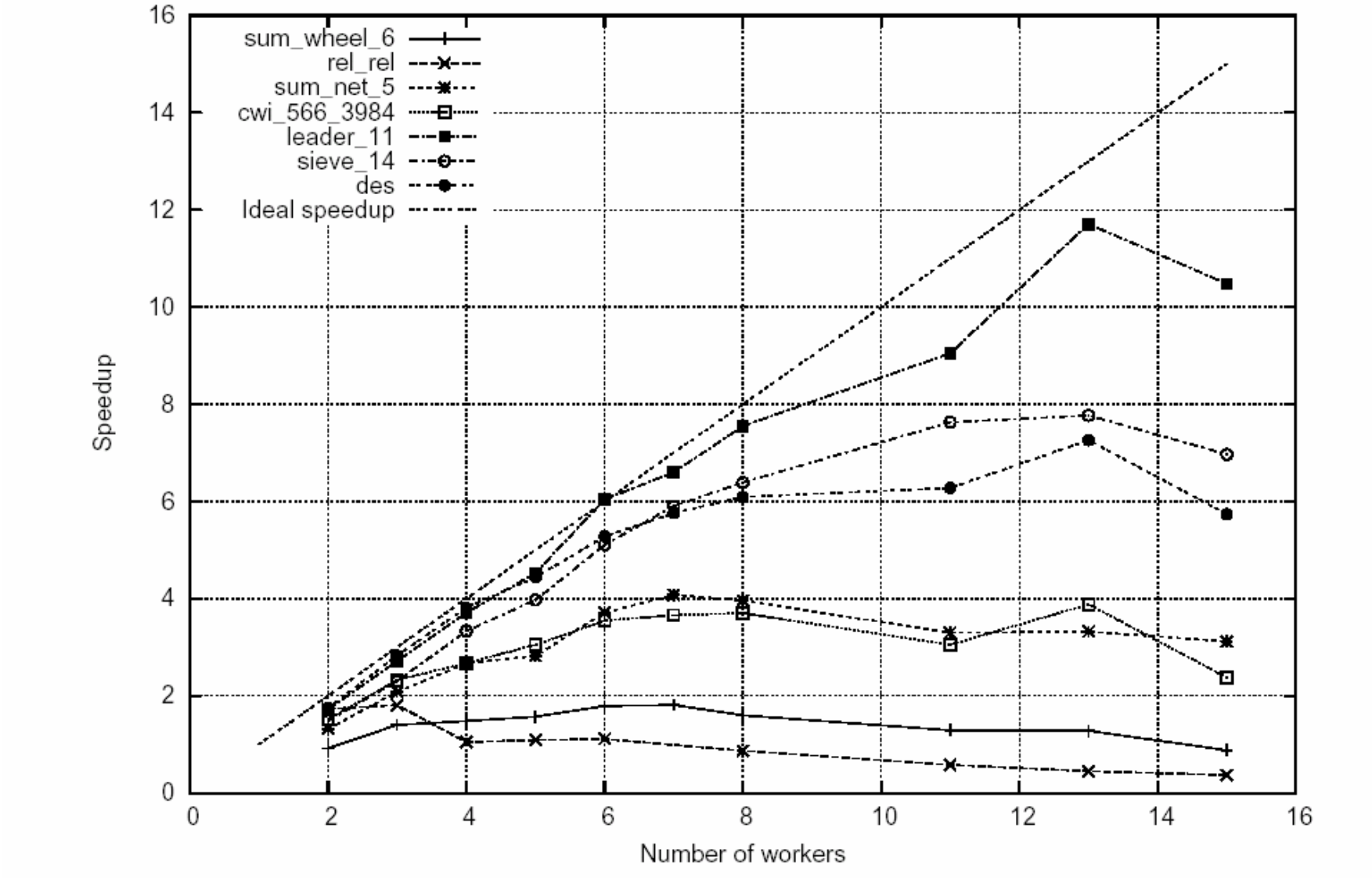
Example	Original			
	states	transitions	τ-transitions	size (KB)
leader_11	2 314 275	16 008 044	16 008 043	13 939
sieve_14	5 152 472	27 595 913	27 589 255	24 674
des	5 189 956	29 359 344	28 315 448	31 816
sum_net_5	533 007	3 169 061	3 169 060	2 752
cwi_566_3984	566 640	3 984 157	3 666 614	4 857
sum_wheel_6	156 957	767 211	767 210	695
rel_rel	150 911	1 249 375	1 147 831	3907

Table 1: Original LTSs sizes before τ-confluence reduction

Example	Reduced						
	states	%	trans.	%	τ-trans.	KB	%
leader_11	68	$3 \cdot 10^{-3}$	67	$4 \cdot 10^{-4}$	66	2	$2 \cdot 10^{-2}$
sieve_14	452	$9 \cdot 10^{-3}$	451	$2 \cdot 10^{-3}$	446	3	$1 \cdot 10^{-2}$
des	3 362	$7 \cdot 10^{-2}$	3 429	$1 \cdot 10^{-2}$	3 230	6	$2 \cdot 10^{-2}$
sum_net_5	2 548	$5 \cdot 10^{-1}$	2 852	$9 \cdot 10^{-2}$	2 851	5	$2 \cdot 10^{-1}$
cwi_566_3984	7 125	1.25	13 433	$3 \cdot 10^{-2}$	12 303	23	$5 \cdot 10^{-2}$
sum_wheel_6	2 881	1.8	3 384	$4 \cdot 10^{-1}$	3 383	6	$8 \cdot 10^{-1}$
rel_rel	121 978	81	603 600	48	566 277	1 308	34

Table 2: Reduced LTSs sizes after τ-confluence reduction, and ratio w.r.t. original LTSs

Distributed vs sequential Tau_Confluence



(small) Demo

Conclusion and future work

- Already done
  - Generic BES resolution library Caesar_Solve [Mateescu-03]
  - Distributed resolution [Joubert-Mateescu-04]
  - Bisimulator and Tau_Confluence
  - Multi-block BES resoluion algorithm [Joubert-05]
  - Model checking for alternation-free mu-calculus
  - Conformance test generation
- Ongoing work
  - Encoding of other equivalences and reductions
    - Markovian bisimulation [Hermanns-Siegle-99]
    - Tau-inertness [Groote-Sellink-90], weak tau-confluence [Groote-vandePol-00]
  - Study of other BES resolution strategies
  - Heterogeneous machines ➔ grids