Checking non-divergence, channel-bound and global-cooperation using SAT-solvers

Florent Avellaneda & Rémi Morin

Aix Marseille University

14 juin 2011

Remark

The design of a distributed system is complex.

Solution

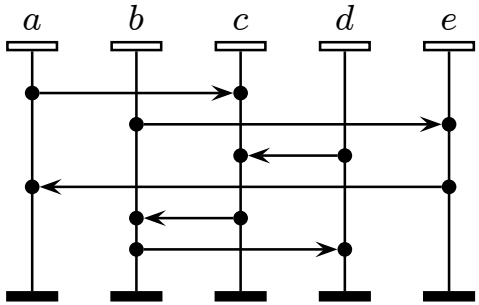
Use modeling.

Modeling tools

MSC (Message Sequence Chart)

Graphical description of message exchanges between processes in causal order.

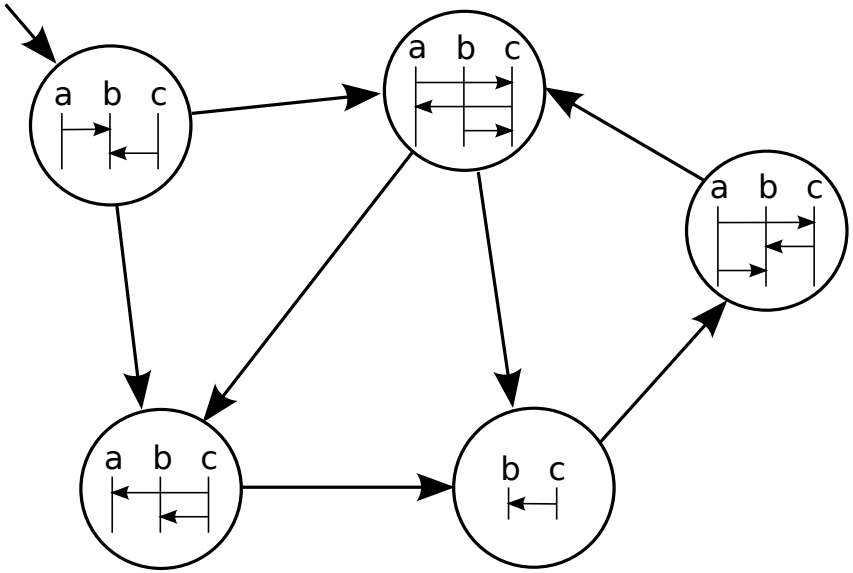
- The events occurring on the same process are linearly ordered.
- A message can be received only after it has been sent.



Modeling tools

MSG (High-level Message Sequence Chart)

Automaton where each transition is labeled by an MSC.



Advantage

We can automatically check properties on the models.

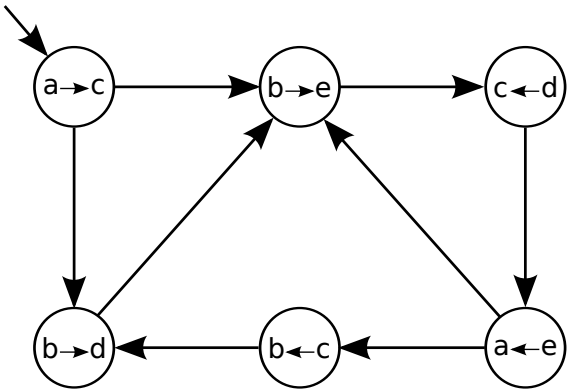
Objective of the presentation

Check some properties of automatic, fast and workable.

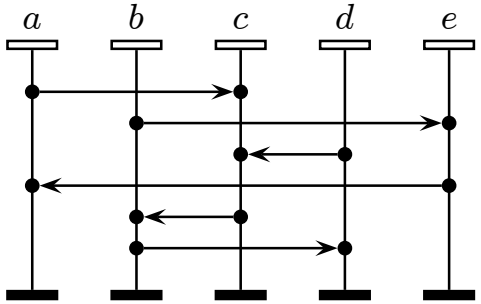
Plan

Basic concepts for the presentation

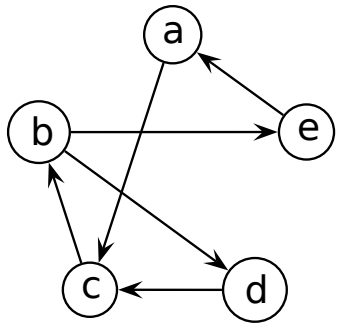
- **Simple** MSGs,
- MSC,
- Communication Graph of an MSC.



Simple MSG.



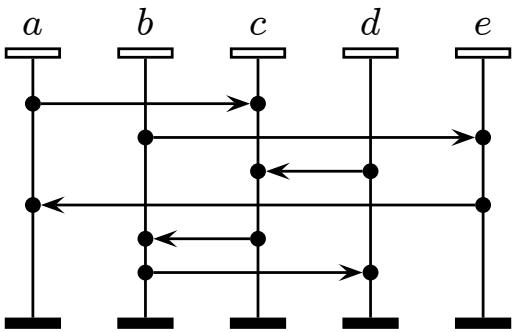
MSC.

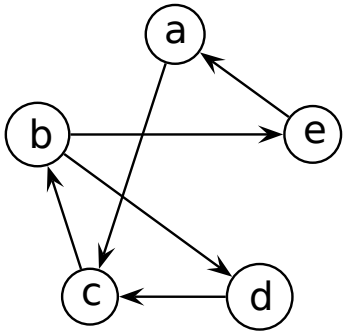


Communication Graph.

Définition

An MSC is *synchronized* if all connected components of the communication graph is strongly connected.





Plan

Plan

Problem description

Remark

Sendings and deliverings of messages often controlled by means of buffers.

Question

How to choose a correct buffer size ?

Approche : Cut problem

- Non-divergence : Is there a buffer size correct ?
- Sizing : Suppose there is a buffer size, what size to choose ?

Ben-Abdallah and Leue (*TACAS*, 1998)

An MSG diverges if and only if there exists a simple loop in which the MSC pattern repeated is not synchronized.

Ben-Abdallah and Leue (*TACAS*, 1998)

Exponential algorithm in the number of states, quadratic in the number of processes.

Alur and Yannakakis (*Concur*, 1999)

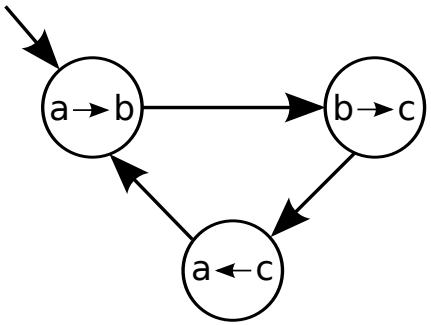
Exponential algorithm in the number of processes, quadratic in the size of the MSG.

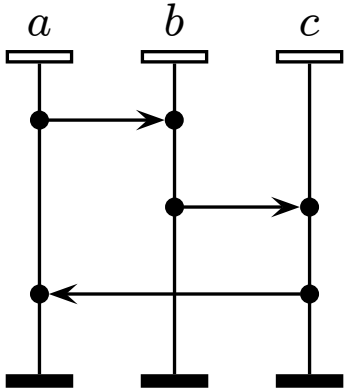
Alur and Yannakakis (*Concur*, 1999)

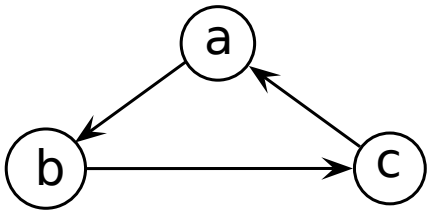
Divergence is NP-complete.

Definition

Channel (i, j) is *synchronized* if for all simple loop containing a label $i \rightarrow j$, there is a path from j to i in the communication graph.







Plan

Result

Reduction from *Divergence* to *SAT*.

Motivation

Using *SAT* solvers to check *non divergence*.

Idea

- Consider each channel one after the other.
- Given an MSG, for each channel (i, j), we construct a formula $Diverge_{ij}$ which is satisfiable iff there is a simple loop for which (i, j) is not synchronized.

Variables

The transitions $\delta \in \Delta$ and the processes $k \in \mathscr{I}$

Describes simple loops

$$Simple\_Loops = \bigwedge \begin{cases} \bigwedge\limits_{\delta \in \Delta} \left(\delta \rightarrow \bigvee\limits_{Dom(\delta')=Cod(\delta)} \delta' \right) \\ \bigwedge\limits_{\delta \in \Delta} \left(\delta \rightarrow \bigvee\limits_{Cod(\delta')=Dom(\delta)} \delta' \right) \\ \bigwedge\limits_{\delta \neq \delta' \text{ and } Dom(\delta)=Dom(\delta')} (\neg\delta \vee \neg\delta') \\ \bigwedge\limits_{\delta \neq \delta' \text{ and } Cod(\delta)=Cod(\delta')} (\neg\delta \vee \neg\delta') \end{cases}$$

True transitions form disjoint simple loops.

Reachable

$$Reachable_j = j \wedge \bigwedge_{s \rightarrow_\delta r} ((\delta \wedge s) \rightarrow r)$$

j and processes reachable from j are true.

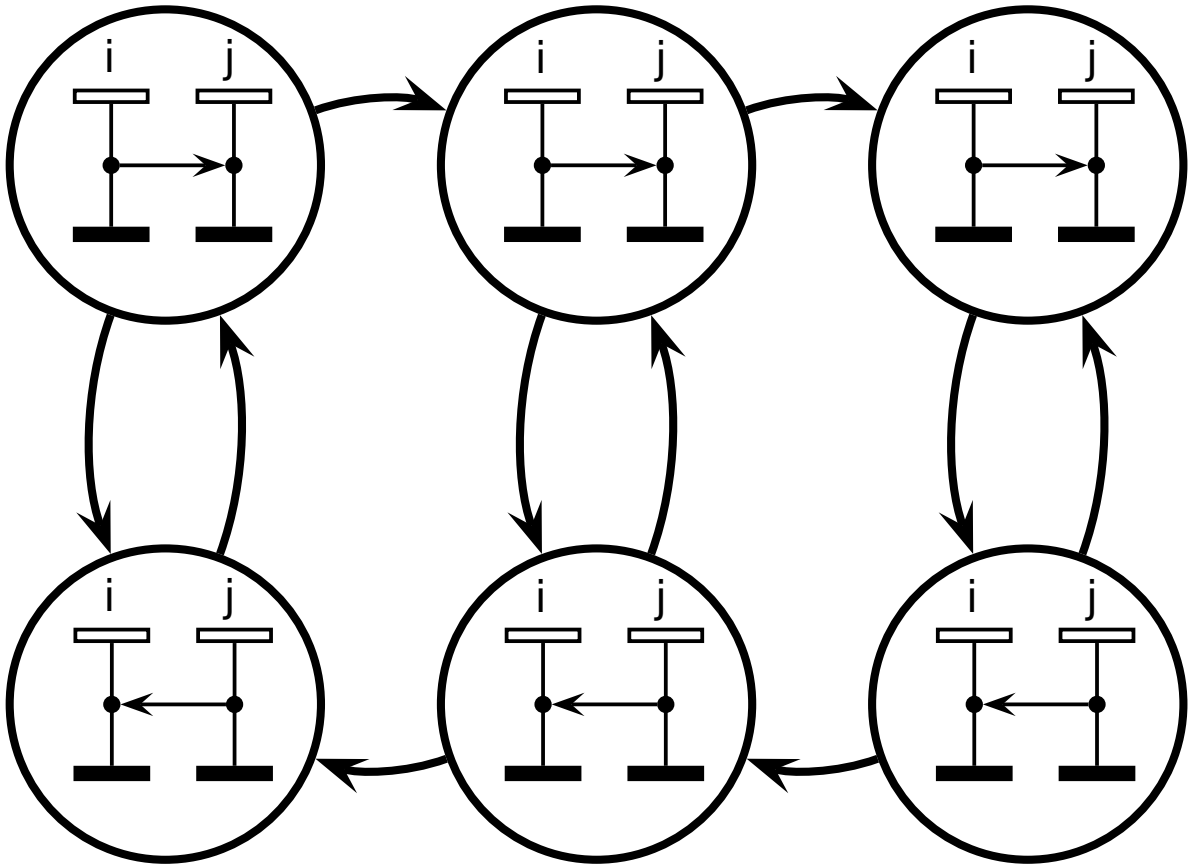
Divergence

$$Divergence_{i,j} = (\neg i) \wedge \bigvee_{i \rightarrow_\delta j} \delta$$

i is false and $i \rightarrow j$ is in the communication graph.

Plan

Simplified sliding window protocol



Window size	τ_{DIV}	τ_{SOFAT}	τ_{MSCan}
10	< 0.01	0.5	0.63
50	< 0.01	10	16
100	< 0.01	150	210
200	0.01	2400	
1000	0.08		
10000	7.1		
20000	25		
50000	160		

FIGURE: Runtime in s. for the simplified sliding window protocol

MSCan : Benedikt Bollig, Carsten Kern, Markus Schlütter, and Volker Stolz. (TACAS 2006)

SOFAT : Loïc Hélouët (SDL forum 1999)

Plan

Plan

Definition

An MSG is a globally-cooperative if for all loops, the communication graph has only one connected component.

Genest, Kuske and Muscholl (2006)

Deciding whether an MSG is globally cooperative is NP-complete.

Genest, Kuske and Muscholl (2006)

Any MSG globally-cooperative is implementable.

Plan

Reduction

Result

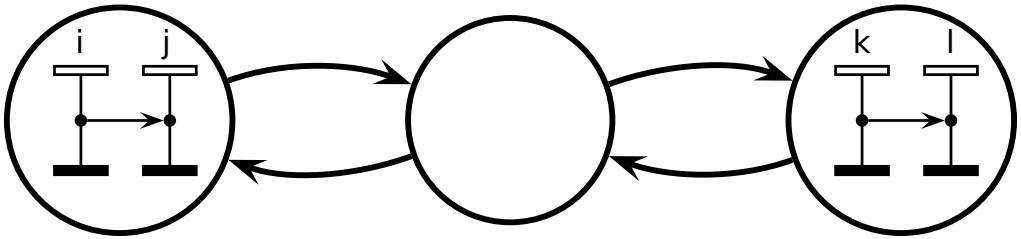
Reduction from *global-cooperation* to *SAT*.

Motivation

Using *SAT* solvers to check *global-cooperation*.

Proposition

Suppose that no edge is labeled by an empty MSC. Then the MSG is globally-cooperative if and only if the communication graph of any simple loop is connected.



Global-cooperation

$$\Phi_{\overline{\text{gc}}}(\mathscr{G}, i, j) = \mathit{Disjoint\_Loops} \wedge \mathit{Junction} \wedge \mathit{Connected}_j \wedge \mathit{Unconnected}_{i,j}$$

Junction

$$\mathit{Junction} = \bigwedge \begin{cases} \bigwedge\limits_{\delta,\delta' \in \Delta \text{ with } \delta \neq \delta'} & \neg\delta_1 \vee \neg\delta'_1 \\ \bigwedge\limits_{\delta \in \Delta \text{ and } x \in [1, N-1]} & \delta_x \rightarrow \delta_{x+1} \\ \bigwedge\limits_{\delta \in \Delta \text{ and } x \in [2, N]} & (\delta_x \wedge \neg\delta_{x-1}) \rightarrow \bigvee\limits_{cod(\delta')=dom(\delta)} \delta'_{x-1} \end{cases}$$

Plan

Window size	τ_{DIV}	τ_{GC}	τ_{SOFAT}	τ_{MSCan}
10	< 0.01	0.01	0.5	0.63
50	< 0.01	0.35	10	16
100	< 0.01	1.90	150	210
200	0.01	10.6	2400	
1000	0.08	1100		
10000	7.1			
20000	25			
50000	160			

FIGURE: Runtime in s. for the simplified sliding window protocol

Plan

Plan

Muscholl et Lohrey (*Inf. & Comput.*, 2004)

The problem "For an MSG and a buffer size, can all scenarios can they run without any overloading ?" is co-NP-complete.

Consequence of *Divergence* is NP-complete

Find an **optimal** *size*, an **approximation** or even a correct *size* is NP-hard.

Plan

First approach

- Consider only the MSG *non-divergent*.
- Find a **reasonable** *size*.

Result

Let a *non divergent* MSG with n states and x processes, then $x \times n$ is a correct buffer size.

Idea

For a non-divergent MSG, if we do not exchange messages in a canal, at each loop a new process will be blocked.

Second approach

We can adapt the reduction of Divergence to :

- check that a size is correct,
- compute the optimal size.

Plan

Results

- Simple reduction from divergence to SAT.
- Reduction from global-cooperation to SAT.
- Simple buffer size for non divergent MSGs.
- Reduction from optimal buffer size to SAT.

Perspectives

- Evaluate with random MSGs and other protocols.
- Try other formula.
- Compare with other SAT-solvers.

Thank you.