Ideal Abstraction for Depth-Bounded Processes

Thomas Wies   Damien Zufferey   Thomas A. Henzinger

IST Austria

October 11, 2011

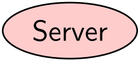
What are Depth-Bounded Processes (DBP) ?

As buzzwords: concurrent/distributed message-passing programs with process creation and mobility. (Warning restrictions may apply.)

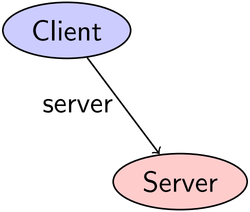
For the programmers: some class of programs using the actor model (Erlang, Scala, Akka, ActorFoundry, . . .)

For the theoreticians: a fragment of the π-calculus.

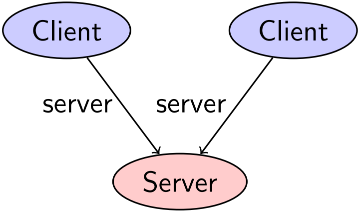
Example: client-server communication pattern



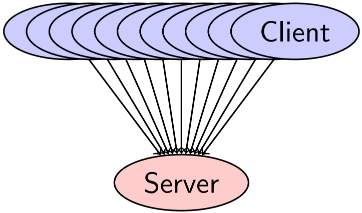
Example: client-server communication pattern



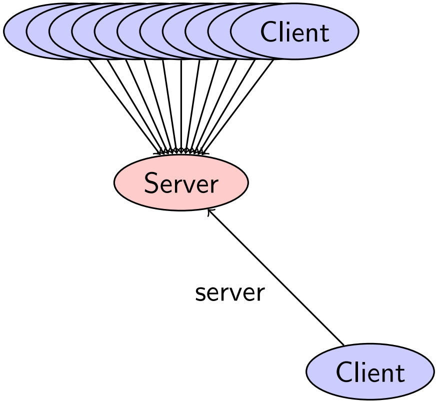
Example: client-server communication pattern



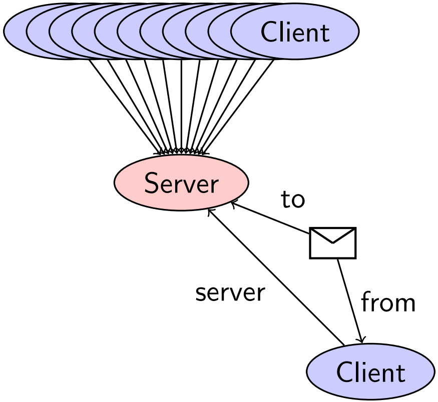
Example: client-server communication pattern



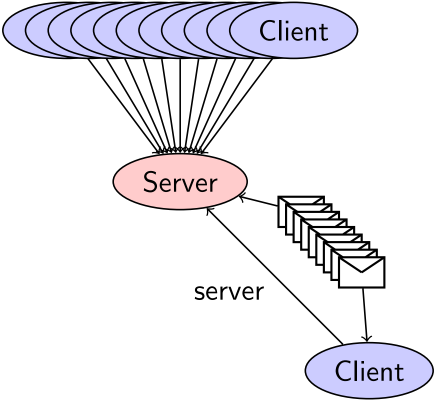
Example: client-server communication pattern



Example: client-server communication pattern

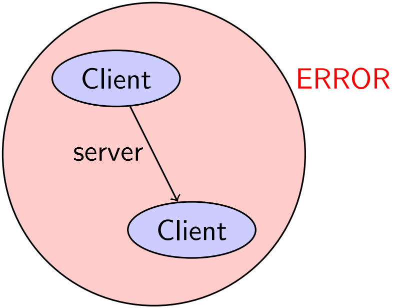


Example: client-server communication pattern

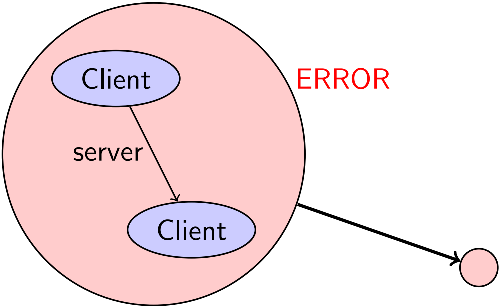


What kind of properties are we looking at ?

Safety properties, more precisely the control-state reachability problem (aka covering problem).



Safety properties, more precisely the control-state reachability problem (aka covering problem).



What kind of properties are we looking at ?

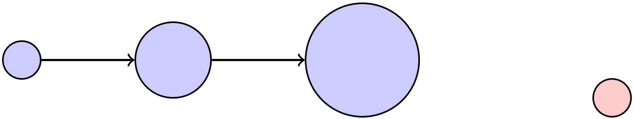
Safety properties, more precisely the control-state reachability problem (aka covering problem).

What kind of properties are we looking at ?

Safety properties, more precisely the control-state reachability problem (aka covering problem).

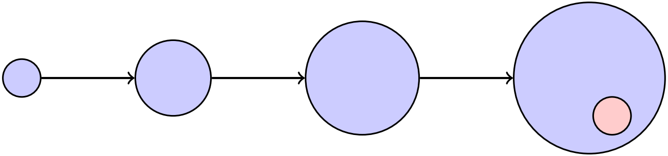
What kind of properties are we looking at ?

Safety properties, more precisely the control-state reachability problem (aka covering problem).



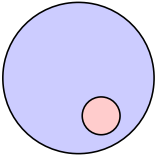
What kind of properties are we looking at ?

Safety properties, more precisely the control-state reachability problem (aka covering problem).

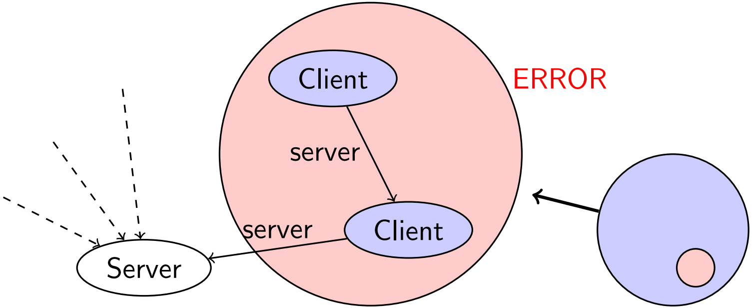


What kind of properties are we looking at ?

Safety properties, more precisely the control-state reachability problem (aka covering problem).



Safety properties, more precisely the control-state reachability problem (aka covering problem).



Formal model: WSTS

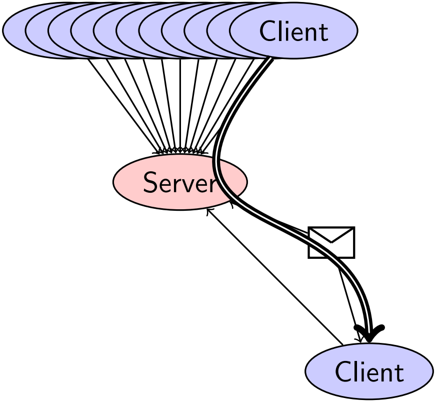
A well-structured transition system (WSTS) is a transition system $\langle S, \rightarrow, \leq \rangle$ such that:

- $\leq$ is a well-quasi-ordering (wqo), i.e. well-founded + no infinite antichain.
- compatibility of $\leq$ w.r.t. $\rightarrow$

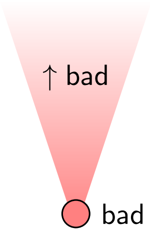
$$\forall \qquad \begin{array}{ccc} t & \xrightarrow{*} & t' \\ \rotatebox[origin=c]{90}{$\leq$} & & \rotatebox[origin=c]{90}{$\leq$} \\ s & \longrightarrow & s' \end{array} \qquad \exists$$

For more detail see:
[Finkel and Schnoebelen, 2001, Abdulla et al., 1996]

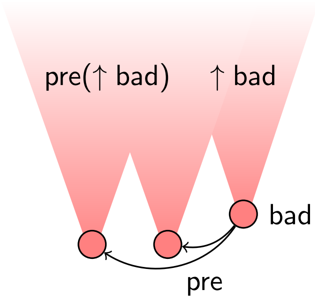
System with a bound on the longest acyclic path.
(Concretely: it is not possible to encode an infinite memory.)



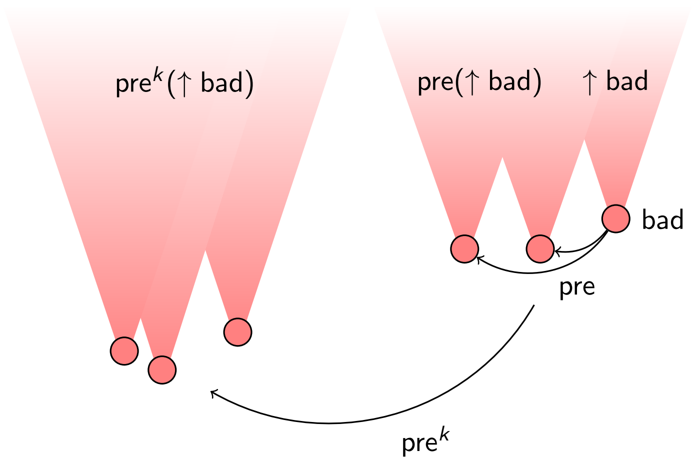
Backward algorithm for covering



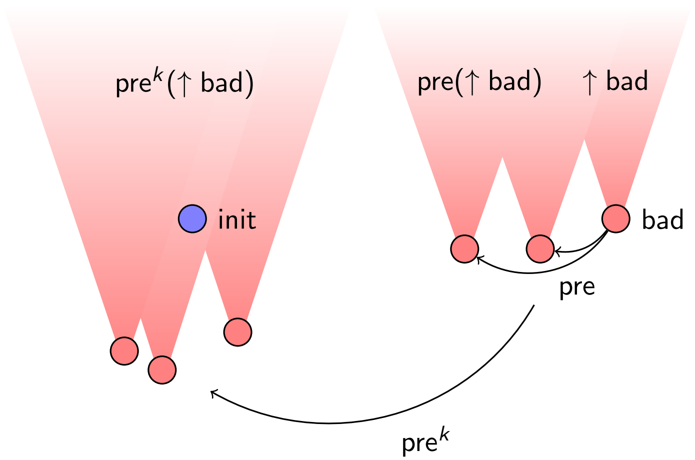
Backward algorithm for covering



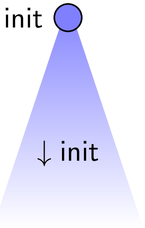
Backward algorithm for covering



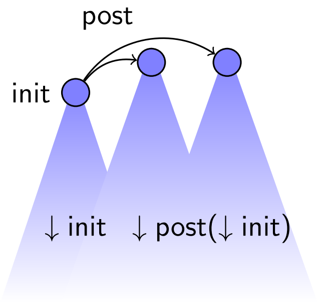
Backward algorithm for covering



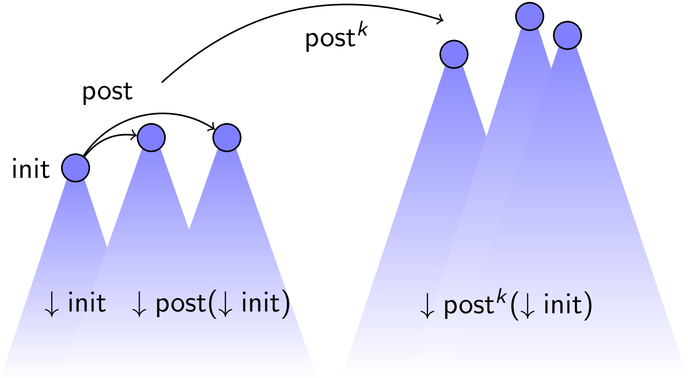
Forward algorithm for covering



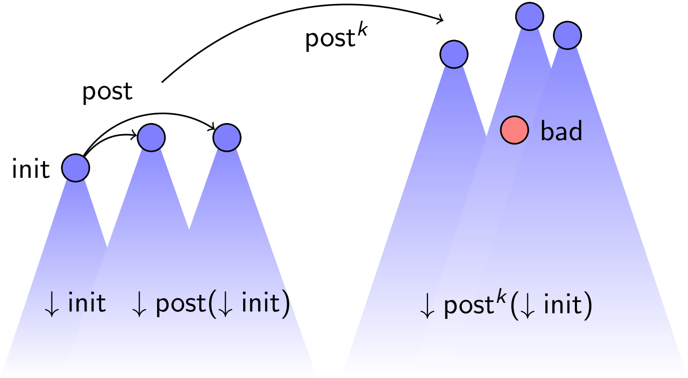
Forward algorithm for covering



Forward algorithm for covering

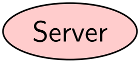


Forward algorithm for covering



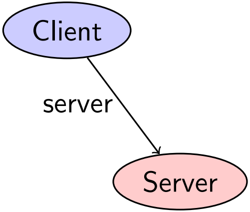
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



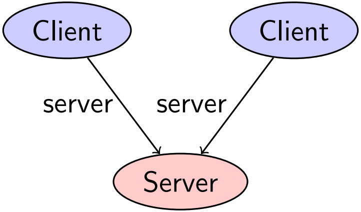
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



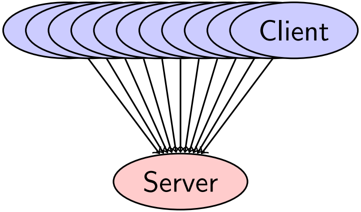
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



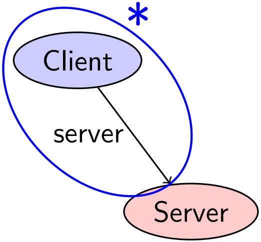
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]

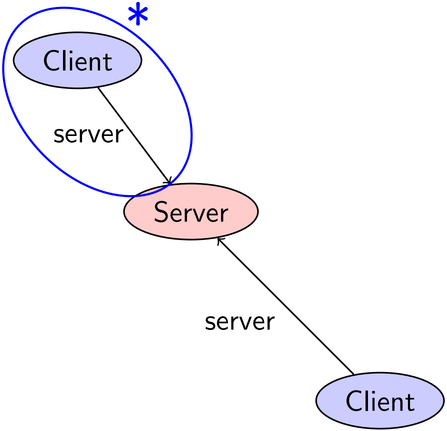


Adequate domain of limits

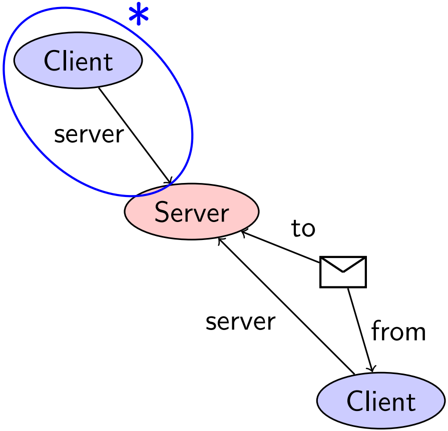
ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]

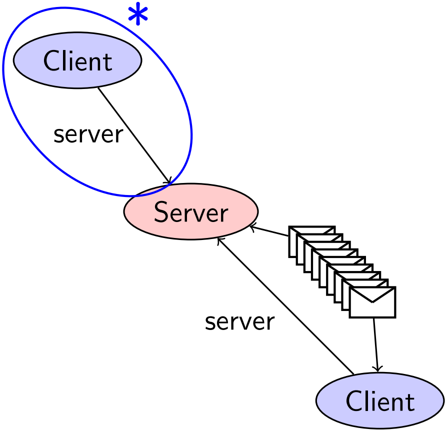


ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]

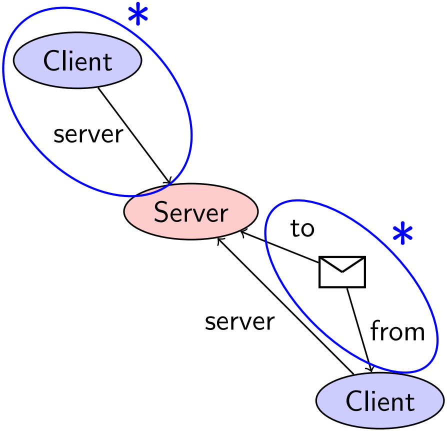


Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]

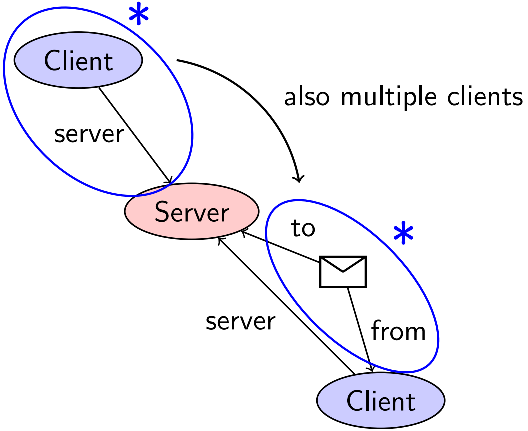


ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



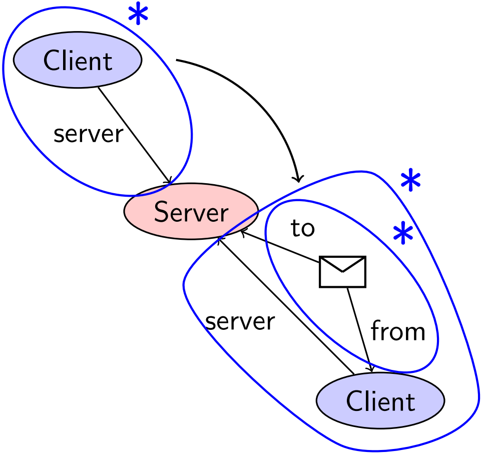
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



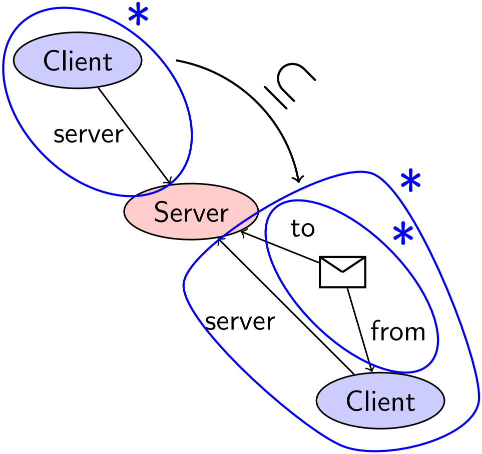
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



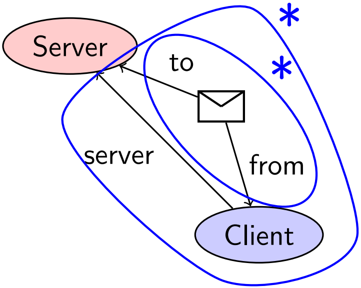
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



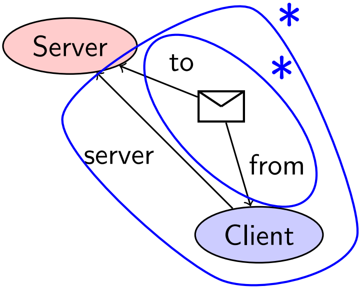
Adequate domain of limits

ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]



ADL: [Geeraerts et al., 2006]
Further developed in [Finkel and Goubault-Larrecq, 2009]
Applied to DBP in [Wies et al., 2010]

$$(\nu x)(\mathit{Server}(x) \mid !(\nu y)(\mathit{Client}(y, x) | !\mathit{Messages}(x, y)))$$



When does acceleration work ? (flat systems)

Usually forward algorithms are based on acceleration. By acceleration we mean computing the result of executing a loop infinitely many time.

We can see this as computing the result of execution traces of length $< \omega^2$. Concretely, it means that the algorithm can saturate the covering set by executing only simple loops (see [Bardin et al., 2005]). This condition is known as flattability.

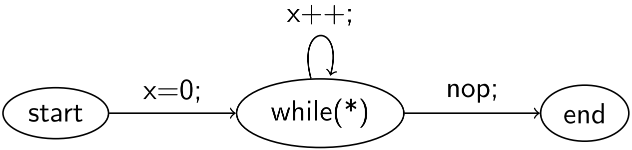
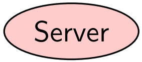
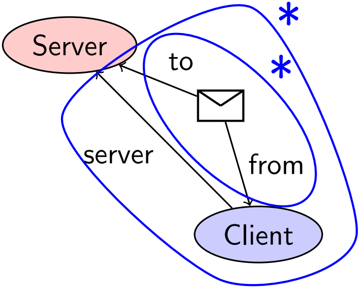


Figure: Example of a flat program

initial configuration:



covering set:

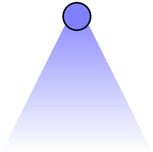


How many steps are there between the initial configuration and the final configuration ?
ω^2 steps

Hence, we need to consider nested loops if we want to compute the covering set.

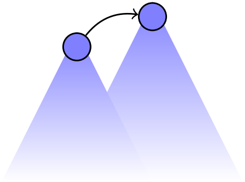
From acceleration to widening

Acceleration considers transitions. Widening only states.

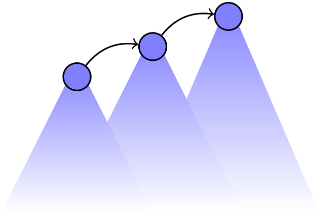


From acceleration to widening

Acceleration considers transitions. Widening only states.

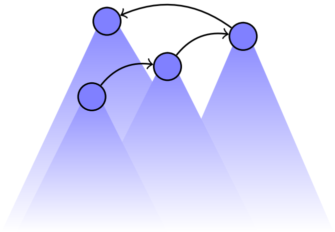


Acceleration considers transitions. Widening only states.



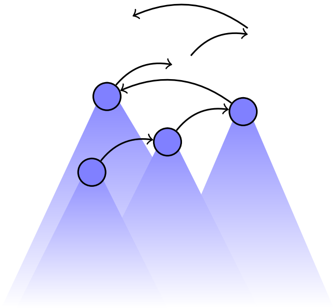
From acceleration to widening

Acceleration considers transitions. Widening only states.

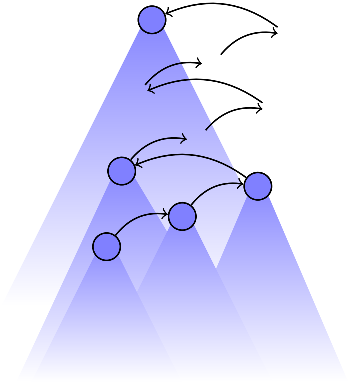


From acceleration to widening

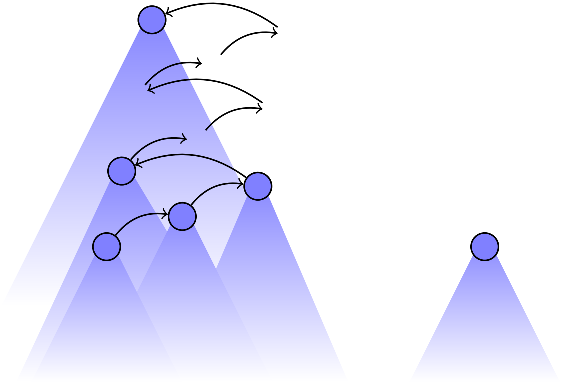
Acceleration considers transitions. Widening only states.



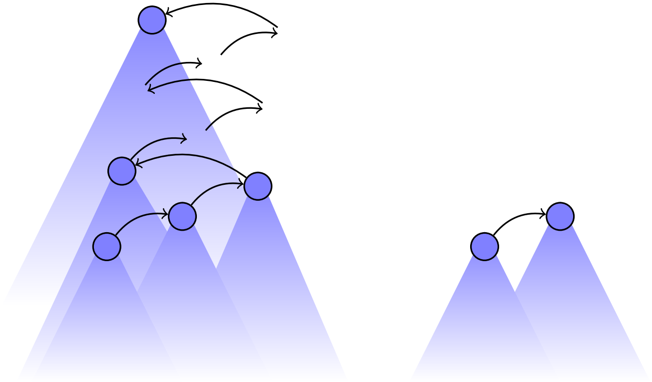
Acceleration considers transitions. Widening only states.



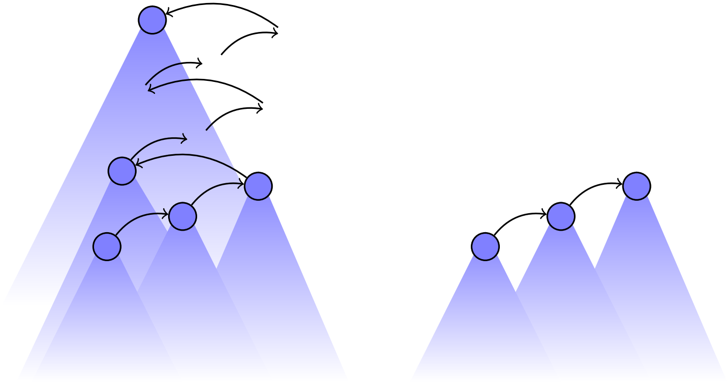
Acceleration considers transitions. Widening only states.



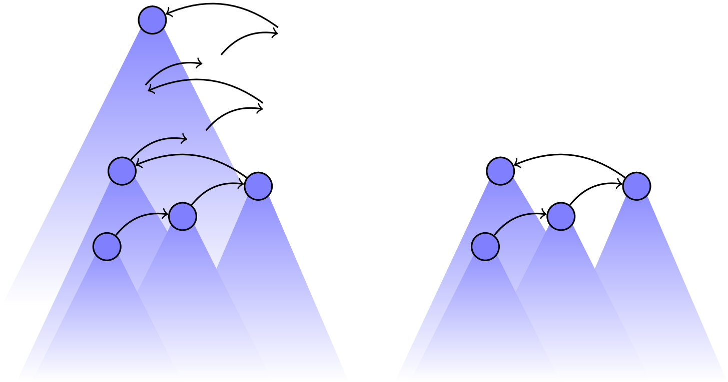
Acceleration considers transitions. Widening only states.



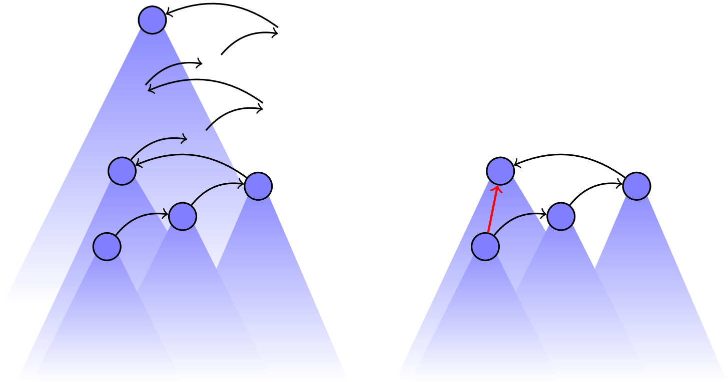
Acceleration considers transitions. Widening only states.



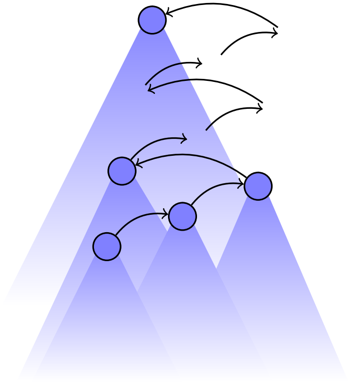
Acceleration considers transitions. Widening only states.



Acceleration considers transitions. Widening only states.



Acceleration considers transitions. Widening only states.



Abstract interpretation: Domains

- Concrete domain: $D = \mathcal{P}(S)$
- Abstract domain: $D_{\downarrow} = \{ \downarrow X \mid X \subseteq S \}$

The abstract domain can be further refined from the set of downward-closed set to the set of ideals (downward-closed and *directed*).

- Abstract domain 2: D_{Idl}

An arbitray downward-closed set can be represented as the finite union of ideals.

Widening (1)

Goal: try to mimic acceleration (when possible), and force termination

A set-widening operator (∇) for a poset X is partial function ($\mathcal{P}(X) \to X$) that satisfies:

Covering : for all $Y \subseteq X$, $y \in Y \Rightarrow y \leq \nabla(Y)$;

Termination : widening of any ascending chain stabilizes.

Reason of using a set-widening operator: we need the history.

Widening (2)

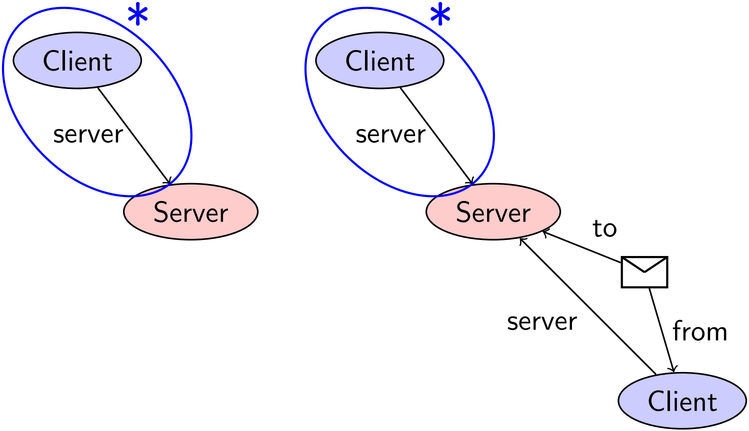
Lifting a widening operators from $Idl(S)$ to D_{Idl}: going from elements of the domain to finite powerset is non-trivial. We assume that the ordering is a *bqo*. Thus $Idl(S)$ is also a bqo.

Given an ascending chain: $C = \{L_i\}_{0 \leq i \leq n}, C \subseteq D_{Idl}$ (history)

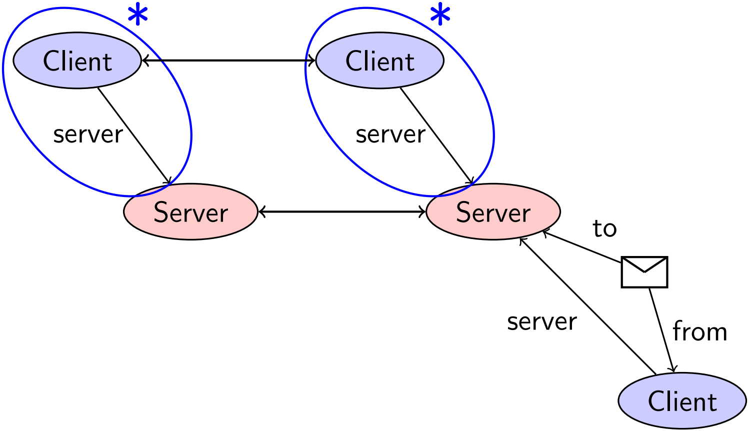
- $\nabla(\{L_0\}) = \{L_0\}$
- $\nabla(\{L_0, \ldots, L_i\}) = \nabla(\{L_0, \ldots, L_{i-1}\}) \sqcup$
  $\{\nabla_S(\mathcal{I}) \ \mid \mathcal{I}$ max ascending chain in$\nabla(\{L_0, \ldots, L_{i-1}\})\}$

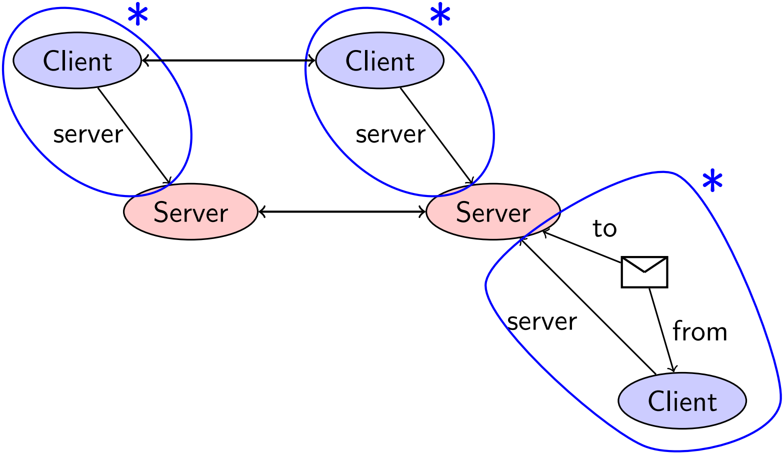
Why a *bqo* ? To avoid having an infinite antichain in $Idl(S)$.

Set-widening for DBP (1)

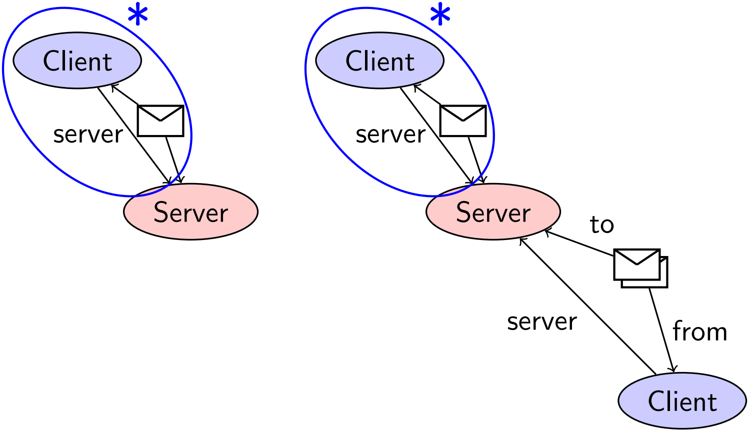


Set-widening for DBP (1)

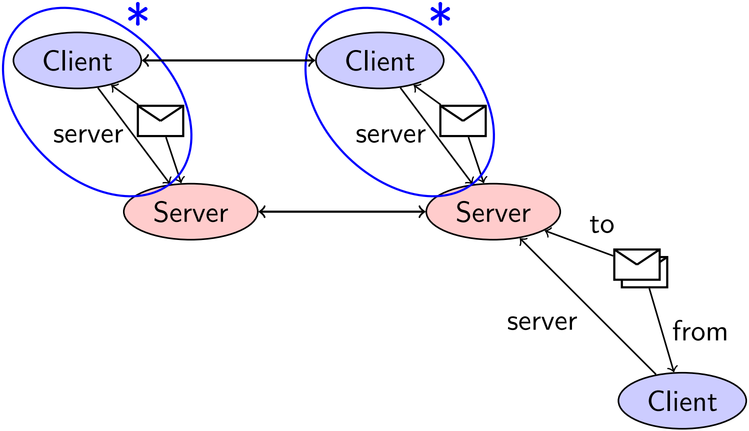



*
Client
server
Server
*
Client
server
Server
*
to
server
from
Client

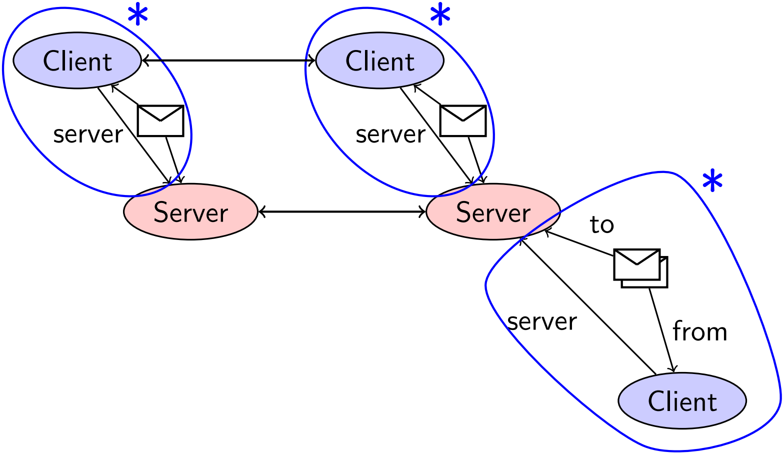
Set-widening for DBP (2)



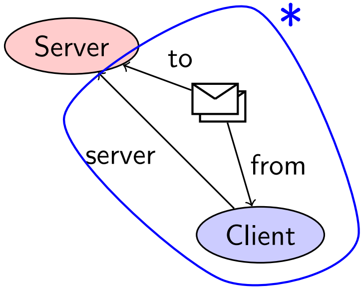
Set-widening for DBP (2)



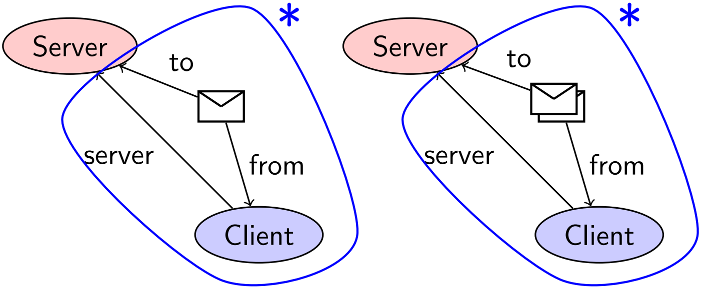
Set-widening for DBP (2)



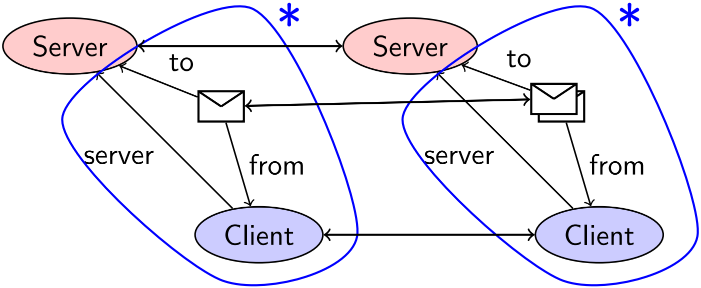
Set-widening for DBP (3)



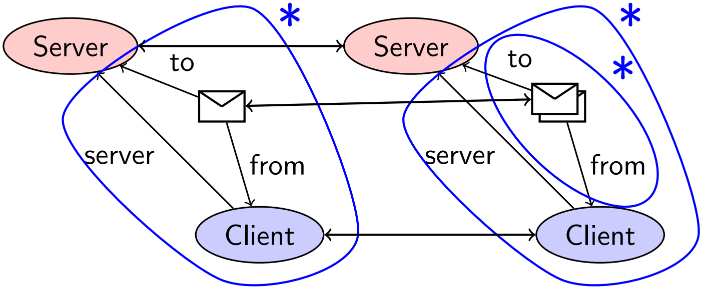
Set-widening for DBP (3)



Set-widening for DBP (3)



Set-widening for DBP (3)



What about the precision ?

- Acceleration and widening seems like the *extreme* ends of some spectrum.
- Is there a class of nested loops for which we can compute exactly the result ?
- Can we get a good characterisation of the programs for which this kind of widening matches acceleration ?

Recap

- DBP is one of the largest fragment of the π-calculus for which interesting verification questions are still decidable.
- Not yet clear what is the right way of handling features such as process creation and mobility.
- WSTS approach gives decidability a result, now we are working on an efficient analysis.

Questions ?

References I

Abdulla, P. A., Cerans, K., Jonsson, B. and Tsay, Y.-K. (1996).
General Decidability Theorems for Infinite-State Systems.
In LICS pp. 313–321,.

Bardin, S., Finkel, A., Leroux, J. and Schnoebelen, P. (2005).
Flat Acceleration in Symbolic Model Checking.
In ATVA pp. 474–488,.

Finkel, A. and Goubault-Larrecq, J. (2009).
Forward Analysis for WSTS, Part I: Completions.
In STACS vol. 09001, of Dagstuhl Sem. Proc. pp. 433–444,.

Finkel, A. and Schnoebelen, P. (2001).
Well-structured transition systems everywhere!
Theor. Comput. Sci. *256*, 63–92.

Geeraerts, G., Raskin, J.-F. and Van Begin, L. (2006).
Expand, Enlarge and Check: New algorithms for the coverability problem of WSTS.
J. Comput. Syst. Sci. *72*, 180–203.

Meyer, R. (2008).
On Boundedness in Depth in the pi-Calculus.
In IFIP TCS vol. 273, of IFIP pp. 477–489, Springer.

Wies, T., Zufferey, D. and Henzinger, T. A. (2010).
Forward Analysis of Depth-Bounded Processes.
In FoSSaCS 2010 vol. 4349, of LNCS pp. 94–108, Springer.