

# Commutation with Termination; Up-to Techniques for Bisimulation

Damien Pous - ENS Lyon, France

ICALP'05  
July 13, 2005  
Lisbon, Portugal

## Outline

### Rewriting

- Confluence
- Commutation
- Generalisation of Newman's Lemma

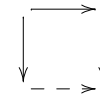
### Bisimulation

- Definition
- Up-to techniques

### Putting it all together

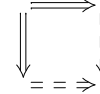
## Rewriting: Confluence

### ▶ Strong confluence:



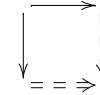
For all  $P, P', Q$  s.t.  $P \rightarrow P'$  and  $P \rightarrow Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow Q'$  and  $P' \rightarrow Q'$ .

### ▶ Confluence:



For all  $P, P', Q$  s.t.  $P \rightarrow^* P'$  and  $P \rightarrow^* Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow^* Q'$  and  $P' \rightarrow^* Q'$ .

### ▶ Local confluence:



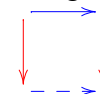
For all  $P, P', Q$  s.t.  $P \rightarrow P'$  and  $P \rightarrow Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow^* Q'$  and  $P' \rightarrow^* Q'$ .

### ▶ Newman's Lemma:

"Local confluence and termination entail confluence".

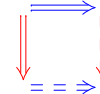
## Rewriting: Commutation

### ▶ Strong commutation:



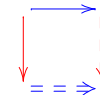
For all  $P, P', Q$  s.t.  $P \rightarrow P'$  and  $P \rightarrow Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow Q'$  and  $P' \rightarrow Q'$ .

### ▶ Commutation:



For all  $P, P', Q$  s.t.  $P \rightarrow^* P'$  and  $P \rightarrow^* Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow^* Q'$  and  $P' \rightarrow^* Q'$ .

### ▶ Local commutation:



For all  $P, P', Q$  s.t.  $P \rightarrow P'$  and  $P \rightarrow Q$ ,  
there exists  $Q'$  s.t.  $Q \rightarrow^* Q'$  and  $P' \rightarrow^* Q'$ .

### ▶ Generalisation of Newman's Lemma ?

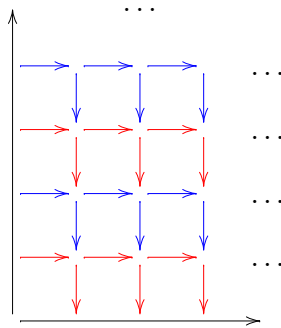
# Rewriting: Generalisation of Newman's Lemma

Commutation is obtained from local commutation and and:

- ▶ the termination of both relations: **No!**



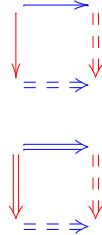
- ▶ the termination of  $\rightarrow \cup \rightarrow$  (standard),
  - ▶ the termination of  $\rightarrow^+ \rightarrow^+$  (this work).
- Neither  $\rightarrow$  nor  $\rightarrow$  need to terminate !



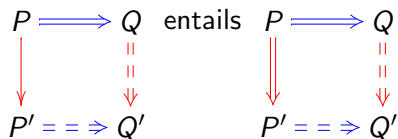
## Proof sketch (1)

- ▶ If  $\left\{ \begin{array}{l} \forall P, P', Q, P \rightarrow P' \wedge P \rightarrow Q \\ \Rightarrow \exists Q', Q \rightarrow^* Q' \wedge P' \rightarrow^* Q' \\ \rightarrow^+ \rightarrow^+ \text{ terminates} \end{array} \right.$ ,

then  $\forall P, P', Q, P \rightarrow^* P' \wedge P \rightarrow^* Q \Rightarrow \exists Q', Q \rightarrow^* Q' \wedge P' \rightarrow^* Q'$ .



- ▶ Semi-local commutation:



- ▶ "Stair" relation:  $\rightsquigarrow \triangleq (\rightarrow^+ \rightarrow^+)^+$

## Proof sketch (2)

- ▶  $\theta(P) : \forall P', Q, P \rightarrow P' \wedge P \rightarrow^* Q \Rightarrow \exists Q', Q \rightarrow^* Q' \wedge P' \rightarrow^* Q'$ .

- ▶ Well-founded induction on the termination of  $\rightsquigarrow = (\rightarrow^+ \rightarrow^+)^+$ : we have to prove  $\forall P, \phi(P) \Rightarrow \theta(P)$ .

External induction hypothesis:  
 $\phi(P) : \forall P'', P \rightsquigarrow P'' \Rightarrow \theta(P'')$ .

- ▶ We reformulate our goal as:

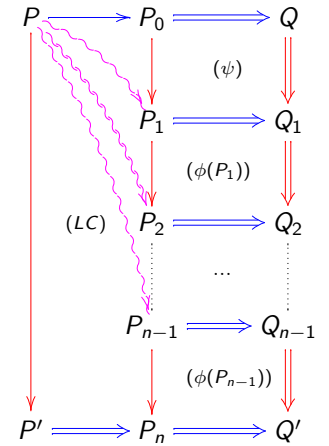
$$\forall P, Q, P \rightarrow^* Q \Rightarrow \phi(P) \Rightarrow \forall P', P \rightarrow P' \Rightarrow \exists Q', Q \rightarrow^* Q' \wedge P' \rightarrow^* Q'.$$

- ▶ Structural induction on  $P \rightarrow^* Q$ .

- ▶ Non-trivial case:  $P \rightarrow P_0 \rightarrow^* Q$ .

Internal induction hypothesis:

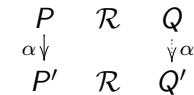
$$\psi : \phi(P_0) \Rightarrow \forall P_1, P_0 \rightarrow P_1 \Rightarrow \exists Q_1, Q_0 \rightarrow^* Q_1 \wedge P_1 \rightarrow^* Q_1.$$



## Bisimulation: Definition

- ▶ LTS: processes  $(P, Q..)$ , labelled transitions  $(P \xrightarrow{\alpha} P')$
- ▶  $\mathcal{R}$  is a **bisimulation** if:

$$\forall P, Q, P', PRQ \wedge P \xrightarrow{\alpha} P' \Rightarrow \exists Q', P'RQ' \wedge Q \xrightarrow{\alpha} Q'$$



- ▶ **bisimilarity**:  $\sim \triangleq \bigcup \{ \mathcal{R}, \mathcal{R} \text{ bisimulation} \}$

## Bisimulation: Definition

- ▶ LTS: processes  $(P, Q..)$ , labelled transitions  $(P \xrightarrow{\alpha} P')$
- ▶ Weak case:
  - ▶  $\alpha \in \{a, b..\} \cup \{\tau\}$ , the **silent** action  $\tau$  is **not observable**.
  - ▶ **Weak transitions**:

$$\begin{cases} \xrightarrow{\tau} \triangleq \xrightarrow{\tau}^* \\ \xrightarrow{a} \triangleq \xrightarrow{\tau^* a \tau^*} \end{cases}$$

- ▶  $\mathcal{R}$  is a **bisimulation** if:

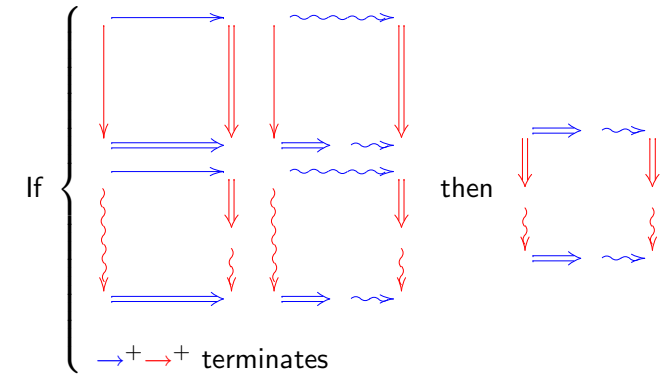
$$\forall P, Q, P', PRQ \wedge P \xrightarrow{\alpha} P' \Rightarrow \exists Q', P'RQ' \wedge Q \xrightarrow{\alpha} Q'$$

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ P' & \mathcal{R} & Q' \end{array} \quad \begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ P' & \mathcal{R} & Q' \end{array}$$

- ▶ **bisimilarity**:  $\approx \triangleq \bigcup \{ \mathcal{R}, \mathcal{R} \text{ bisimulation} \}$

## Putting it all together

- ▶ Extend the commutation result:



- ▶ Take  $\rightarrow = \xrightarrow{\tau}$ ,  $\rightsquigarrow = \xrightarrow{a \tau}$ ,  $\rightarrow = \mathcal{B}$  and  $\rightsquigarrow = \mathcal{R}$

## Bisimulation: Up-to techniques [Milner,Sangiorgi]

- ▶ "Reduce the size of the bisimulation candidate"
- ▶ if  $P \mathcal{R} Q$ , then  $\mathcal{R} \approx$  is a bisimulation, (and  $\mathcal{R} \subseteq \approx$ )

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ P' & \mathcal{R} \approx & Q' \end{array}$$

- ▶ but  $P \mathcal{R} Q$  does **not** entail  $\mathcal{R} \subseteq \approx$

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ P' & \approx \mathcal{R} & Q' \end{array}$$

Consider the LTS " $\tau.a \xrightarrow{\tau} a \xrightarrow{a} 0$ ":

$a \approx \tau.a$ , and  $\mathcal{R} = \{(\tau.a, 0)\}$  satisfies the previous diagram:

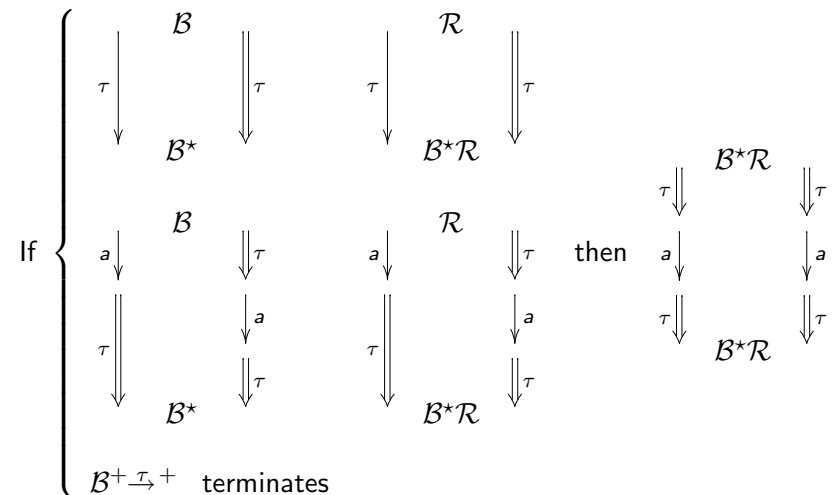
$$\begin{array}{ccc} \tau.a & \mathcal{R} & 0 \\ \tau \downarrow & & \parallel \tau \\ a & \approx & \tau.a \quad \mathcal{R} \quad 0 \end{array}$$

but  $\tau.a \not\approx 0$ .

- ▶ use "Expansion": if  $P \mathcal{R} Q$  then  $\mathcal{R} \subseteq \approx$ .

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ P' & \approx \mathcal{R} \approx & Q' \end{array}$$

## Putting it all together



## Putting it all together

- ▶ Suppose  $P \mathcal{B} Q$  and  $\mathcal{B}^{+\rightarrow+}$  terminates,
 
$$\begin{array}{ccc} P & \mathcal{B} & Q \\ \alpha \downarrow & & \Downarrow \alpha \\ P' & \mathcal{B}^* & Q' \end{array}$$
- ▶ if  $P \mathcal{R} Q$ , then  $\mathcal{B}^*\mathcal{R}$  is a bisimulation,  $\mathcal{R} \subseteq \approx$ .
 
$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \alpha \downarrow & & \Downarrow \alpha \\ P' & \mathcal{B}^*\mathcal{R} & Q' \end{array}$$

## General result

- ▶ Generalisation of Sangiorgi's up-to techniques for *strong* bisimulation.
- ▶ Suppose  $P \mathcal{B} Q$  and  $\mathcal{B}^{+\rightarrow+}$  terminates,
 
$$\begin{array}{ccc} P & \mathcal{B} & Q \\ \alpha \downarrow & & \Downarrow \alpha \\ P' & \mathcal{B}^* & Q' \end{array}$$
  - ▶ if  $P \mathcal{R} Q$  and  $P \mathcal{R} Q$  then  $\mathcal{R} \subseteq \approx$ 



$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \tau \downarrow & \Downarrow \tau & a \downarrow \Downarrow a \\ P' \mathcal{B}^*\mathcal{F}(\mathcal{R})Q' & & P' \mathcal{G}(\mathcal{R})Q' \end{array}$$
 (with some restrictions on  $\mathcal{F}$  and  $\mathcal{G}$ )
  - ▶ if  $P \mathcal{R} Q$  and  $P \mathcal{R} Q$  then  $\mathcal{R} \subseteq \approx$ 

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \tau \downarrow & \Downarrow \tau & a \downarrow \Downarrow a \\ P' \mathcal{B}^*\mathcal{R} \approx Q' & & P'(\mathcal{R} \cup \approx)^*Q' \end{array}$$

## Conclusions, Future Works

- ▶ New up-to techniques, using a new commutation result, all the proofs were checked with the Coq proof assistant.
- ▶ Applying these techniques:
  - ▶ this study originates from the correctness proof of a distributed abstract machine
  - ▶ “up to expansion” is sometimes not enough
  - ▶ find out whether these techniques are enough, by studying other applications
- ▶ Developing the theory:
  - ▶ relationships with the decreasing diagrams of [van Oostrom] (already used by [Fournet] for bisimulation).
  - ▶ general extension of these techniques to the bisimulation setting?

## For Further Reading I

-  M. Bezem, J.W. Klop, V. van Oostrom. Diagram Techniques for Confluence *Information and Computation*, 141(2):172-204, 1998.
-  D. Pous. Web appendix of this paper (with Coq proof scripts): <http://perso.ens-lyon.fr/damien.pous/upto/>.