On the reconstruction of proofs in distributed theorem proving with contraction: a modified Clause-Diffusion method.

Maria Paola Bonacina
Dept. of Computer Science
University of Iowa

Outline

- Proof reconstruction
- Distributed theorem proving
- Problems in proof reconstruction
  - communication
  - backward contraction
- Modified Clause Diffusion
  - uniform fairness
  - sufficient conditions for proof reconstruction
  - guaranteed proof reconstruction
- Discussion

Proof reconstruction

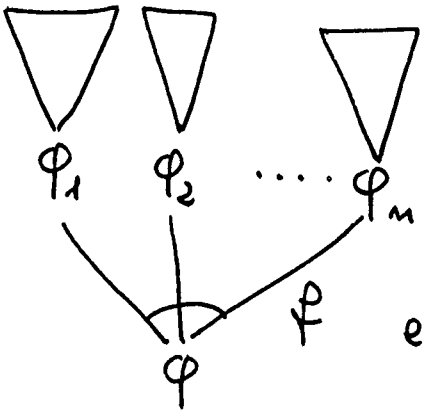
$\mathcal{C} = \langle I, \mathcal{E} \rangle$

$S_0 \vdash_{\mathcal{C}} S_1 \vdash_{\mathcal{C}} \ldots \vdash_{\mathcal{C}} S_i \vdash_{\mathcal{C}} S_{i+1} \ldots$

$\forall \varphi \in \bigcup_{i \geq 0} S_i$

- $\varphi \in S_0$ $\quad at(\varphi) = \varphi$
- $i > 0$

$at(\varphi) =$



e.g. resolution, simplification ...

- Proof: $at(\square)$.

Proof reconstruction

1) associate identifiers to clauses:

domain of identifiers : $(A, \preccurlyeq)$

unambiguous naming scheme:

$$S_0 \preccurlyeq S_1 \preccurlyeq \dots \preccurlyeq S_i \preccurlyeq \dots$$

$$R : A \longrightarrow \bigcup_{i \geq 0} S_i \qquad \text{bijective}$$

2) store id of parents and rule with each clause.

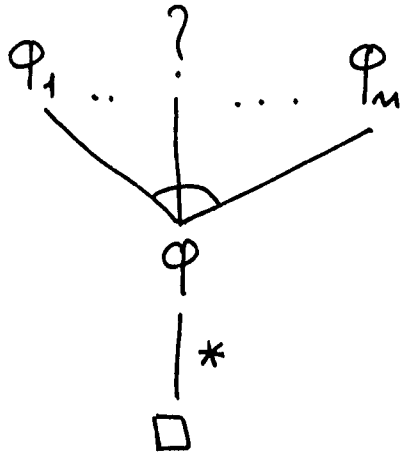
3) retrieve ancestors by id starting with $\square$.

Backward contraction

1) $$\frac{\varphi_1 \dots \varphi_m}{\varphi}$$

2) φ_i deleted (simplification)

3) at($\square$) :



- Forward / backward contraction.

- $(S_0 ; D_0) \vdash_\varphi (S_1 ; D_1) \vdash_\varphi \dots \vdash_\varphi (S_i ; D_i) \vdash_\varphi \dots$

$R : A \longrightarrow \bigcup_{i>0} S_i \cup D_i$ bijective

Distributed theorem proving

$\varphi = \langle I; \Sigma \rangle$

concurrent, asynchronous,

communicating deductive processes

$P_0, P_1, \ldots, P_{n-1}$

$S_0^0 \vdash S_1^0 \vdash \ldots\ldots \vdash S_i^0 \vdash \ldots\ldots$

$S_0^1 \vdash S_1^1 \vdash \ldots\ldots \vdash S_i^1 \vdash \ldots\ldots$

$\vdots$

$S_0^{n-1} \vdash S_1^{n-1} \vdash \ldots\ldots \vdash S_i^{n-1} \vdash \ldots\ldots$

Success: $\exists k \; \exists i \quad \square \in S_i^k$

$at(\square) = ?$

based on S_i^k

Distributed proof reconstruction

- Failures in distributed proof reconstruction
- Sufficient conditions for distributed proof reconstruction
- A Modified Clause Diffusion method that guarantees distributed proof reconstruction with
  - no ad-hoc communication
  - no centralized control

Deduction by Clause-Diffusion

- clauses are assigned to processes:

  P_i "owner" S^i "residents"

- clauses are "diffused" by message-passing (e.g. broadcasting):

  P_i $(S; V; MI; MO)^i$

- expansion inferences are subdivided by ownership:

  P_i

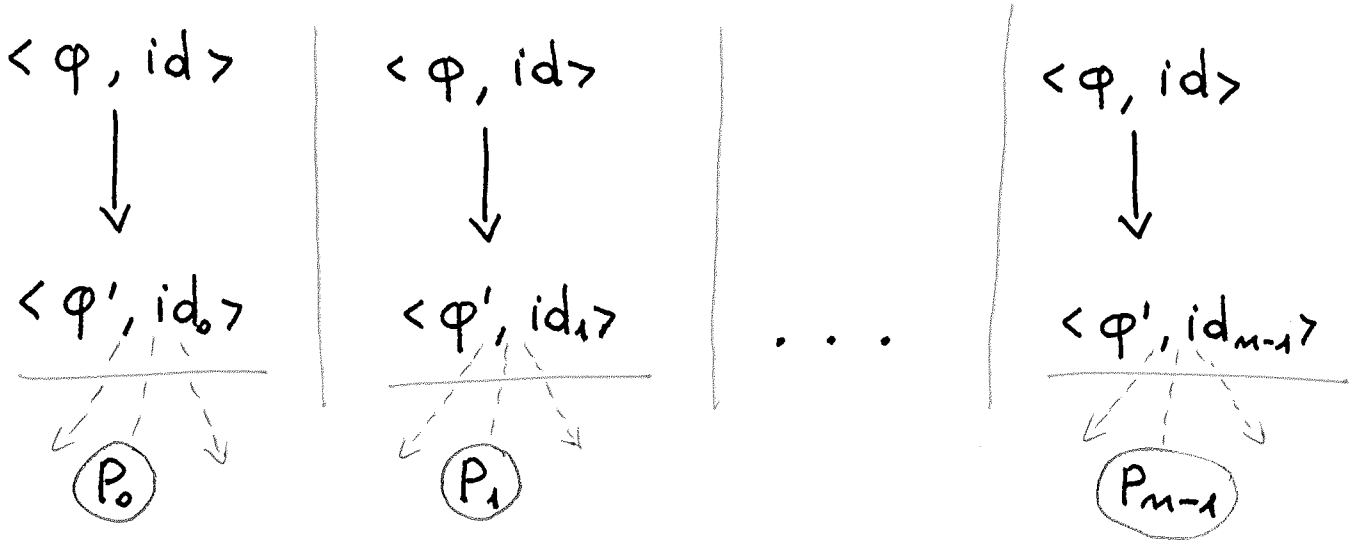
  ψ_1 into ψ_2

  $\psi_2 \in S^i$

  ψ_3

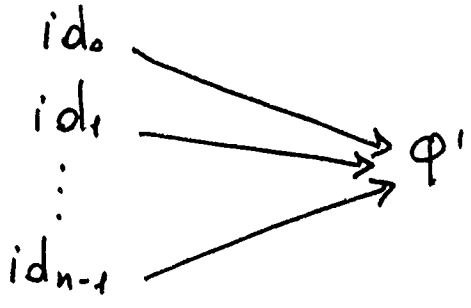
$(S; V; CP; MI; MO; D)$

Distributed backward contraction and proof reconstruction (1)



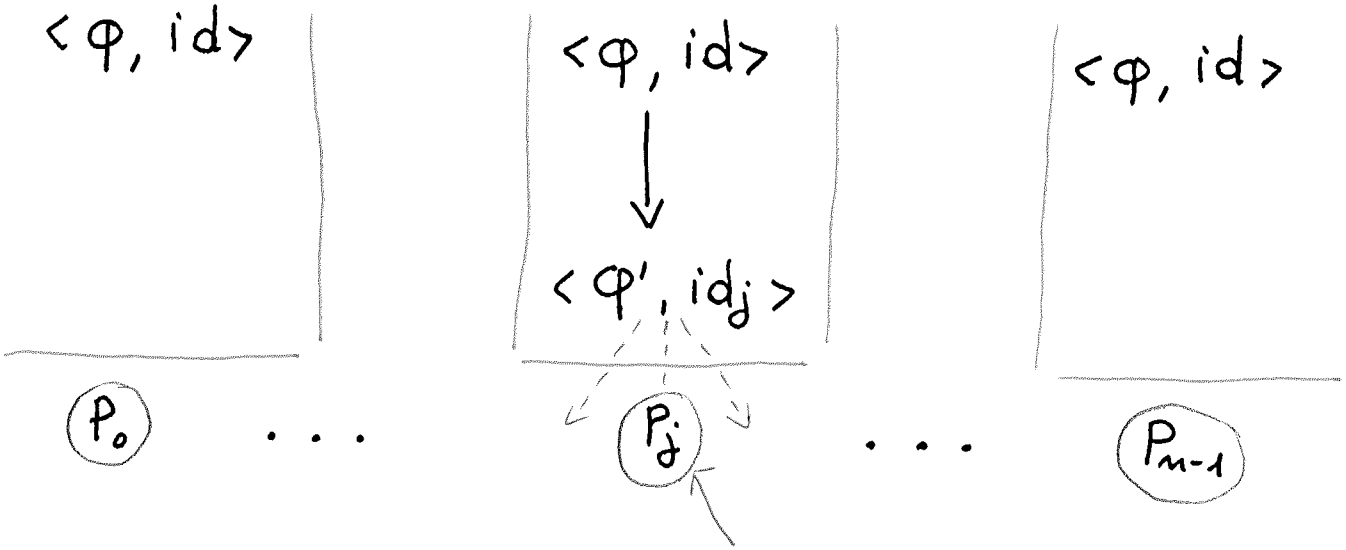
Problems:

- redundancy by duplication
- ambiguous naming scheme:



failures in proof reconstruction.

Distributed backward contraction and proof reconstruction (2)



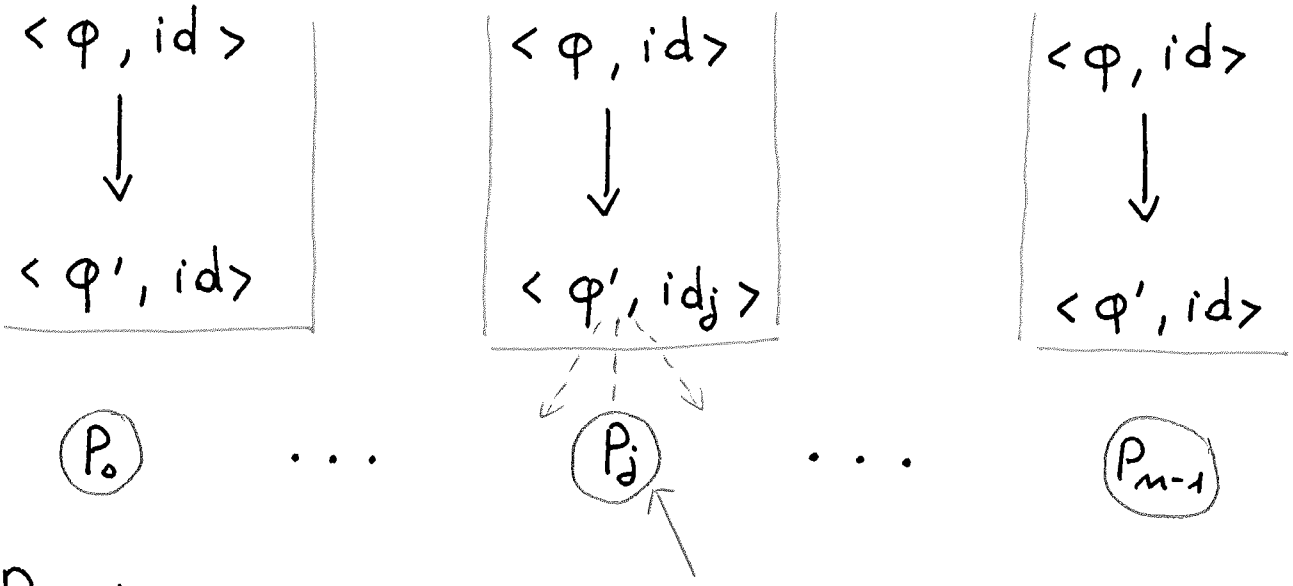
Problem:

too little contraction:

redundancy by lack of contraction.

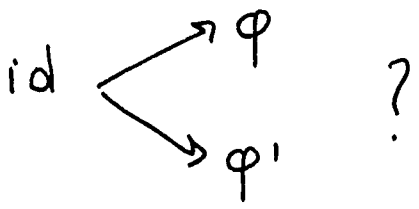
Distributed backward contraction and proof reconstruction (3)

Eager backward contraction:



Problems:

- redundancy by duplication (controlled wrt (1))
- ambiguous naming scheme:



failures in proof reconstruction.

Requirement: globally unambiguous naming scheme

P_0 : $T_0^0 \vdash T_1^0 \vdash \ldots \vdash T_i^0 \vdash \ldots$

P_1 : $T_0^1 \vdash T_1^1 \vdash \ldots \vdash T_i^1 \vdash \ldots$

$\vdots$

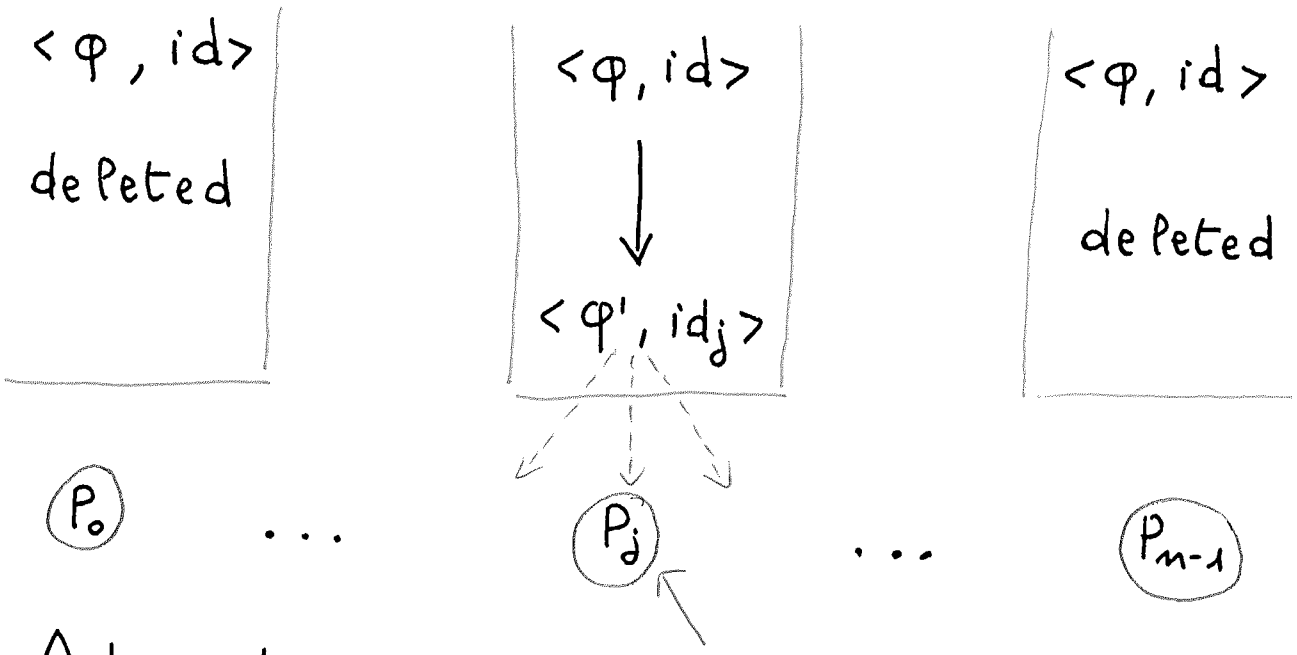
P_{n-1} : $T_0^{n-1} \vdash T_1^{n-1} \vdash \ldots \vdash T_i^{n-1} \vdash \ldots$

$T = (S; V; CP; MI; MO; D)$

$\forall$ P_k $\quad 0 \leq k \leq n-1$

$R: A \longrightarrow \bigcup_{i \geq 0} S_i^k \cup V_i^k \cup D_i^k$ bijective

Solution in Modified Clause Diffusion



Advantages:

- no redundancy by lack of contraction
- minimize redundancy by duplication
- unambiguous naming scheme:

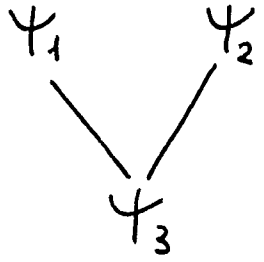
$$id \longrightarrow \varphi$$

$$id_j \longrightarrow \varphi'$$

- uniform treatment of raw clauses

Communication and proof reconstruction

P_i :



expansion
or
(backward)
contraction

- Ψ_3 is diffused

  Ψ_1 / Ψ_2 is not, because deleted by backward contraction

- Ψ_3 is diffused "before" Ψ_1 / Ψ_2

P_j :

$at(\square) =$

failure in proof reconstruction by delayed diffusion

Requirement: comprehensive communication scheme

$P_0 : T_0^0 \vdash T_1^0 \vdash \dots \vdash T_i^0 \vdash \dots$

$P_1 : T_0^1 \vdash T_1^1 \vdash \dots \vdash T_i^1 \vdash \dots$

$\vdots$

$P_{m-1} : T_0^{m-1} \vdash T_1^{m-1} \vdash \dots \vdash T_i^{m-1} \vdash \dots$

$T = (S; V; CP; MI; MO; D)$

$\forall P_k \quad 0 \leq k \leq m-1$

if P_k selects φ as premise at stage $i \geq 0$,

then $\exists P_j$ such that $\boxed{\varphi \in MO_\ell^j}$

for some stage $\ell > 0$.

Requirement: safe communication scheme

P_0 : $T_0^0 \vdash T_1^0 \vdash \ldots \vdash T_i^0 \vdash \ldots$

P_1 : $T_0^1 \vdash T_1^1 \vdash \ldots \vdash T_i^1 \vdash \ldots$

$\vdots$

P_{n-1} : $T_0^{n-1} \vdash T_1^{n-1} \vdash \ldots \vdash T_i^{n-1} \vdash \ldots$

$T = (S; V; CP; MI; MO; D)$

$\forall P_k \quad 0 \leqslant k \leqslant n-1$

if $\boxed{\varphi \in MO_i^k}$ for some stage i, $i \geq 0$,

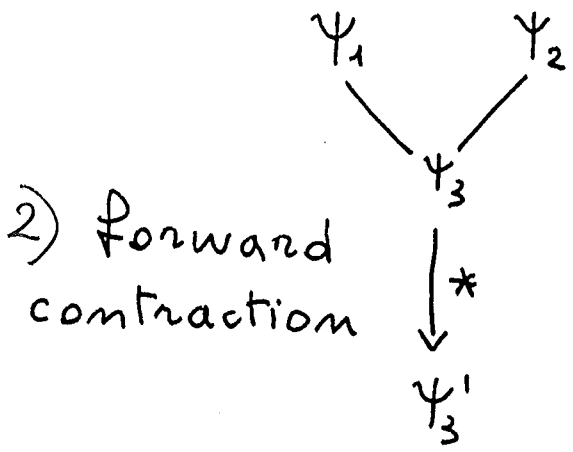
then $\forall P_j$, $0 \leqslant j \neq k \leqslant n-1$,

$\exists p_j \quad p_j \geq 0 \quad \boxed{\varphi \in MI_{p_j}^j}$.

Solution in

Modified Clause - Diffusion

P_i :



1) expansion or (backward) contraction

2) forward contraction

3) choice of owner: P_j

4) naming: $\langle j, i, l \rangle$

5) diffusion: $\langle \psi_3', \langle j, i, l \rangle \rangle$

Advantages:

- comprehensive communication scheme
- naming scheme without repetitions
- uniform treatment of all raw clauses

Modified Clause Diffusion

- Expansion : (S; V; CP; MI; MO; D)
- Forward contraction : (S; V; CP; MI; MO; D)
- Backward contraction : (S; V; CP; MI; MO; D)

Features:

- uniform treatment of expansion and contraction
- simple communication scheme
- distributed proof reconstruction

Uniform fairness

$P_0 \ldots P_{n-1}$ $\quad (S; V; CP; MI; MO; D)$

1) all raw clauses, incoming messages, outgoing messages are processed,

2) all persistent, non-redundant residents are broadcast

3) all expansion inferences from persistent non-redundant clauses in $(S \cup V)^k$ are considered by P_k (S^k) or by others

the derivation is uniformly fair.

Uniform fairness

$P_0 \dots P_{m-1} \qquad (S; V; CP; MI; MO; D)$

1) $\forall k,\ 0 \le k \le m-1,$

$CP^k_\omega = MI^k_\omega = MO^k_\omega = \emptyset,$

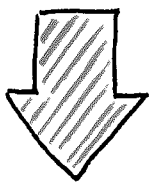
2) $\forall \varphi \in (S_\omega - R(S_\omega))$

$\exists k,\ 0 \le k \le m-1,\ \exists i,\ i \ge 0,\ \varphi \in MO^k_i,$

3) $\forall k,\ 0 \le k \le m-1,$

$$I_e((S \cup V)^k_\omega - R((S \cup V)^k_\omega)) \subseteq \bigcup_{i \ge 0} \bigcup_{j=0}^{m-1} CP^j_i$$

$$I_e(S^k_\omega - R((S \cup V)^k_\omega)) \subseteq \bigcup_{i \ge 0} CP^k_i,$$



$$I_e(S_\omega - R(S_\omega)) \subseteq \bigcup_{k=0}^{m-1} \bigcup_{i \ge 0} CP^k_i.$$

Proof reconstruction

$\mathcal{C}$ $\quad P_0 \dots P_{n-1} \quad (S; V; CP; MI; MO; D)$

1) $\mathcal{C}$ has a globally unambiguous naming scheme
2) contracted clauses from $S \cup V$ are saved in D
3) $\mathcal{C}$ satisfies the three conditions for uniform fairness
4) $\mathcal{C}$ has a comprehensive and safe communication scheme

if P_i generates $\square$ at stage h_i, P_i can reconstruct at($\square$) from its final state $(S; V; CP; MI; MO; D)^i_{h_i}$ -

Discussion

- Local reconstruction of the proof generated by a distributed derivation.

- Analysis of the difficulties with backward contraction and communication.

- Sufficient conditions for distributed proof reconstruction.

- Modified Clause Diffusion
  - uniformly fair $\Rightarrow$ complete
  - allows proof reconstruction with no extra communication no extra control.