# Incremental coinduction for process algebra

Andrei Popescu and Elsa Gunter
University of Illinois
at Urbana-Champaign

# Context

- Process algebra
- Transition system
- Bisimilarity = notion of process equality
- Interactive proofs of bisimilarity

# Bisimilarity

- Processes form Act-labeled transition system,

$$P \xrightarrow{a} P'$$

- Bisimulation: binary relation $\Theta$ on Proc, s.t.

for $P,Q \in Proc$ and $a \in Act$

$$P \;\Theta\; Q \;\wedge\; P \xrightarrow{a} P'$$

$$\Downarrow$$

$$\exists Q'.\; Q \xrightarrow{a} Q' \;\wedge\; P' \;\Theta\; Q'$$

(and the same for Q versus P)

- Bisimilarity, written $\equiv$, is the largest bisimulation

# A more intuitive description of bisimilarity

$P \equiv Q$ iff

- Whenever $P \xrightarrow{a} P'$
- Also $Q \xrightarrow{a} Q'$ for some $Q'$ such that

$P' \equiv Q'$

- Same for $Q$ versus $P$
- And so on, indefinitely

# Example – CCS-like calculus

$\forall \tau \in Act, \ \bar{\cdot} : Act \to Act$ s.t. $a^{\bar{\bar{}}} = a$

- P ::= 0 | a . P | P | Q | ! P

$$a . P \xrightarrow{a} P \ \textbf{(Pref)}$$

$$\frac{P \xrightarrow{a} P'}{P \mid Q \xrightarrow{a} P' \mid Q} \ \textbf{(ParL)} \qquad \frac{Q \xrightarrow{a} Q'}{P \mid Q \xrightarrow{a} P \mid Q'} \ \textbf{(ParR)}$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\bar{a}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \ \textbf{(ParS)} \qquad \frac{P \xrightarrow{a} P'}{!P \xrightarrow{a} !P \mid P'} \ \textbf{(Repl)} \qquad \frac{P \xrightarrow{a} Q' \quad P \xrightarrow{\bar{a}} R'}{!P \xrightarrow{\tau} !P \mid Q' \mid R'} \ \textbf{(ReplS)}$$

# Examples of proof tasks

- $\forall P, Q.\ P \mid Q \equiv Q \mid P$
- $\forall P, Q, R.\ (P \mid Q) \mid R \equiv P \mid (Q \mid R)$
- $\forall P.\ P \mid !P \equiv !P$

# Standard interactive bisimilarity proofs

- Goal: prove $P \equiv Q$

- Formal proof:
  - Define a relation $\Theta$
  - Show $P \; \Theta \; Q$
  - Show $\Theta$ bisimulation

# Standard interactive bisimilarity proofs

- Goal: prove $P \equiv Q$

- Formal proof:
  - Define a relation $\Theta$ - this is the "real" proof
  - Show $P \; \Theta \; Q$
  - Show $\Theta$ bisimulation

# By contrast: intuitive argument for P ≡ Q

Possible continuations of P

$$P \xrightarrow{a_1} P_1' \mid \xrightarrow{a_2} P_2' \mid \ldots \mid \xrightarrow{a_n} P_n'$$

match them (completely) with

Possible continuations of Q

$$Q \xrightarrow{b_1} Q_1' \mid \xrightarrow{b_2} Q_2' \mid \ldots \mid \xrightarrow{b_m} Q_m'$$

E.g., $a_i = b_j$, and further claim $P_i' \equiv Q_j'$

# Intuitive argument for $P \equiv Q$

- For each match (i,j), do the same for new claim, $P_i' \equiv Q_j'$
- Until (pattern) repetitions discovered in the tree of claims

$$P \equiv Q$$

$$\vdots \qquad P_{i2}' \equiv Q_{j2}'$$

$$\vdots \qquad \vdots$$

$$\ldots \qquad \ldots$$

$$\frac{\text{-----------} \qquad \text{-----------}}{P_{i1}' \equiv Q_{j1}' \qquad P_{i2}' \equiv Q_{j2}' \qquad \ldots}$$

$$\frac{\text{----------------------------------------}}{P \equiv Q}$$

# Argument built intuitively then fed into the formal proof

$\forall \Theta$ = The set of all nodes in the "claim tree"

- Prove $\Theta$ bisimulation

Thus:

- Gap between intuition and formalities
- No formal support for building the desired bisimulation incrementally (as in the intuitive argument)

# Our contribution

- Fill this gap between intuition and formalities

- Provide a formal system where
  - Bisimulations can be built incrementally
  - Goal-discharging repetitions/circularities are first-class citizens

# Sample Goals

1. Comm: $\forall P\ Q.\ P \mid Q \equiv Q \mid P$
2. Assoc: $\forall P\ Q\ R.\ (P \mid Q) \mid R \equiv P \mid (Q \mid R)$
3. $\forall P.\ P \mid !P \equiv !P$

Say we proved 1 and 2, and wish to prove 3

# Proof

Hypotheses: Comm, Assoc
(i.e., lemmas known so far)

Conclusion: P | !P ≡ !P

# Proof

Hypotheses: Comm, Assoc

Conclusion: P | !P ≡ !P

Try equational reasoning: Fail

(P | !P ≡ !P  does not follow from just Comm, Assoc via the rules of equational logic:  Refl, Trans, Cong, Subst)

# Proof

Hypotheses: Comm, Assoc

Conclusion: $P \mid !P \equiv !P$

Then unfold $P \mid !P$:

- $P \mid !P \xrightarrow{a} \{\ P' \mid !P,\ P \mid (!P \mid P')\ \}$ if $P \xrightarrow{a} P'$
- $P \mid !P \xrightarrow{\tau} \{\ P \mid (!P \mid (Q' \mid R')),\ Q' \mid (!P \mid R')\ \}$

if $P \xrightarrow{a} Q'$ and $P \xrightarrow{\bar{a}} R'$

# Parenthesis – unfold automatically

- Compose primitive rules of the system until atomic assumptions are reached
- Side-conditions are composed accordingly

$$\frac{P \xrightarrow{a^{\cdot}} R'}{!P \xrightarrow{a^{\cdot}} !P \mid R'}\ (\text{Repl})$$

$$\frac{P \xrightarrow{a} Q' \qquad !P \xrightarrow{a^{\cdot}} !P \mid R'}{P \mid !P \xrightarrow{\tau} Q' \mid (!P \mid R')}\ (\text{ParS})$$

# Back to Proof

Hypotheses: Comm, Assoc

Conclusion: $P \mid !P \equiv !P$

Then unfold $P \mid !P$ and $!P$:

- $P \mid !P \xrightarrow{a} \{ P' \mid !P,\ P \mid (!P \mid P') \}$ if $P \xrightarrow{a} P'$
- $P \mid !P \xrightarrow{\tau} \{ P \mid (!P \mid (Q' \mid R')),\ Q' \mid (!P \mid R') \}$

if $P \xrightarrow{a} Q'$ and $P \xrightarrow{\bar{a}} R'$

- $!P \xrightarrow{a} \{ !P \mid P' \}$ if $P \xrightarrow{a} P'$
- $!P \xrightarrow{\tau} \{ !P \mid (Q' \mid R') \}$ if $P \xrightarrow{a} Q'$ and $P \xrightarrow{\bar{a}} R'$

# Proof

Hypotheses: Comm, Assoc

Conclusion: $P \mid !P \equiv !P$

Then unfold $P \mid !P$ and $!P$:

- $P \mid !P \xrightarrow{a} \{ P' \mid !P,\ P \mid (!P \mid P') \}$ if $P \xrightarrow{a} P'$
- $P \mid !P \xrightarrow{\tau} \{ P \mid (!P \mid (Q' \mid R')),\ Q' \mid (!P \mid R') \}$

if $P \xrightarrow{a} Q'$ and $P \xrightarrow{\bar{a}} R'$

- $!P \xrightarrow{a} \{ !P \mid P' \}$ if $P \xrightarrow{a} P'$
- $!P \xrightarrow{\tau} \{ !P \mid (Q' \mid R') \}$ if $P \xrightarrow{a} Q'$ and $P \xrightarrow{\bar{a}} R'$

From matching if-hypotheses and action labels, obtain 4 new "claims"…

# Proof

Hypotheses: Comm, Assoc

Conclusions:

1. $P' \mid !P \equiv !P \mid P'$
2. $P \mid (!P \mid P') \equiv !P \mid P'$
3. $P \mid (!P \mid (Q' \mid R')) \equiv !P \mid (Q' \mid R')$
4. $Q' \mid (!P \mid R') \equiv !P \mid (Q' \mid R')$

... “claims” becoming new conclusions in the goal

# Proof

Hypotheses: Comm, Assoc, P | !P ≡ !P

Conclusions:

1. P' | !P ≡ !P | P'
2. P | (!P | P') ≡ !P | P'
3. P | (!P | (Q' | R')) ≡ !P | (Q' | R')
4. Q' | (!P | R') ≡ !P | (Q' | R')

Also, previous conclusion becomes hypothesis!

(to watch for possible "repetition of the claims")

# Proof

Hypotheses: Comm, Assoc, P | !P ≡ !P

Conclusions:

1. P' | !P ≡ !P | P'
2. P | (!P | P') ≡ !P | P'
3. P | (!P | (Q' | R')) ≡ !P | (Q' | R')
4. Q' | (!P | R') ≡ !P | (Q' | R')

All 4 conclusions discharged by equational reasoning from hypotheses. **q.e.d.**

# The formal proof in our system

P | !P ≡ !P |-- P' | !P ≡ !P | P' (by EqL)

P | !P ≡ !P |-- P | (!P | P') ≡ !P | P' (by EqL)

P | !P ≡ !P |-- P | (!P | (Q' | R')) ≡ !P | (Q' | R') (by EqL)

P | !P ≡ !P |-- Q' | (!P | R') ≡ !P | (Q' | R') (by EqL)

---

(apply Unfold)

|-- P | !P ≡ !P

(Omiting the reference to lemmas Comm, Assoc)

# The formal proof in our system

$\forall\ P.\ P \mid !P \equiv !P \quad \vdash\ \forall\ P\ P'.\ P \mid (!P \mid P') \equiv !P \mid P'$

Valid inference in Equational Logic (and in FOL)

# Soundness of our proof system

Indeed, the relation $\Theta$ =

$\{ (P \mid !P,\ !P) .\ P \in Proc\} \cup$

$\{ ( P' \mid !P,\ !P \mid P' ) .\ P, P' \in Proc\} \cup$

$\{ ( P \mid (!P \mid P'),\ !P \mid P' ) .\ P, P' \in Proc\} \cup$

$\{ ( P \mid (!P \mid (Q' \mid R')),\ !P \mid (Q' \mid R') ) .\ P, Q', R' \in Proc\} \cup$

$\{ ( Q' \mid (!P \mid R'),\ !P \mid (Q' \mid R') ) .\ P, Q', R' \in Proc\}$

turns out to be a bisimulation

up to bisimilarity and arbitrary contexts

(Davide Sangiorgi)

# Scope

- Process algebra by de Simone SOS rules

$$\frac{X_1 \xrightarrow{a_{1,1}} Y_{1,1} \quad \dots \quad X_1 \xrightarrow{a_{1,n1}} Y_{1,n1} \qquad \vdots \qquad X_k \xrightarrow{a_{k,1}} Y_{k,1} \quad \dots \quad X_k \xrightarrow{a_{k,nk}} Y_{k,nk}}{f(X_1,\dots,X_k) \xrightarrow{b} T(\dots,X_i,\dots,Y_{i,j},\dots)} \; [\, \varphi\,(b,\dots,a_{i,j},\dots)\,]$$

(the $X_i$s distinct, the $Y_{i,j}$s distinct and fresh)

# Isabelle formalization

- Have formalized the proof system and proved its soundness in Isabelle/HOL
- Potential to become an a priori formally certified tool
- Need to write some custom Isabelle tactics to make it into a real tool

# Credits

- Robert de Simone, 1985:

identify an amenable SOS format

- Davide Sangiorgi, 1998:

"up to" techniques for bisimilarity proofs

- Grigore Rosu and Joseph Goguen, 2000:

circular coinduction in hidden logic, applicable to deterministic systems (such as streams)

# Conclusions

- Gap between
  - formal support for interactive bisimilarity proofs
  - intuitive means of building the required bisimulation

- Filled this gap by incremental proof system
  - Based on equational logic
  - Featuring circularities as first-class citizens
  - Applicable to a large class of process algebras
  - Formalized in Isabelle/HOL

# Future work

- Isabelle formalization into user-friendly tool
- Extend the scope
  - Laxer SOS formats
  - Syntax with bindings (Pi-calculus)

# Extra slides – More on the soundness of our proof system

# The retract operator

$Retr : Rel(Proc) \rightarrow Rel(Proc)$

$Retr\ \Theta =$

$\{(P,Q).\ \forall a\ P'.\ P \xrightarrow{a} P'$

$\Downarrow$

$\exists Q'.\ Q \xrightarrow{a} Q' \wedge (P',Q') \in \Theta$

and similarly for Q versus P}

($Retr\ \Theta$ contains all pairs "retracted back" from $\Theta$)

$\Theta$ bisimulation means $\Theta \subseteq Retr\ \Theta$

# Recall our formal proof

P | !P ≡ !P |-- P' | !P ≡ !P | P' (by EqL)

P | !P ≡ !P |-- P | (!P | P') ≡ !P | P' (by EqL)

P | !P ≡ !P |-- P | (!P | (Q' | R')) ≡ !P | (Q' | R') (by EqL)

P | !P ≡ !P |-- Q' | (!P | R') ≡ !P | (Q' | R') (by EqL)

----------(apply Unfold)

|-- P | !P ≡ !P

(Omiting the reference to lemmas Comm, Assoc)

# Explantion in terms of more primitive proof rules

Let $\Theta = \{ (P \mid !P, !P).\ P \in Proc\}$

Need to show

$\Theta \subseteq \equiv$

i.e., $\Theta \subseteq CongCl\ (\{\} \cup \equiv)$, written $\{\} \vdash \Theta$

Would suffice that:

$\Theta$ bisimulation, i.e., $\Theta \subseteq Retr\ \Theta$

But this requirement may be too harsh.

Instead, defer the goal by interpolating relation $\Theta'$ s.t.

$\Theta \subseteq Retr\ \Theta'$ ,

The new goal becomes $\Theta' \subseteq CongCl\ (\Theta \cup \equiv)$,

written $\Theta \vdash \Theta'$ .

# Rules in a more primitive system

- The interpolation rule:

$$\frac{\Theta \subseteq \mathrm{Retr}\,\Theta' \qquad \Theta \vdash \Theta'}{\{\} \vdash \Theta}\ (\mathrm{Interp})$$

More generally:

$$\frac{\Theta \subseteq \mathrm{Retr}\,\Theta' \qquad \Theta \cup \Theta'' \vdash \Theta'}{\Theta'' \vdash \Theta}\ (\mathrm{Interp})$$

- The split rule:

$$\frac{\Theta \vdash \Theta' \qquad \Theta \vdash \Theta''}{\Theta \vdash \Theta' \cup \Theta''}\ (\mathrm{Split})$$

# Obtain the higher-level proof rule

- Natural interpolants $\Theta \subseteq \text{Retr}\,\Theta'$ obtained automatically by syntactic analysis of the SOS rules.
- E.g., for $\Theta = \{ (P \mid !P, !P).\ P \in \text{Proc}\}$,

take $\Theta'$ to be

$\{ ( P' \mid !P,\ !P \mid P' ) .\ P \in \text{Proc}\} \cup$

$\{ ( P \mid (!P \mid P'),\ !P \mid P' ) .\ P \in \text{Proc}\} \cup$

$\{ ( P \mid (!P \mid (Q' \mid R')),\ !P \mid (Q' \mid R') ) .\ P,Q \in \text{Proc}\} \cup$

$\{ ( Q' \mid (!P \mid R'),\ !P \mid (Q' \mid R') ) .\ P,Q \in \text{Proc}\}$

- Then the Split rule splits the 4 $\cup$-components into separate goals

# Hence the higher-level proof rule

$$\frac{P \mid !P \equiv !P \;\vdash\; P' \mid !P \equiv !P \mid P' \quad\quad P \mid !P \equiv !P \;\vdash\; P \mid (!P \mid P') \equiv !P \mid P' \quad\quad P \mid !P \equiv !P \;\vdash\; P \mid (!P \mid (Q' \mid R')) \equiv !P \mid (Q' \mid R') \quad\quad P \mid !P \equiv !P \;\vdash\; Q' \mid (!P \mid R') \equiv !P \mid (Q' \mid R')}{\vdash\; P \mid !P \equiv !P}\ (\text{Unfold})$$