UNIVERSITY OF Southampton
School of Electronics and Computer Science

DERIVING LTS

Pawel Sobocinski
(joint work with Julian Rathke)

IFIP WG1.3 Aussois
07/01/11

PLAN

1. **Introduction**
2. Full asynchrony
3. Asynchrony
4. Synchrony

BACKGROUND

- Process calculi in the CCS/Pi tradition come with two semantics
  - **reduction semantics**
    - "closed" - how the program evolves
    - easy to define
    - contextual preorders/equivalences: reduction precongruence, reduction congruence, barbed congruence
  - **labelled semantics**
    - "open" - how the program interacts
    - harder to define and justify
    - simulation, bisimulation
- Basic underlying issues
  - soundness: eg. is bisimilarity included in contextual equivalence?
  - completeness: eg. is contextual equivalence included in bisimilarity?

REDUCTION SEMANTICS

- Structural congruence $$(P \parallel Q) \parallel R \equiv P \parallel (Q \parallel R)$$ $$P \parallel Q \equiv Q \parallel P$$ $$P \parallel 0 \equiv P$$
- Think of a process as a "chemical soup"
- Reduction TS is usually defined with
  - a number of parametric rules, eg $a!P \parallel a?Q \rightarrow P \parallel Q$
  - a set of "reactive" contexts $$\frac{P \rightarrow P'}{P \| Q \rightarrow P' \| Q}$$
  - closed under structural congruence $$\frac{Q \equiv P \quad P \rightarrow P' \quad P' \equiv Q'}{Q \rightarrow Q'}$$

RELATIVE PUSHOUTS (RPO)

(J. LEIFER R. MILNER, DERIVING BISIMULATION CONGRUENCES FOR REACTIVE SYSTEMS, CONCUR '00)
(P. SEWELL, FROM REWRITE RULES TO BISIMULATION CONGRUENCES, CONCUR '98)

- Passing from
  - "internal" reduction semantics (what processes do) to
  - "external" labelled semantics (how processes interact)

$\chi[P] \rightarrow P'$ & χ is the smallest such context

$$P \xrightarrow{\chi} P'$$

$$\begin{tikzcd}
 & I_4 & \\
I_2 \arrow[ur, "\chi"] & & I_3 \arrow[ul, "d"'] \\
 & 0 \arrow[ul, "P"] \arrow[ur, "l_k \circ \rho"'] &
\end{tikzcd}$$

WHERE RPOS GO WRONG

- The derivation process is global
  - no compositional, inductive presentation (SOS)
  - joint work with Julian Rathke on how to derive SOS

- Often give the wrong equivalences
  - eg. restricting to asynchronous subcalculus still gives synchronous lts
  - problem and solution illustrated in this talk

SOS LABELLED SEMANTICS

- Semantics of a term completely determined by semantics of its subterms
- No structural congruence rule, this is real syntax

$$\frac{P \xrightarrow{a} P'}{P \| Q \xrightarrow{a} P' \| Q}$$

- Our rules are always SOS
  - a set of (positive) SOS rules defines a monotonic function on relations, let Φ be the lfp

$$\Phi : \mathcal{P}(P \times L \times P) \to \mathcal{P}(P \times L \times P)$$

  - **the** LTS defined by a set of rules is $\mathcal{C} \stackrel{\text{def}}{=} \Phi(\varnothing)$

CONTEXTUAL EQUIVALENCE

(K. Honda, N. Yoshida, On reduction-based process semantics, TCS 152(2):436-486, 1995)

- Suppose that reductions cause "changes in heat"
- Observer can
  - introduce new ingredients
  - measure changes in heat

- Reduction precongruence
  - largest precongruence $\lesssim$ that satisfies $P \lesssim Q$ & $P \rightarrow P'$ implies there exists Q' with $Q \rightarrow Q'$ and $P' \lesssim Q'$

- Reduction congruence - symmetric version

LTS AND OBSERVABILITY

- What is the meaning of a labelled transition in an LTS?
  - indication of a possible interaction
- A labelled transition is observable if there exists a contextual characterisation of the label
  - ie $P \xrightarrow{\alpha} P'$ iff there exists context χ_α s.t. ...
    - the ... should be preserved by contextual equivalence

PLAN

1. Introduction
2. **Full asynchrony**
3. Asynchrony
4. Synchrony
5. Infinite processes

FULL ASYNCHRONY

"SOUP OF INTERACTING MOLECULES"

Syntax

$$P \ ::= \ 0 \mid a! \mid a? \mid P \parallel Q \mid \tau$$

Structural congruence

$$(P \parallel Q) \parallel R \ \equiv \ P \parallel (Q \parallel R)$$

$$P \parallel Q \equiv Q \parallel P$$

$$P \parallel 0 \ \equiv \ P$$

Reduction semantics

$$\tau \ \rightarrow \ 0$$

$$a! \parallel a? \ \rightarrow \ 0$$

$$\frac{P \rightarrow P'}{P \| Q \rightarrow P' \| Q}$$

$$\frac{Q \equiv P \quad P \rightarrow P' \quad P' \equiv Q'}{Q \rightarrow Q'}$$

EXPERIMENT 1 - INPUT

- labelled transition = "log of experiment"
- input experiment - observe change in heat after adding an output ($a!$)

$$\frac{}{a? \xrightarrow{a?} 0}\ (\textsc{In})$$

$$\frac{P \xrightarrow{a?} P'}{P \| Q \xrightarrow{a?} P' \| Q}\ (\textsc{In}\|)$$

+ symmetric rule

EXPERIMENT 2 - OUTPUT

- output experiment - observe change in heat after adding an input ($a?$)

$$\frac{}{a! \xrightarrow{a!} 0}\ (\textsc{Out}) \qquad \frac{P \xrightarrow{a!} P'}{P \| Q \xrightarrow{a!} P' \| Q}\ (\textsc{Out}\|)$$

+ symmetric

EXPERIMENT 3 - TAU

- tau experiment - we observe heat but we haven't added anything

$$\frac{}{\tau \xrightarrow{\tau} 0}\ (\textsc{Tau}) \qquad \frac{P \xrightarrow{\tau} P'}{P\|Q \xrightarrow{\tau} P'\|Q}\ (\textsc{Tau}\|)$$

$$\frac{P \xrightarrow{a?} P' \qquad Q \xrightarrow{a!} Q'}{P\|Q \xrightarrow{\tau} P'\|Q'}\ (\textsc{Comm})$$

THE LTS

$$\frac{}{a? \xrightarrow{a?} 0}\ (\textsc{In}) \qquad \frac{P \xrightarrow{a?} P'}{P\|Q \xrightarrow{a?} P'\|Q}\ (\textsc{In}\|)$$

$$\frac{}{a! \xrightarrow{a!} 0}\ (\textsc{Out}) \qquad \frac{P \xrightarrow{a!} P'}{P\|Q \xrightarrow{a!} P'\|Q}\ (\textsc{Out}\|) \qquad \frac{P \xrightarrow{a?} P' \quad Q \xrightarrow{a!} Q'}{P\|Q \xrightarrow{\tau} P'\|Q'}\ (\textsc{Comm})$$

$$\frac{}{\tau \xrightarrow{\tau} 0}\ (\textsc{Tau}) \qquad \frac{P \xrightarrow{\tau} P'}{P\|Q \xrightarrow{\tau} P'\|Q}\ (\textsc{Tau}\|)$$

- Inductive presentation of RPO LTS
- Context lemma:

Let $\chi_{a!} = a? \quad \chi_{a?} = a! \quad \chi_\tau = 0$

$$P \xrightarrow{\alpha} P' \quad \Rightarrow \quad P \parallel \chi_\alpha \rightarrow P'$$

SOUNDNESS

- similarity is contained in reduction precongruence
- bisimilarity is contained in reduction congruence

- **Proof**: tau-labelled transitions agree with reductions and (bi) similarity is a (pre)congruence

- What about completeness?

EXPERIMENT MISMATCH

$$P_1 \stackrel{\text{def}}{=} a? \parallel a! \qquad\qquad P_2 \stackrel{\text{def}}{=} \tau$$

$P_1 \lesssim P_2$ but $P_1 \not\lesssim_{\mathcal{C}} P_2$

(in fact $P_1 \simeq P_2$)

so completeness does not hold...

- Cause of problem: no account of "unsuccessful" experiments

HONDA TOKORO RULES

(K. Honda & M. Tokoro, An object calculus for asynchronous communication, ECOOP `91)

$$\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a?} P' \| a!}\ (\textsc{InHT}) \qquad \frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a!} P' \| a?}\ (\textsc{OutHT})$$

- Rules may appear only at the last place in the derivation
  - ie we are looking at the LTS $\mathcal{HT} \stackrel{\text{def}}{=} \Psi\mathcal{C}$ where

$$\Psi \stackrel{\text{def}}{=} \{(\textsc{InHT}), (\textsc{OutHT})\}$$

- With these rules we have both soundness and completeness

PROOF

- for soundness, enough to show simulation a precongruence
  - $\{(P \parallel R, Q \parallel R) \mid P \precsim Q\}$ is a simulation
    - case $P \parallel R \xrightarrow{\tau} P' \parallel R'$ where $P \xrightarrow{a!} P',\ R \xrightarrow{a?} R'$
      - matched by "real output" $Q \xrightarrow{a!}_{\mathcal{C}} Q' \quad P' \precsim Q'$
      - matched by Honda-Tokoro transition

$$Q' = Q'' \parallel a? \qquad Q \xrightarrow{\tau} Q'' \qquad P' \precsim Q'$$

$$Q \parallel R \xrightarrow{\tau} Q'' \parallel R = Q'' \parallel a? \parallel R' = Q' \parallel R'$$

- for completeness:
  - easy to show: $P \xrightarrow{\alpha}_{\mathcal{HT}} P'$ iff $P \parallel \chi_\alpha \ \rightarrow\ P'$
  - this implies that reduction precongruence is a simulation

PLAN

1. Introduction
2. Full asynchrony
3. **Asynchrony**
4. Synchrony
5. Infinite processes

ASYNCHRONY

Syntax

$$P \ ::= \ 0 \mid a! \mid a?P \mid P \parallel Q \mid \tau P$$

Structural congruence

$$(P \parallel Q) \parallel R \ \equiv \ P \parallel (Q \parallel R)$$

$$P \parallel Q \equiv Q \parallel P$$

$$P \parallel 0 \ \equiv \ P$$

Reduction semantics

$$\tau P \ \rightarrow \ P$$

$$a! \parallel a?P \ \rightarrow \ P$$

$$\frac{P \rightarrow P'}{P \| Q \rightarrow P' \| Q}$$

$$\frac{Q \equiv P \qquad P \rightarrow P' \qquad P' \equiv Q'}{Q \rightarrow Q'}$$

ASYNCHRONOUS EXPERIMENTS

$$\frac{}{a?P \xrightarrow{a?} P}\ (\textsc{In}) \qquad \frac{P \xrightarrow{a?} P'}{P\|Q \xrightarrow{a?} P'\|Q}\ (\textsc{In}\|) \qquad \frac{}{\tau \xrightarrow{\tau} 0}\ (\textsc{Tau})$$

$$\frac{}{a! \xrightarrow{a!\downarrow R} R}\ (\textsc{Out}) \qquad \frac{P \xrightarrow{a!\downarrow R} P'}{P\|Q \xrightarrow{a!\downarrow R} P'\|Q}\ (\textsc{Out}\|) \qquad \frac{P \xrightarrow{\tau} P'}{P\|Q \xrightarrow{\tau} P'\|Q}\ (\textsc{Tau}\|)$$

$$\frac{P \xrightarrow{a?} P' \qquad Q \xrightarrow{a!\downarrow 0} Q'}{P\|Q \xrightarrow{\tau} P'\|Q'}\ (\textsc{Comm})$$

$$\Phi \stackrel{\text{def}}{=} \{(\textsc{Tau}), (\textsc{Tau}\|), (\textsc{In}), (\textsc{In}\|), (\textsc{Out}), (\textsc{Out}\|), (\textsc{Comm})\}$$

$$\mathcal{C}_a \stackrel{\text{def}}{=} \Phi_a(\varnothing)$$

CONTEXT LEMMA & SOUNDNESS

- Context lemma

$$\boxed{\chi_{a!\downarrow R} = a?R} \quad \chi_{a?} = a! \quad \chi_\tau = 0$$

$$P \xrightarrow{\alpha} P' \quad \Rightarrow \quad P \parallel \chi_\alpha \; \rightarrow \; P'$$

- Soundness wrt contextual equivalence

EXPERIMENT MISMATCH

$$P_1 \stackrel{\text{def}}{=} a?a! \qquad P_2 \stackrel{\text{def}}{=} \tau$$

$$P_1 \lesssim P_2 \quad P_1 \not\lesssim_{\mathcal{C}} P_2$$

- This means that some of our observations (labels) are morally unobservable. Which ones?

COMPLETENESS

$$\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a?} P' \| a!}\ (\textsc{InHT}) \qquad \frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a! \downarrow R} P' \| a?R}\ (\textsc{OutHT})$$

- The resulting LTS is sound and complete

PROOF

- Soundness: $\{(P \parallel R, Q \parallel R) \mid P \precsim Q\}$ is a simulation
  - case $P \parallel R \xrightarrow{\tau} P' \parallel R'$

$$P \xrightarrow{a!\downarrow 0}_{\mathcal{C}} P' \quad R \xrightarrow{a?}_{\mathcal{C}} R$$

$$R = R'' \parallel a?S \quad R' = R'' \parallel S$$

$$P \xrightarrow{a!\downarrow S}_{\mathcal{C}} P' \parallel S$$

$$Q \xrightarrow{\tau} Q' \quad Q \xrightarrow{a!\downarrow S}_{\mathcal{HT}} Q' \parallel a?S \qquad P' \parallel S \precsim Q' \parallel a?S$$

$$Q \parallel R \xrightarrow{\tau} Q' \parallel R = Q' \parallel a?S \parallel R''$$

$$P' \parallel R' = P' \parallel S \parallel R''$$

- Completeness: $P \xrightarrow{\alpha}_{\mathcal{HT}} P'$ iff $P \parallel \chi_\alpha \rightarrow P'$

REFINING

- But here outputs are observable!

$$a! \parallel Q \simeq R \qquad \Rightarrow \qquad R = a! \parallel R'$$

proving this is surprisingly tricky

$$\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a?} P' \| a!} \text{(InHT)} \qquad \cancel{\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a!\downarrow R} P' \| a?R} \text{(OutHT)}}$$

- It is good to get rid of HT rules when they are not necessary
  - LTS are smaller
  - bisimulations are easier to construct

ASYNCHRONOUS BISIMULATION

(R. AMADIO, I. CASTELLANI, D. SANGIORGI, ON BISIMULATIONS FOR THE ASYNCHRONOUS PI CALCULUS, TCS 195(2):291-324, 1998)

$$PRQ \ \& \ P \xrightarrow{a?} P' \text{ then either } Q \xrightarrow{a?} Q' \ \& \ P'RQ' \text{ or}$$

$$Q \xrightarrow{\tau} Q' \ \& \ P'R(Q' \parallel a!)$$

- Putting facts about observability into the definition of equivalence
- We don't like this
  - need to reprove basic facts about bisimilarity
  - not clear exactly what is "asynchronous" about the bisimilarity
- We like the principle of getting the "right" labelled transitions into the LTS

PLAN

1. Introduction
2. Full asynchrony
3. Asynchrony
4. **Synchrony**
5. Infinite processes

SYNCHRONY

Syntax

$$P \;::=\; 0 \mid a!P \mid a?P \mid P \parallel Q \mid \tau P$$

Reduction semantics

$$\tau P \;\rightarrow\; P$$

$$a!P \parallel a?Q \;\rightarrow\; P \parallel Q$$

$$\frac{P \rightarrow P'}{P \| Q \rightarrow P' \| Q}$$

$$\frac{Q \equiv P \quad P \rightarrow P' \quad P' \equiv Q'}{Q \rightarrow Q'}$$

Structural congruence

$$(P \parallel Q) \parallel R \;\equiv\; P \parallel (Q \parallel R)$$

$$P \parallel Q \equiv Q \parallel P$$

$$P \parallel 0 \;\equiv\; P$$

SOS

$$\frac{}{a?P \xrightarrow{a?\downarrow R} P\|R}\ (\textsc{In}) \qquad \frac{P \xrightarrow{a?\downarrow R} P'}{P\|Q \xrightarrow{a?\downarrow R} P'\|Q}\ (\textsc{In}\|) \qquad \frac{}{\tau \xrightarrow{\tau} 0}\ (\textsc{Tau})$$

$$\frac{}{a! \xrightarrow{a!\downarrow R} R}\ (\textsc{Out}) \qquad \frac{P \xrightarrow{a!\downarrow R} P'}{P\|Q \xrightarrow{a!\downarrow R} P'\|Q}\ (\textsc{Out}\|) \qquad \frac{P \xrightarrow{\tau} P'}{P\|Q \xrightarrow{\tau} P'\|Q}\ (\textsc{Tau}\|)$$

$$\frac{P \xrightarrow{a?\downarrow 0} P' \qquad Q \xrightarrow{a!\downarrow 0} Q'}{P\|Q \xrightarrow{\tau} P'\|Q'}\ (\textsc{Comm})$$

- Context lemma & soundness

HONDA TOKORO

$$\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a?\downarrow R} P' \| a!R} \ (\textsc{InHT}) \qquad \frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a!\downarrow R} P' \| a?R} \ (\textsc{OutHT})$$

- Again, the LTS completed with HT rules is sound and complete
- This time, both the actions are observable and so both Honda Tokoro rules are unnecessary
  - ie the SOS on the previous slide is sound and complete for contextual equivalence

GENERAL HT RULE FORM

- Suppose that α is an action with an associated context χ_α

$$P \xrightarrow{\alpha} P' \quad \Rightarrow \quad \chi_\alpha(P) \rightarrow P'$$

$$\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{\alpha} \chi_\alpha(P')} \; (\alpha\mathrm{HT})$$

MORALS OF THE STORY

- Labelled transitions are used to
  1. generate the reduction relation inductively
  2. give a proof method for reasoning about contextually defined process equivalence
- The first (choosing experiment) can be done systematically, starting from reductions
- Morally non-observable labels can then be made unobservable using Honda-Tokoro rules, characterising contextual equivalence
  - observability is a calculus-specific notion