Context alterations as labels

Bartek Klin
University of Cambridge, Warsaw University

IFIP WG1.3, Udine, 11/09/09

CCS: Two ways of specification

$$P ::= 0 \mid a.P \mid \bar{a}.P \mid \tau.P \mid P||P$$

Labeled

$$\frac{}{\alpha.P \xrightarrow{\alpha} P}$$

$$\frac{P \xrightarrow{\alpha} P'}{P||Q \xrightarrow{\alpha} P'||Q}$$ **(+symm.)**

$$\frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{\alpha}} Q'}{P||Q \xrightarrow{\tau} P'||Q'}$$

Reactive

$$P||0 \cong P$$
$$P||Q \cong Q||P$$
$$(P||Q)||R \cong P||(Q||R)$$

$$a.P||\bar{a}.Q \rightsquigarrow P||Q$$
$$\tau.P \rightsquigarrow P$$

Aynchronous CCS

$$P ::= 0 \mid a.P \mid \boxed{\bar{a}} \mid \tau.P \mid P||P$$

Labeled

$$\frac{}{\alpha.P \xrightarrow{\alpha} P}$$

$$\boxed{\frac{P \xrightarrow{\tau} P'}{P \xrightarrow{a} P'||\bar{a}}}$$

$$\frac{P \xrightarrow{\alpha} P'}{P||Q \xrightarrow{\alpha} P'||Q}$$ (+symm.)

$$\frac{P \xrightarrow{\alpha} P' \quad Q \xrightarrow{\bar{\alpha}} Q'}{P||Q \xrightarrow{\tau} P'||Q'}$$

Reactive

$$P||0 \cong P$$

$$P||Q \cong Q||P$$

$$(P||Q)||R \cong P||(Q||R)$$

$$a.P|\boxed{\bar{a}} \rightsquigarrow P$$

$$\tau.P \rightsquigarrow P$$

From reactive to labeled

Typical goal:

From a reactive specification,
derive a bisimulation congruence.

[Sew98], [Lei02], [Sob04], [KSS05], [Bon08]...

How about the full relation?

Real goal: a convincing definition of equivalence for reactive specifications.

Any help from Term Rewriting?

In TR, equivalence typically contains reduction:

$$t \rightsquigarrow r \Longrightarrow t \approx r$$

Sensible if some confluence is present.

But we want no confluence!

$$P + Q \rightsquigarrow P \qquad\qquad P + Q \rightsquigarrow Q$$

Idea: systems equivalent iff we can't see a difference.

Idea 1: Saturated semantics

To test a system, we can:

- put it in a context,
- notice that a reaction has happened.

(also clone it, exhaust its capabilities...)

$\approx$ is a bisimulation congruence if $P \approx Q$ implies:

- $C[P] \approx C[Q]$ for all C ,
- if $P \rightsquigarrow P'$ then $Q \rightsquigarrow Q'$ s.t. $P' \approx Q'$.

A simple formalisation

A monoidal reduction system (MRS):
- set A of agents
- monoid $(M, 1, \cdot)$ of contexts
- action $-[-]$ of M on A
- transition relation $\rightsquigarrow$ on A

(Idea: A = terms, M = unary contexts, up to $\cong$)

An LTS presentation: $P \xrightarrow{C[-]} R \iff C[P] \rightsquigarrow R$

Saturated bisimilarity: $\approx_S$

Trouble: divergence

$$P ::= 0 \mid a.P \mid \bar{a}.P \mid \tau.P \mid P||P \mid \boxed{\Omega}$$

$$P||0 \cong P \qquad\qquad a.P||\bar{a}.Q \rightsquigarrow P||Q$$

$$P||Q \cong Q||P \qquad\qquad \tau.P \rightsquigarrow P$$

$$(P||Q)||R \cong P||(Q||R) \qquad\qquad \boxed{\Omega \rightsquigarrow \Omega}$$

$$\Omega \quad \approx \quad \Omega \,||\, a.0$$

Idea: $\bar{a}.0$ **not necessary in** Ω $\qquad ||\bar{a}.0 \rightsquigarrow \Omega||\bar{a}.0$

but necessary in $\Omega||a.0||\bar{a}.0 \rightsquigarrow \Omega$

Idea 2: IPO semantics

To test a system, we can:

- ...
- check if a context is necessary for reduction.

Roughly: if $P \xrightarrow{C[-]} R$

then $P \xrightarrow{D[C[-]]} D[R]$ unnecessary.

IPO LTS	$\subseteq$	Saturated LTS
$\approx_I$	$\subseteq$	$\approx_S$

More structure required

A monoidal reduction system (MRS):

- set A of agents
- monoid $(M, 1, \cdot)$ of contexts
- action $-[-]$ of M on A
- a set of reaction rules $(L, R) \in A \times A$
- a submonoid $D \subseteq M$ of reactive contexts

these define:

- transition relation $\rightsquigarrow$ on A

Trouble: asynchrony

$$P ::= 0 \mid a.P \mid \bar{a} \mid \tau.P \mid P||P$$

$$P||0 \cong P$$
$$P||Q \cong Q||P$$
$$(P||Q)||R \cong P||(Q||R)$$

$$a.P||\bar{a} \leadsto P$$
$$\tau.P \leadsto P$$

(+ summation...)

$$a.\bar{a} + \tau.0 \qquad \not\approx_I \qquad \tau.0$$

$a.\bar{a} + \tau.0 \xrightarrow{-||\bar{a}} \bar{a}$ **but** $\tau.0 \not\xrightarrow{-||\bar{a}}$

The weak scenario

To test a system, we can:

- put it in a context,
- ~~notice that a reaction has happened.~~

If $\rightsquigarrow$ reflexive and transitive:

- $\approx_S$ always the full relation,
- $a.\bar{a} \not\approx_I 0$ in asynchronous CCS.

So: are there further ways to observe systems?

Idea 3: Barbs [MS92]

Barb: a predicate on systems.

Given a selection of barbs,

$\approx$ is a barbed congruence if $P \approx Q$ implies:

- $C[P] \approx C[Q]$ for all C,
- if $P \rightsquigarrow P'$ then $Q \rightsquigarrow Q'$ s.t. $P' \approx Q'$,
- P and Q satisfy the same barbs.

The largest such is what we want.

But: how do we choose barbs?

Idea 4: Consistent theories [HY95]

Assume we can observe something.

$\approx$ is a consistent theory if $P \approx Q$ implies:

- $C[P] \approx C[Q]$ for all C,
- if $P \rightsquigarrow P'$ then $Q \rightsquigarrow Q'$ s.t. $P' \approx Q'$,
- $\approx$ is not a full relation.

Problem: there is no largest such.

Idea: require further that a theory identifies all insensitive systems.

Thm [HY95]: for the π-calculus, the largest such theory exists.

Does it work in general?

- is consistency always good?
- consider a language:
  - -- constants a, b and c,
  - -- unary operator f,
  - -- two reduction rules: $f(a) \rightsquigarrow c \qquad f(b) \rightsquigarrow c$

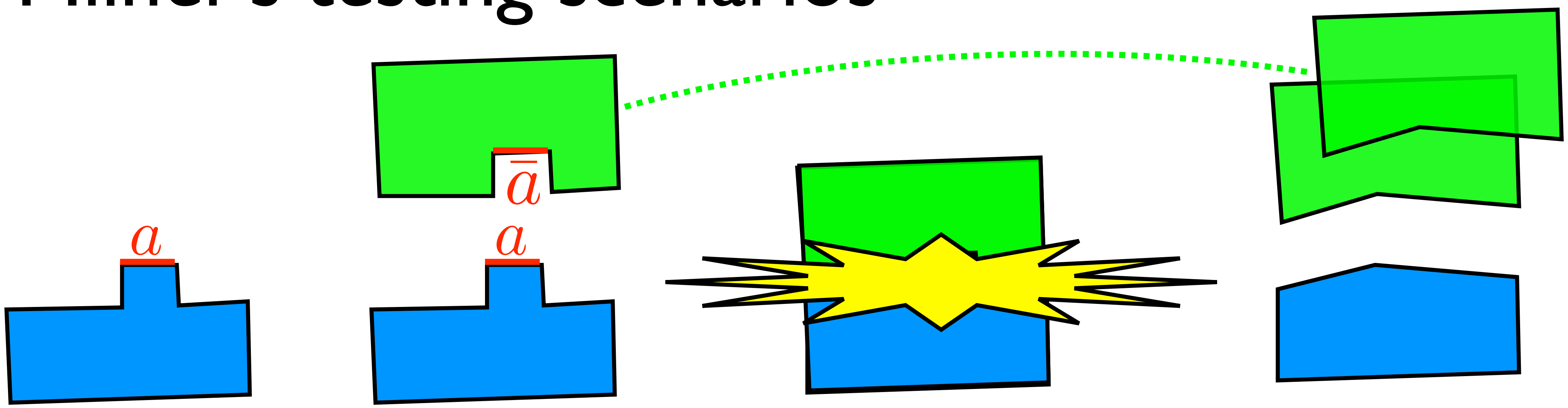
Everything is insensitive except a, b.

Three mutually incomparable theories:

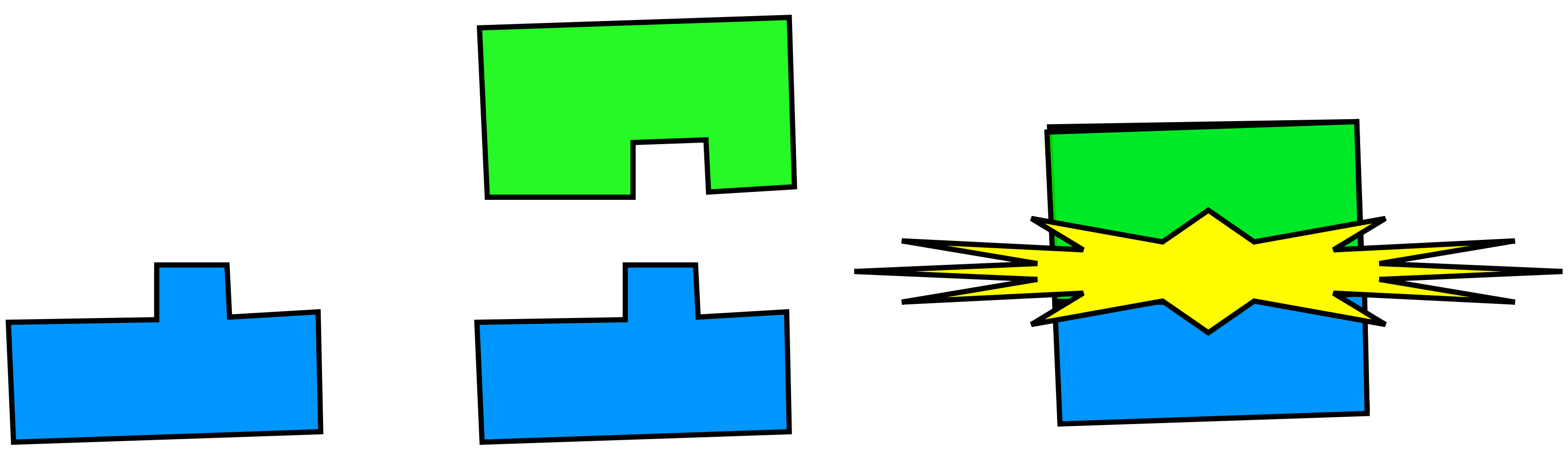
$$\begin{array}{ccc} a & \neq & b \\ \nparallel & & \nparallel \\ & \text{insensitives} & \end{array}$$

What is testing anyway?

A: Milner's testing scenarios



B: Contexts as tests



Idea 5: Pairs of contexts as labels

$$a.P||\bar{a}.Q \rightsquigarrow P||Q$$

$$\boxed{a.P}\,||\bar{a}.Q \rightsquigarrow \boxed{P}\,||Q \qquad a.P \xrightarrow{-||\bar{a}.Q \triangleright -||Q} P$$

$$a.P||\,\boxed{\bar{a}.Q} \rightsquigarrow P||\,\boxed{Q} \qquad \bar{a}.Q \xrightarrow{a.P||- \triangleright P||-} Q$$

Close these under rules:

$$a \xrightarrow{m \triangleright n} b \quad \Longrightarrow a \xrightarrow{km \triangleright kn} b$$

$$a \xrightarrow{mn \triangleright m} n[a]$$

For weak scenario also:

$$a \xrightarrow{m \triangleright m} a$$

$$a \xrightarrow{m \triangleright n} b \xrightarrow{n \triangleright k} c \Longrightarrow a \xrightarrow{m \triangleright k} c$$

Examples

- for CCS with Ω :

$$\Omega || a.0 \xrightarrow{-||\bar{a}.P \triangleright -||P} \Omega$$

but

$$\Omega \not\xrightarrow{-||\bar{a}.P \triangleright -||P}$$

- for asynchronous CCS:

$$a.\bar{a} + \tau.0 \xrightarrow{-||\bar{a} \triangleright -} \bar{a}$$

but also

$$\tau.0 \xrightarrow{-||\bar{a} \triangleright -} \bar{a}$$

Trouble

It is wrong for CCS.

$$P \xrightarrow{-||a.Q \triangleright -||Q} R$$

$$P \xrightarrow{-||a.Q||S \triangleright -||Q||S} R$$

$$P \xrightarrow{-||S||a.Q \triangleright -||S||Q} R$$

?

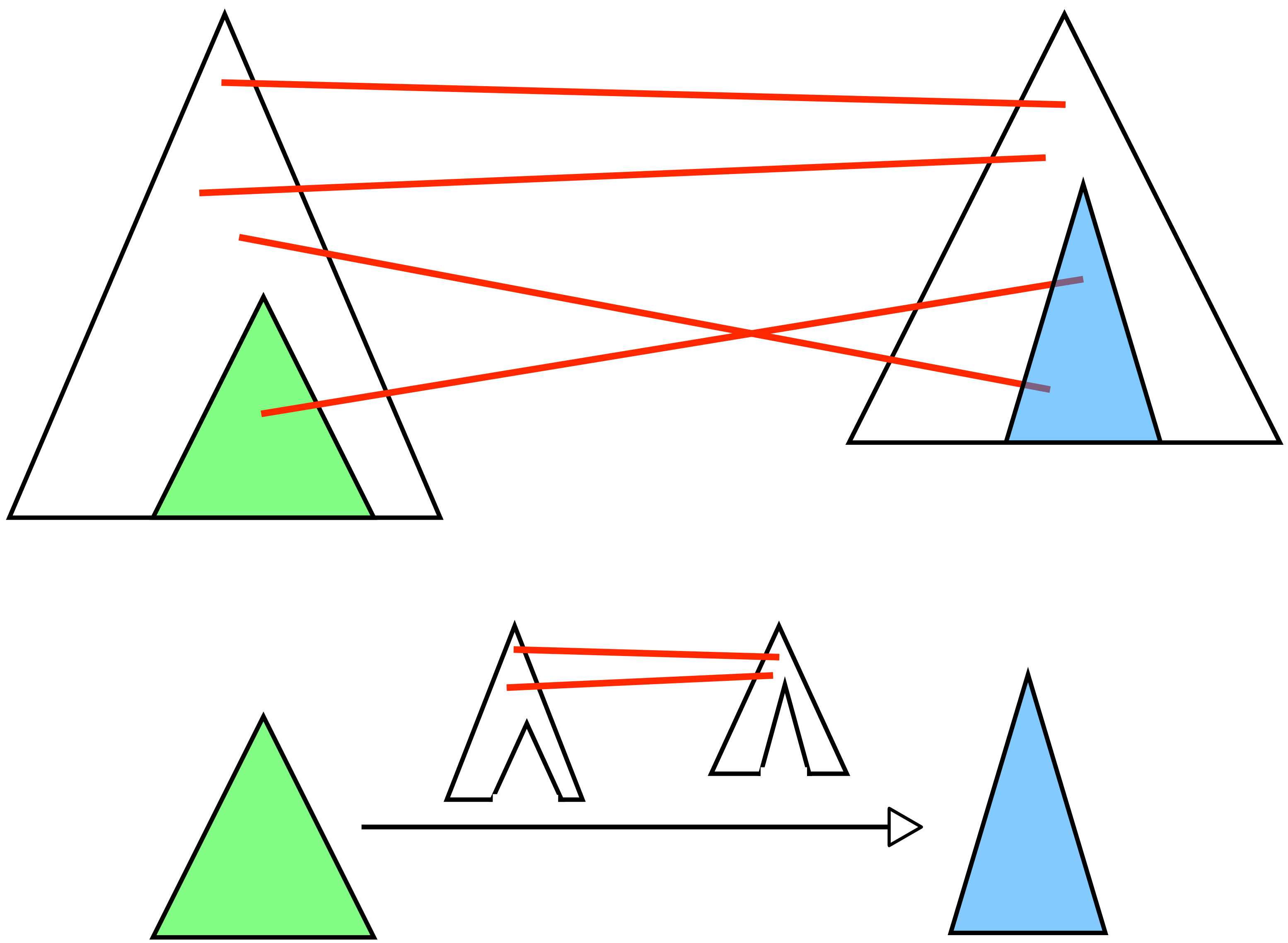
$$P||S \xrightarrow{-||a.Q \triangleright -||Q} R||S$$

Idea 6: change tracking in contexts

$$a.P||\bar{a}.Q \rightsquigarrow P||Q$$

$$a.P \xrightarrow{-||\bar{a}.Q \qquad -||Q} P$$

$$a.P \xrightarrow{-||\bar{a}.Q \qquad -} P||Q$$



Formalisation

Term reactive system:

- signature Σ
- set $\mathcal{R}$ of reactions on closed Σ-terms

Reaction $f : t \rightarrow s$:
relation between nodes of t and s

LTS: $a \xrightarrow{f:t\rightarrow s} b$ iff

$\exists\ g : t[a] \rightarrow b$ **s.t.** $f \cup g : t[a] \rightarrow s[b] \in \mathcal{R}$

Thm: Bisimilarity is a congruence.

(BTW: Structural axioms $\approx$ mutual reductions)

Doubts

1. Abstract enough?

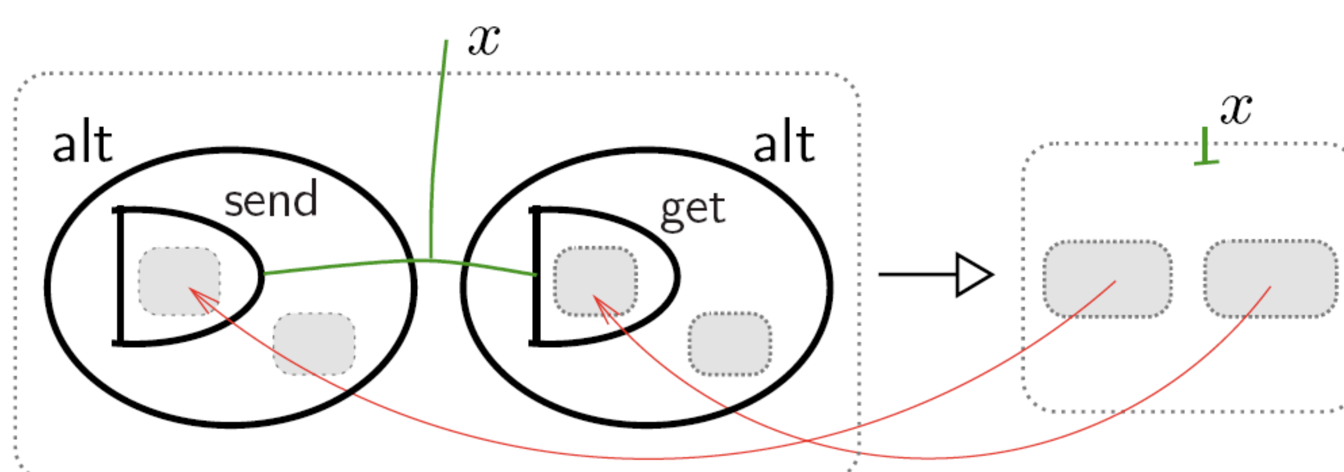
   - category A of agents
   - monoidal category $(M, 1, \otimes)$ of contexts
   - action $-[-]$ of M on A
   - set of arrows $\rightsquigarrow$ in A

Define LTS?

2. General enough?

NB: rich structure on rules required

$$a.P||\bar{a}.Q \rightsquigarrow P||Q$$



Results

1. Bisimilarity for CCS fragment (also with Ω)
2. Asynch. bisimilarity for asynch. CCS fragment

Scribbled:

- the same results for weak scenario

Trimming the labels

In any LTS, labels α and β are equivalent if:

$$P \xrightarrow{\alpha} Q \iff P \xrightarrow{\beta} Q$$

Fact: Labels can be replaced with equivalence classes.

Example: in CCS, all labels of the form

$$-||\bar{a}.Q \qquad -||Q$$

are equivalent.

Call the equivalence class 'a'.

There are also classes '$\bar{a}$', 'τ'...

Slogans and Questions

S1. Tests are contexts, test results are changes to contexts.

S2. Reduction rules contain enough information to track contexts and their changes.

Q1. Does it have to be so complicated?

Q2. More advanced examples?

Q3. Relation to barbs or cons. theories?