On Weak Bisimilarities in CCSK

Ivan Lanese

University of Bologna, Italy/INRIA, France

Joint work with Baptiste Vallée (École Normale Supérieure Paris-Saclay, France)

Outline

Reversible computation

Reversible computation allows computation to proceed not only in the standard, forward direction, but also backwards, recovering past states.

Applications in different areas:

- low-power computing (Landauer 1961)
- optimistic parallel simulation (Carothers et al 1999)
- error recovery in robot assembly operations (Laursen et al 2015)
- debugging (GDB since 2009, WinDbg)
- …

Reversible models of concurrent systems

In many of these areas, concurrent systems are of interest

Reversible extensions of concurrent models and languages have been proposed

Seminal one, RCCS (Danos & Krivine 2004) is a reversible form of CCS (Milner 1980)

Another reversible CCS, CCSK, has been proposed by Phillips & Ulidowski in 2006

Reversible extensions of π-calculus, Petri nets, Erlang, Go and other formalisms have been proposed

Main idea: add history information so that computation can be reversed

Reversibility and concurrency

In a sequential setting actions are undone in reverse order:

$$P \xrightarrow{a} Q \xrightarrow{b} R \qquad\qquad R \xrightarrow{b} Q \xrightarrow{a} P$$

In concurrent systems, a total order of actions may not exist, and if it exists it is not very relevant.

Causal-consistent reversibility (Danos & Krivine 2004)

An action can be reversed iff all its consequences (if any) have been reversed beforehand.

If $P \xrightarrow{a} Q$ causes $Q \xrightarrow{b} R$ then we cannot reverse a before b.

But if $P \xrightarrow{a} Q$ and $Q \xrightarrow{b} R$ are concurrent then we can reverse them in any order:

$$P \xrightarrow{a} Q \xrightarrow{b} R \qquad\qquad R \xrightarrow{a} Q' \xrightarrow{b} P$$

The need for analysis techniques

(Reversible) models allow one to describe systems

We also want to reason on such systems

Many analysis techniques in the literature: (behavioural) types, model checking, behavioural equivalences, …

Bisimilarities

Equivalence relations on processes

A binary relation $\mathcal{R}$ is a **bisimulation** if whenever $P\mathcal{R}Q$:

- If $P \xrightarrow{a} P'$,
- Then there **exist** a state Q' such that $Q \xrightarrow{a} Q'$ and $P'\mathcal{R}Q'$

and vice versa for challenges from Q.
Bisimilarity is the largest bisimulation.

$$
\begin{tikzcd}
P \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"'] & Q \arrow[d, dashed, "a"] \\
P' \arrow[r, dash, dashed, "\mathcal{R}"'] & Q'
\end{tikzcd}
$$

Strong bisimilarity: each action is matched exactly, as above

Weak bisimilarity: internal steps (τ) may be matched by staying idle, and can be done before and after the matching action

Framing the problem

We want to study *bisimilarities*:

for causal-consistent reversibility, since we are interested in concurrent systems (and bisimilarities are tailored for them);

for uncontrolled reversibility: no policy on whether to go forward or backward, or on which action to take if many are enabled;

which are weak: equate processes that do the same visible actions, with possibly different number of internal steps.

Strong bisimilarities have been studied in previous work

Controlled reversibility is left for future work

Selecting the target language

We will work on CCSK

CCS is a simple, yet very used, starting point

A number of works already tackled this or similar settings (Phillips & Ulidowski 2006, Bernardo & Esposito 2023, ...)

RCCS has too much redundancy, reasoning on it is very difficult (we will come back to this)

Outline

Behavioural equivalences for reversible systems

CCSK

Our insights and results

Conclusion

CCSK

CCSK syntax

$$P, Q := \pi.P \mid P + Q \mid (P \mid Q) \mid (\nu a)P \mid 0$$

$$\pi := \alpha \mid \alpha[k]$$

$$\alpha =: a \mid \overline{a} \mid \tau$$

$a, b, \cdots$: actions
$k, m, \cdots$: keys

Keys highlight when the corresponding prefix has been executed, processes without keys are CCS processes.

CCSK semantics: sample rules

Forward	Backward
$$\frac{\mathtt{std}(P)}{\alpha.P \xrightarrow{\alpha[m]}_f \alpha[m].P}$$	$$\frac{\mathtt{std}(P)}{\alpha[m].P \xrightarrow{\alpha[m]}_r \alpha.P}$$
$$\frac{P \xrightarrow{\beta[n]}_f P'}{\alpha[m].P \xrightarrow{\beta[n]}_f \alpha[m].P'}\ m \neq n$$	$$\frac{P \xrightarrow{\beta[n]}_r P'}{\alpha[m].P \xrightarrow{\beta[n]}_r \alpha[m].P'}\ m \neq n$$
$$\frac{P \xrightarrow{\alpha[m]}_f P' \quad Q \xrightarrow{\overline{\alpha}[m]}_f Q'}{P \mid Q \xrightarrow{\tau[m]}_f P' \mid Q'}\ \alpha \neq \tau$$	$$\frac{P \xrightarrow{\alpha[m]}_r P' \quad Q \xrightarrow{\overline{\alpha}[m]}_r Q'}{P \mid Q \xrightarrow{\tau[m]}_r P' \mid Q'}\ \alpha \neq \tau$$

Reachable processes

In reversible calculi only processes which have consistent history information are of interest.

Definition (Reachable process)

A process is *reachable* if there is a derivation leading to it from a process with no keys (standard process).

Starting point for bisimulation definition

We start from the definition of strong bisimulation in [Lanese & Phillips, 2021]:

Definition (Forward-reverse bisimulation)

A symmetric relation $\mathcal{R}$ is a *forward-reverse (FR) bisimulation* if whenever $P \mathrel{\mathcal{R}} Q$:

1. if $P \xrightarrow{\mu}_f P'$ then there is Q' such that $Q \xrightarrow{\mu}_f Q'$ and $P' \mathrel{\mathcal{R}} Q'$;
2. if $P \xrightarrow{\mu}_r P'$ then there is Q' such that $Q \xrightarrow{\mu}_r Q'$ and $P' \mathrel{\mathcal{R}} Q'$.

FR bisimilarity $\sim_{FR}$ is the largest FR bisimulation.

α-conversion of keys

Keys can be:

free: one occurrence, not attached to a τ OR
bound: two occurrences, or one attached to a τ

Key insight

Identity of free keys matters, identity of bound keys does not

$$\overline{a}[n] \mid a[n] \;\mathcal{R}\; \overline{a}[m] \mid a[m] \qquad\qquad \overline{a}[n] \;\not\mathcal{R}\; \overline{a}[m]$$

$\overline{a}[n]$ and $\overline{a}[m]$ behave differently inside context $\bullet \mid a[n]$

Use rules for α-conversion of bound keys.

$$X \equiv X[n/m] \qquad m \text{ bound in } X, n \notin \mathtt{keys}(X)$$

Without α-conversion we would have:

$$\overline{a}[n] \mid a[n] \mid b \;\not\mathcal{R}\; \overline{a}[m] \mid a[m] \mid b$$

since the former could choose m as new key to execute b.

Outline

Behavioural equivalences for reversible systems

CCSK

Our insights and results

Conclusion

Weak bisimilarities

Main design decision: should τ actions be in the same direction as the matched action, or can they be in any direction?

Two options, leading to *(weak) directional bisimilarity* and *(weak) mixed bisimilarity*.

Definition (Mixed Bisimulation)

A symmetric relation $\mathcal{R}$ is a *mixed bisimulation* if whenever $P \mathrel{\mathcal{R}} Q$ we have:

1. if $P \xrightarrow{\tau}_x P'$ then there exists Q' such that $Q \Rightarrow_m Q'$ and $P' \mathrel{\mathcal{R}} Q'$;
2. if $P \xrightarrow{\mu}_x P'$ then there exists Q' such that $Q \overset{\mu}{\Rightarrow}_{m,x} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.

Mixed bisimilarity $\approx_m$ is the largest mixed bisimulation.

$P \overset{\mu}{\Rightarrow}_{m,x} P'$ iff $\exists Q, Q'$ s.t. $(P \Rightarrow_m Q \xrightarrow{\mu}_x Q' \Rightarrow_m P')$.

Weak bisimilarities

Main design decision: should τ actions be in the same direction as the matched action, or can they be in any direction?

Two options, leading to *(weak) directional bisimilarity* and *(weak) mixed bisimilarity*.

Definition (Directional Bisimulation)

A symmetric relation $\mathcal{R}$ is a *directional bisimulation* if whenever $P \mathrel{\mathcal{R}} Q$ we have:

1. if $P \xrightarrow{\tau}_x P'$ then there exists Q' such that $Q \Rightarrow_x Q'$ and $P' \mathrel{\mathcal{R}} Q'$;
2. if $P \xrightarrow{\mu}_x P'$ then there exists Q' such that $Q \overset{\mu}{\Rightarrow}_{d,x} Q'$ and $P' \mathrel{\mathcal{R}} Q'$;

Directional bisimilarity $\approx_d$ is the largest directional bisimulation.

$P \overset{\mu}{\Rightarrow}_{d,x} P'$ iff $\exists Q, Q'$ s.t. $(P \Rightarrow_x Q \xrightarrow{\mu}_x Q' \Rightarrow_x P')$.

Comparison by examples

Mixed	Directional
$a.b + b.a \not\approx_m a \mid b$	$a.b + b.a \not\approx_d a \mid b$
$\tau.a \approx_m a$	$\tau.a \approx_d a$
$\tau \mid a \approx_m a$	$\tau \mid a \approx_d a$
$\tau + a \approx_m a$	$\tau + a \not\approx_d a$
$\tau[m] + a \approx_m a$	$\tau[m] + a \not\approx_d a$

Proposition (Mixed bisimilarity abstracts away from τ steps)

$P \Rightarrow_m Q$ implies $P \approx_m Q$.

Not the case for directional bisimilarity or CCS weak bisimilarity

Hierarchy of Bisimilarities

Proposition (Hierarchy of Bisimilarities)

$$\sim_{FR} \subset \approx_d \subset \begin{cases} \approx_m \\ \approx \end{cases}$$

Rationale for inclusions:

	Abstracts τ	$a.b + b.a \neq a \mid b$
Strong FR $\sim_{FR}$	NO	YES
Directional $\approx_d$	SOME	YES
Mixed $\approx_m$	YES	YES
Weak CCS $\approx$	SOME	NO

Inclusions are strict even if we consider only standard processes
The induced equivalences on CCS processes are in the same relations

Congruence properties

Congruence: $P \mathcal{R} Q \implies C[P] \mathcal{R} C[Q]$ for each context C
If a bisimilarity is a congruence we can reason axiomatically on it

Proposition (Directional bisimilarity is not a congruence)

Directional bisimilarity $\approx_d$ is not a congruence.

Counterexample

$\tau[n] \approx_d 0 \not\Longrightarrow a + \tau[n] \approx_d a + 0$

Proposition (Mixed bisimilarity is a congruence)

Mixed bisimilarity $\approx_m$ is a congruence.

Not the case for CCS weak bisimilarity

Why not RCCS?

Example (In CCSK)

$$a.(P \mid Q) + a.(P \mid Q) \xrightarrow{a[n]}_f a[n].(P \mid Q) + a.(P \mid Q)$$

The axiom $X + P \sim X$ (if $\mathtt{toStd}(X) = P$) allows us to prove:

$$a[n].(P \mid Q) + a.(P \mid Q) \sim a[n].(P \mid Q)$$

Example (In RCCS)

$$\emptyset \rhd a.(P \mid Q) + a.(P \mid Q) \xrightarrow{\emptyset : a}_f^{RCCS} [*, a, a.(P \mid Q)] \cdot \emptyset \rhd (P \mid Q) \equiv$$
$$(< 1 > \cdot [*, a, a.(P \mid Q)] \cdot \emptyset \rhd P) \mid (< 2 > \cdot [*, a, a.(P \mid Q)] \cdot \emptyset \rhd Q)$$

You are welcome to try to find axiom(s) to prove:

$$(< 1 > \cdot [*, \color{blue}{a}, \color{red}{a.(P \mid Q)}] \cdot \emptyset \rhd \color{blue}{P}) \mid (< 2 > \cdot [*, \color{blue}{a}, \color{red}{a.(P \mid Q)}] \cdot \emptyset \rhd \color{blue}{Q}) \sim$$
$$(< 1 > \cdot [*, a, \color{red}{0}] \cdot \emptyset \rhd P) \mid (< 2 > \cdot [*, a, \color{red}{0}] \cdot \emptyset \rhd Q)$$

Outline

Summary

- New forms of weak bisimilarity: directional and mixed

	Weak	Abstracts τ	Truly conc.	Congr.
Strong FR $\sim_{FR}$	NO	NO	YES	YES
Directional $\approx_d$	YES	SOME	YES	NO
Mixed $\approx_m$	YES	YES	YES	YES
Weak CCS $\approx$	YES	SOME	NO	NO

- Mixed bisimilarity:
  - is weak and completely abstracts away from τ actions;
  - is truly concurrent;
  - is a congruence.

  No other known bisimilarity has these properties.

Future work

Mixed bisimilarity is the most interesting result of this paper.

We want to study it more in depth:

- Characterizing it as a barbed congruence
- Finding an inductive characterization on CCS
  - strong one corresponds to hereditary history-preserving bisimilarity
- Finding an axiomatization
  - missing for strong FR bisimilarity as well
- Applying it to more complex calculi (it requires modelling them with no redundancy).

Thanks! Questions?