An Axiomatic Approach to Reversible Computation

Ivan Lanese, Iain Phillips and Irek Ulidowski

March 2, 2020

Outline

Axiomatic approach

Case studies

RCCS

RCCS (Danos & Krivine 2004) is a reversible form of CCS (Milner 1980).

Adds memories so that computations can be reversed.

We suppress the syntax and just show the labelled transition system (LTS):

Forward: $P \xrightarrow{a} Q$

Reverse: $Q \xrightarrow{\underline{a}} P$

General transition: $t : P \xrightarrow{\alpha} Q$

Inverse: $\underline{t} : Q \xrightarrow{\underline{\alpha}} P$

RCCS

Can reverse along the same path taken forwards (backtracking):

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

But takes also concurrency into account.

Key idea

An action can be reversed iff all its consequences have been reversed.

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

But if $P \xrightarrow{a} Q$ and $Q \xrightarrow{b} R$ are independent (concurrent) we can have

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

Here Q' was not visited going forwards, but could have been:

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

RCCS

Concretely, independence means that memories are *coherent* (non-overlapping), so that the transitions belong to different threads.

Causation is not modelled directly in RCCS.

Paths r, s are sequences of transitions $t_1 t_2 \ldots t_n$.

Causal equivalence on paths: $r \approx s$ iff s can be got from r by

1. swapping adjacent independent transitions
2. cancellation $t\underline{t} = \underline{t}t = \epsilon$

Causal Consistency

Causal Consistency (CC)

If r and s are coinitial and cofinal paths then $r \approx s$.

CC has become the dominant property shown for reversible languages.

CC has been shown for RCCS and numerous other reversible calculi:

- μOz (Lienhardt et al 2012)
- Klaim (tuple-based language, Giachino et al 2017)
- reversible Erlang (Lanese et al 2018)
- reversible occurrence nets (Melgratti et al 2019)

Proofs are quite lengthy but mostly take a similar approach.

Our approach

Our idea

If we can show that properties such as CC follow from a small set of axioms, it should be easier to check these properties by verifying the axioms.

We use abstract labelled transition systems with independence (LTSIs).

Related to the occurrence LTSIs of Sassone et al (1996).

- We adopt a minimal set of axioms and add more as needed
- We treat reverse transitions as first-class citizens

Our approach

Usual proof of CC involved showing the Parabolic Lemma (PL) and then showing a weaker form of CC by various means depending on the context.

By studying basic axioms we have the following:

Axioms

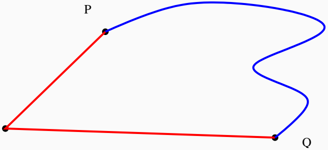
1. Coinitial backward transitions are independent (generalizes backward determinism from sequential reversible models):

$$\begin{tikzcd} Q & \\ & P \arrow[ul, "a"'] \arrow[dl, "b"] \\ R & \end{tikzcd}$$

2. Square property: If transitions are coinitial and independent then:

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

From these we can deduce the Parabolic Lemma:



Axioms

3. Well-foundedness (WF): no infinite reverse path

$$\cdots \xrightarrow{a_{n+1}} P_n \xrightarrow{a_n} \cdots \xrightarrow{a_2} P_1 \xrightarrow{a_1} P_0$$

Cannot reverse to before starting point.

Theorem

If WF and PL then CC.

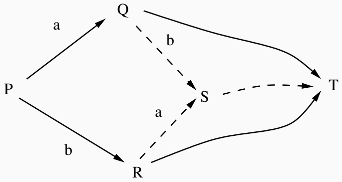
- Success for the axiomatic approach
- Much shorter than existing proofs
- Shows that CC is not much stronger than PL

CC

Existing proofs of CC do not appear to use WF.

They do use further properties which are not deducible from our axioms.

Forward confluence:



Beyond CC

If CC is weaker than thought, how should we characterise our Key Idea?

Split into:

- Causal Safety: if can reverse t then all its consequences have been undone
- Causal Liveness: if all t's consequences have been undone then can reverse t

Events

Since different transitions may represent the same action executed at different points in the computation (after or before some independent event) it is convenient to group together transitions into events.

$$\begin{tikzcd} P \arrow[r, "a"] \arrow[d, "b"] & Q \arrow[d, "b"] \\ R \arrow[r, "a"] & S \end{tikzcd}$$

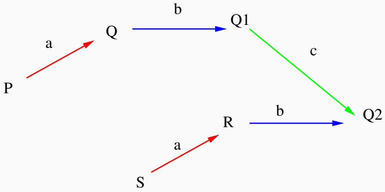
If coinitial transitions in the square are independent then we let

$$P \xrightarrow{\alpha} Q \sim R \xrightarrow{\alpha} S \qquad P \xrightarrow{\beta} R \sim Q \xrightarrow{\beta} S$$

Get two events $[P \xrightarrow{\alpha} Q]$ and $[P \xrightarrow{\beta} R]$ as equivalence classes.

Lift independence to events: $[t_1]$ ci $[t_2]$ if have representatives t_1' and t_2' which are coinitial and independent.

Causal Safety (CS)



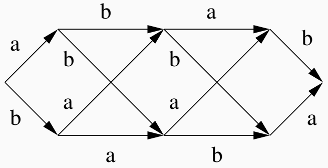
We give three definitions of causal safety:

1. via independence of transitions ($P \xrightarrow{a} Q \mathrel{\iota} Q_1 \xrightarrow{c} Q_2$)
2. via ordering of events ($[P \xrightarrow{a} Q] \not< [Q_1 \xrightarrow{c} Q_2]$)
3. via independence of events ($[P \xrightarrow{a} Q] \;\mathrm{ci}\; [Q_1 \xrightarrow{c} Q_2]$)

With minimal axioms these are all different, but with our full set of axioms they become equivalent.

Example

Satisfies all axioms so far and therefore PL+CC, but not CS and not CL:



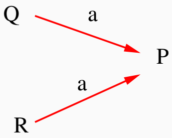
Leftmost a independent on all the b.

CS fails on ba<u>b</u>, CL fails on abb.

We provide further axioms from which CS and CL can be deduced.

Reverse event determinism

RED: reverse event determinism



If $t_1 : Q \xrightarrow{a} P \sim t_2 : R \xrightarrow{a} P$ then $t_1 = t_2$.

A natural property for reversible systems.

Theorem

The following are equivalent under minimal axioms:

1. *NRE: no event can occur (net) twice in a path*
2. *RED: reverse event determinism*
3. *Polychotomy: events are ordered, in conflict or independent*

Showing CC is not enough to show RED - need further axioms.

Axioms

1. SP: square property
2. BTI: backward transitions are independent
3. WF: well-founded
4. CPI: coinitial propagation of independence (around a square)

$$\begin{tikzcd} P \arrow[r, "a"] \arrow[d, "b"] & Q \arrow[d, "b"] \\ R \arrow[r, "a"] & S \end{tikzcd}$$

5. IRE: independence respects events (if $t \sim t' \iota u$ then $t \iota u$)
6. IEC: independence of events is coinitial (if $t \iota u$ then $[t]$ ci $[u]$)

Outline

Axiomatic approach

Case studies

RCCS

Independence coincides with concurrency.

All the axioms are satisfied. Mostly proved in the original paper or trivial. CPI and IRE easy since independence is defined on labels.

We get for free PL, CC, CS and CL (and other minor results).

$\rho\pi$ and Erlang

Similar to RCCS, the main difference is that it has a reduction semantics. However, richer labels have been defined using the memories involved in the transition.

We get for free PL, CC, CS and CL (and other minor results).

Our framework does not apply directly since SP holds only up to label equivalence (due to extrusions).

It can probably be applied to a more abstract LTS, but then one need to study how to take the results back to the original LTS.

Summary

- We present basic axioms which are satisfied by RCCS and other reversible calculi.
- For a new reversible languages, verifying these axioms will be easier than verifying less basic properties.
- We have seen that Causal Consistency is not sufficient, and should be supplemented by Causal Safety and Causal Liveness.
- Our abstract proofs are relatively easy to formalise in a proof assistant.