Proofs about Network Communication: For Humans and Machines

Wolfgang Jeltsch Javier Díaz

Well-Typed The Haskell Consultants · ATIX A Globant Division · Input Output

16th Interaction and Concurrency Experience

Lisbon, Portugal
19 June 2023

Introduction

- Concurrent and distributed systems are often safety-critical
- Machine-checked proofs can provide a high degree of assurance
- Our research program:
  - Targets verification of design refinements
  - Centers on the Ouroboros blockchain consensus protocols
  - Uses the Isabelle proof assistant
- Previous achievement:
  - 👍 A machine-checked correctness proof of broadcast via multicast
- Issue with this proof:
  - 👎 Relies on fundamental but unproved bisimilarity statements
- Now we are delivering the missing proofs
- And show you how to conduct such proofs so that they are:
  - Concise
  - Human-friendly
  - Machine-checked

The Þ-calculus

- A process calculus
- Our language for describing concurrent and distributed systems
  - Protocol specifications
  - Protocol implementations
  - Protocol environments
- Developed by us as part of our research program
- Key properties:
  - General
  - Minimal
  - Suitable for machine-checked proofs
- Similar to the asynchronous π-calculus
- Additional features:
  - Arbitrary data
  - Computation
  - Conditional execution
- Embedded in Isabelle/HOL

The Þ-calculus in detail

- Processes:

$\mathbf{0}$	does nothing
$a \triangleleft x$	sends value x to channel a
$a \triangleright x.\ P\, x$	receives a value x from channel a, performs process $P\, x$
$p \parallel q$	performs processes p and q in parallel
$\nu a.\ P\, a$	introduces a local channel a, performs process $P\, a$

- Constructs capture just the key features of process calculi
  - Concurrency
  - Communication
- For other features we utilize the host language (Isabelle/HOL)
  - Using higher-order abstract syntax (HOAS)
    - Name binding
    - Arbitrary data
    - Computation
    - Conditional execution
  - Using coinduction
    - Repetition

Repetition

- Proofs about coinductively defined processes tend to be low-level
- Solution:
  - Define just a single, general repetition construct via coinduction
  - Show fundamental properties of this construct for later use in proofs
- Repeated receive:

  $a \triangleright^{\infty} x.\, P\, x$ repeatedly receives values x from channel a, initiates the execution of $P\, x$ for each received x

- Definition:

$$a \triangleright^{\infty} x.\, P\, x = a \triangleright x.\, (P\, x \parallel a \triangleright^{\infty} x.\, P\, x)$$

Repeated receive idempotency

- Repeated receive is idempotent
  - With respect to parallel composition
  - Up to bisimilarity
- Formally:

$$a \triangleright^{\infty} x.\, P\, x \parallel a \triangleright^{\infty} x.\, P\, x \sim a \triangleright^{\infty} x.\, P\, x$$

- This fact is used in our correctness proof of broadcast via multicast
- Its proof exemplifies the proof style we advocate here

Background of the proof of repeated receive idempotency

- Þ-calculus transition rules about $\triangleleft$, $\triangleright$, and $\parallel$:

$$\frac{}{a \triangleleft x \xrightarrow{a \triangleleft x} \mathbf{0}} \quad (\triangleleft) \qquad \frac{}{a \triangleright x.\, P\, x \xrightarrow{a \triangleright x} P\, x} \quad (\triangleright)$$

$$\frac{p \xrightarrow{a \triangleleft x} p' \quad q \xrightarrow{a \triangleright x} q'}{p \parallel q \xrightarrow{\tau} p' \parallel q'} \quad (\tau_{\rightarrow}) \qquad \frac{p \xrightarrow{a \triangleright x} p' \quad q \xrightarrow{a \triangleleft x} q'}{p \parallel q \xrightarrow{\tau} p' \parallel q'} \quad (\tau_{\leftarrow})$$

$$\frac{p \xrightarrow{\alpha} p'}{p \parallel q \xrightarrow{\alpha} p' \parallel q} \quad (\parallel_1) \qquad \frac{q \xrightarrow{\alpha} q'}{p \parallel q \xrightarrow{\alpha} p \parallel q'} \quad (\parallel_2)$$

- Definition of repeated receive again:

$$a \triangleright^{\infty} x.\, P\, x = a \triangleright x.\, (P\, x \parallel a \triangleright^{\infty} x.\, P\, x)$$

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
shows $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \sim a \triangleright^{\infty} x.\ P\,x$

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
shows $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \sim a \triangleright^{\infty} x.\ P\,x$
proof coinduction
case (forward_simulation α s)

next
case (backward_simulation α s)

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \sim a \triangleright^{\infty} x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \sim a \triangleright^\infty x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \sim a \triangleright^\infty x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle\ldots\rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \sim a \triangleright^{\infty} x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^{\infty} x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^{\infty} x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^{\infty} x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$
  then have $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \xrightarrow{a \triangleright x} (P\,x \parallel a \triangleright^{\infty} x.\ P\,x) \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \sim a \triangleright^\infty x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  then have $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel (a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x)$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \sim a \triangleright^\infty x.\ P\,x$
proof coinduction
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  then have $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} (P\,x \parallel a \triangleright^\infty x.\ P\,x) \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \sim a \triangleright^\infty x.\ P\,x$
proof (coinduction rule: up_to_rule [**where** $\mathcal{F} = [\sim] \frown \mathcal{M}$])
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^\infty x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$
  then have $a \triangleright^\infty x.\ P\,x \parallel a \triangleright^\infty x.\ P\,x \xrightarrow{a \triangleright x} (P\,x \parallel a \triangleright^\infty x.\ P\,x) \parallel a \triangleright^\infty x.\ P\,x$
    $\langle$proof$\rangle$

qed

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \sim a \triangleright^{\infty} x.\ P\,x$
proof (coinduction rule: up_to_rule [**where** $\mathcal{F} = [\sim] \frown \mathcal{M}$])
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^{\infty} x.\ P\,x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\,x \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^{\infty} x.\ P\,x \xrightarrow{\alpha} s$› **have** $a \triangleright^{\infty} x.\ P\,x \xrightarrow{a \triangleright x} P\,x \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$
  then have $a \triangleright^{\infty} x.\ P\,x \parallel a \triangleright^{\infty} x.\ P\,x \xrightarrow{a \triangleright x} (P\,x \parallel a \triangleright^{\infty} x.\ P\,x) \parallel a \triangleright^{\infty} x.\ P\,x$
    $\langle$proof$\rangle$

qed respectful

Proving repeated receive idempotency

lemma repeated_receive_idempotency:
  shows $a \triangleright^\infty x.\, P\, x \parallel a \triangleright^\infty x.\, P\, x \sim a \triangleright^\infty x.\, P\, x$
proof (coinduction rule: up_to_rule [**where** $\mathcal{F} = [\sim] \frown \mathcal{M}$])
  case (forward_simulation α s)
  $\langle \ldots \rangle$
next
  case (backward_simulation α s)
  from ‹$a \triangleright^\infty x.\, P\, x \xrightarrow{\alpha} s$›
  obtain x **where** $\alpha = a \triangleright x$ **and** $s = P\, x \parallel a \triangleright^\infty x.\, P\, x$
    $\langle$proof$\rangle$
  with ‹$a \triangleright^\infty x.\, P\, x \xrightarrow{\alpha} s$› **have** $a \triangleright^\infty x.\, P\, x \xrightarrow{a \triangleright x} P\, x \parallel a \triangleright^\infty x.\, P\, x$
    $\langle$proof$\rangle$
  then have $a \triangleright^\infty x.\, P\, x \parallel a \triangleright^\infty x.\, P\, x \xrightarrow{a \triangleright x} (P\, x \parallel a \triangleright^\infty x.\, P\, x) \parallel a \triangleright^\infty x.\, P\, x$
    $\langle$proof$\rangle$
  then show *?case*
    $\langle$proof$\rangle$
qed respectful

Tools for bisimulation proofs for humans and machines

- The Isabelle/Isar proof language
  - Closer to usual mathematics than proof terms and tactics scripts
  - Still precise and amenable to machine-checking
- A formalized algebra of "up to" methods
  - Concise bisimulation proofs that are machine-checked
  - Simple construction of custom "up to" methods
- Isabelle's coinduction proof method
  - Structured coinductive proofs
  - Integration of "up to" methods via custom coinduction rules
- Higher-order abstract syntax
  - Less dealing with boring technicalities in proofs

Follow the development

- https://github.com/input-output-hk/equivalence-reasoner
- https://github.com/input-output-hk/transition-systems
- https://github.com/input-output-hk/thorn-calculus
- https://github.com/input-output-hk/network-equivalences