#### A Fault Tolerance Bisimulation Proof for Consensus

#### Adrian Francalanza<sup>1</sup> Matthew Hennessy<sup>2</sup>

<sup>1</sup>Department of Computing Imperial College

<sup>2</sup>Department of Informatics University of Sussex

#### European Symposium on Programming, 2007

Adrian Francalanza, Matthew Hennessy

< 미 > < ( ) > < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) < ( ) <

#### Outline



#### 2 Methodology



Adrian Francalanza, Matthew Hennessy

versities of Somewhere and Elsewhere

#### Outline



2 Methodology



Adrian Francalanza, Matthew Hennessy



Universities of Somewhere and Elsewhere

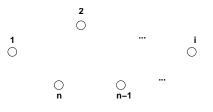
#### Distributed Systems: Consensus

#### Consensus Setting

- n autonomous participants who may independently fail
- hold a value  $v \in V$ .
- must decide on a value  $v' \in V$ .

#### Defining Correctness of Consensus

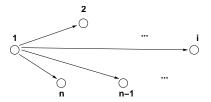
Termination: All non-failing participants must eventually decide. Agreement: No two participants decide on different values. Validity: If all participants are given the same value  $v \in V$  as input, then v is the only possible decision value.



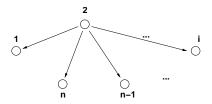
Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

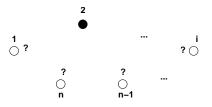


Adrian Francalanza, Matthew Hennessy



Adrian Francalanza, Matthew Hennessy

<日> <目> <目> <目> <日> <</li>
 <日> <</li>

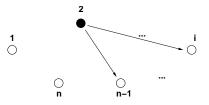


#### Problems caused by Failure

Decision Blocking: a participant waiting forever for a value to be broadcast from a crashed co-ordinator

Adrian Francalanza, Matthew Hennessy

Universities of Somewhere and Elsewhere



#### Problems caused by Failure

Decision Blocking: a participant waiting forever for a value to be broadcast from a crashed co-ordinator

Corrupted Broadcast: a co-ordinator broadcasts its values to a *subset* of the participants before crashing.

Adrian Francalanza, Matthew Hennessy

(ロ) (同) (三) (三) (三) (二) (○) (○)

# Distributed Systems: Consensus with Perfect Failure Detection

Rotating Coordinator Algorithm for Participant i

```
part[1..n]; \\ array of n participants
x_i := input; \\ initialise
for r := 1 to n do {
    if (r = i) then broadcast(x_i);
    if alive(part[r]) then x_i:= input(part[r]);
}
output x_i; \\ decide
```

Adrian Francalanza, Matthew Hennessy

# Distributed Systems: Consensus with Perfect Failure Detection

Rotating Coordinator Algorithm for Participant i

```
part[1..n]; \\ array of n participants
x_i := input; \\ initialise
for r := 1 to n do {
    if (r = i) then broadcast(x_i);
    if alive(part[r]) then x_i:= input(part[r]);
}
output x_i; \\ decide
```

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

Universities of Somewhere and Elsewhere

(ロ) (同) (三) (三) (三) (二) (○) (○)

# Distributed Systems: Consensus with Perfect Failure Detection

Rotating Coordinator Algorithm for Participant i

```
part[1..n]; \\ array of n participants
x_i := input; \\ initialise
for r := 1 to n do {
    if (r = i) then broadcast(x_i);
    if alive(part[r]) then x_i:= input(part[r]);
}
output x_i; \\ decide
```

Adrian Francalanza, Matthew Hennessy

# Distributed Systems: Consensus with Perfect Failure Detection

Rotating Coordinator Algorithm for Participant i

```
part[1..n]; \\ array of n participants
x_i := input; \\ initialise
for r := 1 to n do {
    if (r = i) then broadcast(x_i);
    if alive(part[r]) then x_i:= input(part[r]);
}
output x_i; \\ decide
```

Adrian Francalanza, Matthew Hennessy

・ロト・日本・エート・エート シック

Universities of Somewhere and Elsewhere

#### The Process Calculi Way

## Language: Parallel composition, atomic actions, action hiding, reduction semantics

Bisimulation: Its and  $\approx$  characterises behavioural equivalence

Adrian Francalanza, Matthew Hennessy

もしゃ Alist Alist Alist Alists Ality Al

Universities of Somewhere and Elsewhere

#### The Process Calculi Way

## Language: Parallel composition, atomic actions, action hiding, reduction semantics

Bisimulation: Its and  $\approx$  characterises behavioural equivalence

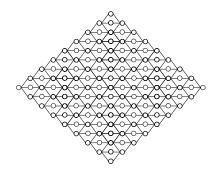
Theorem

#### $P | P | \dots | P \approx SPEC$

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

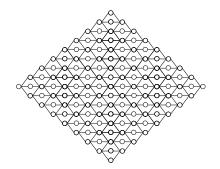
#### The Process Calculi Way (2)



Adrian Francalanza, Matthew Hennessy

<ロ> <四> <四> <日> <日> <日> <日> <日> <日> <日</p>

#### The Process Calculi Way (2)



- complex to understand
- hard to digest
- not intuitive

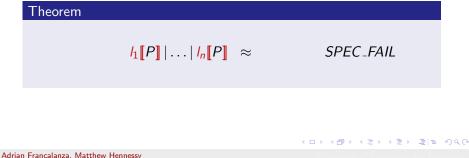
## Language: Parallel composition, atomic actions, action hiding, reduction semantics with failures.

Bisimulation: Its and  $\approx$  characterises behavioural equivalence

# Theorem $l_1[\![P]\!] | \dots | l_n[\![P]\!] \approx$ SPEC\_FAIL Adrian Francalanza, Matthew Hennessy

## Language: Parallel composition, atomic actions, action hiding, reduction semantics with failures.

Bisimulation: Its and  $\approx$  characterises behavioural equivalence



Language: Parallel composition, atomic actions, action hiding, reduction semantics with failures.

$$\overline{(\Gamma, n+1)} \triangleright M \xrightarrow{\tau} (\Gamma - I, n) \triangleright M$$
  $\Gamma \vdash I : alive$ 

Bisimulation: Its and  $\approx$  characterises behavioural equivalence

#### Theorem

 $\Gamma, n-1 \triangleright I_1\llbracket P \rrbracket | \dots | I_n\llbracket P \rrbracket \approx \Gamma, n-1 \triangleright SPEC\_FAIL$ 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

**Jniversities of Somewhere and Elsewhere** 

Expressing Participant i in our process calculus

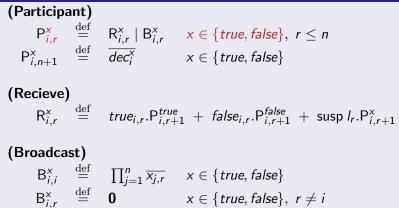
#### (Recieve)

$$\mathsf{R}^{\mathsf{x}}_{i,r} \stackrel{\text{def}}{=} true_{i,r}.\mathsf{P}^{true}_{i,r+1} + false_{i,r}.\mathsf{P}^{false}_{i,r+1} + susp \mathit{I}_r.\mathsf{P}^{\mathsf{x}}_{i,r+1}$$

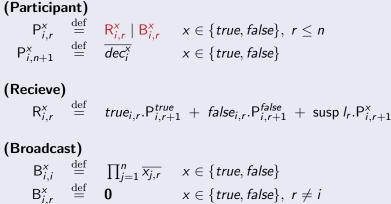
(Broadcast)  

$$\begin{array}{rcl} \mathsf{B}_{i,i}^{x} & \stackrel{\mathrm{def}}{=} & \prod_{j=1}^{n} \overline{x_{j,r}} & x \in \{\textit{true}, \textit{false}\} \\ \mathsf{B}_{i,r}^{x} & \stackrel{\mathrm{def}}{=} & \mathbf{0} & x \in \{\textit{true}, \textit{false}\}, \ r \neq r \end{array}$$









$$x \in \{ true, false \}, r \neq i$$

Expressing Participant *i* in our process calculus

$$\begin{array}{ll} \left( \begin{array}{ccc} \textbf{Participant} \right) \\ P_{i,r}^{x} & \stackrel{\text{def}}{=} & \mathsf{R}_{i,r}^{x} \mid \mathsf{B}_{i,r}^{x} & x \in \{\textit{true},\textit{false}\}, \ r \leq n \\ P_{i,n+1}^{x} & \stackrel{\text{def}}{=} & \overline{\textit{dec}_{i}^{x}} & x \in \{\textit{true},\textit{false}\} \end{array} \end{array}$$

#### (Recieve)

$$\mathsf{R}^{\mathsf{x}}_{i,r} \stackrel{\text{def}}{=} true_{i,r}.\mathsf{P}^{true}_{i,r+1} + false_{i,r}.\mathsf{P}^{false}_{i,r+1} + susp \mathit{I}_r.\mathsf{P}^{\mathsf{x}}_{i,r+1}$$

(Broadcast)  

$$\begin{array}{cccc}
 B_{i,i}^{x} & \stackrel{\text{def}}{=} & \prod_{j=1}^{n} \overline{x_{j,r}} & x \in \{\text{true}, \text{false}\} \\
 B_{i,r}^{x} & \stackrel{\text{def}}{=} & \mathbf{0} & x \in \{\text{true}, \text{false}\}, \ r \neq i \end{array}$$

Adrian Francalanza, Matthew Hennessy

Expressing Participant *i* in our process calculus

$$\begin{array}{rcl} \mathsf{B}_{i,i}^{\mathsf{x}} & \stackrel{\mathrm{def}}{=} & \prod_{j=1}^{n} \overline{\mathsf{x}_{j,r}} & \mathsf{x} \in \{ \textit{true}, \textit{false} \} \\ \mathsf{B}_{i,r}^{\mathsf{x}} & \stackrel{\mathrm{def}}{=} & \mathbf{0} & \mathsf{x} \in \{ \textit{true}, \textit{false} \}, \ r \neq i \end{array}$$

Expressing Participant *i* in our process calculus

(Participant)  $P_{i,r}^{x} \stackrel{\text{def}}{=} R_{i,r}^{x} | B_{i,r}^{x} \quad x \in \{true, false\}, r \leq n$   $P_{i,n+1}^{x} \stackrel{\text{def}}{=} \frac{dec_{i}^{x}}{dec_{i}^{x}} \quad x \in \{true, false\}$ (Recieve)  $R_{i,r}^{x} \stackrel{\text{def}}{=} true_{i,r} \cdot P_{i,r+1}^{true} + false_{i,r} \cdot P_{i,r+1}^{false} + susp I_{r} \cdot P_{i,r+1}^{x}$ (Broadcast)

$$\begin{array}{rcl} \mathsf{B}_{i,i}^{x} & \stackrel{\mathrm{def}}{=} & \prod_{j=1}^{n} \overline{x_{j,r}} & x \in \{ \textit{true}, \textit{false} \} \\ \mathsf{B}_{i,r}^{x} & \stackrel{\mathrm{def}}{=} & \mathbf{0} & x \in \{ \textit{true}, \textit{false} \}, \ r \neq i \end{array}$$

Expressing Participant *i* in our process calculus

(Participant)  

$$P_{i,r}^{x} \stackrel{\text{def}}{=} R_{i,r}^{x} | B_{i,r}^{x} \quad x \in \{true, false\}, r \leq n$$

$$P_{i,n+1}^{x} \stackrel{\text{def}}{=} \overline{dec_{i}^{x}} \quad x \in \{true, false\}$$
(Recieve)  

$$R_{i,n+1}^{x} \stackrel{\text{def}}{=} true; P_{i,n+1}^{true} + false; P_{i,n+1}^{false} + susp l_{n} P_{i,n+1}^{x}$$

$$R_{i,r}^{\mathsf{x}} \stackrel{\text{def}}{=} true_{i,r} \cdot P_{i,r+1}^{true} + false_{i,r} \cdot P_{i,r+1}^{false} + susp l_r \cdot P_{i,r+1}^{\mathsf{x}}$$
(Broadcast)
$$B_{i,i}^{\mathsf{x}} \stackrel{\text{def}}{=} \prod_{i=1}^{n} \overline{x_{i,r}} \quad \mathsf{x} \in \{true, false\}$$

$$x \in \{$$
true, false $\}, r \neq i$ 

Adrian Francalanza, Matthew Hennessy

 $B_{i,r}^{x}$ 

A Fault Tolerance Bisimulation Proof for Consensus

 $\stackrel{\text{def}}{=}$ 

0

#### Composing n Participants to solve Consensus

$$\mathsf{C} \stackrel{\text{def}}{=} \left( \nu_{i,r=1}^{n} \frac{true_{i,r}}{false_{i,r}} \right) \prod_{i=1}^{n} I_{i} \left[ \left[ \begin{array}{c} prop_{i}^{true}.\mathsf{P}_{i,1}^{true} \\ +prop_{i}^{false}.\mathsf{P}_{i,1}^{false} \end{array} \right] \right]$$

Adrian Francalanza, Matthew Hennessy

きょう しん 二川 ふんかく 山や ふしゃ

Universities of Somewhere and Elsewhere

#### Composing n Participants to solve Consensus

$$\mathsf{C} \stackrel{\text{def}}{=} \left( \nu_{i,r=1}^{n} \frac{true_{i,r}}{false_{i,r}} \right) \prod_{i=1}^{n} l_{i} \left[ \left[ \begin{array}{c} prop_{i}^{true}.\mathsf{P}_{i,1}^{true} \\ +prop_{i}^{false}.\mathsf{P}_{i,1}^{false} \end{array} \right] \right]$$

Adrian Francalanza, Matthew Hennessy

もって 正正 ヘル・ヘル・ヘリ・

Universities of Somewhere and Elsewhere

#### Composing n Participants to solve Consensus

$$\mathsf{C} \stackrel{\text{def}}{=} \left( \nu_{i,r=1}^{n} \frac{true_{i,r}}{false_{i,r}} \right) \prod_{i=1}^{n} I_{i} \left[ \left[ \begin{array}{c} prop_{i}^{true}.\mathsf{P}_{i,1}^{true} \\ +prop_{i}^{false}.\mathsf{P}_{i,1}^{false} \end{array} \right] \right]$$

Adrian Francalanza, Matthew Hennessy

きょう しん 二川 ふんかく 山や ふしゃ

Universities of Somewhere and Elsewhere

#### Composing n Participants to solve Consensus

$$\mathsf{C} \stackrel{\text{def}}{=} \left( \nu_{i,r=1}^{n} \frac{true_{i,r}}{false_{i,r}} \right) \prod_{i=1}^{n} I_{i} \left[ \left[ \begin{array}{c} prop_{i}^{true}.\mathsf{P}_{i,1}^{true} \\ +prop_{i}^{false}.\mathsf{P}_{i,1}^{false} \end{array} \right] \right]$$

Adrian Francalanza, Matthew Hennessy

きょう しん 二川 ふんかく 山や ふしゃ

Universities of Somewhere and Elsewhere

#### Composing n Participants to solve Consensus

$$\mathsf{C} \stackrel{\text{def}}{=} \left( \mathcal{V}_{i,r=1}^{n} \frac{true_{i,r}}{false_{i,r}} \right) \prod_{i=1}^{n} I_{i} \left[ \left[ \begin{array}{c} prop_{i}^{true}.\mathsf{P}_{i,1}^{true} \\ +prop_{i}^{false}.\mathsf{P}_{i,1}^{false} \end{array} \right] \right]$$

#### Specification in the presence of Failure

#### VERY COMPLEX!

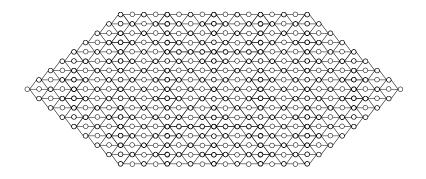
Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

◆□▶ ◆圖▶ ◆圖▶ ★国▶ ●目 めるの

Universities of Somewhere and Elsewhere

#### Bisimulation with Failure



An even bigger, more complex bisimulation!

Adrian Francalanza, Matthew Hennessy

きょう しん 二川 ふんかく 山や ふしゃ

Universities of Somewhere and Elsewhere

#### Outline



#### 2 Methodology



Adrian Francalanza, Matthew Hennessy

Universities of Somewhere and Elsewhere

#### Methodology (1): Testing Harnesses

#### Language: Parallel composition, atomic actions, action hiding, reduction semantics w. failures, immortal location $\star$ . Bisimulation: Its and $\approx$ characterises behavioural equivalence w.r.t immortal observers

#### Theorem

#### $\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket Q \rrbracket | l_1 \llbracket P \rrbracket | \dots | l_n \llbracket P \rrbracket) \approx \Gamma, 0 \triangleright \star \llbracket SPEC \rrbracket$

Adrian Francalanza, Matthew Hennessy

<ロト < 回 > < 目 > < 三 > < 三 > < 三 > の Q @ Universities of Somewhere and Elsewhere

#### Methodology (1): Testing Harnesses

Bisimulation: ...

#### Theorem

$$\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket Q \rrbracket | l_1 \llbracket P \rrbracket | \dots | l_n \llbracket P \rrbracket) \approx \Gamma, 0 \triangleright \star \llbracket SPEC \rrbracket$$

#### Advantages

- **1** Simplifies specification formulation
- 2 Permits separate tests for correctness criteria

Adrian Francalanza, Matthew Hennessy

### Methodology (1): Testing Harnesses

Harnesses For Consensus(Initialisation)IXdefstart. 
$$\prod_{i=1}^{n} \overline{prop_i^{X}}$$
 $x \in \{true, false\}$ Igendefstart.  $\prod_{i=1}^{n} (\overline{prop_i^{true}} + \overline{prop_i^{false}})$  $x \in \{true, false\}$ (Agreement) $A_i^{X}$ def $dec_i^{X}.A_{i+1}^{X} + susp I_i.A_{i+1}^{X}$  $x \in \{true, false\}$  $A_{i+1}^{x}$  $\stackrel{def}{=}$  $ok$  $x \in \{true, false\}$  $A_i^{gen}$  $\stackrel{def}{=}$  $ok$  $x \in \{true, false\}$  $A_i^{gen}$  $\stackrel{def}{=}$  $dec_i^{true}.A_{i+1}^{true} + dec_i^{false}.A_{i+1}^{false} + susp I_i.A_{i+1}^{gen}$ 

Adrian Francalanza, Matthew Hennessy

<ロ> < 四> < 图> < 문> < 문) < 문) 된 1 の Q () Universities of Somewhere and Elsewhere

### Methodology (1): Testing Harnesses

```
Language: ....
Bisimulation: ....
```

Theorem

Agreement and Termination  $\Gamma, n-1 \triangleright (\nu \tilde{m}) (\star \llbracket J^{gen} \mid A_1^{gen} \rrbracket \mid C) \approx \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket$ 

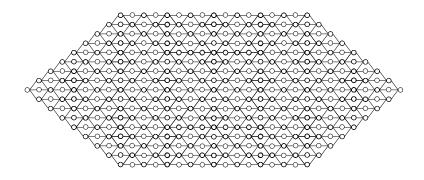
#### Validity

 $\begin{array}{ll} \Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I^{true} \mid A_1^{true} \rrbracket \mid C) &\approx & \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket \\ \Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I^{false} \mid A_1^{false} \rrbracket \mid C) &\approx & \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket \end{array}$ 

 $\tilde{m} = \prod_{i=1}^{n} prop_{i}^{true}, \ prop_{i}^{false}, \ dec_{i}^{true}, \ dec_{i}^{false}$ 

Adrian Francalanza, Matthew Hennessy

### Methodology (1): ... on the bisimulation front

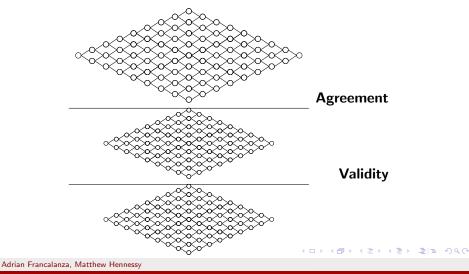


Where we left off... (big, complex bisimulation!)

Adrian Francalanza, Matthew Hennessy

◆ロ> < 個> < 目> < 目> < 回> < 回</li>

## Methodology (1): ... on the bisimulation front



Theorem

### $\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I | A \rrbracket | C) \approx \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket$

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

きょう きょう かんしゃ ふしゃ ふしゃ

Universities of Somewhere and Elsewhere

#### Language: .... Bisimulation: ....

#### Theorem

$$\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I | A \rrbracket) = C \qquad ) \approx \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket$$

Induce failure

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

Language: .... Bisimulation: ....

#### Theorem



Adrian Francalanza, Matthew Hennessy

◆□ → < 団 → < 注 → < 注 → 注 □ → のへの Universities of Somewhere and Elsewhere

Language: ... Bisimulation: ...

Theorem

### $[\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I | A \rrbracket | C) \approx [\Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket$

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

うせん 正則 スポッスポッス ライ

Universities of Somewhere and Elsewhe

Language: ...

Bisimulation: ...

#### Theore<u>m</u>

#### Basic Correctness $\Gamma, \mathbf{0} \triangleright (\nu \tilde{m}) (\star \llbracket l | A \rrbracket | C) \approx \Gamma, \mathbf{0} \triangleright \star \llbracket start. \overline{ok} \rrbracket$

Adrian Francalanza, Matthew Hennessy

きょう きょう かいしょう ふしゃ ふしゃ

Universities of Somewhere and Elsewhere

Theorem

Basic Correctness  $\Gamma, 0 \triangleright (\nu \tilde{m}) (\star \llbracket I | A \rrbracket | C) \approx \Gamma, 0 \triangleright \star \llbracket start. \overline{ok} \rrbracket$ 

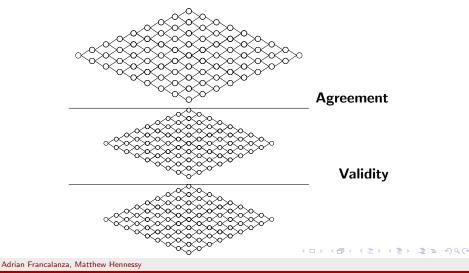
#### **Correctness Preservation** $\Gamma, n-1 \triangleright (\nu \tilde{m})(\star \llbracket I | A \rrbracket | C) \approx \Gamma, 0 \triangleright (\nu \tilde{m})(\star \llbracket I | A \rrbracket | C)$

Adrian Francalanza, Matthew Hennessy

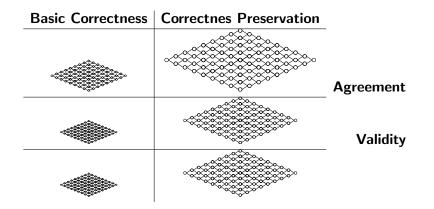
A Fault Tolerance Bisimulation Proof for Consensus

Jniversities of Somewhere and Elsewhere

## Methodology (2): ... on the bisimulation front



Methodology (2): ... on the bisimulation front



Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

# Methodology (2): Advantages

- Natural way how to analyse algorithms in the presence of failure.
- 2 Stages are Independent:
  - Test them in parallel
  - Simpler (failure-free) stage can be used as a vetting stage
- **3 Refined Up-to Techniques**: we have different confluences and structural equivalences under different failure settings.

#### **Confluence** Properties

$$\langle \Gamma, n \rangle \triangleright N \longmapsto_{\beta} \langle \Gamma, n \rangle \triangleright M$$

Adrian Francalanza, Matthew Hennessy

#### **Confluence** Properties

$$\begin{array}{c|c} \langle \Gamma, n \rangle \triangleright N \longmapsto^{\tau}_{\beta} \langle \Gamma, n \rangle \triangleright M \\ \mu \\ \downarrow \\ \langle \Gamma', n' \rangle \triangleright N' \end{array}$$

Adrian Francalanza, Matthew Hennessy

ののの 単同 (ヨン・(ヨン・(型)) (ロン・(ロン・)

#### **Confluence** Properties

$$\begin{array}{c} \langle \Gamma, n \rangle \triangleright N \longmapsto \tau \\ \downarrow \\ \mu \\ \downarrow \\ \langle \Gamma', n' \rangle \triangleright N' \longmapsto \tau \\ \beta \\ \langle \Gamma', n' \rangle \triangleright M' \longmapsto \tau \\ \beta \\ \langle \Gamma', n' \rangle \triangleright M' \end{array}$$

Adrian Francalanza, Matthew Hennessy

<ロ> < 回> < 回> < 回> < 回> < 回> < 回> のQの

#### Structural Equivalence Properties

$$\langle \Gamma, n \rangle \triangleright N \equiv \langle \Gamma, n \rangle \triangleright M$$

Adrian Francalanza, Matthew Hennessy

きょう きん しょう きょう きょう ふう

Universities of Somewhere and Elsewhere

#### Structural Equivalence Properties

$$\begin{array}{ll} \langle \Gamma, n \rangle \triangleright N & \equiv & \langle \Gamma, n \rangle \triangleright M \\ & \mu \\ & \downarrow \\ \langle \Gamma', n' \rangle \triangleright N' \end{array}$$

Adrian Francalanza, Matthew Hennessy

< 미 > < ( ) > < ( ) < ( ) < ( ) </li>
 < ( )

#### Structural Equivalence Properties

$$\begin{array}{ccc} \langle \Gamma, n \rangle \triangleright N & \equiv & \langle \Gamma, n \rangle \triangleright M \\ \mu & & \mu \\ \langle \Gamma', n' \rangle \triangleright N' & \equiv & \langle \Gamma', n' \rangle \triangleright M' \end{array}$$

Adrian Francalanza, Matthew Hennessy

◆□> ◆□> ◆三> ◆□> ◆□> ◆□>

Confluence in a Failure-free Setting

 $\Gamma, 0 \triangleright (\nu a) (I\llbracket \overline{a} \rrbracket | k\llbracket a.P \rrbracket)$ 

Adrian Francalanza, Matthew Hennessy

・ロト・西ト・ヨト・ヨト 山口 ろくの

Universities of Somewhere and Elsewhere

Confluence in a Failure-free Setting

$$\Gamma, 0 \triangleright (\nu a) \left( I[\![\overline{a}]\!] \mid k[\![a.P]\!] \right) \xrightarrow{\tau}_{\beta} \Gamma, 0 \triangleright (\nu a) \left( k[\![P]\!] \right)$$

Adrian Francalanza, Matthew Hennessy

きょう きん しょう きょう きょう ふう

Universities of Somewhere and Elsewhere

Confluence in a Failure-free Setting

$$\Gamma, 0 \triangleright (\nu a) \left( I[\![\overline{a}]\!] \mid k[\![a.P]\!] \right) \xrightarrow{\tau}_{\beta} \Gamma, 0 \triangleright (\nu a) \left( k[\![P]\!] \right)$$

Confluence in a Failure Setting

 $\Gamma, n \triangleright (\nu a) \left( I \llbracket \overline{a} \rrbracket \mid k \llbracket a.P + \text{susp } I.P \rrbracket \right)$ 

Adrian Francalanza, Matthew Hennessy

▲□▶▲圖▶▲≣▶▲≣▶ 副目 ろんの

Universities of Somewhere and Elsewhere

Confluence in a Failure-free Setting

$$\Gamma, 0 \triangleright (\nu a) \left( I[\![\overline{a}]\!] \mid k[\![a.P]\!] \right) \xrightarrow{\tau}_{\beta} \Gamma, 0 \triangleright (\nu a) \left( k[\![P]\!] \right)$$

Confluence in a Failure Setting

 $\Gamma, n \triangleright (\nu a) (I\llbracket \overline{a} \rrbracket | k\llbracket a.P + \text{susp } I.P \rrbracket) \xrightarrow{\tau}_{\beta} \Gamma, n \triangleright (\nu a) (k\llbracket P \rrbracket)$ 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

・ロト・(型ト・(ヨト・(型ト・(ロト

Universities of Somewhere and Elsewhere

#### Structural Equivalence in a Failure-free Setting

$$[\Gamma, 0 \triangleright / \llbracket P + \operatorname{susp} k. Q \rrbracket \equiv [\Gamma, 0 \triangleright / \llbracket P \rrbracket \qquad [\Gamma \vdash k : alive$$

Adrian Francalanza, Matthew Hennessy

#### Confluence Within Consensus

$$\Gamma, n \triangleright \left( \nu \quad \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l.R \rrbracket \right)$$

Adrian Francalanza, Matthew Hennessy

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

#### Confluence Within Consensus

$$\Gamma, n \triangleright \left( \nu \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \underbrace{\left( \underbrace{I_j \llbracket true_{i,j} \rrbracket}_{\text{coordinator}} \mid \underbrace{I_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } I_j.R \rrbracket}_{\text{participant}} \right)}_{\text{participant}}$$

Adrian Francalanza, Matthew Hennessy

◆□ → ◆□ → ◆三 → ◆□ → ◆□ → ◆○ → ◆□

#### Confluence Within Consensus

3 Cases

$$\Gamma, n \triangleright \left( \nu \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right)$$

Adrian Francalanza, Matthew Hennessy

・ロ・・聞・・ヨ・・ヨー うへの

#### Confluence Within Consensus

#### Failure Free

$$\Gamma, \mathbf{0} \triangleright \left( \nu \quad \frac{true_{i,j}}{false_{i,j}} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right)$$

Adrian Francalanza, Matthew Hennessy

・ロ・・聞・・ヨ・・ヨー うへの

Universities of Somewhere and Elsewhere

#### Confluence Within Consensus

#### Failure Free

$$\begin{split} & \Gamma, \mathbf{0} \triangleright \left( \nu \quad \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right) \\ & \equiv \quad \left( \nu true_{i,j}, \ false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

▲□▶ ▲圖▶ ▲圖▶ ▲圖▶ 副目 めんの

Universities of Somewhere and Elsewi

#### Confluence Within Consensus

#### Failure Free

$$\begin{split} & \Gamma, \mathbf{0} \triangleright \left( \nu \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right) \\ & \equiv \left( \nu true_{i,j}, false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q \rrbracket \right) \\ & \equiv \left( \nu true_{i,j}, false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

versities of Somewhere and Elsewher

#### Confluence Within Consensus

#### Failure Free

$$\begin{split} & \Gamma, \mathbf{0} \triangleright \left( \nu \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right) \\ & \equiv \left( \nu true_{i,j}, false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q \rrbracket \right) \\ & \equiv \left( \nu true_{i,j}, false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P \rrbracket \right) \\ & \stackrel{\tau}{\longmapsto}_{\beta} \left( \nu true_{i,j}, false_{i,j} \right) \left( l_i \llbracket P \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

#### Confluence Within Consensus

#### Broadcast same as estimate

$$\Gamma, \mathbf{n} \triangleright \left( \nu \quad \frac{true_{i,j}}{false_{i,j}} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \operatorname{susp} l_j.P \rrbracket \right)$$

Adrian Francalanza, Matthew Hennessy

・ロ・・西・・川・・田・ 山下 うへの

Universities of Somewhere and Elsewhere

#### Confluence Within Consensus

#### Broadcast same as estimate

$$\begin{split} & \Gamma, \mathbf{n} \triangleright \left( \nu \quad \frac{true_{i,j}}{false_{i,j}} \right) \left( I_j \llbracket true_{i,j} \rrbracket \mid I_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } I_j.P \rrbracket \right) \\ & \equiv \quad \left( \nu true_{i,j}, \ false_{i,j} \right) \left( I_j \llbracket true_{i,j} \rrbracket \mid I_i \llbracket true_{i,j}.P + \text{susp } I_j.P \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

きょう きん しょう きょう きょう ふう

Universities of Somewhere and Elsewhe

< □ > < □ > < 三 > < 三 > < 三 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

# Methodology (3): Up-to Techniques

#### Confluence Within Consensus

#### Broadcast same as estimate

$$\begin{split} & \Gamma, \mathbf{n} \triangleright \left( \nu \begin{array}{c} true_{i,j}, \\ false_{i,j} \end{array} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.P \rrbracket \right) \\ & \equiv \left( \nu true_{i,j}, false_{i,j} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + \text{susp } l_j.P \rrbracket \right) \\ & \stackrel{\tau}{\longmapsto}_{\beta} \left( \nu true_{i,j}, false_{i,j} \right) \left( l_i \llbracket P \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

#### Confluence Within Consensus

#### Broadcast different from estimate

$$\Gamma, \mathbf{n} \triangleright \left( \nu \quad \frac{true_{i,j}}{false_{i,j}} \right) \left( l_j \llbracket true_{i,j} \rrbracket \mid l_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } l_j.R \rrbracket \right)$$

Adrian Francalanza, Matthew Hennessy

きょう しん 二川 ふんかく 山や ふしゃ

Universities of Somewhere and Elsewhere

#### Confluence Within Consensus

#### Broadcast different from estimate

$$\begin{split} & \Gamma, \mathbf{n} \triangleright \left( \nu \quad \frac{true_{i,j}}{false_{i,j}} \right) \left( I_j \llbracket true_{i,j} \rrbracket \mid I_i \llbracket true_{i,j}.P + false_{i,j}.Q + \text{susp } I_j.R \rrbracket \right) \\ & \equiv \quad \left( \nu true_{i,j}, \ false_{i,j} \right) \left( I_j \llbracket true_{i,j} \rrbracket \mid I_i \llbracket true_{i,j}.P + \text{susp } I_j.Q \rrbracket \right) \end{split}$$

Adrian Francalanza, Matthew Hennessy

もってい 正則 ふかく ふやく きょう

# Methodology (3): Up-to Techniques

#### Why is it worthwhile ...?

 techniques for attaining fault tolerance are bounded and reused in many algorithms.

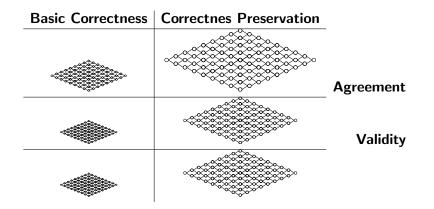
Fault tolerance is attained through replication!
 Space replication: P|P|...|P
 Time replication: P.P...P

Adrian Francalanza, Matthew Hennessy

< 미 > < ( ) > < ( ) < ( ) < ( ) </li>
 < ( )

A Fault Tolerance Bisimulation Proof for Consensus

Methodology (3): ... on the bisimulation front

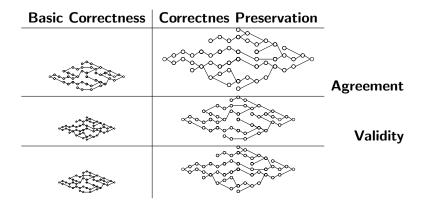


Adrian Francalanza, Matthew Hennessy

< □ > < □ > < 三 > < 三 > < 三 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

A Fault Tolerance Bisimulation Proof for Consensus

## Methodology (3): ... on the bisimulation front



Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

<ロ><団><団><日><日><日><日><日><日><日><日><日><日><100</td>

### Outline



2 Methodology



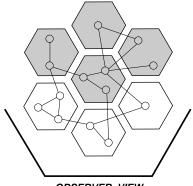
Adrian Francalanza, Matthew Hennessy

Universities of Somewhere and Elsewhere

A Fault Tolerance Bisimulation Proof for Consensus

#### Methodology in 3 acts

- **Testing Harnesses:** Limiting observations to non-failing locations.
- Fault Tolerance: Splitting analysis into basic correctness and correctness preservation phases.
- **Refined Up-to Techniques:** for both failure-free and failure phases.

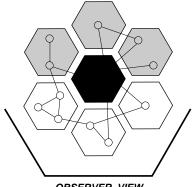


Restrict observation to immortal locations

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus



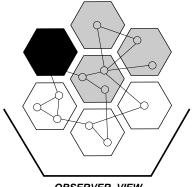
Preserves observation up to 1 failure

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

<ロ> < 四> < 图> < 문> < 문) < 문) 된 1 の Q () Universities of Somewhere and Elsewhere

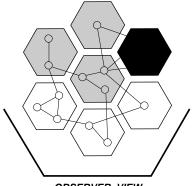


Preserves observation up to 1 failure

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

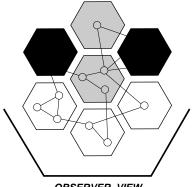


Preserves observation up to 1 failure

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

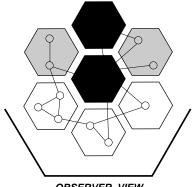


Preserves observation up to 2 failures

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

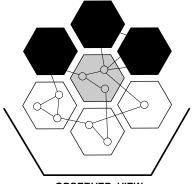


Preserves observation up to 2 failures

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus



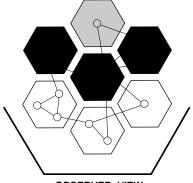
Preserves observation up to 3 failures

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus

<ロ> < 四> < 图> < 문> < 문) < 문) 된 1 の Q () Universities of Somewhere and Elsewhere



Preserves observation up to 3 failures

**OBSERVER VIEW** 

Adrian Francalanza, Matthew Hennessy

A Fault Tolerance Bisimulation Proof for Consensus