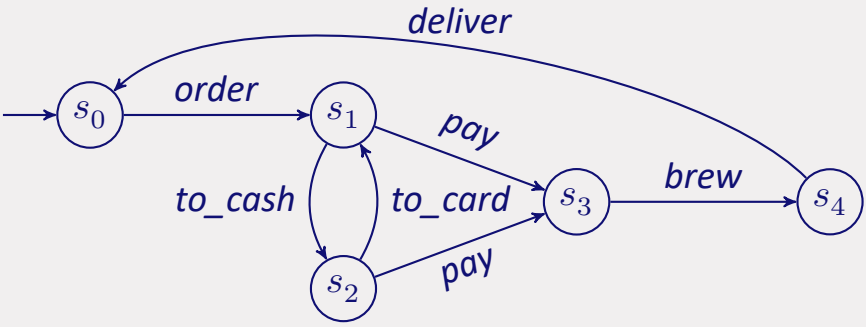
Progress, Justness and Fairness in Modal μ-Calculus Formulae

M.S.C. Spronck, B. Luttik and T.A.C. Willemse

13 September 2024

TU/e

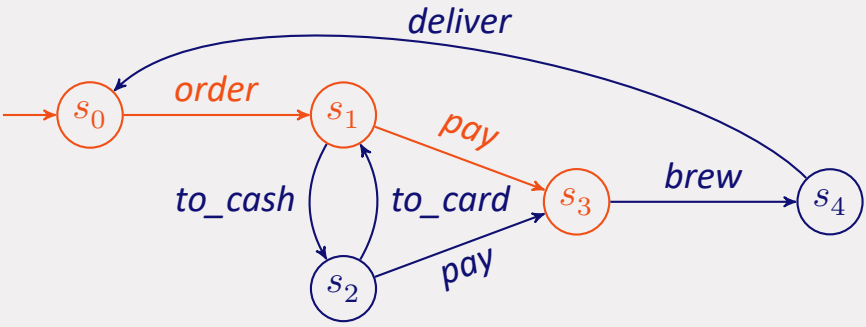
Example



- *Inevitable delivery*: when *order* occurs, inevitably *deliver* will occur

TU/e

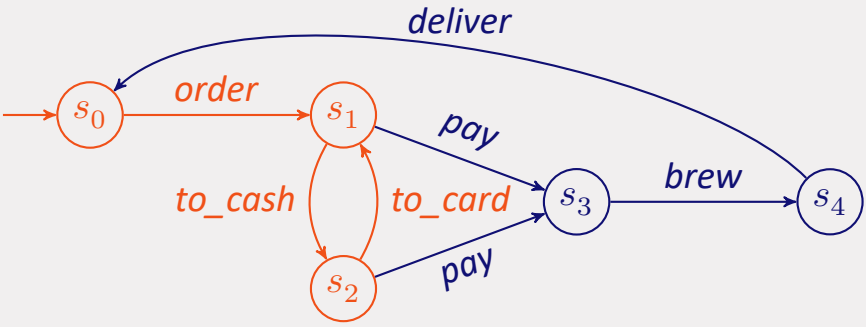
Example



- *Inevitable delivery*: when *order* occurs, inevitably *deliver* will occur

TU/e

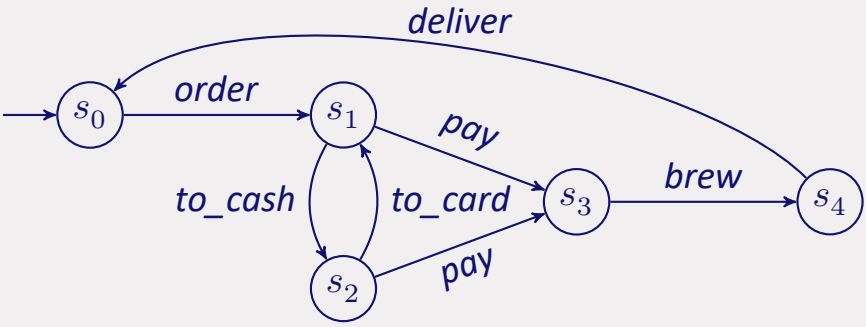
Example



- *Inevitable delivery*: when *order* occurs, inevitably *deliver* will occur

TU/e

Example



- *Inevitable delivery*: when *order* occurs, inevitably *deliver* will occur

TU/e

Problem

- How to restrict verification to “realistic” paths?
- Which paths are “realistic”?

Problem

- How to restrict verification to “realistic” paths?
- Which paths are “realistic”?
  - Already solved!

Problem

- How to restrict verification to “realistic” paths?
- Which paths are “realistic”?
  - Already solved!
- *Completeness criteria*
  - E.g. progress, justness, (weak/strong) fairness

Problem

- How to restrict verification to “realistic” paths?
- Which paths are “realistic”?
  - Already solved!
- *Completeness criteria*
  - E.g. progress, justness, (weak/strong) fairness
- Choose appropriate criterion

Problem

- How to restrict verification to “realistic” paths?
- Which paths are “realistic”?
  - Already solved!
- *Completeness criteria*
  - E.g. progress, justness, (weak/strong) fairness
- Choose appropriate criterion
- How to restrict verification to complete paths?

Solution

- How to restrict verification to complete paths?
- Modify formula representing property

Solution

- How to restrict verification to complete paths?
- Modify formula representing property
- Chosen logic: modal μ-calculus
- Syntax:

$$\phi ::= \mathit{ff} \mid \mathit{tt} \mid X \mid \neg\phi \mid \phi \vee \phi \mid \phi \wedge \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi \mid \mu X.\phi \mid \nu X.\phi$$

Solution

- How to restrict verification to complete paths?
- Modify formula representing property
- Chosen logic: modal μ-calculus
- Syntax:

$$\phi ::= \mathit{ff} \mid \mathit{tt} \mid X \mid \neg\phi \mid \phi \vee \phi \mid \phi \wedge \phi \mid \langle\alpha\rangle\phi \mid [\alpha]\phi \mid \mu X.\phi \mid \nu X.\phi$$

- State-based logic
  - Interweave completeness criterion and property

Designing Formulae

1. Consider multiple properties
    - Single template for many properties
2. Consider multiple completeness criteria
    - Different template formulae for different criteria

Designing Formulae

1. Consider multiple properties
    - Single template for many properties
2. Consider multiple completeness criteria
    - Different template formulae for different criteria
3. Proven correctness

Many Properties

- Dwyer, Avrunin, and Corbett (1999):
  Patterns in property specifications for finite-state verification

Many Properties

- Dwyer, Avrunin, and Corbett (1999):
  Patterns in property specifications for finite-state verification
- Cover subset of patterns
  - 4 behaviours $\times$ 4 scope $=$ 16 patterns
  - Only relevant (liveness) patterns

Template Property

- “A path that violates the property”

Template Property

- "A path that violates the property"
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

Template Property

- "A path that violates the property"
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

TU/e

Template Property

- “A path that violates the property”
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

TU/e

Template Property

- “A path that violates the property”
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

TU/e

Template Property

- “A path that violates the property”
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

TU/e

Template Property

- "A path that violates the property"
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

TU/e

Template Property

- "A path that violates the property"
- A path π is $(\rho, \alpha_f, \alpha_e)$-violating if:

- *Inevitable delivery*: when *order* occurs, inevitably *deliver* will occur
  - $\rho = \mathit{Act}^\star \cdot \mathit{order}$
  - $\alpha_f = \{\mathit{deliver}\}$
  - $\alpha_e = \emptyset$

TU/e

Completeness Criteria

- In presentation:

- In paper:

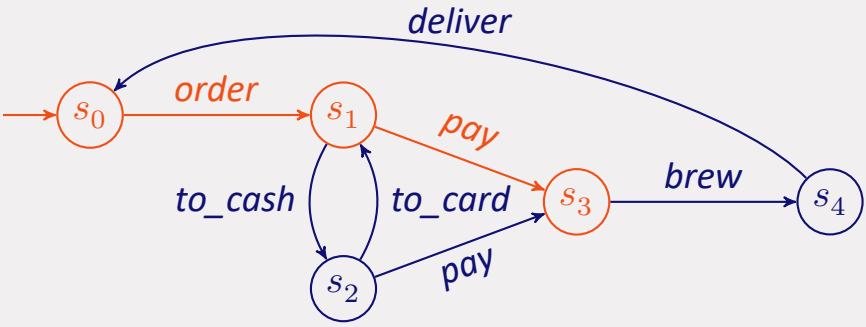
Completeness Criteria

- In presentation:
  - Progress
  - Weak fairness of actions (WFA)
- In paper:

Completeness Criteria

- In presentation:
  - Progress
  - Weak fairness of actions (WFA)
- In paper:
  - Strong fairness of actions (SFA)
  - Justness of actions (JA)
  - Weak hyperfairness of actions (WHFA)
  - Strong hyperfairness of actions (SHFA)

Progress



- Progress: a complete path is infinite or ends in a deadlock

TU/e

Progress Formula

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"

Progress Formula

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

Progress Formula

$$\langle \rho \rangle$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

Progress Formula

$$\langle \rho \rangle \nu X.(\qquad\qquad \langle \overline{\alpha_f} \rangle X)$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

TU/e

Progress Formula

$$\langle \rho \rangle \nu X.(\qquad\qquad \langle \overline{\alpha_f} \rangle X)$$

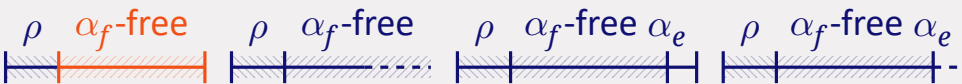
- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

TU/e

Progress Formula

$$\langle \rho \rangle \nu X.(\qquad [Act]ff \vee \langle \overline{\alpha_f} \rangle X)$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:



TU/e

Progress Formula

$$\langle\rho\rangle\nu X.(\langle\alpha_e\rangle tt \vee [Act]ff \vee \langle\overline{\alpha_f}\rangle X)$$

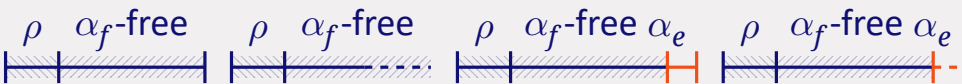
- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

TU/e

Progress Formula

$$\langle\rho\rangle\nu X.(\langle\alpha_e\rangle tt \vee [Act]ff \vee \langle\overline{\alpha_f}\rangle X)$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

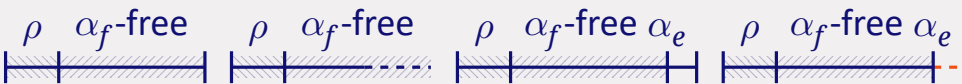


TU/e

Progress Formula

$$\neg\langle\rho\rangle\nu X.(\langle\alpha_e\rangle tt \vee [Act]ff \vee \langle\overline{\alpha_f}\rangle X)$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:



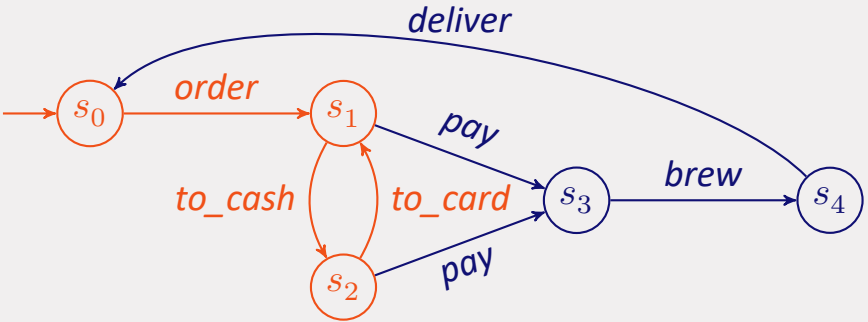
TU/e

Progress Formula

$$\neg\langle\rho\rangle\nu X.(\langle\alpha_e\rangle tt \vee [Act]ff \vee \langle\overline{\alpha_f}\rangle X)$$

- "No path that satisfies progress and is $(\rho, \alpha_f, \alpha_e)$-violating"
- Progress: a complete path is infinite or ends in a deadlock
- $(\rho, \alpha_f, \alpha_e)$-violating:

Weak Fairness of Actions



- WFA: on every suffix of a complete path, every perpetually enabled action occurs
  - Perpetually enabled: enabled in every state

TU/e

Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"

Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"

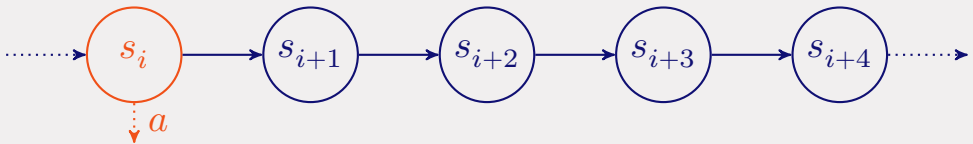
Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs

Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight:

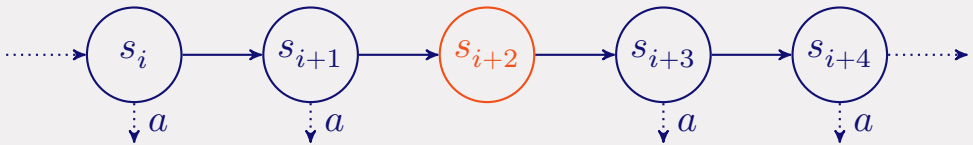
Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...

TU/e

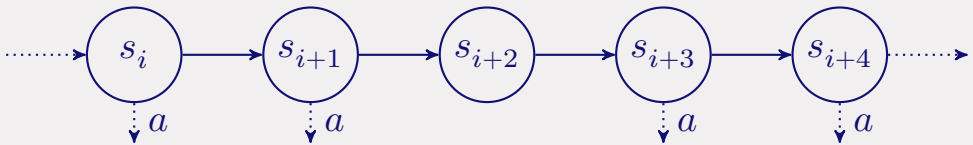
Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...
  - becomes disabled

TU/e

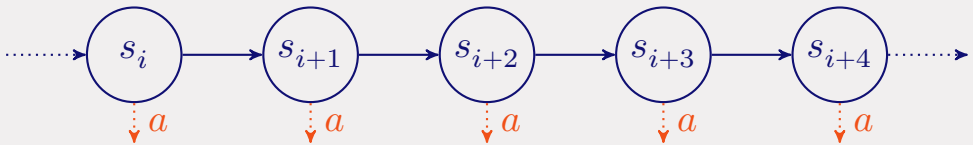
Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...
  - becomes disabled $\Rightarrow$ not perpetually enabled

TU/e

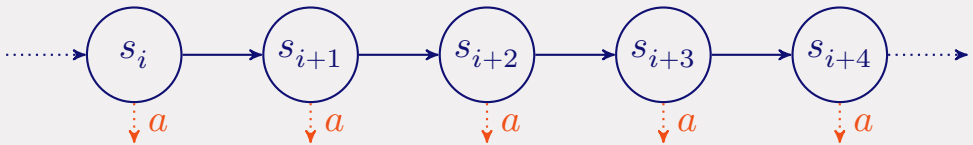
Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...
  - becomes disabled $\Rightarrow$ not perpetually enabled
  - otherwise

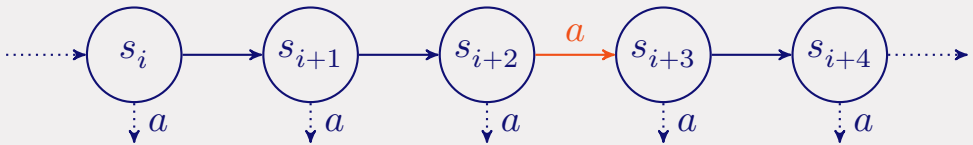
TU/e

Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...
  - becomes disabled $\Rightarrow$ not perpetually enabled
  - otherwise $\Rightarrow$ perpetually enabled

Weak Fairness Formula



- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- Key insight: an action enabled along a WFA path...
  - becomes disabled $\Rightarrow$ not perpetually enabled
  - otherwise $\Rightarrow$ perpetually enabled $\Rightarrow$ must occur

Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \qquad)$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow [a]ff)$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow [a]ff \vee \langle a \rangle tt)$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\quad [a]ff \quad \vee \langle a \quad \rangle tt))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\nu X.(\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\qquad ([a]ff \wedge X) \vee \langle a \qquad \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\nu X.(\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\quad ([a]ff \wedge X) \vee \langle a \quad \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\nu X.(\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\quad ([a]ff \wedge X) \vee \langle a \quad \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\nu X.(\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\qquad\qquad ([a]ff \wedge X) \vee \langle a \qquad \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\nu X.(\bigwedge_{a \in Act} (\langle a \rangle tt \Rightarrow \langle Act^{\star} \rangle (\quad ([a]ff \wedge X) \vee \langle a \quad \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\langle\rho\rangle\nu X.(\bigwedge_{a\in Act}(\langle a\rangle tt \Rightarrow \langle Act^{\star}\rangle(([a]ff \wedge X) \vee \langle a \rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\langle\rho\rangle\nu X.(\bigwedge_{a\in Act}(\langle a\rangle tt \Rightarrow \langle\, \overline{\alpha_f}^{\star}\,\rangle(([a]ff \wedge X) \vee \langle a \setminus \alpha_f\rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\langle\rho\rangle\nu X.(\bigwedge_{a\in Act}(\langle a\rangle tt \Rightarrow\langle\ \overline{\alpha_f}^{\star}\ \rangle(\langle\alpha_e\rangle tt \vee ([a]ff \wedge X) \vee \langle a \setminus \alpha_f\rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\neg\langle\rho\rangle\nu X.(\bigwedge_{a\in Act}(\langle a\rangle tt \Rightarrow\langle\ \overline{\alpha_f}^{\star}\ \rangle(\langle\alpha_e\rangle tt \vee ([a]ff \wedge X) \vee \langle a \setminus \alpha_f\rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Weak Fairness Formula

$$\neg\langle\rho\rangle\nu X.(\bigwedge_{a\in Act}(\langle a\rangle tt \Rightarrow\langle\ \overline{\alpha_f}^{\star}\ \rangle(\langle\alpha_e\rangle tt \vee ([a]ff \wedge X) \vee \langle a \setminus \alpha_f\rangle X)))$$

- "No path that satisfies WFA, progress, and is $(\rho, \alpha_f, \alpha_e)$-violating"
- WFA: on every suffix, every perpetually enabled action occurs
- When an action is enabled, it must eventually be disabled or occur

Strong Fairness, Briefly

- “If infinitely often enabled, occur infinitely often”
- Formula:

$$\neg\langle \rho \cdot \overline{\alpha_f}^{\star} \rangle (\langle \alpha_e \rangle tt \vee [Act]ff \vee \bigvee_{\emptyset \neq F \subseteq Act} \nu X.(\bigwedge_{a \in F} \mu W.([\overline{F}]ff \wedge (\langle a \setminus \alpha_f \rangle X \vee \langle \overline{\alpha_f} \rangle W))))$$

Strong Fairness, Briefly

- “If infinitely often enabled, occur infinitely often”
- Formula:

$$\neg\langle \rho \cdot \overline{\alpha_f}^{\star} \rangle (\langle \alpha_e \rangle \mathit{tt} \vee [\mathit{Act}]\mathit{ff} \vee \bigvee_{\emptyset \neq F \subseteq \mathit{Act}} \nu X.(\bigwedge_{a \in F} \mu W.([\overline{F}]\mathit{ff} \wedge (\langle a \setminus \alpha_f \rangle X \vee \langle \overline{\alpha_f} \rangle W))))$$

- Dividing actions into two sets
  - Exponential

Contributions

- Definition of $(\rho, \alpha_f, \alpha_e)$-violating paths
- Template formulae for multiple completeness criteria
  - Progress
  - Weak fairness of actions
  - Strong fairness of actions
  - Justness of actions
  - Weak hyperfairness of actions
  - Strong hyperfairness of actions
- With blocking actions
- Characterisation of finitely realisable path predicates
- Correctness proofs

Future Work

- Formalisation of proofs
- More completeness criteria and more properties
  - E.g. fairness over sets of actions, state properties
- Verifications with formulae