

2IW05 – Software Specification

Modal Logic - Part III

Mohammad Mousavi

Formal Systems Analysis (FSA)
Model-Driven Software Engineering
Department of Computer Science
TU/Eindhoven

December 20, 2011

- Comments for the first deliverable (those submitted on time and on paper) are available both from Peach and from the web page.
- Comments for the deliverables handed in after the deadline or only electronically will be available soon.
- If you have questions or would like to discuss the comments contact Jerry den Hartog j.d.hartog@tue.nl.

Outline

- 1 Blocks of equations
- 2 Alternation-free modal μ -calculus
- 3 Regular alternation-free modal μ -calculus
- 4 Typical properties

Blocks of equations

Multiple recursion variables: X_1, X_2, \dots

$$\begin{array}{l} X_1 \stackrel{\min}{=} F_1(X_1, X_2, \dots, X_n) \\ X_2 \stackrel{\min}{=} F_2(X_1, X_2, \dots, X_n) \\ \vdots \\ X_n \stackrel{\min}{=} F_n(X_1, X_2, \dots, X_n) \end{array}$$

or

$$\begin{array}{l} X_1 \stackrel{\max}{=} F_1(X_1, X_2, \dots, X_n) \\ X_2 \stackrel{\max}{=} F_2(X_1, X_2, \dots, X_n) \\ \vdots \\ X_n \stackrel{\max}{=} F_n(X_1, X_2, \dots, X_n) \end{array}$$

where $F_i(X_1, X_2, \dots, X_n)$ is a formula generated by

$$F ::= \text{true} \mid \text{false} \mid F \wedge F \mid F \vee F \mid \langle a \rangle F \mid [a] F \mid X_1 \mid X_2 \mid \dots \mid X_n$$

- A variable may depend on another variable

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

- A variable may depend on another variable

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$X \stackrel{\text{max}}{=} [enter]Y \wedge [Act]X \quad Y \stackrel{\text{max}}{=} [enter]false \wedge [Act \setminus leave]Y$$

- A variable may depend on another variable

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$X \stackrel{\text{max}}{=} [enter]Y \wedge [Act]X \quad Y \stackrel{\text{max}}{=} [enter]false \wedge [Act \setminus leave]Y$$

- After each *a* action, another *a* can be done.

- A variable may depend on another variable

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$X \stackrel{\text{max}}{=} [enter]Y \wedge [Act]X \quad Y \stackrel{\text{max}}{=} [enter]false \wedge [Act \setminus leave]Y$$

- After each *a* action, another *a* can be done.

$$X \stackrel{\text{max}}{=} [a]Y \quad Y \stackrel{\text{max}}{=} \langle a \rangle X$$

Variables may even depend on each other cyclicly

Semantics of a block

$$D \equiv \begin{array}{l} X_1 \equiv F_1 \\ X_2 \equiv F_2 \\ \vdots \\ X_n \equiv F_n \end{array}$$

where all equations are least fixed point equations or all equations are greatest fixed point equations

Semantics of a block

$$D \equiv \begin{array}{l} X_1 \equiv F_1 \\ X_2 \equiv F_2 \\ \vdots \\ X_n \equiv F_n \end{array}$$

where all equations are least fixed point equations or all equations are greatest fixed point equations

- semantics associates a set of states to each recursion variable

Semantics of a block

$$D \equiv \begin{array}{l} X_1 \equiv F_1 \\ X_2 \equiv F_2 \\ \vdots \\ X_n \equiv F_n \end{array}$$

where all equations are least fixed point equations or all equations are greatest fixed point equations

- semantics associates a set of states to each recursion variable
- $\mathcal{D} = (2^S)^n$

- Define $O_F : \mathcal{D} \rightarrow 2^S$ such that $O_F(S_1, \dots, S_n)$ is the set of states for which formula F holds under the assumption that X_i holds precisely in the states from S_i

$$O_{X_i}(S_1, \dots, S_n) = S_i$$

$$O_{true}(S_1, \dots, S_n) = S$$

$$O_{false}(S_1, \dots, S_n) = \emptyset$$

$$O_{F_1 \wedge F_2}(S_1, \dots, S_n) = O_{F_1}(S_1, \dots, S_n) \cap O_{F_2}(S_1, \dots, S_n)$$

$$O_{F_1 \vee F_2}(S_1, \dots, S_n) = O_{F_1}(S_1, \dots, S_n) \cup O_{F_2}(S_1, \dots, S_n)$$

$$O_{\langle a \rangle F}(S_1, \dots, S_n) = \langle \cdot a \cdot \rangle O_F(S_1, \dots, S_n)$$

$$O_{[a]F}(S_1, \dots, S_n) = [\cdot a \cdot] O_F(S_1, \dots, S_n)$$

Computing the semantics (minimal fixed point)

$$\begin{aligned} X_1 &\stackrel{\min}{=} F_1(X_1, X_2, \dots, X_n) \\ X_2 &\stackrel{\min}{=} F_2(X_1, X_2, \dots, X_n) \\ &\vdots \\ X_n &\stackrel{\min}{=} F_n(X_1, X_2, \dots, X_n) \end{aligned}$$

Define $\llbracket D \rrbracket : \mathcal{D} \rightarrow \mathcal{D}$

$$\llbracket D \rrbracket (S_1, \dots, S_n) = (O_{F_1}(S_1, \dots, S_n), \dots, O_{F_n}(S_1, \dots, S_n))$$

There exists a natural number $m > 0$ such that

$$\llbracket X_1, \dots, X_n \rrbracket = \llbracket D \rrbracket^m(\emptyset, \dots, \emptyset)$$

Computing the semantics (maximal fixed point)

Let S be a finite set.

$$\begin{aligned} X_1 &\stackrel{\text{max}}{=} F_1(X_1, X_2, \dots, X_n) \\ X_2 &\stackrel{\text{max}}{=} F_2(X_1, X_2, \dots, X_n) \\ &\vdots \\ X_n &\stackrel{\text{max}}{=} F_n(X_1, X_2, \dots, X_n) \end{aligned}$$

There exist a natural number $M > 0$ such that

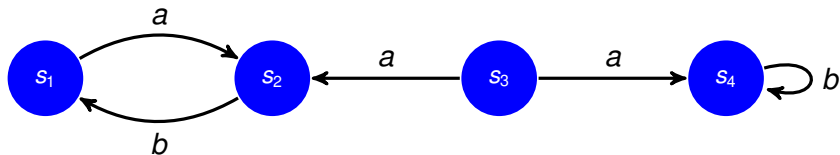
$$\llbracket X_1, \dots, X_n \rrbracket = \llbracket D \rrbracket^M(S, \dots, S)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\text{max}}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\text{max}}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system

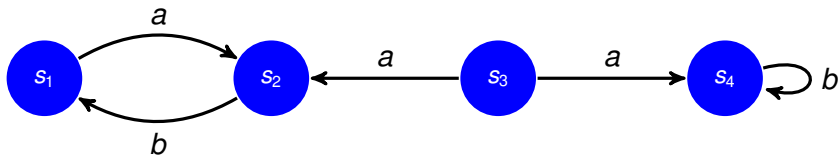


Example

Consider the system of greatest fixed point equations

$$X \stackrel{\text{max}}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\text{max}}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



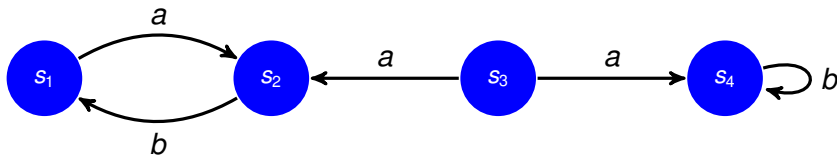
$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\text{max}}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\text{max}}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

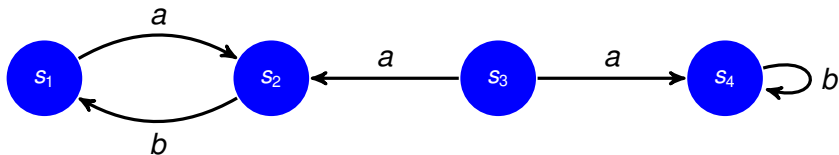
$$\left(\begin{array}{c} S \\ S \end{array} \right)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\text{max}}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\text{max}}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

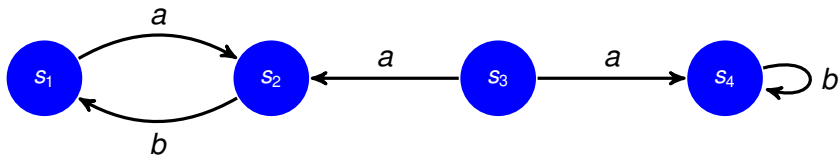
$$\left(\begin{array}{c} S \\ S \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2, s_4\} \end{array} \right)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

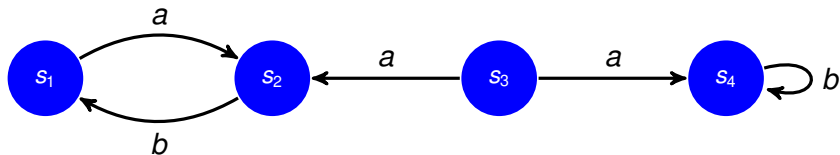
$$\left(\begin{array}{c} S \\ S \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2, s_4\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2\} \end{array} \right)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

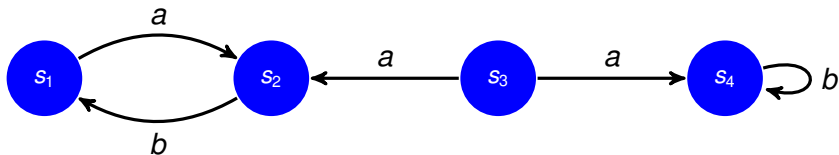
$$\left(\begin{array}{c} S \\ S \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2, s_4\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1\} \\ \{s_2\} \end{array} \right)$$

Example

Consider the system of greatest fixed point equations

$$X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false} \quad Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$$

and determine for which states the formulas X and Y are valid in the labeled transition system



$$\left(\begin{array}{c} S_1 \\ S_2 \end{array} \right) \mapsto \left(\begin{array}{c} \langle \cdot a \cdot \rangle S_2 \cap [\cdot a \cdot] S_2 \cap \{s_1, s_3\} \\ \langle \cdot b \cdot \rangle S_1 \cap [\cdot b \cdot] S_1 \cap \{s_2, s_4\} \end{array} \right)$$

$$\left(\begin{array}{c} S \\ S \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2, s_4\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1, s_3\} \\ \{s_2\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1\} \\ \{s_2\} \end{array} \right) \mapsto \left(\begin{array}{c} \{s_1\} \\ \{s_2\} \end{array} \right)$$

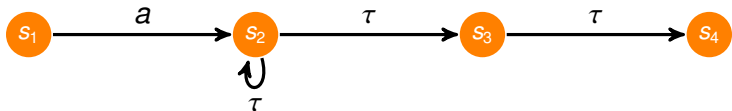
Outline

- 1 Blocks of equations
- 2 Alternation-free modal μ -calculus**
- 3 Regular alternation-free modal μ -calculus
- 4 Typical properties

Example: It is possible to reach a state which has an infinite trace of τ actions (a livelock).

$$X \stackrel{\min}{=} Y \vee \langle Act \rangle X \quad Y \stackrel{\max}{=} \langle \tau \rangle Y$$

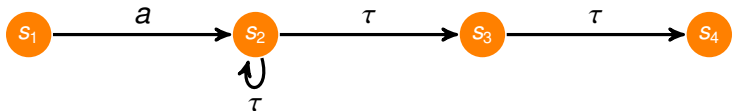
Consider the following labeled transition system:



Example: It is possible to reach a state which has an infinite trace of τ actions (a livelock).

$$X \stackrel{\min}{=} Y \vee \langle Act \rangle X \quad Y \stackrel{\max}{=} \langle \tau \rangle Y$$

Consider the following labeled transition system:

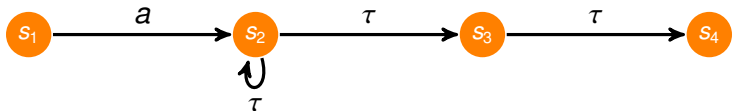


Solution for Y is independent of solution for X and it is the greatest fixed point of the equation $S_Y = \langle \tau \cdot \tau \rangle S_Y$.

Example: It is possible to reach a state which has an infinite trace of τ actions (a livelock).

$$X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X \quad Y \stackrel{\max}{=} \langle \tau \rangle Y$$

Consider the following labeled transition system:



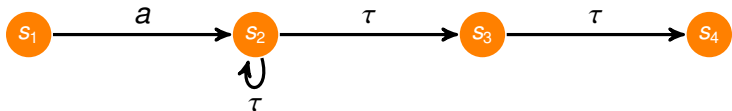
Solution for Y is independent of solution for X and it is the greatest fixed point of the equation $S_Y = \langle \tau \cdot \tau \rangle S_Y$.

Solution for Y is $\{s_2\}$.

Example: It is possible to reach a state which has an infinite trace of τ actions (a livelock).

$$X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X \quad Y \stackrel{\max}{=} \langle \tau \rangle Y$$

Consider the following labeled transition system:



Solution for Y is independent of solution for X and it is the greatest fixed point of the equation $S_Y = \langle \tau \cdot \rangle S_Y$.

Solution for Y is $\{s_2\}$.

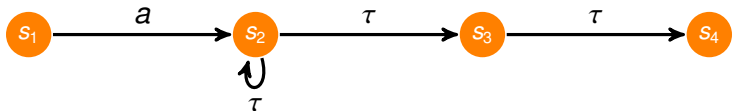
The solution for X is also easily computed to be the least fixed point of the equation $S_X = S_Y \cup \langle \text{Act} \cdot \rangle S_X$ where S_Y is the solution for Y , i.e., $\{s_2\}$:

$$S_X = \{s_2\} \cup \langle \text{Act} \cdot \rangle S_X$$

Example: It is possible to reach a state which has an infinite trace of τ actions (a livelock).

$$X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X \quad Y \stackrel{\max}{=} \langle \tau \rangle Y$$

Consider the following labeled transition system:



Solution for Y is independent of solution for X and it is the greatest fixed point of the equation $S_Y = \langle \tau \cdot \rangle S_Y$.

Solution for Y is $\{s_2\}$.

The solution for X is also easily computed to be the least fixed point of the equation $S_X = S_Y \cup \langle \text{Act} \cdot \rangle S_X$ where S_Y is the solution for Y , i.e., $\{s_2\}$:

$$S_X = \{s_2\} \cup \langle \text{Act} \cdot \rangle S_X$$

The solution is $\{s_1, s_2\}$.

Alternation-free modal μ -calculus

Consider a system of recursive equations

$$\begin{array}{l} X_1 \equiv F_1 \\ X_2 \equiv F_2 \\ \vdots \\ X_n \equiv F_n \end{array} \quad \text{where each } \equiv \text{ is either } \stackrel{\text{min}}{=} \text{ or } \stackrel{\text{max}}{=}.$$

This set of equations is called alternation-free if the set of equations can be partitioned into blocks such that

- the equations in one block all have the same type of fixed point
- the equations in one block only use variables that are defined in that block or in preceding blocks

Examples

$$\text{acyclic } X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X$$
$$Y \stackrel{\max}{=} \langle \tau \rangle Y$$

Examples

acyclic $X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X$
 $Y \stackrel{\max}{=} \langle \tau \rangle Y$

cyclic block $X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false}$
 $Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$

Examples

acyclic $X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X$
 $Y \stackrel{\max}{=} \langle \tau \rangle Y$

cyclic block $X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false}$
 $Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$

cyclic non-block $X \stackrel{\min}{=} Y$
 $Y \stackrel{\max}{=} (\langle a \rangle \text{true} \wedge [c] X) \vee (\langle b \rangle \text{true} \wedge [c] Y)$

Meaning: on every infinite c -trail a is enabled only finitely often and b infinitely often

Examples

acyclic $X \stackrel{\min}{=} Y \vee \langle \text{Act} \rangle X$
 $Y \stackrel{\max}{=} \langle \tau \rangle Y$

cyclic block $X \stackrel{\max}{=} \langle a \rangle Y \wedge [a] Y \wedge [b] \text{false}$
 $Y \stackrel{\max}{=} \langle b \rangle X \wedge [b] X \wedge [a] \text{false}$

cyclic non-block $X \stackrel{\min}{=} Y$
 $Y \stackrel{\max}{=} (\langle a \rangle \text{true} \wedge [c] X) \vee (\langle b \rangle \text{true} \wedge [c] Y)$

Meaning: on every infinite c -trail a is enabled only finitely often and b infinitely often

We will **not** discuss non-alternating-free modal μ -calculus formulas any further!

- 1 Solve block without dependencies on other blocks first using techniques previously introduced

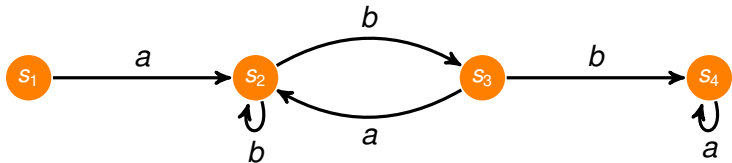
Semantics of alternation-free modal μ -calculus

- 1 Solve block without dependencies on other blocks first using techniques previously introduced
- 2 Instantiate system with the solution thus obtaining new system

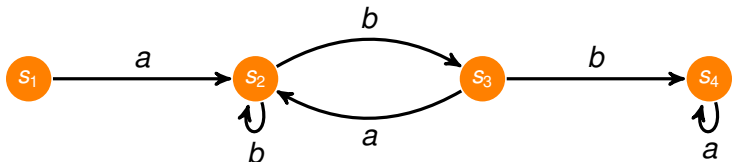
Semantics of alternation-free modal μ -calculus

- 1 Solve block without dependencies on other blocks first using techniques previously introduced
- 2 Instantiate system with the solution thus obtaining new system
- 3 Repeat from step 1. until all variables are solved

Example: $X \stackrel{\min}{\equiv} Y \vee \langle b \rangle X$ $Y \stackrel{\max}{\equiv} \langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y$
Consider the following labeled transition system:

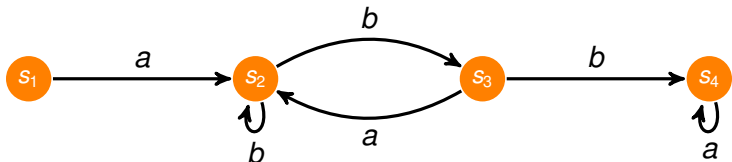


Example: $X \stackrel{\min}{=} Y \vee \langle b \rangle X$ $Y \stackrel{\max}{=} \langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y$
Consider the following labeled transition system:



Two blocks: one containing only X and one containing only Y

Example: $X \stackrel{\min}{=} Y \vee \langle b \rangle X$ $Y \stackrel{\max}{=} \langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y$
 Consider the following labeled transition system:

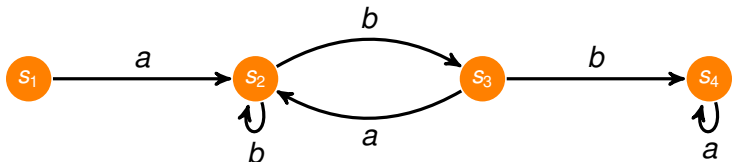


Two blocks: one containing only X and one containing only Y
 Compute first $\llbracket Y \rrbracket$ as the greatest fixed point, say S_Y , of

$$O_{\langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y}(S)$$

using 'traditional' techniques. Thus $S_Y = \{s_3, s_4\}$

Example: $X \stackrel{\min}{=} Y \vee \langle b \rangle X$ $Y \stackrel{\max}{=} \langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y$
 Consider the following labeled transition system:



Two blocks: one containing only X and one containing only Y
 Compute first $\llbracket Y \rrbracket$ as the greatest fixed point, say S_Y , of

$$O_{\langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y}(S)$$

using 'traditional' techniques. Thus $S_Y = \{s_3, s_4\}$

Compute $\llbracket X \rrbracket$ as the least fixed point of

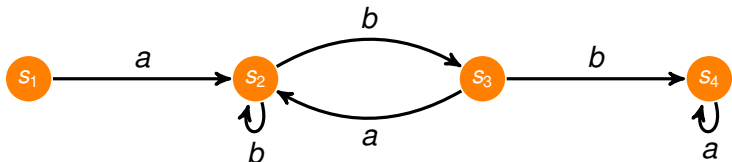
$$O_{Y \vee \langle b \rangle X}(S)$$

where S_Y is substituted for $\llbracket Y \rrbracket$ i.e. the least fixed point of

$$\{s_3, s_4\} \cup O_{\langle b \rangle X}(S)$$

Example: $X \stackrel{\min}{=} Y \vee \langle b \rangle X$ $Y \stackrel{\max}{=} \langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y$

Consider the following labeled transition system:



Two blocks: one containing only X and one containing only Y
 Compute first $\llbracket Y \rrbracket$ as the greatest fixed point, say S_Y , of

$$O_{\langle a \rangle \text{true} \wedge \langle \text{Act} \rangle Y}(S)$$

using 'traditional' techniques. Thus $S_Y = \{s_3, s_4\}$

Compute $\llbracket X \rrbracket$ as the least fixed point of

$$O_{Y \vee \langle b \rangle X}(S)$$

where S_Y is substituted for $\llbracket Y \rrbracket$ i.e. the least fixed point of

$$\{s_3, s_4\} \cup O_{\langle b \rangle X}(S)$$

The solution (for X) is $\{s_2, s_3, s_4\}$

Outline

- 1 Blocks of equations
- 2 Alternation-free modal μ -calculus
- 3 Regular alternation-free modal μ -calculus**
- 4 Typical properties

Syntax for action formulas

$$\alpha ::= a \mid \text{true} \mid \text{false} \mid \bar{\alpha} \mid \alpha \cap \alpha \mid \alpha \cup \alpha$$

Syntax for action formulas

$$\alpha ::= a \mid true \mid false \mid \bar{\alpha} \mid \alpha \cap \alpha \mid \alpha \cup \alpha$$

Set of actions described by action formulas

$$\begin{aligned} \llbracket a \rrbracket &= \{a\} \\ \llbracket true \rrbracket &= Act \\ \llbracket false \rrbracket &= \emptyset \\ \llbracket \bar{\alpha} \rrbracket &= Act \setminus \llbracket \alpha \rrbracket \\ \llbracket \alpha_1 \cap \alpha_2 \rrbracket &= \llbracket \alpha_1 \rrbracket \cap \llbracket \alpha_2 \rrbracket \\ \llbracket \alpha_1 \cup \alpha_2 \rrbracket &= \llbracket \alpha_1 \rrbracket \cup \llbracket \alpha_2 \rrbracket \end{aligned}$$

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions
- 2 α represents the set of sequences consisting of only one action from the set $[[\alpha]]$; note that these only describe sequences containing of one action

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions
- 2 α represents the set of sequences consisting of only one action from the set $[[\alpha]]$; note that these only describe sequences containing of one action
- 3 $+$ denotes union of the sets of sequences described by arguments

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions
- 2 α represents the set of sequences consisting of only one action from the set $[[\alpha]]$; note that these only describe sequences containing of one action
- 3 $+$ denotes union of the sets of sequences described by arguments
- 4 \cdot denotes pairwise concatenation of sequences from sets of sequences described by arguments

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions
- 2 α represents the set of sequences consisting of only one action from the set $[[\alpha]]$; note that these only describe sequences containing of one action
- 3 $+$ denotes union of the sets of sequences described by arguments
- 4 \cdot denotes pairwise concatenation of sequences from sets of sequences described by arguments
- 5 $*$ denotes sequences of arbitrary (also none) concatenations of sequences from the sets of sequences described by argument

Syntax for actions

$$R := \varepsilon \mid \alpha \mid R + R \mid R \cdot R \mid R^* \mid R^+$$

where

- 1 ε represents the empty sequence of actions
- 2 α represents the set of sequences consisting of only one action from the set $[[\alpha]]$; note that these only describe sequences containing of one action
- 3 $+$ denotes union of the sets of sequences described by arguments
- 4 \cdot denotes pairwise concatenation of sequences from sets of sequences described by arguments
- 5 $*$ denotes sequences of arbitrary (also none) concatenations of sequences from the sets of sequences described by argument
- 6 $+$ denotes sequences of the concatenation of at least one sequence from the sets of sequences described by argument

Syntax for formulas

$$F ::= \text{true} \mid \text{false} \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$$

Examples

Syntax for formulas

$$F ::= true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$$

Examples

- $\langle a \cdot b \cdot c \rangle true$ expresses that the sequence $a b c$ can be performed

Syntax for formulas

$$F ::= true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$$

Examples

- $\langle a \cdot b \cdot c \rangle true$ expresses that the sequence $a b c$ can be performed
- $[a \cdot b + c \cdot d] false$ expresses that neither the sequence $a b$ nor the sequence $c d$ is possible

Syntax for formulas

$$F ::= \text{true} \mid \text{false} \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$$

Examples

- $\langle a \cdot b \cdot c \rangle \text{true}$ expresses that the sequence $a b c$ can be performed
- $[a \cdot b + c \cdot d] \text{false}$ expresses that neither the sequence $a b$ nor the sequence $c d$ is possible
- $\langle a^* \rangle F$ expresses that there is a sequence of a -transitions to a state where F holds

Syntax for formulas

$$F ::= true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$$

Examples

- $\langle a \cdot b \cdot c \rangle true$ expresses that the sequence $a b c$ can be performed
- $[a \cdot b + c \cdot d] false$ expresses that neither the sequence $a b$ nor the sequence $c d$ is possible
- $\langle a^* \rangle F$ expresses that there is a sequence of a -transitions to a state where F holds
- $[a^+] F$ expresses that the formula F holds in any state reached by one or more a -transitions

More examples

- 1 it is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter] false$$

More examples

- 1 it is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter] false$$

- 2 there is no deadlock in any reachable state:

$$[true^*] \langle true \rangle true$$

More examples

- 1 it is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

- 2 there is no deadlock in any reachable state:

$$[true^*]\langle true \rangle true$$

- 3 after sending a message it can eventually be received:

$$[send]\langle true^* \cdot receive \rangle true$$

$$\langle true \cdot \bar{a} \rangle true$$

- Step 1** Translate formulas of regular alternation-free modal μ -calculus to formulas of regular alternation-free modal μ -calculus with only simple action formulas (α)

$$\langle true \rangle \langle \bar{a} \rangle true$$

- Step 2** Translate formulas of regular alternation-free modal μ -calculus with only simple action formulas to alternation-free modal μ -calculus (i.e., without action formulas)

$$\langle Act \rangle \langle Act \setminus \{a\} \rangle true$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R] F \mid X_1 \mid X_2 \mid \dots$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\langle \varepsilon \rangle F \mapsto F'$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\begin{aligned}\langle \varepsilon \rangle F &\mapsto F' \\ \langle \alpha \rangle F &\mapsto \langle \alpha \rangle F'\end{aligned}$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\begin{aligned}\langle \varepsilon \rangle F &\mapsto F' \\ \langle \alpha \rangle F &\mapsto \langle \alpha \rangle F' \\ \langle R_1 + R_2 \rangle F &\mapsto \langle R_1 \rangle F' \vee \langle R_2 \rangle F'\end{aligned}$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\begin{aligned}\langle \varepsilon \rangle F &\mapsto F' \\ \langle \alpha \rangle F &\mapsto \langle \alpha \rangle F' \\ \langle R_1 + R_2 \rangle F &\mapsto \langle R_1 \rangle F' \vee \langle R_2 \rangle F' \\ \langle R_1 \cdot R_2 \rangle F &\mapsto \langle R_1 \rangle \langle R_2 \rangle F'\end{aligned}$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\begin{aligned}\langle \varepsilon \rangle F &\mapsto F' \\ \langle \alpha \rangle F &\mapsto \langle \alpha \rangle F' \\ \langle R_1 + R_2 \rangle F &\mapsto \langle R_1 \rangle F' \vee \langle R_2 \rangle F' \\ \langle R_1 \cdot R_2 \rangle F &\mapsto \langle R_1 \rangle \langle R_2 \rangle F' \\ \langle R^* \rangle F &\mapsto X\end{aligned}$$

Step 1

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Translation of $\langle R \rangle F$ (assuming F' is translation of F):

$$\begin{aligned}\langle \varepsilon \rangle F &\mapsto F' \\ \langle \alpha \rangle F &\mapsto \langle \alpha \rangle F' \\ \langle R_1 + R_2 \rangle F &\mapsto \langle R_1 \rangle F' \vee \langle R_2 \rangle F' \\ \langle R_1 \cdot R_2 \rangle F &\mapsto \langle R_1 \rangle \langle R_2 \rangle F' \\ \langle R^* \rangle F &\mapsto X \\ \langle R^+ \rangle F &\mapsto \langle R \rangle \langle R^* \rangle F'\end{aligned}$$

with X a fresh recursion variable defined by

$$X \stackrel{\min}{=} F' \vee \langle R \rangle X$$

Example

After sending a message it can eventually be received:

$$[send]\langle true^* \cdot receive \rangle true$$

Example

After sending a message it can eventually be received:

$$[send]\langle true^* \cdot receive \rangle true$$

represents

$$[send]\langle true^* \cdot receive \rangle true$$
$$\mapsto$$
$$[send]\langle true^* \rangle \langle receive \rangle true$$

Example

After sending a message it can eventually be received:

$$[send]\langle true^* \cdot receive \rangle true$$

represents

$$[send]\langle true^* \cdot receive \rangle true$$
$$\mapsto$$
$$[send]\langle true^* \rangle \langle receive \rangle true$$
$$\mapsto$$
$$[send]X$$

with

$$X \stackrel{\text{min}}{=} \langle receive \rangle true \vee \langle true \rangle X$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$[\varepsilon]F \mapsto F'$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$\begin{aligned} [\varepsilon]F &\mapsto F' \\ [\alpha]F &\mapsto [\alpha]F' \end{aligned}$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$\begin{aligned} [\varepsilon]F &\mapsto F' \\ [\alpha]F &\mapsto [\alpha]F' \\ [R_1 + R_2]F &\mapsto [R_1]F' \wedge [R_2]F' \end{aligned}$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$\begin{aligned} [\varepsilon]F &\mapsto F' \\ [\alpha]F &\mapsto [\alpha]F' \\ [R_1 + R_2]F &\mapsto [R_1]F' \wedge [R_2]F' \\ [R_1 \cdot R_2]F &\mapsto [R_1][R_2]F' \end{aligned}$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$\begin{aligned} [\varepsilon]F &\mapsto F' \\ [\alpha]F &\mapsto [\alpha]F' \\ [R_1 + R_2]F &\mapsto [R_1]F' \wedge [R_2]F' \\ [R_1 \cdot R_2]F &\mapsto [R_1][R_2]F' \\ [R^*]F &\mapsto X \end{aligned}$$

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle R \rangle F \mid [R]F \mid X_1 \mid X_2 \mid \dots$

Step 1

Translation of $[R]F$ (assuming F' is translation of F):

$$\begin{aligned} [\varepsilon]F &\mapsto F' \\ [\alpha]F &\mapsto [\alpha]F' \\ [R_1 + R_2]F &\mapsto [R_1]F' \wedge [R_2]F' \\ [R_1 \cdot R_2]F &\mapsto [R_1][R_2]F' \\ [R^*]F &\mapsto X \\ [R^+]F &\mapsto [R][R^*]F' \end{aligned}$$

with X a fresh recursion variable defined by

$$X \stackrel{\text{max}}{=} F' \wedge [R]X$$

Example

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

Example

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

represents

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

\mapsto

$$[true^*][enter][\overline{leave}^*][enter]false$$

with

Example

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

represents

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

\mapsto

$$[true^*][enter][\overline{leave}^*][enter]false$$

\mapsto

$$[true^*][enter]X$$

with

$$X \stackrel{\max}{=} [enter]false \wedge [\overline{leave}]X$$

Example

It is impossible to do two consecutive *enter* actions without a *leave* action in between:

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

represents

$$[true^* \cdot enter \cdot \overline{leave}^* \cdot enter]false$$

\mapsto

$$[true^*][enter][\overline{leave}^*][enter]false$$

\mapsto

$$[true^*][enter]X$$

\mapsto

Y

with

$$X \stackrel{\max}{=} [enter]false \wedge [\overline{leave}]X \qquad Y \stackrel{\max}{=} [enter]X \wedge [true]Y$$

Step 2

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle \alpha \rangle F \mid [\alpha] F \mid X_1 \mid X_2 \mid \dots$

Step 2

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle \alpha \rangle F \mid [\alpha] F \mid X_1 \mid X_2 \mid \dots$

$$\langle \alpha \rangle F \mapsto \langle [[\alpha]] \rangle F$$

with

$$\begin{aligned} [[a]] &= \{a\} \\ [[true]] &= Act \\ [[false]] &= \emptyset \\ [[\bar{\alpha}]] &= Act \setminus [[\alpha]] \\ [[\alpha_1 \cap \alpha_2]] &= [[\alpha_1]] \cap [[\alpha_2]] \\ [[\alpha_1 \cup \alpha_2]] &= [[\alpha_1]] \cup [[\alpha_2]] \end{aligned}$$

Step 2

$F := true \mid false \mid F \wedge F \mid F \vee F \mid \langle \alpha \rangle F \mid [\alpha] F \mid X_1 \mid X_2 \mid \dots$

$$\langle \alpha \rangle F \mapsto \langle [[\alpha]] \rangle F$$

$$[\alpha] F \mapsto [[\alpha]] F$$

with

$$[[a]] = \{a\}$$

$$[[true]] = Act$$

$$[[false]] = \emptyset$$

$$[[\bar{\alpha}]] = Act \setminus [[\alpha]]$$

$$[[\alpha_1 \cap \alpha_2]] = [[\alpha_1]] \cap [[\alpha_2]]$$

$$[[\alpha_1 \cup \alpha_2]] = [[\alpha_1]] \cup [[\alpha_2]]$$

Example

There is no deadlock in any reachable state:

$$[true^*]\langle true \rangle true$$

Example

There is no deadlock in any reachable state:

$$[true^*]\langle true \rangle true$$

represents

$$\text{Step 1 } [true^*]\langle true \rangle true \quad \mapsto \quad X$$

with

$$X \stackrel{\text{max}}{=} \langle true \rangle true \wedge [true]X$$

Example

There is no deadlock in any reachable state:

$$[true^*]\langle true \rangle true$$

represents

$$\text{Step 1 } [true^*]\langle true \rangle true \quad \mapsto \quad X$$

with

$$X \stackrel{\max}{=} \langle true \rangle true \wedge [true]X$$

$$\text{Step 2 } X \text{ with}$$

$$X \stackrel{\max}{=} \langle Act \rangle true \wedge [Act]X$$

Outline

- 1 Blocks of equations
- 2 Alternation-free modal μ -calculus
- 3 Regular alternation-free modal μ -calculus
- 4 Typical properties**

Typical properties

Safety

- 1 Absence of an *error* action

Typical properties

Safety

- 1 Absence of an *error* action

$[true^* \cdot error]false$

Typical properties

Safety

- 1 Absence of an *error* action

$$[true^* \cdot error]false$$

- 2 Impossibility of doing a *recv* action before a *send* action

Typical properties

Safety

- 1 Absence of an *error* action

$$[true^* \cdot error] false$$

- 2 Impossibility of doing a *recv* action before a *send* action

$$[\overline{send}^* \cdot recv] false$$

Typical properties

Safety

- 1 Absence of an *error* action

$$[true^* \cdot error] false$$

- 2 Impossibility of doing a *recv* action before a *send* action

$$[\overline{send}^* \cdot recv] false$$

- 3 Mutual exclusion of sections delimited by *open* and *close* actions

Typical properties

Safety

- 1 Absence of an *error* action

$$[true^* \cdot error] false$$

- 2 Impossibility of doing a *recv* action before a *send* action

$$[\overline{send}^* \cdot recv] false$$

- 3 Mutual exclusion of sections delimited by *open* and *close* actions

$$[true^* \cdot open1 \cdot \overline{close1}^* \cdot open2] false$$

Typical properties

Liveness

- 1 Deadlock freedom

Typical properties

Liveness

- 1 Deadlock freedom

$[true^*]\langle true \rangle true$

Typical properties

Liveness

- 1 Deadlock freedom

$[true^*]\langle true \rangle true$

- 2 Possibility of doing a *recv* action after a *send* action (and some *errors*)

Typical properties

Liveness

- 1 Deadlock freedom

$$[true^*]\langle true \rangle true$$

- 2 Possibility of doing a *recv* action after a *send* action (and some *errors*)

$$\langle true^* \cdot send \cdot (true^* \cdot error)^* \cdot recv \rangle true$$

Typical properties

Liveness

- 1 Deadlock freedom

$$[true^*]\langle true \rangle true$$

- 2 Possibility of doing a *recv* action after a *send* action (and some *errors*)

$$\langle true^* \cdot send \cdot (true^* \cdot error)^* \cdot recv \rangle true$$

- 3 Unavoidability of doing a *grant* action after a *req* action

Typical properties

Liveness

- 1 Deadlock freedom

$$[true^*]\langle true \rangle true$$

- 2 Possibility of doing a *recv* action after a *send* action (and some *errors*)

$$\langle true^* \cdot send \cdot (true^* \cdot error)^* \cdot recv \rangle true$$

- 3 Unavoidability of doing a *grant* action after a *req* action

$$[true^* \cdot req]X$$

with

$$X \stackrel{\min}{=} \langle true \rangle true \wedge \overline{[grant]}X$$

Typical properties

Fairness

- 1 Livelock freedom

$$[true^*]X$$

with

$$X \stackrel{\text{min}}{=} [\tau]X$$

Typical properties

Fairness

- 1 Livelock freedom

$$[true^*]X$$

with

$$X \stackrel{\text{min}}{=} [\tau]X$$

- 2 Fair reachability (neglecting cycles) of a *recv* action after a *send* action

$$[true^* \cdot send \cdot \overline{recv}^*] \langle true^* \cdot recv \rangle true$$

Material from the chapters 5 and 6 of the book by Aceto et al.:

- all section of chapter 5 on Hennessy-Milner Logic
- all sections of chapter 6 on Hennessy-Milner Logic with Recursive Definitions, except for section 6.4 (Game Characterization for HML with Recursion) and section 6.6 (Characteristic properties)