Logics for processes (II)

Luís S. Barbosa

DI-CCTC
Universidade do Minho
Braga, Portugal

April, 2011

Motivation

Is Hennessy-Milner logic expressive enough?

- It cannot detect deadlock in an arbitrary process
- or general safety: all reachable states verify ϕ
- or general liveness: there is a reachable states which verifies ϕ
- ...

... essentially because

formulas in $\mathcal{M}$ cannot see deeper than their modal depth

where

$$\text{mdepth}(\text{true}) = \text{mdepth}(\text{false}) = 0$$
$$\text{mdepth}(\langle K\rangle\psi) = \text{mdepth}([K]\psi) = \text{mdepth}(\psi) + 1$$
$$\text{mdepth}(\phi \wedge \psi) = \text{mdepth}(\phi \vee \psi) = \max\{\text{mdepth}(\phi), \text{mdepth}(\psi)\}$$

Motivation

Is Hennessy-Milner logic expressive enough?

- It cannot detect deadlock in an arbitrary process
- or general safety: all reachable states verify ϕ
- or general liveness: there is a reachable states which verifies ϕ
- ...

... essentially because

formulas in $\mathcal{M}$ cannot see deeper than their modal depth

where

$$\begin{aligned}
\text{mdepth}(\text{true}) &= \text{mdepth}(\text{false}) = 0 \\
\text{mdepth}(\langle K\rangle\psi) &= \text{mdepth}([K]\psi) = \text{mdepth}(\psi) + 1 \\
\text{mdepth}(\phi \wedge \psi) &= \text{mdepth}(\phi \vee \psi) = \max\{\text{mdepth}(\phi), \text{mdepth}(\psi)\}
\end{aligned}$$

Motivation

Example

ϕ = a taxi eventually returns to its Central

$$\phi = \langle reg \rangle \mathsf{true} \vee \langle - \rangle \langle reg \rangle \mathsf{true} \vee \langle - \rangle \langle - \rangle \langle reg \rangle \mathsf{true} \vee \langle - \rangle \langle - \rangle \langle - \rangle \langle reg \rangle \mathsf{true} \vee \ldots$$

Motivation

Example

$$A \triangleq \sum_{i \geq 0} A_i \quad \text{with} \quad A_0 \triangleq \mathbf{0} \text{ e } A_{i+1} \triangleq a.A_i$$

$$A' \triangleq A + D \quad \text{with} \quad D \triangleq a.D$$

- $A \nsim A'$
- but there is no modal formula in $\mathcal{M}$ to distinguish A from A'
- notice $A' \models \langle a \rangle^{i+1}$true which A_i fails
- a distinguishing formula would require infinite conjunction
- what we want to express is the possibility of doing a in the long run

Temporal properties as limits

idea: introduce recursion in formulas

$$X \triangleq \langle a \rangle X$$

meaning?

- the recursive formula is interpreted as the fixed points of function

$$\|\langle a \rangle\|$$

  in n $\mathcal{P}\mathbb{P}$
- i.e., the solutions, i.e., $S \subseteq \mathbb{P}$ such that of

$$S = \|\langle a \rangle\|(S)$$

- how do we solve this equation?

Solving equations ...

over natural numbers

$$\begin{aligned} x &= 3x && \text{one solution } (x = 0) \\ x &= 1 + x && \text{no solutions} \\ x &= 1x && \text{many solutions (every natural } x\text{)} \end{aligned}$$

over sets of integers

$$\begin{aligned} x &= \{22\} \cap x && \text{one solution } (x = \{22\}) \\ x &= \mathbb{N} \setminus x && \text{no solutions} \\ x &= \{22\} \cup x && \text{many solutions (every } x \text{ st } \{22\} \subseteq x\text{)} \end{aligned}$$

Solving equations ...

over natural numbers

$$
\begin{aligned}
x &= 3x && \text{one solution } (x = 0) \\
x &= 1 + x && \text{no solutions} \\
x &= 1x && \text{many solutions (every natural } x\text{)}
\end{aligned}
$$

over sets of integers

$$
\begin{aligned}
x &= \{22\} \cap x && \text{one solution } (x = \{22\}) \\
x &= \mathbb{N} \setminus x && \text{no solutions} \\
x &= \{22\} \cup x && \text{many solutions (every } x \text{ st } \{22\} \subseteq x\text{)}
\end{aligned}
$$

Solving equations ...

In general, for a monotonic function f, i.e.

$$X \subseteq Y \;\Rightarrow\; f\,X \subseteq f\,Y$$

Knaster-Tarski Theorem [1928]

A monotonic function f in a complete lattice has a

- unique maximal fixed point:

$$\nu_f \;=\; \bigcup \{X \in \mathcal{P}\mathbb{P} \mid X \subseteq f\,X\}$$

- unique minimal fixed point:

$$\mu_f \;=\; \bigcap \{X \in \mathcal{P}\mathbb{P} \mid f\,X \subseteq X\}$$

- moreover the space of its solutions form a complete lattice

Solving equations ...

In general, for a monotonic function f, i.e.

$$X \subseteq Y \;\Rightarrow\; f\,X \subseteq f\,Y$$

Knaster-Tarski Theorem [1928]

A monotonic function f in a complete lattice has a

- unique maximal fixed point:

$$\nu_f \;=\; \bigcup\{X \in \mathcal{P}\mathbb{P} \mid X \subseteq f\,X\}$$

- unique minimal fixed point:

$$\mu_f \;=\; \bigcap\{X \in \mathcal{P}\mathbb{P} \mid f\,X \subseteq X\}$$

- moreover the space of its solutions form a complete lattice

Back to the example ...

$S \in \mathcal{P}\mathbb{P}$ is a pre-fixed point of $\|\langle a \rangle\|$
iff

$$\|\langle a \rangle\|(S) \subseteq S$$

Recalling,

$$\|\langle a \rangle\|(S) = \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\}$$

the set of sets of processes we are interested in is

$$\begin{aligned} \text{Pre} &= \{S \subseteq \mathbb{P} \mid \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\} \subseteq S\} \\ &= \{S \subseteq \mathbb{P} \mid \forall_{Z \in \mathbb{P}} \,.\, (Z \in \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\} \Rightarrow Z \in S)\} \\ &= \{S \subseteq \mathbb{P} \mid \forall_{E \in \mathbb{P}} \,.\, ((\exists_{E' \in S} \,.\, E \xrightarrow{a} E') \Rightarrow E \in S)\} \end{aligned}$$

which can be characterized by predicate

$$\text{(PRE)} \qquad (\exists_{E' \in S} \,.\, E' \xrightarrow{a} E) \Rightarrow E \in S \qquad (\text{for all } E \in \mathbb{P})$$

Back to the example ...

$S \in \mathcal{P}\mathbb{P}$ is a pre-fixed point of $\|\langle a \rangle\|$
iff

$$\|\langle a \rangle\|(S) \ \subseteq \ S$$

Recalling,

$$\|\langle a \rangle\|(S) \ = \ \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\}$$

the set of sets of processes we are interested in is

$$\begin{aligned} \mathsf{Pre} \ &= \ \{S \subseteq \mathbb{P} \mid \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\} \subseteq S\} \\ &= \ \{S \subseteq \mathbb{P} \mid \forall_{Z \in \mathbb{P}} \,.\, (Z \in \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\} \Rightarrow Z \in S)\} \\ &= \ \{S \subseteq \mathbb{P} \mid \forall_{E \in \mathbb{P}} \,.\, ((\exists_{E' \in S} \,.\, E \xrightarrow{a} E') \Rightarrow E \in S)\} \end{aligned}$$

which can be characterized by predicate

$$(\mathrm{PRE}) \qquad (\exists_{E' \in S} \,.\, E' \xrightarrow{a} E) \Rightarrow E \in S \qquad (\text{for all } E \in \mathbb{P})$$

Back to the example ...

The set of pre-fixed points of

$$\|\langle a\rangle\|$$

is

$$\begin{aligned} \text{Pre} &= \{S \subseteq \mathbb{P} \mid \|\langle a\rangle\|(S) \subseteq S\} \\ &= \{S \subseteq \mathbb{P} \mid \forall_{E\in\mathbb{P}} \,.\, ((\exists_{E'\in S} \,.\, E \xrightarrow{a} E') \Rightarrow E \in S)\} \end{aligned}$$

- Clearly, $\{A \triangleq a.A\} \in \text{Pre}$
- but $\emptyset \in \text{Pre}$ as well

Therefore, its least solution is

$$\bigcap \text{Pre} = \emptyset$$

Conclusion: taking the meaning of $X = \langle a\rangle X$ as the least solution of the equation leads us to equate it to false

Back to the example ...

The set of pre-fixed points of

$$\| \langle a \rangle \|$$

is

$$\begin{aligned} \text{Pre} &= \{ S \subseteq \mathbb{P} \mid \| \langle a \rangle \| (S) \subseteq S \} \\ &= \{ S \subseteq \mathbb{P} \mid \forall_{E \in \mathbb{P}} \, . \, ((\exists_{E' \in S} \, . \, E \xrightarrow{a} E') \Rightarrow E \in S) \} \end{aligned}$$

- Clearly, $\{ A \triangleq a.A \} \in \text{Pre}$
- but $\emptyset \in \text{Pre}$ as well

Therefore, its least solution is

$$\bigcap \text{Pre} = \emptyset$$

Conclusion: taking the meaning of $X = \langle a \rangle X$ as the least solution of the equation leads us to equate it to false

... but there is another possibility ...

$S \in \mathcal{P}\mathbb{P}$ is a post-fixed point of

$$\|\langle a\rangle\|$$

iff

$$S \subseteq \|\langle a\rangle\|(S)$$

leading to the following set of post-fixed points

$$\begin{aligned} \text{Post} &= \{S \subseteq \mathbb{P} \mid S \subseteq \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\}\} \\ &= \{S \subseteq \mathbb{P} \mid \forall_{Z \in \mathbb{P}} \,.\, (Z \in S \Rightarrow Z \in \{E \in \mathbb{P} \mid \exists_{E' \in S} \,.\, E \xrightarrow{a} E'\})\} \\ &= \{S \subseteq \mathbb{P} \mid \forall_{E \in \mathbb{P}} \,.\, (E \in S \Rightarrow \exists_{E' \in S} \,.\, E \xrightarrow{a} E')\} \end{aligned}$$

(POST) If $E \in S$ then $E \xrightarrow{a} E'$ for some $E' \in S$ (for all $E \in P$)

- i.e., if $E \in S$ it can perform a and this ability is maintained in its continuation

... but there is another possibility ...

- i.e., if $E \in S$ it can perform a and this ability is maintained in its continuation
- the greatest subset of $\mathbb{P}$ verifying this condition is the set of processes with at least an infinite computation

$$\cdots \xrightarrow{a} E_3 \xrightarrow{a} E_2 \xrightarrow{a} E_1 \xrightarrow{a} E$$

Conclusion: taking the meaning of $X = \langle a \rangle X$ as the greatest solution of the equation characterizes the property occurrence of a is possible

... but there is another possibility ...

- i.e., if $E \in S$ it can perform a and this ability is maintained in its continuation
- the greatest subset of $\mathbb{P}$ verifying this condition is the set of processes with at least an infinite computation

$$\cdots \xrightarrow{a} E_3 \xrightarrow{a} E_2 \xrightarrow{a} E_1 \xrightarrow{a} E$$

Conclusion: taking the meaning of $X = \langle a \rangle X$ as the greatest solution of the equation characterizes the property occurrence of a is possible

The general case

- The meaning (i.e., set of processes) of a formula $X \triangleq \phi X$ where X occurs free in ϕ
- is a solution of equation

$$X = f(X) \qquad \text{with} \quad f(S) = \|\{S/X\}\phi\|$$

in $\mathcal{P}\mathbb{P}$, where $\|.\|$ is extended to formulae with variables by $\|X\| = X$

The general case

The Knaster-Tarski theorem gives precise characterizations of the

- smallest solution: the intersection of all S such that

$$\text{(PRE)} \quad \text{If} \quad E \in f(S) \quad \text{then} \quad E \in S$$

  to be denoted by

$$\mu X \,.\, \phi$$

- greatest solution: the union of all S such that

$$\text{(POST)} \quad \text{If} \quad E \in S \quad \text{then} \quad E \in f(S)$$

  to be denoted by

$$\nu X \,.\, \phi$$

In the previous example:

$$\nu X \,.\, \langle a \rangle \text{true} \qquad \mu X \,.\, \langle a \rangle \text{true}$$

The general case

The Knaster-Tarski theorem gives precise characterizations of the

- smallest solution: the intersection of all S such that

$$\text{(PRE)} \qquad \text{If} \quad E \in f(S) \quad \text{then} \quad E \in S$$

  to be denoted by

$$\mu X \,.\, \phi$$

- greatest solution: the union of all S such that

$$\text{(POST)} \qquad \text{If} \quad E \in S \quad \text{then} \quad E \in f(S)$$

  to be denoted by

$$\nu X \,.\, \phi$$

In the previous example:

$$\nu X \,.\, \langle a \rangle \text{true} \qquad\qquad \mu X \,.\, \langle a \rangle \text{true}$$

The modal μ-calculus: syntax

... Hennessy-Milner + recursion (i.e. fixed points):

$$\phi ::= X \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \langle K \rangle \phi \mid [K]\phi \mid \mu X . \phi \mid \nu X . \phi$$

where $K \subseteq Act$ and X is a set of propositional variables

- Note that

$$\text{true} \stackrel{\text{abv}}{=} \nu X . X \quad \text{and} \quad \text{false} \stackrel{\text{abv}}{=} \mu X . X$$

The modal μ-calculus: syntax

... Hennessy-Milner + recursion (i.e. fixed points):

$$\phi \ ::= \ X \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \langle K \rangle \phi \mid [K]\phi \mid \mu X . \phi \mid \nu X . \phi$$

where $K \subseteq Act$ and X is a set of propositional variables

- Note that

$$\text{true} \stackrel{\text{abv}}{=} \nu X . X \qquad \text{and} \qquad \text{false} \stackrel{\text{abv}}{=} \mu X . X$$

The modal μ-calculus: denotational semantics

- Presence of variables requires models parametric on valuations:

$$V : X \longrightarrow \mathcal{P}\mathbb{P}$$

- Then,

$$\begin{aligned}
\|X\|_V &= V(X) \\
\|\phi_1 \wedge \phi_2\|_V &= \|\phi_1\|_V \cap \|\phi_2\|_V \\
\|\phi_1 \vee \phi_2\|_V &= \|\phi_1\|_V \cup \|\phi_2\|_V \\
\|[K]\phi\|_V &= \|[K]\|(\|\phi\|_V) \\
\|\langle K\rangle\phi\|_V &= \|\langle K\rangle\|(\|\phi\|_V)
\end{aligned}$$

- and add

$$\begin{aligned}
\|\nu X \,.\, \phi\|_V &= \bigcup\{S \in \mathbb{P} \mid S \subseteq \|\{S/X\}\phi\|_V\} \\
\|\mu X \,.\, \phi\|_V &= \bigcap\{S \in \mathbb{P} \mid \|\{S/X\}\phi\|_V \subseteq S\}
\end{aligned}$$

Notes

where

$$\|[K]\| X \;=\; \{F \in \mathbb{P} \mid \text{if } F \xrightarrow{a} F' \;\wedge\; a \in K \;\text{ then }\; F' \in X\}$$

$$\|\langle K\rangle\| X \;=\; \{F \in \mathbb{P} \mid \exists_{F' \in X, a \in K} \,.\, F \xrightarrow{a} F'\}$$

Notes

The modal μ-calculus [Kozen, 1983] is

- decidable
- strictly more expressive than $\textsc{Pdl}$ and $\textsc{Ctl}^*$

Moreover

- The correspondence theorem of the induced temporal logic with bisimilarity is kept

Example 1: $X \triangleq \phi \vee \langle a \rangle X$

Look for fixed points of

$$f(X) \triangleq \|\phi\| \cup \|\langle a \rangle\|(X)$$

Example 1: $X \triangleq \phi \vee \langle a \rangle X$

$$
\begin{aligned}
\text{(PRE)} \quad & \text{If} \quad E \in f(X) \quad \text{then} \quad E \in X \\
\equiv \quad & \text{If} \quad E \in (\|\phi\| \cup \|\langle a \rangle\|(X)) \quad \text{then} \quad E \in X \\
\equiv \quad & \text{If} \quad E \in \{F \mid F \models \phi\} \cup \{F \in \mathbb{P} \mid \exists_{F' \in X} \, . \, F \xrightarrow{a} F'\} \\
& \qquad \text{then} \quad E \in X \\
\equiv \quad & \text{if} \quad E \models \phi \vee \exists_{E' \in X} \, . \, E \xrightarrow{a} E' \quad \text{then} \quad E \in X
\end{aligned}
$$

The smallest set of processes verifying this condition is composed of processes with at least a computation along which a can occur until ϕ holds. Taking its intersection, we end up with processes in which ϕ holds in a finite number of steps.

Example 1: $X \triangleq \phi \vee \langle a \rangle X$

$$
\begin{array}{rlll}
\text{(POST)} & \text{If} \quad E \in X & \text{then} & E \in f(X) \\
\equiv & \text{If} \quad E \in X & \text{then} & E \in (\|\phi\| \cup \|\langle a \rangle\|(X)) \\
\equiv & \text{If} \quad E \in X & \text{then} & E \in \{F \mid F \models \phi\} \cup \{F \in X \mid \exists_{F' \in X} \,.\, F \xrightarrow{a} F'\} \\
\equiv & \text{If} \quad E \in X & \text{then} & E \models \phi \vee \exists_{E' \in X} \,.\, E \xrightarrow{a} E'
\end{array}
$$

The greatest fixed point also includes processes which keep the possibility of doing a without ever reaching a state where ϕ holds.

Example 1: $X \triangleq \phi \vee \langle a \rangle X$

- strong until:

$$\mu X . \phi \vee \langle a \rangle X$$

- weak until

$$\nu X . \phi \vee \langle a \rangle X$$

Relevant particular cases:

- ϕ holds after internal activity:

$$\mu X . \phi \vee \langle \tau \rangle X$$

- ϕ holds in a finite number of steps

$$\mu X . \phi \vee \langle - \rangle X$$

Example 1: $X \triangleq \phi \vee \langle a \rangle X$

- strong until:

$$\mu X \,.\, \phi \vee \langle a \rangle X$$

- weak until

$$\nu X \,.\, \phi \vee \langle a \rangle X$$

Relevant particular cases:

- ϕ holds after internal activity:

$$\mu X \,.\, \phi \vee \langle \tau \rangle X$$

- ϕ holds in a finite number of steps

$$\mu X \,.\, \phi \vee \langle - \rangle X$$

Example 2: $X \triangleq \phi \wedge \langle a \rangle X$

$$\text{(PRE)} \quad \text{If} \quad E \models \phi \wedge \exists_{E' \in X} \, . \, E \xrightarrow{a} E' \quad \text{then} \quad E \in X$$

implies that

$$\mu X \, . \, \phi \wedge \langle a \rangle X \Leftrightarrow \text{false}$$

$$\text{(POST)} \quad \text{If} \quad E \in X \quad \text{then} \quad E \models \phi \wedge \exists_{E' \in X} \, . \, E \xrightarrow{a} E'$$

implies that

$$\nu X \, . \, \phi \wedge \langle a \rangle X$$

denote all processes which verify ϕ and have an infinite computation

$$\cdots \xrightarrow{a} E_3 \xrightarrow{a} E_2 \xrightarrow{a} E_1 \xrightarrow{a} E$$

Example 2: $X \triangleq \phi \wedge \langle a \rangle X$

$$\text{(PRE)} \quad \text{If} \quad E \models \phi \wedge \exists_{E' \in X} . E \xrightarrow{a} E' \quad \text{then} \quad E \in X$$

implies that

$$\mu X . \phi \wedge \langle a \rangle X \Leftrightarrow \text{false}$$

$$\text{(POST)} \quad \text{If} \quad E \in X \quad \text{then} \quad E \models \phi \wedge \exists_{E' \in X} . E \xrightarrow{a} E'$$

implies that

$$\nu X . \phi \wedge \langle a \rangle X$$

denote all processes which verify ϕ and have an infinite computation

$$\cdots \xrightarrow{a} E_3 \xrightarrow{a} E_2 \xrightarrow{a} E_1 \xrightarrow{a} E$$

Example 2: $X \triangleq \phi \wedge \langle a \rangle X$

Variant:

- ϕ holds along a finite or infinite *a*-computation:

$$\nu X \,.\, \phi \wedge (\langle a \rangle X \vee [a]\mathsf{false})$$

In general:

- weak safety:

$$\nu X \,.\, \phi \wedge (\langle K \rangle X \vee [K]\mathsf{false})$$

- weak safety, for $K = Act$:

$$\nu X \,.\, \phi \wedge (\langle - \rangle X \vee [-]\mathsf{false})$$

Example 3: $X \triangleq [-]X$

(POST) If $E \in X$ then $E \in \|[-]\|(X)$

$\equiv$ If $E \in X$ then (if $E \xrightarrow{x} E'$ and $x \in Act$ then $E' \in X$)

implies $\nu X\,.\,[-]X \Leftrightarrow \mathrm{true}$

(PRE) If (if $E \xrightarrow{x} E'$ and $x \in Act$ then $E' \in X$) then $E \in X$

implies $\mu X\,.\,[-]X$ represent convergent processes (why?)

Example 3: $X \triangleq [-]X$

$$\begin{array}{llll}
\text{(POST)} & \text{If} \quad E \in X & \text{then} & E \in \|[-]\|(X) \\
\equiv & \text{If} \quad E \in X & \text{then} & (\text{if} \;\; E \xrightarrow{x} E' \text{ and } x \in Act \;\; \text{then} \;\; E' \in X)
\end{array}$$

implies $\nu X \,.\, [-]X \Leftrightarrow \text{true}$

$$\text{(PRE)} \quad \text{If} \quad (\text{if} \;\; E \xrightarrow{x} E' \text{ and } x \in Act \;\; \text{then} \;\; E' \in X) \quad \text{then} \quad E \in X$$

implies $\mu X \,.\, [-]X$ represent convergent processes (why?)

Safety and liveness

- weak liveness:

$$\mu X \,.\, \phi \vee \langle - \rangle X$$

- strong safety

$$\nu X \,.\, \psi \wedge [-] X$$

making $\psi = \phi^c$ both properties are dual:

- there is at least a computation reaching a state s such that $s \models \phi$
- all states s reached along all computations maintain ϕ, ie, $s \models \phi^c$

Safety and liveness

- weak liveness:

$$\mu X \,.\, \phi \vee \langle - \rangle X$$

- strong safety

$$\nu X \,.\, \psi \wedge [-] X$$

making $\psi = \phi^{c}$ both properties are dual:

- there is at least a computation reaching a state s such that $s \models \phi$
- all states s reached along all computations maintain ϕ, ie, $s \models \phi^{c}$

Safety and liveness

Qualifiers weak and strong refer to a quatification over computations

- weak liveness:

$$\mu X \,.\, \phi \ \vee \ \langle - \rangle X$$

corresponds to Ctl formula $\mathtt{E}\ \mathtt{F}\ \phi$

- strong safety

$$\nu X \,.\, \psi \wedge [-] X$$

corresponds to Ctl formula $\mathtt{A}\ \mathtt{G}\ \psi$

cf, liner time vs branching time

Duality

$$(\mu X \,.\, \phi)^c = \nu X \,.\, \phi^c$$
$$(\nu X \,.\, \phi)^c = \mu X \,.\, \phi^c$$

Example:

- divergence:

$$\nu X \,.\, \langle \tau \rangle X$$

- convergence (= all non observable behaviour is finite)

$$(\nu X \,.\, \langle \tau \rangle X)^c = \mu X \,.\, (\langle \tau \rangle X)^c = \mu X \,.\, [\tau] X$$

Duality

$$(\mu X \,.\, \phi)^{\mathsf{c}} = \nu X \,.\, \phi^{\mathsf{c}}$$
$$(\nu X \,.\, \phi)^{\mathsf{c}} = \mu X \,.\, \phi^{\mathsf{c}}$$

Example:

- divergence:

$$\nu X \,.\, \langle \tau \rangle X$$

- convergence (= all non observable behaviour is finite)

$$(\nu X \,.\, \langle \tau \rangle X)^{\mathsf{c}} = \mu X \,.\, (\langle \tau \rangle X)^{\mathsf{c}} = \mu X \,.\, [\tau] X$$

Safety and liveness

- weak safety:

$$\nu X \,.\, \phi \wedge (\langle - \rangle X \vee [-]\mathsf{false})$$

(there is a computation along which ϕ holds)

- strong liveness

$$\mu X \,.\, \psi \vee ([-] X \wedge \langle - \rangle \mathsf{true})$$

(a state where the complement of ϕ holds can be finitely reached)

State-oriented vs action-oriented

Consider the following strong liveness requirement:
$\phi_0 \ = \ $ *a taxi will end up returning to the Central*

- state-oriented:

$$\mu X \,.\, \langle reg \rangle \mathsf{true} \vee ([-]X \wedge \langle - \rangle \mathsf{true})$$

(all computations reach a state where *reg* can happen)

- action-oriented

$$\mu X \,.\, [-reg]X \wedge \langle - \rangle \mathsf{true}$$

(action *reg* occurs)

Its dual is the action-oriented weak safety:

$$\nu X \,.\, \langle -reg \rangle X \vee [-]\mathsf{false}$$

State-oriented vs action-oriented

Example:

$$A_0 \triangleq a.\sum_{i \geq 0} A_i \quad \text{with} \quad A_{i+1} \triangleq b.A_i$$

For a $k > 0$, process $(A_k \mid A_k)$ verifies 'a certainly occurs'

$$\mu X \,.\, [-a]X \wedge \langle - \rangle \text{true}$$

but fails

$$\mu X \,.\, (\langle - \rangle \text{true} \wedge [-a]\text{false}) \;\vee\; (\langle - \rangle \text{true} \wedge [-]X)$$

which means that a state in which a is inevitable can be reached, because both processes can evolve to a situation in which at least on of them can offer the possibility of doing b.

State-oriented vs action-oriented

Example:

$$A_0 \triangleq a.\sum_{i \geq 0} A_i \quad \text{with} \quad A_{i+1} \triangleq b.A_i$$

For a $k > 0$, process $(A_k \mid A_k)$ verifies '*a* certainly occurs'

$$\mu X \,.\, [-a]X \wedge \langle - \rangle \text{true}$$

but fails

$$\mu X \,.\, (\langle - \rangle \text{true} \wedge [-a]\text{false}) \;\vee\; (\langle - \rangle \text{true} \wedge [-]X)$$

which means that a state in which *a* is inevitable can be reached, because both processes can evolve to a situation in which at least on of them can offer the possibility of doing *b*.

State-oriented vs action-oriented

Example:

$$B_0 \triangleq a.\sum_{i\geq 0} B_i + \sum_{i\geq 0} B_i \quad \text{with} \quad B_{i+1} \triangleq b.B_i$$

Process $(B_k \mid B_k)$, for $k > 0$, fails both properties but verifies

$$\mu X \, . \, \langle a \rangle \text{true} \ \vee \ (\langle - \rangle \text{true} \wedge [-] X)$$

a liveness property stating that a state in which a is possible can be reached (which however is not inevitable!)

Conditional properties

ϕ_1 =
After collecting a passenger (*icr*), the taxi drops him at destination (*fcr*)
Second part of ϕ_1 is strong liveness:

$$\mu X . [-fcr]X \wedge \langle - \rangle \text{true}$$

holding only after *icr*.
Is it enough to write:

$$[icr](\mu X . [-fcr]X \wedge \langle - \rangle \text{true})$$

?
what we want does not depend on the initial state: it is liveness embedded into strong safety:

$$\nu Y . [icr](\mu X . [-fcr]X \wedge \langle - \rangle \text{true}) \wedge [-]Y$$

Conditional properties

ϕ_1 =
After collecting a passenger (*icr*), the taxi drops him at destination (*fcr*)
Second part of ϕ_1 is strong liveness:

$$\mu X \,.\, [-fcr]X \wedge \langle - \rangle \text{true}$$

holding only after *icr*.
Is it enough to write:

$$[icr](\mu X \,.\, [-fcr]X \wedge \langle - \rangle \text{true})$$

?
what we want does not depend on the initial state: it is liveness embedded into strong safety:

$$\nu Y \,.\, [icr](\mu X \,.\, [-fcr]X \wedge \langle - \rangle \text{true}) \;\wedge\; [-]Y$$

Conditional properties

The previous example is conditional liveness but one can also have

- conditional safety:

$$\nu Y \, . \, (\phi^{\mathsf{c}} \vee (\phi \wedge \nu X \, . \, \psi \wedge [-]X)) \wedge [-]Y$$

(whenever ϕ holds, ψ cannot cease to hold)

Cyclic properties

$\phi =$ every second action is *out*
is expressed by

$$\nu X \,.\, [-]([-out]\mathsf{false} \wedge [-]X)$$

$\phi =$ *out* follows *in*, but other actions can occur in between

$$\nu X \,.\, [out]\mathsf{false} \wedge [in](\mu Y \,.\, [in]\mathsf{false} \wedge [out]X \wedge [-out]Y) \wedge [-in]X$$

Note that the use of least fixed points imposes that the amount of computation between *in* and *out* is finite

Cyclic properties

ϕ = every second action is *out*
is expressed by

$$\nu X \,.\, [-]([-out]\mathrm{false} \wedge [-]X)$$

ϕ = *out* follows *in*, but other actions can occur in between

$$\nu X \,.\, [out]\mathrm{false} \wedge [in](\mu Y \,.\, [in]\mathrm{false} \wedge [out]X \wedge [-out]Y) \wedge [-in]X$$

Note that the use of least fixed points imposes that the amount of computation between *in* and *out* is finite

Cyclic properties

ϕ = a state in which *in* can occur, can be reached an infinite number of times

$$\nu X \,.\, \mu Y \,.\, (\langle in \rangle \mathsf{true} \vee \langle - \rangle Y) \wedge ([-]X \wedge \langle - \rangle \mathsf{true})$$

ϕ = *in* occurs an infinite number of times

$$\nu X \,.\, \mu Y \,.\, [-in]Y \wedge [-]X \wedge \langle - \rangle \mathsf{true}$$

ϕ = *in* occurs an finite number of times

$$\mu X \,.\, \nu Y \,.\, [-in]Y \wedge [in]X$$

Cyclic properties

ϕ = a state in which *in* can occur, can be reached an infinite number of times

$$\nu X \,.\, \mu Y \,.\, (\langle in \rangle \mathsf{true} \vee \langle - \rangle Y) \;\wedge\; ([-]X \;\wedge\; \langle - \rangle \mathsf{true})$$

ϕ = *in* occurs an infinite number of times

$$\nu X \,.\, \mu Y \,.\, [-in]Y \wedge [-]X \wedge \langle - \rangle \mathsf{true}$$

ϕ = *in* occurs an finite number of times

$$\mu X \,.\, \nu Y \,.\, [-in]Y \wedge [in]X$$

Cyclic properties

ϕ = a state in which *in* can occur, can be reached an infinite number of times

$$\nu X \,.\, \mu Y \,.\, (\langle in \rangle \mathsf{true} \vee \langle - \rangle Y) \;\wedge\; ([-]X \;\wedge\; \langle - \rangle \mathsf{true})$$

ϕ = *in* occurs an infinite number of times

$$\nu X \,.\, \mu Y \,.\, [-in]Y \wedge [-]X \wedge \langle - \rangle \mathsf{true}$$

ϕ = *in* occurs an finite number of times

$$\mu X \,.\, \nu Y \,.\, [-in]Y \wedge [in]X$$