Introduction to modal logic

Luís S. Barbosa

HASLab - INESC TEC
Universidade do Minho
Braga, Portugal

January, 2012

Overview

The verification problem in architectural design:

- Given a process-oriented architectural specification (eg, in Archery or mCRL2)
- and the system's requirements as properties in a modal logic,
- a model checking algorithm decides whether requirements are valid in the architectural specification; sometimes, witnesses or counter examples can be provided

Which logic?

This lecture plan:

- Introduction to modal logic
- The modal μ-calculus (provided by MCRL2)

The language

Syntax

$$\phi \ ::= \ p \mid \mathsf{true} \mid \mathsf{false} \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \rightarrow \phi_2 \mid \langle m \rangle \phi \mid [m]\phi$$

where $p \in \mathrm{PROP}$ and $m \in \mathrm{MOD}$

Disjunction ($\vee$) and equivalence ($\leftrightarrow$) are defined by abbreviation. The signature of the basic modal language is determined by sets PROP of propositional symbols (typically assumed to be denumerably infinite) and MOD of modality symbols.

The language

Notes

- if there is only one modality in the signature (i.e., MOD is a singleton), write simply $\Diamond\phi$ and $\Box\phi$
- the language has some redundancy: in particular modal connectives are dual (as qualifiers are in first-order logic): $[m]\phi$ is equivalent to $\neg\langle m\rangle\neg\phi$
- define modal depth in a formula ϕ, denoted by $\mathrm{md}\,\phi$ as the maximum level of nesting of modalities in ϕ

The language

Semantics

A model for the language is a pair $\mathfrak{M} = \langle \mathbb{F}, V \rangle$, where

- $\mathfrak{F} = \langle W, \{R_m\}_{m \in \text{MOD}} \rangle$
  is a Kripke frame, ie, a non empty set W and a family of binary relations over W, one for each modality symbol $m \in \text{MOD}$. Elements of W are called points, states, worlds or simply vertices in the directed graphs corresponding to the modality symbols.
- $V : \text{PROP} \longrightarrow \mathcal{P}(W)$ is a valuation.

The language

Safistaction: for a model $\mathfrak{M}$ and a point w

$\mathfrak{M}, w \models \text{true}$		
$\mathfrak{M}, w \not\models \text{false}$		
$\mathfrak{M}, w \models p$	iff	$w \in V(p)$
$\mathfrak{M}, w \models \neg\phi$	iff	$\mathfrak{M}, w \not\models \phi$
$\mathfrak{M}, w \models \phi_1 \wedge \phi_2$	iff	$\mathfrak{M}, w \models \phi_1$ and $\mathfrak{M}, w \models \phi_2$
$\mathfrak{M}, w \models \phi_1 \to \phi_2$	iff	$\mathfrak{M}, w \not\models \phi_1$ or $\mathfrak{M}, w \models \phi_2$
$\mathfrak{M}, w \models \langle m \rangle \phi$	iff	there exists $v \in W$ st $wR_m v$ and $\mathfrak{M}, v \models \phi$
$\mathfrak{M}, w \models [m]\phi$	iff	for all $v \in W$ st $wR_m v$ and $\mathfrak{M}, v \models \phi$

The language

Safistaction

A formula ϕ is

- satisfiable in a model $\mathfrak{M}$ if it is satisfied at some point of $\mathfrak{M}$
- globally satisfied in $\mathfrak{M}$ ($\mathfrak{M} \models \phi$) if it is satisfied at all points in $\mathfrak{M}$
- valid ($\models \phi$) if it is globally satisfied in all models
- a semantic consequence of a set of formulas Γ ($\Gamma \models \phi$) if for all models $\mathfrak{M}$ and all points w, if $\mathfrak{M}, w \models \Gamma$ then $\mathfrak{M}, w \models \phi$

Examples

Temporal logic

- W is a set of instants
- there is a unique modality corresponding to the transitive closure of the next-time relation
- origin: Arthur Prior, an attempt to *deal with temporal information from the inside, capturing the situated nature of our experience and the context-dependent way we talk about it*

Examples

Process logic (Hennessy-Milner logic)

- $\mathrm{PROP} = \emptyset$
- $W = \mathbb{P}$ is a set of states, typically process terms, in a labelled transition system
- each subset $K \subseteq Act$ of actions generates a modality corresponding to transitions labelled by an element of K

Assuming the underlying LTS $\mathfrak{F} = \langle \mathbb{P}, \{p \xrightarrow{K} p' \mid K \subseteq Act\} \rangle$ as the modal frame, satisfaction is abbreviated as

$$p \models \langle K \rangle \phi \quad \text{iff} \quad \exists_{q \in \{p' \mid p \xrightarrow{a} p' \ \wedge\ a \in K\}} \cdot q \models \phi$$

$$p \models [K] \phi \quad \text{iff} \quad \forall_{q \in \{p' \mid p \xrightarrow{a} p' \ \wedge\ a \in K\}} \cdot q \models \phi$$

Examples

Process logic: The taxi network example

- $\phi_0 =$ *In a taxi network, a car can collect a passenger or be allocated by the Central to a pending service*
- $\phi_1 =$ *This applies only to cars already on service*
- $\phi_2 =$ *If a car is allocated to a service, it must first collect the passenger and then plan the route*
- $\phi_3 =$ *On detecting an emergence the taxi becomes inactive*
- $\phi_4 =$ *A car on service is not inactive*

Examples

Process logic: The taxi network example

- $\phi_0 = \langle \mathit{rec}, \mathit{alo} \rangle \mathrm{true}$
- $\phi_1 = [\mathit{onservice}] \langle \mathit{rec}, \mathit{alo} \rangle \mathrm{true}$ or
  $\phi_1 = [\mathit{onservice}] \phi_0$
- $\phi_2 = [\mathit{alo}] \langle \mathit{rec} \rangle \langle \mathit{plan} \rangle \mathrm{true}$
- $\phi_3 = [\mathit{sos}][-]\mathrm{false}$
- $\phi_4 = [\mathit{onservice}] \langle - \rangle \mathrm{true}$

Process logic: typical properties

- inevitability of a: $\langle - \rangle \mathsf{true} \wedge [-a]\mathsf{false}$
- progress: $\langle - \rangle \mathsf{true}$
- deadlock or termination: $[-]\mathsf{false}$
- what about

$$\langle - \rangle \mathsf{false} \quad \text{and} \quad [-]\mathsf{true} \quad ?$$

- satisfaction decided by unfolding the definition of $\models$: no need to compute the transition graph

The first order connection

The standard translation

Boxes and diamonds are essentially a macro notation to encode quantification over accessible states.

The standard translation to first-order logic expands these macros:

$$
\begin{aligned}
ST_x(p) &= P\,x \\
ST_x(\text{true}) &= \text{true} \\
ST_x(\text{false}) &= \text{false} \\
ST_x(\neg\phi) &= \neg ST_x(\phi) \\
ST_x(\phi_1 \wedge \phi_2) &= ST_x(\phi_1) \wedge ST_x(\phi_1) \\
ST_x(\phi_1 \rightarrow \phi_2) &= ST_x(\phi_1) \rightarrow ST_x(\phi_1) \\
ST_x(\langle m\rangle\phi) &= \langle \exists\ y\ \ ::\ \ (xR_m y\ \wedge\ ST_y(\phi))\rangle \\
ST_x([m]\phi) &= \langle \exists\ y\ \ ::\ \ (xR_m y\ \rightarrow\ ST_y(\phi))\rangle
\end{aligned}
$$

The first order connection

Lemma

For any ϕ, $\mathfrak{M}$ and point w in $\mathfrak{M}$,

$$\mathfrak{M}, w \models \phi \quad \text{iff} \quad \mathfrak{M} \models ST_x(\phi)[x \leftarrow w]$$

Note

Note how the (unique) free variable x in ST_x mirrors in first-order the internal perspective: assigning a value to x corresponds to evaluating the modal formula at a certain state.

Bisimulation

Definition

Given two models $\mathfrak{M} = \langle\langle W, R\rangle, V\rangle$ and $\mathfrak{M}' = \langle\langle W', R'\rangle, V'\rangle$, a bisimulation is a non-empty binary relation $S : W \longrightarrow W'$ st whenever wSw' one has that

- points w and w' satisfy the same propositional symbols
- if wRv, then there is a point v' in $\mathfrak{M}'$ st vSv' and $w'Rv'$ (zig)
- if $w'R'v'$, then there is a point v in $\mathfrak{M}$ st vSv' and wRv (zag)

Bisimulation

Definition

- Bisimulations can be used to expand or contract models (cf via tree unraveling and contraction)
- Bisimulation vs model constructions (disjoint union, generated submodels and bounded morphisms)

Note

Note the relation to the notion of bisimulation in transition systems, independently discovered by Park (1982) in Computer Science.

Invariance and definability

Lemma (bisimulation implies modal equivalence)

Given two models $\mathfrak{M} = \langle\langle W, R\rangle, V\rangle$ and $\mathfrak{M}' = \langle\langle W', R'\rangle, V'\rangle$, and a bisimulation $S : W \longrightarrow W'$, if two points w, w' are related by S, i.e., wSw', then w, w' satisfy the same basic modal formulas.

Applications

- to prove bisimulation failures
- to show the undefinability of some structural notions, e.g. irreflexivity is modally undefinable
- to show that typical model constructions are satisfaction preserving
- ...

Invariance and definability

The converse is true only for finite models:

Lemma (modal equivalence implies bisimulation)

if two points w, w' from two finite models $\mathfrak{M} = \langle\langle W, R\rangle, V\rangle$ and $\mathfrak{M}' = \langle\langle W', R'\rangle, V'\rangle$ satisfy the same modal formulas, then there is a bisimulation $S : W \longrightarrow W'$ such that wSw'.

Notes

- this could be repaired by passing to an infinitary modal language with arbitrary (countable) conjunctions and disjunctions.
- the situation is similar to what happens in first-order logic: first-order formulas are invariant for potential isomorphism, but the converse only holds in a weak formulation: two models are potentially isomorphic iff they have the same complete theory in the infinitary first-order logic.

Invariance and definability

Lemma (modal logic vs first-order)

The following are equivalent for all first- order formulas $\phi(x)$ in one free variable x:

1. $\phi(x)$ is invariant for bisimulation.
2. $\phi(x)$ is equivalent to the standard translation of a basic modal formula.

Therefore:

the basic modal language corresponds to the fragment of their first-order correspondence language that is invariant for bisimulation

Invariance and definability

- the basic modal language (interpreted over the class of all models) is computationally better behaved than the corresponding first-order language (interpreted over the same models)
- ... but clearly less expressive

	model checking	satisfiability
ML	PTIME	PSPACE-complete
FOL	PSPACE-complete	undecidable

What are the trade-offs? Can this better computational behaviour be lifted to more expressive modal logics?

Minimal modal logic

proof system **K**

- all formulas with the form of a propositional tautology (including formulas which contain modalities but are truth-functionally tautologous)
- all instances of the axiom schema:

$$\Box(\phi \to \psi) \to (\Box\phi \to \Box\psi)$$

- two proof rules:

$$\text{if } \vdash \phi \text{ and } \vdash \phi \to \psi \text{ then } \vdash \psi \quad (\text{modus ponens})$$

$$\text{if } \vdash \phi \text{ then } \vdash \Box\phi \quad (\text{generalization})$$

Normal modal logics

... are axiomatic extensions to **K**

- different applications of modal logic typically validate different modal axioms
- a normal modal logic is identified with the set of formulas it generates; it is said to be consistent if it does not contain all formulas. This identification immediately induces a lattice structure on the set of all such logics.

Normal modal logics

Modal axioms reflect properties of accessibility relations:

- transitive frames: $\Box\phi \to \Box\,\Box\,\phi$
- simple frames: $\Diamond\phi \to \Box\phi$
- frames consisting of isolated reflexive points: $\phi \leftrightarrow \Box\phi$
- frames consisting of isolated irreflexive points: $\Box$false

But there are classes of frames which are not modally definable, eg, connected, irreflexive, containing a isolated irreflexive point

Richer modal logics

can be obtained in different ways, e.g.

- axiomatic extensions
- introducing more complex satisfaction relations
- support novel semantic capabilities
- ...

Examples

- richer temporal logics
- hybrid logic
- modal μ-calculus

Temporal logics with $\mathcal{U}$ and $\mathcal{S}$

Until and Since

$$\begin{array}{lll} \mathfrak{M}, w \models \phi\,\mathcal{U}\,\psi & \text{iff} & \text{there exists } v \in W \text{ st } wRv \text{ and } \mathfrak{M}, v \models \psi, \\ & & \text{and for all u st } wRu \text{ and } uRv, \text{ one has } \mathfrak{M}, u \models \phi \\ \mathfrak{M}, w \models \phi\,\mathcal{S}\,\psi & \text{iff} & \text{there exists } v \in W \text{ st } vRw \text{ and } \mathfrak{M}, v \models \psi, \\ & & \text{and for all u st } vRu \text{ and } uRw, \text{ one has } \mathfrak{M}, u \models \phi \end{array}$$

- note the $\exists\forall$ qualification pattern: these operators are neither diamonds nor boxes.
- helpful to express guarantee properties, e.g., some event will happen, and a certain condition will hold until then
- ... a plethora of temporal logics: LTL, CTL, CTL*

Hybrid logic

Motivation

Add the possibility of naming points and reason about their identity

Compare:

$$\Diamond(r \wedge p) \;\wedge\; \Diamond(r \wedge q) \;\rightarrow\; \Diamond(p \wedge q)$$

with

$$\Diamond(i \wedge p) \;\wedge\; \Diamond(i \wedge q) \;\rightarrow\; \Diamond(p \wedge q)$$

for $i \in N$ (a nominal)

Hybrid logic

The $@_i$ operator

$$\mathfrak{M}, w \models @_i\phi \qquad \text{iff} \qquad \mathfrak{M}, u \models \phi \text{ and } u \text{ is the state denoted by } i$$

Standard translation to first-order

$$ST_x(i) = (x = i)$$
$$ST_x(@_i\phi) = ST_i(\phi)(x = i)$$

i.e., logic corresponds to a first-order language enriched with constants and equality.

Hybrid logic

Increased frame definability

- irreflexivity: $i \rightarrow \neg\Diamond i$
- asymmetry: $i \rightarrow \neg\Diamond\Diamond i$
- antisymmetry: $i \rightarrow \Box(\Diamond i \rightarrow i)$
- trichotomy: $@_j \Diamond i \ \vee \ @_i j \ \vee \ @_i \Diamond j$

Hybrid logic

Summing up

- basic hybrid logic is a simple notation for capturing the bisimulation-invariant fragment of first-order logic with constants and equality, i.e., a mechanism for equality reasoning in propositional modal logic.
- comes cheap: up to a polynomial, the complexity of the resulting decision problem is no worse than for the basic modal language
- current use in HASLab for reasoning about architectural reconfigurations (Madeira,Martins,Barbosa paper at SEFM'11)

Modal μ-calculus

Intuition

- look at modal formulas as set-theoretic combinators
- introduce mechanisms to specify their fixed points
- Introduced as a generalisation of Hennessy-Milner logic for processes to capture enduring properties.

References

- Original reference: *Results on the propositional μ-calculus*, D. Kozen, 1983.
- Introductory text: *Modal and temporal logics for processes*, C. Stirling, 1996

Revisiting Hennessy-Milner logic

... propositional logic with action modalities

$$\phi \;::=\; \mathsf{true} \;|\; \mathsf{false} \;|\; \neg\phi \;|\; \phi \wedge \phi \;|\; \phi \vee \phi \;|\; \langle a\rangle\phi \;|\; [a]\phi$$

Exercise: prove that

$$\begin{aligned}
\neg\langle a\rangle\phi &= [a]\neg\phi \\
\neg[a]\phi &= \langle a\rangle\neg\phi \\
\langle a\rangle\mathsf{false} &= \mathsf{false} \\
[a]\mathsf{true} &= \mathsf{true} \\
\langle a\rangle(\phi \vee \psi) &= \langle a\rangle\phi \vee \langle a\rangle\psi \\
[a](\phi \wedge \psi) &= [a]\phi \wedge [a]\psi \\
\langle a\rangle\phi \wedge [a]\psi &\Rightarrow \langle a\rangle(\phi \wedge \psi)
\end{aligned}$$

Revisiting Hennessy-Milner logic

Action formulas

$$\alpha \;::=\; a_1 \mid \cdots \mid a_n \;\mid\; \text{true} \;\mid\; \text{false} \;\mid\; -\alpha \;\mid\; \alpha \cup \alpha \;\mid\; \alpha \cap \alpha$$

where

- $a_1 \mid \cdots \mid a_n$ is a set with this single multiaction
- true (universe), false (empty set)
- $-\alpha$ is the set complement

Modalities with action formulas:

$$\langle \alpha \rangle \phi \;=\; \bigvee_{a \in \alpha} \langle a \rangle \phi \qquad [\alpha]\phi \;=\; \bigwedge_{a \in \alpha} [a]\phi$$

Revisiting Hennessy-Milner logic

Adding regular expressions

ie, with regular expressions within modalities

$$\rho \ ::= \epsilon \mid \alpha \mid \rho.\rho \mid \rho + \rho \mid \rho^* \mid \rho^+$$

where

- α is an action formula and ϵ is the empty word
- concatenation $\rho.\rho$, choice $\rho + \rho$ and closures ρ^* and ρ^+

Exercise: prove the following laws

$$\begin{aligned}
\langle \rho_1 + \rho_2 \rangle \phi &= \langle \rho_1 \rangle \phi \vee \langle \rho_2 \rangle \phi \\
[\rho_1 + \rho_2] \phi &= [\rho_1] \phi \wedge [\rho_2] \phi \\
\langle \rho_1 . \rho_2 \rangle \phi &= \langle \rho_1 \rangle \langle \rho_2 \rangle \phi \\
[\rho_1 . \rho_2] \phi &= [\rho_1][\rho_2] \phi
\end{aligned}$$

Revisiting Hennessy-Milner logic

Examples of properties

- $\langle \epsilon \rangle \phi \;=\; [\epsilon]\phi \;=\; \phi$
- $\langle a.a.b \rangle \phi \;=\; \langle a \rangle \langle a \rangle \langle b \rangle \phi$
- $\langle a.b + g.d \rangle \phi$

Safety

- $[\mathrm{true}^*]\phi$
- it is impossible to do two consecutive enter actions without a leave action in between:
  $[\mathrm{true}^*.enter.-leave^*.enter]\mathrm{false}$
- absence of deadlock:
  $[\mathrm{true}^*]\langle \mathrm{true} \rangle \mathrm{true}$

Revisiting Hennessy-Milner logic

Examples of properties

Liveness

- $\langle \mathsf{true}^* \rangle \phi$
- after sending a message, it can eventually be received:
  $[\mathit{send}]\langle \mathsf{true}^* . \mathit{receive} \rangle \mathsf{true}$
- after a send a receive is possible as long as an exception does not happen:
  $[\mathit{send}. - \mathit{excp}^*]\langle \mathsf{true}^* . \mathit{receive} \rangle \mathsf{true}$

The modal μ-calculus

- modalities with regular expressions are not enough in general
- ... but correspond to a subset of the modal μ-calculus [Kozen83]

Add explicit minimal/maximal fixed point operators to Hennessy-Milner logic

$$\phi \ ::= \ X \mid \mathsf{true} \mid \mathsf{false} \mid \neg\phi \mid \phi\wedge\phi \mid \phi\vee\phi \mid \phi\rightarrow\phi \mid \langle a\rangle\phi \mid [a]\phi \mid \mu X\,.\,\phi \mid \nu X\,.\,\phi$$

The modal μ-calculus

Example

$$\phi \;=\; \text{a taxi eventually returns to its Central}$$

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

The modal μ-calculus

The modal μ-calculus (intuition)

- $\mu X \,.\, \phi$ is valid for all those states in the smallest set X that satisfies the equation $X = \phi$ (finite paths, liveness)
- $\nu X \,.\, \phi$ is valid for the states in the largest set X that satisfies the equation $X = \phi$ (infinite paths, safety)

Warning

In order to be sure that a fixed point exists, X must occur positively in the formula, ie preceded by an even number of negations.

Temporal properties as limits

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 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

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

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

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

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

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

Therefore, its least solution is

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

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

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

(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

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

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

  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:

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

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

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

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

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

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

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

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 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

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

Variant:

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

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

In general:

- weak safety:

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

- weak safety, for $K = Act$:

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

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

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

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

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

(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?)

Safety and liveness

- weak liveness:

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

- strong safety

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

making $\psi = \neg\phi$ 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

$$\neg(\mu X \,.\, \phi) = \nu X \,.\, \neg\phi$$
$$\neg(\nu X \,.\, \phi) = \mu X \,.\, \neg\phi$$

Example:

- divergence:

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

- convergence (= all non observable behaviour is finite)

$$\neg(\nu X \,.\, \langle\tau\rangle X) \;=\; \mu X \,.\, \neg(\langle\tau\rangle X) \;=\; \mu X \,.\, [\tau] X$$

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:

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

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

- action-oriented

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

  (action *reg* occurs)

  Its dual is the action-oriented weak safety:

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

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:

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

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

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

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

Conditional properties

$\phi_1 \ =$
After collecting a passenger (*icr*), the taxi drops him at destination (*fcr*)
Second part of ϕ_1 is strong liveness:

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

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

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

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

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

Conditional properties

$\phi_1 \;=$
After collecting a passenger (*icr*), the taxi drops him at destination (*fcr*)
Second part of ϕ_1 is strong liveness:

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

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

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

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

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

Conditional properties

The previous example is conditional liveness but one can also have

- conditional safety:

$$\nu Y . (\neg\phi \vee (\phi \wedge \nu X . \psi \wedge [-]X)) \wedge [-]Y$$

(whenever ϕ holds, ψ cannot cease to hold)

Cyclic properties

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

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

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

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

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

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

Back to mCRL2

Laws

$$\mu X . \phi \Rightarrow \nu X . \phi$$

and self-duals:

$$\neg\mu X . \phi = \nu X . \neg\phi$$
$$\neg\nu X . \phi = \mu X . \neg\phi$$

Translation of regular formulas with closure

$$\langle R^* \rangle \phi = \mu X . \langle R \rangle X \vee \phi$$
$$[R^*]\phi = \nu X . [R]X \wedge \phi$$
$$\langle R^+ \rangle \phi = \langle R \rangle \langle R^* \rangle \phi$$
$$[R^+]\phi = [R][R^*]\phi$$

Example: The dining philosophers problem

Formulas to verify Demo

- No deadlock (every philosopher holds a left fork and waits for a right fork (or vice versa):

```
[true*]<true>true
```

- No starvation (a philosopher cannot acquire 2 forks):

```
forall p:Phil.  [true*.!eat(p)*] <!eat(p)*.eat(p)>true
```

- A philosopher can only eat for a finite consecutive amount of time:

```
forall p:Phil.  nu X. mu Y. [eat(p)]Y && [!eat(p)]X
```

- there is no starvation: for all reachable states it should be possible to eventually perform an `eat(p)` for each possible value of `p:Phil`.

```
[true*](forall p:Phil.  mu Y. ([!eat(p)]Y && <true>true))
```