5. Dynamic Logic & Verification

David Pereira José Proença

RAMDE – Requirements and Model-driven Engineering 2021/22

CISTER – ISEP
Porto, Portugal

`https://cister-labs.github.io/ramde2122`

Recall: What’s in a logic?

A logic

A language

i.e. a collection of well-formed expressions to which meaning can be assigned.

A semantics

describing how language expressions are interpreted as statements about something.

A deductive system

i.e. a collection of rules to derive in a purely syntactic way facts and relationships among semantic objects described in the language.

Note

- a purely syntactic approach (up to the 1940's; the sacred form)
- a model theoretic approach (A. Tarski legacy)

Semantic reasoning: models

- sentences
- models & satisfaction: $\mathfrak{M} \models \phi$
- validity: $\models \phi$ (ϕ is satisfied in every possible structure)
- logical consequence: $\Phi \models \phi$ (ϕ is satisfied in every model of Φ)
- theory: $Th\,\Phi$ (set of logical consequences of a set of sentences Φ)

Syntactic reasoning: deductive systems

Deductive systems $\vdash$

- sequents
- Hilbert systems
- natural deduction
- tableaux systems
- resolution
- $\cdots$

- derivation and proof
- deductive consequence: $\Phi \vdash \phi$
- theorem: $\vdash \phi$

Soundness & completeness

- A deductive system $\vdash$ is sound wrt a semantics $\models$ if for all sentences ϕ

$$\vdash \phi \implies \models \phi$$

(every theorem is valid)

- $\cdots$ complete ...

$$\models \phi \implies \vdash \phi$$

(every valid sentence is a theorem)

Consistency & refutability

For logics with negation and a conjunction operator

- A sentence ϕ is refutable if $\neg\phi$ is a theorem (i.e. $\vdash \neg\phi$)
- A set of sentences Φ is refutable if some finite conjunction of elements in Φ is refutable
- ϕ or Φ is consistent if it is not refutable.

Examples

$$\mathfrak{M} \models \phi$$

- Propositional logic (logic of uninterpreted assertions; models are truth assignments)
- Equational logic (formalises equational reasoning; models are algebras)
- First-order logic (logic of predicates and quatification over structures; models are relational structures)
- **Modal logics**
- ...

Modal Logic

Modal logic (from P. Blackburn, 2007)

Over the years modal logic has been applied in many different ways. It has been used as a tool for reasoning about time, beliefs, computational systems, necessity and possibility, and much else besides.

These applications, though diverse, have something important in common: the key ideas they employ (flows of time, relations between epistemic alternatives, transitions between computational states, networks of possible worlds) can all be represented as simple graph-like structures.

Modal logics are

- tools to talk about relational, or graph-like structures.
- fragments of classical ones, with restricted forms of quantification ...
- ... which tend to be decidable and described in a pointfree notations.

Basic Modal Logic

Syntax

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

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

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 quantifiers are in first-order logic): $[m]\,\phi$ is equivalent to $\neg\langle m\rangle\,\neg\phi$

Example

Models as LTSs over Act.

$MOD = Act$ (sets of actions)

$\langle a\rangle\,\phi$ can be read as "*it must observe a, and* ϕ *must hold after that.*"

$[a]\,\phi$ can be read as "*if it observes a, then* ϕ *must hold after that.*"

Semantics

$\mathfrak{M}, s \models \phi$ – **what does it mean?**

Model definition

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

- $\mathfrak{L} = \langle S, \mathrm{MOD}, \longrightarrow \rangle$ is an LTS:
  - S is a non-empty set of states (or points)
  - MOD are the labels consisting of modality symbols
  - $\longrightarrow \subseteq S \times \mathrm{MOD} \times S$ is the transition relation
- $V : \mathrm{PROP} \longrightarrow \mathcal{P}(S)$ is a valuation.

When MOD = 1

- $\Diamond\phi$ and $\Box\phi$ instead of $\langle\cdot\rangle\,\phi$ and $[\cdot]\,\phi$
- $\mathfrak{L} = \langle S, \longrightarrow \rangle$ instead of $\mathfrak{L} = \langle S, \mathrm{MOD}, \longrightarrow \rangle$
- $\longrightarrow \subseteq S \times S$ instead of $\longrightarrow \subseteq S \times \mathrm{MOD} \times S$

Semantics

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

$$
\begin{array}{lll}
\mathfrak{M}, s \models \text{true} & & \\
\mathfrak{M}, s \not\models \text{false} & & \\
\mathfrak{M}, s \models p & \text{iff} & s \in V(p) \\
\mathfrak{M}, s \models \neg\phi & \text{iff} & \mathfrak{M}, s \not\models \phi \\
\mathfrak{M}, s \models \phi_1 \wedge \phi_2 & \text{iff} & \mathfrak{M}, s \models \phi_1 \;\text{ and }\; \mathfrak{M}, s \models \phi_2 \\
\mathfrak{M}, s \models \phi_1 \rightarrow \phi_2 & \text{iff} & \mathfrak{M}, s \not\models \phi_1 \;\text{ or }\; \mathfrak{M}, s \models \phi_2 \\
\mathfrak{M}, s \models \langle m \rangle\, \phi & \text{iff} & \text{there exists } v \in S \text{ st } s \xrightarrow{m} v \text{ and } \mathfrak{M}, v \models \phi \\
\mathfrak{M}, s \models [m]\, \phi & \text{iff} & \text{for all } v \in S \text{ st } s \xrightarrow{m} v \text{ and } \mathfrak{M}, v \models \phi
\end{array}
$$

Semantics

Satisfaction

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 s, if $\mathfrak{M}, s \models \Gamma$ then $\mathfrak{M}, s \models \phi$

Example: Hennessy-Milner logic

Process logic (Hennessy-Milner logic)

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

Assuming the underlying LTS $\mathfrak{L} = \langle \mathcal{P}, \mathbb{P}(Act), \{\langle p, K, p' \rangle \mid K \subseteq Act\} \rangle$ as the model's LTS, satisfaction is abbreviated as

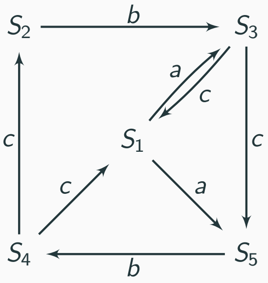
$$\begin{aligned} p \models \langle K \rangle \phi \quad & \text{iff} \quad \exists_{q \in \{p' \mid p \xrightarrow{a} p' \ \wedge \ a \in K\}} \,.\, q \models \phi \\ p \models [K] \phi \quad & \text{iff} \quad \forall_{q \in \{p' \mid p \xrightarrow{a} p' \ \wedge \ a \in K\}} \,.\, q \models \phi \end{aligned}$$

Example: Hennessy-Milner logic

Process Logic Syntax

$$\phi \;::=\; \text{true} \mid \text{false} \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \rightarrow \phi_2 \mid \langle K \rangle\, \phi \mid [K]\, \phi$$

where $K \subseteq Act$



Ex. 5.1: Prove:

1. $S_1 \models [a, b, c]\,(\langle b, c\rangle\, tt)$
2. $S_2 \models [a]\,(\langle b\rangle\, tt \wedge \langle c\rangle\, tt)$
3. $S_1 \not\models [a]\,(\langle b\rangle\, tt \wedge \langle c\rangle\, tt)$
4. $S_2 \models [b]\,[c]\,(\langle a\rangle\, tt \vee \langle b\rangle\, tt)$
5. $S_1 \models [b]\,[c]\,(\langle a\rangle\, tt \vee \langle b\rangle\, tt)$
6. $S_1 \models [a, b]\,\langle b, c\rangle\,(\langle a\rangle\, tt)$

Examples II

$(P, <)$ a strict partial order with infimum 0

I.e., $P = \{0, a, b, c, \ldots\}$,

$a \rightarrow b$ means $a < b$,

$a < b$ and $b < c$ implies $a < c$

$0 < x$, for any $x \neq 0$

there are no loops

some elements may not be comparable

- $P, x \models \Box\text{false}$ if x is a maximal element of P
- $P, 0 \models \Diamond \Box \mathit{false}$ iff ...
- $P, 0 \models \Box\Diamond \Box \mathit{false}$ iff ...

Examples III

Temporal logic

- $\langle T, < \rangle$ where T is a set of time points (instants, execution states , ...) and $<$ is the earlier than relation on T.
- Thus, $\Box\varphi$ (respectively, $\Diamond\varphi$) means that φ holds in all (respectively, some) time points.

Examples IV

Epistemic logic (J. Hintikka, 1962)

- W is a set of agents
- $\alpha \models [K_i]\ \phi$ means that agent i always knows that ϕ is true.
- $\alpha \models \langle K_i \rangle\ \phi$ means that agent i can reach a state where he knows ϕ.
- $\alpha \models (\neg [K_i]\ \phi) \wedge (\neg [K_i]\ \neg \phi)$ means that agent i does not know whether ϕ is true or not.

Many variations exist, modelling knowledge and believes, knowledge of who knows what, distributed knowledge, etc.

Examples V

Deontic logic (G.H. von Wright, 1951)

- Obligations and permissions: must and can do.
- $\alpha \models \Box\, \phi$ means ϕ is obligatory.
- $\alpha \models \Diamond\, \phi$ means ϕ is a possibility.

Each logic accepts a different set of *principles* or *rules* (with variations), that makes their interpretation different.

Exercise

Ex. 5.2: Express the properties in Process Logic

- inevitability of a:
- progress:
- deadlock or termination:

Ex. 5.3: What does this mean?

1. $\langle - \rangle$ false
2. $[-]$ true

"$-$" stands for Act, and "$-x$" abbreviates $Act - \{x\}$

Recall syntax

$$\begin{aligned}
\phi \; ::= \; & \text{true} \\
\mid\; & \text{false} \\
\mid\; & \neg\phi \\
\mid\; & \phi_1 \wedge \phi_2 \\
\mid\; & \phi_1 \rightarrow \phi_2 \\
\mid\; & \langle K \rangle\, \phi \\
\mid\; & [K]\, \phi
\end{aligned}$$

where $K \subseteq Act$

Exercise

Ex. 5.2: Express the properties in Process Logic

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

Ex. 5.3: What does this mean?

1. $\langle - \rangle\, \mathsf{false}$
2. $[-]\, \mathsf{true}$

"$-$" stands for *Act*, and "$-x$" abbreviates $Act - \{x\}$

Recall syntax

$$\begin{aligned} \phi \;::=\; & \mathsf{true} \\ \mid\; & \mathsf{false} \\ \mid\; & \neg\phi \\ \mid\; & \phi_1 \wedge \phi_2 \\ \mid\; & \phi_1 \rightarrow \phi_2 \\ \mid\; & \langle K \rangle\, \phi \\ \mid\; & [K]\, \phi \end{aligned}$$

where $K \subseteq Act$

Express the following using Process Logic

Ex. 5.4: Coffee-machine

1. The user can have tea or coffee.
2. The user can have tea but not coffee.
3. The user can have tea after having 2 consecutive coffees.

Ex. 5.5: a's and b's

1. It is possible to do a after 3 b's, but not more than 1 a.
2. It must be possible to do a after [doing a and then b].
3. After doing a and then b, it is not possible to do a.

Express the following using Process Logic

Ex. 5.6: Taxi network

- $\phi_0 =$ *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*

Process Logic + regular expressions

Process Logic Syntax

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

where E is a regular expression over Act

More expressive than Process Logic. Used by mCRL2.

Examples

- "$\langle a.b.c \rangle$ true" means "$\langle a \rangle \langle b \rangle \langle c \rangle$ true"
- "$[a.b.c]$ false" means "$[a][b][c]$ false"
- "$\langle a^{*}.b \rangle$ true" means that b can be taken after some number of a's.
- "$\langle -^{*}.a \rangle$ true" means that a can eventually be taken
- "$[-^{*}]\langle a + b \rangle$ true" means it is always possible to do a or b

Exercises

Ex. 5.7: What does this mean?

1. $\langle - \rangle\, \mathsf{true}$
2. $[-^*]\langle - \rangle\, \mathsf{true}$
3. $[-^*.a]\langle b \rangle\, \mathsf{true}$
4. $\langle -^*.send \rangle$
   $\langle (-send)^*.recv \rangle\, \mathsf{true}$

Ex. 5.8: Express using logic

1. The user can only have coffee after the coffee button is pressed.
2. The used must have coffee after the coffee button is pressed.
3. It is always possible to turn off the coffee machine.
4. It is always possible to reach a state where the coffee machine can be turned off.
5. It is never possible to add chocolate right after pressing the *latte button*.

Bisimulation and modal equivalence

Bisimulation (of models)

Definition

Given two models $\mathfrak{M} = \langle \mathfrak{L}, V \rangle$ and $\mathfrak{M}' = \langle \mathfrak{L}', V' \rangle$, a bisimulation of $\mathfrak{L}$ and $\mathfrak{L}'$ is also a bisimulation of $\mathfrak{M}$ and $\mathfrak{M}'$ if,

$$\text{whenever } s \; R \; s', \text{ then } V(s) = V'(s')$$

Invariance and definability

Lemma (invariance: bisimulation implies modal equivalence)

Given two models $\mathfrak{M}$ and $\mathfrak{M}'$, and a bisimulation R between their states:

if two states s, s' are related by R (i.e. sRs'),

then s, s' satisfy the same basic modal formulas.

(i.e., for all ϕ: $\mathfrak{M}, s \models \phi \;\Leftrightarrow\; \mathfrak{M}', s' \models \phi$)

Hence

Given 2 models $\mathfrak{M}$ and $\mathfrak{M}'$, if you can find ϕ such that

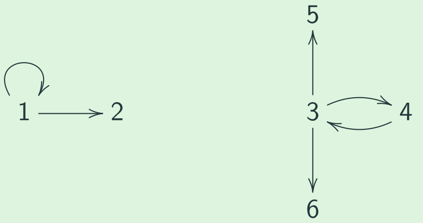
$$\mathfrak{M} \models \phi \text{ and } \mathfrak{M}' \models \phi$$

then they are NOT bisimilar.

Exercise

Ex. 5.9: Bisimilarity and modal equivalence

Consider the following transition systems:



Give a modal formula that can be satisfied at point 1 but not at 3.

Richer modal logics

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

$$\begin{aligned}
\mathfrak{M}, w \models \phi \,\mathcal{U}\, \psi \quad & \text{iff} \quad \text{there exists } v \text{ st } w \leq v \text{ and } \mathfrak{M}, v \models \psi, \text{ and} \\
& \qquad \text{for all } u \text{ st } w \leq u < v, \text{ one has } \mathfrak{M}, u \models \phi \\
\mathfrak{M}, w \models \phi \,\mathcal{S}\, \psi \quad & \text{iff} \quad \text{there exists } v \text{ st } v \leq w \text{ and } \mathfrak{M}, v \models \psi, \text{ and} \\
& \qquad \text{for all } u \text{ st } v < u \leq w, \text{ one has } \mathfrak{M}, u \models \phi
\end{aligned}$$

- Defined for temporal frames $\langle T, < \rangle$ (transitive, asymmetric).
- note the $\exists\forall$ qualification pattern: these operators are neither diamonds nor boxes.
- More general definition for other frames – it becomes more expressive than modal logics.

Exercise

Temporal logics - rewrite using $\mathcal{U}$

- $\Diamond\psi =$
- $\Box\psi =$

Exercise

Temporal logics - rewrite using $\mathcal{U}$

- $\Diamond\psi = tt\,\mathcal{U}\,\psi$
- $\Box\psi =$

Exercise

Temporal logics - rewrite using $\mathcal{U}$

- $\Diamond\psi = tt\,\mathcal{U}\,\psi$
- $\Box\psi = \neg(\Diamond\neg\psi) = \neg(tt\,\mathcal{U}\,\neg\psi)$

Linear temporal logic (LTL)

$$\phi \;:=\; \text{true} \mid p \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \bigcirc\phi \mid \phi_1\,\mathcal{U}\,\phi_2$$

mutual exclusion	$\Box(\neg c_1 \vee \neg c_2)$
liveness	$\Box\Diamond c_1 \wedge \Box\Diamond c_2$
starvation freedom	$(\Box\Diamond w_1 \rightarrow \Box\Diamond c_1) \wedge (\Box\Diamond w_1 \rightarrow \Box\Diamond c_1)$
progress	$\Box(w_1 \rightarrow \Diamond c_1)$
weak fairness	$\Diamond\Box w_1 \rightarrow \Box\Diamond c_1$
eventually forever	$\Diamond\Box w_1$

- First temporal logic to reason about reactive systems [Pnueli, 1977]
- Formulas are interpreted over execution paths
- Express linear-time properties

Computational tree logic (CTL, CTL*)

state formulas to express properties of a state:

$$\Phi \;:=\; \text{true} \mid \Phi \wedge \Phi \mid \neg\Phi \mid \exists\psi \mid \forall\psi$$

path formulas to express properties of a path:

$$\psi \;:=\; \bigcirc\Phi \mid \Phi \,\mathcal{U}\, \Psi$$

mutual exclusion	$\forall \square (\neg c_1 \vee \neg c_2)$
liveness	$\forall \square \forall \lozenge c_1 \wedge \forall \square \forall \lozenge c_2$
order	$\forall \square (c_1 \vee \forall \bigcirc c_2)$

- Branching time structure encode transitive, irreflexive but not necessarily linear flows of time
- flows are trees: past linear; branching future

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 $i \in \mathsf{NOM}$ (a nominal)

Syntax

$$\phi \ ::= \ \ldots \mid p \mid \langle m \rangle \phi \mid [m] \phi \mid i \mid @_i \phi$$

where $p \in \mathsf{PROP}$ and $m \in \mathsf{MOD}$ and $i \in \mathsf{NOM}$

Hybrid logic

Nominals i

- Are special propositional symbols that hold exactly on one state (the state they name)
- In a model the valuation V is extended from

$$V : \mathrm{PROP} \longrightarrow \mathcal{P}(W)$$

to

$$V : \mathrm{PROP} \longrightarrow \mathcal{P}(W) \quad \text{and} \quad V : \mathrm{NOM} \longrightarrow W$$

where NOM is the set of nominals in the model

- Satisfaction:

$$\mathfrak{M}, w \models i \qquad\qquad \text{iff } w = V(i)$$

Hybrid logic

The $@_i$ operator

$$
\begin{array}{lll}
\mathfrak{M}, s \models \text{true} & & \\
\mathfrak{M}, s \not\models \text{false} & & \\
\mathfrak{M}, s \models p & \text{iff} & s \in V(p) \\
\mathfrak{M}, s \models \neg\phi & \text{iff} & \mathfrak{M}, s \not\models \phi \\
\mathfrak{M}, s \models \phi_1 \wedge \phi_2 & \text{iff} & \mathfrak{M}, s \models \phi_1 \;\text{ and }\; \mathfrak{M}, s \models \phi_2 \\
\mathfrak{M}, s \models \phi_1 \rightarrow \phi_2 & \text{iff} & \mathfrak{M}, s \not\models \phi_1 \;\text{ or }\; \mathfrak{M}, s \models \phi_2 \\
\mathfrak{M}, s \models \langle m \rangle\, \phi & \text{iff} & \text{there exists } v \in S \text{ st } s \xrightarrow{m} v \text{ and } \mathfrak{M}, v \models \phi \\
\mathfrak{M}, s \models [m]\, \phi & \text{iff} & \text{for all } v \in S \text{ st } s \xrightarrow{m} v \text{ and } \mathfrak{M}, v \models \phi \\
 & & \\
\mathfrak{M}, s \models @_i\phi & \text{iff} & \mathfrak{M}, u \models \phi \text{ and } u = V(i) \\
 & & [u \text{ is the state denoted by } i]
\end{array}
$$

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