Modal logics[1]

Carles Noguera i Clofent

Institute of Information Theory and Automation
Academy of Sciences of the Czech Republic
Prague, Czech Republic

[1] An acknowledgment is due to Félix Bou for his help in preparing these slides.

Outline

Modalities – 1

Modal logics are logics with modalities.

A modality is a connective of a special kind.

Connectives like $\neg, \rightarrow, \&, \wedge, \vee$ are truth-functional:

- the truth value of $\neg\varphi$ is computed in terms of the truth value of φ
- the truth value of $\varphi \rightarrow \psi$ is computed in terms of the truth value of φ and ψ
- ...

Modalities are not truth-functional.

Modalities – 2

Example (Unary modalities)

- $\Box\varphi$: "it is necessary that φ"
- $\Diamond\varphi$: "it is possible that φ"
- $\mathrm{G}\varphi$: "always in the future φ will be true"
- $\mathrm{F}\varphi$: "at some point in the future φ will be true"
- $\mathrm{P}\varphi$: "at some point in the past φ was true"
- $\mathrm{K}_i\varphi$: "agent i knows that φ"
- $\mathrm{B}_i\varphi$: "agent i believes that φ"
- $[\texttt{prog}]\varphi$: "after any execution of the program $\texttt{prog}$, the state satisfies φ"
- $\langle\texttt{prog}\rangle\varphi$: "there is an execution of the program $\texttt{prog}$ which results in a state satisfying φ"

Basic modal logic: language

- Denumerable set of atomic propositions (variables): $AP = \{p_1, p_2, \ldots\}$
- Connectives of classical logic: $\neg$ and $\rightarrow$ ($\wedge$, $\vee$, $\leftrightarrow$, $\overline{1}$, and $\overline{0}$ are definable)

$$\varphi \wedge \psi = \neg(\varphi \rightarrow \neg\psi)$$
$$\varphi \vee \psi = \neg\varphi \rightarrow \psi$$
$$\varphi \leftrightarrow \psi = (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$
$$\overline{1} = p \rightarrow p$$
$$\overline{0} = \neg\overline{1}$$

- A primitive unary modality: $\Box$ (necessity)
- A defined dual modality: $\Diamond\varphi = \neg\Box\neg\varphi$ (possibility)

Basic modal logic: semantics – 1

Definition

A Kripke structure is a triple $M = \langle W, R, V \rangle$ where:

- $W \neq \emptyset$ (possible worlds)
- $R \subseteq W \times W$ (accessibility relation)
- $V : AP \times W \to \{0, 1\}$ (classical valuation function)

Therefore, a Kripke structure is a graph $\langle W, R \rangle$ with a funtion V telling in each vertice what propositions are true.

Basic modal logic: semantics – 2

Given a Kripke structure $M = \langle W, R, V \rangle$ and a possible world $w \in W$, we define:

$$
\begin{array}{lll}
\langle M, w \rangle \models p & \text{iff} & V(p, w) = 1 \\
\langle M, w \rangle \models \neg\varphi & \text{iff} & \langle M, w \rangle \not\models \varphi \\
\langle M, w \rangle \models \varphi \to \psi & \text{iff} & \langle M, w \rangle \not\models \varphi \text{ or } \langle M, w \rangle \models \psi \\
\langle M, w \rangle \models \Box\varphi & \text{iff} & \langle M, w' \rangle \models \varphi \text{ for each } w' \text{ accessible} \\
 & & \text{from } w \text{ (i.e. } \langle w, w' \rangle \in R)
\end{array}
$$

- φ is true in M if $\langle M, w \rangle \models \varphi$ for each $w \in W$ (in symbols: $M \models \varphi$)
- Semantical consequence: $\Gamma \models_{\mathrm{K}} \varphi$ iff
  for every Kripke structure M, if $M \models \Gamma$ then $M \models \varphi$

Basic modal logic: semantics – 3

Example

- $\Box p \to \Box p$ is a tautology
- $\Box(p \to p)$ is a tautology
- $\Box p \to p$ is not a tautology

Basic modal logic: proof system

Take any axiomatic system for classical logic, for instance:

(C1) $\varphi \to (\psi \to \varphi)$

(C2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

(C3) $(\neg\psi \to \neg\varphi) \to ((\neg\psi \to \varphi) \to \psi)$

(MP) from φ and $\varphi \to \psi$ infer ψ

and add the following axiom and rule:

(K) $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$

(Nec) from φ infer $\Box\varphi$ (necessitation rule)

Let $\vdash_{\mathrm{K}}$ be the corresponding provability relation.

Basic modal logic: completeness theorem

Theorem

Let Γ be a set of formulae and φ be a formula. Then:

$$\Gamma \vdash_{\mathbf{K}} \varphi \quad \textit{iff} \quad \Gamma \models_{\mathbf{K}} \varphi$$

Important axiomatic extensions – 1

Consider the following formulae:

(M) $\Box\varphi \to \varphi$

(B) $\varphi \to \Box\Diamond\varphi$

(D) $\Box\varphi \to \Diamond\varphi$

(4) $\Box\varphi \to \Box\Box\varphi$

(5) $\Diamond\varphi \to \Box\Diamond\varphi$

We can define many axiomatic extensions of K:

$\mathrm{M} = \mathrm{K} + (\mathrm{M})$ $\quad$ $\mathrm{D} = \mathrm{K} + (\mathrm{D})$ $\quad$ $\mathrm{KB} = \mathrm{K} + (\mathrm{B})$

$\mathrm{K4} = \mathrm{K} + (4)$ $\quad$ $\mathrm{K5} = \mathrm{K} + (5)$ $\quad$ $\mathrm{K45} = \mathrm{K} + (4) + (5)$

$\mathrm{D4} = \mathrm{D} + (4)$ $\quad$ $\mathrm{D5} = \mathrm{D} + (5)$ $\quad$ $\mathrm{D45} = \mathrm{D} + (4) + (5)$

$\mathrm{KB5} = \mathrm{KB} + (5)$ $\quad$ $\mathrm{DB} = \mathrm{D} + (\mathrm{B})$ $\quad$ $\mathrm{B} = \mathrm{M} + (\mathrm{B})$

$\mathrm{S4} = \mathrm{M} + (4)$ $\quad$ $\mathrm{S5} = \mathrm{M} + (5)$

Important axiomatic extensions – 2

The additional axioms are chosen according to the properties of the modality one wants to capture. For example:

- $\Box\varphi \to \varphi$: "if I know φ, then φ is true" (epistemic logic); "if φ is provable, then φ is true" (provability logic)
- $\Box\varphi \to \Diamond\varphi$: "if φ is obligatory, then φ is permitted" (deontic logic)
- $\Box\varphi \to \Box\Box\varphi$: "if I know φ, then I know that I know φ" (epistemic logic)

Correspondencies between axioms and their models

Axiom	Kripke structures	Description
$\Box\varphi \to \varphi$	reflexive	for every $w \in W$ $\langle w, w\rangle \in R$
$\varphi \to \Box\Diamond\varphi$	symmetric	$\langle w_1, w_2\rangle \in R$ implies $\langle w_2, w_1\rangle \in R$
$\Box\varphi \to \Diamond\varphi$	serial	$\forall w \in W$ there is $w' \in W$ such that $\langle w, w'\rangle \in R$
$\Box\varphi \to \Box\Box\varphi$	transitive	$\langle w_1, w_2\rangle, \langle w_2, w_3\rangle \in R$ implies $\langle w_1, w_3\rangle \in R$
$\Diamond\varphi \to \Box\Diamond\varphi$	Euclidian	$\langle w_1, w_2\rangle, \langle w_1, w_3\rangle \in R$ implies $\langle w_2, w_3\rangle \in R$

Important axiomatic extensions – 3

Each axiomatic is complete w.r.t. the corresponding class of Kripke structures:

M	reflexive
D	serial
KB	symmetric
K4	transitive
K5	Euclidean
K45	transitive and Euclidean
D4	serial and transitive
D5	serial and Euclidean
D45	serial, transitive, and Euclidean
KB5	symmetric, transitive, and Euclidean
DB	symmetric and serial
B	reflexive and symmetric
S4	reflexive and transitive
S5	equivalence relation

A simple example – 1

- Let A and B be two agents, with two respective Boolean variables a and b.
- All they do is: flip the value of their variable, sleep for a bit, then flip the value back again.
- Their actions are non necessarily simultaneous.

Kripke structure: $M = \langle W = \{w_1, w_2, w_3, w_4\}, R, V \rangle$

$R =$

$\{\langle w_1, w_2\rangle, \langle w_2, w_1\rangle, \langle w_2, w_3\rangle, \langle w_3, w_2\rangle, \langle w_3, w_4\rangle, \langle w_4, w_3\rangle, \langle w_1, w_4\rangle, \langle w_4, w_1\rangle\}$

$V(w_1, a) = 0 \quad V(w_1, b) = 0$

$V(w_2, a) = 1 \quad V(w_2, b) = 0$

$V(w_3, a) = 1 \quad V(w_3, b) = 1$

$V(w_4, a) = 0 \quad V(w_4, b) = 1$

A simple example – 2

We can unwind the state diagram by choosing an initial state and displaying all the possible paths starting there:

- $w_1 \to w_2 \to w_1 \to w_2 \to \ldots$
- $w_1 \to w_2 \to w_1 \to w_4 \to \ldots$
- $w_1 \to w_2 \to w_3 \to w_2 \to \ldots$
- $w_1 \to w_2 \to w_3 \to w_4 \to \ldots$
- $w_1 \to w_4 \to w_1 \to w_2 \to \ldots$
- $w_1 \to w_4 \to w_1 \to w_4 \to \ldots$
- $w_1 \to w_4 \to w_3 \to w_2 \to \ldots$
- $w_1 \to w_4 \to w_3 \to w_4 \to \ldots$

A simple example – 3

The following formulae are true in M:

- $\Diamond\neg a \wedge \Diamond a$
- $\Diamond\neg b \wedge \Diamond b$
- $a \wedge b \rightarrow \Box(\neg a \vee \neg b)$
- $a \wedge b \rightarrow \Diamond\Diamond(a \wedge b)$

Basic modal logic allows to speak about the states that can be reach in finitely-many steps. But we cannot say:

- that some state is reachable (we have to say “reachable in n steps”)
- which process will take us to some particular state
- “there is a process starting at w_1 where b is always false”
- what A knows about B.

Multimodal logic

Take now a collection of accessibility relations R_i, giving modalities $[i]$ and $\langle i \rangle$:

- $\langle M, w \rangle \models [i]\varphi$ iff $\langle M, w' \rangle \models \varphi$ for each w' such that $\langle w, w' \rangle \in R_i$
- $\langle M, w \rangle \models \langle i \rangle \varphi$ iff $\langle M, w' \rangle \models \varphi$ for some w' such that $\langle w, w' \rangle \in R_i$

$\langle i \rangle \varphi = \neg [i] \neg \varphi$

Multimodal logic: dynamic logic

Multimodal logic which allows for composition, union and iteration of program modalities.

In the previous example:

- $a \to [(a :=!a);(a :=!a)]a$ "if a is true, then after executing $(a :=!a)$ twice, a is true again"
- $a \wedge b \to [(a :=!a) \cup (b :=!b)](\neg a \vee \neg b)$ "if a and b are true, then after executing $(a :=!a)$ or $(b :=!b)$, either a or b is false"
- $a \to [(b :=!b)^*]a$ "if a is true, then after finitely-many iterations of $(b :=!b)$, a is still true

Multimodal logic: epistemic logic

If we want to model agent knowledge in a multiagent system, instead of $\Box$ we may take a modality K_i for each agent.

$\mathrm{K}_i\varphi$ "the i-th agent knows that φ_i".

Outline

Idea

Temporal logics are modal logics with a semantics of possible worlds that represent moments in time.

They extend classical logic with a set of temporal modalities that allow to navigate between worlds.

The accessibility relation between worlds determines a model of time (linear or branching).

Linear temporal logic

Linear temporal logic (LTL) is a temporal logic where the accessibility relation characterizes a discrete infinite linear model of time with an initial moment (thus, isomorphic to the natural numbers).

Temporal operators:

- $\bigcirc\varphi$: "φ is true in the next moment in time"
- $\Box\varphi$: "φ is true in all future moments"
- $\Diamond\varphi$: "φ is true in some future moment"
- $\varphi\,\mathcal{U}\,\psi$: "$\varphi$ is true until ψ"

Some formulae in linear temporal logic

- $\Box(\neg passport \vee \neg boarding\_card \rightarrow \bigcirc \neg board\_flight)$
- $\Box(requested \rightarrow \Diamond received)$
- $\Box(received \rightarrow \bigcirc processed)$
- $\Box(processed \rightarrow \Diamond \Box done)$

Semantics of LTL

Kripke structures: $M = \langle \mathbb{N}, I \rangle$ where $I : AP \times \mathbb{N} \to \{0, 1\}$

$\langle M, i \rangle \models p$	iff	$I(p, i) = 1$
$\langle M, i \rangle \models \neg\varphi$	iff	$\langle M, i \rangle \not\models \varphi$
$\langle M, i \rangle \models \varphi \to \psi$	iff	$\langle M, i \rangle \not\models \varphi$ or $\langle M, i \rangle \models \psi$
$\langle M, i \rangle \models \bigcirc\varphi$	iff	$\langle M, i+1 \rangle \models \varphi$
$\langle M, i \rangle \models \Diamond\varphi$	iff	there is $j \geq i$ such that $\langle M, j \rangle \models \varphi$
$\langle M, i \rangle \models \Box\varphi$	iff	for each $j \geq i$, $\langle M, j \rangle \models \varphi$
$\langle M, i \rangle \models \varphi \mathcal{U} \psi$	iff	there is $j \geq i$ such that $\langle M, j \rangle \models \psi$ and for each k such that $i \leq k < j$, $\langle M, k \rangle \models \varphi$

Equivalencies in LTL

- $\Diamond\varphi \leftrightarrow \neg\Box\neg\varphi$
- $\Box\varphi \leftrightarrow \neg\Diamond\neg\varphi$
- $\Diamond\varphi \leftrightarrow \overline{1}\,\mathcal{U}\,\varphi$
- $\Diamond(\varphi \vee \psi) \leftrightarrow \Diamond\varphi \vee \Diamond\psi$
- $\Box(\varphi \wedge \psi) \leftrightarrow \Box\varphi \wedge \Box\psi$
- $\neg\bigcirc\varphi \leftrightarrow \bigcirc\neg\varphi$
- $\neg(\varphi\,\mathcal{U}\,\psi) \leftrightarrow (\neg\psi\,\mathcal{U}\,(\neg\varphi \wedge \neg\psi)) \vee \Box\neg\psi$

Advantages of LTL

- It is a decidable (PSPACE-complete) fragment of classical first-order logic.
- It was originally developed as a tool to represent tense in natural language.
- It has also become useful for Computer Science, in particular in formal specification and verification of concurrent reactive systems.

LTL in Computer Science

It allows to represent important properties:

- Safety properties: "something bad will not happen". Ex: $\Box\neg(reactor\_temp > 1000)$
- Liveness properties: "something good will happen". Ex: $\Diamond(x > 5)$, $\Box(start \to \Diamond terminate)$
- Fairness properties: "if something is attempted infinitely often, then it will be successful infinitely often". Ex: $\Box\Diamond ready \to \Box\Diamond run$

Path semantics for LTL – 1

- Although we are considering a linear notion for time, the structure of processes in the systems we want to model (their state diagram) may not be linear.
- Recall Kripke structures for modal logics can represent state diagrams for these systems.
- Recall that Kripke structures can be unwinded obtaining a collection of linear paths (computations).
- Each linear path is isomorphic to the natural numbers:

  $\pi = s_0 \to s_1 \to \ldots \to s_i \to s_{i+1} \to \ldots$

Path semantics for LTL – 2

Take a Kripke structure $M = \langle W, R, V \rangle$ and a set $W_0 \subseteq W$ (initial states).

- Given a path π starting at a point $s_0 \in W$, we define a Kripke structure $M_\pi = \langle \pi, I_\pi \rangle$ by:

  for each $s \in \pi$ and each $p \in AP$, $I_\pi(p, s) = 1$ iff $V(p, s) = 1$

- Given a path π starting at a point $s_0 \in W$ and a formula φ we define:

  $$\langle M, \pi \rangle \models \varphi \text{ iff } \langle M_\pi, s_0 \rangle \models \varphi$$

- Given a point $s \in W$ and a formula φ we define:

  $\langle M, s \rangle \models \varphi$ iff $\langle M, \pi \rangle \models \varphi$ for every path π starting at s

- Given a formula φ we define:

  $M \models \varphi$ iff $\langle M, s_0 \rangle \models \varphi$ for each initial state $s_0 \in W_0$

Computation tree logic

- LTL implicitly quantifies universally over paths.
- LTL cannot express the existence of a path with a certain property.
- Computation Tree Logic (CTL) explicitly introduces path quantifiers:
- CTL is evaluated over branching-time structures: trees.
- (to be continued in Jordi Sabater's lectures later in this course...)

Bibliography

- P. Blackburn, M. de Rijke, Y. Venema, *Modal logic*, Cambridge Tracts in Theoretical Computer Science, vol. 53, Cambridge University Press, 2001.
- B.F. Chellas, *Modal Logic: an introduction*, Cambridge University Press, 1980.
- M. Huth and M. Ryan, *Logic in computer science: modelling and reasoning about systems*, Cambridge University Press, 2000.
- C. Stirling, *Modal and temporal properties of processes*, Springer-Verlag New York, 2001.