Modal Logics of Programs (Draft)

Dynamic Logic – Part 4

Igor Sedlár

Institute of Computer Science of the Czech Academy of Sciences

Czech Academy of Sciences

Faculty of Arts, Charles University
Fall Semester 2023-24

Modal logic – 1

Recall that Σ is an alphabet of "action letters" and Π is an alphabet of "propositional letters".

Definition 1

The set $\mathbb{F}(\Sigma, \Pi)$ of modal formulas over Σ and Π is defined using the following grammar:

$$\varphi, \psi := \mathtt{p} \in \Pi \mid \neg\varphi \mid \varphi \vee \psi \mid \langle \mathtt{a} \rangle \varphi$$

Boolean operators $\top, \bot, \wedge, \rightarrow, \leftrightarrow$ are defined as usual. Moreover, $[\mathtt{a}]\varphi := \neg\langle \mathtt{a} \rangle \neg\varphi$.

Read $\langle \mathtt{a} \rangle \varphi$ as "φ is possible after a" and $[\mathtt{a}]\varphi$ as "φ is necessary after a".

Modal logic – 2

Recall relational models (for Σ and Π), $M = \langle X, \mathsf{rel}_M, \mathsf{sat}_M \rangle$ where $X \neq \emptyset$, $\mathsf{rel}_M : \Sigma \to 2^{X \times X}$, and $\mathsf{sat}_M : \Pi \to 2^X$.

Definition 2

Given a relational model M, we define $\| - \|_M : \mathbb{F} \to 2^X$ as follows:

- $\|\mathtt{p}\|_M = \mathsf{sat}_M(\mathtt{p})$
- $\|\neg\varphi\|_M = X \setminus \|\varphi\|_M$
- $\|\varphi \vee \psi\|_M = \|\varphi\|_M \cup \|\psi\|_M$
- $\|\langle \mathsf{a} \rangle \varphi\|_M = \langle\!\langle \mathsf{a} \rangle\!\rangle \|\varphi\|_M$ *where* $\langle\!\langle \mathsf{a} \rangle\!\rangle Y = \{x \mid \exists y. \langle x, y \rangle \in \mathsf{rel}_M(\mathsf{a}) \;\;\&\;\; y \in Y\}$

We also write $(M, x) \vDash \varphi$ instead of $x \in \|\varphi\|_M$. Let $Th(M, x) = \{\varphi \mid (M, x) \vDash \varphi\}$.

Modal logic – 3

Definition 3

A formula φ is valid in M iff $\|\varphi\|_M$ is the set of all states in M (notation: $M \vDash \varphi$). A formula φ is valid in a class of models $\mathcal{K}$ iff $M \vDash \varphi$ for all $M \in \mathcal{K}$ (notation: $\mathcal{K} \vDash \varphi$).

Example

Valid:

- $\langle \mathtt{a} \rangle (\varphi \vee \psi) \leftrightarrow \langle \mathtt{a} \rangle \varphi \vee \langle \mathtt{a} \rangle \psi$
- $\langle \mathtt{a} \rangle \bot \leftrightarrow \bot$

Not valid:

- $\langle \mathtt{a} \rangle (\varphi \wedge \psi) \leftrightarrow \langle \mathtt{a} \rangle \varphi \wedge \langle \mathtt{a} \rangle \psi$
- $\langle \mathtt{a} \rangle \top \leftrightarrow \top$

Example

- $M \vDash \langle \mathtt{a} \rangle \top$ iff a terminates when run in any state of M
- $M \vDash \varphi \to [\mathtt{a}] \psi$ iff a is partially correct with respect to precondition φ and postcondition ψ (recall "Hoare triples")

Bisimulation

Definition 4

$(M_1, x_1) \underline{\leftrightarrow} (M_2, x_2)$ *iff*

- $(M_1, x_1) \vDash \mathrm{p}$ *iff* $(M_2, x_2) \vDash \mathrm{p}$ *for all* $\mathrm{p} \in \Pi$
- $x_1 \xrightarrow{\mathtt{a}} y_1$ *only if there is* y_2 *such that* $x_2 \xrightarrow{\mathtt{a}} y_2$ *and* $(M_1, y_1) \underline{\leftrightarrow} (M_2, y_2)$
- $x_2 \xrightarrow{\mathtt{a}} y_2$ *only if there is* y_1 *such that* $x_1 \xrightarrow{\mathtt{a}} y_1$ *and* $(M_1, y_1) \underline{\leftrightarrow} (M_2, y_2)$

Proposition 1

1. *If* $(M_1, x_1) \underline{\leftrightarrow} (M_2, x_2)$*, then* $Th(M_1, x_1) = Th(M_2, x_2)$.
2. *If* M_1, M_2 *are finitely branching,*[a] *then* $Th(M_1, x_1) = Th(M_2, x_2)$ *implies* $(M_1, x_1) \underline{\leftrightarrow} (M_2, x_2)$.

[a] For all $\mathtt{a} \in \Sigma$ and all $y \in X_i$, the set $\mathsf{rel}_{M_i}(\mathtt{a})[y]$ is finite.

Proof (sketch). (1.) Induction on formulas. (2.) Modal equivalence is a bisimulation relation. $\square$

Exercises

1. Finish the proof of Prop. 1.

Notes

- An excellent introduction to modal logic is the “blue book” (Blackburn, de Rijke, Venema, 2001).

References

- P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.