Logic and Computation II

Part 4. Modal logic

Kazuyuki Tanaka

BIMSA

March 18, 2025

北京雁栖湖应用数学研究院
Beijing Institute of Mathematical Sciences and Applications

Logic and Computation

- **Part 4. Modal logic**
- **Part 5. Modal μ-calculus**
- **Part 6. Automata on infinite objects**
- **Part 7. Recursion-theoretic hierarchies**

Part 4. Schedule (tentative)

- March 4, (1) Kripke models and normal logics
- March 6, (2) Kripke completeness
- March 11, (3) Standard translation and bisimulation
- March 13, (4) Decision problems
- March 18, (5) Computational complexity
- March 20, (6) Multi-modal and predicate logics

Recap: Decision Problem, Finite Model Property

Let Γ be a set of modal propositions closed under subformulas.

Definition 4.27

Let $M = (W, R, v)$ be a Kripke model. The equivalence relation $s \sim_\Gamma t$ on W is defined by:

$$\forall \varphi \in \Gamma, \quad M, s \models \varphi \Leftrightarrow M, t \models \varphi.$$

$M_\Gamma = (W_\Gamma, R_\Gamma, v_\Gamma)$ is called a **filtration** of M *through* Γ if the following conditions hold:

(1) $W_\Gamma := W/\sim_\Gamma$, i.e., the set of equivalence classes under $\sim_\Gamma$,

(2) If sRt, then $[s]R_\Gamma[t]$,

(3) If $[s]R_\Gamma[t]$, then for any $\Box\varphi \in \Gamma$, $M, s \models \Box\varphi \Rightarrow M, t \models \varphi$,

(4) $v_\Gamma(p) := \{[s] \mid s \in v(p)\}$ for any atomic proposition p appearing in Γ.

Note that the above definition only specifies the conditions for filtration $(W_\Gamma, R_\Gamma, v_\Gamma)$ but does not guarantee its existence. More specifically, W_Γ and v_Γ exist uniquely by conditions (1) and (4), but the existence of R_Γ satisfying (2) and (3) is not clear.

Lemma 4.28

If Γ is a finite set, then W_Γ is also finite and its cardinality is at most $2^{|\Gamma|}$.

Lemma 4.29

Let M_Γ be the filteration of M through Γ. Then, for any $\varphi \in \Gamma$ and $s \in W$, the following holds:

$$M, s \models \varphi \Leftrightarrow M_\Gamma, [s] \models \varphi.$$

There are two candidates for R_Γ: the strongest R^+ and the weakest R^-, which are defined as follows:

- $[s]R^+[t] \Leftrightarrow \exists s' \in [s] \exists t' \in [t] s' R t'$,
- $[s]R^-[t] \Leftrightarrow$ If $M, s \models \Box\varphi (\in \Gamma)$, then $M, t \models \varphi$.

of a filtration with R^+, R^- and more.

Lemma 4.30

Both R^+ and R^- satisfy both conditions (2) and (3) of filtration. Moreover, R_Γ satisfies both (2) and (3) if and only if for all s, t, $[s]R^+[t] \Rightarrow [s]R_\Gamma[t] \Rightarrow [s]R^-[t]$.

Next, we define the finite model property as follows, although the definition may vary slightly across different sources.

Definition 4.31

A normal modal logic L has the **finite model property** (FMP) if, for any $\varphi \notin L$, there exists a finite model M such that $M \models L$ and $M \not\models \varphi$.

Here, $M \not\models \varphi$ means that there exists some s such that $M, s \models \neg\varphi$. As for the finite **frame** property, additional conditions are required, so we do not introduce it here.

Lemma 4.32

K has the finite model property.

Proof. By the completeness theorem 4.11, K coincides with the set of valid propositions. So, for any $\varphi \notin$ K, there exists a model M (of K) and $s \in W$ such that $M, s \models \neg\varphi$. Let Γ be the set of subformulas of φ, and let M_Γ be a filtration of M through Γ. By Lemma 4.28, M_Γ is finite, and by Lemma 4.29, $M_\Gamma, [s] \models \neg\varphi$, so we are done. □

To prove that a normal modal logic other than K also has the finite model property by the same method, it suffices to find a relation R_Γ which preserves the desired properties of R.

Lemma 4.33

Let $M_\Gamma = (W_\Gamma, R_\Gamma, v_\Gamma)$ be a filtration of M through Γ, and R^+ be the strongest relation. Then,
(1) If R is reflexive/serial, then R_Γ is also reflexive/serial.
(2) If R is symmetric, then R^+ is also symmetric.

Proof.

(1) If R is reflexive, then sRs holds. By condition (2), we have $[s]R_\Gamma[s]$, so R_Γ is also reflexive. The case of seriality follows similarly.

(2) To show the symmetry of R^+, assume $[s]R^+[t]$. By the definition of R^+, there exist $s' \in [s]$ and $t' \in [t]$ such that $s'Rt'$. Since R is symmetric, we have $t'Rs'$. By condition (2), it follows that $[t']R^+[s']$, i.e., $[t]R^+[s]$.

□

Lemma 4.34

Let Γ be a set closed under subformulas, and R^+ be the strongest relation as a filtration, and R^* be the transitive closure of R^+. If R is transitive, then $M^* = (W_\Gamma, R^*, v_\Gamma)$ is a transitive filtration.

Proof.

- Since $sRt \Rightarrow [s]R^+[t] \Rightarrow [s]R^*[t]$, R^* satisfies condition (2) of Definition 4.27.
- To show that R^* satisfies condition (3), assume $[s]R^*[t]$ and $M, s \models \Box\varphi$ with $\Box\varphi \in \Gamma$. We want to show $M, t \models \varphi$.

  Since $[s]R^*[t]$, there exist $s_1, s_2, \ldots, s_k, s_{k+1} = t$ s.t. $[s]R^+[s_1]R^+[s_2]\ldots[s_k]R^+[t]$. First, we have $\exists s' \in [s], \exists s_1' \in [s_1]$ such that $s'Rs_1'$, and since $M, s \models \Box\varphi$, we have $M, s' \models \Box\varphi$ and so $M, s_1' \models \varphi$. Since M is transitive, for any $u \in s_1'R$, we have $u \in s'R$, hence $M, u \models \varphi$, which implies $M, s_1' \models \Box\varphi$. Therefore, $M, s_1 \models \Box\varphi$.

  Repeating this argument, we obtain $M, s_k \models \Box\varphi$, and also $M, t \models \varphi$. This proves R^* satisfies condition (3).
- Therefore, $M^* = (W_\Gamma, R^*, v_\Gamma)$ is a filtration, which is obviously transitive.

- From the above two lemmas, we conclude that the major normal modal logics T, B, D, K4, S4, S5 have the finite model property and are therefore decidable.

- In summary, for such a logic L, we can construct a finite filtration M_Γ of a canonical model M_L through the set of subformulas Γ of φ, which satisfies φ and $F_\Gamma \models L$.

Problem 5

Prove the decidability of S4.2.

§4.6. Computational Complexity

- Once decidability is established, the next concern is the complexity of computation. A rigorous discussion would require more time than available in the course, so we will focus on a few fundamental results and their underlying ideas.
- For a finite model M and a modal formula φ, the time required to determine whether $M, s \models \varphi$ is roughly $|M| \cdot |\varphi|$. Here, we define $|M| = |W| + |R|$, and $|\varphi|$ denotes the length of the formula φ. Thus, to determine whether a formula φ is satisfiable in a model M of a logic L, it is crucial to limit the size $|M|$ of M.
- We first consider the modal logic S5.

Lemma 4.35

If a formula φ is satisfiable in an S5 model, then it is satisfiable in an S5 model with at most $|\varphi|$ states.

Proof. Let $M = (W, R, v)$ be an S5 model and suppose $M, s \models \varphi$. Since R is an equivalence relation, we only need to consider the submodel restricted to the equivalence class $[s]$, which we redefine as $M = (W, R, v)$. This ensures that $R = W \times W$.

For the sake of convenience, we replace all occurrences of $\Box$ in φ with $\neg\Diamond\neg$. We redefine it as φ. Define the set of subformulas of φ as $\mathrm{Sub}(\varphi)$, and let

$$N_\varphi := \{\Diamond\psi \in \mathrm{Sub}(\varphi) : M, s \models \Diamond\psi\}.$$

Clearly, $|N_\varphi| < |\mathrm{Sub}(\varphi)| \leq |\varphi|$.

For each $\Diamond\psi \in N_\varphi$, choose a state $s_\psi \in W$ such that $M, s_\psi \models \psi$, and define a new model $M' = (W', R', v')$ as follows:

$$W' := \{s\} \cup \{s_\psi : \Diamond\psi \in N_\varphi\},$$

$$R' := W' \times W', \quad v' := v \cap (P \times W').$$

Then, for any $s' \in W'$ and any $\psi \in \mathrm{Sub}(\varphi)$,

$$M, s' \models \psi \Leftrightarrow M', s' \models \psi.$$

(This equivalence is left as an exercise.)
Thus, φ is satisfiable in a model with at most $|\varphi|$ states.

Before stating the next theorem, we recall some terminology.

- The class NP consists of decision problems where a solution can be verified in polynomial time w.r.t. the problem size. The satisfiability problem of propositional logic, denote SAT(PC) or just SAT, is a representative of NP problems.
- Moreover, SAT is called NP-**hard**, because any problem in NP can be reduced to SAT in polynomial time. An NP-hard NP problem is also called NP-**complete**.

Theorem 4.36

SAT(S5) is NP-complete.

Proof. Since S5 includes classical propositional logic and SAT(PC) is NP-hard, SAT(S5) is also NP-hard. To show that SAT(S5) is in NP, observe that we can nondeterministically guess a model $M = (W, R, v)$ with $|W| \leq |\varphi|$ and check whether $M, s \models \varphi$ in polynomial time. □

- Next, we consider the complexity of SAT(X) for a normal modal logic $X \subseteq$ S4. In fact, it falls within the class NPSPACE, which consists of problems solvable by a non-deterministic algorithm in a polynomial amount of space. Recall that NPSPACE coincides with the deterministic class PSPACE in polynomial-space. Thus, NPSPACE is closed under complement.
- A PSPACE-**complete** problem is a PSPACE problem which is PSPACE-hard, i.e., any PSPACE problem is polynomial-time reducible to it. A representative PSPACE-complete problem is the validity problem for quantified Boolean formulas (**QBF**), denoted as VAL(QBF) (also as TQBF). Here, QBF allows quantification over Boolean variables, with $\forall x \varphi(x) \equiv \varphi(0) \wedge \varphi(1)$ and $\exists x \varphi(x) \equiv \varphi(0) \vee \varphi(1)$. Note that SAT(QBF) is also PSPACE-complete.

Theorem 4.37 (Ladner's Theorem)

For any normal modal logic $L \subseteq$ S4, both SAT(L) and VAL(L) are PSPACE-hard.

The main idea is to polynomially translate a QBF formula φ into a modal formula $\Psi(\varphi)$ and show:

(1) $\varphi \in \mathsf{SAT}(\mathsf{QBF}) \Rightarrow \Psi(\varphi) \in \mathsf{SAT}(\mathsf{S4})$,

(2) $\Psi(\varphi) \in \mathsf{SAT}(\mathsf{K}) \Rightarrow \varphi \in \mathsf{SAT}(\mathsf{QBF})$.

Since clearly $\Psi(\varphi) \in \mathsf{SAT}(\mathsf{S4}) \Rightarrow \Psi(\varphi) \in \mathsf{SAT}(L) \Rightarrow \Psi(\varphi) \in \mathsf{SAT}(\mathsf{K})$, we obtain

$$\varphi \in \mathsf{SAT}(\mathsf{QBF}) \Leftrightarrow \Psi(\varphi) \in \mathsf{SAT}(L),$$

which implies PSPACE-hardness of $\mathsf{SAT}(L)$ from that of $\mathsf{SAT}(\mathsf{QBF})$. Since PSPACE is closed under complement, $\mathsf{VAL}(L)$ is also PSPACE-hard.

Now we are going to define $\Psi(\varphi)$. First, we may assume that φ is in prenex normal form, written as $Q_1 p_1 \cdots Q_n p_n \theta$. Supposing that φ is true, we construct a "truth tree" for φ, that is, a finite tree labeled with true substitution instances of subformulas of φ. The root of the tree is labelled φ. For a node labeled $\forall x A(x)$, it has two children with $A(0)$ and $A(1)$. A node of $\exists x A(x)$ has one child with either $A(0)$ or $A(1)$ which is true. The leaves are labeled closed instances of θ, all of which are evaluated true.

We want to treat this truth tree T as a transition system (Kripke model) for S4. However, the parent-child relationship in T cannot be simply regarded as a S4 relation. So, we extend T's relation to its reflexive transitive closure, and instead introduce new variables $q_0, q_1, \ldots, q_n$ to represent each level of the tree. The following formula expresses the tree structure:

$$\Psi_1 := q_0 \wedge \bigwedge_{i=0}^{n} \Box^{(n)} \left(q_i \rightarrow \bigwedge_{j \neq i} \neg q_j \right) \wedge \Box^{(n)} \bigwedge_{i=0}^{n-1} (q_i \rightarrow \Diamond q_{i+1}) \, .$$

Here, we define $\Box^0 A := A$, $\Box^{n+1} A := \Box\Box^n A$, and $\Box^{(n)} A := \bigwedge_{i=0}^{n} \Box^i A$. Intuitively, Ψ_1 says that at every node, exactly one of $q_0, q_1, \ldots, q_n$ is true and a node with q_i true has a successor with q_{i+1} true.

Next, we define $\beta_i := q_i \rightarrow \Diamond (q_{i+1} \wedge p_{i+1}) \wedge \Diamond (q_{i+1} \wedge \neg p_{i+1})$ to represent the branching for $\forall x$:

$$\Psi_2 := \bigwedge_{Q_i = \forall} \Box^{(i)} \beta_i .$$

To propagate the truth values of p_i to the next level, we define $\tau_i := (p_i \to \Box p_i) \wedge (\neg p_i \to \Box\neg p_i)$, and set:

$$\Psi_3 := \bigwedge_{j=1}^{n-1} \bigwedge_{i=j}^{n-1} \Box^{(i)} \tau_i .$$

Finally, to ensure that the terminal formula θ holds at the leaves, we define:

$$\Psi_4 := \Box^{(n)} (q_n \to \theta) .$$

Combining all these conditions, we define:

$$\Psi(\varphi) := \Psi_1 \wedge \Psi_2 \wedge \Psi_3 \wedge \Psi_4 .$$

This formula satisfies conditions (1) and (2) as follows.

(1) Suppose that φ is satisfiable in QBF. Consider its truth tree as described above. To construct an S4 model from this tree, we add edges to satisfy reflexivity and transitivity, forming a frame (W, R). Furthermore, we define:

$$\begin{aligned} s \in v(q_i) &\Leftrightarrow s \text{ is a vertex at level } i, \\ s \in v(p_i) &\Leftrightarrow p_i \text{ is assigned 1 at the level-}i\text{ ancestor of } s. \end{aligned}$$

The resulting (W, R, v) is an S4 model that satisfies $\Psi(\varphi)$ at the root.

(2) Suppose that $\Psi(\varphi) \in \mathsf{SAT}(\mathsf{K})$. From a Kripke model that satisfies $\Psi(\varphi)$, we prune unnecessary branches to construct a truth tree of φ. At an $\exists$ node, we select one edge and remove the rest. At a $\forall$ node (level i), we select one edge where p_{i+1} is true and one edge where $\neg p_{i+1}$ is true, removing the rest. This process reconstructs the truth tree of φ, proving that φ is a tautology.

From the above, we conclude that $\mathsf{SAT}(X)$ is PSPACE-hard. □

Theorem 4.38

For any finitely axiomatizable normal modal logic L, the satisfiability problem is in PSPACE.

This follows from the fact that SAT(K) is in PSPACE. The satisfiability problem SAT(L) can be treated as the satisfiability problem for $\Psi + L$ in K. Reference [2] proves this by analyzing a tableau method based on Hintikka sets.

Corollary 4.39

For any finitely axiomatizable normal modal logic $L \subseteq$ S4, both SAT(L) and $\mathrm{VAL}(L)$ are PSPACE-complete.

[2] P. Blackburn, M. de Rijke and Y. Venema, *Modal Logic*, Cambridge Tracts in Theo. Computer Sci., No. 53, Cambridge UP, 2002.

Thank you for your attention!