Logic and Computation II

Part 5. Modal μ-calculus

Kazuyuki Tanaka

BIMSA

April 10, 2025

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

Logic and Computation II

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

Part 5. Schedule (tentative)

- March 27, (1) Introduction to modal μ-calculus and monadic second-order logic
- April 1, (2) Basics of modal μ-calculus
- April 3, (3) The adequacy theorem
- April 8, (4) CTL
- April 10, (5) Applications

§5.4. CTL

As applications of μ-calculus, we introduce CTL (Computation Tree Logic), a representative temporal logic, and two related systems. These logics are widely used in computer science.

Although CTL may have several modal operators, we only focus on two binary operators:

$$A(\varphi U \psi), \quad E(\varphi U \psi)$$

These mean:

- $A(\varphi U \psi)$: On *all* infinite paths, ψ holds eventually and φ holds until then.
- $E(\varphi U \psi)$: On *some* path, ψ holds eventually and φ holds until then.

Here, a path is a sequence of states generated by computation. U stands for "Until". We also include the usual modal operator $\Box$.

Syntax of CTL

Definition (CTL Formula)

Let p be an atomic proposition. A CTL formula is inductively defined as:

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \to \varphi) \mid \Box\varphi \mid \mathsf{A}(\varphi \mathsf{U} \varphi) \mid \mathsf{E}(\varphi \mathsf{U} \varphi)$$

Other logical connectives are defined as usual.
Unless stated otherwise, the frame (W, R) used in CTL is assumed to be **serial**: $\forall s\, \exists t\, (sRt)$.

Semantics of CTL

Definition (Satisfaction Relation)

Let $M = (W, R, v)$ be a relational model. The satisfaction relation $M, s \models \varphi$ is defined inductively as follows:

- For p, $\neg\varphi$, $\varphi \to \psi$ and $\Box\varphi$, the usual clauses apply.
- $M, s_0 \models \mathsf{A}(\varphi \mathsf{U} \psi)$: For every infinite path $s_0 R s_1 R s_2 R \ldots$, there exists i such that $M, s_i \models \psi$ and $M, s_j \models \varphi$ for all $j < i$.
- $M, s_0 \models \mathsf{E}(\varphi \mathsf{U} \psi)$: There exists a finite path $s_0 R s_1 R \ldots R s_i$ such that $M, s_i \models \psi$ and $M, s_j \models \varphi$ for all $j < i$.

Proof System for CTL

Definition (Proof System)

Axioms:

(1) Classical tautologies.

(2) Modal axiom: $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$.

(3) Seriality: $\Box\varphi \to \Diamond\varphi$.

(4) $\mathsf{A}(\varphi \mathsf{U} \psi) \leftrightarrow \psi \lor (\varphi \land \Box\mathsf{A}(\varphi \mathsf{U} \psi))$.

(5) $\mathsf{E}(\varphi \mathsf{U} \psi) \leftrightarrow \psi \lor (\varphi \land \Diamond\mathsf{E}(\varphi \mathsf{U} \psi))$.

Inference Rules:

(6) Modus ponens: from φ and $\varphi \to \psi$, infer ψ.

(7) Necessitation: from φ, infer $\Box\varphi$.

(8) If $\psi \lor (\varphi \land \Box\theta) \to \theta$, then $\mathsf{A}(\varphi \mathsf{U} \psi) \to \theta$.

(9) If $\psi \lor (\varphi \land \Diamond\theta) \to \theta$, then $\mathsf{E}(\varphi \mathsf{U} \psi) \to \theta$.

We write $\vdash_{\mathsf{CTL}} \varphi$ to indicate that φ is provable in this system.

Completeness of CTL

Theorem 1 (Completeness)

$$\vdash_{\mathsf{CTL}} \varphi \iff \models_{\mathsf{CTL}} \varphi$$

Proof. ($\Rightarrow$) Axioms (1)–(7) are straightforward.
We show (8): Assume $\mathsf{A}(\varphi \mathsf{U} \psi) \to \theta$ is not valid. So, $\mathsf{A}(\varphi \mathsf{U} \psi) \to \theta$ is false at some state s in a model M, i.e.,

$$M, s \models \mathsf{A}(\varphi \mathsf{U} \psi) \wedge \neg\theta.$$

We look for a state t along a path from s such that

$$M, t \models (\psi \vee (\varphi \wedge \Box\theta)) \wedge \neg\theta. \quad \ldots (\star)$$

If ψ is true at s, then $(\star)$ holds at s. If not, then by $\mathsf{A}(\varphi \mathsf{U} \psi)$ φ holds at s.
If also $\Box\theta$ holds at $t = s$, then $(\star)$ again holds.
If not, then there exists a successor s' such that $M, s' \models \neg\theta$.
At s', $\mathsf{A}(\varphi \mathsf{U} \psi)$ still holds, and we repeat the reasoning. Proceeding along a path thus constructed, we eventually reach a state t where ψ holds, and at that state $(\star)$ holds.
Hence, $(\psi \vee (\varphi \wedge \Box\theta)) \to \theta$ is not valid. A similar argument proves (9).

Completeness of CTL (a part of the proof)

($\Leftarrow$): Suppose $\nvdash_{\mathsf{CTL}} \varphi$. We aim to construct a finite serial model M such that $M, s \not\models \varphi$.

Let $Sub(\varphi)$ be the set including all the subformulas of φ, closed under the following:

- If $\mathsf{A}(\theta \mathsf{U} \psi) \in Sub(\varphi)$, then it also includes $\Box \mathsf{A}(\theta \mathsf{U} \psi)$
- If $\mathsf{E}(\theta \mathsf{U} \psi) \in Sub(\varphi)$, it includes $\Diamond \mathsf{E}(\theta \mathsf{U} \psi)$

Then put

$$Sub^+(\varphi) := Sub(\varphi) \cup \{\mathsf{A}(\top \mathsf{U} \top), \Box \mathsf{A}(\top \mathsf{U} \top), \top, \Box \top, \bot\}$$

Define a model $M = (W, R, v)$ as follows:

- $W := \{(\Gamma, \Delta) \mid \Gamma \cup \Delta = Sub^+(\varphi)$ is a partition, and $\Gamma \nvdash_{\mathsf{CTL}} \bigvee \Delta\}$
- Transition: $(\Gamma, \Delta) R (\Pi, \Sigma)$ if for every formula $\Box \theta \in \Gamma$, we have $\theta \in \Pi$
- Valuation: $(\Gamma, \Delta) \in v(p)$ iff $p \in \Gamma$

Note that if $\Gamma \cup \Delta \subset Sub^+(\varphi)$ and $\Gamma \nvdash_{\mathsf{CTL}} \bigvee \Delta$, then there exists a partition $\Gamma^+ \cup \Delta^+ = Sub^+(\varphi)$ such that $\Gamma \subset \Gamma^+$, $\Delta \subset \Delta^+$, and still $\Gamma^+ \nvdash_{\mathsf{CTL}} \bigvee \Delta^+$.
$\because$ If $\Gamma \nvdash_{\mathsf{CTL}} \bigvee \Delta$ then for any θ, $\Gamma \cup \{\theta\} \nvdash_{\mathsf{CTL}} \bigvee \Delta$ or $\Gamma \nvdash_{\mathsf{CTL}} \bigvee \Delta \cup \{\theta\}$.

Lemma 2

For any $s = (\Gamma, \Delta) \in W$ *and any formula* θ *that is not of the form* A$(\cdot$U$\cdot)$ *or* E$(\cdot$U$\cdot)$*:*

- *If* $\theta \in \Gamma$*, then* $M, s \models \theta$
- *If* $\theta \in \Delta$*, then* $M, s \not\models \theta$

Proof. By induction on the construction of formula θ.
(1) Case: $\theta = p$ (atomic proposition). By the definition of $v(p)$, $\theta \in \Gamma$ iff $M, s \models \theta$.

(2) Case: $\theta = \varphi \to \psi$. First suppose $\theta \in \Gamma$. Then, $\varphi \in \Gamma$ and $\psi \in \Delta$ implies $\Gamma \vdash_{\mathsf{CTL}} \bigvee \Delta$, a contradiction. Thus, $\varphi \notin \Gamma$ or $\psi \notin \Delta$, that is, $\varphi \in \Delta$ or $\psi \in \Gamma$. By induction hypothesis, $M, s \not\models \varphi$ or $M, s \models \psi$, that is, $M, s \models \varphi \to \psi$. Next, suppose $\theta \in \Delta$. Then, we have $\varphi \notin \Gamma$ and $\psi \notin \Delta$, that is, $\varphi \in \Delta$ and $\psi \in \Gamma$, hence $M, s \not\models \varphi \to \psi$.

(3) Case: $\theta = \Box\varphi$. First suppose $\theta \in \Gamma$. Then, by the definition of transition relation R, $(\Gamma, \Delta)R(\Pi, \Sigma)$ implies $\varphi \in \Pi$, so $M, (\Pi, \Sigma) \models \varphi$. Next suppose $\theta \in \Delta$. We want to show that there exists (Π, Σ) such that $(\Gamma, \Delta)R(\Pi, \Sigma)$ and $\varphi \in \Sigma$. Let $\Gamma/\Box = \{\alpha : \Box\alpha \in \Gamma\}$.
Then, we have $\Gamma/\Box \nvdash_{\mathsf{CTL}} \varphi$. For otherwise, $\Gamma \vdash_{\mathsf{CTL}} \Box\varphi$ $(\in \Delta)$, a contradiction.
Now, we can construct a partition $\Pi \cup \Sigma = Sub^{+}(\varphi)$ such that $\Gamma/\Box \subset \Pi$, $\varphi \in \Delta$, and still $\Pi \nvdash_{\mathsf{CTL}} \bigvee \Sigma$. By $\Gamma/\Box \subset \Pi$, we have $(\Gamma, \Delta)R(\Pi, \Sigma)$.

To extend the truth lemma to formulas involving A$(\cdot \mathrm{U} \cdot)$ or E$(\cdot \mathrm{U} \cdot)$, the model must encode path information explicitly. Such constructions are more involved and omitted here.

Remark: Case: $\theta = \mathrm{A}(\varphi \mathrm{U} \psi)$. Suppose $\theta \in \Gamma$. Then, by axiom (4), either $\psi \in \Gamma$ or (both $\varphi \in \Gamma$ and $\Box \mathrm{A}(\varphi \mathrm{U} \psi) \in \Gamma$). If $\psi \in \Gamma$, then by induction hypothesis, $M, s \models \psi$, hence by the definition of A$(\cdot \mathrm{U} \cdot)$, we have $M, s \models \mathrm{A}(\varphi \mathrm{U} \psi)$. Next assume $\varphi \in \Gamma$ and $\Box \mathrm{A}(\varphi \mathrm{U} \psi) \in \Gamma$. By ind. hyp., $M, s \models \varphi$. Now, take any $s_1 = (\Pi, \Sigma)$ such that $(\Gamma, \Delta) R (\Pi, \Sigma)$. Then, $\theta = \mathrm{A}(\varphi \mathrm{U} \psi) \in \Pi$. So, by the same argument, we have $M, s_1 \models \psi$ or (both $M, s_1 \models \varphi$ and $\Box \mathrm{A}(\varphi \mathrm{U} \psi) \in \Pi$). Thus, we can show that for any path, φ holds always or until ψ holds, which is not sufficient.

Variants of CTL: LTL and CTL*

As important variants of CTL, we introduce:

- **Linear Temporal Logic (LTL)** — temporal logic over linear (non-branching) time
- **CTL*** — combines features of both CTL and LTL

In LTL, only linear sequences of states are considered, so there is no distinction between $\Box$ and $\Diamond$. Both are replaced by the temporal operator X ("next").
Likewise, $\mathsf{A}(\varphi \mathsf{U} \varphi')$ and $\mathsf{E}(\varphi \mathsf{U} \varphi')$ are unified as $\varphi \mathsf{U} \varphi'$ in LTL.

Syntax of LTL

Definition (LTL formulas)

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \to \varphi') \mid X\varphi \mid \varphi \mathsf{U} \varphi'$$

Other logical connectives are defined as usual.

- $X\varphi$: "φ holds at the next state"
- $\varphi \mathsf{U} \varphi'$: "$\varphi'$ eventually holds, and until then φ holds"

Derived temporal operators:

$$\mathsf{F}\varphi := \top \mathsf{U} \varphi \quad \text{(eventually } \varphi \text{ holds)}$$

$$\mathsf{G}\varphi := \neg \mathsf{F} \neg \varphi \quad \text{(always } \varphi \text{ holds)}$$

Semantics of LTL

We assume a serial frame based on the natural numbers $\mathbb{N}$, with each transition corresponding to a successor state.
Atomic propositions $p_1, \ldots, p_n$ are evaluated via binary vectors $\vec{b} \in \{0,1\}^n$. A model becomes an infinite word $\alpha \in (\{0,1\}^n)^\omega$.

Satisfaction Relation

$$\alpha, i \models X\varphi \iff \alpha, i+1 \models \varphi$$
$$\alpha, i \models \varphi \mathsf{U} \psi \iff \exists j \geq i\,(\alpha, j \models \psi \wedge \forall k \in [i, j-1]\ \alpha, k \models \varphi)$$

Exercise. Answer the following:

(1) Show that GFφ expresses "infinitely often φ holds".
(2) What does FGφ express?
(3) Define φWψ to mean: "φ holds while ψ holds".

Introduction to CTL*

CTL* handles branching time globally, and evaluates formulas as LTL on each individual path. In other words, CTL* extends LTL by adding path quantifiers:

- $A\varphi$: φ holds on all paths from the current state
- $E\varphi$: φ holds on some path from the current state

We define satisfaction with respect to a model M, a path $P = s_0, s_1, \ldots,$ and a state s_i:

Satisfaction Relation

- For propositional formulas and $X\psi$, $\varphi \mathrm{U} \psi$: interpret them as in LTL on path P.
- $M, P, s \models A\varphi \iff$ for all paths Q through s, $M, Q, s \models \varphi$
- $M, P, s \models E\varphi \iff$ there exists a path Q through s such that $M, Q, s \models \varphi$

Exercise. Show the following:

(1) For any CTL formula φ, construct a CTL* formula φ^* by:
- Replacing $\Box\psi$ with $AX\psi$
- Translating $A(\psi \mathrm{U} \psi')$, $E(\psi \mathrm{U} \psi')$ as modal combinations

Then:

$$M, s \models \varphi \iff \text{For every path } P \text{ through } s : M, P, s \models \varphi^*$$

(2) In CTL*, the formula EFG p expresses "there exists a path where p holds infinitely often".
Explain why this cannot be expressed in plain CTL.

Summary of Temporal Logics:

- CTL: Branching-time logic, evaluated globally
- LTL: Linear-time logic, evaluated along single paths
- CTL*: Combines CTL and LTL, allows path quantification and temporal reasoning

Notably, CTL* can express properties like:

$$\text{EFG } p \quad \text{(there is a path where } p \text{ holds infinitely often)}$$

which CTL cannot express.
Yet, even CTL* is translatable into modal μ-calculus L_μ.

Dynamic Epistemic Logic (DEL)

In Section 4.9 (0325), we analyzed the initial state of the "Muddy Children Puzzle" using epistemic logic. The story begins when their mother announces, "There is a child with mud on their forehead."

If two children have mud on their foreheads, all the children know that "a child with mud is present." However, reasoning does not begin without this announcement. By announcing φ, it is not just assumed that Eφ, but rather Cφ is assumed.

This logic that deals with changes in knowledge models is called **Dynamic Epistemic Logic (DEL)**. Specifically, the logic that provides common knowledge through public announcements is called **Public Announcement Logic (PAL)**. The simplest formal system of this logic is introduced below. We will not use the operator B_a, and the operator K_a (for $a \in A$) is assumed to satisfy the S5 axiom. Additionally, the new modal operator $[\varphi!]\psi$ is defined to satisfy the following:

$$M, s \models [\varphi!]\psi \iff M, s \models \varphi \implies M[\varphi!], s \models \psi,$$

where $M[\varphi!] = (W', \{R_a \restriction W'\}, v \restriction W')$ and $W' = \{s \in W : M, s \models \varphi\}$. Since we assume $M, s \models \varphi$, W' is non-empty. The operator $[\varphi!]$ represents "the announcement of φ".

Example: Card Game

Consider two players, $\mathtt{I}$ and $\mathtt{II}$, each drawing one card from a deck, making sure the opponent cannot see the card. Ignore the text written on the card and focus on whether it is red (r) or black (b). If $\mathtt{I}$ draws a red card r and $\mathtt{II}$ draws a black card b, the state is denoted as (r, b). The set of possible worlds is:

$$W = \{(r,r),(r,b),(b,r),(b,b)\}.$$

The relations $R_{\mathtt{I}}$ and $R_{\mathtt{II}}$ are equivalence relations, so we can represent them with $\sim_{\mathtt{I}}$ and $\sim_{\mathtt{II}}$, where the relations are reflexive and also satisfy:

$$(r,r) \sim_{\mathtt{I}} (r,b), (b,r) \sim_{\mathtt{I}} (b,b); \quad (r,r) \sim_{\mathtt{II}} (b,r), (r,b) \sim_{\mathtt{II}} (b,b).$$

If it is announced that $\mathtt{I}$ drew a red card r, then the new set of possible worlds is $W' = \{(r,r),(r,b)\}$, and the relation $R_{\mathtt{II}}$ remains only reflexive.

Exercise

Assume that $M \models \neg\varphi$ does not hold. Show the following:

(1) If R_a is reflexive, transitive, or Euclidean, then $R_a[\varphi!]$ will also satisfy these properties.

(2) If R_a is serial, $R_a[\varphi!]$ does not necessarily satisfy this property.

Public Announcement Logic (PAL): Axiom System

The axiom system for PAL is as follows:

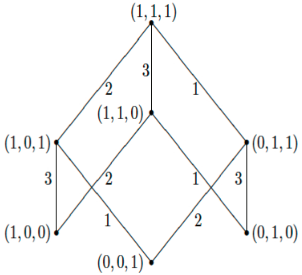
1. For K_a, we have S5 (and optionally K, T, S4, KD45, etc.).
2. $[\varphi!]p \leftrightarrow (\varphi \to p)$, $\quad [\varphi!]\psi \wedge \psi' \leftrightarrow ([\varphi!]\psi \wedge [\varphi!]\psi')$.
3. $[\varphi!]\neg\psi \leftrightarrow (\varphi \to \neg[\varphi!]\psi)$, $\quad [\varphi!]K_a\psi \leftrightarrow (\varphi \to K_a[\varphi!]\psi)$.
4. Inference rule: If ψ, then $[\varphi!]\psi$.

As is clear from the axioms, formulas in PAL can be rewritten as normal EL formulas without the public announcement operator $[\varphi!]$. However, in general, $[\varphi!]\varphi$ does not hold.

Problem.
Let φ be $p \wedge \neg K_a p$. Show that there exists a model where $[\varphi!]\varphi$ does not hold.

Back to the "Muddy Children Puzzle"

Now, let's return to the "Muddy Children Puzzle" where $p = p_1 \vee p_2 \vee p_3$ is announced and becomes common knowledge. As a result, the state $(0, 0, 0)$ is no longer possible, and the model M changes to M', as shown below.

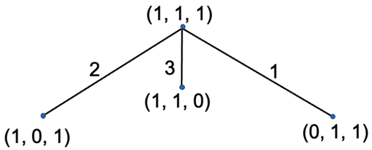


When looking at the state $(0, 0, 1)$, there are no states connected by $\underset{3}{—}$ (except for the child themselves), so we have $M', (0, 0, 1) \models \mathsf{K}_3 p_3$. Thus,

$$M, (0, 0, 1) \models [p!]\mathsf{K}_3 p_3.$$

Puzzle State Progression

If child 3 announces that he does not know if he have mud on his forehead ($\neg \mathsf{K}_3 p_3$), then everyone can infer they are not in any state other than $(0, 0, 1)$. Similarly, since $M', (1, 0, 0) \models \mathsf{K}_1 p_1$, the announcement by child 1 eliminates the possibility of the state $(1, 0, 0)$. Likewise, child 2's announcement eliminates the possibility of the state $(0, 1, 0)$. Thus, the remaining states are as follows:



In this model M'', when looking at the state $(1, 0, 1)$, no states are connected by $\underset{1}{—}$ or $\underset{3}{—}$ (except for the child themselves), so we have:

$$M'', (1, 0, 1) \models \mathsf{K}_1 p_1 \wedge \mathsf{K}_3 p_3.$$

Similarly, for states $(1, 1, 0)$ and $(0, 1, 1)$, the two children with mud on their foreheads will know they have mud on their own forehead.

Final State of the Puzzle

Finally, in the state $(1, 1, 1)$, no child can determine if he has mud on their forehead at this point in model M''. However, if everyone announces they do not know, then all states where exactly two children have mud are eliminated, and only the state $(1, 1, 1)$ remains. Therefore, in the end, everyone will know they have mud on their own forehead.
This concludes the explanation of the muddy children puzzle. Recent developments in modal logic are remarkable, and if possible, I would like to explore this topic further in the future.

Thank you for your attention!