Modal logic and the characterization theorem

Overview of this section:

- Predicate logic has an **undecidable** satisfiability problem and a model checking problem of **high complexity** (PSPACE), hence not perfectly suited for verification of systems.
- We introduce **modal logic**, a fragment of predicate logic whose models are Kripke structures (essentially vertex-labeled directed graphs).
- We show: modal logic has a **decidable** satisfiability problem and a polynomial time decidable model checking problem.
- Temporal logics used in verification (like modal logic, LTL, CTL, $\mu$-calculus) typically do not distinguish structures that are **bisimulation equivalent**.
- We show bisimulation-invariant predicate logic **coincides** with modal logic!
We fix a countable set $\mathbb{P}$ of unary relational symbols.

The set $\text{ML}$ of formulas of modal logic is the smallest set that satisfies the following:

- $p \in \text{ML}$ for each $p \in \mathbb{P}$,
- if $\varphi \in \text{ML}$ then $\neg \varphi \in \text{ML}$,
- if $\varphi_1, \varphi_2 \in \text{ML}$ then $(\varphi_1 \lor \varphi_2) \in \text{ML}$,
- if $\varphi_1, \varphi_2 \in \text{ML}$ then $(\varphi_1 \land \varphi_2) \in \text{ML}$,
- if $\varphi \in \text{ML}$ then $\Diamond \varphi \in \text{ML}$, and
- if $\varphi \in \text{ML}$ then $\Box \varphi \in \text{ML}$.

Example.

\[
((p_1 \land p_2) \lor \neg \Box(p_3 \lor \Diamond \Diamond (p_2 \land \neg p_4))) \in \text{ML}
\]
A Kripke structure is a logical structure $\mathcal{A}$ over some signature $S = P \cup \{E\}$, where $P \subseteq \mathcal{P}$ is finite and where $E$ is a binary relational symbol.

For each formula $\varphi \in \text{ML}$ and each suitable Kripke structure $\mathcal{A}$ and each $a \in U_\mathcal{A}$ we define $(\mathcal{A}, a) \models \varphi$ inductively as follows:

- $(\mathcal{A}, a) \models p$ if and only if $a \in p^\mathcal{A}$,
- $(\mathcal{A}, a) \models \neg \varphi$ if and only if $(\mathcal{A}, a) \not\models \varphi$,
- $(\mathcal{A}, a) \models \varphi_1 \lor \varphi_2$ if and only if $(\mathcal{A}, a) \models \varphi_1$ or $(\mathcal{A}, a) \models \varphi_2$,
- $(\mathcal{A}, a) \models \varphi_1 \land \varphi_2$ if and only if $(\mathcal{A}, a) \models \varphi_1$ and $(\mathcal{A}, a) \models \varphi_2$,
- $(\mathcal{A}, a) \models \lozenge \varphi$ if and only if $(\mathcal{A}, b) \models \varphi$ for some $b \in U_\mathcal{A}$ with $(a, b) \in E^\mathcal{A}$, and
- $(\mathcal{A}, a) \models \Box \varphi$ if and only if $(\mathcal{A}, b) \models \varphi$ for all $b \in U_\mathcal{A}$ with $(a, b) \in E^\mathcal{A}$.
The size $|\varphi|$ of a formula $\varphi$ is defined as follows:

- $|p| = 1$ if for each $p \in \mathbb{P}$,
- $|\neg \varphi| = |\varphi| + 1$,
- $|\varphi_1 \lor \varphi_2| = |\varphi_1 \land \varphi_2| = |\varphi_1| + |\varphi_2| + 1$, and
- $|\Diamond \varphi| = |\Box \varphi| = |\varphi| + 1$.

The set of subformulas $\text{subf}(\varphi)$ of a formula $\varphi$ is defined as follows:

- $\text{subf}(p) = \{p\}$ for each $p \in \mathbb{P}$,
- $\text{subf}(\neg \varphi) = \{\neg \varphi\} \cup \text{subf}(\varphi)$,
- $\text{subf}(\varphi_1 \circ \varphi_2) = \{\varphi_1 \circ \varphi_2\} \cup \text{subf}(\varphi_1) \cup \text{subf}(\varphi_2)$ for each $\circ \in \{\lor, \land\}$, and
- $\text{subf}(\circ \varphi) = \{\circ \varphi\} \cup \text{subf}(\varphi)$ for each $\circ \in \{\Diamond, \Box\}$.

Note that $|\text{subf}(\varphi)| = |\varphi|$. 
Theorem. The following problem is decidable in polynomial time:
INPUT: An ML formula $\varphi$, a suitable Kripke structure $\mathcal{A}$ and some $a \in U_{\mathcal{A}}$.
QUESTION: $(\mathcal{A}, a) \models \varphi$?

Proof (Idea only, details not difficult): For each subformula $\psi$ of $\varphi$ compute the set of $b \in U_{\mathcal{A}}$ such that $(\mathcal{A}, b) \models \psi$. 

Model checking of modal logic
As expected we say that an ML formula $\varphi$ is \textbf{satisfiable} if there exists a suitable Kripke structure $\mathcal{A}$ and some $a \in U_{\mathcal{A}}$ such that $(\mathcal{A}, a) \models \varphi$.

\textbf{Theorem. (Small model property of modal logic)} Assume $\varphi \in \text{ML}$ is satisfiable. Then there exists a suitable Kripke structure $\mathcal{A}$ and some $a \in U_{\mathcal{A}}$ such that

- $(\mathcal{A}, a) \models \varphi$ and
- $|U_{\mathcal{A}}| \leq 2^{|\varphi|}$.

\textbf{Corollary.} Satisfiability of ML is decidable.
Lemma. For each formula $\varphi$ there exists a formula $\overline{\varphi}(x)$ of predicate logic such that for each suitable Kripke structure $\mathcal{A}$ and each $a \in U_\mathcal{A}$ we have

$$(\mathcal{A}, a) \models \varphi \iff \mathcal{A}[x/a] \models \overline{\varphi}.$$ 

Proof.

We define the translation $\overline{\varphi}$ inductively as follows:

- $\overline{\overline{p}(x)} = p(x)$ for each $p \in \mathbb{P}$,
- $\overline{\overline{\neg \varphi}(x)} = \neg \overline{\varphi}(x)$,
- $\overline{\overline{\varphi_1 \circ \varphi_2}(x)} = \overline{\varphi_1}(x) \circ \overline{\varphi_2}(x)$ for each $\circ \in \{\lor, \land\}$,
- $\overline{\overline{\diamond \varphi}(x)} = \exists y(E(x,y) \land \overline{\varphi}(y))$, and
- $\overline{\overline{\Box \varphi}(x)} = \forall y(E(x,y) \rightarrow \overline{\varphi}(y))$.

Note that $\overline{\varphi}$ requires at most two free variables.
Predicate logic vs. modal logic

**Question.** Is every property expressible in predicate logic over Kripke structures expressible in modal logic?

**Answer.** No! Take $\varphi(x) = \exists y E(x, y) \land E(y, x)$ expressing that there exists a cycle of length two (proof later).

We will concern ourselves with the following questions for the rest of this section:

- How to prove that the above property is **not** expressible in modal logic?
- How must we **restrict** the properties expressible in predicate logic to obtain the properties expressible in modal logic?
Bisimulation equivalence

Let $A$ and $B$ be two Kripke structures suitable for some finite signature $S$. A **bisimulation between $A$ and $B$** is a relation $R \subseteq U_A \times U_B$ such that for each $(a, b) \in R$ the following holds:

- $a \in p^A$ if and only if $b \in p^B$ for each $p \in \mathbb{P},$
- for each $(a, a') \in E^A$ there exists some $(b, b') \in E^B$ such that $(a', b') \in R$, and
- for each $(b, b') \in E^B$ there exists some $(a, a') \in E^A$ such that $(a', b') \in R$.

Given $a \in U_A$ and $b \in U_B$ we say $(A, a)$ and $(B, b)$ are **bisimilar** (we write $(A, a) \sim (B, b)$ for short) if $(a, b) \in R$ for some bisimulation $R$ between $A$ and $B$. 
Bisimulation as a game

Consider the following bisimulation game from $\langle (A_1, a_1), (A_2, a_2) \rangle$ (on signature $S$) played between Attacker and Defender:

- Attacker chooses some $i \in \{1, 2\}$ and some $(a_i, a_i') \in E^{A_i}$.
- Defender answers with some $(a_{3-i}, a'_{3-i}) \in E^{A_{3-i}}$.
- The game continues in $\langle (A_1, a_1'), (A_2, a_2') \rangle$.

Who wins a play?

- If along the play there is some pair $\langle (A_1, x_1), (A_2, x_2) \rangle$ and a $p \in S$ such that $x_1 \in p^{A_1} \Leftrightarrow x_2 \in p^{A_2}$, then Attacker wins!
- If the play ends such that Defender cannot answer Attacker’s move (no successor), then Attacker wins.
- If the play ends $\langle (A_1, x_1), (A_2, x_2) \rangle$, where $x_1, x_2$ are both dead ends, then Defender wins.
- Defender wins each infinite play.
For each $\ell \geq 0$ we define the finite approximant $\sim_\ell$ between $A$ and $B$ (over signature $S$) as follows:

$$\sim_0 = \{(a, b) \in U_A \times U_B \mid \forall p \in S \cap \mathbb{P} : a \in p^A \iff b \in p^B\},$$

$$\sim_{\ell+1} = \{a \sim_\ell b \mid \forall (a, a') \in E^A \exists (b, b') \in E^B : a' \sim_\ell b' \land \forall (b, b') \in E^B \exists (a, a') \in E^A : a' \sim_\ell b'\}$$

One easily sees that $\sim_\ell$ is an equivalence relation for each $\ell \in \mathbb{N}$.

Moreover $\subseteq \sim_\ell$ for each $\ell \in \mathbb{N}$. 
Theorem. Defender has a winning strategy from \( ((A, a), (B, b)) \) if and only if \( (A, a) \sim (B, b) \).

Theorem. Defender has a winning strategy from \( ((A, a), (B, b)) \) in the \( \ell \) round game if and only if \( (A, a) \sim_\ell (B, b) \).

Fact. Bisimulation is insensitive to disjoint sums: We have \( (A, a) \sim (B, b) \) if and only if \( (A + C, a) \sim (B, b) \), where \( A + C \) denotes the disjoint sum of \( A \) and \( C \).
\(
\sim \ell \text{ and } \text{ML}_\ell
\)

For each \( \varphi \in \text{ML} \), let us define the modal depth \( \text{md}(\varphi) \) as follows:

- \( \text{md}(p) = 0 \) for each \( p \in \mathbb{P} \),
- \( \text{md}(\neg \varphi) = \text{md}(\varphi) \),
- \( \text{md}(\varphi_1 \lor \varphi_2) = \text{md}(\varphi_1 \land \varphi_2) = \max\{\text{md}(\varphi_1), \text{md}(\varphi_2)\} \), and
- \( \text{md}(\lozenge \varphi) = \text{md}(\Box \varphi) = \text{md}(\varphi) + 1 \).

For each \( \ell \geq 0 \) define \( \text{ML}_\ell = \{\varphi \in \text{ML} | \text{md}(\varphi) = k\} \).

**Lemma.** Let \( \ell \in \mathbb{N} \). Let \( A \) and \( B \) be Kripke structures over a finite signature \( S \) and let \( a \in U_A \) and \( b \in U_B \). Then we have:

1. \( \sim_\ell \) has finitely many equivalence classes.
2. \((A, a) \sim_\ell (B, b) \) iff \((A, a) \models \varphi \iff (B, b) \models \varphi \) for all \( \varphi \in \text{ML}_\ell \).
3. Each equivalence class of \( \sim_\ell \) is definable by some \( \text{ML}_\ell \) formula.
A Kripke structure $\mathcal{A}$ is a tree (structure) if $(U_\mathcal{A}, E^\mathcal{A})$ is a directed tree, i.e. $\mathcal{A}$ is acyclic, the symmetric closure of $E^\mathcal{A}$ is connected and each node has at most one incoming edge.

A tree $\mathcal{A}$ has depth $\ell$ if each path in $\mathcal{A}$ has length at most $\ell$.

For $\ell \geq 0$ we say $(\mathcal{A}, a)$ is $\ell$-locally a tree structure if $\mathcal{A} \upharpoonright N_\ell(a)$ is a tree structure.

Lemma.

1. $(\mathcal{A}, a) \sim_\ell (\mathcal{B}, b)$ iff $(\mathcal{A} \upharpoonright N_\ell(a), a) \sim_\ell (\mathcal{B} \upharpoonright N_\ell(b), b)$.
2. If $\mathcal{A}$ and $\mathcal{B}$ are trees of depth $\ell$, then

   $$(\mathcal{A}, a) \sim_\ell (\mathcal{B}, b) \iff (\mathcal{A}, a) \sim (\mathcal{B}, b).$$
The unravelling of $\mathcal{A}$ at some $a \in U_{\mathcal{A}}$ is the tree $\mathcal{A}_a^*$, where

- $U_{\mathcal{A}_a^*} = \{ \pi | \pi \text{ is a finite path in } \mathcal{A} \text{ starting at } a \}$.
- $E_{\mathcal{A}_a^*} = \{ (\pi, \pi') \in (U_{\mathcal{A}_a^*})^2 | \exists (u, v) \in E^\mathcal{A} : \pi' = \pi(x, y) \}$.

**Lemma.** Let $\mathcal{A}$ be a Kripke structure and let $a \in U_{\mathcal{A}}$. Then we have

- $(\mathcal{A}_a^*, a) \sim (\mathcal{A}, a)$.
- $(\mathcal{A}_a^* \upharpoonright N_\ell(a), a) \sim_\ell (\mathcal{A}, a)$. 
A predicate logic formula $F(x)$ over a Kripke signature is **bisimulation invariant** if the following holds for all suitable $(A, a), (B, b)$:

$$(A, a) \sim (B, b) \implies (A_{[x/a]} \models F \iff B_{[x/b]} \models F)$$

A predicate logic formula $F(x)$ over a Kripke signature is **$\ell$-local** if for all suitable $(A, a)$ we have

$$A_{[x/a]} \models F \iff A \upharpoonright N_\ell(a)_{[x/a]} \models F$$
The Characterization Theorem

Theorem (van Benthem/Rosen, proof by Otto). The following are equivalent for any predicate logic formula $F(x)$ over a Kripke signature with $qr(F) = q$:

- $F(x)$ is bisimulation-invariant.
- $F(x)$ is logically equivalent to some $\text{ML}_\ell$ formula, where $\ell = 2^q - 1$.

The same holds when restricted to the class of finite Kripke structures.
Proof Outline of Characterization Theorem

We prove the Characterization Theorem in three steps:

(1) Any bisimulation invariant $F(x)$ of predicate logic is $\ell$-local for $\ell = 2^q - 1$, where $q = qr(F)$.

(2) Any bisimulation invariant $F(x)$ that is $\ell$-local is even invariant under $\ell$-bisimulation equivalence $\sim_\ell$.

(3) Any property invariant under $\ell$-bisimulation equivalence is definable in $\text{ML}_\ell$. 