Lecture 3: tree unravelling, bisimulations and the Hennessy-Milner theorem

September 15, 2016

Tree-like models

Definition

Let $\mathfrak{M}$ be of similarity type (O, τ). Set $u \prec v$ if there is some $\Delta \in O$ and some tuple $v_1 ... v_n$ such that $R_\Delta u v_1 ... v_n$ and $v \in \{v_1, ..., v_n\}$.

Definition

A model $\mathfrak{M}$ of similarity type (O, τ) is said to be *tree-like* if the structure $(W, \prec)$ is a tree. The root of this tree is then called the root of the model.

Note

For the basic modal language, a tree-like model (W, R, V) is just a tree with a valuation on it!

Tree unravelling

Intuition: encode all the information about possible transitions in a model in a tree-like structure.

Definition

Let $\mathfrak{M}$ be a model of similarity type (O, τ) and $w \in W$. Then the *unravelling* of $\mathfrak{M}$ at w is defined to be (W', R', V') where:

- W' consists of all non-empty words over W beginning with w
- $R'_\Delta = \{\langle \vec{u}, \vec{u} \cdot v_1, \ldots, \vec{u} \cdot v_n \rangle \mid \langle \mathrm{last}(\vec{u}), v_1, \ldots, v_n \rangle \in R_\Delta\}$
- $\vec{u} \in V'(p)$ iff $\mathrm{last}(\vec{u}) \in V(p)$

Note that the root of the unravelling is just w, viewed as a word of a single letter!

Proposition

Let $\mathfrak{M}$ be any model, $w \in W$ and let $\mathfrak{M}'$ be the unravelling of $\mathfrak{M}$ at w. Then:

$$\mathfrak{M}', w \quad \leftrightsquigarrow \quad \mathfrak{M}, w$$

Proof.

The map last : $W' \to W$ is a bounded morphism! ∎

Tree-like model property

Theorem

Let φ be any modal formula. If φ is satisfied in some model, it is also satisfied in a tree-like model.

Modal logic and trees

Proposition

K *is the modal logic of trees.*

Proof.

If a formula φ belongs to **K** then it is valid on all frames, hence it is certainly valid on all trees in particular.
Conversely, if φ is *not* valid on all frames, then $\neg\varphi$ is satisfied on some pointed model. Hence $\neg\varphi$ is also true on the tree unravelling, and thus φ is not valid on all trees. ∎

A category of Kripke models

Proposition

Let $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3$ be Kripke models. Then:

- *The identity map $\mathrm{Id} : W_i \to W_i$ is a bounded morphism from $\mathfrak{M}_i$ to itself.*
- *If $f : \mathfrak{M}_1 \to \mathfrak{M}_2$ and $g : \mathfrak{M}_2 \to \mathfrak{M}_3$ are bounded morphisms, then the composition $g \circ f : \mathfrak{M}_1 \to \mathfrak{M}_3$ is also a bounded morphism.*

The mathematical term for this situation is that Kripke models form a *category*, in which the arrows are bounded morphisms. This categorical perspective on modal logic culminates in *co-algebraic logic* - but that is a different course entirely!

Question:

Is there a single, general and natural concept that covers disjoint unions, generated submodels and bounded morphisms?

Bisimulation: a unifying concept

Idea

Two pointed models $\mathfrak{M}, w$ and $\mathfrak{M}', w'$ for the basic modal language are bisimilar iff:

- w and w' satisfy the same propositional variables,
- every successor of w is bisimilar with a successor of w',
- every successor of w' is bisimilar with a sucessor of w.

But this is circular...

Bisimulations for the basic modal language

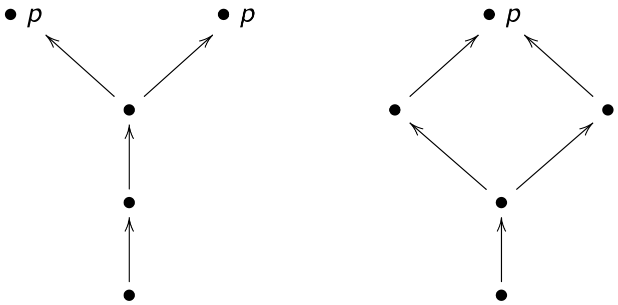
Definition

Let $\mathfrak{M}, \mathfrak{M}'$ be models for the basic modal language, and let $Z \subseteq W \times W'$. Then Z is said to be a *bisimulation* for $\mathfrak{M}, \mathfrak{M}'$ if, whenever wZw':

- (Atomic condition) $w \in V(p)$ iff $w' \in V'(p)$, for all p,
- (Forth condition) if wRv then there exists $v' \in W'$ such that $w'R'v'$ and vZv'
- (Back condition) if $w'R'v'$ then there exists $v \in W$ such that wRv and vZv'.

The pointed models $\mathfrak{M}, w$ and $\mathfrak{M}', w'$ are said to be *bisimilar*, written $\mathfrak{M}, w \underline{\longleftrightarrow} \mathfrak{M}', w'$, if *there exists* a bisimulation Z relating w to w'.

Example



Bisimulations (general case)

Definition

Let $\mathfrak{M}, \mathfrak{M}'$ be models for a given similarity type, and let $Z \subseteq W \times W'$. Then Z is said to be a *bisimulation* for $\mathfrak{M}, \mathfrak{M}'$ if, whenever wZw':

- (Atomic condition) $w \in V(p)$ iff $w' \in V'(p)$, for all p,
- (Forth condition) if $R_\Delta wv_1 \ldots v_n$ then there exist $v'_1, \ldots, v'_n \in W'$ such that $R'_\Delta w' v'_1 \ldots v'_n$ and $v_i Z v'_i$
- (Back condition) if $R'_\Delta w' v'_1 \ldots v'_n$ then there exist $v_1, \ldots, v_n \in W$ such that $R_\Delta wv_1 \ldots v_n$ and $v_i Z v'_i$.

Proposition

Modal logic is bisimulation invariant:

$$\mathfrak{M}, w \underline{\longleftrightarrow} \mathfrak{M}', w' \quad \Rightarrow \quad \mathfrak{M}, w \leftrightsquigarrow \mathfrak{M}', w'$$

Bisimulations in computer science

Behavioural equivalence

Two processes (computer programs, operating systems, elevators, vending machines...) are said to be *behaviourally equivalent* if they cannot be distinguished by an external observer/user.

Formally: "processes" are generally modelled as labelled transition systems, and *behavioural equivalence is bisimilarity*!

Bisimulation invariance is *the* defining property of modal logic:

The van Benthem characterization theorem

"Modal logic is the bisimulation invariant fragment of FOL"

Disjoint unions, generated submodels and bounded morphisms are instances of bisimulations. In particular:

Proposition

A map $f : \mathfrak{M} \to \mathfrak{M}'$ is a bounded morphism iff its graph is a bisimulation.

Note

It is *not* the case that all modally equivalent models are bisimilar!

Proof.

We can construct modally equivalent models, one with arbitrarily long but only finite paths, and one with an infinite path... ∎

Pebble games

A neat explanation is given by "pebble games", similar to EF-games in model theory:

n-round pebble game

Two-player game, "Spoiler" vs. "Duplicator". Start with one "pebble" placed on each model. If the pebbles are place on worlds satisfying different propositional variables then the game ends and Spoiler wins. Otherwise Spoiler moves a pebble to a successor, Duplicator responds by moving the other pebble to a successor. This goes on for at most n rounds, and if either player gets stuck then the other player wins.

Modal depth (basic modal language)

- $\mathsf{md}(p) = \mathsf{md}(\bot) = 0$
- $\mathsf{md}(\neg\varphi) = \mathsf{md}(\varphi)$
- $\mathsf{md}(\varphi \vee \psi) = \max(\mathsf{md}(\varphi), \mathsf{md}(\psi))$
- $\mathsf{md}(\Diamond\varphi) = \mathsf{md}(\varphi) + 1$

Proposition

There are, up to logical equivalence, only finitely many formulas of modal depth $\leq n$.

Proposition

Let $\mathfrak{M}, w$ and $\mathfrak{M}', w'$ be any two pointed models. The following are equivalent:

- *Duplicator has a winning strategy against Spoiler in the n-round pebble game,*
- *$\mathfrak{M}, w$ and $\mathfrak{M}, w'$ satisfy the same formulas of modal depth $\leq n$.*

The infinite pebble game

Same as the n-round pebble game, but there are *no bounds* on the length of matches, and Duplicator wins all infinite matches.

Proposition

Let $\mathfrak{M}, w$ and $\mathfrak{M}', w'$ be any two pointed models. The following are equivalent:

- *Duplicator has a winning strategy against Spoiler in the infinite pebble game,*
- $\mathfrak{M}, w \underline{\longleftrightarrow} \mathfrak{M}, w'$.

Image-finite models

Recall the definition of the relation $\prec$ induced by a model.

Definition

Let $\mathfrak{M}$ be a model of any given similarity type. Then $\mathfrak{M}$ is said to be *image-finite* if, for all $u \in W$, the set

$$\{v \in W \mid u \prec v\}$$

is finite.

Note

Of course, every finite model is image-finite.

The Hennessy-Milner Theorem

Theorem

Let $\mathfrak{M}, w$ and $\mathfrak{M}', w'$ be any two image-finite pointed models. Then:

$$\mathfrak{M}, w \;\leftrightsquigarrow\; \mathfrak{M}', w' \text{ iff } \mathfrak{M}, w \underline{\longleftrightarrow} \mathfrak{M}', w'$$

Proof.

For image-finite models, *modal equivalence is a bisimulation*! ∎

PDL and safety for bisimulation

Definition

Let $\mathfrak{M}, \mathfrak{M}'$ be two models in the similarity type of regular PDL. We say that a relation Z between $\mathfrak{M}$ and $\mathfrak{M}'$ is an *atomic bisimulation* if it is a bisimulation between the models $(W, \{R_a\}_{a \in \mathcal{A}}, V)$ and $(W', \{R'_a\}_{a \in \mathcal{A}}, V')$.

Clearly, every bisimulation in this similarity type is an atomic bisimulation, but the converse is not generally true. However:

Proposition (Safety for bisimulation)

Let Z be any relation between $\mathfrak{M}$ and $\mathfrak{M}'$. If both $\mathfrak{M}$ and $\mathfrak{M}'$ are regular models, then Z is a bisimulation iff it is an atomic bisimulation.

By contrast, "converse" is *not* safe for bisimulation!

The lattice of bisimulations

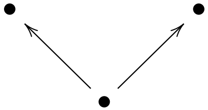
Proposition

The union of any family of bisimulations is a bisimulation, hence the bisimulations between any two models form a complete lattice under set inclusion.

Note

Meet is *not* intersection!

Example: consider the family of all bisimulations relating the root of the following model to itself:



Finally:

Proposition

Let Z_1 be a bisimulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$, and let Z_2 be a bisimulation between $\mathfrak{M}_2$ and $\mathfrak{M}_3$. Then the composition $Z_1; Z_2$ is a bisimulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$.

Corollary

"Bisimilarity" is an equivalence relation.