

# Finite Models for Coalgebraic Modal Logic

---

Lutz Schröder

# Introduction

- Coalgebra: generic modelling paradigm for reactive systems
- Suitable specification logic: **coalgebraic modal logic** (CML)
  - Respects behavioral equivalence, i.e. **encapsulation** of the state space
  - Sufficiently intuitive for use in actual software specification (CCSL, CoCASL)
- CML subsumes many (more or less) well-known modal logics:
  - Hennessy-Milner logic
  - Graded modal logic ( $[k]\phi$ ,  $k \in \mathbb{N}$ )
  - Probabilistic modal logic ( $\langle p \rangle$ ,  $p \in \mathbb{Q}$ )

## Here,

- We exhibit a **finite model** construction for CML
- Corollary: a (known) **weak completeness result** (Pattinson 03)
- Prove that CML is **always** axiomatizable in rank 1
- Corollary: CML has the (semantic) **finite model property**
- Obtain **decidability** for a large class of functors (Pattinson 03: functors preserving finite sets)
- Obtain general **complexity bound**

# Modal Logic in CoCASL

```

spec NoHOGGING =
  sort In
  sort State
  then free %modal {
    type Set ::= {} | {--}(State) | -- ∪ --(Set; Set)
    op -- ∪ -- : Set × Set → Set,
      assoc, comm, idem, unit {}
  }
  then cotype State ::= (next : In → Set)
    •  $\forall i : In . \langle next(i)^* \rangle [next(i)] \text{ false}$ 

```

# Coalgebra

$T : \mathbf{Set} \rightarrow \mathbf{Set}$  functor

Coalgebra  $(X, \xi) = \text{map } \xi : X \rightarrow TX$

Morphisms:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \downarrow \xi & & \downarrow \zeta \\
 TX & \xrightarrow{Tf} & TY
 \end{array}$$

$(Z, \zeta)$  **final**  $\iff \forall (X, \xi). \exists! f : (X, \xi) \rightarrow (Z, \zeta)$ .

## Predicate Liftings

A **predicate lifting** (Pattinson 04) for  $T$  is a natural transformation

$$\lambda : 2^- \rightarrow 2^{T^{op}}$$

Predicate lifting  $\lambda$  has **transpose**

$$\lambda^b : T \rightarrow 2^{2^-}.$$

A set  $\Lambda$  of predicate liftings is **separating** if

$$(\lambda_X^b : T \rightarrow 2^{(2^-)})_{\lambda \in \Lambda}$$

is injective at each  $X$ .

# Coalgebraic Modal Logic

$\Lambda$  set of predicate liftings:  $\mathcal{L}(\Lambda)$  defined by

$$\phi ::= \perp \mid \phi \wedge \psi \mid \neg\phi \mid [\lambda] \phi;$$

then define  $\vee$  etc.

$\kappa$  regular cardinal:  $\mathcal{L}^\kappa(\Lambda)$  with  $\kappa$ -ary conjunction.

Semantics in  $T$ -coalgebra  $(X, \xi)$ :

$$x \models_{(X, \xi)} [\lambda] \phi \iff \xi(x) \in \lambda_X \llbracket \phi \rrbracket_{(X, \xi)}.$$

# CML vs. Behavioral Equivalence

$\mathcal{L}^\kappa(\Lambda)$  is **adequate**, i.e. behaviorally equivalent states are logically indistinguishable under  $\mathcal{L}^\kappa(\Lambda)$ .

Conversely:

**Theorem** (Pattinson 04, LS 05) Let  $T$  be  $\kappa$ -accessible and let  $\Lambda$  be a separating set of predicate liftings. Then  $\mathcal{L}^\kappa(\Lambda)$  is **expressive**, i.e. logically indistinguishable states are behaviorally equivalent.

## Example: Hennessy-Milner Logic

$$TX = \mathfrak{P}_\omega(I \times X)$$

$T$ -coalgebras are **labelled transition systems**

Separating set  $\{\lambda^{\forall, i} \mid i \in I\}$ , where

$$\lambda_X^{\forall, i}(A) = \{B \subset I \times X \mid (i, x) \in B \Rightarrow x \in A\}.$$

Then  $[\lambda^{\forall, i}] = \square_i$

## Example: Atomic Propositions

$TX = \wp(V)$ ,  $V$  set of **atomic propositions**

Separating set  $\{\lambda^a \mid a \in V\}$ , where

$$\lambda^a(A) = \{C \subset V \mid a \in C\}.$$

Then  $[\lambda^a]\phi$  is just the atomic proposition  $a$ .

Combine this canonically with other functors, e.g.

$$TX = \wp(X) \times \wp(V)$$

for standard modal logic.

## Example: Graded Modal Logic

$TX = \mathcal{B}_{\mathbb{N}}X$  **finite multisets**  $\sum n_i x_i$ ,  $n_i \in \mathbb{N}$ ,  $x_i \in X$

$\mathcal{B}_{\mathbb{N}}$ -coalgebras are **multigraphs**, where edges have multiplicities

Separating set  $\{\lambda^k \mid k \in \mathbb{N}\}$ , where

$$\lambda_X^k(A) = \left\{ \sum n_i x_i \mid \sum_{x_i \notin A} n_i \leq k \right\}$$

Non-normal operators  $[k] = [\lambda^k]$  of **graded modal logic**

Variant: replace  $\mathbb{N}$  by  $\mathbb{Z} \rightsquigarrow$  non-monotonic operators.

## Example: Probabilistic Modal Logic

$D_\omega X$  probability distributions  $P$  with finite support

$TX = D_\omega X \times \mathfrak{P}(V)$  ( $V \neq \emptyset$  to avoid triviality).

$T$ -coalgebras are **probabilistic transition systems** or **probabilistic type spaces** (Heifetz/Mongin 01).

(Similarly: **reactive** and **generative probabilistic automata**, Bartels et al. CMCS 03).

Separating set: atomic propositions and  $\{\lambda^p \mid p \in [0, 1] \cap \mathbb{Q}\}$ ,

$$\lambda^p(A) = \{P \mid PA \geq p\}.$$

Modal operators  $\langle p \rangle = [\lambda^p]$  of **probabilistic modal logic**.

# Compactness

All of the above are **non-compact**

Not necessarily due to size restrictions:

$$\Phi = \{\langle 1 - 1/n \rangle a \mid n \in \mathbb{N}\} \cup \{\neg \langle 1 \rangle a\}$$

All finite subsets of  $\Phi$  are satisfiable, but not  $\Phi$ .

# Proof Systems

(Pattinson 03, Cirstea/Pattinson 04, Kupke et al. 04)

**Axiom set**  $Ax$  of **rank-1-clauses**, i.e. clauses over atoms

$$[\lambda]\phi, \text{ where } \lambda \in \Lambda, \phi \in \text{Prop}(V)$$

Deduction:

- Propositional reasoning
- Instances of axioms
- **Congruence rule**

$$\frac{\phi \leftrightarrow \psi}{[\lambda]\phi \leftrightarrow [\lambda]\psi}$$

## Reflexivity

Rank-1-clause  $\phi$  is valid if (essentially: iff)  $\phi\sigma$  holds for all  $\wp(X)$ -valuations  $\sigma$

**Definition**  $Ax$  is **reflexive** if every clause over atoms  $[\lambda]A$ ,  $A \subset X$ , that holds in  $TX$  is **derivable**.

Reflexive sets of valid clauses induce sound and **weakly complete** proof systems (Pattinson 03, Cirstea/Pattinson 04).

**Theorem** The set of all valid rank-1-clauses is reflexive

PROOF: Show that rules with premises of rank 0 and conclusions of rank 1 are derivable.

# Atoms and Hintikka Sets

- Set  $\Sigma$  of formulae is **closed**  $\iff$ 
  - closed under subformulae and
  - closed under **normalized negation**  $\sim$ .
- **Atom** = maximal (formally) consistent subset of  $\Sigma$ ;
- **Hintikka** set  $A \subset \Sigma$ :
  - $\perp \notin A$ ,
  - $\phi \wedge \psi \in A \iff \phi \in A \wedge \psi \in A$
  - $\phi \in A \iff \sim \phi \notin A$ .

# The Finite Model Construction

Construct model from closed  $\Sigma$ :

- States = atoms
- Evolution map  $\xi$ : require, for all  $[\lambda]\phi \in \Sigma$ ,

$$\xi(A) \in \lambda\{B \mid \phi \in B\} \iff [\lambda]\phi \in A \quad (*)$$

- $\xi$  exists if  $Ax$  is reflexive
- **Truth lemma**:  $A \models \phi \iff \phi \in A$

Apply this to closure  $\Sigma(\phi)$  of  $\{\phi\}$ .

## Fallout from the FMC

- $\phi$  consistent  $\Rightarrow$  satisfiable in **small** finite model ( $\leq 2^{|\phi|}$ )
- Corollary: **weak completeness** —  
reflexive sets induce weakly complete proof systems
- Corollary: **Finite model property** —  
every satisfiable formula is satisfiable in a (small) finite model  
(Proof: every functor admits a reflexive set)

# The Existence Problem

$X$  finite set,

$\phi$  conjunctive clause over atoms  $[\lambda]a$

$\sigma$   $\wp(X)$ -valuation:

Decide whether  $\phi\sigma$  is satisfiable in  $TX$ .

## A Decision Procedure

**Truth lemma** needs only Hintikka sets satisfying (\*).

Thus, given a decision procedure for  $\Lambda$ -existence:

**Algorithm 1:** For all sets  $S$  of Hintikka sets:

1. if  $\forall A \in S. \phi \notin A$  then continue
2. if

$$\bigwedge_{[\lambda]\phi \in A} [\lambda]\{B \in S \mid \psi \in B\} \wedge \bigwedge_{\sim[\lambda]\phi \in A} \neg[\lambda]\{B \in S \mid \psi \in B\}$$

is satisfiable for all  $A \in S$  then output **yes** else continue

Failure for all  $S \Rightarrow$  output **no**

# Decidability, Semidecidability, Complexity

**Theorem** If  $\Lambda$ -existence is decidable, then satisfiability is decidable for  $\mathcal{L}(\Lambda)$ .

**Algorithm 2:** Same as Algorithm 1, but choose  $S$  non-deterministically

**Theorem** If  $\Lambda$ -existence is semidecidable, then satisfiability is semidecidable for  $\mathcal{L}(\Lambda)$ .

**Theorem** If  $\Lambda$ -existence is in  $NP$ , then satisfiability is in  $NEXPTIME$ .

# Examples

- Graded modal logic
  - $\Lambda$ -existence via integer linear programming, in  $NP$
  - thus: GML is in  $NEXPTIME$
  - known to be in  $PSPACE$  (Tobies 01)
- Probabilistic modal logic
  - $\Lambda$ -existence via linear programming, in  $P$
  - thus: PML is in  $NEXPTIME$
  - Decidability of PML is implicit in Heifetz/Mongin 01, but no complexity bound.

# Conclusion

- Have established a finite model property for coalgebraic modal logic
- obtained weak completeness and **decidability**
- CML is frequently in *NEXPTIME*
- Recover known decidability results for GML and PML
- First complexity bound for PML

# Future Work

- Better generic bound? (Limit: *PSPACE*)
- Better methods/bounds under more specific conditions (shallow model methods)?
- Strong completeness
  - using infinitary rules, or
  - under ‘unboundedness’ conditions?