Modal Separation Logics and Friends

Stéphane Demri

CNRS

iMF^2, University of Udine

Udine, February 2019

Updating models

- Fascinating realm of (modal) logics updating models:
  - logics of public announcement [Lutz, AAMAS'06]
  - sabotage modal logics [van Benthem, 2002]
  - relation-changing modal logics [Fervari, PhD 2014]
  - separation logics [Reynolds, LICS'02]
  - modal separation logic DMBI [Courtault & Galmiche, JLC 2018]
  - logics with reactive Kripke semantics [Gabbay, Book 2013]

Updating models

- Fascinating realm of (modal) logics updating models:
  - logics of public announcement [Lutz, AAMAS'06]
  - sabotage modal logics [van Benthem, 2002]
  - relation-changing modal logics [Fervari, PhD 2014]
  - separation logics [Reynolds, LICS'02]
  - modal separation logic DMBI [Courtault & Galmiche, JLC 2018]
  - logics with reactive Kripke semantics [Gabbay, Book 2013]
- This work: combining separation logics with modal logics, and relationships with quantified CTL.

Floyd-Hoare logic

- Hoare triple: $\{\phi\}\ \mathtt{C}\ \{\psi\}$ [Hoare, C. ACM 69; Floyd, 1967]
- Proof system with axioms and deduction rules to derive new triples.
- Approach at the heart of deductive verification.

Floyd-Hoare logic

- Hoare triple: $\{\phi\}\ \mathtt{C}\ \{\psi\}$ [Hoare, C. ACM 69; Floyd, 1967]
- Proof system with axioms and deduction rules to derive new triples.
- Approach at the heart of deductive verification.
- Strengthening preconditions / weakening postconditions:

$$\frac{\phi \Rightarrow \phi' \quad \{\phi'\}\ \mathtt{C}\ \{\psi\} \quad \psi \Rightarrow \psi'}{\{\phi\}\ \mathtt{C}\ \{\psi'\}}$$

- Hoare's assignment axiom:

$$\frac{}{\{\phi[\mathtt{e}/\mathtt{x}]\}\ \mathtt{x} \leftarrow \mathtt{e}\ \{\phi\}}$$

Frame rule and separating conjunction

- Frame rule:

$$\frac{\{\phi\}\ \mathtt{C}\ \{\psi\}}{\{\phi * \psi'\}\ \mathtt{C}\ \{\psi * \psi'\}}$$

  where $\mathtt{C}$ does not mess with ψ'.

$$\frac{\{\mathtt{x} \hookrightarrow 5\}\ {}^*\mathtt{x} \leftarrow 4\ \{\mathtt{x} \hookrightarrow 4\}}{\{\mathtt{x} \hookrightarrow 5 * \mathtt{y} \hookrightarrow 3\}\ {}^*\mathtt{x} \leftarrow 4\ \{\mathtt{x} \hookrightarrow 4 * \mathtt{y} \hookrightarrow 3\}}$$

- $(\mathfrak{s}, \mathfrak{h}) \models \mathtt{x} \hookrightarrow 5 * \mathtt{y} \hookrightarrow 3$ implies $(\mathfrak{s}, \mathfrak{h}) \models \mathtt{x} \neq \mathtt{y}$.

Memory states with one record field

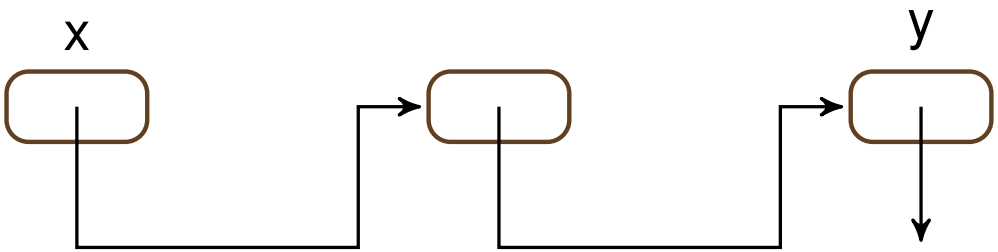
- Program variables PVAR $= \{\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \ldots\}$.

- $\mathtt{Loc}$: countably infinite set of locations
  $\mathtt{Val}$: countably infinite set of values with $\mathtt{Loc} \subseteq \mathtt{Val}$.

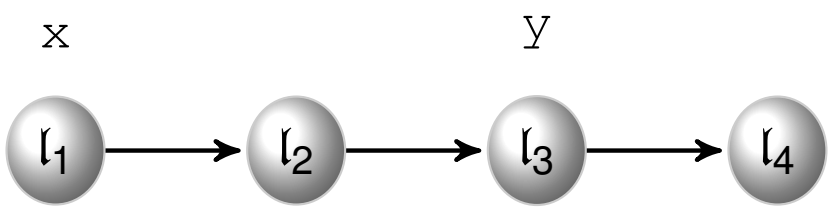
Memory states with one record field

- Program variables PVAR $= \{\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \ldots\}$.
- $\mathtt{Loc}$: countably infinite set of locations
  $\mathtt{Val}$: countably infinite set of values with $\mathtt{Loc} \subseteq \mathtt{Val}$.
- Memory state $(\mathfrak{s}, \mathfrak{h})$:
  - Store $\mathfrak{s}$: PVAR $\to \mathtt{Val}$.
  - Heap $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{\mathit{fin}} \mathtt{Val}$ (finite domain).
    (richer models, e.g. with $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{\mathit{fin}} \mathtt{Val}^k$)
  - In this talk, we assume $\mathtt{Loc} = \mathtt{Val} = \mathbb{N}$.

Graphical representation

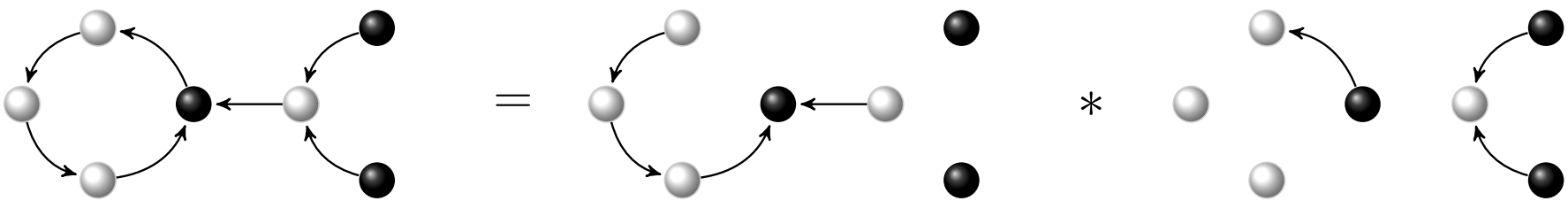


$$\mathfrak{s}(\mathtt{x}) = \mathfrak{l}_1$$
$$\mathfrak{s}(\mathtt{y}) = \mathfrak{l}_3$$
$$\mathrm{dom}(\mathfrak{h}) = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$$
$$\mathfrak{h}(\mathfrak{l}_1) = \mathfrak{l}_2$$
$$\mathfrak{h}(\mathfrak{l}_2) = \mathfrak{l}_3$$
$$\mathfrak{h}(\mathfrak{l}_3) = \mathfrak{l}_4$$



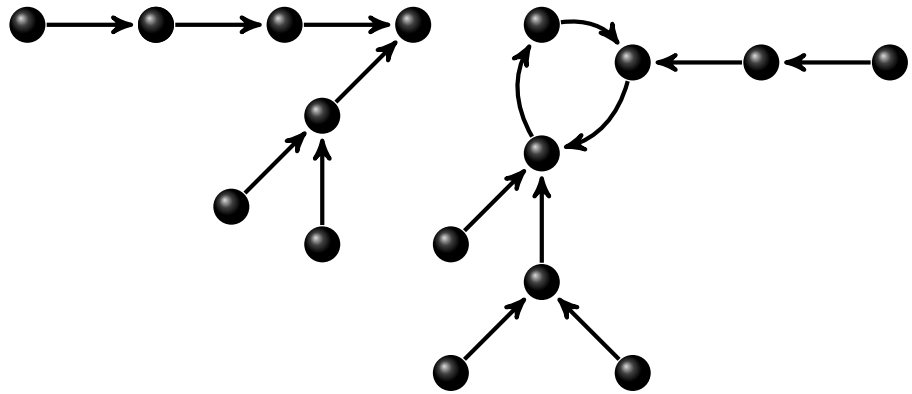
Disjoint heaps

- Disjoint heaps: $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$ (noted $\mathfrak{h}_1 \perp \mathfrak{h}_2$).
- When $\mathfrak{h}_1 \perp \mathfrak{h}_2$, disjoint heap $\mathfrak{h}_1 \uplus \mathfrak{h}_2$.



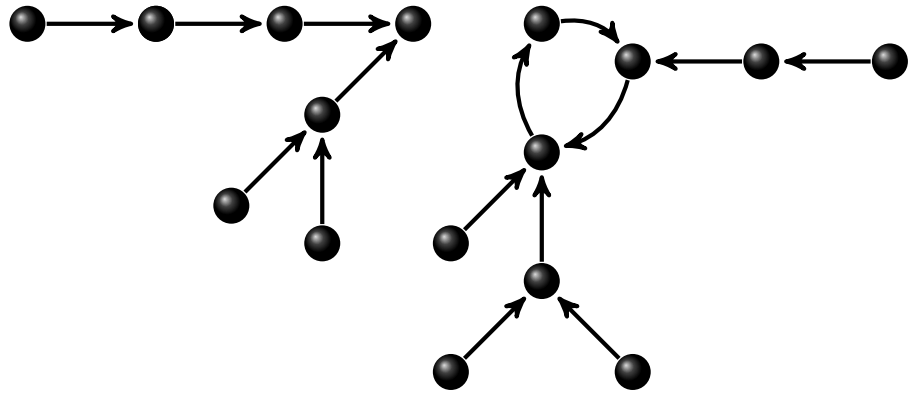
One record field leads to tree-like structures

- A forest of tree-like structures:

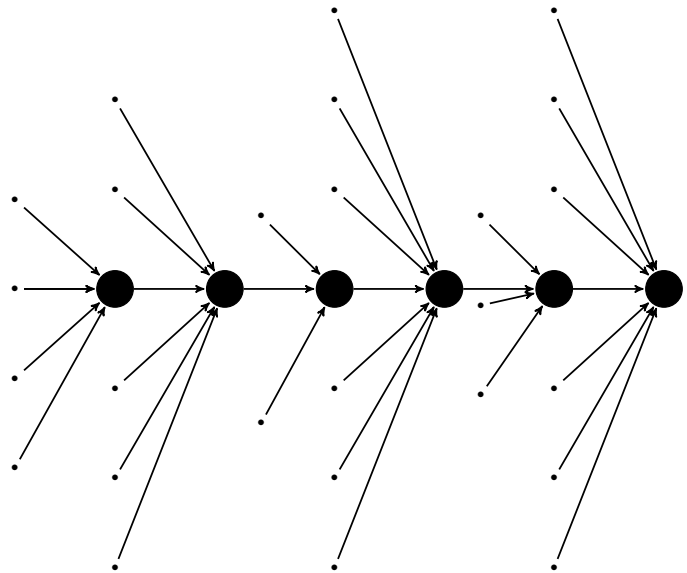


One record field leads to tree-like structures

- A forest of tree-like structures:



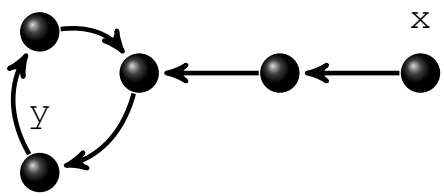
- A word-like structure:



Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, as an alternative to first-order separation logics.

- To propose a uniform framework so that the logics can be understood either as modal logics or as separation logics.

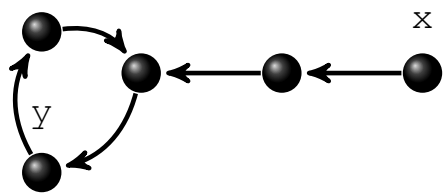


$(\mathtt{ls}(\mathtt{x},\mathtt{y}) * \top)$ vs. $@_{\mathtt{x}}\mathsf{EF}\mathtt{y}$

Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, as an alternative to first-order separation logics.

- To propose a uniform framework so that the logics can be understood either as modal logics or as separation logics.



$(\mathtt{ls}(\mathtt{x},\mathtt{y}) * \top)$ vs. $@_{\mathtt{x}}\mathsf{EF}\mathtt{y}$

- As by-products, we introduce variants of
  - hybrid separation logics [Brotherston & Villard, POPL'14]
  - relation-changing modal logics [Fervari, PhD 2014]

- Related work: description logics for shape analysis.
  See e.g. [Georgieva & Maier, SEFM'05; Calvanese et al., IFM'14]

Modal separation logic $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$

[Demri & Fervari, AiML'18]

- Formulae:

$$\phi ::= p \mid \mathtt{emp} \mid \neg\phi \mid \phi \vee \phi \mid \Diamond\phi \mid \langle \neq \rangle \phi \mid \phi * \phi$$

Modal separation logic $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$

[Demri & Fervari, AiML'18]

- Formulae:

$$\phi ::= p \mid \mathtt{emp} \mid \neg\phi \mid \phi \vee \phi \mid \Diamond\phi \mid \langle\neq\rangle\phi \mid \phi * \phi$$

- Models $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$:
  - $\mathfrak{R} \subseteq \mathbb{N} \times \mathbb{N}$ is finite and weakly functional (deterministic),
  - $\mathfrak{V} : \mathrm{PROP} \to \mathcal{P}(\mathbb{N})$.

- Disjoint unions $\mathfrak{M}_1 \uplus \mathfrak{M}_2$.

- The models have an infinite domain and a finite relation encoding the heap.

Semantics

$$\mathfrak{M}, \mathfrak{l} \models p \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{l} \in \mathfrak{V}(p)$$

$$\mathfrak{M}, \mathfrak{l} \models \Diamond\phi \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{M}, \mathfrak{l}' \models \phi, \text{ for some } \mathfrak{l}' \in \mathbb{N} \text{ such that } (\mathfrak{l}, \mathfrak{l}') \in \mathfrak{R}$$

$$\mathfrak{M}, \mathfrak{l} \models \langle\neq\rangle\phi \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{M}, \mathfrak{l}' \models \phi, \text{ for some } \mathfrak{l}' \in \mathbb{N} \text{ such that } \mathfrak{l}' \neq \mathfrak{l}$$

Semantics

$$\mathfrak{M}, \mathfrak{l} \models p \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{l} \in \mathfrak{V}(p)$$

$$\mathfrak{M}, \mathfrak{l} \models \Diamond\phi \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{M}, \mathfrak{l}' \models \phi, \text{ for some } \mathfrak{l}' \in \mathbb{N} \text{ such that } (\mathfrak{l}, \mathfrak{l}') \in \mathfrak{R}$$

$$\mathfrak{M}, \mathfrak{l} \models \langle\neq\rangle\phi \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{M}, \mathfrak{l}' \models \phi, \text{ for some } \mathfrak{l}' \in \mathbb{N} \text{ such that } \mathfrak{l}' \neq \mathfrak{l}$$

$$\mathfrak{M}, \mathfrak{l} \models \mathtt{emp} \quad \overset{\text{def}}{\Leftrightarrow} \quad \mathfrak{R} = \emptyset$$

$$\mathfrak{M}, \mathfrak{l} \models \phi_1 * \phi_2 \quad \overset{\text{def}}{\Leftrightarrow} \quad \langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, \mathfrak{l} \models \phi_1 \text{ and } \langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, \mathfrak{l} \models \phi_2, \text{ for some partition } \{\mathfrak{R}_1, \mathfrak{R}_2\} \text{ of } \mathfrak{R}$$

Examples

$$\langle \mathrm{U} \rangle \phi \stackrel{\text{def}}{=} \phi \vee \langle \neq \rangle \phi \qquad \texttt{size} \geq k \stackrel{\text{def}}{=} \underbrace{\neg\texttt{emp} * \cdots * \neg\texttt{emp}}_{k \text{ times}}$$

Examples

$$\langle \mathrm{U} \rangle \phi \stackrel{\text{def}}{=} \phi \vee \langle \neq \rangle \phi \qquad \mathtt{size} \geq k \stackrel{\text{def}}{=} \underbrace{\neg \mathtt{emp} * \cdots * \neg \mathtt{emp}}_{k \text{ times}}$$

- Nominal in hybrid modal logic: propositional variable true at a unique state/world/location of the model.

$$\langle \mathrm{U} \rangle (x \wedge [\neq] \neg x)$$

Examples

$$\langle \mathrm{U} \rangle \phi \stackrel{\text{def}}{=} \phi \vee \langle \neq \rangle \phi \qquad \mathtt{size} \geq k \stackrel{\text{def}}{=} \underbrace{\neg \mathtt{emp} * \cdots * \neg \mathtt{emp}}_{k \text{ times}}$$

- Nominal in hybrid modal logic: propositional variable true at a unique state/world/location of the model.

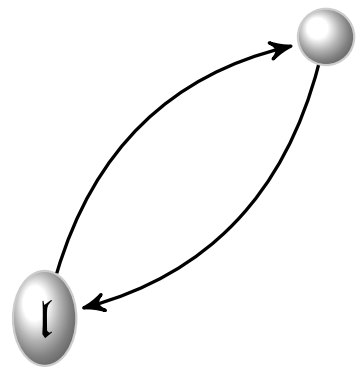
$$\langle \mathrm{U} \rangle (x \wedge [\neq] \neg x)$$

- The model is a loop of length 2 visiting the current location:

$$\mathtt{size} \geq 2 \wedge \neg \mathtt{size} \geq 3 \wedge \Diamond\Diamond\Diamond\top \wedge$$

$$\neg(\neg \mathtt{emp} * \Diamond\Diamond\Diamond\top) \wedge \neg\Diamond(\neg \mathtt{emp} * \Diamond\Diamond\Diamond\top)$$

(in $\mathrm{MSL}(*, \Diamond)$, but not expressible in Alt$_1$/prop. $\mathrm{SL}(*, -\!\!*)$)



Relationships with prop. separation logic $\mathrm{SL}(*)$

- Formulae:

$$\phi ::= \mathtt{x} = \mathtt{y} \mid \mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{emp} \mid \neg\phi \mid \phi \wedge \phi \mid \phi * \phi$$

Relationships with prop. separation logic $\mathrm{SL}(*)$

- Formulae:

$$\phi ::= \mathtt{x} = \mathtt{y} \mid \mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{emp} \mid \neg\phi \mid \phi \wedge \phi \mid \phi * \phi$$

- Satisfaction relation:

$$\begin{array}{lcl}
(\mathfrak{s},\mathfrak{h}) \models \mathtt{x} = \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & \mathfrak{s}(\mathtt{x}) = \mathfrak{s}(\mathtt{y}) \\
(\mathfrak{s},\mathfrak{h}) \models \mathtt{emp} & \overset{\text{def}}{\Leftrightarrow} & \mathrm{dom}(\mathfrak{h}) = \emptyset \\
(\mathfrak{s},\mathfrak{h}) \models \mathtt{x} \hookrightarrow \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & \mathfrak{s}(\mathtt{x}) \in \mathrm{dom}(\mathfrak{h}) \text{ and } \mathfrak{h}(\mathfrak{s}(\mathtt{x})) = \mathfrak{s}(\mathtt{y}) \\
(\mathfrak{s},\mathfrak{h}) \models \phi_1 * \phi_2 & \overset{\text{def}}{\Leftrightarrow} & \text{there are } \mathfrak{h}_1 \text{ and } \mathfrak{h}_2 \text{ s.t. } \mathfrak{h}_1 \uplus \mathfrak{h}_2 = \mathfrak{h}, \\
 & & (\mathfrak{s},\mathfrak{h}_1) \models \phi_1 \text{ and } (\mathfrak{s},\mathfrak{h}_2) \models \phi_2
\end{array}$$

Relationships with prop. separation logic $\mathrm{SL}(*)$

- Formulae:

$$\phi ::= \mathtt{x} = \mathtt{y} \mid \mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{emp} \mid \neg\phi \mid \phi \wedge \phi \mid \phi * \phi$$

- Satisfaction relation:

$$\begin{array}{lcl}
(\mathfrak{s},\mathfrak{h}) \models \mathtt{x} = \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & \mathfrak{s}(\mathtt{x}) = \mathfrak{s}(\mathtt{y}) \\
(\mathfrak{s},\mathfrak{h}) \models \mathtt{emp} & \overset{\text{def}}{\Leftrightarrow} & \mathrm{dom}(\mathfrak{h}) = \emptyset \\
(\mathfrak{s},\mathfrak{h}) \models \mathtt{x} \hookrightarrow \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & \mathfrak{s}(\mathtt{x}) \in \mathrm{dom}(\mathfrak{h}) \text{ and } \mathfrak{h}(\mathfrak{s}(\mathtt{x})) = \mathfrak{s}(\mathtt{y}) \\
(\mathfrak{s},\mathfrak{h}) \models \phi_1 * \phi_2 & \overset{\text{def}}{\Leftrightarrow} & \text{there are } \mathfrak{h}_1 \text{ and } \mathfrak{h}_2 \text{ s.t. } \mathfrak{h}_1 \uplus \mathfrak{h}_2 = \mathfrak{h}, \\
 & & (\mathfrak{s},\mathfrak{h}_1) \models \phi_1 \text{ and } (\mathfrak{s},\mathfrak{h}_2) \models \phi_2
\end{array}$$

- Encoding $\mathrm{SL}(*)$ into $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$:

$$\mathtt{x} = \mathtt{y} \approx \langle \mathrm{U} \rangle (\mathtt{x} \wedge \mathtt{y}) \qquad \mathtt{x} \hookrightarrow \mathtt{y} \approx \langle \mathrm{U} \rangle (\mathtt{x} \wedge \Diamond \mathtt{y})$$

(assuming that $\mathtt{x}$ and $\mathtt{y}$ are nominals in $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$)

TOWER upper bound for $\mathrm{SAT}(\mathrm{MSL}(*, \Diamond, \langle\neq\rangle))$

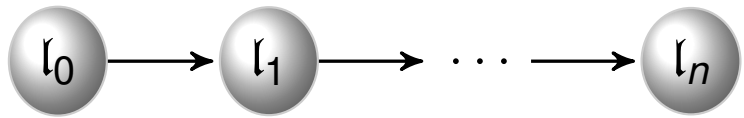
- $\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle)$: variant with finite models.
- Reduction $\mathrm{SAT}(\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)) \to \mathrm{SAT}(\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle))$.

TOWER upper bound for $\mathrm{SAT}(\mathrm{MSL}(*, \Diamond, \langle\neq\rangle))$

- $\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle)$: variant with finite models.
- Reduction $\mathrm{SAT}(\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)) \to \mathrm{SAT}(\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle))$.
- $\mathrm{SAT}(\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle))$ is in TOWER.
  - TOWER: class of problems of time complexity bounded by a tower of exponentials, whose height is an elementary function of the input. [Schmitz, TOCT 2016]
  - Reduction from satisfiability for $\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle)$ into satisfiability for the weak MSO theory of $(\mathfrak{D}, \mathfrak{f}, =)$.
  - Internalisation of the semantics for $\mathrm{MSL}^f(*, \Diamond, \langle\neq\rangle)$.

TOWER-hardness

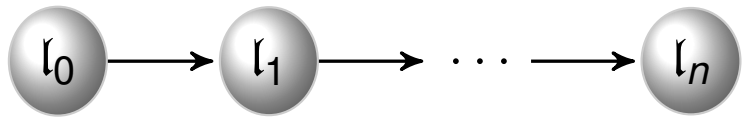
- Linear model:



- There is a formula $\phi_{\exists\mathtt{ls}}$ in $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$ such that $\mathfrak{M} \models \phi_{\exists\mathtt{ls}}$ iff $\mathfrak{M}$ is linear.

TOWER-hardness

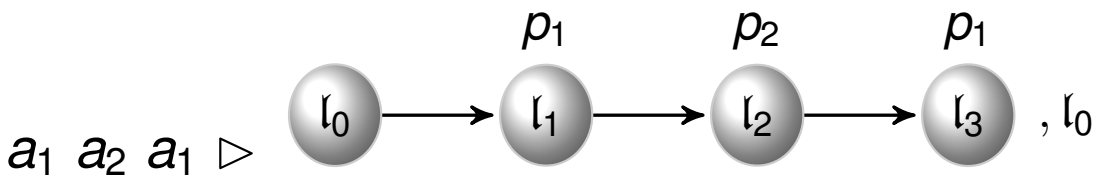
- Linear model:



- There is a formula $\phi_{\exists\mathtt{1s}}$ in $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$ such that $\mathfrak{M} \models \phi_{\exists\mathtt{1s}}$ iff $\mathfrak{M}$ is linear.
- Star-free expressions

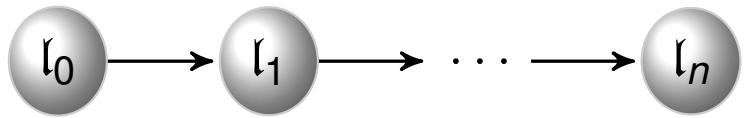
$$e ::= a \mid \varepsilon \mid e \cup e \mid ee \mid \sim e$$

  - Nonemptiness problem is TOWER-complete.
    [Meyer & Stockmeyer, STOC'73; Schmitz, ToCT 2016]
  - Encoding words by linear models.



TOWER-hardness

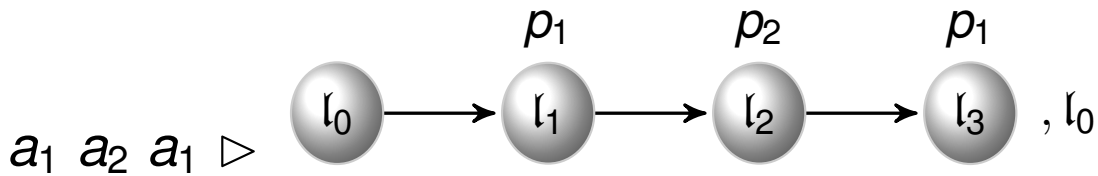
- Linear model:



- There is a formula $\phi_{\exists \mathtt{1s}}$ in $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$ such that $\mathfrak{M} \models \phi_{\exists \mathtt{1s}}$ iff $\mathfrak{M}$ is linear.
- Star-free expressions

$$e ::= a \mid \varepsilon \mid e \cup e \mid ee \mid \sim e$$

  - Nonemptiness problem is TOWER-complete.
    [Meyer & Stockmeyer, STOC'73; Schmitz, ToCT 2016]
  - Encoding words by linear models.



- $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$ satisfiability problem is TOWER-hard.
  [Demri & Fervari, AiML'18]

Variants

- Other results.
  1. The satisfiability problems for $\mathrm{MSL}(*, \Diamond)$ and $\mathrm{MSL}(*, \langle\neq\rangle)$ are NP-complete. (for $\mathrm{SL}(*)$, PSPACE-completeness)
  2. Undecidability of $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$ + magic wand $-\!\!*$.

[Demri & Fervari, AiML'18]

Variants

- Other results.
  1. The satisfiability problems for $\mathrm{MSL}(*, \Diamond)$ and $\mathrm{MSL}(*, \langle \neq \rangle)$ are NP-complete. (for $\mathrm{SL}(*)$, PSPACE-completeness)
  2. Undecidability of $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$ + magic wand $\mathrel{-\!\!*}$.

     [Demri & Fervari, AiML'18]
  3. Modal logic for heaps MLH($*$) is TOWER-complete.

     [Demri & Deters, TOCL 2015]

Variants

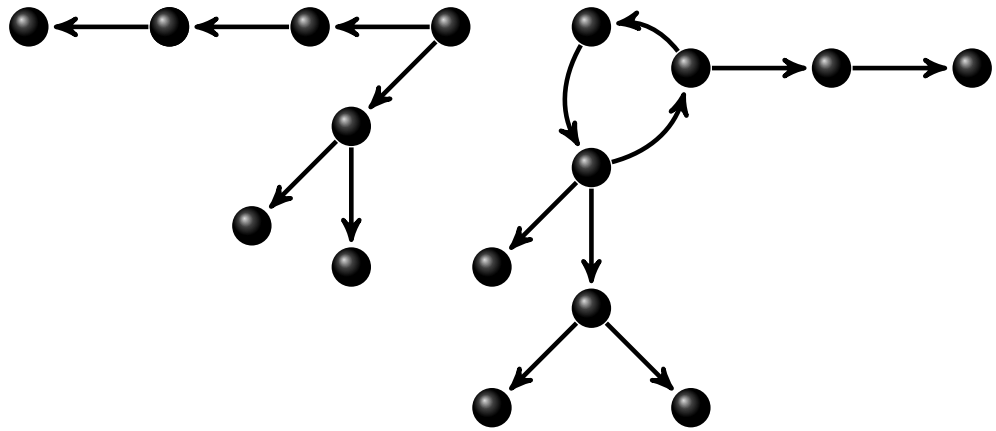
- Other results.
  1. The satisfiability problems for $\mathrm{MSL}(*, \Diamond)$ and $\mathrm{MSL}(*, \langle\neq\rangle)$ are NP-complete. (for $\mathrm{SL}(*)$, PSPACE-completeness)
  2. Undecidability of $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$ + magic wand $-\!\!*$.

     [Demri & Fervari, AiML'18]
  3. Modal logic for heaps MLH($*$) is TOWER-complete.

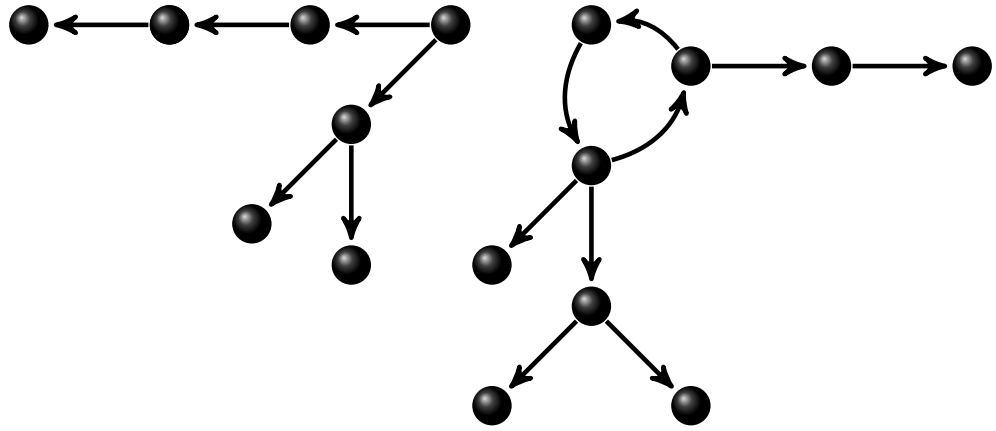
     [Demri & Deters, TOCL 2015]

- Adding the converse modality.
  - $\mathfrak{M}, \mathfrak{l} \models \Diamond^{-1}\phi \overset{\text{def}}{\Leftrightarrow} \mathfrak{M}, \mathfrak{l}' \models \phi$, for some $\mathfrak{l}' \in \mathbb{N}$ s.t. $(\mathfrak{l}', \mathfrak{l}) \in \mathfrak{R}$.
  - Satisfiability problem for $\mathrm{MSL}(*, \Diamond, \Diamond^{-1}, \langle\neq\rangle)$ in TOWER.
  - Satisfiability problem for $\mathrm{MSL}(*, \Diamond^{-1})$ is PSPACE-hard.

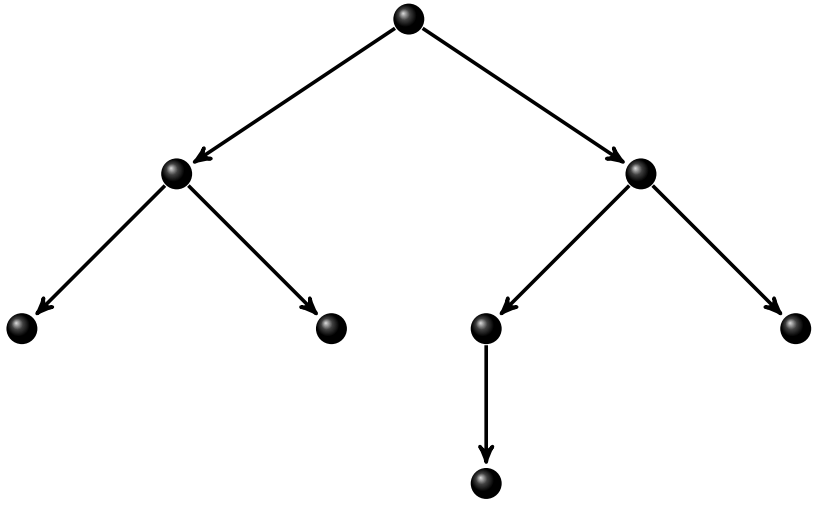
Structures for interpreting $\mathrm{MSL}(*, \Diamond^{-1})$ in $\mathrm{MSL}(*, \Diamond)$



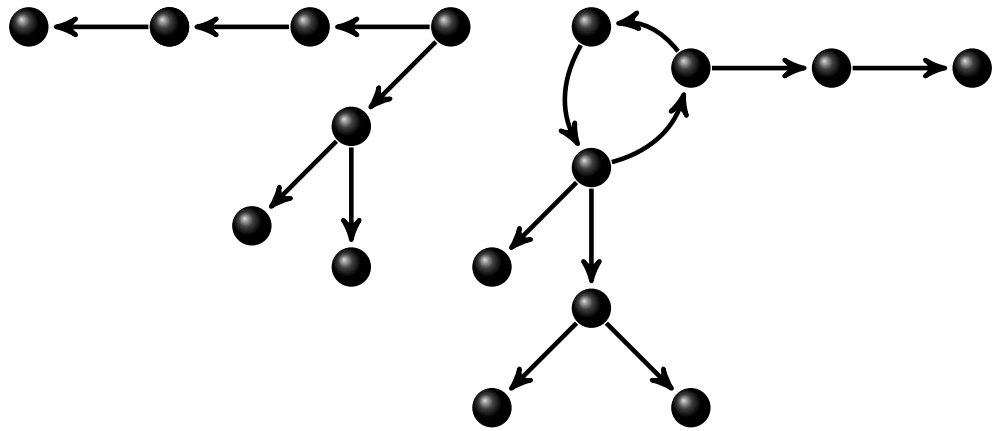
Structures for interpreting $\mathrm{MSL}(*, \diamond^{-1})$ in $\mathrm{MSL}(*, \diamond)$



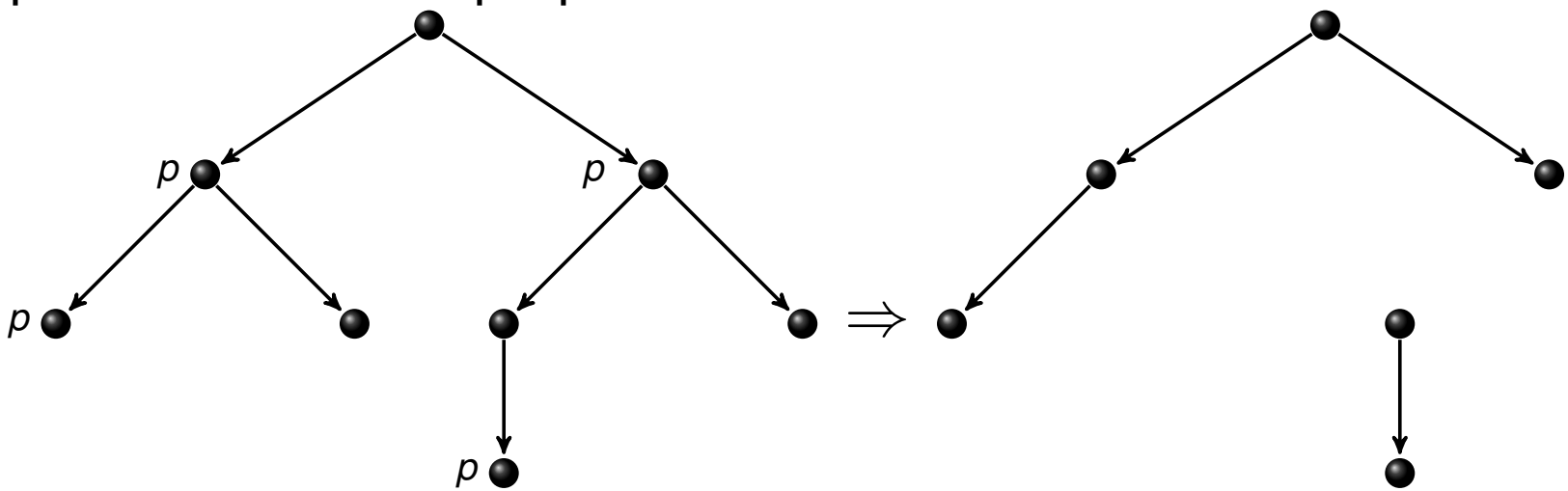
- Separating conjunction is strongly related to second-order quantification over propositions.



Structures for interpreting $\mathrm{MSL}(*, \Diamond^{-1})$ in $\mathrm{MSL}(*, \Diamond)$



- Separating conjunction is strongly related to second-order quantification over propositions.



QCTL^t: QCTL **under the tree semantics**

[Laroussinie & Markey, LMCS 2014]

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \mathbf{EX}\phi \mid \mathbf{E}(\phi \mathbf{U} \phi) \mid \mathbf{A}(\phi \mathbf{U} \phi) \mid \exists p\ \phi$$

- Models are total Kripke structures $\mathcal{K} = (W, R, l)$.
- $\mathcal{K}, w \models \exists p\ \phi$ iff there is $\mathcal{K}'$ s.t. $\mathcal{K} \approx_{\mathrm{AP}\setminus\{p\}} \mathcal{K}'$ & $\mathcal{K}', w \models \phi$.

QCTL^t: QCTL **under the tree semantics**

[Laroussinie & Markey, LMCS 2014]

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \mathbf{EX}\phi \mid \mathbf{E}(\phi \mathbf{U} \phi) \mid \mathbf{A}(\phi \mathbf{U} \phi) \mid \exists p\ \phi$$

- Models are total Kripke structures $\mathcal{K} = (W, R, l)$.
- $\mathcal{K}, w \models \exists p\ \phi$ iff there is $\mathcal{K}'$ s.t. $\mathcal{K} \approx_{\mathrm{AP}\setminus\{p\}} \mathcal{K}'$ & $\mathcal{K}', w \models \phi$.
- Satisfiability problem for QCTL^s (structure semantics):

  input: a quantified CTL formula ϕ.
  output: 1 iff there is a finite total Kripke structure satisfying ϕ.

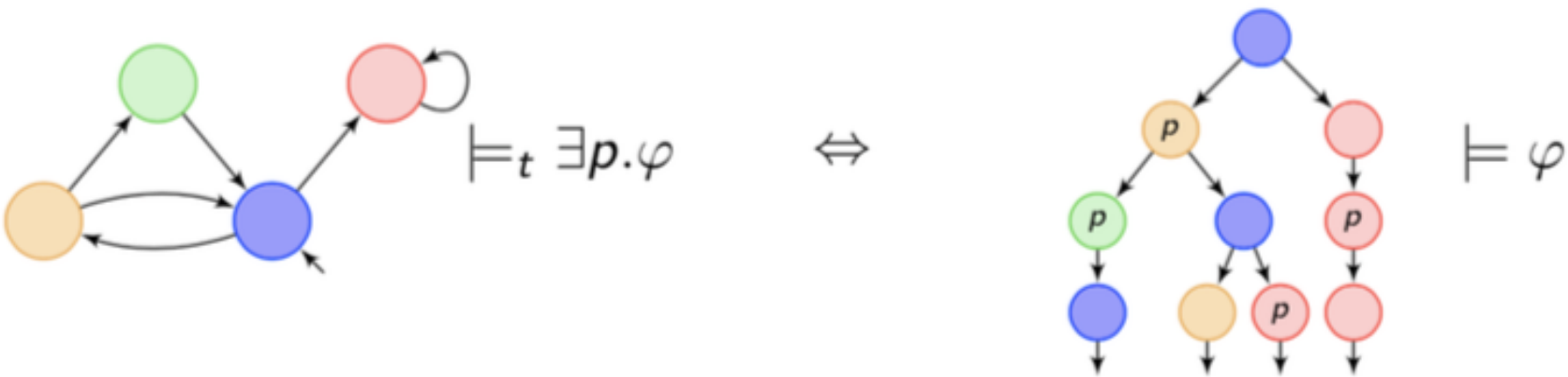
Tree semantics

- Satisfiability problem for QCTL^t (tree semantics):

  input: a quantified CTL formula ϕ.

  output: 1 iff there is a finite total Kripke structure whose tree unfolding satisfies ϕ.

  ($\approx$ finite-branching trees with infinite branches)



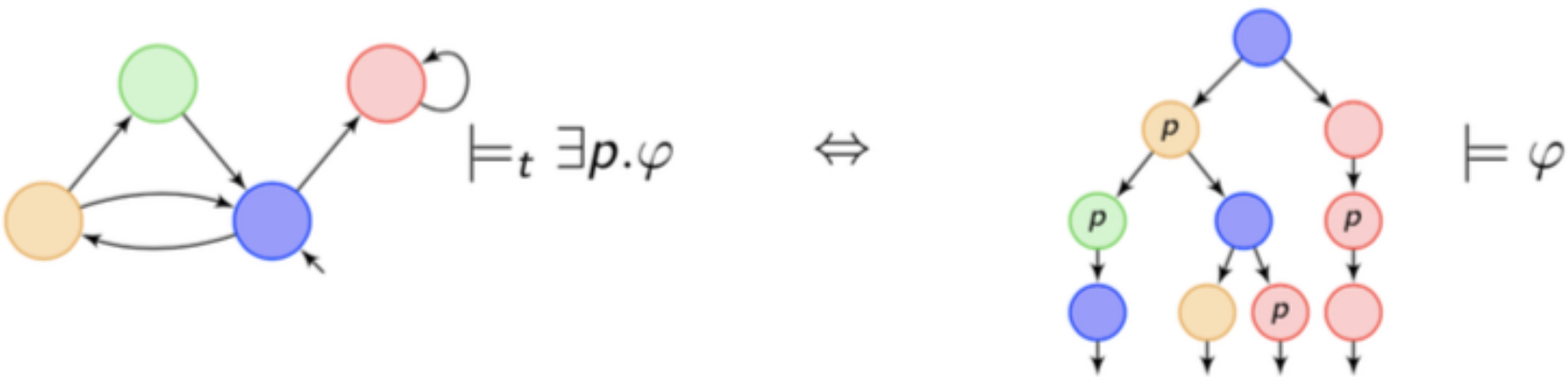
Tree semantics

- Satisfiability problem for QCTL^t (tree semantics):

  input: a quantified CTL formula ϕ.

  output: 1 iff there is a finite total Kripke structure whose tree unfolding satisfies ϕ.

  ($\approx$ finite-branching trees with infinite branches)



- SAT(QCTL^t) is TOWER-complete.
  SAT(QCTL^s) is undecidable.

[Laroussinie & Markey, LMCS 2014]

Other results and fragments

- Modal logics K and S4 augmented with propositional quantification are undecidable. [Fine, Theoria 72]

Other results and fragments

- Modal logics K and S4 augmented with propositional quantification are undecidable. [Fine, Theoria 72]

- $\mathrm{QCTL}^{t}_{\mathbf{X}}$: QCTL^{t} restriction to **EX**.
  $\mathrm{QCTL}^{t}_{\mathbf{XF}}$: QCTL^{t} restriction to **EXEF**.
  $\mathrm{QCTL}^{ft}_{\mathbf{X}}$, $\mathrm{QCTL}^{ft}_{\mathbf{XF}}$: finite tree semantics.

Other results and fragments

- Modal logics K and S4 augmented with propositional quantification are undecidable. [Fine, Theoria 72]

- $\mathrm{QCTL}^{t}_{\mathbf{X}}$: QCTL^{t} restriction to **EX**.
  $\mathrm{QCTL}^{t}_{\mathbf{XF}}$: QCTL^{t} restriction to **EXEF**.
  $\mathrm{QCTL}^{ft}_{\mathbf{X}}$, $\mathrm{QCTL}^{ft}_{\mathbf{XF}}$: finite tree semantics.

- What about $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{X}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{X}})$?

- What about $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{XF}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{XF}})$?

Bounding the branching degree

- $\mathrm{QCTL}^{t}_{\mathbf{X},\leq N}$: variant of $\mathrm{QCTL}^{t}_{\mathbf{X}}$ with N-bounded tree models.

Bounding the branching degree

- $\mathrm{QCTL}^{t}_{\mathbf{X},\leq N}$: variant of $\mathrm{QCTL}^{t}_{\mathbf{X}}$ with N-bounded tree models.

- $\mathrm{AEXP}_{\mathrm{POL}}$: class of problems decidable with an exponential-time ATM with a polynomial number of alternations.

$$\mathrm{NEXPTIME} \subseteq \mathrm{AEXP}_{\mathrm{POL}} \subseteq \mathrm{EXPSPACE}$$

- $\mathrm{AEXP}_{\mathrm{POL}}$-complete alternating multi-tiling problem to show that the model-checking problem for $B\bar{E}$ with regular expressions is $\mathrm{AEXP}_{\mathrm{POL}}$-hard.

[Bozzelli et al., GANDALF'17; Molinari, PhD 2019]

Bounding the branching degree

- $\mathrm{QCTL}^{t}_{\mathbf{X},\leq N}$: variant of $\mathrm{QCTL}^{t}_{\mathbf{X}}$ with N-bounded tree models.

- $\mathrm{AExp}_{\mathrm{POL}}$: class of problems decidable with an exponential-time ATM with a polynomial number of alternations.

$$\mathrm{NEXPTIME} \subseteq \mathrm{AExp}_{\mathrm{POL}} \subseteq \mathrm{EXPSPACE}$$

- $\mathrm{AExp}_{\mathrm{POL}}$-complete alternating multi-tiling problem to show that the model-checking problem for $B\bar{E}$ with regular expressions is $\mathrm{AExp}_{\mathrm{POL}}$-hard.

[Bozzelli et al., GANDALF'17; Molinari, PhD 2019]

- For all $N \geq 2$, $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{X},\leq N})$ is $\mathrm{AExp}_{\mathrm{POL}}$-complete.

- $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{X},\leq 1})$ is PSPACE-complete (easy).

How to prove TOWER-hardness

- Uniform elementary reduction from k-NEXPTIME-complete tiling problems $\texttt{Tiling}_k$.
- $\mathfrak{t}(0,n)=n$ and $\mathfrak{t}(k+1,n)=2^{\mathfrak{t}(k,n)}$.
- $\texttt{Tiling}_k$:

  input:
  - $(\mathcal{T},\mathcal{H},\mathcal{V})$ (tile types, horizontal and vertical matching relations),
  - $c=t_0,t_1,\ldots,t_{n-1}\in\mathcal{T}^n$: initial condition.

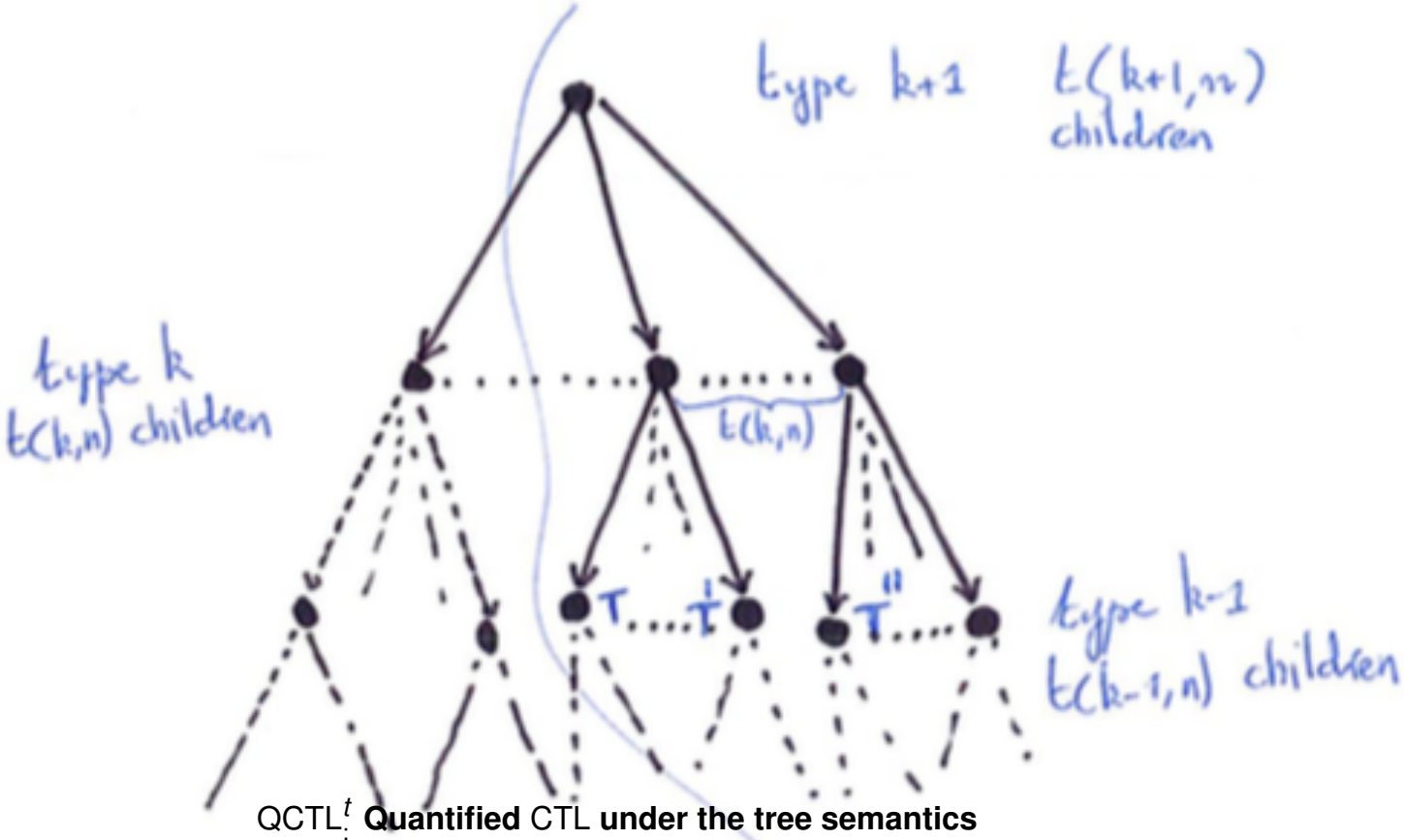
  output: 1 iff the grid $[0,\mathfrak{t}(k,n)-1]\times[0,\mathfrak{t}(k,n)-1]$ can be tiled (with usual constraints)?

High-level description of the reduction from $\mathtt{Tiling}_k$

- Grid $[0, \mathfrak{t}(k,n) - 1] \times [0, \mathfrak{t}(k,n) - 1]$ as a tree model:
  - The root ε has $\mathfrak{t}(k+1, n)$ children.
  - $\mathfrak{t}(k,n)$ children of ε are distinguished and receive a number in $[0, \mathfrak{t}(k,n) - 1]$.

High-level description of the reduction from $\texttt{Tiling}_k$

- Grid $[0, \mathfrak{t}(k,n)-1] \times [0, \mathfrak{t}(k,n)-1]$ as a tree model:
  - The root ε has $\mathfrak{t}(k+1,n)$ children.
  - $\mathfrak{t}(k,n)$ children of ε are distinguished and receive a number in $[0, \mathfrak{t}(k,n)-1]$.
  - Each child of ε has exactly $\mathfrak{t}(k,n)$ children and each child has a number in $[0, \mathfrak{t}(k,n)-1]$.



Ingredient I: local nominals

- A toolkit for introducing local nominals x.
  - $\texttt{nom}(x, k)$: there is exactly one descendant at depth k satisfying x.
  - $@^k_x\phi$: this unique descendant satisfies ϕ.
  - $\texttt{diff-nom}(x_1, \ldots, x_\alpha, k)$: α distinct descendants at depth k.

- Simulation of first-order quantification on a given set of nodes of bounded depth.

Ingredient I: local nominals

- A toolkit for introducing local nominals x.
  - $\texttt{nom}(x, k)$: there is exactly one descendant at depth k satisfying x.
  - $@^k_x \phi$: this unique descendant satisfies ϕ.
  - $\texttt{diff-nom}(x_1, \ldots, x_\alpha, k)$: α distinct descendants at depth k.

- Simulation of first-order quantification on a given set of nodes of bounded depth.

- At most 2^n children ($\Diamond_{\leq 2^n} \top$ in graded modal logics):

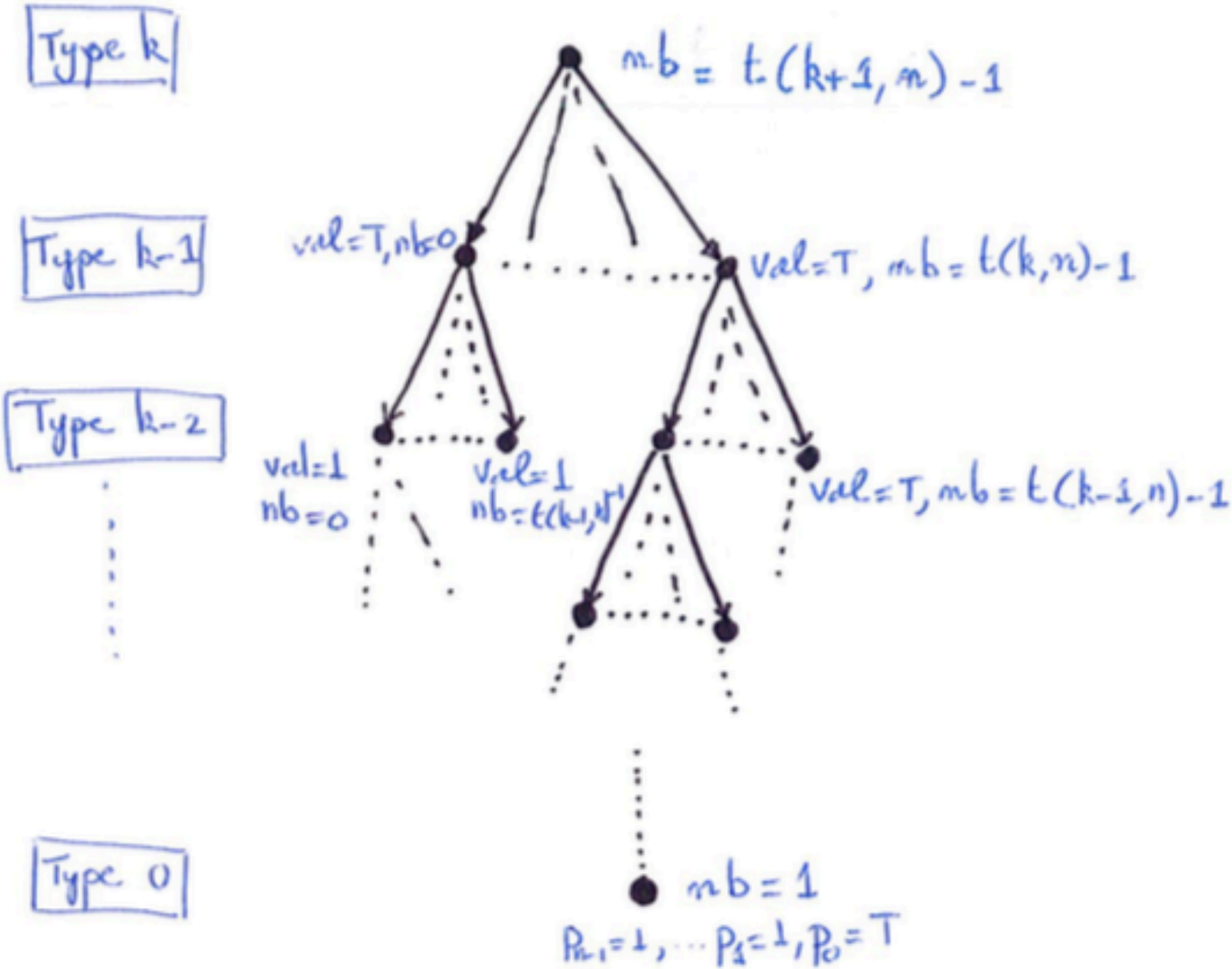
$$\exists\, p_0, \ldots, p_{n-1}\ \forall x, y\ \texttt{diff-nom}(x, y, 1) \rightarrow$$

$$\neg\Big(\bigwedge_{i \in [0, n-1]} @^1_x p_i \leftrightarrow @^1_y p_i\Big).$$

[David & Laroussinie & Markey, CONCUR'16]

Ingredient II: enforcing $\mathfrak{t}(k, n)$ children

- The most difficult and substantial part of the proof.
- Any node is of type 0.
- Node v of type $k > 0$:
  - every child is of type $k - 1$.
  - v has $\mathfrak{t}(k, n)$ children numbered from 0 to $\mathfrak{t}(k, n) - 1$.
- A number for a node of type 0 is encoded by $p_{n-1}, \ldots, p_0$.
- A number for a node of type $k > 0$
  - is encoded by the truth value *val* on its children,
  - it belongs to $[0, \mathfrak{t}(k + 1, n) - 1]$.


Type k
Type k-1
Type k-2
Type 0
nb = t(k+1, n) - 1
val=T, nb=0
val=T, nb = t(k,n)-1
val=1
nb=0
val=1
val=T, nb = t(k-1,n)-1
nb = 1
P_{n-1}=1, ... P_1=1, P_0=T

Specifications for a node of type $k > 0$

- Every child is of type $k - 1$.
- There is a child with number equal to zero.
- Distinct children have distinct numbers in $[0, \mathfrak{t}(k, n) - 1]$.
- If a child has number $m < \mathfrak{t}(k, n) - 1$, then there is a sibling with number equal to $m + 1$.

$$\mathrm{type}(k) \stackrel{\text{def}}{=} \mathbf{AX}(\mathrm{type}(k-1)) \wedge \mathbf{EX}(\mathrm{first}(k-1)) \wedge \mathrm{uniq}(k) \wedge \mathrm{compl}(k).$$

- $\mathrm{SAT}(\mathrm{QCTL}^t_{\mathbf{X}})$ is TOWER-complete. [Demri & Bednarczyk, Sub.]
  (many developments are omitted here)

Harvest of TOWER-complete modal logics

- $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{F}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{XF}})$ are TOWER-complete.
- $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{F}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{XF}})$ are TOWER-complete too!

Harvest of TOWER-complete modal logics

- $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{F}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{t}_{\mathbf{XF}})$ are TOWER-complete.
- $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{F}})$ and $\mathrm{SAT}(\mathrm{QCTL}^{ft}_{\mathbf{XF}})$ are TOWER-complete too!
- Characterisation for standard modal logics:
  - K: finite trees. ($\Diamond \approx \mathbf{EX}$)
  - GL (after Gödel & Löb): finite transitive trees. ($\Diamond \approx \mathbf{EXEF}$)
  - S4: reflexive and transitive trees. ($\Diamond \approx \mathbf{EF}$)
  - etc.
- Over the appropriate classes of trees, these modal logics with propositional quantification are TOWER-complete.
- E.g., for GL, it corresponds exactly to $\mathrm{QCTL}^{ft}_{\mathbf{XF}}$.

Concluding remarks

- Separation logics share many features with modal/temporal logics.
- On the spotlight, quantified temporal logics and interval temporal logics (untouched in this talk).
- See also relationships with ambient logic on trees.

[Calcagno et al., TLDI'03; Calcagno et al., POPL'05]

Concluding remarks

- Separation logics share many features with modal/temporal logics.
- On the spotlight, quantified temporal logics and interval temporal logics (untouched in this talk).
- See also relationships with ambient logic on trees.

  [Calcagno et al., TLDI'03; Calcagno et al., POPL'05]
- Some on-going works:
  - Complexity characterisation for $\mathrm{MSL}(*, \Diamond^{-1})$, $\mathrm{MSL}(*, \Diamond^{-1}, \Diamond)$ or $\mathrm{MSL}(*, \Diamond^{-1}, \langle \neq \rangle)$.
  - Proof systems for such logics.
    See the recent paper [Demri & Fervari & Mansutti, JELIA'19].