Modal Separation Logics: Complexity and Axiomatisation

Stéphane Demri

CNRS, France

Joint works with Raul Fervari & Alessio Mansutti

Formal Methods and AI, Rennes

May 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]
  - one-agent refinement modal logic [Bozzelli & van Ditmarsch & Pinchinat, TCS 2015]
  - 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 Hilbert-style axiomatisation.

Frame rule and separating conjunction

- Separation logic:
  - Extension of Floyd-Hoare logic for (concurrent) programs with mutable data structures.
  - Introduced by Ishtiaq, O'Hearn, Pym, Reynolds, Yang.
    See also [Burstall, MI 72]
  - Extension of Hoare logic with separating connectives $*$ and $-\!\!*$.
    [O'Hearn, Reynolds & Yang, CSL'01; Reynolds, LICS'02]

- Frame rule:

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

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

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

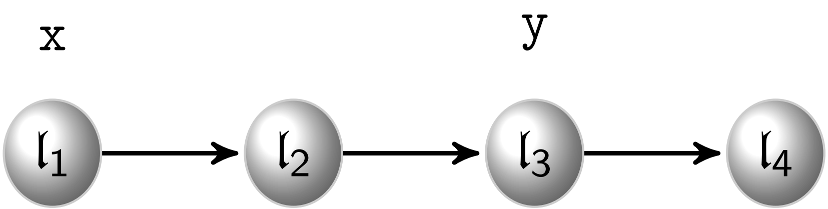
- $(\mathfrak{s}, \mathfrak{h}) \models \mathtt{x} \hookrightarrow 5 * \mathtt{y} \hookrightarrow 3$ implies $(\mathfrak{s}, \mathfrak{h}) \models \mathtt{x} \neq \mathtt{y}$.

Memory states with one record field

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

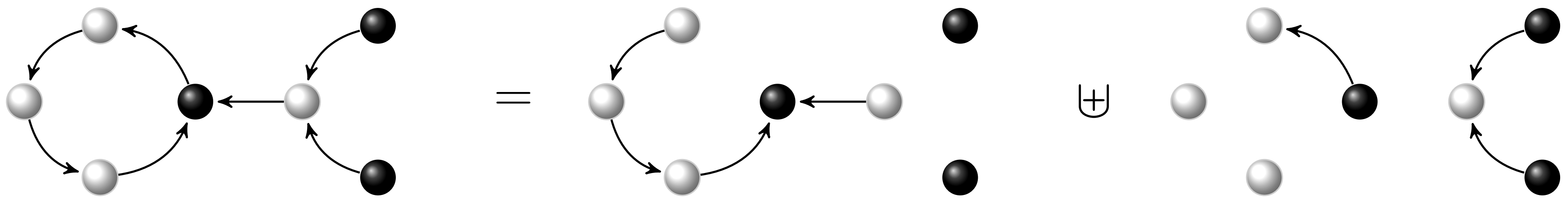
- $\mathtt{Loc}$: countably infinite set of locations
  $\mathtt{Val}$: countably infinite set of values with $\mathtt{Loc} \subseteq \mathtt{Val}$.

- Memory state $(\mathfrak{s}, \mathfrak{h})$:
  - Store $\mathfrak{s}$: PVAR $\rightarrow \mathtt{Val}$.
  - Heap $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{\mathit{fin}} \mathtt{Val}$ (finite domain).
    (richer models exist, e.g. with $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{\mathit{fin}} \mathtt{Val}^k$, $k > 1$)
  - In this talk, we assume $\mathtt{Loc} = \mathtt{Val} = \mathbb{N}$.



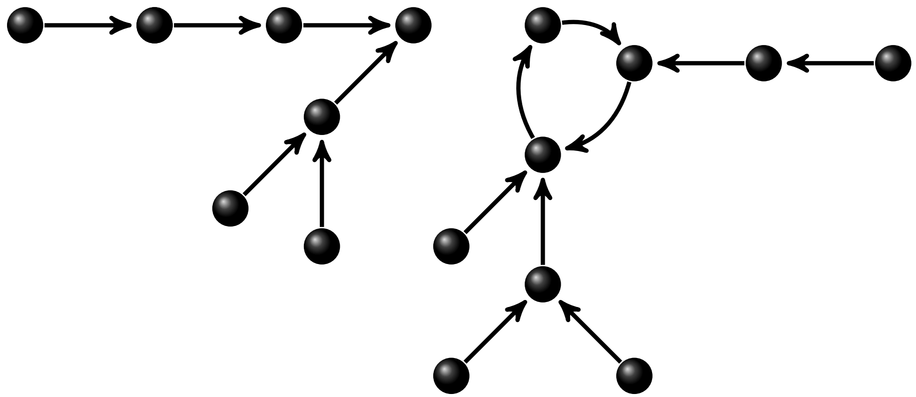
Disjoint heaps

- The heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are disjoint iff $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$.
- When $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are disjoint, $\mathfrak{h}_1 \uplus \mathfrak{h}_2$ is their disjoint union.

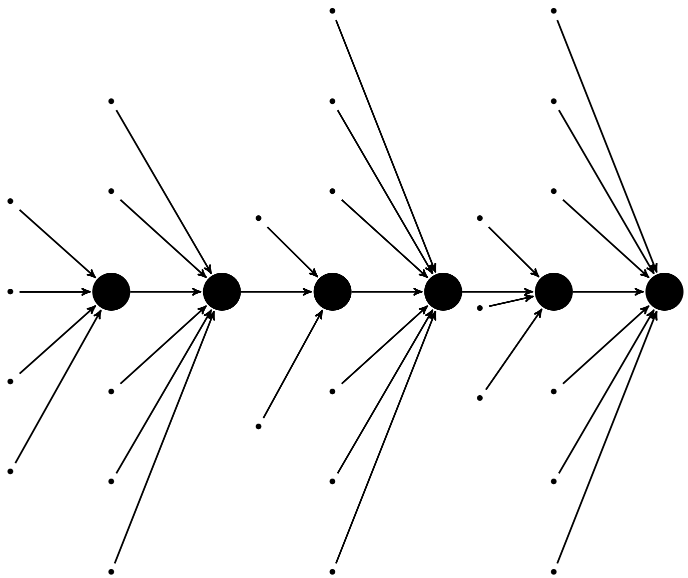


The models are forest-like structures

- A forest of tree-like structures:



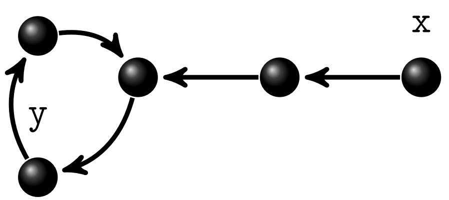
- A word-like structure:



Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, as an alternative to first-order separation logic 1SL.

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



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

- 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:

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

- 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 universe and a finite relation encoding the heap.

Semantics

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

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

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

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

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

Examples

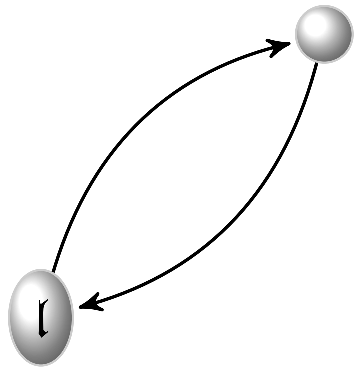
$$\langle \mathrm{U} \rangle \phi \stackrel{\text{def}}{=} \phi \vee \langle \neq \rangle \phi \quad \mathtt{size} \geq k \stackrel{\text{def}}{=} \underbrace{\neg\mathtt{emp} * \cdots * \neg\mathtt{emp}}_{k \text{ times}}$$

- Nominal x as in hybrid (modal) logics.

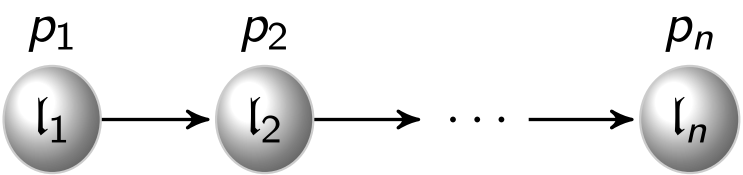
$$\langle \mathrm{U} \rangle (x \wedge [\neq] \neg x)$$

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

$$\mathtt{size} \geq 2 \wedge \neg \mathtt{size} \geq 3 \wedge \Diamond\Diamond\Diamond\top \wedge$$
$$\neg(\neg\mathtt{emp} * \Diamond\Diamond\Diamond\top) \wedge \neg\Diamond(\neg\mathtt{emp} * \Diamond\Diamond\Diamond\top)$$



- $p_1 \wedge \Diamond(p_2 \wedge \Diamond(p_3 \wedge \cdots \Diamond(p_n \wedge \Box \perp) \cdots))$:



Tower-completeness of $\mathrm{SAT}(\mathrm{MSL}(*, \Diamond, \langle \neq \rangle))$

- Linear model:

$$\mathfrak{l}_0 \longrightarrow \mathfrak{l}_1 \longrightarrow \cdots \longrightarrow \mathfrak{l}_n$$

- 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.

- Star-free expressions

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

  - Nonemptiness problem is $\textsc{Tower}$-complete.
    [Meyer & Stockmeyer, STOC'73; Schmitz, ToCT 2016]

  - Encoding words by linear models.

$$a_1\ a_2\ a_1 \ \triangleright\ \mathfrak{l}_0 \longrightarrow \overset{p_1}{\mathfrak{l}_1} \longrightarrow \overset{p_2}{\mathfrak{l}_2} \longrightarrow \overset{p_1}{\mathfrak{l}_3}\ , \mathfrak{l}_0$$

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

Variants

- The satisfiability problems for $\mathrm{MSL}(*, \Diamond)$ and $\mathrm{MSL}(*, \langle \neq \rangle)$ are $\textsc{np}$-complete. (for $\mathrm{SL}(*)$, $\textsc{pspace}$-completeness)

- Undecidability of $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$ $+$ magic wand $-\!\!*$.

  [Demri & Fervari, AiML'18]

- Modal logic for heaps MLH($*$) is $\textsc{Tower}$-complete.

  [Demri & Deters, TOCL 2015]

Hilbert-style axiomatisation of $\mathrm{MSL}(*, \Diamond)$

- Designing internal calculi for separation-like logics is not an easy task.

- Proof systems for abstract separation logics with labels or nominals:
  - Hybrid separation logics. [Brotherston & Villard, POPL'14]
  - Sequent-style calculi. [Hou et al., TOCL 2018]
  - Tableaux-based calculi. [Docherty & Pym, FOSSACS'18]

  See also [Galmiche & Mery, JLC 2010]

- Puristic approach: only formulae in $\mathrm{MSL}(*, \Diamond)$ are used.

- Design a subclass of formulae in $\mathrm{MSL}(*, \Diamond)$ that captures the expressive power of $\mathrm{MSL}(*, \Diamond)$.

- Calculus also for $\mathrm{MSL}(*, \langle\neq\rangle)$ by adapting Segerberg's axiomatisation for von Wright's logic of elsewhere.

  See e.g. [Segerberg, Theoria 1981]

Method to axiomatise $\mathrm{MSL}(*, \Diamond)$

- The Hilbert-style proof system is made of three parts:
  1. Axioms and rule from propositional calculus.
  2. Axiomatisation for Boolean combinations of core formulae.
  3. Axioms and rules to transform any formula into a Boolean combination of core formulae.

- Only formulae in $\mathrm{MSL}(*, \Diamond)$ are used !

- Boolean combinations of core formulae capture $\mathrm{MSL}(*, \Diamond)$.

Core formulae

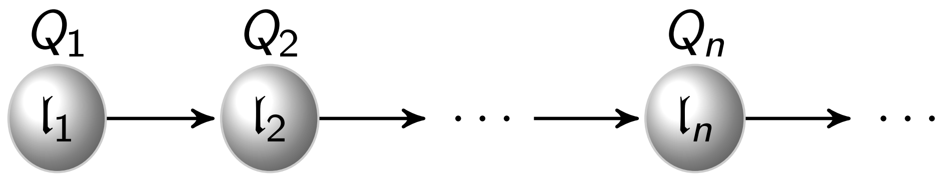
- Size formulae $\mathtt{size} \geq \beta$ and graph formulae $\mathcal{G}$

$$\ell := \top \mid \bot \mid p \mid \neg p \qquad Q := \ell \mid Q \wedge Q$$

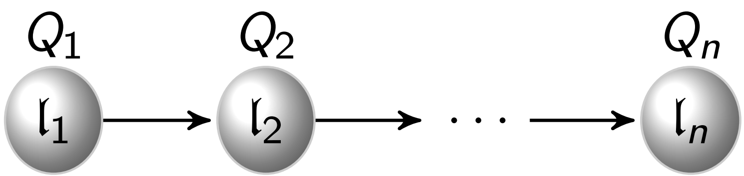
$$\mathcal{G} := |Q,\dots,Q\rangle \mid |Q,\dots,Q] \mid |Q,\dots,\overleftarrow{Q,\dots,Q}|,$$

$p \in \mathrm{PROP}$, $\mathcal{G}$ contains at least one Q.

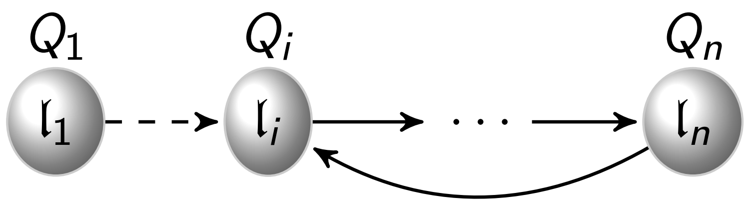
$|Q_1,\dots,Q_n\rangle$:



$|Q_1,\dots,Q_n]$:

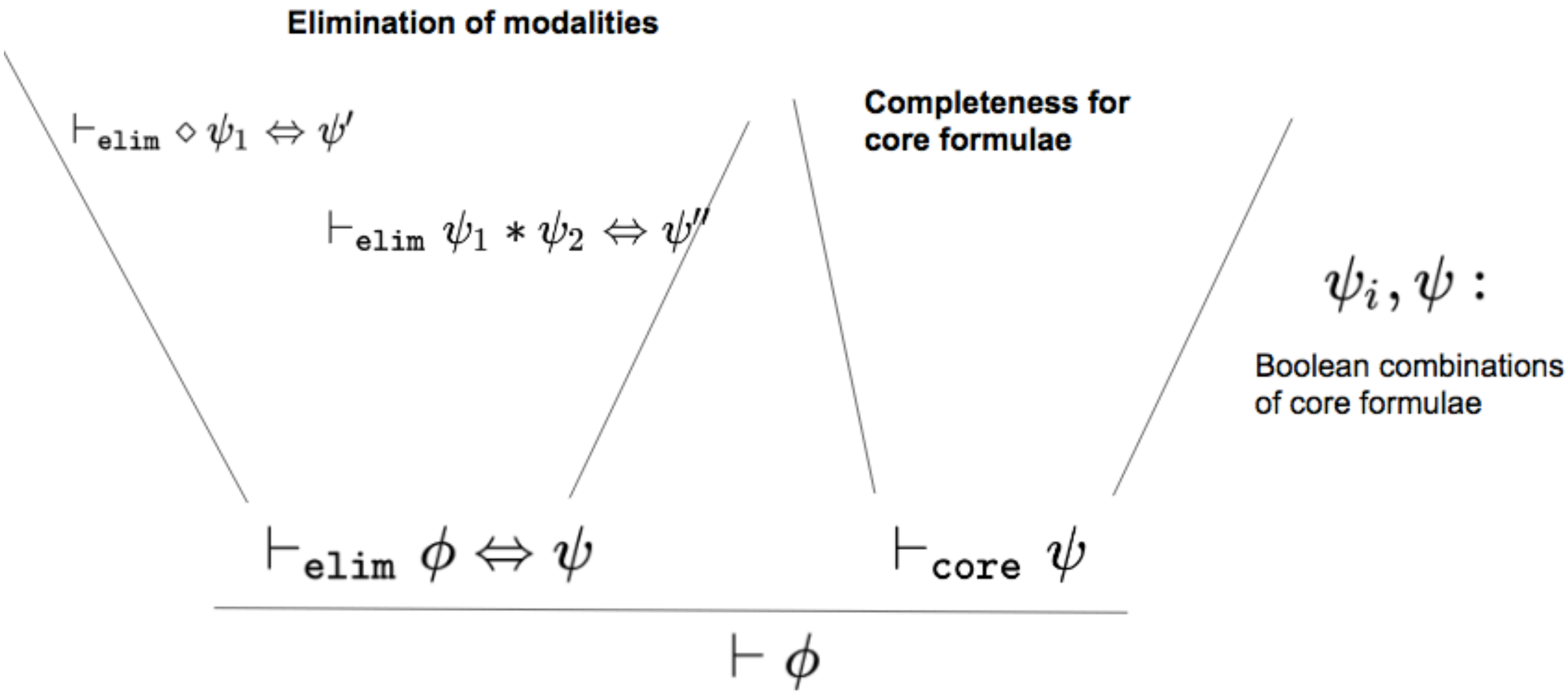


$|Q_1,\dots,\overleftarrow{Q_i,\dots,Q_n}|$:



- The core formulae are logically equivalent to formulae in MSL$(*, \Diamond)$.

Eliminating modalities & reasoning on core formulae



Axioms and inference rules

- Axioms dedicated to size formulae and inconsistencies, e.g.

$$\texttt{size} \geq 0 \qquad \texttt{size} \geq \beta{+}1 \Rightarrow \texttt{size} \geq \beta$$

- Axioms dedicated to conjunctions and negations, e.g.

$$|Q_1,\ldots,\overleftarrow{Q_i,\ldots,Q_n}| \wedge |Q'_1,\ldots,Q'_i,\ldots,Q'_n\overleftarrow{\,}| \Leftrightarrow |Q_1 \wedge Q'_1,\ldots,Q_i \wedge Q'_i,\ldots,\overleftarrow{Q_n \wedge Q'_n}|$$

- Axioms and rules to eliminate $\Diamond$ and $*$, e.g.

$$\Diamond(|Q_1,\ldots,Q_n\rangle) \Leftrightarrow |\top,\overleftarrow{Q_1,\ldots,Q_n}| \vee |\top,Q_1,\ldots,Q_n\rangle \qquad \frac{\phi \Rightarrow \psi}{\Diamond\phi \Rightarrow \Diamond\psi}$$

- Completeness of the calculus with the additional axiom:

$$p \Leftrightarrow (|p\rangle \vee \overleftarrow{[p] \vee |p\ }|).$$

[Demri & Fervari & Mansutti, JELIA'19]

Concluding remarks

- Introduction to basic modal separation logics and investigations on their complexity and axiomatisation.

- Other results: axiomatisation of $\mathsf{MSL}(*, \langle \neq \rangle)$, addition of $\mathrel{-\!\!*}$, etc.... See the papers in AiML'18 and JELIA'19

- Some on-going works:
  - Complexity for $\mathsf{MSL}(*, \Diamond^{-1})$ or $\mathsf{MSL}(*, \Diamond^{-1}, \Diamond)$.

  - Relationships with *QCTL*, see [Bednarczyk & Demri, LICS'19]