Separation Logics: A Modal Perspective

Raul Fervari
FAMAF-UNC & CONICET (Argentina)

LIRa seminar, ILLC, UvA
Amsterdam, NL, 2019

Joint work with Stéphane Demri & Alessio Mansutti (LSV, U. Paris-Saclay & CNRS, France)

Updating models

- Fascinating realm of (modal) logics updating models:
  - logics of public announcement [Plaza, 1989; Lutz, AAMAS'06]
  - sabotage modal logics [van Benthem, 2002]
  - relation-changing modal logics [Fervari, PhD 2014]
  - separation logics [Reynolds, LICS'02]
  - one-agent refinement modal logic [Bozzelli & van Ditmarsch & Pinchinat, TCS 2015]
  - 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 [Plaza, 1989; Lutz, AAMAS'06]
  - sabotage modal logics [van Benthem, 2002]
  - relation-changing modal logics [Fervari, PhD 2014]
  - separation logics [Reynolds, LICS'02]
  - one-agent refinement modal logic [Bozzelli & van Ditmarsch & Pinchinat, TCS 2015]
  - modal separation logic DMBI [Courtault & Galmiche, JLC 2018]
  - logics with reactive Kripke semantics [Gabbay, Book 2013]
- This work: **combining** separation logics with modal logics, leading to new relation-changing modal logics.

Frame rule and separating conjunction

- Separation logic:
  - Extension of Floyd-Hoare logic for (concurrent) programs with mutable data structures.
  - Extension of Hoare logic with separating connectives $*$ and $-\!*$.

    [O'Hearn, Reynolds & Yang, CSL'01; Reynolds, LICS'02]

Frame rule and separating conjunction

- Separation logic:
  - Extension of Floyd-Hoare logic for (concurrent) programs with mutable data structures.
  - 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 C does not mess with ψ'.

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

Frame rule and separating conjunction

- Separation logic:
  - Extension of Floyd-Hoare logic for (concurrent) programs with mutable data structures.
  - 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 states with one record field

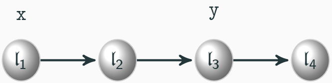
- Program variables $\text{PVAR} = \{\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \ldots\}$.
- $\mathtt{Loc}$: countably infinite set of locations

  $\mathtt{Val}$: countably infinite set of values with $\mathtt{Loc} \subseteq \mathtt{Val}$.
- Memory state $(\mathfrak{s}, \mathfrak{h})$:
  - Store $\mathfrak{s} : \text{PVAR} \rightarrow \mathtt{Val}$.
  - Heap $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{\mathit{fin}} \mathtt{Val}$ (finite domain).
  - In this talk, we assume $\mathtt{Loc} = \mathtt{Val} = \mathbb{N}$.

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

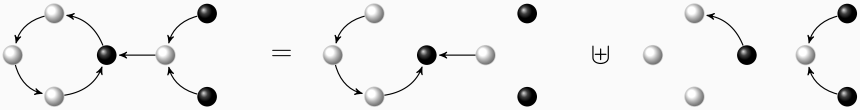
  $\mathtt{Val}$: countably infinite set of values with $\mathtt{Loc} \subseteq \mathtt{Val}$.
- Memory state $(\mathfrak{s}, \mathfrak{h})$:
  - Store $\mathfrak{s}$: PVAR $\rightarrow \mathtt{Val}$.
  - Heap $\mathfrak{h} : \mathtt{Loc} \rightharpoonup_{fin} \mathtt{Val}$ (finite domain).
  - In this talk, we assume $\mathtt{Loc} = \mathtt{Val} = \mathbb{N}$.



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

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.



Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, alternative to FOSL

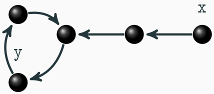
  [Demri & Fervari, AiML'18].

Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, alternative to FOSL

  [Demri & Fervari, AiML'18].

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



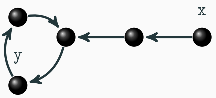
$(\mathtt{ls}(\mathtt{x}, \mathtt{y}) * \top)$ vs. $@_{\mathtt{x}}\mathsf{EF}\mathtt{y}$

Motivations for modal separation logics

- Modal separation logics: Kripke-style semantics with modal and separating connectives, alternative to FOSL

  [Demri & Fervari, AiML'18].

- 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]

Modal separation logic MSL

- Formulae:

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

Modal separation logic MSL

- Formulae:

$$\phi ::= p \mid \texttt{emp} \mid \neg\phi \mid \phi \vee \phi \mid \Diamond\phi \mid \langle\neq\rangle\phi \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi$$

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

Modal separation logic MSL

- Formulae:

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

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

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

Modal separation logic MSL

- Formulae:

$$\phi ::= p \mid \texttt{emp} \mid \neg\phi \mid \phi \vee \phi \mid \Diamond\phi \mid \langle\neq\rangle\phi \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi$$

- Models $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$:
  - $\mathfrak{R} \subseteq \mathbb{N} \times \mathbb{N}$ is finite and functional,
  - $\mathfrak{V} : \mathrm{PROP} \rightarrow \mathcal{P}(\mathbb{N})$.
- Disjoint unions $\mathfrak{M}_1 \uplus \mathfrak{M}_2$.
- The models have an infinite universe and a finite relation encoding the heap.

Semantics

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

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

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

Semantics

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

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

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

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

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

$$\mathfrak{M}, \mathfrak{l} \models \phi_1 \mathrel{-\!\!*} \phi_2 \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \text{for all } \mathfrak{M}' = \langle\mathbb{N}, \mathfrak{R}', \mathfrak{V}\rangle \text{ such that } \mathfrak{R} \cup \mathfrak{R}' \text{ is finite}$$
$$\text{and functional, and } \mathfrak{R} \cap \mathfrak{R}' = \emptyset,$$
$$\mathfrak{M}', \mathfrak{l} \models \phi_1 \text{ implies } \langle\mathbb{N}, \mathfrak{R} \cup \mathfrak{R}', \mathfrak{V}\rangle, \mathfrak{l} \models \phi_2.$$

Examples

- Universal modality:

$$\langle \mathrm{U} \rangle \phi \stackrel{\mathsf{def}}{=} \phi \vee \langle \neq \rangle \phi$$

Examples

- Universal modality:

$$\langle \mathrm{U} \rangle \phi \stackrel{\mathsf{def}}{=} \phi \vee \langle \neq \rangle \phi$$

- $\mathtt{emp}$ is definable (in fragments with $\Diamond + \langle \neq \rangle$):

$$\mathtt{emp} \stackrel{\mathsf{def}}{=} [\mathrm{U}]\Box\bot$$

Examples

- Universal modality:

$$\langle \mathrm{U} \rangle \phi \stackrel{\mathsf{def}}{=} \phi \vee \langle \neq \rangle \phi$$

- $\mathtt{emp}$ is definable (in fragments with $\Diamond + \langle \neq \rangle$):

$$\mathtt{emp} \stackrel{\mathsf{def}}{=} [\mathrm{U}]\Box\bot$$

- Size of the accessibility relation:

$$\mathtt{size} \geq k \stackrel{\mathsf{def}}{=} \underbrace{\neg\mathtt{emp} * \cdots * \neg\mathtt{emp}}_{k \text{ times}}$$

Examples

- Universal modality:

$$\langle \mathrm{U} \rangle \phi \stackrel{\mathsf{def}}{=} \phi \vee \langle \neq \rangle \phi$$

- emp is definable (in fragments with $\Diamond + \langle \neq \rangle$):

$$\mathtt{emp} \stackrel{\mathsf{def}}{=} [\mathrm{U}]\Box\bot$$

- Size of the accessibility relation:

$$\mathtt{size} \geq k \stackrel{\mathsf{def}}{=} \underbrace{\neg\mathtt{emp} * \cdots * \neg\mathtt{emp}}_{k \text{ times}}$$

- Nominal x as in hybrid (modal) logics.

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

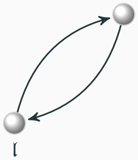
Examples

- The formula $(\Diamond\top * \Diamond\top)$ is a contradiction.

Examples

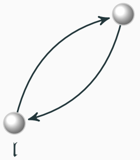
- The formula $(\Diamond\top * \Diamond\top)$ is a contradiction.
- The model is a loop of length 2 visiting the current location $\mathfrak{l}$:

$$\texttt{size} \geq 2 \land \neg\texttt{size} \geq 3 \land \Diamond\Diamond\Diamond\top\land$$
$$\neg(\neg\texttt{emp} * \Diamond\Diamond\Diamond\top) \land \neg\Diamond(\neg\texttt{emp} * \Diamond\Diamond\Diamond\top)$$

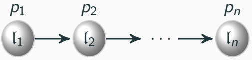


- The formula $(\Diamond\top \ast \Diamond\top)$ is a contradiction.
- The model is a loop of length 2 visiting the current location $\mathfrak{l}$:

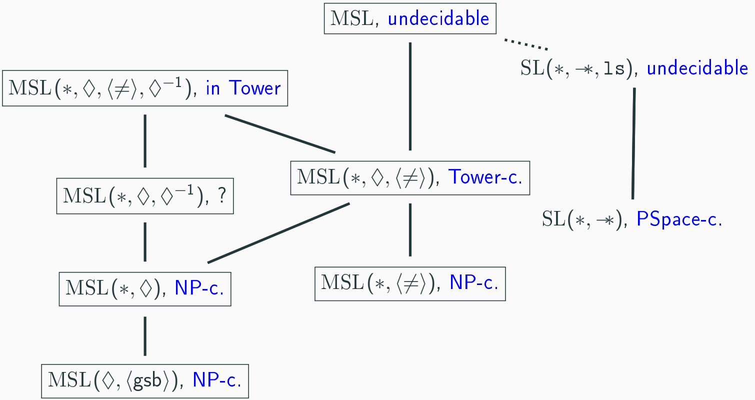
$$\texttt{size} \geq 2 \wedge \neg\texttt{size} \geq 3 \wedge \Diamond\Diamond\Diamond\top \wedge$$
$$\neg(\neg\texttt{emp} \ast \Diamond\Diamond\Diamond\top) \wedge \neg\Diamond(\neg\texttt{emp} \ast \Diamond\Diamond\Diamond\top)$$



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



Overview about satisfiability problems



- PSpace-C. of SL($*$, $-\!\!*$) [Calcagno & Yang & O'Hearn, FSTTCS'01]
- Undec. of SL($*$, $-\!\!*$, ls) [Demri & Lozes & Mansutti, FOSSACS'18]
- Complexity class Tower [Schmitz, ToCT 2016]

Axiomatising Modal Separation Logics

- Main challenges:
  - dealing with languages lacking uniform substitution.

Axiomatising Modal Separation Logics

- Main challenges:
  - dealing with languages lacking uniform substitution.
  - puristic approach: systems without external features (e.g. labels).

Axiomatising Modal Separation Logics

- Main challenges:
  - dealing with languages lacking uniform substitution.
  - puristic approach: systems without external features (e.g. labels).
- 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]

Axiomatising Modal Separation Logics

- Main challenges:
  - dealing with languages lacking uniform substitution.
  - puristic approach: systems without external features (e.g. labels).
- 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]
- Our approach: design a subclass of formulae in $\mathrm{MSL}(*, \Diamond)$ that captures the expressive power of $\mathrm{MSL}(*, \Diamond)$ **("core formulae")**.

  [Demri & Fervari & Mansutti, JELIA'19]

Axiomatising Modal Separation Logics

- Main challenges:
  - dealing with languages lacking uniform substitution.
  - puristic approach: systems without external features (e.g. labels).
- 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]
- Our approach: design a subclass of formulae in $\mathrm{MSL}(*, \Diamond)$ that captures the expressive power of $\mathrm{MSL}(*, \Diamond)$ **("core formulae")**.

  [Demri & Fervari & Mansutti, JELIA'19]
- Calculus for $\mathrm{MSL}(*, \langle\neq\rangle)$ adapting [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.

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!

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!
- Similar to Dynamic Epistemic Logic's reduction axioms.

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!
- Similar to Dynamic Epistemic Logic's reduction axioms.
- Boolean combinations of core formulae capture $\mathrm{MSL}(*, \Diamond)$.

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.

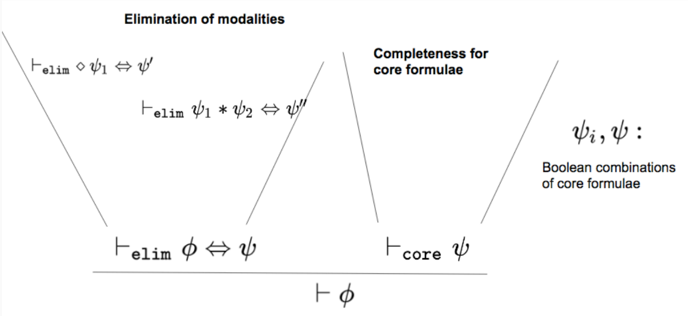
- Only formulae in $\mathrm{MSL}(*, \Diamond)$ are used!

- Similar to Dynamic Epistemic Logic's reduction axioms.

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

- Intuitively, each formula is equivalent to (Boolean combination of):
  - a modal part, and
  - a size part.

Eliminating modalities & reasoning on core formulae



Hilbert-style system for $\mathrm{MSL}(*, \Diamond)$

- The modal part is named graph formula

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

Hilbert-style system for $\mathrm{MSL}(*, \Diamond)$

- The modal part is named graph formula

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

$$\mathcal{G} \quad := \quad |Q, \ldots, Q\rangle \mid |Q, \ldots, Q] \mid |Q, \ldots, \overset{\curvearrowleft}{Q}, \ldots, Q|$$

Hilbert-style system for $\mathrm{MSL}(*, \Diamond)$

- The modal part is named graph formula

$$\ell \quad := \quad \top \mid \bot \mid p \mid \neg p \qquad\qquad Q := \ell \mid Q \wedge Q$$
$$\mathcal{G} \quad := \quad |Q, \ldots, Q\rangle \mid |Q, \ldots, Q] \mid |Q, \ldots, \overset{\downarrow}{Q}, \ldots, Q\rceil$$

- For a size formula we have

$$\mathtt{size} \geq \beta \quad \text{or} \quad \neg\mathtt{size} \geq \beta, \qquad (\beta \in \mathbb{N})$$

Hilbert-style system for $\mathrm{MSL}(*, \Diamond)$

- The modal part is named graph formula

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

$$\mathcal{G} \quad := \quad |Q, \ldots, Q\rangle \mid |Q, \ldots, Q] \mid |Q, \ldots, \overset{\downarrow}{Q}, \ldots, Q|$$

- For a size formula we have

$$\mathtt{size} \geq \beta \quad \text{or} \quad \neg\mathtt{size} \geq \beta, \qquad (\beta \in \mathbb{N})$$

- **Claim:** Each $\mathrm{MSL}(*, \Diamond)$-formula is equivalent to a Boolean combination of formulas of the shape

$$\mathcal{G} \wedge \mathtt{size} \geq \beta \quad \text{or} \quad \mathcal{G} \wedge \mathtt{size} \geq \beta \wedge \neg\mathtt{size} \geq \beta'$$

Intuitive semantics of graph formulae

$|Q_1, \ldots, Q_n\rangle$ characterises: 

Intuitive semantics of graph formulae

$|Q_1, \ldots, Q_n\rangle$ characterises:

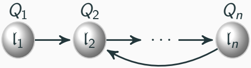
$|Q_1, \ldots, Q_n]$ characterises:

Intuitive semantics of graph formulae

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

$|Q_1, \dots, Q_n]$ characterises:

$|Q_1, \overleftarrow{Q_2, \dots, Q_n}|$ characterises:

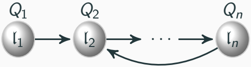


Intuitive semantics of graph formulae

$|Q_1, \ldots, Q_n\rangle$ characterises:

$|Q_1, \ldots, Q_n]$ characterises:

$|Q_1, \overleftarrow{Q_2, \ldots, Q_n}|$ characterises:



Claim: Graph formulae are definable in $\mathrm{MSL}(*, \Diamond)$.

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 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.

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

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.

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

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

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

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.

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

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

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

- Completeness of the calculus with the additional axiom:

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

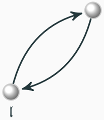
[Demri & Fervari & Mansutti, JELIA'19]

From $\mathrm{MSL}(*, \Diamond)$ to core formulae - example

The formula

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

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



can be shown equivalent to

$$\mathtt{size} \geq 2 \land \neg \mathtt{size} \geq 3 \land |\top, \top|$$

Concluding remarks

- Introduction to basic modal separation logics and investigations on their complexity and axiomatisation.
- Axiomatisations for the fragment $\mathrm{MSL}(*, \Diamond, \langle \neq \rangle)$?

Concluding remarks

- Introduction to basic modal separation logics and investigations on their complexity and axiomatisation.
- Axiomatisations for the fragment $\mathrm{MSL}(*, \Diamond, \langle\neq\rangle)$?
- Some ongoing works:
  - Expressivity and complexity for $\mathrm{MSL}(*, \Diamond^{-1})$?
    (with B. Bednarczyk, S. Demri & A. Mansutti).
  - Tableaux methods for core formulae.
    (with A. Saravia).