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 \( \bullet \).
  [O’Hearn, Reynolds & Yang, CSL’01; Reynolds, LICS’02]

• Frame rule:

\[
\begin{align*}
\{ \phi \} C \{ \psi \} & \quad \frac{\{ \phi \} C \{ \psi \}}{\{ \phi * \psi' \} C \{ \psi * \psi' \}} \\
\text{where } C \text{ does not mess with } \psi'.
\end{align*}
\]

\[
\begin{align*}
\{ x \leftarrow 5 \} * x \leftarrow 4 & \quad \frac{\{ x \leftarrow 4 \}}{\{ x \leftarrow 5 * y \leftarrow 3 \} * x \leftarrow 4 \quad \frac{\{ x \leftarrow 4 * y \leftarrow 3 \}}{\{ x \leftarrow 5 * y \leftarrow 3 \} * x \leftarrow 4 \quad \frac{\{ x \leftarrow 4 * y \leftarrow 3 \}}{\{ x \leftarrow 5 * y \leftarrow 3 \} * x \leftarrow 4 \quad \frac{\{ x \leftarrow 4 * y \leftarrow 3 \}}{\{ x \leftarrow 5 * y \leftarrow 3 \}}}
\end{align*}
\]

• \((s, h) \models x \leftarrow 5 * y \leftarrow 3\) implies \((s, h) \models x \neq y\).
Memory states with one record field

- Program variables \( \text{PVAR} = \{x_1, x_2, x_3, \ldots\} \).

- \( \text{Loc} \): countably infinite set of locations
  \( \text{Val} \): countably infinite set of values with \( \text{Loc} \subseteq \text{Val} \).

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

- The heaps $h_1$ and $h_2$ are disjoint iff $\text{dom}(h_1) \cap \text{dom}(h_2) = \emptyset$.
- When $h_1$ and $h_2$ are disjoint, $h_1 \uplus h_2$ is their disjoint union.

\[
\begin{array}{c}
\text{\includegraphics[width=0.4\textwidth]{disjoint_heaps}}
\end{array}
\]
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.

\[(\mathsf{ls}(x, y) \ast \top) \text{ vs. } @_x \mathsf{EF} y\]

• 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 $\text{MSL}(\ast, \Diamond, \langle \neq \rangle)$

[Demri & Fervari, AiML’18]

- Formulae:
  $$\phi ::= p \mid \text{emp} \mid \neg \phi \mid \phi \lor \phi \mid \Diamond \phi \mid \langle \neq \rangle \phi \mid \phi \ast \phi$$

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

- Disjoint unions $M_1 \uplus M_2$.

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

\[ M, l \models p \quad \text{def} \quad l \in \mathcal{V}(p) \]

\[ M, l \models \Diamond \phi \quad \text{def} \quad M, l' \models \phi, \text{ for some } l' \in \mathbb{N} \text{ such that } (l, l') \in \mathcal{R} \]

\[ M, l \models \langle \neq \rangle \phi \quad \text{def} \quad M, l' \models \phi, \text{ for some } l' \in \mathbb{N} \text{ such that } l' \neq l \]

\[ M, l \models \text{emp} \quad \text{def} \quad \mathcal{R} = \emptyset \]

\[ M, l \models \phi_1 \star \phi_2 \quad \text{def} \quad \langle \mathbb{N}, \mathcal{R}_1, \mathcal{V} \rangle, l \models \phi_1 \text{ and } \langle \mathbb{N}, \mathcal{R}_2, \mathcal{V} \rangle, l \models \phi_2, \text{ for some partition } \{\mathcal{R}_1, \mathcal{R}_2\} \text{ of } \mathcal{R} \]
Examples

\[ \langle U \rangle \phi \overset{\text{def}}{=} \phi \lor \langle \not= \rangle \phi \quad \text{size} \geq k \overset{\text{def}}{=} \neg \text{emp} \cdot \cdots \cdot \neg \text{emp} \quad (k \text{ times}) \]

- Nominal \( x \) as in hybrid (modal) logics.

\[ \langle U \rangle (x \land \neg \not= \neg x) \]

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

\[ \text{size} \geq 2 \land \neg \text{size} \geq 3 \land \Diamond \Diamond \Diamond \top \land \neg (\neg \text{emp} \cdot \Diamond \Diamond \Diamond \top) \land \neg \Diamond (\neg \text{emp} \cdot \Diamond \Diamond \Diamond \top) \]

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

Modal separation logics
Tower-completeness of SAT(MSL(*, ◊, ⟨≠⟩))

• Linear model:

\[ l_0 \rightarrow l_1 \rightarrow \cdots \rightarrow l_n \]

• There is a formula \( \phi_{\exists l_1} \) in MSL(*, ◊, ⟨≠⟩) such that \( \mathcal{M} \models \phi_{\exists l_1} \) iff \( \mathcal{M} \) 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.

\[ a_1 a_2 a_1 \triangleright l_0 \rightarrow l_1 \rightarrow l_2 \rightarrow l_3, l_0 \]

• MSL(*, ◊, ⟨≠⟩) satisfiability problem is TOWER-hard.

[Demri & Fervari, AiML’18]
Variants

• The satisfiability problems for $\text{MSL}(\ast, \Diamond)$ and $\text{MSL}(\ast, \langle \not= \rangle)$ are $\text{NP}$-complete. (for $\text{SL}(\ast)$, $\text{PSPACE}$-completeness)

• Undecidability of $\text{MSL}(\ast, \Diamond, \langle \not= \rangle) + \text{magic wand} \not\ast$.
  [Demri & Fervari, AiML’18]

• Modal logic for heaps $\text{MLH}(\ast)$ is $\text{TOWER}$-complete.
  [Demri & Deters, TOCL 2015]
Hilbert-style axiomatisation of $\text{MSL}(\ast, \Diamond)$

- 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 $\text{MSL}(\ast, \Diamond)$ are used.

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

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

  See e.g. [Segerberg, Theoria 1981]
Method to axiomatise $\text{MSL}(\ast, \diamond)$

- 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 $\text{MSL}(\ast, \diamond)$ are used!

- Boolean combinations of core formulae capture $\text{MSL}(\ast, \diamond)$. 
Core formulae

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

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

$$
\mathcal{G} := |Q,\ldots,Q| \mid |Q,\ldots,Q| \mid |Q,\ldots,\neg Q,\ldots,Q|
$$

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

- The core formulae are logically equivalent to formulae in $\text{MSL}(*,\diamond)$.
Eliminating modalities & reasoning on core formulae

Elimination of modalities

\[ \vdash_{\text{elim}} \Diamond \psi_1 \iff \psi' \]

\[ \vdash_{\text{elim}} \psi_1 \ast \psi_2 \iff \psi'' \]

\[ \vdash_{\text{elim}} \phi \iff \psi \]

\[ \vdash_{\text{core}} \psi \]

\[ \vdash \phi \]

Completeness for core formulae

\[ \psi, \psi_i : \]

Boolean combinations of core formulae

Hilbert-style axiomatisation for MSL\((\ast, \Diamond)\)
Axioms and inference rules

- Axioms dedicated to size formulae and inconsistencies, e.g.
  \[ \text{size} \geq 0 \quad \text{size} \geq \beta + 1 \Rightarrow \text{size} \geq \beta \]

- Axioms dedicated to conjunctions and negations, e.g.
  \[ |Q_1, \ldots, Q_i, \ldots, Q_n \rangle \land |Q'_1, \ldots, Q'_i, \ldots, Q'_n \rangle \Leftrightarrow |Q_1 \land Q'_1, \ldots, Q_i \land Q'_i, \ldots, Q_n \land Q'_n | \]

- Axioms and rules to eliminate \( \Diamond \) and \( * \), e.g.
  \[
  \Diamond(|Q_1, \ldots, Q_n \rangle) \Leftrightarrow |\top, Q_1, \ldots, Q_n \rangle \lor |\top, Q_1, \ldots, Q_n \rangle
  \]
  \[
  \phi \Rightarrow \psi
  \]
  \[
  \Diamond \phi \Rightarrow \Diamond \psi
  \]

- Completeness of the calculus with the additional axiom:
  \[
  p \Leftrightarrow (|p \rangle \lor |\top, p \rangle \lor |p \rangle).
  \]

[Demri & Fervari & Mansutti, JELIA’19]
Concluding remarks

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

- Other results: axiomatisation of $\text{MSL}(\ast, \langle \neq \rangle)$, addition of $\neg \ast$, etc. See the papers in AiML’18 and JELIA’19

- Some on-going works:
  - Complexity for $\text{MSL}(\ast, \Diamond^{-1})$ or $\text{MSL}(\ast, \Diamond^{-1}, \Diamond)$.
  - Relationships with $QCTL$, see [Bednarczyk & Demri, LICS’19]