Modal Separation Logics and Friends

Stéphane Demri
demri@lsv.fr

Joint works with M. Deters, R. Fervari, A. Mansutti, etc.

University of Helsinki

November 2019
Updating models

- Fascinating realm of (modal) logics updating models:
  - logics of public announcement [Lutz, AAMAS’06]
  - sabotage modal logics [van Benthem, 2002]
  - propositional team logics [Väänänen, 2007]
  - separation logics [Reynolds, LICS’02]
  - logic with separating modalities LSM [Courtault & Galmiche & Pym, TCS 2016]
  - modal separation logic DMBI [Courtault & Galmiche, JLC 2018]
  - logics with reactive Kripke semantics [Gabbay, 2013]
Updating models

• Fascinating realm of (modal) logics updating models:
  • logics of public announcement [Lutz, AAMAS’06]
  • sabotage modal logics [van Benthem, 2002]
  • propositional team logics [Väänänen, 2007]
  • separation logics [Reynolds, LICS’02]
  • logic with separating modalities LSM [Courtault & Galmiche & Pym, TCS 2016]
  • modal separation logic DMBI [Courtault & Galmiche, JLC 2018]
  • logics with reactive Kripke semantics [Gabbay, 2013]

• This work: combining separation logics with modal logics.
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 $\text{Loc} \subseteq \text{Val}$. 

Separation logic(s) in a nutshell
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).
  - In this talk, we assume $\text{Loc} = \text{Val} = \mathbb{N}$.

Separation logic(s) in a nutshell
Disjoint heaps

- Disjoint heaps: \( \text{dom}(h_1) \cap \text{dom}(h_2) = \emptyset \) (noted \( h_1 \perp h_2 \)).

- When \( h_1 \perp h_2 \), disjoint heap \( h_1 \uplus h_2 \).
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:
First-order SL

- **Quantified variables** \( \text{FVAR} = \{u_1, u_2, u_3, \ldots\} \).

- **Expressions**: \( e ::= x_i \mid u_j \)

- ** Atomic formulae**:
  \[ \pi ::= e = e' \mid e \leftrightarrow e' \mid \text{emp} \mid \bot \]

- **Formulae**:
  \[ \phi ::= \pi \mid \phi \land \psi \mid \neg \phi \mid \phi * \psi \mid \phi \to \psi \mid \exists u \phi \]
Modal separation logics

- [Brochenin & Demri & Lozes, IC 2012] $\text{SL}(\ast), \text{SL}(\rightarrow\ast)$
- [Demri & Galmiche & Larchey-Wendling & Mery, CSR’14] $\text{1SL}$
- [Demri & Deters, CSL-LICS’14] $\text{2SL}(\rightarrow\ast)$
- [Echenim & Iosif & Peltier, FoSSaCS’19] Prenex-SL
- [Echenim & Iosif & Peltier, TABLEAUX’19] BSR-SL
- [Mansutti, sub. 2019] $\text{1SL}(\ast, \text{alloc}, \rightarrow^+)$
Variants of SL(\(*\))

- SL(\(*\)) + $n$ is decidable by translation into 1SL(\(*\)).
  [Brochenin & Demri & Lozes, IC 2012]

- 2SL(\(*\)) is TOWER-hard by reduction from Propositional Interval Temporal Logic PITL.
  [Demri & Deters, ToCL 2015]
Variants of SL(•)

- SL(•) + $\nabla^n$ is decidable by translation into 1SL(•).
  [Brochenin & Demri & Lozes, IC 2012]

- 2SL(•) is TOWER-hard by reduction from Propositional Interval Temporal Logic PITL.
  [Demri & Deters, ToCL 2015]

- Modal logic for heaps MLH.
  \[ \phi ::= T | \neg \phi | \phi \land \phi | \diamond \phi | \diamond^{-1} \phi | \langle \neq \rangle \phi | \langle \ast \rangle \phi | \phi \star \phi | \phi \Rightarrow \phi. \]

- Models $M = (\mathbb{N}, R)$ with finite and weakly functional $R$.

- $M, l \models \phi_1 \star \phi_2 \iff (\mathbb{N}, R_1), l \models \phi_1$ and $(\mathbb{N}, R_2), l \models \phi_2$ for some partition $\{R_1, R_2\}$ of $R$. 

Modal separation logics
Variants of SL(*)

- SL(*) + $\n$ is decidable by translation into 1SL(*).
  [Brochenin & Demri & Lozes, IC 2012]

- 2SL(*) is TOWER-hard by reduction from Propositional Interval Temporal Logic PITL.
  [Demri & Deters, ToCL 2015]

- Modal logic for heaps MLH.
  - $\phi ::= \top | \neg \phi | \phi \land \phi | \diamond \phi | \diamond^{-1} \phi | \langle \neq \rangle \phi |
  \langle * \rangle \phi | \phi * \phi | \phi \rightarrow \phi.$

  - Models $M = (\mathbb{N}, R)$ with finite and weakly functional $R$.

  - $M, I \models \phi_1 * \phi_2 \iff (\mathbb{N}, R_1), I \models \phi_1$ and $(\mathbb{N}, R_2), I \models \phi_2$ for some partition $\{R_1, R_2\}$ of $R$.

  - MLH (*) is decidable by translation into 2SL(*).

  - Reduction from PITL to MLH (*), whence TOWER-completeness.
  [Demri & Deters, ToCL 2015]
Variants of SL(*)

- \( SL(*) + \overset{n}{\bigcirc} \) is decidable by translation into \( 1SL(*) \).
  \[ \text{[Brochenin & Demri & Lozes, IC 2012]} \]

- \( 2SL(*) \) is \textsc{Tower}-hard by reduction from Propositional Interval Temporal Logic PITL.
  \[ \text{[Demri & Deters, ToCL 2015]} \]

- Modal logic for heaps \( \text{MLH} \).
  - \( \phi ::= \top | \neg \phi | \phi \land \phi | \Diamond \phi | \Diamond^{-1} \phi | \langle \neq \rangle \phi | \langle \star \rangle \phi | \phi \ast \phi | \phi \rightarrow \phi. \)

  - Models \( \mathcal{M} = (\mathbb{N}, \mathcal{R}) \) with finite and weakly functional \( \mathcal{R} \).

  - \( \mathcal{M}, I \models \phi_1 \ast \phi_2 \iff (\mathbb{N}, \mathcal{R}_1), I \models \phi_1 \) and \((\mathbb{N}, \mathcal{R}_2), I \models \phi_2 \) for some partition \( \{\mathcal{R}_1, \mathcal{R}_2\} \) of \( \mathcal{R} \).

  - \( \text{MLH} (*) \) is decidable by translation into \( 2SL(*) \).

  - Reduction from PITL to \( \text{MLH} (*) \), whence \textsc{Tower}-completeness.
    \[ \text{[Demri & Deters, ToCL 2015]} \]

  - \textsc{Tower}-hardness for \( \text{MLH} (\top, \Diamond, \langle U \rangle, \ast) \) \[ \text{[Mansutti, sub. 2019]} \]
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.

\[(\text{ls}(x, y) \land T) \text{ vs. } \mathord{\@_xEF_y}\]
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.

\[ (\text{ls}(x, y) \land T) \text{ vs. } @x \text{EF} y \]

• 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:

$$\phi ::= p \mid \text{emp} \mid \neg \phi \mid \phi \lor \phi \mid \Diamond \phi \mid \langle \neq \rangle \phi \mid \phi \ast \phi$$
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 \( M = \langle N, R, V \rangle \):
  - \( R \subseteq N \times N \) is finite and weakly functional (deterministic),
  - \( V : \text{PROP} \rightarrow \mathcal{P}(N) \).

- Disjoint unions \( M_1 \uplus M_2 \).

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

\[ \mathcal{M}, l \models p \iff l \in \mathcal{V}(p) \]

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

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

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

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

\( M, l \models \langle \neq \rangle \phi \quad \overset{\text{def}}{\iff} \quad M, l' \models \phi, \text{ for some } l' \in \mathbb{N} \text{ such that } l' \neq l \)

\( M, l \models \text{emp} \quad \overset{\text{def}}{\iff} \quad R = \emptyset \)

\( M, l \models \phi_1 \ast \phi_2 \quad \overset{\text{def}}{\iff} \quad \langle \mathbb{N}, R_1, \mathcal{V} \rangle, l \models \phi_1 \text{ and } \langle \mathbb{N}, R_2, \mathcal{V} \rangle, l \models \phi_2, \text{ for some partition } \{R_1, R_2\} \text{ of } R \)
Examples

$$\langle \mathbf{U} \rangle \phi \overset{\text{def}}{=} \phi \lor \langle \neq \rangle \phi \quad \text{size} \geq k \overset{\text{def}}{=} \neg \text{emp} \times \cdots \times \neg \text{emp}$$

$$k \text{ times}$$
Examples

\[
\langle U \rangle \phi \overset{\text{def}}{=} \phi \lor \langle \neq \rangle \phi \quad \text{size } \geq k \overset{\text{def}}{=} \underbrace{\neg \text{emp} \cdot \cdots \cdot \neg \text{emp}}_{k \text{ times}}
\]

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

\[
\langle U \rangle (x \land [\neq] \neg x)
\]
Examples

\[ \langle U \rangle \phi \overset{\text{def}}{=} \phi \lor \langle \neq \rangle \phi \quad \text{size} \geq k = \underbrace{\neg \text{emp} \cdots \neg \text{emp}}_k \]

- Nominal in hybrid modal logic: propositional variable true at a unique state/world/location of the model.
  \[ \langle U \rangle (x \land [\neq] \neg x) \]

- The model is a loop of length 2 visiting the current location:
  \[
  \text{size} \geq 2 \land \neg \text{size} \geq 3 \land \Diamond \Diamond \Diamond T \land \\
  \neg (\neg \text{emp} \ast \Diamond \Diamond \Diamond T) \land \neg \Diamond (\neg \text{emp} \ast \Diamond \Diamond \Diamond T) \\
  \text{(in MSL}(\ast, \Diamond), \text{ but not expressible in Alt}_1/0\text{SL}(\ast, \neg \ast))
  \]

Modal separation logics
Tower upper bound for $\text{SAT}(\text{MSL}(\ast, \Diamond, \langle \neq \rangle))$

- $\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle)$: variant with finite models.

- Reduction $\text{SAT}(\text{MSL}(\ast, \Diamond, \langle \neq \rangle)) \rightarrow \text{SAT}(\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle))$. 
**Tower upper bound for** $\text{SAT}(\text{MSL}(\ast, \Diamond, \langle \neq \rangle))$

- $\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle)$: variant with finite models.

- Reduction $\text{SAT}(\text{MSL}(\ast, \Diamond, \langle \neq \rangle)) \rightarrow \text{SAT}(\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle))$.

- $\text{SAT}(\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle))$ is in $\text{TOWER}$.

  - $\text{TOWER}$: 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 $\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle)$ into satisfiability for the weak MSO theory of $(\mathcal{Q}, f, =)$.

  - Internalisation of the semantics for $\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle)$. 
Towards lower bounds: encoding linear structures

- Linear model:
  \[ l_0 \rightarrow l_1 \rightarrow \cdots \rightarrow l_n \]

- Leaves:

- Pre-roots:
Loops

- Loop:

- $\mathcal{M}$ is linear iff $\mathcal{M}$ is loop-free and has a unique leaf.
Loops

- Loop:

- $M$ is linear iff $M$ is loop-free and has a unique leaf.

- $\exists \text{Loop} \stackrel{\text{def}}{=} \top \ast (([U]\square\diamond \top) \land \neg \text{emp})$  \hfill ([U]\phi \stackrel{\text{def}}{=} \phi \land [\neq]\phi)

- $M \models \exists \text{Loop}$ iff $M$ has at least one loop.
Auxiliary formulae

\[ (\forall) \phi \overset{\text{def}}{=} (\exists U)(\phi \land [\neq] \neg \phi) \quad \text{size} = 1 \overset{\text{def}}{=} \neg \text{emp} \land \neg (\neg \text{emp} \land \neg \text{emp}) \]
Auxiliary formulae

\[ \langle !\rangle \phi \overset{\text{def}}{=} \langle U \rangle (\phi \land [\neq] \neg \phi) \quad \text{size} = 1 \overset{\text{def}}{=} \neg \text{emp} \land \neg (\neg \text{emp} \land \neg \text{emp}) \]

\[ \text{PRoot} \overset{\text{def}}{=} \lozenge \Box \bot \]

\[ \text{UniqTreePRoot} \overset{\text{def}}{=} \neg \exists \text{Loop} \land ((\neg (\neg \text{emp} \land \neg \text{emp})) \lor \langle !\rangle \text{PRoot}) \]

\[ \text{Leaf} \overset{\text{def}}{=} (\lozenge T \land \text{size} = 1) \lor (\lozenge T \land \neg \text{PRoot} \land ((\text{size} = 1 \land \lozenge T) \ast \text{UniqTreePRoot}) \]

Modal separation logics
Auxiliary formulae

\[ \langle ! \rangle \phi \overset{\text{def}}{=} \langle U \rangle (\phi \land \lnot \phi) \quad \text{size} = 1 \overset{\text{def}}{=} \lnot \text{emp} \land \lnot (\lnot \text{emp} \land \lnot \text{emp}) \]

\[ \text{PRoot} \overset{\text{def}}{=} \Diamond \Box \bot \]

\[ \text{UniqTreePRoot} \overset{\text{def}}{=} \neg \exists \text{Loop} \land ((\neg (\neg \text{emp} \land \lnot \text{emp})) \lor \langle ! \rangle \text{PRoot}) \]

\[ \text{Leaf} \overset{\text{def}}{=} (\Diamond T \land \text{size} = 1) \lor (\Diamond T \land \neg \text{PRoot} \land ((\text{size} = 1 \land \Diamond T) \ast \text{UniqTreePRoot}) \]

- \( M, I \models \text{UniqTreePRoot} \) iff \( M \) is loop-free and either \( K \) is empty or \( \Lambda \) has at most one MCC and a unique pre-root.
Auxiliary formulae

\[ \langle ! \rangle \phi \overset{\text{def}}{=} \langle U \rangle (\phi \land \neg \neg \phi) \quad \text{size} = 1 \overset{\text{def}}{=} \neg \text{emp} \land \neg (\neg \text{emp} \land \neg \text{emp}) \]

\[ \text{PRoot} \overset{\text{def}}{=} \lozenge \Box \bot \]

\[ \text{UniqTreePRoot} \overset{\text{def}}{=} \neg \exists \text{Loop} \land ((\neg (\neg \text{emp} \land \neg \text{emp})) \lor \langle ! \rangle \text{PRoot}) \]

\[ \text{Leaf} \overset{\text{def}}{=} (\lozenge T \land \text{size} = 1) \lor (\lozenge T \land \neg \text{PRoot} \land ((\text{size} = 1 \land \lozenge T) \ast \text{UniqTreePRoot}) \]

- \( \mathcal{M}, I \models \text{UniqTreePRoot} \) iff \( \mathcal{M} \) is loop-free and either \( \mathcal{R} \) is empty or (\( \mathcal{M} \) has at most one MCC and a unique pre-root).

- Assuming that \( \mathcal{M} \models \text{UniqTreePRoot} \), we have \( \mathcal{M}, I \models \text{Leaf} \) iff \( I \) is a leaf.
Characterisation of linear structures

- $\phi_{ls} \overset{\text{def}}{=} \text{emp} \lor (\text{UniqTreePRoot} \land \langle ! \rangle \text{Leaf})$.

- $\mathcal{M} \models \phi_{ls}$ iff $\mathcal{M}$ is linear.
Characterisation of linear structures

• $\phi_{\text{ls}} \overset{\text{def}}{=} \text{emp} \lor (\text{UniqTreePRoot} \land (\langle ! \rangle \text{Leaf})).

• $\mathcal{M} \models \phi_{\text{ls}}$ iff $\mathcal{M}$ is linear.

• $\text{ls}(x, y)$ from symbolic heap fragment can be encoded by

\[
\phi_{\text{ls}}(x, y) \overset{\text{def}}{=} \phi_{\text{ls}} \land ((\text{emp} \land (\langle U \rangle (x \land y))) \lor (\langle U \rangle (x \land \text{Leaf}) \land (\langle U \rangle (\text{PRoot} \land \langle Y \rangle)))).
\]
Characterisation of linear structures

- $\phi_{\exists ls} \overset{\text{def}}{=} \text{emp} \lor (\text{UniqTreePRoot} \land \langle ! \rangle \text{Leaf})$.

- $M \models \phi_{\exists ls}$ iff $M$ is linear.

- $ls(x, y)$ from symbolic heap fragment can be encoded by

$$\phi_{ls}(x, y) \overset{\text{def}}{=} \phi_{\exists ls} \land ((\text{emp} \land \langle U \rangle (x \land y)) \lor (\langle U \rangle (x \land \text{Leaf}) \land (\langle U \rangle (\text{PRoot} \land \Diamond y))))$$

- So, $0\text{SL}(\ast, \ast, ls)$ can be encoded into $\text{MSL}(\ast, \ast, \Diamond, \langle \neq \rangle)$:
  - $x = y \approx \langle U \rangle (x \land y)$
  - $x \leftarrow y \approx \langle U \rangle (x \land \Diamond y)$
Characterisation of linear structures

- $\phi_{\text{ls}} \overset{\text{def}}{=} \text{emp} \lor (\text{UniqTreePRoot} \land \langle ! \rangle \text{Leaf})$.

- $\mathcal{M} \models \phi_{\text{ls}}$ iff $\mathcal{M}$ is linear.

- ls$(x, y)$ from symbolic heap fragment can be encoded by
  
  $\phi_{\text{ls}}(x, y) \overset{\text{def}}{=} \phi_{\text{ls}} \land ((\text{emp} \land \langle U \rangle (x \land y)) \lor (\langle U \rangle (x \land \text{Leaf}) \land \langle U \rangle (\text{PRoot} \land \Diamond y)))$

- So, $\text{0SL}(\ast, \ast, \text{ls})$ can be encoded into $\text{MSL}(\ast, \ast, \Diamond, \langle \neq \rangle)$:
  - $x = y \ni \langle U \rangle (x \land y)$
  - $x \leftarrow y \ni \langle U \rangle (x \land \Diamond y)$

- Satisfiability for $\text{0SL}(\ast, \ast, \text{ls})$ is undecidable.
  
  [Demri & Lozes & Mansutti, FoSSaCS’18]

- $\text{MSL}(\ast, \ast, \Diamond, \langle \neq \rangle)$ satisfiability problem is undecidable.
  Further refined for $\text{MSL}(\ast, \ast, \Diamond)$
  
  [Mansutti, priv. com.]
Nonemptiness problem for star-free expressions

- 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]
Nonemptiness problem for star-free expressions

- Star-free expressions:
  \[ e ::= a \mid \varepsilon \mid e \cup e \mid ee \mid \sim e \]

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

- Encoding words by linear models.
**Tower-hardness of** $\text{MSL}(*, \Diamond, \langle \neq \rangle)$

[Demri & Fervari, AiML’18]

\[ a_i \overset{\text{def}}{=} p_i \land \bigwedge_{j \neq i} \neg p_j \]

\[ T(e) \overset{\text{def}}{=} ([\bigvee_i a_i] \land \phi_{\exists l}s \land (\text{emp} \land t(e)) \lor (\neg \text{emp} \land \text{Leaf} \land t(e))) \]

(evaluation done on the leaf)
TOWER-hardness of MSL(\(*, \Diamond, \langle \not\equiv \rangle\))

[Demri & Fervari, AiML’18]

\[ a_i \overset{\text{def}}{=} p_i \land \bigwedge_{j \neq i} \neg p_j \]

\[ T(e) \overset{\text{def}}{=} ([\bigcup_i a_i] \land \phi_{\exists l} \land (\text{emp} \land t(e))) \lor (\neg \text{emp} \land \text{Leaf} \land t(e)) \]

(evaluation done on the leaf)

\[ t(\varepsilon) \overset{\text{def}}{=} \text{emp} \]
\[ t(a_i) \overset{\text{def}}{=} (\Diamond a_i) \land \text{size} = 1 \]

\[ t(\sim e) \overset{\text{def}}{=} \neg t(e) \]
\[ t(e_1 \cup e_2) \overset{\text{def}}{=} t(e_1) \lor t(e_2) \]

\[ t(e_1 e_2) \overset{\text{def}}{=} \psi_1 \lor \psi_2 \lor \psi_3 \lor \psi_4 \]

\[ \psi_1 \overset{\text{def}}{=} \text{emp} \land t(e_1) \land t(e_2) \]
\[ \psi_2 \overset{\text{def}}{=} (t(e_1) \land \text{emp}) \ast t(e_2) \]
\[ \psi_3 \overset{\text{def}}{=} t(e_1) \ast (t(e_2) \land \text{emp}) \]
\[ \psi_4 \overset{\text{def}}{=} (\phi_{\exists l} \land \neg \text{emp} \land t(e_1)) \ast (\phi_{\exists l} \land \neg \text{emp} \land \langle U \rangle(\text{Leaf} \land t(e_2))) \]

Modal separation logics
Hilbert-style axiomatisation for $\text{MSL}(\ast, \Diamond)$

[Demri & Fervari & Mansutti, JELIA’19]

- Designing internal calculi for separation-like logics is not an easy task. See Alessio’s talk.

- 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.

- As a by-product, we characterise the expressive power of $\text{MSL}(\ast, \Diamond)$. 
Method to axiomatise $\text{MSL}(\ast, \Diamond)$

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

- 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 $\text{MSL}(\ast, \Diamond)$.
Method to axiomatise \( \text{MSL}(\ast, \Diamond) \)

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

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

- Similarly, Boolean combinations of \( x = y, x \leftrightarrow y, \) \( \text{alloc}(x) \), and \( \text{size} \geq \beta \) capture quantifier-free \( \text{SL}(\ast, \neg \ast) \).
Core formulae

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

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

$$G := |Q,\ldots, Q\rangle \mid |Q,\ldots, Q\rangle \mid |Q,\ldots, \overline{Q},\ldots, Q\rangle,$$

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

Hilbert-style axiomatisation for MSL($\ast, \diamond$)
Core formulae

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

\[
\ell := T \mid \bot \mid p \mid \neg p \quad Q := \ell \mid Q \land Q
\]

\[
\mathcal{G} := |Q, \ldots, Q\rangle \mid |Q, \ldots, Q\rangle \mid |Q, \ldots, \overline{Q}, \ldots, Q\rangle,
\]

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

- The core formulae are logically equivalent to formulae in \( \text{MSL}(\ast, \Diamond) \).

Hilbert-style axiomatisation for \( \text{MSL}(\ast, \Diamond) \)
Axioms for Boolean combinations of core formulae

- Axioms dedicated to size formulae and inconsistencies:

\[
\begin{align*}
\text{size} & \geq 0 \quad \text{size} \geq \beta + 1 \Rightarrow \text{size} \geq \beta \\
|Q_1, \ldots, Q_n? & \Rightarrow \text{size} \geq \#(|Q_1, \ldots, Q_n?) \quad \neg|\ldots, Q^\perp, \ldots? 
\end{align*}
\]
Axioms for Boolean combinations of core formulae

- Axioms dedicated to size formulae and inconsistencies:

\[
\text{size} \geq 0 \quad \text{size} \geq \beta + 1 \Rightarrow \text{size} \geq \beta
\]

\[
|Q_1, \ldots, Q_n? \Rightarrow \text{size} \geq \#(|Q_1, \ldots, Q_n?) \quad \neg|\ldots, Q^\perp, \ldots?
\]

- Examples of axioms dedicated to conjunctions:

\[
|Q_1, \ldots, Q_i, \ldots, Q_n \rangle \land |Q'_1, \ldots, Q'_i, \ldots, Q'_n\rangle \iff |Q_1 \land Q'_1, \ldots, Q_i \land Q'_i, \ldots, Q_n \land Q'_n\rangle
\]

\[
|Q_1, \ldots, Q_n \rangle \land |Q'_1, \ldots, Q'_i, \ldots, Q'_m\rangle \iff |Q_1 \land Q'_1, \ldots, Q_n \land Q'_n, Q'_n+1, \ldots, Q'_i, \ldots, Q'_m\rangle
\]

\[n < i \leq m\]

- Axioms dedicated to negations are built on the same principle.
Axioms and rule to eliminate

- $\Diamond (\phi \lor \psi) \iff \Diamond (\phi) \lor \Diamond (\psi)$; $\Diamond (\{Q_1, \ldots, Q_n\}) \iff \top, Q_1, \ldots, Q_n$.

- $\Diamond (\phi \land S) \iff \Diamond (\phi) \land S$  
  
  $S$ is a size formula
Axioms and rule to eliminate

- $\Diamond(\phi \lor \psi) \iff \Diamond(\phi) \lor \Diamond(\psi)$; $\Diamond([Q_1, \ldots, Q_n]) \iff [\top, Q_1, \ldots, Q_n]$.

- $\Diamond(\phi \land S) \iff \Diamond(\phi) \land S$ \hspace{1cm} $S$ is a size formula

- $\Diamond([Q_1, \ldots, Q_n]) \iff [\top, Q_1, \ldots, Q_n] \lor [\top, Q_1, \ldots, Q_n]$.

- $\Diamond([\vec{Q}_i, \ldots, Q]) \iff [\top, Q_1, \ldots, \vec{Q}_i, \ldots, Q]$ \hspace{1cm} $i \geq 2$

- $\Diamond([\vec{Q}_1, \ldots, Q_{n-1}, Q]) \iff [\vec{Q}_n, Q_1, \ldots, Q_{n-1}] \lor [\top, \vec{Q}_1, \ldots, Q_{n-1}, Q]$.

- Regularity rule:

\[
\begin{align*}
\phi \Rightarrow \psi \\
\Diamond \phi \Rightarrow \Diamond \psi
\end{align*}
\]
Completeness

• + Axioms and rule to eliminate $\ast$ including some BI axioms.

• For all Boolean combinations of core formulae $\phi_1, \phi_2$,
  – there is a Boolean combination of core formulae $\psi$ such that $\Diamond \phi_1 \iff \psi$ is derivable;
  – there is a Boolean combination of core formulae $\psi$ such that $\phi_1 \ast \phi_2 \iff \psi$ is derivable.
Completeness

• + Axioms and rule to eliminate ∗ including some BI axioms.

• For all Boolean combinations of core formulae \( \phi_1, \phi_2, \)
  – there is a Boolean combination of core formulae \( \psi \) such that \( \Diamond \phi_1 \iff \psi \) is derivable;
  – there is a Boolean combination of core formulae \( \psi \) such that \( \phi_1 \ast \phi_2 \iff \psi \) is derivable.

• Completeness of the calculus with the additional axiom:

\[
p \iff (|p \lor p\rangle \lor \hat{p}).
\]

[Demri & Fervari & Mansutti, JELIA’19]

• Completeness proof: first reduce a formula to a Boolean combination of core formulae and prove completeness of the calculus for the restriction to Boolean combinations.
Concluding remarks

- Presentation of a specific (simple) way to combine (local) modalities and (global) separating connectives.
Concluding remarks

- Presentation of a specific (simple) way to combine (local) modalities and (global) separating connectives.

- Related work:
  - On-going work on modal logics with composition on finite trees. With B. Bednarczyk, R. Fervari and A. Mansutti. \textsc{Tower}-hardness of MSL(\texttt{\star}, \texttt{\bigcirc}^{-1}).
  
  - Label-free proof systems for separation logics. See Alessio’s talk \cite{Demri & Lozes & Mansutti, CSL’20}
Concluding remarks

• Presentation of a specific (simple) way to combine (local) modalities and (global) separating connectives.

• Related work:
  – On-going work on modal logics with composition on finite trees. With B. Bednarczyk, R. Fervari and A. Mansutti. \textsc{Tower}-hardness of MSL(\(*, \Diamond^{-1}\)).
  – Label-free proof systems for separation logics. See Alessio’s talk [Demri & Lozes & Mansutti, CSL’20]

• Open question: modal separation logics of elementary complexity between MSL(\(*, \Diamond\) \cup MSL(\(*, \langle \neq \rangle\)) and MSL(\(*, \Diamond, \langle \neq \rangle\))?