A Framework for Modalities and Separating Connectives

Stéphane Demri

CNRS, France

Imperial College

April 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]
  - logic with separating modalities LSM [Courtauld & Galmiche & Pym, TCS 2016]
  - modal separation logic DMBI [Courtauld & 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 Bentem, 2002]
  • relation-changing modal logics
    [Fervari, PhD 2014]
  • 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, Book 2013]

• This work: combining separation logics with modal logics, relationships with quantified CTL, and Hilbert-style axiomatisation.
Floyd-Hoare logic

- Hoare triple: $\{\phi\} \ 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: $\{\phi\} \ C \ \{\psi\}$ [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:

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

  $\{\phi\} \ C \ \{\psi'\}$

• Hoare’s assignment axiom:

  $\{\phi[e/x]\} \ x \leftarrow \ e \ \{\phi\}$
Frame rule and separating conjunction

- Frame rule:

\[
\begin{array}{c}
\{\phi\} \; C \; \{\psi\} \\
\{\phi * \psi'\} \; C \; \{\psi * \psi'\}
\end{array}
\]

where \( C \) does not mess with \( \psi' \).

- \( (s, h) \models x \leftarrow 5 \leftarrow 4 \) 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 $\text{Loc} \subseteq \text{Val}$. 

Separation logic(s) in a nutshell
Memory states with one record field

• Program variables $PVAR = \{x_1, x_2, x_3, \ldots\}$.

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

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

Separation logic(s) in a nutshell
Graphical representation

\[ x \rightarrow s(x) = l_1 \]
\[ y \rightarrow s(y) = l_3 \]
\[ \text{dom}(h) = \{l_1, l_2, l_3\} \]
\[ h(l_1) = l_2 \]
\[ h(l_2) = l_3 \]
\[ h(l_3) = l_4 \]
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 \( h_1 \uplus h_2 \).
The models are forest-like structures

- A forest of tree-like structures:
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 logics.

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

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

By-products:
- 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]
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.

\((1s(x, y) \land T)\) vs. \(\Diamond_x EF y\)

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

- Related work: description logics for shape analysis.
  See e.g. \[\text{[Georgieva & Maier, SEFM'05; Calvanese et al., IFM'14]}\]
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 universe and a finite relation encoding the heap.
Semantics

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

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

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

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

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

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

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

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

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

\[ k \text{ times} \]
**Examples**

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

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

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

\[ \langle U \rangle \phi \overset{\text{def}}{=} \phi \lor \langle \neq \rangle \phi \quad \text{size} \geq k \overset{\text{def}}{=} \overbrace{\neg \text{emp} \ast \cdots \ast \neg \text{emp}}^{k \text{ times}} \]

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

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

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

\[
\begin{align*}
\text{size} \geq 2 & \land \neg \text{size} \geq 3 & \land \Diamond \Diamond \Diamond \top \land \\
\neg (\neg \text{emp} \ast \Diamond \Diamond \Diamond \top) & \land \neg \Diamond (\neg \text{emp} \ast \Diamond \Diamond \Diamond \top)
\end{align*}
\]

(in MSL(*, \Diamond), but not expressible in Alt_1/prop. SL(*, \neg *))
Relationships with prop. separation logic $SL(\star)$

- Formulae:

\[ \phi ::= x = y \mid x \leftrightarrow y \mid \text{emp} \mid \neg \phi \mid \phi \land \phi \mid \phi \ast \phi \]
Relationships with prop. separation logic $SL(\ast)$

- **Formulae:**
  \[
  \phi ::= x = y \mid x \leftrightarrow y \mid \text{emp} \mid \neg \phi \mid \phi \land \phi \mid \phi \ast \phi
  \]

- **Satisfaction relation:**
  \[
  (s, h) \models x = y \quad \overset{\text{def}}{\iff} \quad s(x) = s(y)
  \]
  \[
  (s, h) \models \text{emp} \quad \overset{\text{def}}{\iff} \quad \text{dom}(h) = \emptyset
  \]
  \[
  (s, h) \models x \leftrightarrow y \quad \overset{\text{def}}{\iff} \quad s(x) \in \text{dom}(h) \text{ and } h(s(x)) = s(y)
  \]
  \[
  (s, h) \models \phi_1 \ast \phi_2 \quad \overset{\text{def}}{\iff} \quad \text{there are } h_1 \text{ and } h_2 \text{ s.t. } h_1 \uplus h_2 = h, \quad (s, h_1) \models \phi_1 \text{ and } (s, h_2) \models \phi_2
  \]
Relationships with prop. separation logic $SL(\ast)$

- Formulae:
  \[
  \phi ::= x = y \mid x \leftrightarrow y \mid \text{emp} \mid \neg \phi \mid \phi \land \phi \mid \phi \ast \phi
  \]

- Satisfaction relation:
  \[
  (s, h) \models x = y \overset{\text{def}}{\iff} s(x) = s(y) \\
  (s, h) \models \text{emp} \overset{\text{def}}{\iff} \text{dom}(h) = \emptyset \\
  (s, h) \models x \leftrightarrow y \overset{\text{def}}{\iff} s(x) \in \text{dom}(h) \text{ and } h(s(x)) = s(y) \\
  (s, h) \models \phi_1 \ast \phi_2 \overset{\text{def}}{\iff} \text{there are } h_1 \text{ and } h_2 \text{ s.t. } h_1 \uplus h_2 = h, (s, h_1) \models \phi_1 \text{ and } (s, h_2) \models \phi_2
  \]

- Encoding $SL(\ast)$ into $MSL(\ast, \Diamond, \langle \neq \rangle)$:
  \[
  x = y \approx \langle U \rangle(x \land y) \quad x \leftrightarrow y \approx \langle U \rangle(x \land \Diamond y)
  \]
  (assuming that $x$ and $y$ are nominals in $MSL(\ast, \Diamond, \langle \neq \rangle)$)
Tower upper bound for $\text{SAT}(\text{MSL}(\star, \Diamond, \langle \neq \rangle))$

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

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

  - Internalisation of the semantics for $\text{MSL}^f(\ast, \Diamond, \langle \neq \rangle)$. 

Modal separation logics
Tower-hardness

- Linear model:

- There is a formula $\phi_{\exists 1s}$ in $\text{MSL} (\ast, \Diamond, \langle \neq \rangle)$ such that $\mathcal{M} \models \phi_{\exists 1s}$ iff $\mathcal{M}$ is linear.
Tower-hardness

• Linear model:

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

• There is a formula \( \phi_{\exists 1s} \) in MSL(\(*, \Diamond, \langle \neq \rangle\)) such that \( M \models \phi_{\exists 1s} \) iff \( M \) 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.

\[ a_1 \ a_2 \ a_1 \]
Tower-hardness

- Linear model:

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

- There is a formula \( \phi_{\exists l_s} \) in \( \text{MSL}(\ast, \Diamond, \langle \neq \rangle) \) such that \( M \models \phi_{\exists l_s} \) iff \( M \) is linear.

- Star-free expressions

  \[
  e ::= a \mid \varepsilon \mid e \cup e \mid ee \mid \sim e
  \]

- Nonemptiness problem is \( \text{TOWER} \)-complete.
  
  [Meyer & Stockmeyer, STOC’73; Schmitz, ToCT 2016]

- Encoding words by linear models.

- \( \text{MSL}(\ast, \Diamond, \langle \neq \rangle) \) satisfiability problem is \( \text{TOWER} \)-hard.

  [Demri & Fervari, AiML’18]
Variants

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

[Demri & Fervari, AiML’18]
Variants

- Other results.
  1. The satisfiability problems for $\text{MSL}(\ast, \diamond)$ and $\text{MSL}(\ast, \langle \neq \rangle)$ are $\text{NP}$-complete. (for $\text{SL}(\ast)$, $\text{PSPACE}$-completeness)
  2. Undecidability of $\text{MSL}(\ast, \diamond, \langle \neq \rangle) + \text{magic wand} \not\rightarrow$.
     [Demri & Fervari, AiML’18]
  3. Modal logic for heaps $\text{MLH}(\ast)$ is $\text{TOWER}$-complete.
     [Demri & Deters, TOCL 2015]
Variants

• Other results.

1. The satisfiability problems for $\text{MSL}(\ast, \lozenge)$ and $\text{MSL}(\ast, \langle \neq \rangle)$ are $\text{NP}$-complete. (for $\text{SL}(\ast)$, $\text{PSPACE}$-completeness)

2. Undecidability of $\text{MSL}(\ast, \lozenge, \langle \neq \rangle) + \text{magic wand } \ast$.  

[Demri & Fervari, AiML’18]

3. Modal logic for heaps $\text{MLH}(\ast)$ is $\text{TOWER}$-complete. 

[Demri & Deters, TOCL 2015]

• Adding the converse modality.

- $\mathcal{M}, l \models \lozenge^{-1}\phi \iff \mathcal{M}, l' \models \phi$, for some $l' \in \mathbb{N}$ s.t. $(l', l) \in R$.

- Satisfiability problem for $\text{MSL}(\ast, \lozenge, \lozenge^{-1}, \langle \neq \rangle)$ in $\text{TOWER}$. 

Modal separation logics
Structures for interpreting $\text{MSL}(\ast, \Diamond^{-1})$ in $\text{MSL}(\ast, \Diamond)$

Modal separation logics
Separating conjunction is strongly related to second-order quantification over propositions.
Structures for interpreting $\text{MSL}(\ast, \lozenge^{-1})$ in $\text{MSL}(\ast, \lozenge)$

- Separating conjunction is strongly related to second-order quantification over propositions.
QCTL$^t$: QCTL under the tree semantics

[Laroussinie & Markey, LMCS 2014]

\[
\phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \text{EX}\phi \mid \exists p \ \phi \quad (\Diamond \approx \text{EX}) \\
\mid E(\phi U \phi) \mid A(\phi U \phi)
\]

- Models are total Kripke structures $\mathcal{K} = (W, R, I)$.
- $\mathcal{K}, w \models \exists p \ \phi$ iff there is $\mathcal{K}'$ s.t. $\mathcal{K} \simeq_{\text{AP}\{p\}} \mathcal{K}'$ & $\mathcal{K}', w \models \phi$. 
**QCTL\(^t\): QCTL under the tree semantics**

[Laroussinie & Markey, LMCS 2014]

\[\phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \text{EX}\phi \mid \exists p \phi \quad (\Diamond \equiv \text{EX})\]

\[\mid \text{E}(\phi U \phi) \mid \text{A}(\phi U \phi)\]

- Models are total Kripke structures \(\mathcal{K} = (W, R, I)\).

- \(\mathcal{K}, w \models \exists p \phi\) iff there is \(\mathcal{K}'\) s.t. \(\mathcal{K} \equiv_{\text{AP}\{p\}} \mathcal{K}' \) & \(\mathcal{K}', w \models \phi\).

- Satisfiability problem for QCTL\(^s\) (structure semantics):
  - **input:** a quantified CTL formula \(\phi\).
  - **output:** 1 iff there is a finite total Kripke structure satisfying \(\phi\).
Tree semantics

• Satisfiability problem for QCTL\(_t\) (tree semantics):

  **input:** a quantified CTL formula \(\phi\).
  **output:** 1 iff there is a finite total Kripke structure whose tree unfolding satisfies \(\phi\).
  (\(\approx\) finite-branching trees with infinite branches)

\[
|\models t \exists p. \varphi \iff |\models \varphi
\]
Tree semantics

- Satisfiability problem for $\text{QCTL}^t$ (tree semantics):
  - **input:** a quantified CTL formula $\phi$.
  - **output:** 1 iff there is a finite total Kripke structure whose tree unfolding satisfies $\phi$.

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

\[ \models_t \exists p. \varphi \iff \models \varphi \]

- $\text{SAT}(\text{QCTL}^t)$ is $\text{TOWER}$-complete.
- $\text{SAT}(\text{QCTL}^s)$ is undecidable.

[Laoussinie & 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]

- $\text{QCTL}^t_X$: $\text{QCTL}^t$ restriction to $\text{EX}$.
  $\text{QCTL}^{ft}_X$, $\text{QCTL}^{ft}_{XF}$: finite tree semantics.
Other results and fragments

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

• QCTL$^t_X$: QCTL$^t$ restriction to EX.
  QCTL$^{ft}_X$, QCTL$^{ft}_{X_F}$: finite tree semantics.

• What about SAT(QCTL$^t_X$) and SAT(QCTL$^{ft}_X$)?
How to prove Tower-hardness

• Uniform elementary reduction from $k$-NEXPTIME-complete tiling problems $\text{Tiling}_k$.

• $t(0, n) = n$ and $t(k + 1, n) = 2^{t(k, n)}$.

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

  **output:** 1 iff the grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$ can be tiled (with usual constraints)?
High-level description of the reduction from $\text{Tiling}_k$

- Grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$ as a tree model:
  - The root $\varepsilon$ has $t(k + 1, n)$ children.
  - $t(k, n)$ children of $\varepsilon$ are distinguished and receive a number in $[0, t(k, n) - 1]$. 
High-level description of the reduction from $Tiling_k$

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

![Diagram](image-url)

Encoding of the grid $[0, t(k, n) - 1] \times [0, t(k, n) - 1]$
Enforcing $t(k, n)$ children

Type $k$

$nb = t(k + 1, n) - 1$

Type $(k-1)$

$val = \top, nb = 0$

Type $(k-2)$

$val = \bot

$nb = 0$

-val = \bot

$nb = t(k - 1, n) - 1$

Type 0

$nb = 1$

$p_{n-1} = \ldots = p_1 = \bot, p_0 = \top$

QCTL$^*$ Quantified CTL under the tree semantics
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 $[0, t(k, n) - 1]$.

- If a child has number $m < t(k, n) - 1$, then there is a sibling with number equal to $m + 1$. 

QCTL$^t$: Quantified CTL under the tree semantics
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 $[0, t(k, n) - 1]$.

- If a child has number $m < t(k, n) - 1$, then there is a sibling with number equal to $m + 1$.

\[
\text{type}(k) \overset{\text{def}}{=} \text{AX}(\text{type}(k - 1)) \land \text{EX}(\text{first}(k - 1)) \land \text{uniq}(k) \land \text{compl}(k).
\]
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 $[0, t(k, n) - 1]$.

- If a child has number $m < t(k, n) - 1$, then there is a sibling with number equal to $m + 1$.

\[
type(k) \overset{\text{def}}{=} AX(type(k-1)) \land EX(first(k-1)) \land uniq(k) \land compl(k).
\]

- \text{SAT}(\text{QCTL}_{tX}) \text{ is Tower-complete} [\text{Bednarczyk \\ & Demri, LICS’19}]
  
  (many developments are omitted here)
Hilbert-style axiomatisation of $\text{MSL}(\ast, \lozenge)$

- 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]

- Puristic approach: only formulae in $\text{MSL}(\ast, \lozenge)$ are used.

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

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

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

- Boolean combination of core formulae capture $\text{MSL}(\ast, \diamondsuit)$. 
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 combination of core formulae capture $\text{MSL}(\ast, \Diamond)$.

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

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

\[
\ell := \top | \bot | p | \neg p \quad Q := \ell | Q \land Q
\]

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

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

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

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

$$\mathcal{G} := \langle Q, \ldots, Q \rangle \mid \langle Q, \ldots, Q \rangle \mid \langle Q, \ldots, \bar{Q}, \ldots, Q \rangle,$$

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

- $|Q_1, \ldots, Q_n\rangle$:
  ![Diagram 1](image1.png)

- $[Q_1, \ldots, Q_n]$:
  ![Diagram 2](image2.png)

- $[Q_1, \ldots, \bar{Q}_i, \ldots, Q_n]$:
  ![Diagram 3](image3.png)

• The core formulae are logically equivalent to formulae in MSL($\ast, \diamond$).
Axioms for Boolean combinations of core formulae

- Axioms dedicated to size formulae and inconsistencies:

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

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

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

\[
|Q_1,\ldots, Q_n| \land |Q'_1,\ldots, Q'_i,\ldots, Q'_m| \Leftrightarrow |Q_1 \land Q'_1,\ldots, Q_n \land Q'_n, Q'_{n+1}, \ldots, \hat{Q}_i, \ldots, Q'_m|
\]

\[
n < i \leq m
\]

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

- ♣(φ ∨ ψ) ⇔ ♣(φ) ∨ ♣(ψ); ♣([Q₁,..., Qₙ]) ⇔ [T, Q₁,..., Qₙ].

- ♣(φ ∧ S) ⇔ ♣(φ) ∧ S \quad S \text{ is a size formula}
Axioms and rule to eliminate ♦

• ♦(φ ∨ ψ) ⇔ ♦(φ) ∨ ♦(ψ); ♦(|Q_1,...,Q_n|) ⇔ |T, Q_1,..., Q_n|.

• ♦(φ ∧ S) ⇔ ♦(φ) ∧ S

  \(S\) is a size formula

• ♦(|Q_1,\ldots,Q_n\rangle) ⇔ |\overline{T}, Q_1,..., Q_n| ∨ |T, Q_1,..., Q_n\rangle.

• ♦(|Q_1,...,\overline{Q_i},..., Q_n|) ⇔ |\overline{T}, Q_1,...,\overline{Q_i},..., Q_n| \quad i \geq 2

• ♦(|\overline{Q}_1,..., Q_{n-1}, Q_n|) ⇔ |\overline{Q}_n, Q_1,..., Q_{n-1}| ∨ |T, \overline{Q}_1,..., Q_{n-1}, Q_n|.

• Regularity rule:

\[
\frac{\phi \Rightarrow \psi}{\diamond \phi \Rightarrow \diamond \psi}
\]

Hilbert-style axiomatisation for MSL(\(*, \diamond\))

29
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.

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.
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:

$$p \iff (|p\rangle \lor |\overline{p}\rangle) \lor \overline{|p\rangle}.$$  

[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

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

- See also relationships with ambient logic on trees.
  
  [Calcagno et al., TLDI’03; Calcagno et al., POPL’05]
Concluding remarks

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

• 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 MSL(∗, ◇−1), MSL(∗, ◇−1, ◇) or MSL(∗, ◇−1, ⟨≠⟩).
  – Expressive power of modal logics on trees with separating connectives.
    With B. Bednarczyk, R. Fervari and A. Mansutti.