Axiomatising Logics with Separating Conjunction and Modalities

Jelia'19

Stéphane Demri[1], Raul Fervari[2], **Alessio Mansutti**[1]

[1]LSV, CNRS, ENS Paris-Saclay, France

[2]CONICET, Universidad Nacional de Córdoba, Argentina

The fascinating realm of model-updating logics

- Logic of bunched implication [O'Hearn, Pym – BSL'99]
- Separation logic [Reynolds – LICS'02]
- Logics of public announcement [Lutz – AAMAS'06]
- Sabotage modal logics [Aucher et al. – M4M'07]
- One agent refinement modal logic [Bozzelli et al. – JELIA'12]
- **Modal Separation Logics** (`MSL`) [Demri, Fervari – AIML'18]
- `MSL` for resource dynamics [Courtault, Galmiche – JLC'18]

Hilbert-style axiomatisation for model-updating logics

- Designing internal calculi for model-updating logics is not easy.
- Usually, external features are introduced in order to define sound and complete calculi:
  - nominals (e.g. Hybrid SL) [Brotherston, Villard – POPL'14]
  - labels (e.g. bunched implication) [Docherty, Pym – FOSSACS'18]

In this work: we use a "general" approach to define Hilbert-style axiom systems for `MSL`.

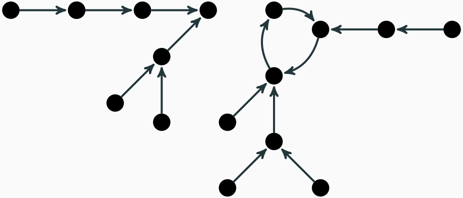
$\Rightarrow$ All axioms and rules involve only formulae from the target logic.

Modal separation logics

Models $\mathfrak{M} = (\mathfrak{U}, \mathfrak{R}, \mathfrak{V})$:

- $\mathfrak{U}$ infinite and countable,
- $\mathfrak{R} \subseteq \mathfrak{U} \times \mathfrak{U}$ is finite and weakly functional (deterministic),
- $\mathfrak{V} : \mathrm{PROP} \to \mathcal{P}(\mathfrak{U})$.

i.e. same models of the modal logic $\mathtt{Alt}_1$.



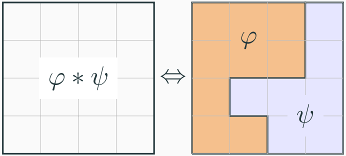
Disjoint union $\mathfrak{M}_1 + \mathfrak{M}_2 =$ union of the accessibility relations.
It is defined iff the relation we obtain is still functional.

Modal separation logics $\mathtt{MSL}(*, \Diamond, \langle\neq\rangle)$

$$\varphi ::= \overbrace{p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \langle\neq\rangle\varphi}^{\text{modal logic of inequality [de Rijke, JSL'92]}} \mid \overbrace{\mathtt{emp} \mid \varphi * \varphi}^{\text{separation logic}}$$

Interpreted on pointed models: $\mathfrak{M} = (\mathfrak{U}, \mathfrak{R}, \mathfrak{V})$ and $\mathfrak{w} \in \mathfrak{U}$.

- $\mathfrak{M}, \mathfrak{w} \models \langle\neq\rangle\varphi$ iff there is $\mathfrak{w}' \in \mathfrak{U} \setminus \{\mathfrak{w}\}$: $\mathfrak{M}, \mathfrak{w}' \models \varphi$.
- $\mathfrak{M}, \mathfrak{w} \models \mathtt{emp}$ iff $\mathfrak{R} = \emptyset$.
- $\mathfrak{M}, \mathfrak{w} \models \varphi * \psi$ iff $\mathfrak{M}_1, \mathfrak{w} \models \varphi$, $\mathfrak{M}_2, \mathfrak{w} \models \psi$ for some $\mathfrak{M}_1 + \mathfrak{M}_2 = \mathfrak{M}$.



What can $\mathtt{MSL}(*, \Diamond, \langle\neq\rangle)$ do?

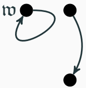
$\mathtt{MSL}(*, \Diamond)$, i.e. $\mathtt{MSL}(*, \Diamond, \langle\neq\rangle)$ without $\langle\neq\rangle$, is more expressive than $\mathtt{Alt}_1$:

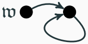
- The cardinality of $\mathfrak{R}$ is at least β:

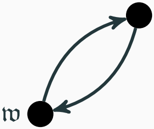
$$\mathtt{size} \geq \beta \stackrel{\textsf{def}}{=} \underbrace{\neg\mathtt{emp} * \cdots * \neg\mathtt{emp}}_{\beta\ \text{times}}$$

- The model is a loop of length 2 visiting the current world $\mathfrak{w}$:

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

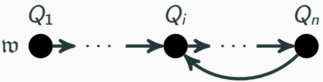






What do we know about $\mathtt{MSL}$?

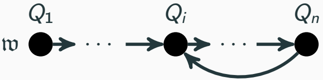
- $\mathrm{SAT}(\mathtt{MSL}(*, \Diamond, \langle \neq \rangle))$ is $\mathtt{Tower}$-complete.
- $\mathrm{SAT}(\mathtt{MSL}(*, \Diamond))$ and $\mathrm{SAT}(\mathtt{MSL}(*, \langle \neq \rangle))$ are $\mathtt{NP}$-complete.
  - proofs are done by defining model abstractions
  - E.g. for $\mathtt{MSL}(*, \Diamond)$, $\quad (Q_i \subseteq \mathrm{PROP})$



$+$ bound on $\mathrm{card}(\mathfrak{R})$

What do we know about MSL?

- SAT(MSL($*, \Diamond, \langle\neq\rangle$)) is Tower-complete.
- SAT(MSL($*, \Diamond$)) and SAT(MSL($*, \langle\neq\rangle$)) are NP-complete.
  - proofs are done by defining model abstractions
  - E.g. for MSL($*, \Diamond$), $(Q_i \subseteq \mathrm{PROP})$



\+ bound on $\mathrm{card}(\mathfrak{R})$

- The equivalence relation $\approx$ induced by this abstraction characterises the indistinguishability relation of MSL($*, \Diamond$).

Can we use this for axiomatisation?

Core formulae for $\texttt{MSL}(*, \Diamond)$

- From the indistinguishability relation $\approx$, define a set of *core formulae* capturing the equivalence classes of $\approx$.

Theorem (A Gaifman locality result for $\texttt{MSL}(*, \Diamond)$)

Every formula of $\texttt{MSL}(*, \Diamond)$ *is logically equivalent to a Boolean combination of core formulae.*

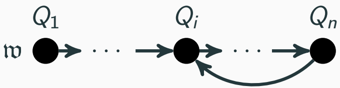
Core formulae for $\mathtt{MSL}(*, \Diamond)$

- From the indistinguishability relation $\approx$, define a set of *core formulae* capturing the equivalence classes of $\approx$.

Theorem (A Gaifman locality result for $\mathtt{MSL}(*, \Diamond)$)

Every formula of $\mathtt{MSL}(*, \Diamond)$ is logically equivalent to a Boolean combination of core formulae.

- Core formulae: Size formulae $\mathtt{size} \geq \beta$ and *graph formulae*, e.g. a formula of $\mathtt{MSL}(*, \Diamond)$ that characterises



- **Important:** The core formulae are all formulae from $\mathtt{MSL}(*, \Diamond)$.

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

The proof system is made of three parts:

1. Axioms and rules from propositional calculus;
2. Axioms for Boolean combinations of core formulae (**Bool**($\mathtt{Core}$));
3. Axioms and rules to transform every formula into a Boolean combination of core formulae.
   - Require for every φ, ψ in **Bool**($\mathtt{Core}$) to exhibit formulae in **Bool**($\mathtt{Core}$) that are equivalent to $\varphi * \psi$ and $\Diamond\varphi$.
   - Replay syntactically the proof of Gaifman locality for $\mathtt{MSL}(*, \Diamond)$.

(Similar to *reduction axioms* used in Dynamic epistemic logic)

Eliminating modalities & reasoning on core formulae

Elimination of modalities

$\vdash_{\texttt{elim}} \psi_1 * \psi_2 \Leftrightarrow \psi_3$

$\vdash_{\texttt{elim}} \Diamond\psi_4 \Leftrightarrow \psi_5$

Completeness for core formulae

$$\frac{\vdash_{\texttt{elim}} \varphi \Leftrightarrow \psi \qquad\qquad \vdash_{\texttt{core}} \psi}{\vdash \varphi}$$

where φ in $\texttt{MSL}(*, \Diamond)$, and ψ_i, ψ are in $\textbf{Bool}(\texttt{Core})$.

Concluding remarks

- Hilbert-style axiomatisation of $\mathtt{MSL}(*, \Diamond)$ and $\mathtt{MSL}(*, \langle \neq \rangle)$.
- Axiomatisations derived from the abstractions used for complexity.
- Reusable method in practice: now used to axiomatise propositional $\mathtt{SL}$ and a guarded fragment of $\mathtt{FOSL}$. [Demri, Lozes, M. – sub.]

Possible continuations:

- Axiomatisation of $\mathtt{MSL}(*, \Diamond, \langle \neq \rangle)$.
- Calculi with optimal complexities.
  - tableaux calculi for $\mathtt{MSL}(*, \Diamond)$. [Fervari, Saravia – ongoing]