Assertion-consistency lattices

Michael Huth
Computing
Imperial College London

and

Shekhar Pradhan
Philosophy
Central Missouri State University

Outline

1. Motivation

Outline

1. Motivation
2. Under-specified models

Outline

1. Motivation

2. Under-specified models

3. Assertion-consistency lattices

Outline

1. Motivation
2. Under-specified models
3. Assertion-consistency lattices
4. De Morgan lattices

Outline

1. Motivation
2. Under-specified models
3. Assertion-consistency lattices
4. De Morgan lattices
5. Multiple-valued modal logic

Outline

1. Motivation
2. Under-specified models
3. Assertion-consistency lattices
4. De Morgan lattices
5. Multiple-valued modal logic
6. Multiple-valued abstraction

Outline

1. Motivation
2. Under-specified models
3. Assertion-consistency lattices
4. De Morgan lattices
5. Multiple-valued modal logic
6. Multiple-valued abstraction
7. Conclusions.

Motivation

Distributed systems/agents need to store and share incomplete information in a fault-tolerant manner.

Examples are

Motivation

Distributed systems/agents need to store and share incomplete information in a fault-tolerant manner.

Examples are

- “group membership” and “fault detection” as components of fault-tolerant distributed systems;

Motivation

Distributed systems/agents need to store and share incomplete information in a fault-tolerant manner.

Examples are

- "group membership" and "fault detection" as components of fault-tolerant distributed systems;
- software engineering requirements derived from multiple stakeholders in a design; and an

Motivation

Distributed systems/agents need to store and share incomplete information in a fault-tolerant manner.

Examples are

- "group membership" and "fault detection" as components of fault-tolerant distributed systems;
- software engineering requirements derived from multiple stakeholders in a design; and an
- intelligent agents' architecture.

Motivation

Distributed systems/agents need to store and share incomplete information in a fault-tolerant manner.

Examples are

- “group membership” and “fault detection” as components of fault-tolerant distributed systems;
- software engineering requirements derived from multiple stakeholders in a design; and an
- intelligent agents’ architecture.

In the presence of inconsistencies, we wish to retain *standard* logical reasoning principles as much as possible.

Under-specified models

```
sig Class {  -- in D. Jacksons Alloy [Jackson00]
 pub, priv : set Method,
 field : set Field }
sig Object {
 type : Class,
 method : set Method,
 field : set Field }
fact { all o : Object | o.method = o.type.(pub + priv) }
fun Scenario(o1, o2 : Object) {  -- consistency check
 some o1.method && o1.type != o2.type }
assert Safety{  -- validity check
 all o:Object | no o.method & o.type.pub & o.type.priv }
```

Under-specified models

```
sig Class {  -- in D. Jacksons Alloy [Jackson00]
 pub, priv : set Method,
 field : set Field }
sig Object {
 type : Class,
 method : set Method,
 field : set Field }
fact { all o : Object | o.method = o.type.(pub + priv) }
fun Scenario(o1, o2 : Object) {  -- consistency check
 some o1.method && o1.type != o2.type }
assert Safety{  -- validity check
 all o:Object | no o.method & o.type.pub & o.type.priv }
```

Queries are valid (true), inconsistent (false) or neither ($\perp$).

Assertion-consistency lattices

A (complete) *AC-lattice* is a tuple $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}}, \mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$, where $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ and $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ are partial orders that induce (complete) lattices, and $\neg_{\mathrm{a}} : \mathcal{L}_{\mathrm{a}} \to \mathcal{L}_{\mathrm{c}}$ and $\neg_{\mathrm{c}} : \mathcal{L}_{\mathrm{c}} \to \mathcal{L}_{\mathrm{a}}$ are functions that meet the axioms of Figure 1 (left).

$$
\begin{array}{ll}
\neg_{\mathrm{a}}\neg_{\mathrm{c}}\phi = \phi & \neg\neg\phi = \phi \\
\neg_{\mathrm{c}}\neg_{\mathrm{a}}\phi = \phi & \neg(\phi \wedge \psi) = \neg\phi \vee \neg\psi \\
\phi \leq_{\mathrm{a}} \psi \Rightarrow \neg_{\mathrm{a}}\psi \leq_{\mathrm{c}} \neg_{\mathrm{a}}\phi & \neg(\phi \vee \psi) = \neg\phi \wedge \neg\psi \\
\phi \leq_{\mathrm{c}} \psi \Rightarrow \neg_{\mathrm{c}}\psi \leq_{\mathrm{a}} \neg_{\mathrm{c}}\phi & \phi \leq \psi = \neg\psi \leq \neg\phi.
\end{array}
$$

Figure 1: Axioms for AC-lattices (left) and De Morgan lattices [2] (right).

Example from model theory

Given a class of models $\mathbf{C}$, a countable set of queries $\mathcal{L}$, and assertion and consistency checks $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ (respectively).

Example from model theory

Given a class of models $\mathbf{C}$, a countable set of queries $\mathcal{L}$, and assertion and consistency checks $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ (respectively).

- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, define $\phi \leq_{\mathrm{m}} \psi$ iff for all models $\mathcal{M} \in \mathbf{C}$, $\mathcal{M} \models^{\mathrm{m}} \phi$ implies $\mathcal{M} \models^{\mathrm{m}} \psi$.

Example from model theory

Given a class of models $\mathbf{C}$, a countable set of queries $\mathcal{L}$, and assertion and consistency checks $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ (respectively).

- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, define $\phi \leq_{\mathrm{m}} \psi$ iff for all models $\mathcal{M} \in \mathbf{C}$, $\mathcal{M} \models^{\mathrm{m}} \phi$ implies $\mathcal{M} \models^{\mathrm{m}} \psi$.
- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the definitions $[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\psi \in \mathcal{L} \mid \psi \leq_{\mathrm{m}} \phi,\ \phi \leq_{\mathrm{m}} \psi\}$ and $\neg_{\mathrm{m}}[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} [\neg\phi]_{\neg\mathrm{m}}$ determine countable sets $\mathcal{L}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{[\phi]_{\mathrm{m}} \mid \phi \in \mathcal{L}\}$ and functions $\neg_{\mathrm{m}} : \mathcal{L}_{\mathrm{m}} \to \mathcal{L}_{\neg\mathrm{m}}$.

Example from model theory

Given a class of models $\mathbf{C}$, a countable set of queries $\mathcal{L}$, and assertion and consistency checks $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ (respectively).

- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, define $\phi \leq_{\mathrm{m}} \psi$ iff for all models $\mathcal{M} \in \mathbf{C}$, $\mathcal{M} \models^{\mathrm{m}} \phi$ implies $\mathcal{M} \models^{\mathrm{m}} \psi$.
- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the definitions $[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\psi \in \mathcal{L} \mid \psi \leq_{\mathrm{m}} \phi,\ \phi \leq_{\mathrm{m}} \psi\}$ and $\neg_{\mathrm{m}}[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} [\neg\phi]_{\neg\mathrm{m}}$ determine countable sets $\mathcal{L}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{[\phi]_{\mathrm{m}} \mid \phi \in \mathcal{L}\}$ and functions $\neg_{\mathrm{m}} : \mathcal{L}_{\mathrm{m}} \to \mathcal{L}_{\neg\mathrm{m}}$.
- We set $[\phi]_{\mathrm{m}} \leq_{\mathrm{m}} [\psi]_{\mathrm{m}}$ iff there are $\phi' \in [\phi]_{\mathrm{m}}$ and $\psi' \in [\psi]_{\mathrm{m}}$ such that $\phi' \leq_{\mathrm{m}} \psi'$.

Example from model theory

Given a class of models $\mathbf{C}$, a countable set of queries $\mathcal{L}$, and assertion and consistency checks $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$ (respectively).

- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, define $\phi \leq_{\mathrm{m}} \psi$ iff for all models $\mathcal{M} \in \mathbf{C}$, $\mathcal{M} \models^{\mathrm{m}} \phi$ implies $\mathcal{M} \models^{\mathrm{m}} \psi$.
- For $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the definitions $[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\psi \in \mathcal{L} \mid \psi \leq_{\mathrm{m}} \phi,\ \phi \leq_{\mathrm{m}} \psi\}$ and $\neg_{\mathrm{m}}[\phi]_{\mathrm{m}} \stackrel{\mathrm{def}}{=} [\neg\phi]_{\neg\mathrm{m}}$ determine countable sets $\mathcal{L}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{[\phi]_{\mathrm{m}} \mid \phi \in \mathcal{L}\}$ and functions $\neg_{\mathrm{m}} : \mathcal{L}_{\mathrm{m}} \to \mathcal{L}_{\neg\mathrm{m}}$.
- We set $[\phi]_{\mathrm{m}} \leq_{\mathrm{m}} [\psi]_{\mathrm{m}}$ iff there are $\phi' \in [\phi]_{\mathrm{m}}$ and $\psi' \in [\psi]_{\mathrm{m}}$ such that $\phi' \leq_{\mathrm{m}} \psi'$.

These data specify a countable AC-lattice.

Example from topology

Let $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ be the complete lattice of closed subsets of a topological space X, ordered by inclusion $(\leq_{\mathrm{a}})$.

Example from topology

Let $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ be the complete lattice of closed subsets of a topological space X, ordered by inclusion $(\leq_{\mathrm{a}})$.

Dually, let $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ be the complete lattice of open subsets of X, ordered by inclusion $(\leq_{\mathrm{c}})$. This gives rise to an AC-lattice, where the negations are set complementation.

Example from topology

Let $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ be the complete lattice of closed subsets of a topological space X, ordered by inclusion $(\leq_{\mathrm{a}})$.

Dually, let $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ be the complete lattice of open subsets of X, ordered by inclusion $(\leq_{\mathrm{c}})$. This gives rise to an AC-lattice, where the negations are set complementation.

Special case of interest: X a finite partial order in the Alexandroff topology.

Example from topology

Let $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ be the complete lattice of closed subsets of a topological space X, ordered by inclusion ($\leq_{\mathrm{a}}$).

Dually, let $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ be the complete lattice of open subsets of X, ordered by inclusion ($\leq_{\mathrm{c}}$). This gives rise to an AC-lattice, where the negations are set complementation.

Special case of interest: X a finite partial order in the Alexandroff topology.

Representation theory for AC-lattices?

Finite distributive AC-lattices

For any preorder $(V, \leq)$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \setminus_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \setminus_{\mathrm{c}})$ is an AC-lattice.

Finite distributive AC-lattices

For any preorder $(V, \leq)$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \setminus_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \setminus_{\mathrm{c}})$ is an AC-lattice.

Conversely, every AC-lattice $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}}, \mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$ whose partial orders $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ and $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ induce finite, distributive lattices can be represented in that form, where $\setminus_{\mathrm{a}} = \overline{(\epsilon_V)_{\mathcal{L}}}$ and $\setminus_{\mathrm{c}} = \overline{(\eta_V)_{\mathcal{U}}}$ change to

$$\neg_{\mathrm{a}} = \overline{(\epsilon_V \circ i)_{\mathcal{L}}} \qquad \neg_{\mathrm{c}} = \overline{(\eta_V \circ i^{-1})_{\mathcal{U}}}$$

(respectively) for some $i \in \mathrm{Aut}(V, \leq)$.

Finite distributive AC-lattices

For any preorder $(V, \leq)$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \backslash_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \backslash_{\mathrm{c}})$ is an AC-lattice.

Conversely, every AC-lattice $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}}, \mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$ whose partial orders $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ and $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}})$ induce finite, distributive lattices can be represented in that form, where $\backslash_{\mathrm{a}} = \overline{(\epsilon_V)}_{\mathcal{L}}$ and $\backslash_{\mathrm{c}} = \overline{(\eta_V)}_{\mathcal{U}}$ change to

$$\neg_{\mathrm{a}} = \overline{(\epsilon_V \circ i)}_{\mathcal{L}} \qquad \neg_{\mathrm{c}} = \overline{(\eta_V \circ i^{-1})}_{\mathcal{U}}$$

(respectively) for some $i \in \mathrm{Aut}(V, \leq)$.

Note: $\overline{(\cdot)}_{\mathcal{L}}$ is lifting for lower powerdomain functor $\mathsf{L}(\cdot)$ and $\overline{(\cdot)}_{\mathcal{U}}$ is lifting for $\mathsf{U}(\cdot)$; the latter determined by $\mathsf{U}(f) = \backslash_{\mathrm{a}} \circ \mathsf{L}(f) \circ \backslash_{\mathrm{c}}$.

De Morgan lattices

Up to isos, De Morgan lattices are those AC-lattices for which $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}})$ equals $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$.

De Morgan lattices

Up to isos, De Morgan lattices are those AC-lattices for which $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}})$ equals $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$.

For any preorder $(V, \leq)$ and monotone map $i\colon (V, \leq) \to (V, \leq^{\mathrm{op}})$ with $i = i \circ i$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \neg)$ is a De Morgan lattice, where

$$\neg L = \{i(v) \mid v \in V \setminus L\}.$$

De Morgan lattices

Up to isos, De Morgan lattices are those AC-lattices for which $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}})$ equals $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$.

For any preorder $(V, \leq)$ and monotone map $i\colon (V, \leq) \to (V, \leq^{\mathrm{op}})$ with $i = i \circ i$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \neg)$ is a De Morgan lattice, where

$$\neg L = \{i(v) \mid v \in V \setminus L\}.$$

Conversely, every finite, distributive De Morgan lattice $(\mathcal{L}, \leq, \neg)$ can be represented in that form, where $(V, \leq)$ is a finite partial order.

Positive example

Consider $V = \{v, w\}$ in the discrete ordering.

Positive example

Consider $V = \{v, w\}$ in the discrete ordering.

- There are exactly two anti-tone idempotent maps on $(V, \leq)$, the identity id and sw which permutes v and w.

Positive example

Consider $V = \{v, w\}$ in the discrete ordering.

- There are exactly two anti-tone idempotent maps on $(V, \leq)$, the identity id and sw which permutes v and w.

- This gives rise to two different De Morgan negations: $\neg_{\mathrm{a}} \stackrel{\mathrm{def}}{=} \overline{(\epsilon_V \circ \mathrm{id})}_{\mathcal{L}}$ and $\neg'_{\mathrm{a}} \stackrel{\mathrm{def}}{=} \overline{(\epsilon_V \circ \mathrm{sw})}_{\mathcal{L}}$.

Positive example

Consider $V = \{v, w\}$ in the discrete ordering.

- There are exactly two anti-tone idempotent maps on $(V, \leq)$, the identity id and sw which permutes v and w.
- This gives rise to two different De Morgan negations: $\neg_{\mathrm{a}} \stackrel{\mathrm{def}}{=} \overline{(\epsilon_V \circ \mathrm{id})}_{\mathcal{L}}$ and $\neg'_{\mathrm{a}} \stackrel{\mathrm{def}}{=} \overline{(\epsilon_V \circ \mathrm{sw})}_{\mathcal{L}}$.
- We have $\neg_{\mathrm{a}}\{v\} = \{w\}$, and $\neg_{\mathrm{a}}\{w\} = \{v\}$, $\neg'_{\mathrm{a}}\{v\} = \{v\}$, and $\neg'_{\mathrm{a}}\{w\} = \{w\}$.

Positive example

Consider $V = \{v, w\}$ in the discrete ordering.

- There are exactly two anti-tone idempotent maps on $(V, \leq)$, the identity id and sw which permutes v and w.
- This gives rise to two different De Morgan negations: $\neg_{\mathrm{a}} \stackrel{\text{def}}{=} \overline{(\epsilon_V \circ \mathrm{id})}_{\mathcal{L}}$ and $\neg'_{\mathrm{a}} \stackrel{\text{def}}{=} \overline{(\epsilon_V \circ \mathrm{sw})}_{\mathcal{L}}$.
- We have $\neg_{\mathrm{a}}\{v\} = \{w\}$, and $\neg_{\mathrm{a}}\{w\} = \{v\}$, $\neg'_{\mathrm{a}}\{v\} = \{v\}$, and $\neg'_{\mathrm{a}}\{w\} = \{w\}$.
- Thus, the first negation is the classical one, $\backslash_{\mathrm{a}}$, and the second negation renders Belnap's four-valued logic [1]. We also know that this lattice cannot have any other De Morgan negations.

Negative example

Consider $V = \{x, y, z\}$ where y and z are incomparable but have higher priority than x.

Negative example

Consider $V = \{x, y, z\}$ where y and z are incomparable but have higher priority than x.

- This partial order is not self-dual; in particular, there cannot be an anti-tone map $i \colon (V, \leq) \to (V, \leq)$ with $i = i \circ i$.

Negative example

Consider $V = \{x, y, z\}$ where y and z are incomparable but have higher priority than x.

- This partial order is not self-dual; in particular, there cannot be an anti-tone map $i \colon (V, \leq) \to (V, \leq)$ with $i = i \circ i$.
- Thus, we know that $\mathsf{L}(V, \leq)$ cannot have a De Morgan negation.

Negative example

Consider $V = \{x, y, z\}$ where y and z are incomparable but have higher priority than x.

- This partial order is not self-dual; in particular, there cannot be an anti-tone map $i\colon (V, \leq) \to (V, \leq)$ with $i = i \circ i$.
- Thus, we know that $\mathsf{L}(V, \leq)$ cannot have a De Morgan negation.
- To see this explicitly, the third axiom of Figure 1(right) renders $\{\} = \neg\{x, y, z\} = \neg(\{x, y\} \cup \{x, z\}) = \neg\{x, y\} \cap \neg\{x, z\}$. Thus, at least one of the sets $\neg\{x, y\}$ and $\neg\{x, z\}$ has to be empty. But then $\neg$ cannot be a bijection, since $\{\} = \neg\{x, y, z\}$.

Negative example

Consider $V = \{x, y, z\}$ where y and z are incomparable but have higher priority than x.

- This partial order is not self-dual; in particular, there cannot be an anti-tone map $i\colon (V, \leq) \to (V, \leq)$ with $i = i \circ i$.
- Thus, we know that $\mathsf{L}(V, \leq)$ cannot have a De Morgan negation.
- To see this explicitly, the third axiom of Figure 1(right) renders $\{\} = \neg\{x, y, z\} = \neg(\{x, y\} \cup \{x, z\}) = \neg\{x, y\} \cap \neg\{x, z\}$. Thus, at least one of the sets $\neg\{x, y\}$ and $\neg\{x, z\}$ has to be empty. But then $\neg$ cannot be a bijection, since $\{\} = \neg\{x, y, z\}$.
- Of course, $(\mathsf{L}(V, \leq), \subseteq, \setminus_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \setminus_{\mathrm{c}})$ is an AC-lattice.

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

- $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$.

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

- $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$.
- The set of views V is endowed with a preorder $\leq$ of *priorities*.

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

- $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$.
- The set of views V is endowed with a preorder $\leq$ of *priorities*.
- **(Assertion obligations)** $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$ *obliges* viewpoint v to "assert" ϕ in *every* refinement $\mathcal{N}_v$; that is, it should be the case that $\mathcal{N}_v \models^{\mathrm{a}} \phi$, and

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

- $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$.
- The set of views V is endowed with a preorder $\leq$ of *priorities*.
- **(Assertion obligations)** $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$ *obliges* viewpoint v to "assert" ϕ in *every* refinement $\mathcal{N}_v$; that is, it should be the case that $\mathcal{N}_v \models^{\mathrm{a}} \phi$, and
- **(Consistency obligations)** $\mathcal{N}_v \models^{\mathrm{c}} \phi$ *obliges* v' to "hold ϕ as possible" in *every* abstraction $\mathcal{M}_{v'}$; that is, it should be the case that $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$.

Multiple-valued modal logic

Consider finite collections $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ and $\mathcal{N} = (\mathcal{N}_v)_{v \in V}$ of models. We lift single-view notions to multiple viewpoints.

- $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$.
- The set of views V is endowed with a preorder $\leq$ of *priorities*.
- **(Assertion obligations)** $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$ *obliges* viewpoint v to "assert" ϕ in *every* refinement $\mathcal{N}_v$; that is, it should be the case that $\mathcal{N}_v \models^{\mathrm{a}} \phi$, and
- **(Consistency obligations)** $\mathcal{N}_v \models^{\mathrm{c}} \phi$ *obliges* v' to "hold ϕ as possible" in *every* abstraction $\mathcal{M}_{v'}$; that is, it should be the case that $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$.

Such obligations, and their resulting conflicts, can be statically analyzed *within* the collection $\mathcal{M}$, assuming the refinement is sound in single viewpoints.

Multiple-valued semantics

Our semantics maintains autonomy and accountability of views as well as the portability of single-view technology:

Multiple-valued semantics

Our semantics maintains autonomy and accountability of views as well as the portability of single-view technology:

$$
\begin{aligned}
\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}} &\stackrel{\text{def}}{=} \{v \in V \mid \exists v' \in V : v \leq v',\ \mathcal{M}_{v'} \models^{\mathrm{a}} \phi\} \\
\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{c}} &\stackrel{\text{def}}{=} \{v \in V \mid \exists v' \in V : v' \leq v,\ \mathcal{M}_{v'} \models^{\mathrm{c}} \phi\} \\
\{\!|\mathcal{M} : \phi|\!\} &\stackrel{\text{def}}{=} (\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}}, \{\!|\mathcal{M} : \phi|\!\}^{\mathrm{c}}).
\end{aligned}
$$

Multiple-valued semantics

Our semantics maintains autonomy and accountability of views as well as the portability of single-view technology:

$$
\begin{array}{rcl}
\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}} & \stackrel{\mathrm{def}}{=} & \{v \in V \mid \exists v' \in V : v \leq v',\ \mathcal{M}_{v'} \models^{\mathrm{a}} \phi\} \\
\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{c}} & \stackrel{\mathrm{def}}{=} & \{v \in V \mid \exists v' \in V : v' \leq v,\ \mathcal{M}_{v'} \models^{\mathrm{c}} \phi\} \\
\{\!|\mathcal{M} : \phi|\!\} & \stackrel{\mathrm{def}}{=} & (\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}}, \{\!|\mathcal{M} : \phi|\!\}^{\mathrm{c}}).
\end{array}
$$

Example: locate conflicts among views; any v in

$$\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}} \cap \{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{a}}$$

has a conflict regarding ϕ.

Multiple-valued model checking

```
U = V;
L = emptyset;
while (U != emptyset) {
% invariants: L contained in { M : phi }^a,
%   { M : phi }^a contained in L union U
  for all v in max(U) {
    if (check(M[v], phi)) {
      L = L union { v' | v' <= v };
      U = U \ { v' | v' <= v };
    } else {
      U = U \ { v };
    }
  }
} post: L = { M : phi }^a
```

AC-lattice in mixed powerdomain

For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, any collection of models $\mathcal{M}$ determines a partial order $\mathbf{M}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mid \phi \in \mathcal{L}\}$, ordered by inclusion, and a negation operation $\neg^{\mathrm{m}} : \mathbf{M}_{\mathrm{m}} \to \mathbf{M}_{\neg\mathrm{m}}$:

$$\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}.$$

AC-lattice in mixed powerdomain

For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, any collection of models $\mathcal{M}$ determines a partial order $\mathbf{M}_{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mid \phi \in \mathcal{L}\}$, ordered by inclusion, and a negation operation $\neg^{\mathrm{m}} : \mathbf{M}_{\mathrm{m}} \to \mathbf{M}_{\neg\mathrm{m}}$:

$$\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}.$$

The *mixed power-domain* [3, 4] $\mathsf{M}_{(V,\leq)}$ is the sublattice of $(\mathsf{L}(V, \leq), \subseteq) \times (\mathsf{U}(V, \leq), \supseteq)$, consisting of all pairs (L, U) that satisfy the consistency condition $L = \{v \in V \mid \exists u \in L \cap U : v \leq u\}$.

AC-lattice in mixed powerdomain

For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, any collection of models $\mathcal{M}$ determines a partial order $\mathbf{M}_\mathrm{m} \stackrel{\text{def}}{=} \{\{\!|\mathcal{M} : \phi|\!\}^\mathrm{m} \mid \phi \in \mathcal{L}\}$, ordered by inclusion, and a negation operation $\neg^\mathrm{m} : \mathbf{M}_\mathrm{m} \to \mathbf{M}_{\neg\mathrm{m}}$:

$$\neg^\mathrm{m}\{\!|\mathcal{M} : \phi|\!\}^\mathrm{m} \;\stackrel{\text{def}}{=}\; \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}.$$

The *mixed power-domain* [3, 4] $\mathsf{M}_{(V,\leq)}$ is the sublattice of $(\mathsf{L}(V,\leq), \subseteq) \times (\mathsf{U}(V,\leq), \supseteq)$, consisting of all pairs (L, U) that satisfy the consistency condition $L = \{v \in V \mid \exists u \in L \cap U : v \leq u\}$.

The tuple $(\mathbf{M}_\mathrm{a}, \subseteq, \neg^\mathrm{a}, \mathbf{M}_\mathrm{c}, \subseteq, \neg^\mathrm{c})$ is an AC-lattice satisfying $\{\!|\mathcal{M} : \phi|\!\} \in \mathsf{M}_{(V,\leq)}$ for all ϕ.

AC-lattice in mixed powerdomain

For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, any collection of models $\mathcal{M}$ determines a partial order $\mathbf{M}_{\mathrm{m}} \stackrel{\text{def}}{=} \{\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mid \phi \in \mathcal{L}\}$, ordered by inclusion, and a negation operation $\neg^{\mathrm{m}} : \mathbf{M}_{\mathrm{m}} \to \mathbf{M}_{\neg\mathrm{m}}$:

$$\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \;\stackrel{\text{def}}{=}\; \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}.$$

The *mixed power-domain* [3, 4] $\mathsf{M}_{(V,\leq)}$ is the sublattice of $(\mathsf{L}(V, \leq), \subseteq) \times (\mathsf{U}(V, \leq), \supseteq)$, consisting of all pairs (L, U) that satisfy the consistency condition $L = \{v \in V \mid \exists u \in L \cap U : v \leq u\}$.

The tuple $(\mathbf{M}_{\mathrm{a}}, \subseteq, \neg^{\mathrm{a}}, \mathbf{M}_{\mathrm{c}}, \subseteq, \neg^{\mathrm{c}})$ is an AC-lattice satisfying $\{\!|\mathcal{M} : \phi|\!\} \in \mathsf{M}_{(V,\leq)}$ for all ϕ.

In a “Platonic” world — all obligations are fulfilled — , the lattices $(\mathbf{M}_{\mathrm{a}}, \subseteq)$ and $(\mathbf{M}_{\mathrm{c}}, \subseteq)$ are distributive.

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Three kinds of negation:

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Three kinds of negation:

- syntactically: $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mapsto \{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{m}}$;

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Three kinds of negation:

- syntactically: $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mapsto \{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{m}}$;
- syntactically with change of mode: $\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}$;

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Three kinds of negation:

- syntactically: $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mapsto \{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{m}}$;
- syntactically with change of mode:
  $\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}$;
- Heyting negations within $\mathsf{L}(V)$ and $\mathsf{U}(V)$.

Lift of semantic laws and negation

The semantics $\{\!|\mathcal{M} : \cdot|\!\} : \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ factors through the canonical projection $\phi \mapsto [\phi]_{\mathrm{m}}$ of type $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Three kinds of negation:

- syntactically: $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \mapsto \{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{m}}$;
- syntactically with change of mode:
  $\neg^{\mathrm{m}}\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}} \stackrel{\mathrm{def}}{=} \{\!|\mathcal{M} : \neg\phi|\!\}^{\neg\mathrm{m}}$;
- Heyting negations within $\mathsf{L}(V)$ and $\mathsf{U}(V)$.

All negations are equal in Platonic worlds of completely specified models.

More general relationships between these negations: see the paper.

Multiple-valued abstraction

We may now use this machinery to specify a version of Fitting's multi-valued modal logic such that

Multiple-valued abstraction

We may now use this machinery to specify a version of Fitting's multi-valued modal logic such that

- single-view models are under-specified;

Multiple-valued abstraction

We may now use this machinery to specify a version of Fitting's multi-valued modal logic such that

- single-view models are under-specified;
- abstraction and refinement is sound for query logic;

Multiple-valued abstraction

We may now use this machinery to specify a version of Fitting's multi-valued modal logic such that

- single-view models are under-specified;
- abstraction and refinement is sound for query logic;
- model checking is reducible to single-view checking; and

Multiple-valued abstraction

We may now use this machinery to specify a version of Fitting's multi-valued modal logic such that

- single-view models are under-specified;
- abstraction and refinement is sound for query logic;
- model checking is reducible to single-view checking; and
- semantic laws of single-view modal logic are preserved.

Conclusions

We presented assertion-consistency lattices as natural denotation spaces in the context of model checking under-specified models.

Conclusions

We presented assertion-consistency lattices as natural denotation spaces in the context of model checking under-specified models.

We classified finite distributive AC-lattices and De Morgan lattices.

Conclusions

We presented assertion-consistency lattices as natural denotation spaces in the context of model checking under-specified models.

We classified finite distributive AC-lattices and De Morgan lattices.

We specified a semantics for conflict location and detection in multiple-viewpoint settings.

Conclusions

We presented assertion-consistency lattices as natural denotation spaces in the context of model checking under-specified models.

We classified finite distributive AC-lattices and De Morgan lattices.

We specified a semantics for conflict location and detection in multiple-viewpoint settings.

We discussed how various forms of negation relate in this setting.

Conclusions

We presented assertion-consistency lattices as natural denotation spaces in the context of model checking under-specified models.

We classified finite distributive AC-lattices and De Morgan lattices.

We specified a semantics for conflict location and detection in multiple-viewpoint settings.

We discussed how various forms of negation relate in this setting.

We suggested applications of this framework to abstraction-based reasoning in multiple-valued modal logics.

Paper: `www.doc.ic.ac.uk/~mrh/huthpradhan02.ps`

References

[1] N. Belnap. A useful four-valued logic. In J. M. Dunn, editor, *Modern Uses of Many-Valued Logic*, pages 8–37. Reidel, 1977.

[2] J. M. Dunn. *What Is Negation*, chapter A Comparative Study of Various Model-Theoretic Treatments of Negation: A History of Formal Negation. Kluwer Academic Publishers, 1999.

[3] C. Gunter. The mixed power domain. *Theoretical Computer Science*, 103:311–334, 1992.

[4] R. Heckmann. Power domains and second order predicates. *Theoretical Computer Science*, 111:59–88, 1993.