Lifting assertion and consistency checkers from single to multiple viewpoints

Michael Huth
Department of Computing, Imperial College
London, United Kingdom, mrh@doc.ic.ac.uk

Shekhar Pradhan
Central Missouri State University
Warrensburg, Missouri, pradhan@cmsu1.cmsu.edu

Abstract

Using a priority preorder on requirements or specifications, we lift established property-verification techniques of three-valued model checking from single to multiple viewpoints. This lift guarantees a maximal degree of autonomy and accountability to single views, automatically synthesizes single-analysis results for multiple-view consistency and assertion checking, allows the re-use of single-view technology (e.g. standard model checkers), and transforms many meta-results (e.g. soundness of abstraction) from the single-view to the multiple-view setting. We formulate assertion-consistency lattices as a proper denotational universe for this lift, show that their symmetric versions are DeMorgan lattices, and classify both structures through (idempotent) order-isomorphisms on (self-dual) priority preorders in the finite case. In particular, this lift generalizes Fitting's multiple-valued semantics of modal logic in that our treatment of negation generalizes Heyting negation beyond fully specified and consistent models. We compare our approach to existing work on multiple-valued model checking.

1. Introduction

Motivation. During software development life cycles one invariably has to construct, maintain, and change requirements and specifications that stem from a number of stake-holders who express their own viewpoints of the expected state and behavior of a software artifact [25, 35]. This necessary multiplicity of perspectives makes the formal analysis of such descriptions difficult, if not impossible: viewpoints often have informal, semi-formal, or non-executable descriptions; multiple descriptions of the same behavior very likely give rise to *inconsistencies*; and existing static-analysis methods (e.g. model checking [31, 8, 9]) don't directly enable assertion checking or the detection of inconsistencies in a collection of executable models, where each model represents a particular point of view. As static-analysis tools slowly but steadily find their way into industrial research and development, one has very compelling reasons for extending their reach to the reasoning about software artifacts in the presence of multiple stake-holders. The adoption and training for the competent use of model-checking tools such as SMV [26] and Spin [21], which has over 4000 installations worldwide, also exert enormous economic and managerial pressure on multiple-viewpoint frameworks to make use of single-view tools. At the same time, individual stake-holders want to retain sufficient autonomy and accountability for their design and analysis activities, thereby enabling informed and constructive negotiations of design issues among stake-holders. These demands create a genuine opportunity to *re-use* in the multiple-view setting existing single-view model-checking technology such as model description languages, property specification languages and their patterns, refinement and abstraction techniques, model-checking and model-construction algorithms, their implementations/data structures, fairness, etc. In the sequel, we refer to such a loose bundle of know-how as a *model-checking framework*.

Scope of our results. In this paper, we lay the foundations for a *systematic re-use* of existing model-checking frameworks in the design and analysis of systems under multiple viewpoints. Our definitions and results are basically independent of the specific details of a single-view model-checking framework (e.g. its data structures, property logic, etc) and apply to all three-valued model-checking frameworks.[1] Without compromising any of the objectives aforementioned, our lift of such frameworks to the multiple-view setting transfers meta-results about single-view model checking to practically important meta-results of multiple-view checking (e.g. soundness of refinement), and introduces little computational overhead on the complexity of the underlying single-view assertion and consistency checking. We present AC-lattices[2] as our denotational structures which distinguish themselves in their treatment of negation. We then go on to show that whereas each finite AC-lattice corresponds to an order-automorphism on a finite prior-

[1] Our results specialize to standard two-valued abstraction-based model checking, but are then, as usual [11], limited to universal properties.

[2] Assertion-consistency lattices.

ity preorder the corresponding result for DeMorgan lattices [14] requires the preorder to be self-dual via an idempotent order-isomorphism. This corroborates our need to generalize DeMorgan lattices to AC-lattices, structures that allow for the inevitable asymmetry in requirements.

Three-valued model checking. Our work rests on the premise that sound notions of abstraction and (stepwise) refinement are crucial ingredients of frameworks for assertion and consistency checking. Sound abstraction is typically limited to *universal* properties [11]. However, checking the inconsistency of a universal ϕ requires reasoning about an *existential* property $\neg\phi$.[3] Moreover, many interesting system properties are non-trivial combinations of universal and existential aspects. Therefore, model-checking frameworks for multiple viewpoints require sound assertion and consistency checks of a logic with *unrestricted* use of negation and quantification. Three-valued model-checking frameworks (e.g. [4, 32, 23]) fulfill this requirement, conservatively extend conventional model-checking frameworks, and support consistency and assertion checking through the instrumented re-use of conventional, two-valued model checkers, as pioneered in [5]. Such three-valued approaches already exist for Kripke structures [12, 4, 5], labeled transition systems [30, 29, 23, 18], and models of first-order logic [24] with relational closure [32]. A three-valued structure explicitly specifies and distinguishes mandatory (denoted "a" for **a**ssertion) from merely possible (denoted "c" for **c**onsistency) state and behavior. As a specification of a single view v, such a structure may express v's own specification through its mandatory state and behavior, whereas its possible state and behavior are those aspects that viewpoint v is willing to "accept", if stipulated by other points of view. As a running example, we will consider a three-valued model-checking framework for a branching-time temporal logic that subsumes CTL [9], thus enabling a comparison to a semantics [16, 7] and model checker [15] for *multiple-valued* CTL.

Key issues. In transferring single-view model checks to a multiple-view setting, two key issues are present. First, how does one handle a check of property ϕ in view v, if some observables of ϕ have specified state or behavior outside of v only? Second, given a collection of views, how should we organize the analysis results from these single views into information about multiple viewpoints? Our earlier work [24] and other recent work on three-valued model checking [4, 32, 23], where external observables are modeled through possible state and behavior, adequately deals with the first issue. This paper addresses the second question by proposing one particular *automatic* synthesis of single-view analysis results that uses a light-weight and flexible *preorder of priorities* among views to derive a multiple-valued semantics that can reason about properties as well as expose inconsistencies, thus enabling rational discourse between all stake-holders. We base this choice on the fact that prioritizing is widely recognized as a key instrument in dealing with requirements [25, 34, 35].

[3] Similarly, consistency checking involves existential quantification over models.

Outline of paper. In Section 2, we axiomatize three-valued model-checking frameworks, give an example, and define AC-lattices as their denotational universes. We represent finite, distributive AC-lattices (DeMorgan lattices) through (idempotent) order-isomorphisms on (self-dual) finite preorders. Section 3 discusses how a preorder of priorities between views determines a multiple-valued semantics of single-view design and analysis results. We lift single-view meta-results to multiple-valued semantics — notably refinement, abstraction, the model-checking engine, and the semantic laws of the three-valued model-checking framework. Lifted denotations give rise to an AC-lattice. We show how this lift can be used for multiple-view assertion and consistency checking and the detection of inconsistencies. In particular, the lift of negation turns out to be a generalization of Heyting negation to collections of underdetermined models (Theorem 5). In Section 4, we develop a multiple-view semantics of a branching-time temporal logic with fixed-points that interprets logical connectives compositionally over a multiple-valued AC-lattice of meaning. This turns out to be our lifted semantics which we compare to existing work on multiple-valued modal logic [16, 15]. Finally, Section 5 concludes.

2. Three-valued model-checking frameworks

The models $\mathcal{M}$ of three-valued model-checking frameworks have a countable property logic of formulas ($\phi \in \mathcal{L}$) with negation ($\neg$), conjunction ($\wedge$), and atomic propositions ($y \in \mathtt{AP}$) among its operators. Models and atomic propositions may well have structure, e.g. as a set of relations and their types, but we will abstract from such details here. These models are *three-valued*, since their specifications consist of a *mandatory* part (state and behavior that is asserted and has to be realized), and a *possible* part (state and behavior that is consistent with the asserted state and behavior). This implicitly defines the *disallowed* state and behavior which, according to the specifications, are neither mandatory nor possible. As an example, we consider one-letter Kripke modal transition systems $\mathcal{M}$ [23] with signature $\mathtt{AP}$ — referred to as *three-valued Kripke structures* in this paper — which can be represented as pairs $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$ of ordinary Kripke structures $\mathcal{M}^{\mathrm{a}} = (\Sigma, R^{\mathrm{a}} \subseteq \Sigma \times \Sigma, L^{\mathrm{a}} \colon \Sigma \to \mathcal{P}(\mathtt{AP}))$ and

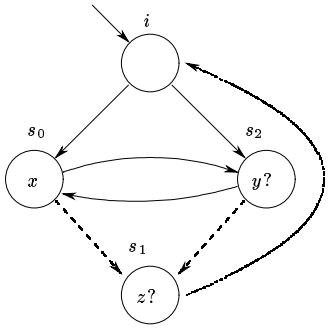

Figure 1. A three-valued Kripke structure modeling laptop modes.

$$
\begin{aligned}
[\![Z]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \rho^{\mathrm{m}}(Z) \\
[\![y]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \{s \in \Sigma \mid y \in L^{\mathrm{m}}(s)\} \\
[\![\neg\phi]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \Sigma \setminus [\![\phi]\!]^{\neg\mathrm{m}}_{\rho} \\
[\![\phi_1 \wedge \phi_2]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} [\![\phi_1]\!]^{\mathrm{m}}_{\rho} \cap [\![\phi_2]\!]^{\mathrm{m}}_{\rho} \\
[\![\mathsf{EX}\,\phi]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \mathrm{pre}^{\mathrm{m}}([\![\phi]\!]^{\mathrm{m}}_{\rho}) \\
[\![\mu Z.\phi]\!]^{\mathrm{m}}_{\rho} &\stackrel{\text{def}}{=} \mathrm{lfp}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\text{def}}{=} [\![\phi]\!]^{\mathrm{m}}_{\rho^{\mathrm{m}}[Z \mapsto A]}.
\end{aligned}
$$

Figure 2. Property semantics over three-valued Kripke structures for mode $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

$\mathcal{M}^{\mathrm{c}} = (\Sigma, R^{\mathrm{c}} \subseteq \Sigma \times \Sigma, L^{\mathrm{c}} \colon \Sigma \to \mathcal{P}(\mathtt{AP}))$ with signature $\mathtt{AP}$, where $\mathcal{M}^{\mathrm{a}}$ specifies mandatory and $\mathcal{M}^{\mathrm{c}}$ possible state and behavior (respectively). These two descriptions are made consistent by imposing that each mandatory state transition or proposition be also possible: $R^{\mathrm{a}} \subseteq R^{\mathrm{c}}$ and $L^{\mathrm{a}}(s) \subseteq L^{\mathrm{c}}(s)$ for all $s \in \Sigma$ [30, 23]; see Example 1 below. For state propositions ($y \in \mathtt{AP}$) and recursion variables ($Z \in \mathrm{var}$), we define a property logic

$$\phi ::= Z \mid y \mid \neg\phi \mid \phi \wedge \phi \mid \mathsf{EX}\,\phi \mid \mu Z.\phi \qquad (1)$$

where all ϕ in $\mu Z.\phi$ are formally monotone [3]. For each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, referred to as the *mode of analysis*, the semantics $[\![\phi]\!]^{\mathrm{m}}_{\rho} \subseteq \Sigma$ for properties, interpreted over three-valued Kripke structures, is depicted in Figure 2, where $\mathrm{pre}^{\mathrm{m}}(A) \stackrel{\text{def}}{=} \{s \in \Sigma \mid \exists s' \in \Sigma \colon (s, s') \in R^{\mathrm{m}},\ s' \in A\}$ for $A \subseteq \Sigma$ and environments (ρ^{m}) have type $\mathrm{var} \to \mathcal{P}(\Sigma)$. We write $s \models^{\mathrm{m}}_{\rho} \phi$ iff $s \in [\![\phi]\!]^{\mathrm{m}}_{\rho}$.

Example 1 (Laptop modes [22]) *Figure 1 shows a three-valued Kripke structure that models the modes of a laptop, where x, y, and z denote "AC powered", "battery powered", and "in suspend mode" (respectively). The labeling in the Figure means $x \in L^{\mathrm{a}}(s_0) \cap L^{\mathrm{c}}(s_0)$, $y \in L^{\mathrm{c}}(s_2) \setminus L^{\mathrm{a}}(s_2)$, and $z \in L^{\mathrm{c}}(s_1) \setminus L^{\mathrm{a}}(s_1)$. Dashed lines represent transitions in $R^{\mathrm{c}} \setminus R^{\mathrm{a}}$; solid lines denote transitions in $R^{\mathrm{a}} \cap R^{\mathrm{c}}$. The mandatory part of that model specifies the state and behavior of the laptop's AC power supply. The possible part specifies an additional power source (a battery) and a suspend mode for the machine. The property $\mathrm{AG\,EF}\, z$ — "all reachable states can reach a state in suspend mode" — is expressible in (1) as $\neg\mu Y.\neg(\mu W.z \vee (\mathsf{EX}\,(W) \wedge \mathsf{EX}\,(\neg(v \wedge \neg v)))) \vee \mathsf{EX}\,(Y)$. This formula is an invalid assertion[4] (we don't have $(\mathcal{M}, i) \models^{\mathrm{a}} \mathrm{AG\,EF}\, z$), but a consistent condition (we do have $(\mathcal{M}, i) \models^{\mathrm{c}} \mathrm{AG\,EF}\, z$).*

[4] If convenient, we identify models $\mathcal{M}$ with pointed ones [33] $(\mathcal{M}, i)$.

The evaluation of $(\mathcal{M}, i) \models^{\mathrm{a}} \mathrm{AG\,EF}\, z$ effectively checks whether all R^{c}-reachable states contain a R^{a}-path to a state s, where $z \in L^{\mathrm{a}}(s)$. The evaluation of $(\mathcal{M}, i) \models^{\mathrm{c}} \mathrm{AG\,EF}\, z$ conducts the same analysis but swaps the modes of paths.

One can show that three-valued Kripke structures are an instance of a three-valued model-checking framework.

Definition 1 (Three-valued model-checking framework) *A three-valued model-checking framework consists of*

#1 two satisfaction relations, one for assertion checking ($\mathcal{M} \models^{\mathrm{a}} \phi$), one for consistency checking ($\mathcal{M} \models^{\mathrm{c}} \phi$) — we refer to $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$ as the mode of analysis*;*

#2 consistency of models in that $\mathcal{M} \models^{\mathrm{a}} \phi$ always implies $\mathcal{M} \models^{\mathrm{c}} \phi$;

#3 for $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the semantics of conjunction as $\mathcal{M} \models^{\mathrm{m}} \phi_1 \wedge \phi_2$ iff $\mathcal{M} \models^{\mathrm{m}} \phi_1$ and $\mathcal{M} \models^{\mathrm{m}} \phi_2$;[5]

#4 for $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the semantics of negation as $\mathcal{M} \models^{\mathrm{m}} \neg\phi$ iff not $\mathcal{M} \models^{\neg\mathrm{m}} \phi$, where

$$\neg\mathrm{a} \stackrel{\text{def}}{=} \mathrm{c} \qquad \neg\mathrm{c} \stackrel{\text{def}}{=} \mathrm{a}; \qquad (2)$$

#5 for $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$, the semantics $\mathcal{M} \models^{\mathrm{m}} y$ ($y \in \mathtt{AP}$) determined by the specifications in $\mathcal{M}$;

#6 no $\mathcal{M}$ and ϕ with $\mathcal{M} \models^{\mathrm{a}} \phi \wedge \neg\phi$ (consistency of $\models^{\mathrm{a}}$);

#7 a formal notion of refinement *(a* preorder *$\prec$) between models, where $\mathcal{N} \prec \mathcal{M}$ means that $\mathcal{N}$ refines (is abstracted by) $\mathcal{M}$;*

[5] This property won't hold for the stronger semantics of Bruns and Godefroid in [5].

#8 sound assertion and consistency checking with respect to refinement: for all ϕ, if $\mathcal{N} \prec \mathcal{M}$, then (i) $\mathcal{M} \models^{\mathrm{a}} \phi$ implies $\mathcal{N} \models^{\mathrm{a}} \phi$, and (ii) $\mathcal{N} \models^{\mathrm{c}} \phi$ implies $\mathcal{M} \models^{\mathrm{c}} \phi$; and

#9 the property that $\models^{\mathrm{a}}$ equals $\models^{\mathrm{c}}$ on models that specify mandatory state or behavior only.

These properties have redundancy. For example, in the context of properties #3 and #4, properties #2 and #6 are equivalent. We remark that the properties above determine a semantics for propositional logic which is equivalent to Kleene's strong three-valued interpretation [27].

Proposition 1 (Examples) *Partial Kripke structures [4], extended labeled transition systems [4], modal transition systems [30], partial models of first-order logic [24], and (modal) shape graphs [32, 23] are three-valued model-checking frameworks that meet the nine properties above.*

Three-valued model-checking frameworks are intimately tied to a lattice-like structure.

Definition 2 (AC-lattices and DeMorgan 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 $\neg_{\mathrm{a}} \colon \mathcal{L}_{\mathrm{a}} \to \mathcal{L}_{\mathrm{c}}$ and $\neg_{\mathrm{c}} \colon \mathcal{L}_{\mathrm{c}} \to \mathcal{L}_{\mathrm{a}}$ are functions that meet the axioms of Figure 3 (left). A (complete)* DeMorgan lattice *is a tuple $(\mathcal{L}, \leq, \neg)$, where $(\mathcal{L}, \leq)$ is a partial order that induces a (complete) lattice, and $\neg \colon \mathcal{L} \to \mathcal{L}$ is a function that meet the axioms of Figure 3 (right).*

Note that the axioms of Figure 3 (left) spell out that the partial orders $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ and $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}{}^{\mathrm{op}})$ are isomorphic via $\neg_{\mathrm{a}}$ and $\neg_{\mathrm{c}}$. Bilattices [17] can also be represented as pairs of lattices, except that the treatment of negation for one mode (truth ordering) significantly differs from that of the other mode (knowledge ordering). In particular, these lattices may not be dually isomorphic. This asymmetry of negation rules out their use in our context. AC-lattices are crucial to the contributions of this paper: the quotient space for logical equivalences of three-valued model checks (Theorem 1), the denotation space for the synthesis of model checks under multiple points of view (Theorem 4), and DeMorgan lattices — denotation spaces of multiple-valued modal logics [16] — are all AC-lattices (Proposition 2).

Proposition 2 (DeMorgan lattices as AC-lattices) *Up to order-isomorphism, DeMorgan lattices are in one-to-one correspondence to AC-lattices, where $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}})$ is equal to $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$.*

Proof: See Appendix.

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

Figure 3. Axioms for AC-lattices (left) and DeMorgan lattices [14] (right).

A class $\mathbf{C}$ of models of a three-valued model checking framework — e.g. all countable three-valued Kripke structures with signature AP — determines two preorders of logical entailment whose space of equivalence classes, an AC-lattice, captures the semantics laws for assertions and consistency checks of class $\mathbf{C}$.[6]

Definition 3 (Entailment) *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 $[\phi]_{\mathrm{m}} \stackrel{\text{def}}{=} \{\psi \in \mathcal{L} \mid \psi \leq_{\mathrm{m}} \phi,\ \phi \leq_{\mathrm{m}} \psi\}$ and $\neg_{\mathrm{m}}[\phi]_{\mathrm{m}} \stackrel{\text{def}}{=} [\neg\phi]_{\neg_{\mathrm{m}}}$ determine countable sets $\mathcal{L}_{\mathrm{m}} \stackrel{\text{def}}{=} \{[\phi]_{\mathrm{m}} \mid \phi \in \mathcal{L}\}$ and functions $\neg_{\mathrm{m}} \colon \mathcal{L}_{\mathrm{m}} \to \mathcal{L}_{\neg_{\mathrm{m}}}$. 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 $\phi' \leq_{\mathrm{m}} \psi'$.*

The need for two notions of logical equivalences in the presence of under-determined models is illustrated by the example below.

Example 2 (Semantic laws) *For partial Kripke structures [4] and the semantics of [4], we have $[\bot]_{\mathrm{a}} = [\phi \wedge \neg\phi]_{\mathrm{a}}$ but we* don't *have $[\bot]_{\mathrm{c}} = [\phi \wedge \neg\phi]_{\mathrm{c}}$. For partial Kripke structures and the strong semantics of [5], we have $[\bot]_{\mathrm{c}} = [\phi \wedge \neg\phi]_{\mathrm{c}}$ and $[\top]_{\mathrm{a}} = [\phi \vee \neg\phi]_{\mathrm{a}}$.*

Theorem 1 (Model theory and its AC-lattice)

1. *For any three-valued model-checking framework, Definition 3 specifies a countable AC-lattice.*
2. *If we restrict the range of models in Definition 3 to those that specify mandatory state and behavior only, then this AC-lattice is a countable DeMorgan lattice.*

Proof: See the Appendix.

In the AC-lattice above, assertion and consistency checking are connected through $[\neg\phi]_{\mathrm{m}} = \{\neg\psi \mid \psi \in [\phi]_{\neg_{\mathrm{m}}}\}$ for each $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$.

Example 3 (Topologies as AC-lattices) *Let $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ be the complete lattice of closed subsets of a topological space*

[6] We will omit the parameter $\mathbf{C}$ from these preorders as its nature will be clear from the context, or irrelevant.

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.

We now give representation theorems (Theorem 2 and Theorem 3 below) for finite, distributive AC-lattices and DeMorgan lattices. Our representation of finite, distribute AC-lattices turns out to be an instance of Example 3, except that set complementation is precomposed with an order-isomorphism on the underlying preorder. In subsequent sections, we argue that our context of use requires that this automorphism be the identity. Finite, distributive DeMorgan lattices have the same representation, with the additional requirement that the underlying preorder be self-dual via an idempotent anti-tone order-isomorphism. Although DeMorgan lattices have been used for multiple-valued model checking [7], this result suggests that they are ill-suited for an approach that is driven by priority requirements — which never are symmetric in practice. The proof of these results requires standard machinery of power-domains [1].

Definition 4 (Power-domains) *Given a preorder $(V, \leq)$, $\mathsf{L}(V, \leq)$ denotes the set of lower subsets of V.*[7] *Let $\eta_V \colon (V, \leq) \to (\mathsf{L}(V, \leq), \subseteq)$, $\eta_V(v) \stackrel{\text{def}}{=} {\downarrow}v = \{v' \in V \mid v' \leq v\}$. Given a monotone map $f \colon (V, \leq) \to (L, \leq)$ into a complete lattice, we write $\overline{(f)}_{\mathcal{L}}$ for the unique sup-map*[8] *satisfying $\overline{(f)}_{\mathcal{L}} \circ \eta_V = f$. This defines the lower power-domain functor [1] $\mathsf{L}(g) \stackrel{\text{def}}{=} \overline{(\eta_W \circ g)}_{\mathcal{L}}$, where $g \colon (V, \leq) \to (W, \sqsubseteq)$ is a monotone map. Dually, we write $\mathsf{U}(V, \leq)$ for the set of upper subsets of V*[9] *and $\backslash_{\mathrm{a}} \colon (\mathsf{L}(V, \leq), \subseteq) \to (\mathsf{U}(V, \leq), \supseteq)$ and $\backslash_{\mathrm{c}} \colon (\mathsf{U}(V, \leq), \supseteq) \to (\mathsf{L}(V, \leq), \subseteq)$ for set complementation. Let $\epsilon_V \stackrel{\text{def}}{=} \backslash_{\mathrm{a}} \circ \eta_V \colon (V, \leq) \to (\mathsf{U}(V, \leq), \supseteq)$. For f as above, we write $\overline{(f)}_{\mathcal{U}}$ for the unique sup-map satisfying $\overline{(f)}_{\mathcal{U}} \circ \epsilon_V = f$. This defines the* complemented lower power-domain functor $\mathsf{U}(g) \stackrel{\text{def}}{=} \overline{(\epsilon_W \circ g)}_{\mathcal{U}}$ *for g as above. Finally, let $\mathrm{Aut}(V, \leq)$ be the set of order-isomorphisms of type $(V, \leq) \to (V, \leq)$.*

Proposition 3 (Dual functors) *1. $\mathsf{U}(\cdot) \colon \mathbf{Pre} \to \mathbf{Lat}$ is a monotone functor between the categories of preorders and monotone maps and complete lattices and sup-maps.*

2. *We have $\backslash_{\mathrm{a}} = \overline{(\epsilon_V)}_{\mathcal{L}}$, $\backslash_{\mathrm{c}} = \overline{(\eta_V)}_{\mathcal{U}}$, $\eta_V = \backslash_{\mathrm{c}} \circ \epsilon_V$, and $\mathsf{U}(f) = \backslash_{\mathrm{a}} \circ \mathsf{L}(f) \circ \backslash_{\mathrm{c}}$.*
3. *The functors $\mathsf{L}(\cdot)$ and $\mathsf{U}(\cdot)$ restrict to isomorphisms of type $\mathrm{Aut}((V, \leq)) \to \mathrm{Aut}(\mathsf{L}(V, \leq))$ and $\mathrm{Aut}((V, \leq)) \to \mathrm{Aut}(\mathsf{U}(V, \leq))$ (respectively).*

[7] A subset L of V is a *lower set* iff $v \in L$ and $v' \leq v$ imply $v' \in L$.

[8] A function $f \colon L \to L'$ between complete lattices L and L' is a sup-map iff $f(\bigvee X) = \bigvee f(X)$ for all $X \subseteq L$.

[9] A subset U of V is an *upper set* iff $v \in U$ and $v \leq v'$ imply $v' \in U$.

Proof: See Appendix.

Theorem 2 (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*

$$\neg_{\mathrm{a}} = \overline{(\epsilon_V \circ i)}_{\mathcal{L}} \qquad \neg_{\mathrm{c}} = \overline{(\eta_V \circ i^{-1})}_{\mathcal{U}} \tag{3}$$

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

Proof: See Appendix.

Theorem 3 (Finite, distributive DeMorgan lattices) *For any preorder $(V, \leq)$ and an anti-tone and idempotent map $i \colon (V, \leq) \to (V, \leq)$,*[10] *the tuple $(\mathsf{L}(V, \leq), \subseteq, \neg)$ is a DeMorgan lattice, where*

$$\neg L = \{i(v) \mid v \in V \setminus L\}. \tag{4}$$

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

Proof: See the Appendix.

Example 4 (Representation of DeMorgan lattices)

1. *For a positive example, consider the finite, self-dual partial order $V = \{v, w\}$ 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 DeMorgan 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 [2]. By Theorem 3, this lattice cannot have any other DeMorgan negations.*
2. *For a negative example, consider the finite partial order of priorities $(V, \leq)$, where $V = \{x, y, z\}$ and 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, idempotent map $i \colon (V, \leq) \to (V, \leq)$. By Theorem 3, $\mathsf{L}(V, \leq)$ cannot have a DeMorgan negation. To see this explicitly, the third axiom of Figure 3(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, $(\mathsf{L}(V, \leq), \subseteq, \backslash_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \backslash_{\mathrm{c}})$ is an AC-lattice.*

[10] A map $f \colon (V, \leq) \to (V, \leq)$ is anti-tone and idempotent if $v \leq v'$ implies $f(v') \leq f(v)$ and if $f(f(v)) = v$ for all $v, v' \in V$.

The examples above illustrate that the partial-order quotient of a preorder $(V, \leq)$ will not be self-dual, if that preorder denotes realistic priorities of requirements. Thus, DeMorgan lattices are an inadequate denotational universe for synthesizing single-view analysis according to a preorder of priorities. But AC-lattices, as their generalizations beyond self-dual priorities, are suitable denotation spaces for any kind of preorder. This mathematical justification is corroborated by the intuition that, in under-determined models, denotations of assertion checks ($\in \mathcal{L}_{\mathrm{a}}$) may not be denotations of consistency checks ($\in \mathcal{L}_{\mathrm{c}}$) and vice versa.

3. Lifting single-view analysis

In the sequel, we write $\mathcal{M}$ and $\mathcal{N}$ for *finite* collections $(\mathcal{M}_v)_{v \in V}$ and $(\mathcal{N}_v)_{v \in V}$ of models $\mathcal{M}_v$ and $\mathcal{N}_v$ (respectively) of a three-valued model-checking framework. We make no assumptions about the degree of precision that each view imposes on model checks $\mathcal{M}_v \models^{\mathrm{m}} \phi$ that mention external behavior, nor do we restrict the sound techniques utilized in gaining that precision — be they (three-valued) versions of compositional model checking [10], module checking [28], etc.

Definition 5 (Refinement of collections of models) *For $\mathcal{M}$ and $\mathcal{N}$ as above, we say that $\mathcal{N} \prec \mathcal{M}$ iff, for each $v \in V$, $\mathcal{N}_v \prec \mathcal{M}_v$ in the underlying three-valued model-checking framework.*

Note that $\mathcal{M} \prec \mathcal{M}$ holds since refinements are preorders (property #7). We assume that the set of views V be endowed with a preorder $\leq$ of *priorities*: $v \leq v'$ denotes that view v' has equal or higher priority over view v, suggesting that $\mathcal{M}_{v'}$ is a more abstract, higher-level or authoritative description of the underlying artifact, whereas $\mathcal{M}_v$ specifies a more concrete, lower-level, or less important aspect. We understand $v \leq v'$ to create — for all instances of $\mathcal{N} \prec \mathcal{M}$ — the obligation that whatever is asserted in a model $\mathcal{M}_{v'} \in \mathcal{M}$ *should* be asserted in model $\mathcal{N}_v \in \mathcal{N}$ and whatever is possible in $\mathcal{N}_v$ *should* be possible in $\mathcal{M}_{v'}$:

- **(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 $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$.

We argue that such obligations, and their resulting conflicts, can be statically analyzed *within* the collection $\mathcal{M}$ of three-valued models.

Proposition 4 (Sound obligation checking) *Let $\mathcal{N} \prec \mathcal{M}$. For all ϕ,*

1. *if $v \leq v'$ obliges $\mathcal{M}_v$ to assert ϕ, then it also obliges $\mathcal{N}_v$ to assert ϕ.*
2. *if $v \leq v'$ obliges $\mathcal{N}_{v'}$ to hold ϕ possible, then it also obliges $\mathcal{M}_{v'}$ to hold ϕ possible.*

Proof: If $v \leq v'$ obliges $\mathcal{M}_v$ to assert ϕ; then $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$, $\mathcal{N}_{v'} \prec \mathcal{M}_{v'}$, and property #8 imply $\mathcal{N}_{v'} \models^{\mathrm{a}} \phi$. But then $v \leq v'$ creates an obligation for $\mathcal{N}_v$ to assert ϕ. The argument for item 2 is dual. ∎

Thus, any assertion obligation detected within $\mathcal{M}$ persists as an assertion obligation in all its refinements. Conversely, any consistency obligation detected in any of $\mathcal{M}$'s refinements, persists and can be detected within $\mathcal{M}$.

Definition 6 (Platonic world) *A collection $\mathcal{M}$ is* Platonic *iff all the obligations of the priority ordering $\leq$ are fulfilled in $\mathcal{M}$. In other words, if $v \leq v'$ implies that $\mathcal{M}_v \prec \mathcal{M}_{v'}$ in the underlying three-valued model-checking framework.*

If $\mathcal{M}$ is not Platonic, then it may not meet its own obligations of the priority preorder. But we claim that we can successfully perform assertion and consistency checks within $\mathcal{M}$ in the presence of conflicting and inconsistent obligations. Moreover, these checks can be used to expose the conflicts in those obligations.

Example 5 (Exposing conflicting obligations) *Suppose that $v \leq v'$, $v \leq v''$, $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$, and $\mathcal{M}_{v''} \models^{\mathrm{a}} \neg\phi$. Now for any refinement $\mathcal{N}_v$ of $\mathcal{M}_v$, which may be a concrete implementation, we are obliged to assert both ϕ and $\neg\phi$, and a contradiction is apparent.*

The ontology of our framework does not require any connections between the priority preorder $\leq$ on viewpoints — which is based on system needs, empirical evidence or any other mechanisms for prioritizing — and the preorder $\prec$ of refinement between models $\mathcal{M}_v$ of viewpoints v. As the example above already suggests, it is this independence that allows us to model and expose inconsistencies across viewpoints. In a Platonic world, all assertion and consistency obligations are met and no contradictions will arise *within* that world (Proposition 5). Alas, in our actual world of software design and analysis the consistency requirements between multiple viewpoints may be violated at a number of, if not all, instances of $\leq$ — due to the conflicts of interests between different stake-holders, specification or implementation errors, miscommunication, or other sources of conflict.

In the remainder of this section, we develop a tool that collects assertion and consistency obligations and has the power to trace the origin of contradictions, thereby enabling conflict resolution through tool-informed changes in the viewpoints and/or the priorities. But much more significantly, the approach we develop here also has the power to

detect this contradiction in the requirements of v' and v'' without having to construct an *inconsistent* model $\mathcal{N}_v$ with its resulting "logical collapse". We avoid the use of inconsistent models by assuming that some later refinement of $\mathcal{M}_v$ will satisfy the obligations of $v \leq v'$ and $v \leq v''$ — which may not be a correct assumption — and by pretending that the models in $\mathcal{M}$ already satisfy these obligations — which may be false. This non-standard treatment of truth permits us to efficiently detect the conflicting requirements of v' and v'' by processing the models in $\mathcal{M}$ and to do this by exploiting the order structure of $\leq$. The resulting semantics of negation turns out to generalize Heyting negation to under-specified collections of models (Theorem 5). Our semantic tool for effectively analyzing assertion and consistency checks maintains autonomy and accountability of views as well as the portability of single-view technology:

$$\begin{array}{rcl} \{|\mathcal{M}:\phi|\}^{\mathrm{a}} & \stackrel{\text{def}}{=} & \{v \in V \mid \exists v' \in V : v \leq v',\ \mathcal{M}_{v'} \models^{\mathrm{a}} \phi\} \\ \{|\mathcal{M}:\phi|\}^{\mathrm{c}} & \stackrel{\text{def}}{=} & \{v \in V \mid \exists v' \in V : v' \leq v,\ \mathcal{M}_{v'} \models^{\mathrm{c}} \phi\} \\ \{|\mathcal{M}:\phi|\} & \stackrel{\text{def}}{=} & (\{|\mathcal{M}:\phi|\}^{\mathrm{a}}, \{|\mathcal{M}:\phi|\}^{\mathrm{c}}). \end{array} \quad (5)$$

Sets $\{|\mathcal{M}:\phi|\}^{\mathrm{a}}$ are in $\mathsf{L}(V,\leq)$ and collect all views v that have equal or lower priority than some view v' in which the assertion ϕ holds; sets $\{|\mathcal{M}:\phi|\}^{\mathrm{c}}$ are in $\mathsf{U}(V,\leq)$ and comprise all views v that have equal or higher priority than some view v' in which ϕ is consistent. The set $\{|\mathcal{M}:\phi|\}^{\mathrm{a}}$ contains all the views that are *obliged* to assert ϕ according to $\mathcal{M}$, whereas the set $\{|\mathcal{M}:\phi|\}^{\mathrm{c}}$ contains all those views that are *obliged* to hold that ϕ is possible according to $\mathcal{M}$. By Proposition 4, all assertion obligations created by priorities persist in refinements (item 1). Dually, consistency obligations that are created by priorities and not met in a model are also not met in any of its subsequent refinements: if the obligation that $\mathcal{M}_v$ holds ϕ possible is not met, then $\mathcal{M}_v \not\models^{\mathrm{c}} \phi$ implies $\mathcal{M}_v \models^{\mathrm{a}} \neg\phi$, meaning $\mathcal{N}_v \not\models^{\mathrm{c}} \phi$ for all refinements $\mathcal{N}_v \prec \mathcal{M}_v$.

The semantics in (5) is still meaningful if single views use different ontologies for expressing and analyzing their partial views, assuming that one can state the properties of interest in all ontologies involved. Apart from assertion and consistency checking in multiple views, we may use this semantics to detect and locate conflicts among views:

$$\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \cap \{|\mathcal{M}:\neg\phi|\}^{\mathrm{a}} \quad (6)$$

represents all those views v that face an inconsistency regarding property ϕ: there are views v', v'' with equal or higher priorities than v that oblige v to assert ϕ and $\neg\phi$ (respectively).[11] More generally, for a finite set of formulas Γ, the set $\cap\{\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \mid \phi \in \Gamma\}$ collects those views that are obliged to assert the conjunction $\wedge\Gamma$. In a Platonic world $\{|\mathcal{M}:\phi|\}^{\mathrm{a}}$ ($\{|\mathcal{M}:\phi|\}^{\mathrm{c}}$) coincides with the set of all views in which the assertion (consistency check) ϕ holds.

[11] Note that property #6 ensures that $v = v' = v''$ cannot occur.

Proposition 5 (Consistency in Platonic world) *All Platonic worlds $\mathcal{M}$ meet all their own assertion and consistency obligations; in particular, the set in (6) is empty.*

Proof: The first claim is immediate from the definition of (5) and property #8, noting that preorders are reflexive. As for the second claim, assume that v is in $\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \cap \{|\mathcal{M}:\neg\phi|\}^{\mathrm{a}}$. By definition of $\{|\mathcal{M}:\cdot|\}^{\mathrm{a}}$, there exist $v', v'' \in V$ such that (i) $v \leq v''$ and $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$; and (ii) $v \leq v''$ and $\mathcal{M}_{v''} \models^{\mathrm{a}} \neg\phi$. Since the priority preorder realizes refinements, we may use property #8 on (i), resulting in $\mathcal{M}_v \models^{\mathrm{a}} \phi$; and on (ii), obtaining $\mathcal{M}_v \models^{\mathrm{a}} \neg\phi$. In summary, we conclude $\mathcal{M}_v \models^{\mathrm{a}} \phi \wedge \neg\phi$, contradicting property #6. ∎

Proposition 6 (Meet in Platonic world) *In any world, $\{|\mathcal{M}:\phi\wedge\psi|\}^{\mathrm{m}} \subseteq \{|\mathcal{M}:\phi|\}^{\mathrm{m}} \cap \{|\mathcal{M}:\psi|\}^{\mathrm{m}}$. In a Platonic world, this inclusion is equality.*

Proof: If $v \in \{|\mathcal{M}:\phi\wedge\psi|\}^{\mathrm{c}}$, then there is some $v' \in V$ with $v' \leq v$ and $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi \wedge \psi$. But then $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$ and $\mathcal{M}_{v'} \models^{\mathrm{c}} \psi$ follow. Thus, $v \in \{|\mathcal{M}:\phi|\}^{\mathrm{c}} \cap \{|\mathcal{M}:\psi|\}^{\mathrm{c}}$. Conversely, let $w \in \{|\mathcal{M}:\phi|\}^{\mathrm{c}} \cap \{|\mathcal{M}:\psi|\}^{\mathrm{c}}$. Then there exist $w', w'' \in V$ with $w', w'' \leq w$, $\mathcal{M}_{w'} \models^{\mathrm{c}} \phi$, and $\mathcal{M}_{w''} \models^{\mathrm{c}} \psi$. In a Platonic world, $w', w'' \leq w$ then imply $\mathcal{M}_w \models^{\mathrm{c}} \phi$, and $\mathcal{M}_w \models^{\mathrm{c}} \psi$, so $\mathcal{M}_w \models^{\mathrm{c}} \phi \wedge \psi$. Since $w \leq w$, this renders $w \in \{|\mathcal{M}:\phi\wedge\psi|\}^{\mathrm{c}}$. The proof for mode a is dual. ∎

The straightforward consistency requirement $\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \subseteq \{|\mathcal{M}:\phi|\}^{\mathrm{c}}$ for our synthesis of assertion and consistency checking does not hold in general. Interestingly enough, the mixed power-domain [19, 20] provides a weaker consistency condition of this sort.

Definition 7 (Multiple-valued AC-lattice operations) *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 $\neg^{\mathrm{m}} : \mathbf{M}_{\mathrm{m}} \to \mathbf{M}_{\neg\mathrm{m}}$:*

$$\neg^{\mathrm{m}}\{|\mathcal{M}:\phi|\}^{\mathrm{m}} \stackrel{\text{def}}{=} \{|\mathcal{M}:\neg\phi|\}^{\neg\mathrm{m}}. \quad (7)$$

The mixed power-domain *[19, 20] $\mathsf{M}_{(V,\leq)}$ 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*

$$L = \{v \in V \mid \exists u \in L \cap U : v \leq u\}. \quad (8)$$

Example 6 (Mixed consistency) *Clearly, if L is set as $\{|\mathcal{M}:\phi|\}^{\mathrm{a}}$ and U is set as $\{|\mathcal{M}:\phi|\}^{\mathrm{c}}$ then equation (8) holds whenever $\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \subseteq \{|\mathcal{M}:\phi|\}^{\mathrm{c}}$. However, equation (8) expresses a weaker consistency condition than $\{|\mathcal{M}:\phi|\}^{\mathrm{a}} \subseteq \{|\mathcal{M}:\phi|\}^{\mathrm{c}}$. Let $v \leq v' \leq v''$. Let $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$, $\mathcal{M}_{v''} \models^{\mathrm{c}} \phi$,*

$\mathcal{M}_{v''} \models^{\mathrm{c}} \neg\phi$, *and* $\mathcal{M}_v \models^{\mathrm{a}} \neg\phi$. *Then* $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} = \{v, v'\}$ *and* $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{c}} = \{v', v''\}$. *These satisfy (8) but* $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} \not\subseteq \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{c}}$.

Theorem 4 (AC-lattice of denotations) *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, the lattices* $(\mathbf{M}_{\mathrm{a}}, \subseteq)$ *and* $(\mathbf{M}_{\mathrm{c}}, \subseteq)$ *are distributive.*

Proof:

1. Clearly, $L \stackrel{\text{def}}{=} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} \in \mathsf{L}(V,\leq)$ and $U \stackrel{\text{def}}{=} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{c}} \in \mathsf{U}(V,\leq)$. We show that L and U as defined satisfy (8). In (8), the right-hand side is always contained in the left-hand side. Conversely, let $v \in L$. Then there is some $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$. So $v' \in L$ since $v' \leq v'$. Since $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$ implies $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$ (property #2), we infer $v' \in U$. Thus, $v' \in L \cap U$ and $v \leq v'$ show that v is an element of the right-hand side.

2. Note that $\neg_m \neg_{\neg m} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}} = \neg_m \{\!|\mathcal{M}:\neg\phi|\!\}^{\neg\mathrm{m}} = \{\!|\mathcal{M}:\neg\neg\phi|\!\}^{\mathrm{m}}$. But the latter set equals $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}}$ since $[\neg\neg\phi]_{\mathrm{m}} = [\phi]_{\mathrm{m}}$.

3. Let $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} \leq_{\mathrm{a}} \{\!|\mathcal{M}:\psi|\!\}^{\mathrm{a}}$. For $v \in \{\!|\mathcal{M}:\neg\psi|\!\}^{\mathrm{c}}$ there exists some $v' \in V$ with $v' \leq v$ and $\mathcal{M}_{v'} \models^{\mathrm{c}} \neg\psi$, i.e. we have that $\mathcal{M}_{v'} \not\models^{\mathrm{a}} \psi$. From $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} \leq_{\mathrm{a}} \{\!|\mathcal{M}:\psi|\!\}^{\mathrm{a}}$ and $v' \leq v'$, we therefore infer that $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$ is not the case, so $\mathcal{M}_{v'} \models^{\mathrm{c}} \neg\phi$ holds. Thus, $v \in \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{c}}$. Hence $\{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{c}} \leq_{\mathrm{c}} \{\!|\mathcal{M}:\neg\psi|\!\}^{\mathrm{c}}$. The other axiom is shown dually.

4. Since existential quantification distributes over disjunctions, $\{\!|\mathcal{M}:\phi \vee \psi|\!\}^{\mathrm{m}} = \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}} \cup \{\!|\mathcal{M}:\psi|\!\}^{\mathrm{m}}$. Thus, $(\mathbf{M}_{\mathrm{a}}, \leq_{\mathrm{a}})$ and $(\mathbf{M}_{\mathrm{c}}, \leq_{\mathrm{c}})$ have joins, so they are both (complete) lattices.

5. The claim about distributivity is a consequence of Proposition 6 and the previous item. ∎

As in any lattice, the meet operation in $\mathbf{M}_{\mathrm{m}}$ is expressible via its join operation. It is also expressible in the logic. Using that existential quantification distributes over disjunctions, $\{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}} \wedge \{\!|\mathcal{M}:\psi|\!\}^{\mathrm{m}}$ equals $\{\!|\mathcal{M}:\eta|\!\}^{\mathrm{m}}$, where η is defined as

$$\bigvee \{\gamma \mid \{\!|\mathcal{M}:\gamma|\!\}^{\mathrm{m}} \leq_{\mathrm{m}} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}}, \{\!|\mathcal{M}:\psi|\!\}^{\mathrm{m}}\}. \quad (9)$$

In case that $\mathcal{L}$ has no infinite disjunction, the set comprehension in (9) can be restricted to a finite set of representatives of the equivalence relation $\cong_{\mathrm{m}}$, defined by $\gamma \cong_{\mathrm{m}} \gamma'$ iff $\{\!|\mathcal{M}:\gamma|\!\}^{\mathrm{m}} = \{\!|\mathcal{M}:\gamma'|\!\}^{\mathrm{m}}$.

We can lift meta-results of the single-view model-checking framework to our multiple-view semantics in (5), even in a non-Platonic world.

Remark 1 (Lift of semantic laws) *The semantics* $\{\!|\mathcal{M}:\cdot|\!\}: \mathcal{L} \to \mathsf{M}_{(V,\leq)}$ *in (5) factors through the canonical projection* $\phi \mapsto [\phi]_{\mathrm{m}}$ *of type* $\mathcal{L} \to \mathcal{L}_{\mathrm{m}}$.

Since the interpretation of negation is absolutely crucial for assertion and consistency checking, we compare our lifted semantics of $\neg$ to set complement and the Heyting negations $\neg_{\mathrm{A}}: \mathsf{L}(V,\leq) \to \mathsf{L}(V,\leq)$ and $\neg_{\mathrm{C}}: \mathsf{U}(V,\leq) \to \mathsf{U}(V,\leq)$ (respectively):[12]

$$\neg_{\mathrm{A}} L \stackrel{\text{def}}{=} \bigcup \{L' \in \mathsf{L}(V,\leq) \mid L \cap L' = \{\}\} \quad (10)$$

$$\neg_{\mathrm{C}} U \stackrel{\text{def}}{=} \bigcap \{U' \in \mathsf{U}(V,\leq) \mid U \cup U' = V\}. \quad (11)$$

Theorem 5 (Lift of negation) *Let* $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$ *and* $\phi \in \mathcal{L}$.

1. *We have* $V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\neg\mathrm{m}} \subseteq \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{m}}$.

2. *In a Platonic world,* $V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\neg\mathrm{m}}$ *equals* $\{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{m}}$. *This set is contained in* $\neg_{\mathrm{M}} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}}$ *if* $\mathrm{m} = \mathrm{a}$ *or if* $[\top]_{\mathrm{a}} = [\phi \vee \neg\phi]_{\mathrm{a}}$.[13]

3. *If all viewpoints* $\mathcal{M}_v$ $(v \in V)$ *specify mandatory state and behavior only, then* $\neg_{\mathrm{M}} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}} \subseteq \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{m}}$.

4. *In a Platonic world with mandatory state and behavior only,* $V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\neg\mathrm{m}} = \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{m}} \subseteq \neg_{\mathrm{M}} \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{m}}$, *where all three forms of negation are equal if* $\mathrm{m} = \mathrm{a}$ *or if* $[\top]_{\mathrm{a}} = [\phi \vee \neg\phi]_{\mathrm{a}}$.

Proof:

1. Let $v \in V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}}$. Thus, for all $v' \in V$ with $v \leq v'$, we have $\mathcal{M}_{v'} \not\models^{\mathrm{a}} \phi$, i.e. $\mathcal{M}_{v'} \models^{\mathrm{c}} \neg\phi$. Since $v \leq v$, we infer $v \in \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{c}}$. Dually, let $v \in V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{c}}$. Thus, for all $v' \in V$ with $v' \leq v$, we have $\mathcal{M}_{v'} \not\models^{\mathrm{c}} \phi$, i.e. $\mathcal{M}_{v'} \models^{\mathrm{a}} \neg\phi$. Since $v \leq v$, we infer $v \in \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{a}}$.

2.(a) To show equality, let $v \in \{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{a}}$. Then there exists some $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'} \models^{\mathrm{a}} \neg\phi$. If there is some $v'' \in V$ with $v'' \leq v$ and $\mathcal{M}_{v''} \models^{\mathrm{c}} \phi$, then $v'' \leq v \leq v'$ implies $\mathcal{M}_{v'} \models^{\mathrm{c}} \phi$ in a Platonic world (property #8). But this contradicts $\mathcal{M}_{v'} \models^{\mathrm{a}} \neg\phi$ by property #4. Thus, $v \in V \setminus \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{c}}$. This and item 1 establish equality. The proof for the other combination of modes is dual.

2.(b) To show the inclusion for a, using (10) and $\{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{a}} \in \mathsf{L}(V,\leq)$, we are done if $\{\!|\mathcal{M}:\neg\phi|\!\}^{\mathrm{a}} \cap \{\!|\mathcal{M}:\phi|\!\}^{\mathrm{a}} = \{\}$, which follows from Proposition 5.

[12] In any Heyting algebra, $\neg = \neg \circ \neg \circ \neg$, so its image of $\neg \circ \neg$ is a DeMorgan lattice.

[13] The latter holds for the generalized model-checking of Bruns & Godefroid [5], but not for the semantics of Figure 2.

2.(c) To show the inclusion for c, let $v \in \{|\mathcal{M} : \neg\phi|\}^{\mathrm{c}}$. By (11), it suffices to show that for any $U' \in \mathsf{U}(V, \leq)$ with $V = \{|\mathcal{M} : \phi|\}^{\mathrm{c}} \cup U'$ we have $v \in U'$. Since $v \in \{|\mathcal{M} : \neg\phi|\}^{\mathrm{c}}$, there is some $v' \in V$ with $v' \leq v$ and $\mathcal{M}_{v'} \models^{\mathrm{c}} \neg\phi$. If $v \notin U'$, then $V = \{|\mathcal{M} : \phi|\}^{\mathrm{c}} \cup U'$ implies $v \in \{|\mathcal{M} : \phi|\}^{\mathrm{c}}$. So then there exists some $v'' \in V$ with $v'' \leq v$ and $\mathcal{M}_{v''} \models^{\mathrm{c}} \phi$. In a Platonic world, we get $\mathcal{M}_v \models^{\mathrm{c}} \phi$ and $\mathcal{M}_v \models^{\mathrm{c}} \neg\phi$, contradicting $[\top]_{\mathrm{a}} = [\phi \vee \neg\phi]_{\mathrm{a}}$.

3.(a) Let $L \in \mathsf{L}(V, \leq)$ with $L \cap \{|\mathcal{M} : \phi|\}^{\mathrm{a}} = \{\}$. By (10), it suffices to show that $L \subseteq \{|\mathcal{M} : \neg\phi|\}^{\mathrm{a}}$. For any $v \in L$, we have $v \notin \{|\mathcal{M} : \phi|\}^{\mathrm{a}}$, so there cannot be any $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$. Since $v \leq v$, we conclude $\mathcal{M}_v \not\models^{\mathrm{a}} \phi$, i.e. $\mathcal{M}_v \models^{\mathrm{c}} \neg\phi$. Now, property #9 renders $\mathcal{M}_v \models^{\mathrm{a}} \neg\phi$.

3.(b) Dually, since $\{|\mathcal{M} : \neg\phi|\}^{\mathrm{c}}$ is an upper set, it suffices to show that $\{|\mathcal{M} : \neg\phi|\}^{\mathrm{c}} \cup \{|\mathcal{M} : \phi|\}^{\mathrm{c}}$ equals V. But for any $v \in V \setminus \{|\mathcal{M} : \phi|\}^{\mathrm{c}}$, $v \leq v$ implies that $\mathcal{M}_v \models^{\mathrm{c}} \phi$ is not the case, i.e. $\mathcal{M}_v \models^{\mathrm{c}} \neg\phi$ holds by property #9. Therefore, $v \in \{|\mathcal{M} : \neg\phi|\}^{\mathrm{c}}$.

4. This follows from items 2 and 3. ∎

In each $\mathcal{M}_v$, state and behavior external to viewpoint v need to be expressed through possible state and behavior. Thus, models cannot specify only mandatory behavior and states; furthermore, even though $\mathcal{M}$ normally cannot be expected to be Platonic, by *pretending* it is Platonic (i.e., by collecting all priority-based obligations as in (5)) we detect and locate inconsistencies, if desired. In this respect our semantics deviates significantly from $\neg_{\mathrm{A}}$ and $\neg_{\mathrm{C}}$ since $L \cap \neg_{\mathrm{A}} L = \{\}$ and $U \cup \neg_{\mathrm{C}} U = V$ hold for any preorder $(V, \leq)$. Additionally, our interpretation of $\neg$ respects both the priority preorder and single-views' autonomy to the extent possible: under the assumption that the world is Platonic, view v accepts the assertion (consistency check) $\neg\phi$ as an obligation iff there is a view v' with equal or higher (lower) priority that actually verifies the assertion (consistency check) $\neg\phi$ in its model.

Crucially, our lift of single-view technology preserves soundness of (stepwise) refinement.

Theorem 6 (Lift of sound refinement) *For each* $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$ *and* $\phi \in \mathcal{L}$*, if* $\mathcal{N} \prec \mathcal{M}$*, then*

$$\{|\mathcal{M} : \phi|\} \;\leq\; \{|\mathcal{N} : \phi|\} \qquad \text{in } \mathsf{M}_{(V,\leq)}. \tag{12}$$

Proof: Let $v \in \{|\mathcal{M} : \phi|\}^{\mathrm{a}}$. Then there exists some $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'} \models^{\mathrm{a}} \phi$. But then $\mathcal{N}_{v'} \prec \mathcal{M}_{v'}$ implies $\mathcal{N}_{v'} \models^{\mathrm{a}} \phi$, by property #8, and therefore $v \in \{|\mathcal{N} : \phi|\}^{\mathrm{a}}$. The proof for the second statement is dual. ∎

```
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 };
    }
  }
}
```

Figure 4. Model-checking algorithm for computing the set $\{|\mathcal{M} : \phi|\}^{\mathrm{a}}$. The call `check(M[v], phi)` decides whether $\mathcal{M}_v \models^{\mathrm{a}} \phi$.

The significance of this theorem is that assertion and consistency checking in (5) as well as the detection and location of inconsistencies using (6) are preserved under actual refinements of some or all of the viewpoints, *regardless of whether this happens in a Platonic or a non-Platonic world*. Thus, stake-holders may use familiar sound technology for their model checks — such as semantic laws, proof theory, and abstraction techniques — and all analysis results remain relevant for all refinements. Our lift preserves even the model-checking engine. In computing the denotations $\{|\mathcal{M} : \phi|\}^{\mathrm{m}}$, it is intuitively clear that the priority preorder efficiently guides the use of a single-view model checker to drive that computation. For $\{|\mathcal{M} : \phi|\}^{\mathrm{a}}$, the algorithm is depicted in Figure 4. It is clear how to dualize this algorithm for computing $\{|\mathcal{M} : \phi|\}^{\mathrm{c}}$, and we omit its description.

Theorem 7 (Lift of model checker) *The correctness of the decision procedure* `check(M[v], phi)` *implies that the algorithm in Figure 4 terminates and that* `L` *equals* $\{|\mathcal{M} : \phi|\}^{\mathrm{a}}$ *upon program termination. If the underlying three-valued model-checking framework is based on Kripke structures [4] or labeled transition systems [30, 23, 18], then* `check(M[v], phi)` *can be implemented as an instrumented call to a conventional model checker such as SMV or SPIN.*

Proof: See the Appendix.

The complexity of computing $\{|\mathcal{M} : \phi|\}^{\mathrm{m}}$ depends on the complexity of deciding $\mathcal{M}_v \models^{\mathrm{m}} \phi$; the cost of computing and specifying single-view models $\mathcal{M}_v$; and the structure of the priority preorder $(V, \leq)$ — its width, height, etc. In the worst case, the algorithm of Figure 4 needs to make $|V|$ many calls to `check(M[v], phi)`. Not only does

this algorithm extend the reach of multiple-valued model checking from self-dual [7, 6] to arbitrary preorders, it may also dramatically improve the algorithms of [7, 6] — which compute over the lattice $\mathsf{L}(V,\leq)$ — since $|\mathsf{L}(V,\leq)|$ may be exponential in $|V|$.

4. Multiple-valued modal logic

Existing work on multiple-valued modal logics either considers a Platonic world whose models have mandatory state and behavior only [16] or presents single-view models as multiple-valued specifications to begin with [15]. Fitting [16] presents a semantics and proof theory of modal logic, where state properties and state transitions of models take on values in some finite, distributive lattice $\mathsf{L}(V,\leq)$. Fitting's models $\mathcal{M} = (\Sigma, R, L)$ of type $(V,\leq)$ have state transitions $R\colon \Sigma\times\Sigma \to \mathsf{L}(V,\leq)$ and labelings $L\colon \Sigma\times\mathtt{AP} \to \mathsf{L}(V,\leq)$ that map into $\mathsf{L}(V,\leq)$; if V is a singleton $\{*\}$, these models are ordinary Kripke structures where $\{*\}$ denotes truth (mandatory state and behavior) and $\{\}$ denotes falsity (disallowed state and behavior). We extend Fitting's multiple-valued models and their multiple-valued compositional semantics [16] to under-specified models.

Definition 8 (Multiple-valued Kripke structures) *A* multiple-valued Kripke structure (mvKS) of type $(V,\leq)$ *is a pair* $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$ *of Fitting models of type* $(V,\leq)$ *with* $\mathcal{M}^{\mathrm{m}} = (\Sigma, R^{\mathrm{m}}, L^{\mathrm{m}})$, $\mathrm{m} \in \{\mathrm{a},\mathrm{c}\}$, *such that* $R^{\mathrm{a}}(s,s') \leq R^{\mathrm{c}}(s,s')$ *and* $L^{\mathrm{a}}(s,y) \leq L^{\mathrm{c}}(s,y)$ *for all* $s,s' \in \Sigma$ *and* $y \in \mathtt{AP}$.

A property semantics for mvKSs is given in Figure 5, where environments ρ^{m} have type $\mathrm{var} \to (\Sigma \to \mathsf{L}(V,\leq))$. Note the treatment of negation, the meaning of $\neg\phi$ in mode m is the set complement of the meaning of ϕ in mode $\neg\mathrm{m}$; and fixed points $\mathrm{lfp}^{\mathrm{a}}\, F^{\mathrm{a}}$ and $\mathrm{lfp}^{\mathrm{c}}\, F^{\mathrm{c}}$, which are least fixed points in $(\mathsf{L}(V,\leq),\subseteq)$ and $(\mathsf{U}(V,\leq),\subseteq)$ (respectively).

Definition 9 (Induced three-valued Kripke structures) *For a mvKS* $(\mathcal{M}^{\mathrm{a}}, \mathcal{M}^{\mathrm{c}})$ *of type* $(V,\leq)$ *with* $\mathcal{M}^{\mathrm{m}} = (\Sigma, R^{\mathrm{m}}, L^{\mathrm{m}})$ *and any* $v \in V$, *we define a pair of Kripke structures* $\mathcal{M}_v \stackrel{\mathrm{def}}{=} (\mathcal{M}^{\mathrm{a}}_v, \mathcal{M}^{\mathrm{c}}_v)$ *via functions* $\pi^{\mathrm{a}}_v\colon \mathsf{L}(V,\leq) \to \mathsf{L}(\{*\})$ *and* $\pi^{\mathrm{c}}_v\colon \mathsf{U}(V,\leq) \to \mathsf{U}(\{*\})$ *which map any set that contains* v *to* $\{*\}$ *and any other set to* $\{\}$. *We set*

$$\mathcal{M}^{\mathrm{m}}_v \stackrel{\mathrm{def}}{=} (\Sigma, \pi^{\mathrm{m}}_v \circ R^{\mathrm{m}}, \pi^{\mathrm{m}}_v \circ L^{\mathrm{m}}) \tag{13}$$

for each $\mathrm{m} \in \{\mathrm{a},\mathrm{c}\}$. *These Kripke structures retain the initial state* i *of the mvKS, if applicable.*

Proposition 7 (Priorities as refinements) *The models* $\mathcal{M}_v$ *of (13) are three-valued Kripke structures. The identity relation on states makes this collection a Platonic world.*

$$\begin{aligned}
[\![\, Z \,]\!]^{\mathrm{m}}_\rho\, s &\stackrel{\mathrm{def}}{=} \rho^{\mathrm{m}}(Z)\, s \\
[\![\, y \,]\!]^{\mathrm{m}}_\rho\, s &\stackrel{\mathrm{def}}{=} L^{\mathrm{m}}(s,y) \\
[\![\, \neg\phi \,]\!]^{\mathrm{m}}_\rho\, s &\stackrel{\mathrm{def}}{=} V \setminus [\![\, \phi \,]\!]^{\neg\mathrm{m}}_\rho\, s \\
[\![\, \phi_1 \wedge \phi_2 \,]\!]^{\mathrm{m}}_\rho\, s &\stackrel{\mathrm{def}}{=} [\![\, \phi_1 \,]\!]^{\mathrm{m}}_\rho\, s \cap [\![\, \phi_2 \,]\!]^{\mathrm{m}}_\rho\, s \\
[\![\, \mathsf{EX}\,\phi \,]\!]^{\mathrm{m}}_\rho\, s &\stackrel{\mathrm{def}}{=} \bigcup_{s'\in\Sigma} R^{\mathrm{m}}(s,s') \cap [\![\, \phi \,]\!]^{\mathrm{m}}_\rho\, s' \\
[\![\, \mu Z.\phi \,]\!]^{\mathrm{m}}_\rho &\stackrel{\mathrm{def}}{=} \mathrm{lfp}^{\mathrm{m}}\, F^{\mathrm{m}};\ \text{where } F^{\mathrm{m}}(A) \stackrel{\mathrm{def}}{=} [\![\, \phi \,]\!]^{\mathrm{m}}_{\rho^{\mathrm{m}}[Z\mapsto A]}.
\end{aligned}$$

Figure 5. Property semantics for multiple-valued Kripke structures.

Proof: See the Appendix.

The collection of models $\mathcal{M} = (\mathcal{M}_v)_{v\in V}$ of (13) defines a multiple-valued semantics $\{\!|\mathcal{M}\colon\phi|\!\}^{\mathrm{m}}_\rho$ through Figure 2 and (5). We call a model $\mathcal{M}$ *finitary* if the syntactic approximations $\mu_m Z.\phi$ ($m \geq 0$) [3] of least fixed points $\mu Z.\phi$ are sound and complete in each model $\mathcal{M}_v$ for $\models^{\mathrm{a}}$ and $\models^{\mathrm{c}}$.

Theorem 8 (Soundness & completeness of lift) *Let each model* $\mathcal{M}_v$ *of (13) be finitary and* $\mathrm{m} \in \{\mathrm{a},\mathrm{c}\}$. *Then*

$$\{\!|\mathcal{M}\colon\phi|\!\}^{\mathrm{m}}_\rho = [\![\, \phi \,]\!]^{\mathrm{m}}_\rho\, i. \tag{14}$$

Proof: See the Appendix.

We obtain a sound notion of refinement for mvKSs that is simply the point-wise lift of the refinement of one-letter Kripke MTSs [23].

Corollary 1 (Soundness of refinement) *Let* $\mathcal{M}$ *and* $\mathcal{N}$ *be mvKSs of type* $(V,\leq)$ *with initial states* i *and* j *(respectively) such that* $\mathcal{N} \prec \mathcal{M}$. *For all* ρ *and* ϕ,

$$[\![\, \phi \,]\!]^{\mathrm{c}}_\rho\, j \subseteq [\![\, \phi \,]\!]^{\mathrm{c}}_\rho\, i \quad \text{and} \quad [\![\, \phi \,]\!]^{\mathrm{a}}_\rho\, j \supseteq [\![\, \phi \,]\!]^{\mathrm{a}}_\rho\, i. \tag{15}$$

Proof: This follows from Theorems 6 and 8. ∎

Note the mode of the ordering in (15): assertions that are validated on abstractions remain valid on refinements; checks that are consistent on a refinement are also consistent on its abstraction. MvKSs are under-specified versions of Fitting's models, since the latter models correspond to those mvKSs, where $\mathcal{M}^{\mathrm{a}}$ equals $\mathcal{M}^{\mathrm{c}}$. In that case, each $\mathcal{M}_v$ corresponds to a Kripke structure.

Corollary 2 (Fitting's semantics) *Let* $\mathcal{M}^{\mathrm{a}}$ *equal* $\mathcal{M}^{\mathrm{c}}$. *If* ϕ *is negation-free, then the semantics* $[\![\, \phi \,]\!]^{\mathrm{a}}_\rho$ *of Figure 5 equals Fitting's semantics.*

Proof: See the Appendix.

For Fitting's models and semantics, a weaker version of Theorem 8 can be proved in mode a and for negation-free formulas only, where the equality in (14) turns into $\subseteq$ only. The restriction to negation-free formulas and the weakening of equality are due to the fact that $v \leq v'$ then implies that $\mathcal{M}^{\mathrm{a}}_{v'}$ is a simulation of $\mathcal{M}^{\mathrm{a}}_{v}$ that preserves atomic properties [33], but such simulations are *uni*-directional and preserve *universal* properties only. Fitting's models and semantics are also used by Chechik and Easterbrook [15, 7], except that they choose a negation operator that satisfies the axioms of Figure 3 (right). By Theorem 3, they implicitly assume and choose some idempotent anti-tone map $i\colon (V,\leq) \to (V,\leq)$. Thus, we may compare our semantics to the one of Chechik and Easterbrook [7] only if there exists such a map i, $\mathcal{M}^{\mathrm{a}}$ equals $\mathcal{M}^{\mathrm{c}}$, and negation is defined as in (4). In re-defining $\neg\mathrm{a} \stackrel{\text{def}}{=} \mathrm{a}$, one can therefore re-interpret the semantics of Figure 5 in mode a only. If i satisfies

$$\forall\, (L,U) \in \mathsf{M}_{(V,\leq)},\ v \in L \text{ iff } i(v) \notin U \qquad (16)$$

then it is not hard to see that this re-defined semantics coincides with our $[\![\cdot]\!]^{\mathrm{a}}_{\rho}$. In fact, this equality requires (16) to hold for all elements of $\mathsf{M}_{(V,\leq)}$ that are denotations of formulas. However, it is unlikely that a heuristically chosen i meets condition (16). If we take $L = U = \{v\}$ in Example 4.2, then choosing i to be id we get $v \in L$ and $i(v) \in U$. A meaningful comparison of the performance of the tools in [15] with that of the algorithm in Figure 4 can therefore only be conducted for choices of i that meet (16).

5. Conclusions

We gave axioms for assertion-consistency lattices and three-valued model-checking frameworks and showed that these notions are intimately connected and occur naturally in property-verification, proof theory, and multiple-viewpoint analysis of under-determined models. We characterized finite, distributive AC-lattices (and their symmetric versions, DeMorgan lattices) through preorders endowed with an (idempotent anti-tone) order-isomorphism. We demonstrated that three-valued model checking and AC-lattices as their denotation spaces can be systematically lifted to property verification and requirement elicitation under multiple points of view. This lift applies to the semantics of negation, refinement and abstraction, model-checking algorithms, and other important model checking techniques such as fairness [13, 22]. We compared our approach to Fitting's multiple-valued modal logic [16] (within which sound abstraction-based model checking is limited to universal properties) and its variation proposed by Chechik and Easterbrook [7] (where the denotation space requires a self-dual partial order with an idempotent anti-tone order-isomorphism). For a multiple-viewpoint analysis based on a preorder of priorities, these two semantics are therefore ill-suited. Finally, we emphasize that our three-valued approach not only ensures the instrumented use of single-view model checkers — driven by a priority preorder — and property preservation and sound refinement for logics with unrestricted negation and quantification, it also allows for the efficient computation of sound abstractions (e.g. [18]) which, by construction, can be used to verify assertions and to refute consistency checks.

In future work, we plan to extend the language of priorities to more expressive formalisms for the design and analysis of distributed software engineering systems.

References

[1] S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Oxford Univ. Press, 1994.

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

[3] J. C. Bradfield. *Verifying Temporal Properties Of Systems*. Birkhäuser, Boston, Mass., 1991.

[4] G. Bruns and P. Godefroid. Model Checking Partial State Spaces with 3-Valued Temporal Logics. In *Proceedings of the 11th Conference on Computer Aided Verification*, volume 1633 of *Lecture Notes in Computer Science*, pages 274–287. Springer Verlag, July 1999.

[5] G. Bruns and P. Godefroid. Generalized Model Checking: Reasoning about Partial State Spaces. In *Proceedings of CONCUR'2000 (11th International Conference on Concurrency Theory)*, volume 1877 of *Lecture Notes in Computer Science*, pages 168–182. Springer Verlag, August 2000.

[6] M. Chechik, B. Devereux, S. Easterbrook, A. Y. C. Lai, and V. Petrovykh. Efficient Multi-valued Model-Checking Using Lattice Representations. In K. G. Larsen and M. Nielsen, editors, *Proceedings of CONCUR'2000 (11th International Conference on Concurrency Theory)*, volume 2154 of *Lecture Notes in Computer Science*, pages 441–455. Springer Verlag, August 2001.

[7] M. Chechik, S. M. Easterbrook, and V. Petrovykh. Model-Checking over Multi-Valued Logics. In J. N. Oliveira and P. Zave, editors, *Proceedings, Formal Methods Europe (FME-01)*, volume 2021, pages 72–98, Berlin, Germany, 12-16 March 2001.

[8] E. M. Clarke and E. A. Emerson. Synthesis of synchronization skeletons for branching time temporal logic. In D. Kozen, editor, *Logic of Programs Workshop*, number 131 in LNCS. Springer Verlag, 1981.

[9] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, January 2000.

[10] E. M. Clarke, D. E. Long, and K. L. McMillan. Compositional Model Checking. In *Proceedings of the Fourth Annual Symposium on Logic in Computer Science*, pages 353–361, Washington D. C., 1989. IEEE Computer Society Press.

[11] E.M. Clarke, O. Grumberg, and D.E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, 1994.

[12] D. Dams. *Abstract interpretation and partition refinement for model checking*. PhD thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.

[13] D. Dams, R. Gerth, and O. Grumberg. Fair Model Checking Of Abstractions. In M. Leuschel, A. Podelski, C.R. Ramakrishnan, and U. Ultes-Nitsche, editors, *Proceedings of the Workshop on Verification and Computational Logic (VCL'2000)*, DSSE-TR-2000-6. University of Southhampton, July 2000.

[14] 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.

[15] S. M. Easterbrook and M. Chechik. A Framework for Multi-Valued Reasoning over Inconsistent Viewpoints. In *Proceedings, 23rd International Conference on Software Engineering (ICSE-01)*, pages 411–420, Toronto, Canada, May 12-19 2001. IEEE Computer Society Press.

[16] M. Fitting. Many-valued modal logics II. *Fundamenta Informaticae*, 17:55–73, 1992.

[17] M. C. Fitting. Bilattices in Logic Programming. In *The 20th International Symposium on Multiple-Valued Logic*, pages 238–246. IEEE, 1990.

[18] P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based Model Checking using Modal Transition Systems. In *Proceedings of the International Conference on Theory and Practice of Concurrency*, volume 2154 of *Lecture Notes in Computer Science*, pages 426–440. Springer Verlag, August 2001.

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

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

[21] G. Holzmann. The model checker SPIN. *IEEE Transactions on Software Engineering*, 23:279–295, 1997.

[22] M. Huth. Model checking modal transition systems using Kripke structures. In *Third International Workshop on Verification, Model Checking and Abstract Interpretation*, Lecture Notes in Computer Science, Venice, Italy, January 21-22 2002. Springer Verlag. To appear.

[23] M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In Sands D., editor, *Proceedings of the European Symposium on Programming (ESOP'2001)*, pages 155–169. Springer Verlag, April 2001.

[24] M. Huth and S. Pradhan. Model-Checking View-Based Partial Specifications. In S. Brookes and M. Mislove, editors, *Electronic Notes in Theoretical Computer Science*, volume 45. Elsevier Science Publishers, 2001.

[25] M. Jackson. *Software Requirements & Specifications*. Addison-Wesley, ACM Press, 1995.

[26] K.L. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.

[27] S. C. Kleene. *Introduction to Metamathematics*. Van Nostrand, 1952.

[28] O. Kupferman and M. Vardi. Module checking. In *Proceedings of the Eight International Conference on Computer Aided Verification*, pages 75–86. Springer Verlag, 1996.

[29] K. G. Larsen. Modal Specifications. In J. Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, number 407 in Lecture Notes in Computer Science, pages 232–246. Springer Verlag, June 12–14 1989. International Workshop, Grenoble, France.

[30] K. G. Larsen and B. Thomsen. A Modal Process Logic. In *Third Annual Symposium on Logic in Computer Science*, pages 203–210. IEEE Computer Society Press, 1988.

[31] J. P. Quielle and J. Sifakis. Specification and verification of concurrent systems in cesar. In *Proceedings of the fifth International Symposium on Programming*, 1981.

[32] M. Sagiv, T. Reps, and R. Wilhelm. Parametric Shape Analysis via 3-Valued Logic. In *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of programming languages*, pages 105–118, January 20-22, San Antonio, Texas 1999.

[33] D. A. Schmidt. Binary relations for abstraction and refinement. *Elsevier Electronic Notes in Computer Science*, November 1999. Workshop on Refinement and Abstraction, Osaka, Japan. To appear.

[34] K. Wiegers. First Things First: Prioritizing Requirements. *Software Development Online*, September 1999.

[35] R. R. Young. *Effective Requirements Practices*. Information Technology Series. Addison-Wesley, 2001.

Proof of Proposition 2: First, the axioms for a DeMorgan lattice $(\mathcal{L}, \leq, \neg)$ in Figure 3 clearly imply that $(\mathcal{L}, \leq, \neg, \mathcal{L}, \leq, \neg)$ meets the axioms of an AC-lattice. Conversely, consider an AC-lattice, where $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}, \neg_{\mathrm{a}})$ equals $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}, \neg_{\mathrm{c}})$. Then the axioms for AC-lattices readily imply the first and last axiom of DeMorgan lattices. The second and third axioms follow from the fact that $\neg_{\mathrm{a}} \colon (\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}) \to (\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}{}^{\mathrm{op}})$ is an order-isomorphism with $\neg_{\mathrm{c}} \colon (\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}{}^{\mathrm{op}}) \to (\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ as order-inverse. ∎

Proof of Theorem 1:

1. Let $\mathrm{m} \in \{\mathrm{a}, \mathrm{c}\}$. First, given $\mathcal{M} \models^{\mathrm{m}} \neg\neg\phi$, we have $\mathcal{M} \not\models^{\neg\mathrm{m}} \neg\phi$, i.e. $\mathcal{M} \models^{\mathrm{m}} \phi$. Thus, $\neg\neg\phi \leq_{\mathrm{m}} \phi$. Similarly, we show $\phi \leq_{\mathrm{m}} \neg\neg\phi$. Therefore, $[\phi]_{\mathrm{m}} =$

$[\neg\neg\phi]_{\mathrm{m}}$, but the latter equals $\neg_{\neg\mathrm{m}}\neg_{\mathrm{m}}[\phi]_{\mathrm{m}}$ by definition. Second, let $[\phi]_{\mathrm{m}} \leq_{\mathrm{m}} [\psi]_{\mathrm{m}}$ with ϕ' and ψ' as respective witnesses. If $\mathcal{M} \models^{\neg\mathrm{m}} \neg\psi'$, then we have $\mathcal{M} \not\models^{\mathrm{m}} \psi'$. Since $\phi' \leq_{\mathrm{m}} \psi'$, we conclude $\mathcal{M} \not\models^{\mathrm{m}} \phi'$, i.e. $\mathcal{M} \models^{\neg\mathrm{m}} \neg\phi'$. Thus, $\neg_{\mathrm{m}}[\psi]_{\mathrm{m}} = [\neg\psi]_{\neg\mathrm{m}} \leq_{\neg\mathrm{m}} [\neg\phi]_{\neg\mathrm{m}} = \neg_{\mathrm{m}}[\phi]_{\mathrm{m}}$. Third, we claim that the meet of $[\phi]_{\mathrm{m}}$ and $[\psi]_{\mathrm{m}}$ is $[\phi \wedge \psi]_{\mathrm{m}}$. Since $\phi \wedge \psi \leq_{\mathrm{m}} \phi, \psi$ we know that $[\phi \wedge \psi]_{\mathrm{m}}$ is a lower bound of $[\phi]_{\mathrm{m}}$ and $[\psi]_{\mathrm{m}}$. If $[\eta]_{\mathrm{m}}$ is another such lower bound, then there are $\eta', \eta'' \in [\eta]_{\mathrm{m}}$ and $\phi'' \in [\phi]_{\mathrm{m}}$ and $\psi'' \in [\psi]_{\mathrm{m}}$ such that $\eta' \leq_{\mathrm{m}} \phi''$ and $\eta'' \leq_{\mathrm{m}} \psi''$. Given $\mathcal{M} \models^{\mathrm{m}} \eta$, we have $\mathcal{M} \models^{\mathrm{m}} \eta'$ and $\mathcal{M} \models^{\mathrm{m}} \eta''$, for $\eta', \eta'' \in [\eta]_{\mathrm{m}}$. Then $\eta' \leq_{\mathrm{m}} \phi$ and $\eta'' \leq_{\mathrm{m}} \psi$ follow and imply $\mathcal{M} \models^{\mathrm{m}} \phi$ and $\mathcal{M} \models^{\mathrm{m}} \psi$ (respectively). Thus, $\mathcal{M} \models^{\mathrm{m}} \phi \wedge \psi$ shows $\eta \leq_{\mathrm{m}} \phi \wedge \psi$ and so $[\eta]_{\mathrm{m}} \leq_{\mathrm{m}} [\phi \wedge \psi]_{\mathrm{m}}$ follows.

2. By property #9, $[\phi]_{\mathrm{a}} = [\phi]_{\mathrm{c}}$ for all ϕ, so $\mathcal{L}_{\mathrm{a}} = \mathcal{L}_{\mathrm{c}}$ and $\leq_{\mathrm{a}}$ equals $\leq_{\mathrm{c}}$. We then apply Proposition 2. ∎

Proof of Proposition 3:

1. The proof that $\mathsf{U}(\cdot)$ is a monotone functor is routine, noting that $U = \bigcap_{v \notin U} \epsilon_V(v)$ for each $U \in \mathsf{U}(V, \leq)$, so $\overline{(f)}_{\mathcal{U}}(U) \stackrel{\text{def}}{=} \bigvee\{f(v) \mid v \notin U\}$.

2. The first three equations are immediate. Finally, $\neg_{\mathrm{a}} \circ \mathsf{L}(f) \circ \neg_{\mathrm{c}}$ is a sup-map, so it suffices to show $(\neg_{\mathrm{a}} \circ \mathsf{L}(f) \circ \neg_{\mathrm{c}}) \circ \epsilon_V = \epsilon_W \circ f$. But $(\neg_{\mathrm{a}} \circ \mathsf{L}(f) \circ \neg_{\mathrm{c}}) \circ \epsilon_V = \neg_{\mathrm{a}} \circ (\mathsf{L}(f) \circ \eta_V) = \neg_{\mathrm{a}} \circ (\eta_W \circ f) = \epsilon_W \circ f$.

3. Clearly, automorphisms are lifted by functors, so $f \mapsto \mathsf{L}(f) \colon \mathrm{Aut}(V, \leq) \to \mathrm{Aut}(\mathsf{L}(V, \leq))$ is an injection, as the functor is faithful. Conversely, given $g \in \mathrm{Aut}(\mathsf{L}(V, \leq))$, the map $\underline{g \circ \eta_V} \colon (V, \leq) \to \mathsf{L}((V, \leq))$ is monotone and so $\overline{(g \circ \eta_V)}_{\mathcal{L}}$ is well defined, but $g = \overline{(g \circ \eta_V)}_{\mathcal{L}}$ since g is also a sup-map ρ with $\rho \circ \eta_V = g \circ \eta_V$. The proof for $\mathsf{U}(\cdot)$ follows from this and $\mathsf{U}(f) = \backslash_{\mathrm{a}} \circ \mathsf{L}(f) \circ \backslash_{\mathrm{c}}$.

∎

Proof of Theorem 2: Given a preorder $(V, \leq)$, the tuple $(\mathsf{L}(V, \leq), \subseteq, \backslash_{\mathrm{a}}, \mathsf{U}(V, \leq), \subseteq, \backslash_{\mathrm{c}})$ is an instance of Example 3, where $\mathsf{U}(V, \leq)$ is the collection of open and $\mathsf{L}(V, \leq)$ the collection of closed subsets of V. Conversely, by Stone duality there exists an order-isomorphism $\Phi \colon (\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}) \cong \mathsf{L}(V, \leq)$ [1] for some finite partial order $(V, \leq)$ since $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}})$ is a finite, distributive lattice. But then $\backslash_{\mathrm{c}} \circ \Phi \circ \neg_{\mathrm{c}} \colon (\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}{}^{\mathrm{op}}) \to (\mathsf{U}(V, \leq), \supseteq)$ is an order-isomorphism as well. Thus, we may assume $(\mathcal{L}_{\mathrm{a}}, \leq_{\mathrm{a}}) = \mathsf{L}(V, \leq)$ and $(\mathcal{L}_{\mathrm{c}}, \leq_{\mathrm{c}}{}^{\mathrm{op}}) = (\mathsf{U}(V, \leq), \supseteq)$. Since $\neg_{\mathrm{a}}$ preserves complete primes as an order-isomorphism and since the set of complete primes of $(\mathsf{U}(V, \leq), \supseteq)$ is the image of ϵ_V, we infer that for every $v \in V$ there is a unique $i(v) \in V$ with $\neg_{\mathrm{a}}(\eta_V(v)) = \epsilon_V(i(v))$. Since ϵ_V is an order-isomorphism onto its image, $i \colon (V, \leq) \to (V, \leq)$ is monotone. Thus, $\neg_{\mathrm{a}} \circ \eta_V = \epsilon_V \circ i$ implies $\neg_{\mathrm{a}} = \overline{(\epsilon_V \circ i)}_{\mathcal{L}}$. Dually, we infer the existence of a monotone map $j \colon \underline{(V, \leq)} \to (V, \leq)$ with $\neg_{\mathrm{c}} \circ \epsilon_V = \eta_V \circ j$, and so $\neg_{\mathrm{c}} = \underline{(\eta_V \circ j)}_{\mathcal{U}}$. Thus, it suffices to show $j = i^{-1}$. But $\epsilon_V \circ i = \neg_{\mathrm{a}} \circ \eta_V = (\neg_{\mathrm{a}} \circ \backslash_{\mathrm{c}}) \circ \epsilon_V$ implies $\neg_{\mathrm{a}} \circ \backslash_{\mathrm{c}} = \mathsf{U}(i)$. Dually, $\eta_V \circ j = \neg_{\mathrm{c}} \circ \epsilon_V = (\neg_{\mathrm{c}} \circ \backslash_{\mathrm{a}}) \circ \eta_V$ implies $\neg_{\mathrm{c}} \circ \backslash_{\mathrm{a}} = \mathsf{L}(j)$. But $\mathsf{L}(i) = \backslash_{\mathrm{c}} \circ \mathsf{U}(i) \circ \backslash_{\mathrm{a}} = \backslash_{\mathrm{c}} \circ (\neg_{\mathrm{a}} \circ \backslash_{\mathrm{c}}) \circ \backslash_{\mathrm{a}} = \backslash_{\mathrm{c}} \circ \neg_{\mathrm{a}}$. From this we immediately get that $\mathsf{L}(i)$ is the inverse of $\mathsf{L}(j)$. Thus, $j = i^{-1}$. ∎

Proof of Theorem 3:

1. Let $i \colon (V, \leq) \to (V, \leq)$ be an anti-tone idempotent map. The map $\neg \colon \mathsf{L}(V, \leq) \to \mathsf{L}(V, \leq)$, defined in (4), is well defined as i is anti-tone; $\neg$ is clearly anti-tone (with respect to set inclusion). We compute $\neg\neg L = \{i(w) \mid w = i(v) \text{ implies } v \notin V \setminus L\} = \{i(i(v)) \mid v \in L\}$ since i is onto and one-to-one. Thus, $\neg\neg L = L$ and so $\neg$ establishes an order-isomorphism between $\mathsf{L}(V, \leq)$ and its dual. Therefore, $(\mathsf{L}(V, \leq), \subseteq, \neg)$ is a finite, distributive DeMorgan lattice.

2. Given a finite, distributive DeMorgan lattice $(\mathcal{L}, \leq, \neg)$, Stone duality guarantees an order-isomorphism $\phi \colon (\mathcal{L}, \leq) \to (\mathsf{L}(V, \leq), \subseteq)$ for some finite partial order $(V, \leq)$. But then the map $\mathrm{neg} \stackrel{\text{def}}{=} \phi \circ \neg \circ \phi^{-1}$ is anti-tone and idempotent on $\mathsf{L}(V, \leq)$. Thus, it is an order-isomorphism of type $\mathsf{L}(V, \leq) \to \mathsf{L}(V, \leq)^{\mathrm{op}}$ and, therefore, maps complete primes of $\mathsf{L}(V, \leq)$ (all elements of the form $\downarrow v$, $v \in V$) to complete co-primes of $\mathsf{L}(V, \leq)$ (all elements of the form $V \setminus \uparrow v$, $v \in V$). Thus, $\mathrm{neg}(\downarrow v) = V \setminus \uparrow i(v)$ for a unique $i(v)$ in V. It is routine to check that the map $v \mapsto i(v) \colon (V, \leq) \to (V, \leq)$ is anti-tone. Dually, neg maps complete co-primes of $\mathsf{L}(V, \leq)$ to complete primes of $\mathsf{L}(V, \leq)$. Thus, $\mathrm{neg}(V \setminus \uparrow v) = \downarrow j(v)$ for a unique $j(v)$ in V. The map $v \mapsto j(v) \colon (V, \leq) \to (V, \leq)$ is anti-tone. The equation $\downarrow v = \mathrm{neg}(\mathrm{neg}(\downarrow v))$ renders $j(i(v)) = v$ for all $v \in V$. Dually, equation $V \setminus \uparrow v = \mathrm{neg}(\mathrm{neg}(V \setminus \uparrow v))$ yields $i(j(v)) = v$ for all $v \in V$, so i is an isomorphism with j as inverse.

   We claim that $j = i$. We compute $\downarrow v = \mathrm{neg}(\mathrm{neg}(\downarrow v)) = \mathrm{neg}(V \setminus \uparrow i(v)) = \mathrm{neg}(\bigcup\{\downarrow w \mid w \in V \setminus \uparrow i(v)\}) = \bigcap\{\mathrm{neg}(\downarrow w) \mid i(v) \not\leq w\} = \bigcap\{V \setminus \uparrow i(w) \mid i(v) \not\leq w\}$. In particular, v is an element of the latter set. Therefore we have

$$\forall w \in V,\ i(v) \not\leq w \text{ implies } i(w) \not\leq v. \qquad (17)$$

For $w \stackrel{\text{def}}{=} j(v)$, $i(w) = i(j(v)) = v \leq v$ therefore implies $i(v) \leq w = j(v)$. Since i is anti-tone, this results in $v = i(j(v)) \leq i(i(v))$. Suppose that it is not the case that $i(i(v)) \leq v$. Then $v \in V \setminus \uparrow i(i(v))$, i.e. $\downarrow v \subseteq V \setminus \uparrow i(i(v)) = \mathrm{neg}(\downarrow i(v))$. But then $\downarrow i(v) = \mathrm{neg}(\mathrm{neg}(\downarrow i(v))) \subseteq \mathrm{neg}(\downarrow v) = V \setminus \uparrow i(v)$ implies $i(v) \in V \setminus \uparrow i(v)$, a contradiction.

Finally, we show that neg is defined as in (4). Given $L \in \mathsf{L}(V, \leq)$, we have $\mathrm{neg}(L) = \mathrm{neg}(\bigcup_{v' \in L} \downarrow v') = \bigcap_{v' \in L} \mathrm{neg}(\downarrow v') = \bigcap_{v' \in L} V \setminus \uparrow i(v') \stackrel{\text{def}}{=} A$. We claim that A equals $B \stackrel{\text{def}}{=} \{i(v) \mid v \in V \setminus L\}$:

- If $w \in A$, then $v' \in L$ implies $i(v') \not\leq w$, i.e. $i(w) \not\leq v'$ since i is an anti-tone order-isomorphism. Thus, $i(w) \in V \setminus L$ since L is a lower set. Therefore, $w = i(i(w)) \in B$.
- If $w \in B$, then $w = i(v)$ for some $v \in V \setminus L$. Given $v' \in L$, we have $v \not\leq v'$ since $v \in V \setminus L$ and $L \in \mathsf{L}(V, \leq)$. Thus, $i(v') \not\leq i(v) = w$ shows $w \in V \setminus \uparrow i(v')$, i.e. $w \in A$. ∎

Proof of Theorem 7: Before execution of the while-statement, the invariants hold since $L = \{\}$ and $L \cup U = V$. The if-branch removes from L only elements that cannot be in $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{m}}$, due to property #8; it leaves the value of $L \cup U$ invariant. Thus, this branch maintains both invariants. The else-branch only removes v from U which cannot violate the second invariant since v cannot be in $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}}$. In any event, the finite set U gets smaller with each iteration of the while-statement, ensuring termination. Upon termination, U is empty, so the conjunction of both invariants states that $\{\!|\mathcal{M} : \phi|\!\}^{\mathrm{a}}$ equals L. The claims about the instrumented use of standard model checkers follow from work in [5], [18], and [22]. ∎

Proof of Proposition 7: We refer to [23] for a formal definition of refinement of Kripke MTSs. By definition, the identity relation relates initial states. If the set $\pi^{\mathrm{a}}_{v'}(R^{\mathrm{a}}(s, s'))$ is non-empty (must-transition [30, 23]), then v' is contained in the lower set $R^{\mathrm{a}}(s, s')$. Thus, $v \leq v'$ implies $v \in R^{\mathrm{a}}(s, s')$, so $\pi^{\mathrm{a}}_{v}(R^{\mathrm{a}}(s, s'))$ is non-empty as well. Dually, let $\pi^{\mathrm{c}}_{v}(R^{\mathrm{c}}(s, s'))$ be non-empty (may-transition [30, 23]). Then v is contained in the upper set $R^{\mathrm{c}}(s, s')$. Thus, $v \leq v'$ implies $v' \in R^{\mathrm{c}}(s, s')$, so $\pi^{\mathrm{a}}_{v'}(R^{\mathrm{c}}(s, s'))$ is non-empty as well. The arguments for the labeling function are reasoned similar to the previous case. ∎

Proof of Theorem 8:

1. For Z, $[\![Z]\!]^{\mathrm{c}}_{\rho} i = \rho^{\mathrm{c}}(Z)\, i$ which equals $\{v \in V \mid \exists v' \in V : v' \leq v,\ v' \in \rho^{\mathrm{c}}(Z)\, i\}$ since $\rho^{\mathrm{c}}(Z)\, i$ is an upper set in $(V, \leq)$. But the latter set is $\{v \in V \mid \exists v' \in V : v' \leq v,\ \mathcal{M}_{v'} \models^{\mathrm{c}}_{\rho_{v'}} Z\}$, which is $\{\!|\mathcal{M} : Z|\!\}^{\mathrm{c}}_{\rho}$. The proof for mode a is dual.

2. For y, $[\![y]\!]^{\mathrm{a}}_{\rho} i = L^{\mathrm{a}}(i, y)$ which equals $\{v \in V \mid \exists v' \in V : v \leq v',\ v' \in L^{\mathrm{a}}(i, y)\}$ since $L^{\mathrm{a}}(i, y)$ is a lower set in $(V, \leq)$. But the latter set is $\{v \in V \mid \exists v' \in V : v \leq v',\ \mathcal{M}_{v'} \models^{\mathrm{a}}_{\rho_{v'}} y\}$, which is $\{\!|\mathcal{M} : y|\!\}^{\mathrm{a}}_{\rho}$. The proof for mode c is dual.

3. For $\neg\phi$, $[\![\neg\phi]\!]^{\mathrm{m}}_{\rho} i = V \setminus [\![\phi]\!]^{\neg \mathrm{m}}_{\rho} i$ which, by induction, equals $V \setminus \{\!|\mathcal{M} : \phi|\!\}^{\neg \mathrm{m}}_{\rho}$. By Theorem 5.2, this equals $\{\!|\mathcal{M} : \neg\phi|\!\}^{\mathrm{m}}_{\rho}$.

4. For $\mathsf{EX}\,\phi$, we show this for mode a only; the proof for mode c is dual. First, let $v \in [\![\mathsf{EX}\,\phi]\!]^{\mathrm{a}}_{\rho} i$. So there exists some $i' \in \Sigma$ with $v \in R^{\mathrm{a}}(i, i')$ and $v \in [\![\phi]\!]^{\mathrm{a}}_{\rho} i'$. By induction, the latter implies[14] $v \in \{\!|\mathcal{M}[i \mapsto i'] : \phi|\!\}^{\mathrm{a}}_{\rho}$. So there exists some $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'}[i \mapsto i'] \models^{\mathrm{a}}_{\rho_{v'}} \phi$. Then Proposition 7 and property #8 render $\mathcal{M}_{v}[i \mapsto i'] \models^{\mathrm{a}}_{\rho_{v}} \phi$. Since $v \in R^{\mathrm{a}}(i, i')$, we infer $\mathcal{M}_{v} \models^{\mathrm{a}}_{\rho_{v}} \mathsf{EX}\,\phi$, so $v \in \{\!|\mathcal{M} : \mathsf{EX}\,\phi|\!\}^{\mathrm{a}}_{\rho}$ since $v \leq v$. Conversely, let $w \in \{\!|\mathcal{M} : \mathsf{EX}\,\phi|\!\}^{\mathrm{a}}_{\rho}$. Then there exists $w' \in V$ with $w \leq w'$ and $\mathcal{M}_{w'} \models^{\mathrm{a}}_{\rho_{w'}} \mathsf{EX}\,\phi$. Proposition 7 and property #8 then imply $\mathcal{M}_{w} \models^{\mathrm{a}}_{\rho_{w}} \mathsf{EX}\,\phi$. So there exists some $i'' \in \Sigma$ with $w \in R^{\mathrm{a}}(i, i'')$ and $\mathcal{M}_{w}[i \mapsto i''] \models^{\mathrm{a}}_{\rho_{w}} \phi$. The latter and $w \leq w$ imply $w \in \{\!|\mathcal{M}[i \mapsto i''] : \phi|\!\}^{\mathrm{a}}_{\rho}$ which, by induction, equals $[\![\phi]\!]^{\mathrm{a}}_{\rho} i''$. Thus, $w \in R^{\mathrm{a}}(i, i'')$ implies $w \in [\![\mathsf{EX}\,\phi]\!]^{\mathrm{a}}_{\rho}$.

5. For $\mu Z.\phi$, let $v \in [\![\mu Z.\phi]\!]^{\mathrm{a}}_{\rho} i$. Since the model is finitary, there is some $k \geq 0$ such that v is in $[\![\mu_k Z.\phi]\!]^{\mathrm{a}}_{\rho} i$ which, by induction, equals $\{\!|\mathcal{M} : \mu_k Z.\phi|\!\}^{\mathrm{a}}_{\rho}$. Therefore, there is some $v' \in V$ with $v \leq v'$ and $\mathcal{M}_{v'} \models^{\mathrm{a}}_{\rho_{v'}} \mu_k Z.\phi$. But then $\mathcal{M}_{v'} \models^{\mathrm{a}}_{\rho_{v'}} \mu Z.\phi$ follows from the monotonicity of the least-fixed-point iteration. So $v \leq v'$ implies $v \in \{\!|\mathcal{M} : \mu Z.\phi|\!\}^{\mathrm{a}}_{\rho}$. Conversely, let $w \in \{\!|\mathcal{M} : \mu Z.\phi|\!\}^{\mathrm{a}}_{\rho}$. Then there exists some $w' \in V$ with $w \leq w'$ and $\mathcal{M}_{w'} \models^{\mathrm{a}}_{\rho_{w'}} \mu Z.\phi$. But then there is some $l \leq 0$ with $\mathcal{M}_{w'} \models^{\mathrm{a}}_{\rho_{w'}} \mu_l Z.\phi$. Therefore, $w \in \{\!|\mathcal{M} : \mu_l Z.\phi|\!\}^{\mathrm{a}}_{\rho}$ which, by induction, equals $[\![\mu_l Z.\phi]\!]^{\mathrm{a}}_{\rho} i$, which is contained in $[\![\mu Z.\phi]\!]^{\mathrm{a}}_{\rho} i$. The proof for mode c is dual. ∎

Proof of Corollary 2: If ϕ is negation-free, then the clause for negation in Figure 5 is never invoked and all other clauses render Fitting's semantics as in [16]. ∎

[14] We write $[i \mapsto i']$ to update the initial state from i to i'.