

Lifting assertion and consistency checkers from single to multiple viewpoints

Michael Huth, Imperial College, London
Shekhar Pradhan, Central Missouri State University, Warrensburg

Relevant papers: see www.doc.ic.ac.uk/~mrh/research.html

This talk: see www.doc.ic.ac.uk/~mrh/ucl02.ps

1

Outline

We define viewpoints as partial models of first-order logic that have only limited access to a global signature and interpret global terms and formulas over such viewpoints.

We decompose this single-view semantics into two semantics whose consensus recovers the original one.

A translation of formulas into negation normal form then reduces our three-valued semantics to the standard semantics of first-order logic.

We then systematically lift single-view model-checking frameworks to model-checking under multiple points of view.

2

First-order logic signature and syntax

Terms t and formulas ϕ are defined by the grammar

$$\begin{aligned} t & ::= x \mid f(t, t, \dots, t) \\ \phi & ::= \top \mid P(t, t, \dots, t) \mid \neg\phi \mid \phi \wedge \phi \mid \exists x \phi, \end{aligned}$$

where x , f , and P range over sets of variables \mathcal{X} , function symbols \mathcal{F} , and predicate symbols \mathcal{P} (respectively), resulting in the signature

$$\Sigma \stackrel{\text{def}}{=} (\mathcal{X}, \mathcal{F}, \mathcal{P}).$$

3

Partial models

Fixing a nonempty, finite set of elements \mathcal{U} — the global semantic universe — we define models that are partial in that they have access to a part of Σ and \mathcal{U} only.

Definition 4.2.1 [Partial models] A *partial model* \mathcal{M}_v for (Σ, \mathcal{U}) consists of

1. a signature $\Sigma_v = (\mathcal{X}_v, \mathcal{F}_v, \mathcal{P}_v)$ such that $\mathcal{X}_v \subseteq \mathcal{X}$, $\mathcal{F}_v \subseteq \mathcal{F}$, and $\mathcal{P}_v \subseteq \mathcal{P}$;
2. a nonempty set of elements \mathcal{U}_v with $\mathcal{U}_v \subseteq \mathcal{U}$;
3. for all $f \in \mathcal{F}_v$, a (total) function $f^v: \mathcal{U}_v^n \rightarrow \mathcal{U}_v$; and
4. for all $P \in \mathcal{P}_v$, a relation $P^v \subseteq \mathcal{U}_v^n$.

The v in \mathcal{M}_v indicates that this model is a particular “view” of models of sort Σ .

4

Upper powerdomain

For a finite partial order (P, \leq) , the *upper powerdomain of P* , $\mathbf{U}(P)$, is the collection of all nonempty upper sets of P , ordered by *reverse inclusion* \supseteq .

For a monotone function $f: P \rightarrow Q$ between finite partial orders, we define the (total) function $\mathbf{U}(f): \mathbf{U}(P) \rightarrow \mathbf{U}(Q)$ as

$$\mathbf{U}(f)(U) \stackrel{\text{def}}{=} \{q \in Q \mid \text{for some } u \in U, f(u) \leq q\}.$$

$\mathbf{U}(\cdot)$ is a functor on the category of finite partial orders and monotone functions.

Example

1. For the discrete $\mathbb{B} \stackrel{\text{def}}{=} \{\text{false}, \text{true}\}$,
 $\mathbf{U}(\mathbb{B}) = \{\{\text{false}, \text{true}\}, \{\text{false}\}, \{\text{true}\}\}$, where the first one is the least element and the other two are maximal elements. Note that $\mathbf{U}(\mathbb{B}) \cong \mathbf{U}(\mathbf{U}(\mathbb{B}))$.
2. For a finite set \mathcal{U}_v , $\mathbf{U}(\mathcal{U}_v)$ consists of all nonempty subsets of \mathcal{U}_v ordered by \supseteq . The least element of $\mathbf{U}(\mathcal{U}_v)$ is \mathcal{U}_v , and its maximal elements are all singleton sets $\{u\}$ ($u \in \mathcal{U}_v$).
3. For classical equality $=^{\mathbb{B}}: \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$, $\mathbf{U}(=^{\mathbb{B}})$ is a conservative extension of $=^{\mathbb{B}}$ from \mathbb{B} to $\mathbf{U}(\mathbb{B})$ which returns $\{\text{false}, \text{true}\}$ iff at least one of its arguments equals $\{\text{false}, \text{true}\}$.

Propositional logic on $\mathbf{U}(\mathbb{B})$

Let $\neg^{\mathbb{B}}$, $\wedge^{\mathbb{B}}$, and $\vee^{\mathbb{B}}$ be the standard interpretations of negation, conjunction, and n -ary disjunction on \mathbb{B} . We define

$$\neg^s \stackrel{\text{def}}{=} \mathbf{U}(\neg^{\mathbb{B}}) \quad \wedge^s \stackrel{\text{def}}{=} \mathbf{U}(\wedge^{\mathbb{B}}) \quad \vee^s \stackrel{\text{def}}{=} \mathbf{U}(\vee^{\mathbb{B}})$$

as our interpretation of propositional logic on $\mathbf{U}(\mathbb{B})$. This is well defined as any functions on a discrete set are monotone.

We set $\text{true} \stackrel{\text{def}}{=} \{\text{true}\}$, $\text{false} \stackrel{\text{def}}{=} \{\text{false}\}$, and $\mathbf{U} \stackrel{\text{def}}{=} \{\text{false}, \text{true}\}$.

The value \mathbf{U} suggests that truth is *under-determined*.

7

Characterization of propositional logic in $\mathbf{U}(\mathbb{B})$

1. The function \neg^s maps true to false, false to true, and \mathbf{U} to \mathbf{U} .
2. The function $x \wedge^s y$ returns false if x or y equals false; otherwise, if x or y equals \mathbf{U} , it returns \mathbf{U} ; otherwise, it returns true.
3. The expression $\vee_j^s x_j$ returns true if x_j equals true for some j with $1 \leq j \leq n$; otherwise, it returns \mathbf{U} if $x_{j'}$ equals \mathbf{U} for some j' with $1 \leq j' \leq n$; otherwise, it returns false.

8

Semantics of global terms: $\llbracket t \rrbracket_\rho^v \in \mathbf{U}(\mathcal{U}_v)$

$$\llbracket x \rrbracket_\rho^v \stackrel{\text{def}}{=} \begin{cases} \{\rho(x)\} & \text{if } x \in \mathcal{X}_v \\ \mathcal{U}_v & \text{otherwise (why not } \perp?). \end{cases}$$

where $\rho: \mathcal{X}_v \rightarrow \mathcal{U}_v$. Thus, we model the fact that the name x is not known in this view by evaluating it to “possibly any element in this view”. For function symbols, we proceed similarly:

$$\llbracket f(t_1, \dots, t_n) \rrbracket_\rho^v \stackrel{\text{def}}{=} \begin{cases} \{f^v(u_1, \dots, u_n) \mid u_i \in \llbracket t_i \rrbracket_\rho^v\} & \text{if } f \in \mathcal{F}_v \\ \mathcal{U}_v & \text{otherwise.} \end{cases}$$

If $f \in \mathcal{F}_v$, then the semantics of $f(t_1, \dots, t_n)$ above is obtained by applying $\mathbf{U}(\cdot)$ to the interpretation f^v of type $\mathcal{U}_v^n \rightarrow \mathcal{U}_v$ in the partial model.

9

Example

Let $\mathcal{U}_v \stackrel{\text{def}}{=} \{0, 2, 4, 6, \dots, 96, 98\}$.

Suppose that $+^v$ and $*^v$ denote the operations of addition and multiplication (respectively), executed “modulo 100”. For example, $*^v(46, 78) = 24$ and $*^v(78, 0) = 0$.

Let $x \notin \mathcal{X}_v$. Then

$$\llbracket +(6, x) \rrbracket_\rho^v = \{6 + u \pmod{100} \mid u \in \mathcal{U}_v\} = \mathcal{U}_v$$

$$\llbracket *(0, x) \rrbracket_\rho^v = \{0\}.$$

10

Semantics of global formulas: $\llbracket \phi \rrbracket_\rho^v \in \mathbf{U}(\mathbb{B})$

Clearly, $\llbracket \top \rrbracket_\rho^v \stackrel{\text{def}}{=} \text{true}$. For atomic predicates, we need to lift P^v to subsets:

$$\llbracket P(t_1, \dots, t_n) \rrbracket_\rho^v \stackrel{\text{def}}{=} \begin{cases} \text{true} & \text{if } P \in \mathcal{P}_v \ \& \ \llbracket \prod_i t_i \rrbracket_\rho^v \subseteq P^v \\ \text{false} & \text{if } P \in \mathcal{P}_v \ \& \ \llbracket \prod_i t_i \rrbracket_\rho^v \cap P^v = \emptyset \\ \mathbf{U} & \text{otherwise.} \end{cases}$$

The side conditions above can be verified automatically if the sets $\llbracket t_i \rrbracket_\rho^v$ and P^v can be expressed as quantifier-free formulas of first-order logic. If $P \in \mathcal{P}_v$, then the lift above computes $\mathbf{U}(P^v)$.

11

Semantics of remaining connectives

The interpretation of the remaining connectives uses our propositional logic on $\mathbf{U}(\mathbb{B})$:

$$\begin{aligned} \llbracket \neg \phi \rrbracket_\rho^v &\stackrel{\text{def}}{=} \neg^s \llbracket \phi \rrbracket_\rho^v \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket_\rho^v &\stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_\rho^v \wedge^s \llbracket \phi_2 \rrbracket_\rho^v \\ \llbracket \exists x \phi \rrbracket_\rho^v &\stackrel{\text{def}}{=} \bigvee_{u \in \mathcal{U}_v} \llbracket \phi \rrbracket_{\rho[x \mapsto u]}^v, \end{aligned}$$

where $\rho[x \mapsto u]$ contains the same bindings as ρ , except that it binds x to u . For $\exists x \phi$, it does not matter whether x is in \mathcal{X}_v since $\exists x$ binds the name x and thereby makes it “locally known” by extending the current environment ρ .

12

Example

Revisiting the “modulo 100” example, let $>^v$ be the standard interpretation “strictly greater than” of $>$ on \mathcal{U}_v .

The formula $(6 + x) > 4$ evaluates to \mathbb{U} and the formula $(0 * x) > 2$ evaluates to false.

The reason for the former is that some instances of $P^v(u_1, \dots, u_n)$ hold (e.g. $(6 + 0) >^v 4$), but not all of them (e.g. not $(6 + 98) >^v 4$).

Conservative extension of first-order logic

Let \mathcal{M}_v be a partial model for (Σ, \mathcal{U}) such that $\Sigma_v = \Sigma$.

For all ϕ and ρ , the set $\llbracket \phi \rrbracket_\rho^v$ is a singleton $\{d\}$, where $d \in \{\text{true}, \text{false}\}$.

Moreover, the truth value d coincides with the usual first-order logic semantics of ϕ in the model \mathcal{M}_v . That is,

$$d = \text{true} \quad \text{iff} \quad \mathcal{M}_v \models \phi$$

holds for the standard satisfaction relation \models of first-order logic.

Refinement of partial models

Let \mathcal{M}_{v_1} and \mathcal{M}_{v_2} be two partial models for (Σ, \mathcal{U}) with signatures $\Sigma_{v_1} = (\mathcal{X}_{v_1}, \mathcal{F}_{v_1}, \mathcal{P}_{v_1})$ and $\Sigma_{v_2} = (\mathcal{X}_{v_2}, \mathcal{F}_{v_2}, \mathcal{P}_{v_2})$ (respectively).

Then \mathcal{M}_{v_1} *refines* \mathcal{M}_{v_2} , denoted by $\mathcal{M}_{v_1} \sqsubseteq \mathcal{M}_{v_2}$, iff

1. the signature and universe of \mathcal{M}_{v_1} extend those of \mathcal{M}_{v_2} :
 $\mathcal{X}_{v_2} \subseteq \mathcal{X}_{v_1}$, $\mathcal{F}_{v_2} \subseteq \mathcal{F}_{v_1}$, $\mathcal{P}_{v_2} \subseteq \mathcal{P}_{v_1}$, and $\mathcal{U}_{v_2} \subseteq \mathcal{U}_{v_1}$; and
2. \mathcal{M}_{v_1} conservatively extends the semantics of functions and predicates that are in the signature of \mathcal{M}_{v_2} :

$$f \in \mathcal{F}_{v_2}, u_i \in \mathcal{U}_{v_2} \Rightarrow f^{v_2}(u_1, \dots, u_n) = f^{v_1}(u_1, \dots, u_n)$$

$$P \in \mathcal{P}_{v_2}, u_i \in \mathcal{U}_{v_2} \Rightarrow (u_1, \dots, u_n) \in P^{v_2} \text{ iff } (u_1, \dots, u_n) \in P^{v_1}.$$

15

Example

The “modulo 100” model \mathcal{M}_v is refined by the partial model $\mathcal{M}_{v'}$, where

$$\Sigma_{v'} = \Sigma_v$$

$$\mathcal{U}_{v'} = \{0, 1, 2, 3, \dots, 98, 99\},$$

and $+^{v'}$ and $*^{v'}$ are the interpretations of addition and multiplication “modulo 100” (respectively).

We can further refine $\mathcal{M}_{v'}$ to $\mathcal{M}_{v''}$ by making x an element of $\mathcal{X}_{v''}$.

Lemma: The relation \sqsubseteq is a partial order on the set of all partial models for (Σ, \mathcal{U}) .

16

Unsound semantics

Our semantics is *not* sound: $\mathcal{M}_{v_1} \sqsubseteq \mathcal{M}_{v_2}$ does not imply $\llbracket \phi \rrbracket_{\rho}^{v_2} \sqsubseteq \llbracket \phi \rrbracket_{\rho}^{v_1}$ for all ϕ . The latter is a way of expressing the requirement that v_1 has more precise knowledge of the “model” than v_2 , but that this knowledge is consistent with that of v_2 .

Recall that \mathcal{M}_v is refined by the model $\mathcal{M}_{v''}$. The formula $\exists x (98 < x)$ evaluates to false in \mathcal{M}_v since 98 is the maximal element of \mathcal{U}_v , but it evaluates to true in the refining model $\mathcal{M}_{v''}$ since it has 99 as a witness.

Note that this could only happen because \mathcal{M}_v had a somewhat limited view of the natural numbers contained in the interval $[0, 99]$.

Sound semantics for fixed universe

Let \mathcal{M}_{v_i} be partial models for (Σ, \mathcal{U}) with signatures Σ_{v_i} ($i = 1, 2$) such that $\mathcal{M}_{v_1} \sqsubseteq \mathcal{M}_{v_2}$ and $\mathcal{U}_{v_1} = \mathcal{U}_{v_2}$. Let ρ be an environment for \mathcal{M}_{v_2} .

1. For all terms t over Σ , $\llbracket t \rrbracket_{\rho}^{v_2} \sqsubseteq \llbracket t \rrbracket_{\rho}^{v_1}$ in $\mathbf{U}(\mathcal{U}_{v_2})$.
2. For all formulas ϕ over Σ , $\llbracket \phi \rrbracket_{\rho}^{v_2} \sqsubseteq \llbracket \phi \rrbracket_{\rho}^{v_1}$ in $\mathbf{U}(\mathbb{B})$.

View semantics as consensus

We define two functions Opt^s and Pess^s of type $\mathbf{U}(\mathbb{B}) \rightarrow \mathbf{U}(\mathbb{B})$ by

$$\text{Pess}^s(x) \stackrel{\text{def}}{=} \bigwedge^{\mathbb{B}} x \quad \text{Opt}^s(x) \stackrel{\text{def}}{=} \bigvee^{\mathbb{B}} x.$$

Note that these functions leave true and false fixed, but promote \mathbf{U} to a proper truth value:

$$\text{Pess}^s(\mathbf{U}) = \text{false} \quad \text{Opt}^s(\mathbf{U}) = \text{true}.$$

These functions are used to cast \mathbf{U} values, arising from the evaluation of atomic formulas $P(t_1, \dots, t_n)$, to proper truth values; they are dual:

$$\text{Pess}^s = \neg^s \circ \text{Opt}^s \circ \neg^s \quad \text{Opt}^s = \neg^s \circ \text{Pess}^s \circ \neg^s.$$

19

Semantics with modes $\text{o}(v)$ and $\text{p}(v)$

$$\begin{aligned} \llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^{\text{o}(v)} &\stackrel{\text{def}}{=} \text{Opt}^v(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v) \\ \llbracket \neg\phi \rrbracket_{\rho}^{\text{o}(v)} &\stackrel{\text{def}}{=} \neg^s \llbracket \phi \rrbracket_{\rho}^{\text{p}(v)} \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\rho}^{\text{o}(v)} &\stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_{\rho}^{\text{o}(v)} \wedge^s \llbracket \phi_2 \rrbracket_{\rho}^{\text{o}(v)} \\ \llbracket \exists x \phi \rrbracket_{\rho}^{\text{o}(v)} &\stackrel{\text{def}}{=} \bigvee_{u \in U}^s \llbracket \phi \rrbracket_{\rho[x \mapsto u]}^{\text{o}(v)} \\ \llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^{\text{p}(v)} &\stackrel{\text{def}}{=} \text{Pess}^v(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v) \\ \llbracket \neg\phi \rrbracket_{\rho}^{\text{p}(v)} &\stackrel{\text{def}}{=} \neg^s \llbracket \phi \rrbracket_{\rho}^{\text{o}(v)} \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\rho}^{\text{p}(v)} &\stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_{\rho}^{\text{p}(v)} \wedge^s \llbracket \phi_2 \rrbracket_{\rho}^{\text{p}(v)} \\ \llbracket \exists x \phi \rrbracket_{\rho}^{\text{p}(v)} &\stackrel{\text{def}}{=} \bigvee_{u \in U}^s \llbracket \phi \rrbracket_{\rho[x \mapsto u]}^{\text{p}(v)}. \end{aligned}$$

20

Kleene's alignment operator (Kleene 1952)

Kleene's alignment operation may be defined as a function of type $\mathbf{U}(\mathbb{B}) \times \mathbf{U}(\mathbb{B}) \rightarrow \mathbf{U}(\mathbb{B})$: for an input pair (x, y) it returns x in case that x equals y ; otherwise, it returns \mathbf{U} . This function is simply the *binary union operator*

$$\cup : \mathbf{U}(\mathbb{B}) \times \mathbf{U}(\mathbb{B}) \rightarrow \mathbf{U}(\mathbb{B}).$$

Kleene's alignment operator allows us to split our semantics into two "conventional", but co-dependent ones. We have

$$\llbracket \phi \rrbracket_{\rho}^v = \llbracket \phi \rrbracket_{\rho}^{\mathbf{p}(v)} \cup \llbracket \phi \rrbracket_{\rho}^{\mathbf{o}(v)}.$$

Consistency of $\llbracket \cdot \rrbracket_{\rho}^{\mathbf{p}(v)}$

Let \mathcal{M}_v be a partial model, ϕ a global formula, and ρ a (local) environment $\rho: \mathcal{X}_v \rightarrow \mathcal{U}_v$. Then

$$\llbracket \phi \wedge \neg\phi \rrbracket_{\rho}^{\mathbf{p}(v)} = \text{false}.$$

Consistency in entailment form

For all partial models \mathcal{M}_v , global formulas ϕ , and local environments ρ , we have

$$\Vdash \phi \Vdash_{\rho}^{\text{p}(v)} = \text{true} \quad \Rightarrow \quad \Vdash \phi \Vdash_{\rho}^{\text{o}(v)} = \text{true}.$$

Semantics of complete models

Let \mathcal{M}_v be a partial model for (Σ, \mathcal{U}) with $\Sigma_v = \Sigma$. Then $\Vdash \phi \Vdash_{\rho}^{\text{p}(v)} = \Vdash \phi \Vdash_{\rho}^{\text{o}(v)}$ for all global formulas ϕ and local environments ρ .

A first reduction of $\llbracket \cdot \rrbracket_\rho^v$

Let \mathcal{M}_v be a partial model for (Σ, \mathcal{U}) , ϕ a global formula, and ρ a local environment. Then

$$\begin{aligned}\llbracket \phi \rrbracket_\rho^v &= \llbracket \phi \rrbracket_{\rho^{\text{p}(v)} \cup \neg^s} \neg \phi \rrbracket_\rho^{\text{p}(v)} \\ \llbracket \phi \rrbracket_\rho^v &= \llbracket \phi \rrbracket_{\rho^{\text{o}(v)} \cup \neg^s} \neg \phi \rrbracket_\rho^{\text{o}(v)}.\end{aligned}$$

Thus, we may use a black box that computes $\llbracket \cdot \rrbracket_{\rho^{\text{p}(v)}}$ to compute $\llbracket \phi \rrbracket_\rho^v$. Alternatively, we may use a black box that computes $\llbracket \cdot \rrbracket_{\rho^{\text{o}(v)}}$.

Negation normal forms for model checks

For each signature Σ and each ϕ of our logic, we now use the DeMorgan laws to compute the standard negation normal form $T(\phi)$, an element generated by the grammar

$$L ::= P(t, t, \dots, t) \mid \neg P(t, t, \dots, t)$$

$$\phi ::= \perp \mid \top \mid L \mid \phi \wedge \phi \mid \phi \vee \phi \mid \exists x \phi \mid \forall x \phi.$$

We use the standard translation $\phi \rightarrow T(\phi)$, where the domain of this translation is all expressions of the original grammar and the range is the grammar above.

Semantics of $T(\phi)$: $\llbracket T(\phi) \rrbracket_{\rho}^{n(v)} \in \mathbf{U}(\mathbb{B})$

$$\begin{aligned}
\llbracket \perp \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \text{false} \\
\llbracket \top \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \text{true} \\
\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \text{Pess}^s(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v) \\
\llbracket \neg P(t_1, \dots, t_n) \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \neg^s \text{Opt}^s(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v) \\
\llbracket \phi_1 \wedge \phi_2 \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_{\rho}^{n(v)} \wedge^s \llbracket \phi_2 \rrbracket_{\rho}^{n(v)} \\
\llbracket \phi_1 \vee \phi_2 \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_{\rho}^{n(v)} \vee^s \llbracket \phi_2 \rrbracket_{\rho}^{n(v)} \\
\llbracket \exists x \phi \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \bigvee_{u \in \mathcal{U}_v}^s \llbracket \phi \rrbracket_{\rho[x \mapsto u]}^{n(v)} \\
\llbracket \forall x \phi \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \bigwedge_{u \in \mathcal{U}_v}^s \llbracket \phi \rrbracket_{\rho[x \mapsto u]}^{n(v)}.
\end{aligned}$$

27

Comments

The function \vee^s is the binary version of \bigvee^s . The semantics for $\forall x$, the function \wedge^s , has the same type as \bigvee^s and is defined as

$$\wedge^s \stackrel{\text{def}}{=} \neg^s \circ \bigvee^s \circ \prod \neg^s.$$

The semantics $\llbracket \cdot \rrbracket_{\rho}^{n(v)}$ always computes over $\mathbf{U}(\mathbb{B}) \setminus \{\mathbf{U}\}$ only, except for the evaluation of $\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v$ in the clauses for $P(t_1, \dots, t_n)$ and $\neg P(t_1, \dots, t_n)$; such values get immediately lifted to proper truth values by means of Pess^s and $\neg^s \text{Opt}^s$ (respectively):

$$\begin{aligned}
\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \text{Pess}^s(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v) \\
\llbracket \neg P(t_1, \dots, t_n) \rrbracket_{\rho}^{n(v)} &\stackrel{\text{def}}{=} \neg^s \text{Opt}^s(\llbracket P(t_1, \dots, t_n) \rrbracket_{\rho}^v).
\end{aligned}$$

28

A second reduction of $\llbracket \cdot \rrbracket_\rho^v$

Let \mathcal{M}_v be a partial model for (Σ, \mathcal{U}) , ϕ a global formula, and ρ a local environment. Then

$$\llbracket \phi \rrbracket_\rho^{p(v)} = \llbracket T(\phi) \rrbracket_\rho^{n(v)}.$$

29

Model construction

We compute $\llbracket T(\phi) \rrbracket_\rho^{n(v)}$ in a *standard* model of first-order logic over $(\Sigma \cup \{\bar{P} \mid P \in \mathcal{P}\}, \mathcal{U}(\mathcal{U}_v))$. For that, we extend the signature with “complementary” predicate symbols \bar{P} for each $P \in \mathcal{P}_v$ and interpret P_n^v and \bar{P}_n^v as n -ary relations over $\mathcal{U}(\mathcal{U}_v)$:

$$\begin{aligned} P_n^v &\stackrel{\text{def}}{=} \{(u_1, \dots, u_n) \in \prod \mathcal{U}(\mathcal{U}_v) \mid \text{Pess}^s(\llbracket P(u_1, \dots, u_n) \rrbracket_\rho^v) = \text{true}\} \\ \bar{P}_n^v &\stackrel{\text{def}}{=} \{(u_1, \dots, u_n) \in \prod \mathcal{U}(\mathcal{U}_v) \mid \neg^s \text{Opt}^s(\llbracket P(u_1, \dots, u_n) \rrbracket_\rho^v) = \text{true}\}. \end{aligned}$$

The consistency of this model is represented by the fact that $P_n^v \cap \bar{P}_n^v = \emptyset$ ($P \in \mathcal{P}$). This holds since $\text{Pess}^s(x) = \text{true}$ and $\text{Opt}^s(x) = \text{false}$ imply $x = \text{true}$ and $x = \text{false}$ (respectively).

However,

$P_n^v \cup \bar{P}_n^v = \{(u_1, \dots, u_n) \in \prod \mathcal{U}(\mathcal{U}_v) \mid \llbracket P(u_1, \dots, u_n) \rrbracket_\rho^v \neq \mathcal{U}\}$ is different from $\prod \mathcal{U}(\mathcal{U}_v)$ in general.

30

Lifting single-view model-checking to multiple viewpoints

1. assertion checks are “pessimistic”:

$$\mathcal{M}_v \models^a \phi \stackrel{\text{def}}{=} \llbracket \phi \rrbracket_{\rho}^{\text{p}(v)} = \{\text{true}\};$$

2. consistency checks are “optimistic”:

$$\mathcal{M}_v \models^c \phi \stackrel{\text{def}}{=} \llbracket \phi \rrbracket_{\rho}^{\text{o}(v)} = \{\text{true}\}.$$

Can one lift this semantics to a *collection* $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$, where (V, \leq) is a finite preorder of priorities?

Assertion and consistency obligations

$$\{\llbracket \mathcal{M} : \phi \rrbracket^a\} \stackrel{\text{def}}{=} \{v \in V \mid \exists v' \in V : v \leq v', \mathcal{M}_{v'} \models^a \phi\}$$

is a lower set in (V, \leq) and computes all viewpoints v that inherit an **assertion obligation** from a viewpoint with higher priority.

$$\{\llbracket \mathcal{M} : \phi \rrbracket^c\} \stackrel{\text{def}}{=} \{v \in V \mid \exists v' \in V : v' \leq v, \mathcal{M}_{v'} \models^c \phi\}$$

is an upper set in (V, \leq) and computes all viewpoints v that inherit a **consistency obligation** from a viewpoint with lower priority.

This order duality occurs because of the soundness of assertion and consistency checking with respect to refinement: for all ϕ , if $\mathcal{N} \prec \mathcal{M}$, then (i) $\mathcal{M} \models^a \phi$ implies $\mathcal{N} \models^a \phi$, and (ii) $\mathcal{N} \models^c \phi$ implies $\mathcal{M} \models^c \phi$.

Main results

Platonic world: If $v \leq v'$ implies $\mathcal{M}_v \prec \mathcal{M}_{v'}$, then all obligations of the priority ordering are fulfilled and no inconsistencies arise.

Obligation checking within \mathcal{M} is sound with respect to refinement.

The algorithm for computing $\{\mathcal{M}: \phi\}^m$, $m \in \{a, c\}$, efficiently lifts the model-checking engine for \models^m .

The denotation space for $(\{\mathcal{M}: \phi\}^a, \{\mathcal{M}: \phi\}^c)$ is an **assertion-consistency lattice**, a generalization of DeMorgan lattices to preorders that are not necessarily self dual.

Interesting connections to multiple-valued modal logics: (Fitting 1992).

Axioms for AC-lattices and DeMorgan lattices

$$\begin{array}{ll}
 \neg_a \neg_c \phi = \phi & \neg \neg \phi = \phi \\
 \neg_c \neg_a \phi = \phi & \neg(\phi \wedge \psi) = \neg \phi \vee \neg \psi \\
 \phi \leq_a \psi \Rightarrow \neg_a \psi \leq_c \neg_a \phi & \neg(\phi \vee \psi) = \neg \phi \wedge \neg \psi \\
 \phi \leq_c \psi \Rightarrow \neg_c \psi \leq_a \neg_c \phi & \phi \leq \psi = \neg \psi \leq \neg \phi.
 \end{array}$$

Figure 1: Axioms for AC-lattices (left) and DeMorgan lattices (right).

Representing AC-lattices and DeMorgan lattices

Finite, distributive AC-lattices: For any preorder (V, \leq) , the tuple $(\mathbf{L}(V, \leq), \subseteq, \setminus, \mathbf{U}(V, \leq), \subseteq, \setminus)$ is an AC-lattice. Conversely, every finite, distributive AC-lattice can be represented in that form, where \setminus is “distorted” by some order-isomorphism $i \in \text{Aut}(V, \leq)$.

Finite, distributive DeMorgan lattices: For any preorder (V, \leq) and an anti-tone and idempotent map $i: (V, \leq) \rightarrow (V, \leq)$,^a the tuple $(\mathbf{L}(V, \leq), \subseteq, \neg)$ is a DeMorgan lattice, where $\neg L = \{i(v) \mid v \in V \setminus L\}$. Conversely, every finite, distributive DeMorgan lattice $(\mathcal{L}, \leq, \neg)$ can be represented in that form, where (V, \leq) is a finite partial order.

^aA map $f: (V, \leq) \rightarrow (V, \leq)$ 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 upshot

Bad news: DeMorgan lattices require that (V, \leq) is isomorphic to its order dual (V, \leq^{op}) : they are ill suited for *prioritized requirements*

Good news: AC-lattices provide sensible and robust spaces of meaning for every priority preorder, even in the context of multiple points of view.

Related work

- (Bruns & Godefroid 1999);
- (Jackson 1995) and (Jackson 1999);
- (Sagiv et al. 1999) and (Yahav 2001);
- (Cousot & Cousot 2000);
- (Guerra 2000);
- (Chechik & Easterbrook 2001).

Conclusions

(This page is intentionally left blank.)