Belief Semantics of Authorization Logic

Andrew K. Hirsch
Department of Computer Science
George Washington University
Washington, D.C., United States
akhirsch@gwu.edu

Michael R. Clarkson
Department of Computer Science
George Washington University
Washington, D.C., United States
clarkson@gwu.edu

ABSTRACT
A formal belief semantics for authorization logics is given. The belief semantics is proved to subsume a standard Kripke semantics. The belief semantics yields a direct representation of principals’ beliefs, without resorting to the technical machinery used in Kripke semantics. A proof system is given for the logic; that system is proved sound with respect to the belief and Kripke semantics. The soundness proofs are mechanized in Coq.

Categories and Subject Descriptors
D.4.6 [Operating Systems]: Security and Protection—Access controls; F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic—modal logic, model theory, proof theory, mechanical theorem proving

Keywords
Authorization logic; NAL; CDD

1. INTRODUCTION
Authorization logics are used in computer security to reason about whether principals — computer or human agents — are permitted to take actions in computer systems. The distinguishing feature of authorization logics is their use of a says connective: intuitively, if principal \( p \) believes that formula \( \phi \) holds, then formula \( p \) says \( \phi \) holds. Access control decisions can then be made by reasoning about (i) the beliefs of principals, (ii) how those beliefs can be combined to derive logical consequences, and (iii) whether those consequences entail guard formulas, which must hold for actions to be permitted.

Many systems that employ authorization logics have been proposed (see [1,10] for surveys; see also [5,9,11,12,17,23,28,29,32,35,40,42,15,52]), but few authorization logics have been given a formal semantics [4,18,19,22,26]. Though semantics might not be immediately necessary to deploy authorization logics in real systems, semantics yield insight into the meaning of formulas, and semantics enable proof systems to be proved sound—which might require proof rules and axioms to be corrected, if there are any lurking errors in the proof system.

For the sake of security, it is worthwhile to carry out such soundness proofs. Given only a proof system, we must trust that the proof system is correct. But given a proof system and a soundness proof, which shows that any provable formula is semantically valid, we now have evidence that the proof system is correct, hence trustworthy. The soundness proof thus relocates trust from the proof system to the proof itself—as well as to the semantics, which ideally offers more intuition about formulas than the proof system itself.

Semantics of authorization logics are usually based on possible worlds, as used by Kripke [31]. Kripke semantics posit an indexed accessibility relation on possible worlds. If at world \( w \), principal \( p \) considers world \( w' \) to be possible, then \( (w, w') \) is in \( p \)'s accessibility relation. We denote this as \( w \leq_p w' \). Authorization logics use Kripke semantics to give meaning to the says connective: semantically, \( p \) says \( \phi \) holds in a world \( w \) iff for all worlds \( w' \) such that \( w \leq_p w' \) formula \( \phi \) holds in world \( w' \). Hence a principal says \( \phi \) iff \( \phi \) holds in all worlds the principal considers possible.

The use of Kripke semantics in authorization logic thus requires installation of possible worlds and accessibility relations into the semantics, solely to give meaning to says. That’s useful for studying properties of logics and for building decision procedures. But, unfortunately, it doesn’t seem to correspond to how principals reason in real-world systems. Rather than explicitly considering possible worlds and relations between them, principals typically begin with some set of base formulas they believe to hold—perhaps because they have received digitally signed messages encoding those formulas, or perhaps because they invoke system calls that return information—then proceed to reason from those formulas. So could we instead stipulate that each principal \( p \) have a set of beliefs \( \omega(p) \), called the worldview of \( p \), such that \( p \) says \( \phi \) holds iff \( \phi \in \omega(p) \)? That is, a principal says \( \phi \) iff \( \phi \) is in the worldview of the principal.

This paper answers that question in the affirmative. We give two semantics for an authorization logic: a Kripke semantics (§2), and a new belief semantics (§3), which employs

\[ \text{The says connective is, therefore, closely related to the modal necessity operator } \Box \text{ and the epistemic knowledge operator } K \text{.} \]

\[ \text{Worldviews were first employed by NAL [43], which pioneered an informal semantics based on them.} \]
worldviews to interpret says[^1] We show [4] that belief semantics subsume Kripke semantics, in the sense that a belief model can be constructed from any Kripke model. A formula is valid in the Kripke model iff it is valid in the constructed belief model. As a result, the technical machinery of Kripke semantics can be replaced by belief semantics. This potentially increases the trustworthiness of an authorization system, because the semantics is closer to how principals reason in real systems.

The particular logical system we introduce in this paper is FOCAL, First-Order Constructive Authorization Logic. FOCAL extends a well-known authorization logic, cut-down dependency core calculus (CDD) [2], from a propositional language to a language with first-order functions and relations on system state. Functions and relations are essential for reasoning about authorization in a real operating system—as exemplified in Nexus Authorization Logic (NAL) [43], of which FOCAL and CDD are both fragments.

Having given two semantics for FOCAL, we then turn to the problem of proving soundness. It turns out that the NAL proof system is unsound with respect to the semantics presented here: NAL allows derivation of a well-known formula (cf. §5.2) that our semantics deems invalid. A priori, the fault could lie with our semantics or with NAL’s proof system. However, if the logic is to be used in a distributed setting without globally-agreed upon state, then the proof system should not allow the formula to be derived. So if NAL is to be used in such settings, its proof system needs to be corrected. CDD is also unsound with respect to our semantics. However, CDD has been proved sound with respect to one of Kripke semantics [34].

To achieve soundness for FOCAL, we develop a revised proof system; the key technical change is using localized hypotheses in the proof rules. In §5.2 we prove the soundness of our proof system with respect to both our belief and Kripke semantics. This result yields the first soundness proof for an authorization-logic proof system.

Having relocated trust into the soundness proof, we then seek a means to increase the trustworthiness of that proof. We formalize the syntax, proof system, belief semantics, and Kripke semantics in the Coq proof assistant[^3] and we mechanize the proofs of soundness for both the belief semantics and the Kripke semantics. That mechanization relocates trust from our soundness proof to Coq, which is well-studied and the basis of many other formalizations. Our Coq formalization contains about 2,400 lines of code[^4].

This paper thus advances the theory of computer security with the following novel contributions:

- the first formal belief semantics for authorization logic,
- a proof that Kripke semantics can be transformed into belief semantics,
- a proof system that is sound with respect to belief and Kripke semantics, and

[^1]: Our belief models are an instance of the syntactic approach to modeling knowledge [13][15][30][37].
[^3]: Our implementation is available from http://faculty.cs.gwu.edu/~clarkson/projects/focal/

$$\begin{align*}
\tau & ::= \ x \mid f(\tau, \ldots, \tau) \\
\phi & ::= \ true \mid false \mid \ r(\tau, \ldots, \tau) \mid t_1 = t_2 \\
& \mid \ \phi_1 \land \phi_2 \mid \phi_1 \lor \phi_2 \mid \phi_1 \Rightarrow \phi_2 \mid \neg \phi \\
& \mid (\forall x : \phi) \mid (\exists x : \phi) \\
& \mid \ t \ \text{says} \ \phi \mid t_1 \ \text{says} \ \phi
\end{align*}$$

Figure 1: Syntax of FOCAL

- the first machine-checked proof of soundness for an authorization-logic proof system.

We proceed as follows. §2 presents FOCAL’s belief semantics; and §3 the Kripke semantics. §4 relates the belief semantics to the Kripke semantics. §5 gives a proof system and proves its soundness with respect to both semantics. §6 discusses related work, and §7 concludes. All proofs appear in the appendix.

2. BELIEF SEMANTICS

FOCAL is a constructive, first-order, multimodal logic. The key features that distinguish it as an authorization logic are the says and speaksfor connectives, invented by Lampson et al. [32]. These are used to reason about authorization—for example, access control in a distributed system can be modeled in the following standard way:

**Example 1.** A guard implements access control for a printer $p$. To permit printing to $p$, the guard must be convinced that guard formula $\text{PrintServer says printTo}(p)$ holds, where $\text{PrintServer}$ is the principal representing the server process. That formula means $\text{PrintServer believes printTo}(p)$ holds. To grant printer access to user $u$, the print server can issue the statement $u \ \text{says} \ \text{speaksfor} \ \text{PrintServer}$. That formula means anything $u$ says, the PrintServer must also say. So if $u \ \text{says} \ \text{printTo}(p)$, then $\text{PrintServer says printTo}(p)$, which satisfies the guard formula hence affords the user access.

Figure 1 gives the formal syntax of FOCAL. There are two syntactic classes, terms $\tau$ and formulas $\phi$. Metavariable $x$ ranges over first-order variables, $f$ over first-order functions, and $r$ over first-order relations.

Formulas of FOCAL do not permit monadic second-order universal quantification, unlike CDD and NAL. In NAL, that quantifier was used only to define false and speaksfor as syntactic sugar. FOCAL instead adds these as primitive connectives to the logic. FOCAL also defines $\neg \phi$ as a primitive connective, but it could equivalently be defined as syntactic sugar for $\phi \Rightarrow \text{false}$.

Syntactically, FOCAL is thus CDD without second-order quantification, but with first-order terms and quantification and a primitive speaksfor connective. Likewise, FOCAL is NAL without second-order quantification, subprincipals, group principals, and restricted delegation, but with a primitive speaksfor connective.

2.1 Semantic models

The belief semantics of FOCAL combines first-order constructive models with worldviews, which are used to interpret says and speaksfor. To our knowledge, this semantics is new in the study of authorization logics. Our presentation mostly follows the semantics of intuitionistic predicate calculus given by Troelstra and van Dalen [48].
First-order models. A first-order model with equality is a tuple \((D,\preceq,R,F)\). The purpose of a first-order model is to interpret the first-order fragment of the logic, specifically first-order quantification, functions, and relations. \(D\) is a set, the domain of individuals. Semantically, quantification in the logic ranges over these individuals. \(R\) is a set \(\{r_i \mid i \in I\}\) of relations on \(D\), indexed by set \(I\). Likewise, \(F\) is a set \(\{f_j \mid j \in J\}\) of functions on \(D\), indexed by set \(J\). There is a distinguished equality relation \(\equiv\), which is an equivalence relation on \(D\), such that equal individuals are indistinguishable by relations and functions.

To interpret first-order variables, the semantics employs valuation functions, which map variables to individuals. We write \(v(x)\) to denote the individual that variable \(x\) represents in valuation \(v\). And we write \(v[d/x]\) to denote the valuation that is the same as \(v\) except that \(v(x) = d\).

Constructive models. A constructive model is a tuple \((W,\leq,s,P,\omega)\). The purpose of constructive models is to extend first-order models to interpret the constructive fragment of the logic, specifically implication and universal quantification. \(W\) is a set, the possible worlds. We denote an individual world as \(w\). Intuitively, a world \(w\) represents the state of knowledge of a constructive reasoner. Constructive accessibility relation \(\leq\) is a partial order on \(W\). If \(w \leq w'\), then the constructive reasoner’s state of knowledge could grow from \(w\) to \(w'\). But unlike in classical logic, the reasoner need not commit to a formula \(\phi\) being either true or false at a world. Suppose that at world \(w'\), where \(w \leq w'\), the reasoner concludes that \(\neg \phi\) holds. But at world \(w\), the reasoner has not yet concluded that either \(\phi\) or \(\neg \phi\) holds. Then Excluded Middle \((\phi \lor \neg \phi)\) doesn’t hold at \(w\).

Function \(s\) is the first-order interpretation function. It assigns a first-order model \((D_w,\preceq_w,R_w,F_w)\) to each world \(w\). Let the individual elements of \(R_w\) be denoted as \(r_{i,w}\), and the elements of \(F_w\) as \(f_{j,w}\). Thus, \(s\) enables a potentially different first-order interpretation at each world. But to help ensure that the constructive reasoner’s state of knowledge only grows—hence never invalidates a previously admitted construction—we require \(s\) to be monotonic w.r.t. \(\leq\). That is, if \(w \leq w'\) then (i) \(D_w \subseteq D_{w'}\), (ii) \(d =_{w} d'\) implies \(d =_{w'} d'\), (iii) \(r_{i,w} \subseteq r_{i,w'}\), and (iv) for all tuples \(d\) of individuals in \(D_w\), it holds that \(f_{j,w}(d) =_{w} f_{j,w'}(d)\).

It’s natural to wonder why we chose to introduce possible worlds into the semantics here after arguing against them in \(\text{§}\). Note, though, that the worlds in the constructive model are being used to model only the constructive reasoner—\(\text{§}\) which we might think of as the guard, who exists outside the worldview and the elements of \(W\) into the semantics here after arguing against them in the constructive reasoner’s state of knowledge could grow from \(w\) to \(w'\).

Belief models. A belief model is a tuple \((W,\leq,s,P,\omega)\). The purpose of belief models is to extend constructive models to interpret says and speaksfor. The first part of a belief model, \((W,\leq,s)\), must itself be a constructive model. The next part, \(P\), is the set of principals. Although individuals can vary from world to world in a model, the set of principals is fixed across the entire model. Assuming a fixed set of principals is consistent with other authorization logics [15,19,22], with constructive multimodal logics [43,51] (which have a fixed set of modalities), and with classical multimodal epistemic logics [15] (which have an indexed set modalities, typically denoted \(K_i\), where the index set is fixed)—even though constructivist philosophy might deem it more sensible to allow \(P\) to grow with \(\leq\).

Because we make no syntactic distinction between individuals and principals, all principals must also be individuals: \(P\) must be a subset of \(D_w\) for every \(w\). First-order quantification can therefore range over individuals as well as principals. For example, to quantify over all principals, we can write \((\forall x : \text{IsPrin}(x) \Rightarrow \phi)\), where \(\text{IsPrin}\) is a relation that holds for all \(x \in P\). Nonetheless, this does not constitute truly intuitionistic quantification, because the domain of principals is constant. Quantification over a non-constant domain of principals is theoretically of interest, but we know of no authorization logic that has used it.

We define an equality relation \(\equiv\) on principals, such that principals are equal iff they are equal at all worlds. Formally, \(w \equiv w'\) iff, for all \(w,\) it holds that \(p =_{w} p'\).

The final part of a belief model, worldview function \(\omega\), yields the beliefs of a principal \(p\): the set of formulas that \(p\) believes to hold in world \(w\) under first-order valuation \(v\) is \(\omega(w,p,v)\). For sake of simplicity, [1] used notation \(\omega(p)\) when first presenting the idea of worldviews. Now that we’re being precise, we also include \(w\) and \(v\) as arguments. To ensure that the constructive reasoner’s knowledge grows monotonically, worldviews must be monotonic w.r.t. \(\leq\):

**Worldview Monotonicity:** If \(w \leq w'\) then \(\omega(w,p,v) \subseteq \omega(w',p,v)\).

To ensure that whenever principals are equal they have the same worldview, we require the following:

**Worldview Equality:** If \(p \equiv p'\), then, for all \(w\) and \(v\), it holds that \(\omega(w,p,v) = \omega(w,p',v)\).

And we also require the following conditions to ensure that valuations cannot cause worldviews to distinguish alpha-equivalent formulas:

**Worldview Valuations:**

1. If \(x \notin \text{FV}(\phi)\) then \(\phi \in \omega(w,p,v)\) iff, for all \(d \in D_w\), it holds that \(\phi \in \omega(w,p,v[d/x])\).
2. If \( x \in FV(\phi) \) and \( y \notin FV(\phi) \) then, for all \( d \in D_w \), it holds that \( \phi \in \omega(w, p, v[d/x]) \) if \( \phi[y/x] \in \omega(w, p, v[d/y]) \), where \( \phi[y/x] \) denotes the capture-avoiding substitution of \( y \) for \( x \) in formula \( \phi \).

Condition (1) ensures that if \( x \) is irrelevant to \( \phi \), then the value of \( x \) is also irrelevant to whether \( p \) believes \( \phi \). Condition (2) ensures that if \( x \) is relevant to \( \phi \), then only its value—not its name—is relevant to whether \( p \) believes \( \phi \).

2.2 Semantic validity

Figure 2 gives a belief semantics of FOCAL. The validity judgment is written \( B, u, v \models \phi \) where \( B \) is a belief model and \( w \) is a world in that model. As is standard, \( B \models \phi \) holds iff, for all \( u \) and \( v \), it holds that \( B, u, v \models \phi \); whenever \( B \models \phi \), then \( \phi \) is a necessary formula in model \( B \). And \( B, v \models \phi \) holds iff for all \( u \), it holds that \( B, u, v \models \phi \); whenever \( B, v \models \phi \), then \( \phi \) is a valuation-necessary formula. Likewise, \( \models \phi \) holds iff, for all \( B \), it holds that \( B \models \phi \); and whenever \( \models \phi \), then \( \phi \) is a validity. Let \( B, u, v \models \Gamma \), where \( \Gamma \) is a set of formulas, denote that for all \( \psi \in \Gamma \), it holds that \( B, u, v \models \psi \). Finally, \( \Gamma \models \phi \) holds iff, for all \( B, w \), and \( v \), it holds that \( B, w, v \models \Gamma \) implies \( B, w, v \models \phi \); whenever \( \Gamma \models \phi \), then \( \phi \) is a logical consequence of \( \Gamma \).

The semantics relies on an auxiliary interpretation function \( \mu \) that maps syntactic terms \( \tau \) to semantic individuals:

\[
\mu(x) = v(x) \\
\mu(f_j(\vec{\tau})) = f_j(\vec{\mu})
\]

Implicitly, \( \mu \) is parameterized on belief model \( B \), world \( w \), and valuation \( v \), but for notational simplicity we omit writing these as arguments to \( \mu \) unless necessary for disambiguation. Variables \( x \) are interpreted by looking up their value in \( v \); functions \( f_j \) are interpreted by applying their first-order interpretation \( f_j(\vec{w}) \) at world \( w \) to the interpretation of their arguments. Notation \( \vec{\tau} \) represents a list \( \tau_1, \tau_2, \ldots, \tau_n \) of terms. And \( \vec{\mu} \) denotes the pointwise application of \( \mu \) to each element of that list, producing \( \mu(\tau_1), \ldots, \mu(\tau_n) \).

The first-order, constructive fragment of the semantics is routine. The semantics of \( \models \) is the intuitive semantics we wished for in \[1\]. A principal \( \mu(\tau) \) says \( \phi \) exactly when \( \phi \) is in that principal’s worldview \( \omega(w, \mu(\tau), v) \). And a principal \( \mu(\tau_1) \) speaks for another principal \( \mu(\tau_2) \) exactly when, in all constructively accessible worlds, everything \( \mu(\tau_1) \) says, \( \mu(\tau_2) \) also says.

Note that some syntactic terms may represent individuals that are not principals. For example, the integer 42 is presumably not a principal in \( P \), but it could be an individual in some domain \( D_w \). An alternative would be to make FOCAL a two-sorted logic, with one sort for individuals and another sort for principals. Instead, we allow individuals who aren’t principals to have beliefs, because it simplifies the definition of the logic. The worldviews of non-principal individuals contain all formulas. Formally, for any individual \( d \) such that \( d \notin P \), and for any world \( w \), valuation \( v \), and formula \( \phi \), it holds that \( \phi \in \omega(w, d, v) \).

We impose a few well-formedness conditions on worldviews in this semantics, in addition to Worldview Monotonicity and Worldview Equality. Worldviews must be closed under logical consequence—that is, principals must believe all the formulas that are a consequence of their beliefs.

Worldview Closure: If \( \Gamma \subseteq \omega(w, p, v) \) and \( \Gamma \models \phi \), then \( \phi \in \omega(w, p, v) \).

Worldview Closure means that principals are fully logically omniscient \[15\]. With its known benefits and flaws \[39,47\], this has been a standard assumption in authorization logics since their inception \[32\].

The remaining well-formedness conditions are optional, in the sense that they are necessary only to achieve soundness of particular proof rules in \[3\]. Eliminate those rules, and the following conditions would be eliminated.

Worldviews must ensure that \( \models \) is a transparent modality. That is, for any principal \( p \), it holds that \( p \models \phi \) exactly when \( p \models (p \models \phi) \).

Says Transparency: \( \phi \in \omega(w, \mu(\tau), v) \) iff \( \tau \models \phi \in \omega(w, \mu(\tau), v) \).

So \( \models \) supports positive introspection: if \( p \) believes that \( \phi \) holds, then \( p \) is aware of that belief, therefore \( p \) believes that \( p \) believes that \( \phi \) holds. The converse of that holds as well. Recent authorization logics include transparency \[3,43\], and it is well known (though sometimes vigorously debated) in epistemic logic \[25,27\]. Says Transparency corresponds to rules \( S-A \) and \( S-A \) in \[3\].

Worldviews must enable principals to delegate, or hand-off, to other principals: if a principal \( q \) believes that \( p \) speaks for \( q \), it should hold that \( p \) does speak for \( q \). Hand-off, as the following axiom, existed in the earliest authorization logic \[32\]:

\[
(q \models (p \text{ speaks for } q)) \Rightarrow (p \text{ speaks for } q)
\]

To support it, we adopt a condition that ensures whenever \( q \) believes \( p \) speaks for \( q \), then it really does:

Belief Hand-off: If \( (p \text{ speaks for } q) \in \omega(w, q, v) \) then \( \omega(w, p, v) \subseteq \omega(w, q, v) \).

Belief Hand-off corresponds to rule \( SF-i \) in \[3\].

3. KRIPEK SEMANTICS

The Kripke semantics of FOCAL combines first-order constructive models with modal (Kripke) models \[13,27,44\]. Similar semantic models have been explored before (see, e.g., \[18,22,51\]). Indeed, the only non-standard part of our semantics is the treatment of \( \text{speaks for} \), and that part turns out to be a generalization of previous classical semantics. Nonetheless, we are not aware of any authorization logic semantics that is equivalent to or subsumes our semantics. First-order and constructive models were already presented in \[3\] so we begin here with modal models.

3.1 Modal models

A modal model is a tuple \((W, \leq, s, P, A)\). The purpose of modal models is to extend constructive models to interpret \( \models \) and \( \models \). The first part of a modal model, \((W, \leq, s)\), must itself be a constructive model. The next part, \( P \), is the set of principals. As with belief models, all principals must be individuals, so \( P \) must be a subset of \( D_w \) for every \( w \). Principal equality relation \( =d \) is defined just as in belief models. The final part of a modal model, \( A \), is a set \( \{\leq_p \mid p \in P\} \) of binary relations on \( W \), called the principal accessibility relations \[6\]. If \( w \leq w' \), then at world \( w \), principal \( p \) considers world \( w' \) possible. To ensure that equal principals have the same beliefs, we require

\[6\]In our notation, an unsubscripted \( \leq \) always denotes the constructive relation, and a subscripted \( \leq \) always denotes a principal relation.
Figure 2: FOCAL validity judgment for belief semantics

\[
\begin{align*}
B, w, v & \models \tau \text{ says } \phi & \text{always} \\
B, w, v & \models \tau_1 \text{ speaksfor } \tau_2 & \text{never} \\
B, w, v & \models \tau_1 = \tau_2 & \iff \mu(\tau_1) = \mu(\tau_2) \\
B, w, v & \models \phi_1 \land \phi_2 & \iff B, w, v \models \phi_1 \land B, w, v \models \phi_2 \\
B, w, v & \models \phi_1 \lor \phi_2 & \iff B, w, v \models \phi_1 \lor B, w, v \models \phi_2 \\
B, w, v & \models \phi \rightarrow \phi_2 & \iff \text{for all } w' \geq w : B, w', v \models \phi \implies B, w', v \models \phi_2 \\
B, w, v & \models \forall x : \phi & \iff \text{for all } w' \geq w : B, w', v \models \phi \\
B, w, v & \models \exists x : \phi & \iff \text{there exists } d \in D_{\omega'} : B, w, v[d/x] \models \phi \\
B, w, v & \models \tau \text{ says } \phi & \iff \phi \in \omega(w, \mu(\tau), v) \\
B, w, v & \models \tau_1 \text{ speaksfor } \tau_2 & \iff \text{for all } w' \geq w : \omega(w', \mu(\tau_1), v) \subseteq \omega(w', \mu(\tau_2), v) \\
\end{align*}
\]

Figure 3: FOCAL validity judgment for Kripke semantics

Accessibility Equality: If \( p \models p' \), then \( \leq_p = \leq_{p'} \).

Like \( \leq \) in a constructive model, we require \( s \) to be monotonic w.r.t. each \( \leq_p \). This requirement enforces a kind of constructivity on each principal \( p \), such that from a world in which individual \( d \) is constructed, \( p \) cannot consider possible any world in which \( d \) has not been constructed. Unlike \( \leq \), none of the \( \leq_p \) are required to be partial orders: they are not required to satisfy reflexivity, anti-symmetry, or transitivity.

That non-requirement raises an important question. In epistemic logics, the properties of what we call the “principal accessibility relations” determine what kind of knowledge is modeled \[20\]. If, for example, these relations must be reflexive, then the logic models veridical knowledge: if \( p \) says \( \phi \), then \( \phi \) indeed holds. But that is not the kind of knowledge we seek to model with FOCAL, because principals may say things that in fact do not hold. So what are the right properties, or frame conditions, to require of our principal accessibility relations? We briefly delay presenting them, so that we can present the Kripke semantics.

3.2 Semantic validity

Figure 3 gives a Kripke semantics of FOCAL. The validity judgment is written \( K, w, v \models \phi \) where \( K \) is a modal model and \( w \) is a world in that model. Only the judgments for the says and speaksfor connectives are given in figure 3 \[20\]. For the remaining connectives, the Kripke semantics is the same as the belief semantics in figure 2. Interpretation function \( \mu \) remains unchanged from figure 2 except that it is now implicitly parameterized on \( K \) instead of \( B \).

To understand the semantics of says, first observe the following. Suppose that, for all worlds \( w' \), it holds that \( w \leq w' \) implies \( w = w' \). Then the semantics of says simplifies to the standard semantics of \( \Box \) in classical modal logic \[27\].

\[
K, w, v \models \tau \text{ says } \phi & \iff \text{for all } w' \geq w : w \leq w' \leq \mu(\tau, v) \implies K, w', v \models \phi.
\]

That is, a principal believes a formula holds whenever that formula holds in all accessible worlds. The purpose of the quantification over \( w' \), where \( w \leq w' \), in the unmodified semantics of says is to achieve monotonicity of the constructive reasoner:

**Proposition 1.** If \( K, w, v \models \phi \) and \( w \leq w' \) then \( K, w', v \models \phi \).

That is, whenever \( \phi \) holds at a world \( w \), if the constructive reasoner is able to reach an extended state of knowledge at world \( w' \), then \( \phi \) should continue to hold at \( w' \). Without the quantification over \( w' \), where \( w \leq w' \), in the semantics of says, monotonicity is not guaranteed to hold. Constructive modal logics have, unsurprisingly, also used this semantics for \( \Box \) \[14\], \[15\], and a similar semantics has been used in authorization logic \[18\].

Note that, if there do not exist any worlds \( w' \) and \( w'' \) such that \( w \leq w' \leq w'' \), then at \( w \), principal \( \tau \) will say any formula \( \phi \), including false. When a principal says false at world \( w \), we deem that principal compromised at \( w \). As for the semantics of speaksfor, it might be tempting to try defining it as syntactic sugar:

\[
\tau_1 \text{ speaksfor } \tau_2 \equiv \forall \phi : \tau_1 \text{ says } \phi \rightarrow \tau_2 \text{ says } \phi
\]

However, the formula on the right-hand side is not a well-formed formula of FOCAL, because it quantifies over syntactic formulas. So the semantics of speaksfor cannot interpret it directly in terms of says \[20\].

Instead, the FOCAL semantics of speaksfor generalizes the classical Kripke semantics of speaksfor \[14\], \[20\]. Classically,

\[
K, w, v \models \tau_1 \text{ speaksfor } \tau_2 & \iff \leq_{\mu(\tau_1)} \supseteq \leq_{\mu(\tau_2)} \ 	ext{ if l lo l}
\]

This condition corresponds to the axiom of excluded middle. So it makes sense that adding the frame condition would result in the classical semantics of \( \Box \).
Note how, if $w \leq w'$, the conditions reduce to the classical definitions of transitivity and density. Those classical conditions are exactly what guarantee transparency in classical modal logic.

IT and ID are not quite sufficient to yield transparency. By also imposing the following frame condition, we do achieve transparency

\[ F2: \text{If } w \leq v \leq v', \text{ then there exists a } w' \text{ such that } w \leq w' \leq v'. \]

$F2$ is depicted in Figure 4. It is difficult to motivate $F2$ solely in terms of authorization logic, though it has been proposed in several Kripke semantics for constructive modal logics \[14,16,41,44\]. But there are two reasons why $F2$ is desirable for FOCAL:

- Assuming $F2$ holds, IT and ID are not only sufficient but also necessary conditions for transparency—a result that follows from work by Plotkin and Stirling \[41\]. So in the presence of $F2$, transparency in FOCAL is precisely characterized by IT and ID.

- Suppose FOCAL were to be extended with a $\Diamond$ modality. It could be written $\tau \text{ suspects } \phi$, with semantics $K, w, v \models \tau \text{ suspects } \phi$ if there exists $w'$ such that $w \leq w' \leq v$ and $K, w', v \models \phi$. We would want $\text{says}$ and $\text{suspects}$ to interact smoothly. For example, it would be reasonable to expect that $\neg (\tau \text{ suspects } \phi)$ implies $\tau \text{ says } \neg \phi$. For $\tau$ does not suspect $\phi$ holds anywhere, then $\tau$ should believe $\neg \phi$ holds. Condition $F2$ guarantees that implication \[11\]. So $F2$ prepares FOCAL for future extension with a $\text{suspects}$ modality. \[17\]

To ensure the validity of hand-off, we impose the following frame condition:

\[ H: \text{For all principals } p \text{ and worlds } w, \text{ if there do not exist any worlds } w' \text{ and } w'' \text{ such that } w \leq w' \leq w'', \text{ then, for all } p', \text{ it must hold that } \leq_{w(p)} \subseteq \leq_{w'(p')}. \]

This condition guarantees that if a principal $p$ becomes compromised at world $w$, then the reachable component of its accessibility relation will be a subset of all other principals’. By the FOCAL semantics of $\text{speaksfor}$, all other principals therefore speak for $p$ at $w$.

Each frame condition above was imposed, not for ad hoc purposes, but because of a specific need in the proof of the soundness result of \[3\]. So with appropriate deletion of rules from the proof system, each of the above frame conditions could be eliminated. IT and ID should be removed if rules $\text{SAYS-LI}$ and $\text{SAYS-RI}$ (from figure 3) are removed; $F2$ should be removed if rule $\text{SAYS-LRI}$ is removed; and $H$ should be removed if rule $\text{SF-I}$ is removed.

Finally, we impose one additional condition to achieve the equivalence results (Theorem 1 and Proposition 2) of \[4\].

\[ F2 \] is the name given this condition by Simpson \[44\].

\[ F2 \] were $\text{suspects}$ to be added to FOCAL, it would also be desirable to impose a fourth frame condition: if $w \leq w'$ and $w \leq v$, then there exists a $v'$ such that $w < v'$ and $w' \leq v'$. This condition, named F1 by Simpson \[44\], guarantees that $\tau \text{ suspects } \phi$ implies $\neg (\tau \text{ says } \neg \phi)$. It also guarantees monotonicity (cf. Proposition 1) for $\text{suspects}$. Figure 4 depicts F1. Simpson \[44\, p. 51\] argues that F1 and F2 could be seen as fundamental, not artificial, frame conditions for constructive modal logics.
WSF: $K, w, v \models \tau$ speaks for $\tau'$ iff, for all $\phi$, if $K, w, v \models \tau$ says $\phi$ then $K, w, v \models \tau'$ says $\phi$.

This condition restricts the class of Kripke models to those where speaks for is the weak speaks for connective. In fact, we’d prefer to use WSF directly as the semantics of speaks for in figure 3.4. But it wouldn’t be a well-founded definition of $\models$, because $\phi$ could itself be $\tau$ speaks for $\tau'$, leading to a circularity in the semantic definition. So we instead impose WSF as a separate axiom.

4. SEMANTIC TRANSFORMATION

We have now given two semantics for FOCAL, a belief semantics (§) and a Kripke semantics (§). How are these two semantics related? It turns out that a Kripke model can be transformed into a belief model, but the converse does not hold—as we now explain.

Given a modal model $K$, there is a natural way to construct a belief model from it: assign each principal a worldview containing exactly the formulas that the principal says in $K$. Call this construction $k2b$, and let $k2b(K)$ denote the resulting belief model.

To give a precise definition of $k2b$, we need to introduce a new notation. Given a principal $p \in P$, formula $p$ says $\phi$ is not necessarily well-formed, because $p$ is not necessarily a syntactic term. So let $K, w, v \models p$ says $\phi$ be defined as follows: for all $w'$ and $w''$ such that $w \leq w' \leq w''$, it holds that $K, w'', v \models \phi$. This definition simply unrolls the semantics of says to produce something well-formed.

The precise definition of $k2b$ is as follows: if $K = (W, \leq, s, P, A)$, then $k2b(K)$ is belief model $(W, \leq, s, P, \omega)$, where $\omega(w, p, v)$ is defined to be $\{ \phi | K, w, v \models p$ says $\phi \}$.

Our first concern is whether $k2b(K)$ produces a belief model that is equivalent to $K$. In particular, a formula should be valid in $K$ iff it is valid in $k2b(K)$. Construction $k2b$ does produce equivalent models:

**Theorem 1.** For all $K$, $w$, $v$, and $\phi$, $K, w, v \models \phi$ iff $k2b(K), w, v \models \phi$.

Our second concern is whether $k2b(K)$ satisfies all the conditions required by § Worldview Monotonicity, Worldview Equality, Worldview Closure, Says Transparency, and Belief Hand-off. If a belief model $B$ does satisfy these conditions, then $B$ is well-formed. And modal model $K$ is well-formed if it satisfies all the conditions required by § Accessibility Equality, IT, ID, F2, H, and WSF. Construction $k2b$ does, indeed, produce well-formed belief models:

**Proposition 2.** For all well-formed modal models $K$, belief model $k2b(K)$ is well-formed.

We might wonder whether there is a construction that can soundly transform belief models into Kripke models. Consider trying to transform the following belief model $B$ into a Kripke model:

$$B$$ has a single world $w$ and a proposition (i.e. a nullary relation) $X$, such that, for all $v$, it holds that $B, w, v \not\models X$. Suppose that principal $p$'s worldview contains $X$—i.e., for all $v$, it holds that $X \in \omega(w, p, v)$—and that $p$’s worldview does not contain false. By the semantics of says, it holds that $B, w, v \models p$ says $X$.

When transforming $B$ to a Kripke model $K$, what edges could we put in $\leq_p$? There are only two choices: $\leq_p$ could be empty, or $\leq_p$ could contain the single edge $(w, w)$. If $\leq_p$ is empty, then $p$ is compromised, hence $p$ says false. That contradicts our assumption that false is not in $p$’s worldview. If $w \leq_p w'$, then for $w'$ and $w''$ such that $w \leq w' \leq w''$, it does not hold that $K, w'', v \models X$, because $w$ and $w''$ can only be instantiated as $w$, and because $B, w, v \not\models X$. Hence $p$ does not say $X$. That contradicts our assumption that $X$ is in $p$’s worldview. So we cannot construct an accessibility relation $\leq_p$ that causes the resulting Kripke semantics to preserve validity of formulas from the belief semantics.

There is, therefore, no construction that can soundly transform belief models into Kripke models—unless, perhaps, the set of worlds is permitted to change. We conjecture that it is possible to synthesize a new set of possible worlds, and equivalence relations on them, yielding a Kripke model that preserves validity of formulas from the belief model.

5. PROOF SYSTEM

FOCAL’s derivability judgment is written $\Gamma \vdash \phi$ where $\Gamma$ is a set of formulas called the context. As is standard, we write $\vdash \phi$ when $\Gamma$ is the empty set. In that case, $\phi$ is a theorem. We write $\Gamma, \phi$ to denote $\Gamma \cup \{\phi\}$.

Figure 5 presents the proof system. In it, $\phi[\tau/x]$ denotes capture-avoiding substitution of $\tau$ for $x$ in $\phi$. The first-order fragment of the proof system is routine (e.g., [38, 46, 50]). Because of IMP, the deduction theorem holds for FOCAL [24]. SAYS-LRI, SAYS-LI, and SAYS-RI use notation $\tau$ says $\Gamma$, which means that $\tau$ says all the formulas in set $\Gamma$. Formally, $\tau$ says $\Gamma$ is defined as $\{ \tau$ says $\phi | \phi \in \Gamma \}$.

The usual sequent calculus structural rules of contraction and exchange are admissible. But weakening (our rule WEAK) is not admissible: it must be directly included in the proof system, because the conclusions of SAYS-LRI, SAYS-LI, and SAYS-RI capture their entire context $\Gamma$ inside says.

SAYS-LRI corresponds to standard axiom $K$ along with rule $N$ from epistemic logic; SAYS-RI, to standard axiom 4; and SAYS-LI, to the converse C4 3 of 4:

$$K: \vdash (p$ says $(\phi \Rightarrow \psi)) \Rightarrow (p$ says $\phi) \Rightarrow (p$ says $\psi),$$

$$N: \text{ From } \vdash \phi \text{ infer } \vdash p$ says $\phi,$

$$4: \vdash (p$ says $\phi) \Rightarrow (p$ says $(p$ says $\phi)),$

$$C4: \vdash (p$ says $(p$ says $\phi)) \Rightarrow (p$ says $\phi).$$

$K$ and SAYS-LRI mean that modus ponens applies inside says. They correspond to Worldview Closure. C4 and 4, along with SAYS-LI and SAYS-RI, mean that $p$ says $(p$ says $\phi)$ is equivalent to $p$ says $\phi$; they correspond to Says Transparency

---

14These formulas are localized hypotheses, which the proof system uses instead of the hypothetical judgments found in natural deduction systems. Similar to the left-hand side $\Gamma \Rightarrow \Delta$, the localized hypotheses are assumptions being used to derive right-hand side $\Delta$. Unlike a sequent, $\Gamma$ is a set, not a sequence.

15Under the usual constructive definition of $\neg \phi \Rightarrow false$, rules NOT-I and NOT-E are admissible and could be eliminated from the proof system.
in the belief semantics. In the Kripke semantics, \( \text{SAYS-RI} \) corresponds to \( \Gamma \), and \( \text{SAYS-LI} \), to \( \Theta \). (Note, we do not argue that 4 and C4 are necessary in authorization logics; we simply show how to support them.)

\( \text{SF-I} \) corresponds to hand-off \( \mathcal{I} \). \( \text{SF-E} \) uses \text{speaksfor} to deduce beliefs. \( \text{SF-R} \) and \( \text{SF-T} \) state that \text{speaksfor} is reflexive and transitive.

### 5.1 Soundness

Our first soundness theorem for FOCAL states that if \( \phi \) is provable from assumptions \( \Gamma \), and that if a belief model validates all the formulas in \( \Gamma \), then that model must also validate \( \phi \). Therefore, any provable formula is valid in the belief semantics:

**Theorem 2.** If \( \Gamma \vdash \phi \) and \( B, w, v \models \Gamma \), then \( B, w, v \models \phi \).

The result is, to our knowledge, the first proof of soundness for an authorization logic w.r.t. a belief semantics. The proof of theorem 2 relies on the following proposition, which states monotonicity of validity w.r.t. \( \leq \):

**Proposition 3.** If \( B, w, v \models \phi \) and \( w \leq w' \) then \( B, w', v \models \phi \).

Our second soundness theorem for FOCAL states that any provable formula is valid in the Kripke semantics:

**Theorem 3.** If \( \Gamma \vdash \phi \) and \( K, w, v \models \Gamma \), then \( K, w, v \models \phi \).

The proof of that theorem relies on proposition 1 (monotonicity of the Kripke semantics). We have mechanized the proofs of theorems 2 and 3 and propositions 1 and 3 in Coq.

### 5.2 State in distributed systems

FOCAL was derived from CDD [2] and NAL [13]. But we deliberately designed the FOCAL proof system such that its theory differs in one important way from theirs. We discuss our motivation for this change, next.

There are two standard ways of “importing” beliefs into a principal’s worldview. The first is rule \( \text{N} \) from [2] also known as the rule of Necessitation: from \( \vdash \phi \), infer \( \vdash p \text{ says } \phi \). The second is an axiom known as Unit: \( \vdash \phi \Rightarrow (p \text{ says } \phi) \).

Though superficially similar, it is well-known that Necessitation and Unit lead to different theories. Abadi [3] explores some of the proof-theoretic differences, particularly some of the surprising consequences of Unit in classical authorization logic. In the example below, we focus on one difference that does not seem to have been explored in constructive authorization logic:

**Example 2.** Machines \( M_1 \) and \( M_2 \) execute processes \( P_1 \) and \( P_2 \), respectively. \( M_1 \) has a register \( R \). Let \( Z \) be a proposition representing “register \( R \) is currently set to zero.” According to Unit, \( \vdash Z \Rightarrow (P_1 \text{ says } Z) \) and \( \vdash Z \Rightarrow (P_2 \text{ says } Z) \). The former means that a process on a machine knows the current contents of a register on that machine; the latter means that a process on a different machine must also know the current contents of the register. But according to Necessitation, if \( \vdash Z \) then \( \vdash Z \Rightarrow (P_1 \text{ says } Z) \). Only if \( R \) is guaranteed to be constant—i.e., it can never at any time be anything other than zero—must the two processes say so.

Unit, therefore, is appropriate when propositions (or relations or functions) represent global state upon which all principals are guaranteed to agree. But when propositions represent local state that could be unknown to some principals, Unit would arguably be an invalid axiom. A counter-model demonstrating Unit’s invalidity is easy to construct—for example, stipulate a world \( w \) at which \( Z \) holds, and let \( P_1 \)’s worldview contain \( Z \) but \( P_2 \)’s worldview not contain \( Z \). That counter-model doesn’t apply to Necessitation, because \( Z \) is not a theorem in it, therefore the principals may disagree on \( Z \)’s validity.

Prior work has objected to Unit for other reasons (cf. [6]), but not for this difference between local and global state. We are unaware of any authorization logic that rejects Ne-
cessitation, which is widely accepted along with axiom $K$ (cf. 5 in normal modal logic 27).

FOCAL is designed for reasoning about state in distributed systems, where principals (such as machines) may have local state, and where global state does not necessarily exist—the reading at a clock, for example, is not agreed upon by all principals. So Unit would be invalid for FOCAL principals; Necessitation is the appropriate choice. We therefore include Necessitation in FOCAL in the form of rule SAYS-LRI. Having that rule in our proof system is equivalent to having both Necessitation and $K$ in a natural-deduction proof system 27 p. 214, where SAYS-LRI is called LRI. Unit, on the other hand, is invalid in FOCAL’s semantics, and FOCAL’s proof system is sound w.r.t. its semantics, so it’s impossible to derive Unit in FOCAL.

Similarly, NAL principals do not necessarily agree upon global state. NAL does include Necessitation as an inference rule and does not include Unit as an axiom. However, NAL permits Unit to be derived as a theorem 19.

NAL’s proof system is, therefore, arguably unsound w.r.t. our belief semantics: there is a formula (Unit) that is a theorem of the system but that is not semantically valid.

NAL extends CDD’s proof system, so we might suspect that CDD is also unsound w.r.t. our semantics. And it is. However, CDD has been proved sound w.r.t. a lax logic semantics 19. That semantics employs a different intuition about says than NAL. CDD understands $p$ says $\phi$ to mean “when combining the [statement $\phi$] that the [guard] believes with those that [$p$] contributes, the [guard] can conclude $\phi$... the [guard’s] participation is left implicit” 2 p. 13. In other words, the guard’s beliefs are imported into $p$’s beliefs at each world. That results in a different meaning of says than FOCAL or NAL employs.

Since Abadi’s invention of CDD 2, the says connective is frequently assumed to satisfy the monad 30 laws, which include Unit. But FOCAL rejects Unit, so FOCAL’s says connective is not a monad. The monad laws also include an axiom named Bind, which turns out to be invalid in FOCAL’s semantics 19. We don’t know whether rejecting the monad laws will have any practical impact on FOCAL. But the seminal authorization logic, ABLP 4, didn’t adopt the monad laws. Likewise, Garg and Pfenning 21 reject Unit in their authorization logic BL_0: they demonstrate that Unit leads to counterintuitive interpretations of some formulas involving delegation. And Abadi 1 notes that Unit “should be used with caution (if at all),” suggesting that it be replaced with the weaker axiom $(p$ says $\phi) \Rightarrow (q$ says $p$ says $\phi)$. Genovese et al. 22 carry out that suggestion. So in rejecting the monad laws, FOCAL is at least in good company.

6. RELATED WORK

FOCAL has the first formal belief semantics of any authorization logic. Belief semantics have been used in only one other authorization logic, NAL 43, which has only an informal semantics based on worldviews.

But many of the pieces of FOCAL, including its semantics and proof system, are naturally derived from previous work. We summarize here what we borrowed vs. what we invented; the main body of the paper contains detailed citations. FOCAL’s belief semantics is a standard first-order constructive semantics, but the addition of worldviews to interpret says and speaksfor is novel (with the exception of NAL, which used worldviews informally). FOCAL’s Kripke semantics for everything except speaksfor is likewise standard, and its frame conditions (except H and WSF) are already well-known in constructive modal logic, but the application of IT and ID to authorization logic seems to be novel. FOCAL’s proof system, excluding says and speaksfor, is a straightforward first-order constructive proof system. The fragment for says is our own adaptation of natural-deduction rules for the $\Box$ connective. The fragment for speaksfor corresponds to standard definitions used in many authorization logics.

Semantic structures similar to our belief models have been investigated in the context of epistemic logic 13, 14, 27. Konolige 30 proves an equivalence result for classical propositional logic similar to our theorem 1.

Garg and Abadi 19 give a Kripke semantics for a logic they call ICL, which could be regarded as a propositional fragment of FOCAL. The ICL semantics of says, however, uses invisible worlds to permit principals to be oblivious to the truth of formulas at some worlds. That makes Unit 32 valid in ICL, whereas Unit is invalid in FOCAL.

Garg 18 studies the proof theory of a logic called DTL_0, and gives a Kripke semantics that uses both invisible worlds and fallible worlds, at which false is permitted to be valid. Instead of Unit, it uses the axiom $p$ says $(p$ says $\phi)$ $\Rightarrow \phi$. That axiom is unsound in FOCAL. DTL_0 does not have a speaksfor connective.

Genovese et al. 22 study several uses for Kripke semantics with an authorization logic they call BL_0, which could also be regarded as a propositional fragment of FOCAL. They show how to generate evidence for why an access should be denied, how to find all logical consequences of an authorization policy, and how to determine which additional credentials would allow an access. However, the Kripke semantics of BL_0 differs from FOCAL’s in its interpretation of both says and speaksfor, so the results of Genovese et al. are not immediately applicable to FOCAL.

Garg and Pfenning 24 prove non-interference properties for a first-order constructive authorization logic. Such properties mean that one principal’s beliefs cannot interfere with another principal’s beliefs unless there is some trust relationship between those principals. Abadi 2 also proves such a property for dependency core calculus (DCC), which is the basis of authorization logic CDD. We conjecture that similar properties could be proved for FOCAL.

7. CONCLUDING REMARKS

This work began with the idea of giving a Kripke semantics to NAL. Proving soundness—at first on paper, not in Coq—turned out to be surprising, because Unit is semantically invalid but derivable in NAL (§5.2). The complexity
of the resulting Kripke semantics motivated us to seek a simpler semantics. We were inspired by the informal view semantics of the NAL rationale\textsuperscript{[13]} and elaborated that into our belief semantics\textsuperscript{[3]}.

In future work, we plan to upgrade FOCAL to handle NAL’s advanced features, including intensional group principals.

Mechanizing the proofs of soundness in Coq was frequently rewarding. It exposed several bugs (in either our proof system or our semantics) and gave us high confidence in the correctness of the result. We expect further benefits, too. Other researchers can now use our formalization as a basis for mechanizing results about authorization logics. And from the formalization of the FOCAL proof system in Coq, we could next extract a verified theorem checker. It would input a proof of a FOCAL formula, expressed in the FOCAL proof system, and output whether the proof is correct. Coq would verify that the checker correctly implements the FOCAL proof system. After FOCAL is upgraded to handle all of NAL’s features, the resulting theorem checker could replace the current Nexus\textsuperscript{45} theorem checker, which is implemented in C. A verified theorem checker would arguably be more trustworthy than the C implementation, thus increasing the trustworthiness of the operating system.

Our goal was to increase the trustworthiness of authorization logics, hence our concentration on soundness results. Another worthwhile goal would be to increase the utility of authorization logics, and toward that end we could investigate the completeness of FOCAL: are all valid formulas provable? A few authorization logics—ICL\textsuperscript{[19]}, DTL\textsubscript{0}\textsuperscript{[18]} and BL\textsubscript{sf}\textsuperscript{[22]}—do have completeness results for Kripke semantics; however, none of those is immediately applicable to FOCAL\textsuperscript{[20]}.

We leave adaptation of them as future work.

Acknowledgments

Fred B. Schneider consulted on the design of the proof system and the Kripke semantics, and he suggested the idea of proving an equivalence between belief and Kripke semantics. We thank him, Martin Abadi, Deepak Garg, Joe Halpern, Dexter Kozen, Colin Stirling, and Kevin Walsh for discussions related to this work. We also thank Adam Chlipala, Kristopher Micinski, and the coq-club mailing list for assistance with Coq. The anonymous reviewers of CSF 2013 and CCS 2013 provided invaluable feedback. The Kripke semantics of FOCAL was created while Clarkson was a post-doctoral researcher at Cornell. This work was supported in part by AFOSR grants F9550-06-0019, FA9550-11-1-0137, and FA9550-12-1-0334, NSF grants 0430161, 0964409, and CCF-0424422 (TRUST), ONR grants N00014-01-1-0968 and N00014-09-1-0652, and a grant from Microsoft.

8. REFERENCES


APPENDIX: PROOFS

Proposition 1
If $K, w, v \models \phi$ and $w \leq w'$ then $K, w', v \models \phi$.

Proof. By structural induction on $\phi$. This proof has been mechanized in Coq.

Theorem 1
For all well-formed modal models $K$, it holds that $K, w, v \models \phi$ iff $k2b(K), w, v \models \phi$.

Proof. First, we show the forward direction: $K, w, v \models \phi$ implies $k2b(K), w, v \models \phi$. All of the cases except says and speaksfor are straightforward, because those are the only two cases where the interpretation of formulas differs in the two semantics.

- Case $\phi = \tau$ says $\psi$. Suppose $K, w, v \models \tau$ says $\psi$. By the definition of $k2b$, formula $\psi \in \omega(w, \mu(\tau), v)$. By the belief semantics of says, it must hold that $k2b(K), w, v \models \tau$ says $\psi$.

- Case $\phi = \tau$ speaksfor $\tau'$. Assume $K, w, v \models \tau$ speaksfor $\tau'$. We need to show that, for all $w' \geq w$, it holds that $\omega(w', \mu(\tau), v) \subseteq \omega(w', \mu(\tau'), v)$. So let $w'$ and $\psi$ be arbitrary such that $w' \geq w$ and $\psi \in \omega(w', \mu(\tau), v)$, and we'll show that $\psi \in \omega(w', \mu(\tau'), v)$.

Second, we show the backward direction: $K, w, v \models \phi$ is implied by $k2b(K), w, v \models \phi$. Again, all of the cases except says and speaksfor are straightforward, because those are the only two cases where the interpretation of formulas differs in the two semantics.

- Case $\phi = \tau$ says $\psi$. Suppose $k2b(K), w, v \models \tau$ says $\psi$. By the belief semantics of says, we have that $\psi \in \omega(w, \mu(\tau), v)$. By the definition of $k2b$, it holds that $K, w, v \models \tau$ says $\psi$.

- Case $\phi = \tau$ speaksfor $\tau'$. Assume $k2b(K), w, v \models \tau$ speaksfor $\tau'$. By the belief semantics of speaksfor, we have that, for all $w' \geq w$, it holds that $\omega(w', \mu(\tau), v) \subseteq \omega(w, \mu(\tau'), v)$. Let $w'$ be arbitrary such that $w' \geq w$. Then $\omega(w, \mu(\tau), v) \subseteq \omega(w, \mu(\tau'), v)$. By the definitions of $k2b$ and subset, it follows that, for all $\phi$, if $K, w, v \models \tau$ says $\phi$ then $K, w, v \models \tau$ says $\phi$. By WSF, we therefore have that $K, w, v \models \tau$ speaksfor $\tau'$.

Proposition 2
For all well-formed modal models $K$, belief model $k2b(K)$ is well-formed.

Proof. Let $B = k2b(K)$. For $B$ to be well-formed it must satisfy several conditions, which were defined in [2]. We now show that these hold for any such $B$ constructed by $k2b$.

1. Worldview Monotonicity. Assume $w \leq w'$ and $\phi \in \omega(w, p, v)$. By the latter assumption and the definition of $k2b$, we have that $K, w, v \models \rho$ says $\phi$. From proposition 1 it follows that $K, w', v \models \rho$ says $\phi$. By the definition of $k2b$, it then holds that $\phi \in \omega(w', p, v)$. Therefore $\omega(w, p, v) \subseteq \omega(w', p, v)$.

2. Worldview Equality. Assume $p \equiv p'$. Then by Accessibility Equality, $\leq_p$ equals $\leq_{p'}$. By the Kripke semantics of says, it follows that $K, w, v \models \rho$ says $\phi$ iff $K, w, v \models p'$ says $\phi$. By the definition of $k2b$, therefore, $\omega(w, p, v) = \omega(w, p', v)$.

3. Worldview Closure. Assume $\Gamma \subseteq \omega(w, p, v)$ and $\Gamma \models \phi$. Then by the definition of $k2b$, we have that $\omega(w, p, v)$ is well-formed. Therefore $\omega(w, p, v) \subseteq \omega(w, p', v)$.

4. Says Transparency. We prove the “iff” by proving both directions independently.

- ($\Rightarrow$) Assume $\phi \in \omega(w, p, v)$. By the definition of $k2b$, it holds that $P, w, v \models \rho$ says $\phi$. From IT and F2, it follows that $K, w, v \models \rho$ says $\phi$. By the definition of $k2b$, therefore, $\rho$ says $\phi \in \omega(w, p, v)$.

- ($\Leftarrow$) Assume $\rho$ says $\phi \in \omega(w, p, v)$. By the definition of $k2b$, it holds that $K, w, v \models \rho$ says $\phi$. From ID, it follows that $K, w, v \models \rho$ says $\phi$. By the definition of $k2b$, therefore, $\phi \in \omega(w, p, v)$.

5. Belief Hand-off. We actually prove a stronger result—an “iff” rather than just an “if”. By the definitions of subset and $k2b$, we have that $\omega(w, p, v) \subseteq \omega(w, q, v)$ holds iff for all $\phi$, if $K, w, v \models \rho$ says $\phi$ then $K, w, v \models q$ says $\phi$. By WSF, that holds iff $K, w, v \models \rho$ speaksfor $\rho$. By the fact below, that holds iff $K, w, v \models \rho$ speaksfor $\rho$. By the definition of $k2b$, that holds iff $\rho$ speaksfor $\rho$ in $\omega(w, q, v)$.

Fact: in the Kripke semantics, $\models \rho$ speaksfor $\rho$ iff $\rho$ speaksfor $\rho$. The proof of that fact has been mechanized in Coq.

Theorem 2
If $\Gamma \models \phi$ and $B, w, v \models \Gamma$, then $B, w, v \models \phi$.

Proof. By induction on the derivation of $\Gamma \models \phi$. This proof has been mechanized in Coq.

Theorem 3
If $\Gamma \models \phi$ and $K, w, v \models \Gamma$, then $K, w, v \models \phi$.

Proof. By induction on the derivation of $\Gamma \models \phi$. This proof has been mechanized in Coq.

Proposition 3
If $B, w, v \models \phi$ and $w \leq w'$ then $B, w', v \models \phi$.

Proof. By structural induction on $\phi$. This proof has been mechanized in Coq.