1

Modal Logics with a Linear Hierarchy of Local Propositional Quantifiers[1]

Kai Engelhardt, Ron van der Meyden[2], and Kaile Su[3]

ABSTRACT. Local propositions arise in the context of the semantics for logics of knowledge in multi-agent systems. A proposition is local to an agent when it depends only on that agent's local state. We consider a logic, LLP, that extends S5, the modal logic of necessity (in which the modality refers to truth at all worlds) by adding a quantifier ranging over the set of all propositions and, for each agent, a propositional quantifier ranging over the agent's local propositions. LLP is able to express a large variety of epistemic modalities, including knowledge, common knowledge and distributed knowledge. However, this expressiveness comes at a cost: the logic is equivalent to second order predicate logic when two independent agents are present [5], hence undecidable and not axiomatizable. This paper identifies a class of multi-agent S5 structures, *hierarchical structures*, in which the agents' information has the structure of a linear hierarchy. All systems with just a single agent are hierarchical. It is shown that LLP becomes decidable with respect to hierarchical systems. The main result of the paper is the completeness of an axiomatization for the hierarchical case.

1 Introduction

Although modal logics are most commonly studied in their propositional forms, which may often be interpreted in first order logic, the topic of modal logics with second order expressive power is almost as old as the field itself. Motivated by earlier applications of quantification over propositions in the

[1]Research supported by Australian Research Council Large grant A10030007.

[2]School of Computer Science and Engineering, The University of New South Wales, Sydney 2052 Australia, for $X \in$ {kaie, meyden}, email: X@cse.unsw.edu.au , www: http://www.cse.unsw.edu.au/~X.

[3]Institute of Logic and Cognition, Zhongshan University, China, email issskls@zsu.edu.cn. Work of the third author performed while a visiting fellow at UNSW. Also partially supported by the National Natural Science Foundation of China under Grant 60073056, the Guangdong Provincial Natural Science Foundation under Grant 001174, and the MOE Project of Key Research Institute of Humanities and Social Science in University.

Advances in Modal Logic, Volume 4, 1–22.

context of conditional logic, Kripke's early work on the semantics of modal logic [14] already contains an axiomatization of the logic S5 combined with quantification over propositions.

Kripke's assumptions concerning the range of the propositional quantifiers were somewhat unnatural, however. Further progress in the area was made in the 1960's, with Fine, Bull, and Kaplan [8, 2, 13] establishing axiomatizations and decidability results of several more natural variants. Decidability of S5 plus propositional quantification can be seen from the decidability of monadic second order logic [1].

The above works consider logics with a single modality. Motivated by applications of the logic of knowledge in distributed systems [10], Engelhardt, van der Meyden, and Moses [5] consider propositional quantification in a multi-modal S5 setting. A natural notion in this setting is that of *local* propositions. Local propositions arise in the context of the semantics for *logics of knowledge* in distributed systems due to Halpern and Moses [10]. In this semantics, each agent in a system has in each configuration of the system a local state, representing the information it has about the global state of the system and its history. A proposition is local for the agent when it is a function of this local state.

Engelhardt, van der Meyden, and Moses [5] show that S5 (with the modality interpreted as truth in all possible worlds) when combined with quantification over local propositions provides a framework that is able to express a large variety of epistemic modalities, including knowledge, common knowledge, and distributed knowledge [6].

In the most general case, in which more than one independent agent is involved, the logic obtained by adding local propositional quantifiers to S5 is highly undecidable [5], (indeed, equivalent to second order predicate logic) hence this logic is also not axiomatizable. After introducing syntax and semantics of this logic in Sect. 2, we identify a natural restriction on the semantic structures, expressing that the agents' information has the structure of a linear hierarchy, with respect to which the logic is decidable even in the multi-agent case. The single agent case satisfies this condition. A practical example in which hierarchical structures arise is information-based models for computer security, which frequently assume a linear hierarchy of secrecy levels [4]. We provide an axiomatization for the hierarchical case in Sect. 3. Bounded model property, decidability, and completeness follow from a normal form result presented in Sect. 4. Sect. 5 concludes and indicates directions for future work.

2 Syntax and Semantics

We deal with a class of Kripke structures suited to a multi-modal logic, of the kind used in the literature on reasoning about knowledge [6]. Let *Prop* be an infinite set of propositional variables. A *Kripke structure for n agents* $M = (W, R_1, \ldots, R_n, \pi)$ consists of a set W of possible worlds, binary accessibility relations $R_1, \ldots, R_n \subseteq W^2$, and an assignment $\pi : \mathit{Prop} \longrightarrow 2^W$ of propositions to the propositional variables. Each relation R_i represents the information available to agent i. Intuitively, $u\, R_i\, v$ for two worlds u and v when, from agent i's point of view, these worlds are indistinguishable. As is usual in the literature on knowledge, we assume that the accessibility relations R_i are equivalence relations. Structures satisfying this restriction are called *S5$_n$ structures*.

A *proposition* in such a structure is a subset of the set of worlds W, intuitively, just the worlds where the proposition is true. We will be concerned with a special class of propositions. For each agent i, a proposition is called *i-local* if it is a union of R_i-equivalence classes. Intuitively, the i-local propositions are those that depend only upon agent i's information. Agent i can always determine whether a given i-local proposition is true.

While the class of S5$_n$ structures is standard, the language we consider is not the usual one from the knowledge literature. Write p for a typical element of *Prop*. Define the language $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ with typical element ϕ by:

$$\phi ::= p \;\mid\; \neg\phi \;\mid\; \phi \wedge \phi \;\mid\; \Box\phi \;\mid\; \forall p\,(\phi) \;\mid\; \forall_i p\,(\phi)$$

We employ parentheses to indicate aggregation and take *true*, $\vee$, $\Diamond$, $\exists p\,()$, and the remaining familiar connectives to be defined in the usual way. Intuitively, $\Box\phi$ says that ϕ is true in all possible worlds. The formula $\forall p\,(\phi)$ says that ϕ is true for all assignments of a proposition to the propositional variable p. The meaning of $\forall_i p\,(\phi)$ is similar, but here p is restricted to range over i-local propositions.

These intuitions are made precise as follows. Another S5$_n$ structure $M' = (W', R'_1, \ldots, R'_n, \pi')$ is a p-variant of M (denoted $M' \simeq_p M$) if it differs from M at most on the interpretation of p. That is, $M' \simeq_p M$ if we have $W' = W$, the relation $R'_i = R_i$ for each $i = 1 \ldots n$, and $\pi'(q) = \pi(q)$ for all $q \in \mathit{Prop} \setminus \{p\}$. If, moreover, $\pi'(p)$ is i-local then M' is called an *i-local p-variant* (denoted $M' \simeq^i_p M$). Formulas are interpreted at a world w of a structure M by means of the satisfaction relation $\models$, defined inductively by:

$$
\begin{array}{rcl}
M, w \models p & \text{iff} & w \in \pi(p) \\
M, w \models \neg\phi & \text{iff} & M, w \not\models \phi \\
M, w \models \phi \wedge \psi & \text{iff} & M, w \models \phi \text{ and } M, w \models \psi \\
M, w \models \Box\phi & \text{iff} & \forall v \in W\, (M, v \models \phi) \\
M, w \models \forall p\, (\phi) & \text{iff} & \forall M' \simeq_p M\, (M', w \models \phi) \\
M, w \models \forall_i p\, (\phi) & \text{iff} & \forall M' \simeq_p^i M\, (M', w \models \phi)
\end{array}
$$

Let $\mathcal{M}$ be a class of Kripke structures for n agents. We say that ϕ is *satisfiable* in $\mathcal{M}$ iff $M, w \models \phi$ for some $M \in \mathcal{M}$ and some possible world w of M.

We write $\mathcal{L}_{(o_1,\ldots,o_m)}$ for the language generated from a set *Prop* of propositional variables by $\vee$, $\neg$, and operators o_i. Fine, Bull, and Kaplan discussed axiomatizations of $\mathcal{L}_{(\forall,\Box)}$ [8, 2, 13] and Fine already claimed decidability. The local propositional quantifiers were introduced in [5]. These quantifiers are of interest because they are able to express many of the knowledge-like notions, including common knowledge and distributed knowledge, that have been discussed in the literature. This point is discussed at greater length elsewhere [5]. We confine ourselves here to an illustration using the standard knowledge operators K_i and modalities L_i expressing *i-locality* of formulas. The semantics of these operators is defined as follows.

$$
\begin{array}{rcl}
M, w \models K_i\phi & \text{iff} & \forall v \in W\, (w\, R_i\, v \Rightarrow M, v \models \phi) \\
M, w \models L_i\phi & \text{iff} & \{\, v \in W \mid M, v \models \phi \,\} \text{ is } i\text{-local}
\end{array}
$$

The expressive power of $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ is illustrated by the fact that the operators $\forall_i$, K_i, and L_i are interexpressible in the presence of $\Box$ and $\forall$:

$$K_i\phi \equiv \exists_i p\, (p \wedge \Box(p \to \phi)) \quad \text{, provided } p \text{ not free in } \phi \tag{1}$$

$$L_i\phi \equiv \exists_i p\, (\Box(p \equiv \phi)) \quad \text{, provided } p \text{ not free in } \phi \tag{2}$$

$$\forall_i p\, (\phi) \equiv \forall p\, (L_i p \to \phi) \tag{3}$$

Note that in $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ one can express that the set of worlds at which p is true is an R_i-equivalence class, which we abbreviate to $\mathcal{E}_i p$:

$$\mathcal{E}_i p \equiv \Diamond p \wedge L_i p \wedge \forall_i q\, (\Diamond(p \wedge q) \to \Box(p \to q)) \tag{4}$$

Unfortunately, the expressiveness of $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ comes at a cost. Even if there are just two agents, satisfiability is undecidable for this language [5], when interpreted over all $\mathrm{S5}_n$ structures. As the use of two agents appears essential in this result, this motivates the consideration of two variants: (i) the single agent case, and (ii) restricted classes of structures. We focus in this paper on the following class that subsumes both variants. An $S5_n$ structure $(W, R_1, \ldots, R_n, \pi)$ is *hierarchical* if $R_{i-1} \subseteq R_i$, for $1 < i \leq n$. That is, in such structures, i-local propositions are also $(i-1)$-local, and $\forall_i$-quantification is weaker than $\forall_{i-1}$-quantification. Note that every $S5_1$ structure is hierarchical, so results on hierarchical structures also apply to the single agent case.

3 A Proof System

Our axiomatization of hierarchical $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ below consists of an adaptation of Fine's for $\mathcal{L}_{(\forall,\Box)}$ [8]. Fine's axiomatization consists of the following. For the propositional basis, we have the usual axioms and inference rule:

$$\text{all substitution instances of propositional tautologies} \qquad \textbf{PC}$$

$$\phi \to \psi, \phi \vdash \psi \qquad \textbf{MP}$$

The operator $\Box$ is interpreted as necessity, so we have the axioms and inference rules of S5 for this modality:

$$\vdash \Box\phi \to \phi \qquad \textbf{T}_{\Box}$$

$$\vdash \Diamond\phi \to \Box\Diamond\phi \qquad \textbf{5}_{\Box}$$

$$\vdash \Box(\phi \to \psi) \to (\Box\phi \to \Box\psi) \qquad \textbf{K}_{\Box}$$

$$\phi \vdash \Box\phi \qquad \textbf{RN}_{\Box}$$

For the universal quantification over propositions, we have a set of axioms and a rule of inference that resemble closely the usual rules for predicate logic, the main difference being that we substitute formulas where we would substitute terms in predicate logic:

$$\vdash \forall p\,(\phi) \to \phi[^{\psi}/_{p}] \text{ , where } \psi \text{ is free for } p \text{ in } \phi \qquad \textbf{1}_{\forall}$$

$$\vdash \forall p\,(\phi \to \psi) \to (\forall p\,(\phi) \to \forall p\,(\psi)) \qquad \textbf{K}_{\forall}$$

$$\vdash \phi \to \forall p\,(\phi) \text{ , where } p \text{ not free in } \phi \qquad \textbf{N}_{\forall}$$

$$\phi \vdash \forall p\,(\phi) \qquad \textbf{G}$$

Additionally, we have an axiom that captures the fact that the lattice of propositions in a Kripke structure is atomic. The following axiom can be understood as saying that the proposition p, which is true only at the current world, is a subset of all propositions true at the current world.

$$\vdash \exists p\,(p \wedge \forall q\,(q \to \Box(p \to q))) \qquad \textbf{AT}$$

Fine [8] established that the above axioms are sound and complete for $\mathcal{L}_{(\forall,\Box)}$.

We note the following property of the axiomatization. Let ψ be a formula with free variables including e and p. Let $p_1, p_2 \in \mathit{Prop}$ be free for p in ψ. The formula

$$\forall p_1 \left(\forall p_2 \left(\Box(e \to (p_1 \equiv p_2)) \to (\psi[^{p_1}/_{p}] \equiv \psi[^{p_2}/_{p}])\right)\right)$$

expresses that the truth value of ψ *depends only on the values of* p *in* e. Then for formulas $\alpha_1, \ldots, \alpha_k$ free for e in a formula ψ we have

$$\vdash \begin{pmatrix} \forall e \left(\forall p_1, p_2 \left(\Box(e \to (p_1 \equiv p_2)) \to (\psi[^{p_1}/_{p}] \equiv \psi[^{p_2}/_{p}])\right)\right) \\ \wedge \bigwedge_{i \neq j} \Box(\neg(\alpha_i \wedge \alpha_j)) \\ \to \exists p \left(\bigwedge_{i=1}^{k} \psi[^{\alpha_i}/_{e}]\right) \end{pmatrix} \qquad \textbf{Ch}$$

Intuitively, this formula says that if ψ depends only on the values of p in e then we may take a set of propositions that have some desirable properties on a finite, mutually exclusive collection of pieces e of the model (defined by the α_i), and combine these propositions into a single proposition p that satisfies ψ on each piece e.

We now extend the axioms above to an axiomatization for $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$. (In this axiomatization, we take the previous axioms **PC** – **AT** to refer to $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$-formulas.) We add three sets of axioms. The first set consists of axioms relating the local propositional quantifiers to the standard propositional quantifier. The second set concerns the hierarchy between the local quantifiers. The final axiom generalizes the finite choice property.

For each of the universal quantification operators over i-local propositions for $1 \leq i \leq n$, the following axioms characterize the local quantifiers. We use $L_i\phi$ as an abbreviation for $\exists_i p\,(\Box(p \equiv \phi))$, which expresses that ϕ is an i-local proposition, as noted above. The first axiom characterizes i-local propositional quantification as the restriction of propositional quantification to i-local propositions:

$$\vdash \forall_i p\,(\phi) \equiv \forall p\,(L_i p \to \phi) \qquad \textbf{Def}\forall_i$$

The following axiom says that locality of a proposition is independent of the world.

$$\vdash L_i\phi \to \Box L_i\phi \qquad \textbf{NL}_i$$

The following is a variant of the atomicity axiom, but dealing with local propositions.

$$\vdash \exists_i p\,(p \wedge \Box(p \to \forall_i q\,(q \to \Box(p \to q)))) \qquad \textbf{AT}_i$$

Intuitively, this axioms says that there exists an i-local proposition p which is, at every world where p holds, the smallest i-local proposition holding at that world. Next, we have an axiom that says that local propositions are closed under union.

$$\vdash \forall p\,(\theta(p) \to L_i p) \to L_i(\exists q\,(\theta(q) \wedge q)) \qquad \mathbf{U}_i$$

where $\theta(q)$ is some formula with free variable q. To establish the hierarchy on the agents' knowledge, for $1 < i \leq n$, we have the following:

$$\vdash \forall p\,(\phi) \to \forall_1 p\,(\phi) \qquad \mathbf{H}_\forall$$

$$\vdash \forall_{i-1} p\,(\phi) \to \forall_i p\,(\phi) \qquad \mathbf{H}_{\forall_i}$$

The final axiom generalizes the finite choice property **Ch** noted above:

$$\vdash \left(\begin{array}{c} \forall e\,(\forall p_1, p_2\,(\Box(e \to (p_1 \equiv p_2)) \to (\psi[^{p_1}/_p] \equiv \psi[^{p_2}/_p]))) \\ \wedge\, \forall e, e' \left(\theta \wedge \theta[^{e'}/_e] \to (\Diamond(e \wedge e') \to \Box(e \equiv e'))\right) \\ \to (\forall e\,(\theta \to \exists p\,(\psi)) \to \exists p\,(\forall e\,(\theta \to \psi))) \end{array} \right) \qquad \textbf{Choice}$$

where θ is a formula not containing p free. The antecedent of this axiom states that ψ depends only on the values of p in e, and that the formula θ defines a collection of disjoint sets of worlds. The conclusion of the formula says that if for each of these sets of worlds e there exists proposition p making ψ true, then there is a single proposition p that makes ψ true for all the sets e satisfying θ simultaneously. This axiom is valid if the axiom of choice holds in our semantic meta-theory.

This axiom is also valid for $\mathcal{L}_{(\forall,\Box)}$, but does not need to be stated as part of the axiomatization for that language because of its limited expressive power. A difference that emerges in $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ is that we may take θ to express properties such as $\mathcal{E}_i e$, i.e., "e is an R_i-equivalence class", that define an infinite collection of disjoint sets. This is not possible for $\mathcal{L}_{(\forall,\Box)}$. (This impossibility claim follows from the completeness proof for $\mathcal{L}_{(\forall,\Box)}$, which is given below.)

Write $\texttt{LLPH}_n$ for the above set of axioms and inference rules. We say that ϕ is *derivable*, and write $\vdash \phi$, when the formula ϕ can be derived using the axioms and rules of inference above. The main result of the paper is the following.[1]

THEOREM 1 *Assume the axiom of choice holds meta-theoretically. Then* $\texttt{LLPH}_n$ *is a sound and complete axiomatization of* $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ *with respect*

[1] We have not investigated completeness when we do not assume the axiom of choice semantically.

to hierarchical $S5_n$ structures. The language has the finite model property with respect to these structures.

3.1 Some Theorems of $\texttt{LLPH}_n$

We list some derived rules and theorems of $\texttt{LLPH}_n$. We first note that a set of axioms and a rule for the local quantifiers, corresponding to the axioms and rule for the global propositional quantifier, can be straightforwardly derived using $\mathbf{Def}\forall_i$:

$$\vdash \forall_i p\,(\phi) \to (L_i\psi \to \phi[^{\psi}/_{p}]) \text{ , where } \psi \text{ is free for } p \text{ in } \phi \qquad \mathbf{1}_{\forall_i}$$
$$\vdash \forall_i p\,(\phi \to \psi) \to (\forall_i p\,(\phi) \to \forall_i p\,(\psi)) \qquad \mathbf{K}_{\forall_i}$$
$$L_i p \to \phi \vdash \forall_i p\,(\phi) \qquad \mathbf{G}_i$$
$$\vdash \phi \to \forall_i p\,(\phi) \text{ , where } p \text{ not free in } \phi \qquad \mathbf{N}_{\forall_i}$$

The Barcan formula is derivable using the same argument used to derive it in predicate S5 [11].

$$\vdash \forall p\,(\Box\phi) \equiv \Box\forall p\,(\phi)$$

Using $\mathbf{NL}_i$, we also obtain the Barcan formula for the i-local quantifiers.

$$\vdash \forall_i p\,(\Box\phi) \equiv \Box\forall_i p\,(\phi)$$

We can also establish some additional properties of the locality predicate. Using $\mathbf{AT}_i$ and $\mathbf{U}_i$, we obtain that the set of local propositions is closed under complementation:

$$\vdash L_i\phi \to L_i\neg\phi \qquad \mathbf{Comp}_i$$

Defining $K_i\phi$ as an abbreviation for $\exists_i p\,(p \wedge \Box(p \to \phi))$, we can now derive that K_i satisfies the axioms and rule of S5:

$$\vdash K_i(\phi \to \psi) \to (K_i\phi \to K_i\psi) \qquad \mathbf{K}_{K_i}$$
$$\vdash K_i\phi \to \phi \qquad \mathbf{T}_{K_i}$$
$$\vdash \neg K_i\phi \to K_i\neg\phi \qquad \mathbf{5}_{K_i}$$
$$\phi \vdash K_i\phi \qquad \mathbf{N}_{K_i}$$

The proof of $\mathbf{K}_{K_i}$ uses the fact that the local propositions are closed under intersection, which follows from $\mathbf{Comp}_i$ and $\mathbf{U}_i$. The proof of $\mathbf{5}_{K_i}$ uses $\mathbf{AT}_i$. Finally, we have some derivable formulas that express properties of R_i-equivalence classes and their relation to local propositions:

$$\vdash \mathcal{E}_i e \to \Box \mathcal{E}_i e \qquad \mathbf{EC}_1$$

$$\vdash \mathcal{E}_i e \land \forall e' \, (\Box(e' \to e) \land \mathcal{E}_{i-1} e' \to \Box(e' \to \phi)) \to \Box(e \to \phi) \qquad \mathbf{EC}_2$$

$$\vdash \forall e \, (\mathcal{E}_i e \to \Box(e \to p) \lor \Box(e \to \neg p)) \to L_i p \qquad \mathbf{EC}_3$$

$$\vdash (\mathcal{E}_i e \land \Diamond(e \land p) \land \Diamond(e \land \neg p)) \to \neg L_i p \qquad \mathbf{EC}_4$$

$\mathbf{EC}_1$ says that whether or not a proposition is an equivalence class is independent of the world of evaluation. The fact that an R_i-equivalence class is the union of the R_{i-1}-equivalence classes it contains is expressed by $\mathbf{EC}_2$. The formulas $\mathbf{EC}_3$ and $\mathbf{EC}_4$ allow us to derive conclusions about the i-locality of a proposition. Intuitively, a proposition is i-local if it is determinate within each R_i-equivalence class.

4 A Normal Form

The proof of the completeness result for $\mathtt{LLPH}_n$ is by means of a normal form for $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ over hierarchical structures. A side effect of the normal form result is a proof that the logic is decidable.

4.1 Completeness for $\mathcal{L}_{(\forall,\Box)}$

Since the construction for $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ is moderately complex, we first illustrate the idea of the proof on the restricted case of $\mathcal{L}_{(\forall,\Box)}$. (Note that since models for this language have no accessibility relations, all structures are hierarchical.) We discuss the generalizations required to deal with $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ in the next section. (The axiomatization $\mathtt{LLPH}_0$ for $\mathcal{L}_{(\forall,\Box)}$ omits the axioms for the local quantifiers and their hierarchy.)

Decidability and completeness for $\mathcal{L}_{(\forall,\Box)}$ were already established by Fine and Kaplan [8, 13]. They have proofs based on the *graded modalities* [9, 12, 7, 3].[2] These are the unary modalities C_l, for l a natural number. The semantics for the graded modal logic $\mathcal{L}_{(\mathsf{C}_1,\mathsf{C}_2,\ldots)}$ is based on the same set of structures as used for $\mathcal{L}_{(\forall,\Box)}$, i.e., Kripke structures for 0 agents of the form $M = (W, \pi)$. The semantics of the graded modalities is defined by

[2] As the proofs in the readily accessible literature are sketchy, we do not know if the completeness arguments used by these authors are the same as those we present. Our expression of the graded modalities is similar to those by Fine and Kaplan. Fine states that decidability can be proved by a quantifier elimination argument using the graded modalities and that this can be used to prove completeness but does not provide details of the normal form.

$M, w \models \mathsf{C}_l\phi$ if there are at least l distinct possible worlds $v \in W$ with $M, v \models \phi$.

Note that we may express the graded modal logic formula $\mathsf{C}_l\phi$ in $\mathcal{L}_{(\forall,\Box)}$ as[3]

$$\exists q_1 \ldots \exists q_l \left(\bigwedge_{1 \leq i < j \leq l} \Box[q_i \rightarrow \neg q_j] \wedge \bigwedge_{i=1}^{l} (\Diamond q_i \wedge \Box[q_i \rightarrow \phi]) \right)$$

where q_i is the i-th propositional variable not free in ϕ and $1 \leq i \leq l$. We use $\mathsf{E}_l\phi$ as an abbreviation for the translation of the graded modal logic formula $\mathsf{C}_l\phi \wedge \neg \mathsf{C}_{l+1}\phi$, which states that there are exactly l worlds satisfying ϕ. We also define the abbreviation $\mathsf{M}_{l,N}\phi$, to be $\mathsf{E}_l\phi$ if $l < N$ and $\mathsf{C}_l\phi$ if $l \geq N$.

Let $\mathbf{p} = p_1, \ldots, p_m$ be a vector of propositional variables. Define a *point atom* for $\mathbf{p}$ to be a formula of the form $l_1 \wedge \ldots \wedge l_m$ where each l_i is either p_i or $\neg p_i$. Write $\mathrm{PA}(\mathbf{p})$ for the set of point atoms of $\mathbf{p}$.

Given a point atom a for $\mathbf{p}$ and a number N, define an *N-bounded count* of a to be either a formula of the form $\mathsf{E}_l a$ where $l < N$, or the formula $\mathsf{C}_N a$. Define a *$(\mathbf{p}, k)$-atom* to be a formula of the form

$$a \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} c_b$$

where a is a point atom for $\mathbf{p}$ and c_b is an 2^k-bounded count of b for each $b \in \mathrm{PA}(\mathbf{p})$, such that c_a is not $\mathsf{E}_0 a$. We write $\mathrm{At}(\mathbf{p}, k)$ for the set of $(\mathbf{p}, k)$-atoms. These atoms have the following properties.

LEMMA 2

1. *If $A, A' \in \mathrm{At}(\mathbf{p}, k)$ are distinct atoms, then* $\vdash \neg(A \wedge A')$.
2. $\vdash \bigvee_{A \in \mathrm{At}(\mathbf{p},k)} A$
3. *If $A, A' \in \mathrm{At}(\mathbf{p}, k)$ then* $\vdash A \rightarrow \Diamond A'$ *or* $\vdash A \rightarrow \neg\Diamond A'$
4. *If $A \in \mathrm{At}(\mathbf{p}, k+1)$ and $B \in \mathrm{At}(\mathbf{p} \cdot q, k)$ then* $\vdash A \rightarrow \exists q\,(B)$ *or* $\vdash A \rightarrow \neg\exists q\,(B)$.

Sketch of the proof. For part 1, note that if A and A' are distinct then they differ either in their point atoms, or they disagree about the count of some atom b. In the first case, we have $\vdash \neg(A \wedge A')$ by propositional reasoning, and in the second case, we get the result by reasoning about the quantificational encoding of the counting modalities.

Part 2 is established by noting that $\vdash \bigvee_{k=0}^{N-1} \mathsf{E}_k(b) \vee \mathsf{C}_N(b)$ for each point atom b. The result is obtained by conjoining these formulas, distributing,

[3] The approach used here results in an exponential blowup when l is expressed in binary form since the quantifier prefix then has length exponential in the length of l. However, there exists another translation that involves only a linear blowup in this case.

and then eliminating cases containing a conjunct of the form $a \wedge \mathsf{C}_0 a$ using the fact that $\vdash a \rightarrow \neg \mathsf{C}_0 a$.

For part 3, let $A = a \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} c_b$ and $A' = a' \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} c'_b$. We consider two cases, depending on whether there exists a point atom b such that $c_b \neq c'_b$. Suppose first that such an atom b exists. Note that $\vdash c_b \rightarrow \Box c_b$. It follows by S5 reasoning that $\vdash A \wedge \Diamond A' \rightarrow \Diamond(c_b \wedge c'_b)$, which gives that $\vdash A \rightarrow \neg \Diamond A'$ since $\vdash \neg(c_b \wedge c'_b)$. In the second case, we have $c_b = c'_b$ for all point atoms b. In particular, $c_{a'} = c'_{a'}$ is not $\mathsf{E}_0 a'$. It follows that $\vdash A \rightarrow \Diamond(a')$. Moreover, for each point atom b we have $\vdash c_b \rightarrow \Box c_b$, so it follows that $\vdash A \rightarrow \Diamond(a' \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} c_b))$. Since $c_b = c'_b$ for each b, this is just $\vdash A \rightarrow \Diamond(A')$.

For part 4, let A be a $(\mathbf{p}, k+1)$-atom of the form $a \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} c_b$ where each c_b is a 2^{k+1}-bounded count of b. Let B be a $(\mathbf{p} \cdot q, k+1)$-atom, which we write in the form $a' \wedge \bigwedge_{b \in \mathrm{PA}(\mathbf{p})} (c_b^+ \wedge c_b^-)$. Here c_b^+ is a 2^k bounded count of $b \wedge q$ and c_b^- is a 2^k bounded count of $b \wedge \neg q$.

Define a *q-partition* of a 2^{k+1} bounded count c_b of an atom $b \in \mathrm{PA}(\mathbf{p})$ to be a formula of the form $c_+ \wedge c_-$ where c_+ is a 2^k bounded count of $b \wedge q$ and c_- is a 2^k bounded count of $b \wedge \neg q$, subject to the following:

1. if c_b is $\mathsf{E}_l b$, then c_+ is $\mathsf{M}_{l_+, 2^k}(b \wedge q)$ and c_- is $\mathsf{M}_{l_-, 2^k}(b \wedge \neg q)$ where $l_+ + l_- = l$;
2. if c_b is $\mathsf{C}_{2^{k+1}} b$ then
   (a) c_+ is $\mathsf{C}_{2^k}(b \wedge q)$ and c_- is $\mathsf{C}_{2^k}(b \wedge \neg q)$, or
   (b) c_+ is $\mathsf{C}_{2^k}(b \wedge q)$ and c_- is $\mathsf{E}_{l_-}(b \wedge \neg q)$ where $l_- < 2^k$, or
   (c) c_+ is $\mathsf{E}_{l_+}(b \wedge q)$ where $l_+ < 2^k$ and c_- is $\mathsf{C}_{2^k}(b \wedge \neg q)$.

   That is, c_+ and c_- can be any combination of 2^k-bounded counts in which at least one has the operator C_{2^k}.

Then we may show that if $c^+ \wedge c^-$ is a q-partition of c_b, then we have $\vdash c_b \rightarrow \exists q\, (c^+ \wedge c^-)$. Moreover, we have $\vdash b \wedge c_b \rightarrow \exists q\, (b \wedge q \wedge c^+ \wedge c^-)$ and $\vdash b \wedge c_b \rightarrow \exists q\, (b \wedge \neg q \wedge c^+ \wedge c^-)$. Conversely, if $c^+ \wedge c^-$ is not a q-partition of c_b, then $\vdash c_b \rightarrow \neg \exists q\, (c^+ \wedge c^-)$.

Define B to be *q-compatible* with A if either $b = a \wedge q$ or $b = a \wedge \neg q$ and for all point atoms $b \in \mathrm{PA}(\mathbf{p})$ we have that $c_b^+ \wedge c_b^-$ is a q-partition of c_b. Then, if B is q-compatible with A, it follows from the observations of the previous paragraph that

$$\vdash A \rightarrow \exists q \left(a' \wedge c_a^+ \wedge c_a^-\right) \wedge \bigwedge\nolimits_{b \in \mathrm{PA}(\mathbf{p}) \setminus \{a\}} \exists q \left(c_b^+ \wedge c_b^-\right) \quad .$$

Using **Ch** and the fact that point atoms correspond to mutually exclusive propositions, we obtain that $\vdash A \rightarrow \exists q\,(B)$. Conversely, if B is not q-compatible with A, then we have either that the point atom a' is neither $a \wedge q$ nor $a \wedge \neg q$, or there exists a point atom b such that $c_b^+ \wedge c_b^-$ is not a q-partition of c_b. If a' is neither $a \wedge q$ nor $a \wedge \neg q$, we plainly have $\vdash A \rightarrow \neg\exists q\,(B)$. If $c_b^+ \wedge c_b^-$ is not a q-partition of c_b, then $\vdash A \rightarrow \neg\exists q\,(B)$ follows using the observation of the previous paragraph. ∎

Using Lemma 2, we may now establish the following result.

LEMMA 3 *If A is a* $(\mathbf{p}, k)$-atom *and ϕ is a formula of $\mathcal{L}_{(\forall,\Box)}$ of quantification depth at most k with free variables amongst* $\mathbf{p}$, *then either $\vdash A \rightarrow \phi$ or $\vdash A \rightarrow \neg\phi$.*

Proof. By induction on k, and, within each k, on the complexity of ϕ. The cases where ϕ is a propositional variable or formed from simpler formulas using negation or conjunction are straightforward, from completeness of the propositional fragment of the logic.

Suppose ϕ is $\Box\psi$. (Here ϕ and ψ have the same quantification depth k.) We consider two cases, depending on whether there exists a point atom $A' \in \mathrm{At}(\mathbf{p}, k)$ such that $\vdash A \rightarrow \Diamond A'$ and $\vdash A' \rightarrow \psi$. If this is the case, then it follows that $\vdash A \rightarrow \Diamond\psi$, i.e. $\vdash A \rightarrow \neg\Box\psi$, by S5 reasoning. Otherwise, for all $A' \in \mathrm{At}(\mathbf{p}, k)$, if $\vdash A \rightarrow \Diamond A'$ then not $\vdash A' \rightarrow \psi$. Let $\tilde{A}$ be the set of $(\mathbf{p}, k)$-atoms A' such that $\vdash A \rightarrow \Diamond A'$. By the induction hypothesis,it follows that $\vdash A' \rightarrow \neg\psi$ for all $A' \in \tilde{A}$. Now by Lemma 2.3, we have that $\vdash A \rightarrow \Box\neg A'$ for all $(\mathbf{p}, k)$-atoms not in $\tilde{A}$. Hence, by Lemma 2.2 and S5 reasoning, we obtain that $\vdash A \rightarrow \Box(\bigvee_{A' \in \tilde{A}} A')$. It follows that $\vdash A \rightarrow \Box\psi$.

The proof of the case where ψ is $\forall q(\psi)$ is almost identical to the proof of the case for $\Box\psi$, with the following exceptions. In this case, we take ϕ to have quantification depth $k+1$, so A is a $(\mathbf{p}, k+1)$-atom. The formula ψ in this case has quantification depth k, and in place of the $(\mathbf{p}, k+1)$-atoms A' in the preceding paragraph, we use $(\mathbf{p} \cdot q, k)$-atoms B. The rest of the argument follows as above, but we use Lemma 2.4 in place of Lemma 2.3. ∎

For the completeness proof, we now argue as follows. Let ϕ be a consistent formula of quantification depth k with free variables $\mathbf{p}$. By Lemma 2.1, we have $\vdash \bigvee_{A \in \mathrm{At}(\mathbf{p},k)} A$. Hence, by Lemma 3 there exists a $(\mathbf{p}, k)$-atom A such that $\vdash A \rightarrow \phi$. It is now straightforward to construct a finite model M with a world w such that $M, w \models A$, since this amounts merely to creating the right number of worlds for each point atom. It now follows that $M, w \models \phi$ by soundness. Clearly, the proof also establishes the finite model property.

4.2 Dealing with $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$

We now show how the proof idea of the previous section can be generalized to give a normal form and completeness proof for $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$. The basic structure of the completeness proof will be the same: we identify a kind of atom generalizing the $(\mathbf{p},k)$-atoms of the previous section, and prove a results analogous to Lemma 2.

As above, atoms count certain sorts of objects up to a given bound, which depends on the formula we are dealing with. However, where for $\mathcal{L}_{(\forall,\Box)}$ it suffices to count worlds satisfying a point atom, we now also need to count equivalence classes, and to distinguish equivalence classes having different internal structure in this count. We distinguish equivalence classes of the most highly informed agent (agent 1) according to the number of worlds of each propositional type they contain. That is, we relativize the normal form formulas of the previous section to each equivalence class of agent 1, and then count the number of distinct such relativizations that we obtain, just as we did with worlds in the previous section. This gives a normal form for the language $\mathcal{L}_{(\forall,\forall_1,\Box)}$. To deal with additional agents, we recursively apply the construction, using at each level the normal form for the previous level.

As we proceed up the levels, when dealing with a formula ϕ of quantification depth k, the bound up to which we count (which was 2^k in the previous section) increases, depending on i (an agent), $\mathbf{p}$ (the list of free variables of ϕ) and the quantification depth k.

Recall that $\mathcal{E}_i e$ expresses that the set of worlds satisfying e is an R_i-equivalence class. Consequently, just as $\mathcal{L}_{(\forall,\Box)}$ permits counting of worlds, $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ permits counting of equivalence classes. We write $\mathsf{E}^i_k x(\phi)$ as an abbreviation for the formula expressing that there exists exactly k distinct R_i-equivalence classes x such that ϕ holds. We use $x \subseteq y$ as an abbreviation for $\Box(x \to y)$. We will also write $\mathsf{E}^i_k x \subseteq y(\phi)$ for $\mathsf{E}^i_k x(x \subseteq y \wedge \phi)$. Similarly, we write $\mathsf{C}^i_k x(\phi)$ as an abbreviation for the formula expressing that there exists at least k distinct R_i-equivalence classes x such that ϕ holds, and use $\mathsf{C}^i_k x \subseteq y(\phi)$ for $\mathsf{C}^i_k x(x \subseteq y \wedge \phi)$. For uniformity, it is convenient to treat E^0_k and C^0_k as notations for E_k and C_k, respectively.

It is convenient to represent the normal form by means of the following objects, which we call $(i,\mathbf{p},k)$-*trees*, where $\mathbf{p} = p_1,\ldots,p_m$ is a vector of propositional variables, k a natural number and $0 \le i \le n+1$. We write $\mathbf{p}^+$ for $p_1,\ldots,p_m,p_{m+1}$. The definition of the set $\mathcal{T}_{i,\mathbf{p},k}$ of $(i,\mathbf{p},k)$-trees is by induction on i. Set $\mathcal{T}_{0,\mathbf{p},k} = 2^{\mathbf{p}}$, i.e., the power set of $\mathbf{p}$. For $i = 1,\ldots,n+1$, we define $\mathcal{T}_{i,\mathbf{p},k}$ to be the set of functions $u : \mathcal{T}_{i-1,\mathbf{p},k} \longrightarrow \{0,\ldots,N_{i-1,\mathbf{p},k}\}$ such that $u(t) \neq 0$ for some $t \in \mathcal{T}_{i-1,\mathbf{p},k}$. Here, the $N_{i,\mathbf{p},k}$ are the numbers defined by the following mutual recursion with the definition of $(i,\mathbf{p},k)$-

trees:

$$N_{0,\mathbf{p},k} = 2^k$$
$$N_{i,\mathbf{p},0} = 1$$
$$N_{i,\mathbf{p},k+1} = |\mathcal{T}_{i,\mathbf{p}^+,k}| \cdot N_{i,\mathbf{p}^+,k}$$

Note that

$$|\mathcal{T}_{i,\mathbf{p},k}| = (1 + N_{i-1,\mathbf{p},k})^{|\mathcal{T}_{i-1,\mathbf{p},k}|} - 1 \ .$$

It is not too difficult to verify that this recursion is well defined. A *branch* in a tree $t \in \mathcal{T}_{i,\mathbf{p},k}$ is a sequence of trees $t_i, t_{i-1}, \ldots, t_0$ where $t_j \in \mathcal{T}_{j,\mathbf{p},k}$ for each $j = 0, \ldots, i$ such that $t = t_i$ and $t_j(t_{j-1}) \neq 0$ for each $j = 1, \ldots, i$.

Each $(i, \mathbf{p}, k)$-tree corresponds to a formula as follows. It is convenient to define the expression $\mathsf{M}_l^{i,\mathbf{p},k} x \subseteq y(\phi)$ to be $\mathsf{E}_l^i x \subseteq y(\phi)$ if $l < N_{i,\mathbf{p},k}$ and to be $\mathsf{C}^i_{N_{i,\mathbf{p},k}} x \subseteq y(\phi)$ if $l \geq N_{i,\mathbf{p},k}$. With every $(i, \mathbf{p}, k)$-tree u, we associate a distinct propositional variable e_u. Given an $(i, \mathbf{p}, k)$-tree u, we define the formula ϕ_u, by induction on i. When $i = 0$, we define ϕ_u to be the point atom $\bigwedge_{j=1}^m l_j$, where $l_j = p_i$ if $p_j \in u$ and $l_j = \neg p_i$ otherwise. When $1 \leq i \leq n + 1$, we define the formula corresponding to an $(i, \mathbf{p}, k)$-tree u to be the formula

$$\phi_u(e_u) = \bigwedge\nolimits_{t \in \mathcal{T}_{i-1,\mathbf{p},k}} \mathsf{M}_{u(t)}^{i-1,\mathbf{p},k} e_t \subseteq e_u(\phi_t(e_t)) \ .$$

Clearly, $\phi_t(e_t)$ has only the variables e_t and $\mathbf{p}$ free.

The normal form uses the set of distinct propositional variables $\mathbf{c} = \{c_1, \ldots, c_n\}$. Let $A_\mathbf{c}$ be the formula

$$\bigwedge\nolimits_{j=1}^n (c_j \wedge \mathcal{E}_j c_j) \ .$$

Intuitively, $A_\mathbf{c}$ says that each c_i corresponds to the R_i-equivalence class containing the current world.

From now on, we call a formula a $(\mathbf{p}, k)$-*atom* if it is of the form

$$\exists \mathbf{c}(A_\mathbf{c} \wedge \phi_{t_0} \wedge \bigwedge\nolimits_{i=1}^n \phi_{t_i}(c_i) \wedge \phi_{t_{n+1}}(\mathit{true})) \ ,$$

where $t_i \in \mathcal{T}_{i,\mathbf{p},k}$ for each i, and $t_{n+1}, \ldots, t_0$ is a branch in t_{n+1}. Again, we write $\mathrm{At}(\mathbf{p}, k)$ for the set of $(\mathbf{p}, k)$-atoms. These atoms have the following properties. The first four of these are identical to the properties of Lemma 2. However, we have some new properties relating to the local propositional quantifiers.

LEMMA 4

1. *If $A, A' \in \mathrm{At}(\mathbf{p}, k)$ are distinct atoms, then* $\vdash \neg(A \wedge A')$.

2. $\vdash \bigvee_{A \in \mathrm{At}(\mathbf{p},k)} A$

3. *If* $A, A' \in \mathrm{At}(\mathbf{p},k)$ *then* $\vdash A \rightarrow \Diamond A'$ *or* $\vdash A \rightarrow \neg \Diamond A'$

4. *If* $A \in \mathrm{At}(\mathbf{p},k+1)$ *and* $B \in \mathrm{At}(\mathbf{p}\cdot q,k)$ *then* $\vdash A \rightarrow \exists q\,(B)$ *or* $\vdash A \rightarrow \neg\exists q\,(B)$.

5. *If* $A \in \mathrm{At}(\mathbf{p},k)$ *and* p *is one of the propositions in* $\mathbf{p}$ *then* $\vdash A \rightarrow L_i p$ *or* $\vdash A \rightarrow \neg L_i p$.

6. *If* $A \in \mathrm{At}(\mathbf{p},k+1)$ *and* $B \in \mathrm{At}(\mathbf{p}\cdot q,k)$ *then* $\vdash A \rightarrow \exists_i q\,(B)$ *or* $\vdash A \rightarrow \neg\exists_i q\,(B)$.

We defer discussion of the proof. Using this result, we may obtain a result directly analogous to Lemma 3.

LEMMA 5 *If* A *is a* $(\mathbf{p},k)$*-atom and* ϕ *is a formula of* $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ *of quantification depth at most* k*, with free variables* $\mathbf{p}$ *then either* $\vdash A \rightarrow \phi$ *or* $\vdash A \rightarrow \neg\phi$.

The proof of Lemma 5 is identical to that of Lemma 3, except that we now have a new case for ϕ of the form $\exists_i p\,(\phi')$. The proof for this case follows exactly along the lines of the proof for the case $\exists p\,(\phi')$ in the proof of Lemma 3, but uses Lemma 4.6 in place of Lemma 2.4.

As in the previous section, it then follows straightforwardly that a consistent formula is equivalent to a disjunction of $(\mathbf{p},k)$-atoms, and we may give a completeness and finite model argument exactly as before.

The bulk of the work of the completeness proof is therefore in the proof of Lemma 4. We now sketch some of the key steps of this proof, focussing on part 4.

As a first observation, we note that the formulas $\phi_u(e)$ have the following basic properties:

LEMMA 6

1. *If* $u, v \in \mathcal{T}_{i,\mathbf{p},k}$ *and* $u \neq v$ *then* $\vdash \neg(\phi_u(e) \wedge \phi_v(e))$.

2. $\vdash \mathcal{E}_i e \rightarrow \bigvee_{v \in \mathcal{T}_{i,\mathbf{p},k}} \phi_v(e)$.

One of the key steps in the proof of Lemma 2.4 is the notion of partition of a count. In the proof of Lemma 2, we dealt with counts of point atoms a, which split into two point atoms $a \wedge q$ and $a \wedge \neg q$ when taking a new proposition q into consideration. We now need to deal with a partition of a formula that counts equivalence classes satisfying a counting property, rather than a type of world. These nests of equivalence classes split into a larger and more complex collection of nests of equivalence classes when we add a new proposition.

To handle this, we introduce a notion of *compatibility* that generalizes the partition of a count of a point atom a into counts of the point atoms $a \wedge q$ and $a \wedge \neg q$. For $u \in \mathcal{T}_{i,\mathbf{p},k+1}$ we define a set $\mathcal{C}(u) \subseteq \mathcal{T}_{i,\mathbf{p}^+,k}$, of $(i, \mathbf{p}^+, k)$-trees. If $v \in \mathcal{C}(u)$ then we say that v is *compatible* with u. The definition is by induction on i, as follows. If $i = 0$ then $v \in \mathcal{C}(u)$ if $u = v \cap \{p_1, \ldots, p_m\}$. For $i > 0$, $v \in \mathcal{C}(u)$ if there exists a function $f : \mathcal{T}_{i-1,\mathbf{p},k+1} \times \mathcal{T}_{i-1,\mathbf{p}^+,k} \to [0, \ldots, N_{i-1,\mathbf{p}^+,k}]$ such that

C1. for all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ and all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$, if $f(t,t') \neq 0$ then $t' \in \mathcal{C}(t)$,

C2. for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$, we have $v(t') = \min\left(N_{i-1,\mathbf{p}^+,k}, \sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t')\right)$, and

C3. for all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$, if $f(t,t') < N_{i-1,\mathbf{p}^+,k}$ for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$ then $u(t) = \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$ otherwise $u(t) \geq \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$.

We may then prove the following results that mirror the observations concerning partitions in the proof of Lemma 2.

LEMMA 7 *Let* $u \in \mathcal{T}_{i,\mathbf{p},k+1}$ *and* $v \in \mathcal{T}_{i,\mathbf{p}^+,k}$.

1. *If* $v \in \mathcal{C}(u)$ *then* $\vdash \phi_u \to \exists p_{m+1}(\phi_v)$.
2. *If* $v \notin \mathcal{C}(u)$ *then* $\vdash \phi_u \to \neg\exists p_{m+1}(\phi_v)$.

Rather than give the full proof of this proof-theoretic result, we give the proof of a closely related semantic result, and describe the key steps required to mirror this proof within our proof system. The first part of Lemma 7 corresponds to the following semantic result.

PROPOSITION 8 *Suppose that* $u \in \mathcal{T}_{i,\mathbf{p},k+1}$ *and* $v \in \mathcal{T}_{i,\mathbf{p}^+,k}$. *If* $v \in \mathcal{C}(u)$ *then* $\models \phi_u \to \exists p_{m+1}(\phi_v)$.

Proof. The proof is by induction on i. The base case is straightforward. When $i = 0$, if $v \in \mathcal{C}(u)$ then we have either $\phi_v = \phi_u \wedge p_{m+1}$ or $\phi_v = \phi_u \wedge \neg p_{m+1}$ and the claim is immediate from $\mathbf{1}_\forall$.

We now establish the inductive step. Let $i \in \{1, \ldots, n\}$, let $u \in \mathcal{T}_{i,\mathbf{p},k+1}$, let $v \in \mathcal{C}(u)$, and let f be the witness to compatibility. Suppose $M \models \phi_u(e)$. For each $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$, let $S(t)$ be the set of R_{i-1}-equivalence classes

$U \subseteq \pi(e)$ such that $M[U/e] \models \phi_t(e)$. Then $|S(t)| = u(t)$ if $u(t) < N_{i-1,\mathbf{p},k+1}$ and $|S(t)| \geq N_{i-1,\mathbf{p},k+1}$ otherwise. Note that by Lemma 6.1, we have that if $t_1 \neq t_2$ are both $(i, \mathbf{p}, k+1)$-trees, then $S(t_1) \cap S(t_2) = \emptyset$.

For each $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$, we partition $S(t)$ into a disjoint union

$$S(t) = \bigcup_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} S(t,t')$$

in such a way that $|S(t,t')| = f(t,t')$ if $f(t,t') < N_{i-1,\mathbf{p}^+,k}$ and $|S(t,t')| \geq f(t,t')$ if $f(t,t') = N_{i-1,\mathbf{p}^+,k}$. The reason we can partition in this way is as follows. By **C3**, there are two possibilities.

1. The first possibility is that $f(t,t') < N_{i-1,\mathbf{p}^+,k}$ for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$. In this case, we have

$$u(t) = \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t') < |\mathcal{T}_{i-1,\mathbf{p}^+,k}| \cdot N_{i-1,\mathbf{p}^+,k} = N_{i-1,\mathbf{p},k+1} \ .$$

   It follows that $|S(t)| = u(t) = \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$, so we partition $S(t)$ in such a way that $|S(t,t')| = f(t,t')$ for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$.

2. The second possibility is that $f(t,t'_0) = N_{i-1,\mathbf{p}^+,k}$ for some t'_0. In this case we are still guaranteed that $u(t) \geq \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$, and since $M \models \phi_u(e)$ we have that $|S(t)| \geq u(t)$. In this case we first partition $\sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$ of the elements of $S(t)$ as before, and then place any remaining elements of $S(t)$ in $S(t,t'_0)$. Clearly we then have $|S(t,t')| = f(t,t')$ for $t' \neq t'_0$, and both $|S(t,t')| \geq f(t,t')$ and $f(t,t') = N_{i-1,\mathbf{p}^+,k}$ in the case $t' = t'_0$, so the constraint on the partitioning is satisfied.

For each R_{i-1}-equivalence class U in $S(t,t')$, we have $M[U/e] \models \phi_t(e)$. By the induction hypothesis, we have $\models \phi_t \rightarrow \exists p_{m+1}\, (\phi_{t'})$ for all $t' \in \mathcal{C}(t)$. Since the sets $S(t,t')$ are disjoint, for each such set the equivalence classes $U \in S(t,t')$ are disjoint, the formulas $\phi_{t'}$ depend only on the values of p_m+1 in U, and the propositions witnessing these facts may be aggregated into a single proposition P such that $M[P/p_{m+1}, U/e] \models \phi_{t'}(e)$ for all $U \in S(t,t')$, all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ and all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$.

Write $S'(t')$ for the set of R_{i-1}-equivalence classes U in $\pi(e)$ such that $M[P/p_{m+1}, U/e] \models \phi_{t'}(e)$. Then

$$S'(t') = \bigcup_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} S(t,t')$$

is a partition of $S'(t')$. To see this, note that $S(t,t') \subseteq S'(t')$ for each t by construction of P. By Lemma 6.2, each R_{i-1}-equivalence class U in $\pi(e)$ is in $S(t)$ for some $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$, hence in $S(t,t'')$ for some $t'' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$. By Lemma 6.1 and construction of P, we cannot have $t'' \neq t'$ if $M[P/p_{m+1}, U/e] \models \phi_{t'}(e)$. This proves the containment in the other direction. The union is therefore a partition because all the sets $S(t,t')$ are disjoint.

We now claim that $M[P/p_{m+1}] \models \phi_v(e)$. We show this by establishing that $M[P/p_{m+1}] \models \mathsf{M}^{i-1,\mathbf{p}^+,k}_{v(t')} e' \subseteq e(\phi_{t'}(e'))$ for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$. There are two cases.

1. First, suppose $v(t') < N_{i-1,\mathbf{p}^+,k}$. Then by **C2**, we have that $v(t') = \sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') < N_{i-1,\mathbf{p}^+,k}$, so $f(t,t') < N_{i-1,\mathbf{p}^+,k}$ for each $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$. Thus, for each $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$, we have

$$|S'(t')| = \sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} |S(t,t')| = \sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') = v(t') \ ,$$

   hence $M[P/p_{m+1}] \models \mathsf{E}^{i-1}_{v(t')} e' \subseteq e(\phi_{t'}(e'))$, as is required to establish $M[P/p_{m+1}] \models \mathsf{M}^{i-1,\mathbf{p}^+,k}_{v(t')} e' \subseteq e(\phi_{t'}(e'))$ in case that $v(t') < N_{i-1,\mathbf{p}^+,k}$.

2. In the other case, where $v(t') = N_{i-1,\mathbf{p}^+,k}$, we have by **C2** that $\sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') \geq N_{i-1,\mathbf{p}^+,k}$. Since we always have $|S(t,t')| \geq f(t,t')$, we have

$$|S'(t')| = \sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} S(t,t') \geq \sum_{t\in\mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') \geq N_{i-1,\mathbf{p}^+,k} \ .$$

   Thus, $M[P/p_{m+1}] \models \mathsf{C}^{i-1}_{N_{i-1,\mathbf{p}^+,k}} e' \subseteq e(\phi_{t'}(e'))$, again as required.

■

The main difficulty in converting this proof into a proof of Lemma 7.1, is its use of the axiom of choice. To capture this in the proof system, we use axiom **Choice**, with the formula θ as $\mathcal{E}_i p \wedge \Box(p \to e)$, and ψ as a disjunction that describes the mapping from the R_{i-1}-equivalence classes e' in e to the formulas $\phi_{t'}(e')$ that the construction chooses to make them satisfy.

For the second part of Lemma 7, we note the following semantic result.

PROPOSITION 9 *Suppose* $u \in \mathcal{T}_{i,m,k+1}$ *and* $v \in \mathcal{T}_{i,m+1,k}$ *is not compatible with* u. *Then* $\models \phi_u \to \neg\exists p_{m+1}\, (\phi_v)$.

Proof. Suppose $v \notin \mathcal{C}(u)$. We proceed by induction on i. For $i = 0$, the claim is straightforward, since one of ϕ_v and ϕ_v contains, for some $j = 1 \ldots m$, a conjunct p_j whereas the other contains a conjunct $\neg p_j$. For $i > 0$, suppose that v is not compatible with u, and that $M \models \phi_u(e)$. Let M' be a p_{m+1}-variant of M. We suppose that $M' \models \phi_v(e)$ and derive the contradiction that $v \in \mathcal{C}(u)$.

Define $S(t)$ for $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ to be the set of R_{i-1}-equivalence classes U in $\pi(e)$ such that $M'[U/e] \models \phi_t(e)$. Similarly, define $S'(t')$ for $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$ to be the set of R_{i-1}-equivalence classes U in $\pi(e)$ such that $M'[U/e] \models \phi_{t'}(e)$. Additionally, define $S(t,t') = S(t) \cap S'(t')$. By Lemma 6, each of the collections $\{ S(t) \mid t \in \mathcal{T}_{i-1,\mathbf{p},k+1} \}$, $\left\{ S'(t') \;\middle|\; t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k} \right\}$ and $\left\{ S(t,t') \;\middle|\; t \in \mathcal{T}_{i-1,\mathbf{p},k+1}, t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k} \right\}$ partition the set of R_{i-1}-equivalence classes U in $\pi(e)$.

Define $f(t,t') = \min(N_{i-1,\mathbf{p}^+,k}, |S(t,t')|)$. We show that f satisfies all the conditions of the definition of compatibility in order to witness that $v \in \mathcal{C}(u)$.

C1: If $f(t,t') \neq 0$ then there exists an R_{i-1}-equivalence class U in e such that $M'[U/e] \models \phi_t(e) \wedge \phi_{t'}(e)$, hence $M[U/e] \models \phi_t(e) \wedge \exists p_{m+1}(\phi_{t'}(e))$. Thus, we do not have $\models \phi_t(e) \to \neg\exists p_{m+1}(\phi_{t'}(e))$. By the induction hypothesis, we have $t' \in \mathcal{C}(t)$.

C2: We consider two cases. Suppose first that $v(t') < N_{i-1,\mathbf{p}^+,k}$. Since $M' \models \phi_v(e)$, we have $v(t') = |S'(t')| < N_{i-1,\mathbf{p}^+,k}$. Consequently, for all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ we also have $|S(t,t')| < N_{i-1,\mathbf{p}^+,k}$, so $f(t,t') = |S(t,t')|$. Thus,

$$\sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') = \sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} |S(t,t')| = |S(t')| = v(t').$$

It follows that $v(t') = \min(\sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t'), N_{i-1,\mathbf{p}^+,k})$.

In the other case, suppose that $v(t') = N_{i-1,\mathbf{p}^+,k}$. We break this case down into two possibilities. Suppose first that there exists $t_0 \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ such that $|S(t_0,t')| \geq N_{i-1,\mathbf{p}^+,k}$. Then $f(t_0,t') = N_{i-1,\mathbf{p}^+,k}$, so

$$\min\left(\sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t'), N_{i-1,\mathbf{p}^+,k}\right) = N_{i-1,\mathbf{p}^+,k} = v(t') \ .$$

Alternately, if $|S(t,t')| < N_{i-1,\mathbf{p}^+,k}$ for all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ then for all $t \in \mathcal{T}_{i-1,\mathbf{p},k+1}$ we have $f(t,t') = |S(t,t')|$. Thus, $\sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') = \sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} |S(t,t')| = |S(t')| \geq N_{i-1,\mathbf{p}^+,k}$. Hence

$$\min\left(\sum_{t \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t'), N_{i-1,\mathbf{p}^+,k}\right) = N_{i-1,\mathbf{p}^+,k} = v(t') \ .$$

C3: Note that we always have $f(t,t') \leq |S(t,t')|$, hence

$$\sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t') \leq \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} |S(t,t')| = |S(t')| \ .$$

Since $f(t,t') \leq N_{i-1,\mathbf{p}^+,k}$, we have

$$\sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t') \leq |\mathcal{T}_{i-1,\mathbf{p}^+,k}| \cdot N_{i-1,\mathbf{p}^+,k} = N_{i-1,\mathbf{p},k+1}$$

Thus $\sum_{t' \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') \leq \min(|S(t)|, N_{i-1,\mathbf{p},k+1})$. Since $M \models \phi_u(e)$, we have $\min(|S(t)|, N_{i-1,\mathbf{p},k+1}) = u(t)$. It follows that we always have $\sum_{t' \in \mathcal{T}_{i-1,\mathbf{p},k+1}} f(t,t') \leq u(t)$. In the case that $f(t,t') < N_{i-1,\mathbf{p}^+,k}$ for all $t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}$, we have also $f(t,t') = |S(t,t')|$. Thus

$$\begin{aligned} |S(t)| &= \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} |S(t,t')| \\ &= \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t') \\ &< |\mathcal{T}_{i-1,\mathbf{p}^+,k}| \cdot N_{i-1,\mathbf{p}^+,k} \\ &= N_{i-1,\mathbf{p},k+1} \ . \end{aligned}$$

Since $M \models \phi_u(e)$, it follows that $u(t) = |S(t)| = \sum_{t' \in \mathcal{T}_{i-1,\mathbf{p}^+,k}} f(t,t')$. ∎

The main step in converting this semantic proof to a proof-theoretic argument is to replace the use of satisfiability by a consistency argument.

Just as in the proof of Lemma 2.4, we needed to treat the atom a as a special case, establishing that $\vdash a \wedge c_a \to \exists q(a' \to c_a^+ \wedge c_a^-)$, we actually need a slight strengthening of Lemma 7 that deals with branches rather than trees. For this we need a generalized notion of compatibility. Define a branch $v_i, \ldots, v_0$ in a tree $v_i \in \mathcal{T}_{i,\mathbf{p}^+,k}$ to be *compatible* with a branch $u_i, \ldots, u_0$ in a tree $u_i \in \mathcal{T}_{i,\mathbf{p},k+1}$ when v_0 is compatible with u_0, and there exist functions $f_1, \ldots, f_i$ such that for each $j = 1, \ldots, i$, the function f_j witnesses that v_j is compatible with u_j, and $f_j(u_{j-1}, v_{j-1}) \neq 0$. We write $\text{Chain}(e_0, \ldots, e_i)$ for $\bigwedge_{j=0}^{i-1} e_j \subseteq e_{j+1} \wedge \bigwedge_{j=0}^{i} \mathcal{E}_j e_j$. That is, $\text{Chain}(e_0, \ldots, e_i)$ says that $e_0, \ldots, e_i$ is a nested set of equivalence classes.

LEMMA 10 *Let $u_i \in \mathcal{T}_{i,\mathbf{p},k+1}$ and let $u_i, \ldots, u_0$ be a branch in u_i. Similarly, let $v_i \in \mathcal{T}_{i,\mathbf{p}^+,k}$ and let $v_i, \ldots, v_0$ be a branch in v_i. Then if $v_i, \ldots, v_0$ is compatible with $u_i, \ldots, u_0$, we have*

$$\vdash \text{Chain}(e_0, \ldots, e_i) \wedge \bigwedge_{j=0}^{i} \phi_{u_j}(e_j) \to \exists p_{m+1} \left(\bigwedge_{j=0}^{i} \phi_{v_j}(e_j) \right) \ ,$$

else

$$\vdash \text{Chain}(e_0, \ldots, e_i) \wedge \bigwedge_{j=0}^{i} \phi_{u_j}(e_j) \rightarrow \neg\exists p_{m+1} \left(\bigwedge_{j=0}^{i} \phi_{v_j}(e_j) \right) .$$

The proof of Lemma 10 is very similar to the proof of Lemma 7: we simply need to add some special treatment of the proposition p_{m+1} along the distinguished branch.

Lemma 4.4 now follows easily from Lemma 10. Parts 1 − 3 of Lemma 4 can be established by arguments similar to those in the proof of Lemma 2. For part 5, we use $\mathbf{EC}_2$ (Section 3.1) and an induction on i to show that for $(i, \mathbf{p}, k)$-trees u and propositions p in $\mathbf{p}$, we have $\vdash \mathcal{E}_i e \wedge \phi_u(e) \rightarrow \Box(e \rightarrow p)$ or $\vdash \mathcal{E}_i e \wedge \phi_u(e) \rightarrow \neg\Box(e \rightarrow p)$, and also $\vdash \mathcal{E}_i e \wedge \phi_u(e) \rightarrow \Box(e \rightarrow \neg p)$ or $\vdash \mathcal{E}_i e \wedge \phi_u(e) \rightarrow \neg\Box(e \rightarrow \neg p)$. From this we obtain, using $\mathbf{EC}_3$ and $\mathbf{EC}_4$, that when u is an $(n+1, \mathbf{p}, k)$-tree and p is one of the propositions in $\mathbf{p}$, either $\vdash \phi_u(\mathit{true}) \rightarrow L_i p$ or $\vdash \phi_u(\mathit{true}) \rightarrow \neg L_i p$. Part 5 of Lemma 4 follows from this. Part 6 follows from part 4 and part 5 using $\mathbf{Def}\forall_i$.

5 Conclusion

The results presented in this paper leave open a number of questions concerning $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$. One of these is the complexity of the language with respect to hierarchical structures: we will report on this in the full version. (Note that decidability follows from the finite model property we have established.) Another question is the effect of restrictions on the range of quantification. We have interpreted the quantifiers to range over all propositions. For $\mathcal{L}_{(\forall,\Box)}$, Fine [8] proved completeness with respect to semantics for quantification that place various restrictions of the range of quantification, such as the assumption that this space forms a boolean algebra. We do not know yet what the effect of such assumptions would be on our logic.

Tenney showed a bounded model property for the monadic second-order theory of an equivalence relation [15]. His language and $\mathcal{L}_{(\forall,\forall_1,\Box)}$ are of equal expressive power and effectively translatable. Consequently our axiomatization $\texttt{LLPH}_1$ translates to an axiomatization of Tenney's language. Moreover, Tenney's bounds on model-sizes are similar to the ones we calculated for $\mathcal{L}_{(\forall,\forall_1,\Box)}$.

The class of models for which we are able to axiomatize the language $\mathcal{L}_{(\forall,\forall_1,\ldots,\forall_n,\Box)}$ can be generalized slightly from the hierarchical models to *locally* hierarchical models. These are models in which for all pairs U, V of propositions, with U an R_i-equivalence class and V an R_j-equivalence class, we have one of $U \cap V = \emptyset$, $U \subseteq V$ or $V \subseteq U$. We leave further discussion of this to the full paper.

Acknowledgments: Thanks to Phokion Kolaitis for drawing our attention to Tenney's paper, and several of the AIML participants for suggesting the extension to locally hierarchical models.

BIBLIOGRAPHY

[1] H. Behmann. Beiträge zur Algebra der Logik, insbesondere zum Entscheidungsproblem. *Mathematische Annalen*, 86:163–229, 1922.

[2] R. Bull. On modal logic with propositional quantifiers. *The Journal of Symbolic Logic*, 34:257–263, 1969.

[3] C. Cerratto. Graded modalities V. *Studia Logica*, 53:61–73, 1992.

[4] D. E. Denning. A lattice model of secure information flow. *Communications of the ACM*, 19(5):236–243, May 1976. Papers from the Fifth ACM Symposium on Operating Systems Principles (Univ. Texas, Austin, Tex., 1975).

[5] K. Engelhardt, R. van der Meyden, and Y. Moses. Knowledge and the logic of local propositions. In I. Gilboa, editor, *Theoretical Aspects of Rationality and Knowledge, Proceedings of the Seventh Conference (TARK 1998)*, pages 29–41. Morgan Kaufmann, July 1998.

[6] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning About Knowledge.* MIT-Press, 1995.

[7] M. Fattorosi Barnaba and F. de Caro. Graded modalities I. *Studia Logica*, 44:197–221, 1985.

[8] K. Fine. Propositional quantifiers in modal logic. *Theoria*, 36:336–346, 1970.

[9] K. Fine. In so many possible worlds. *Notre Dame Journal of Formal Logic*, 13:516–520, 1972.

[10] J. Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM*, 37(3):549–587, July 1990.

[11] G. E. Hughes and M. J. Cresswell. *A New Introduction to Modal Logic.* Routledge, London, New York, 1996.

[12] D. Kaplan. S5 with multiple possibility (Abstract). *The Journal of Symbolic Logic*, 35:355–356, 1970.

[13] D. Kaplan. S5 with quantifiable propositional variables (Abstract). *The Journal of Symbolic Logic*, 35:355, 1970.

[14] S. A. Kripke. A completeness theorem in modal logic. *The Journal of Symbolic Logic*, 24:1–14, 1959.

[15] R. L. Tenney. Second-order Ehrenfeucht games and the decidability of the second-order theory of an equivalence relation. *Journal of the Australian Mathematical Society, Series A*, 20:323–331, 1975.