ZERO-ONE LAWS FOR MODAL LOGIC*

Joseph Y. Halpern†
IBM Research Division
Almaden Research Center, K53/802
650 Harry Rd. San Jose, CA 95120

Bruce Kapron‡
Department of Computer Science
University of Victoria
Victoria, BC
CANADA V8W 3P6

June 15, 1994

Abstract

We show that a 0-1 law holds for propositional modal logic, both for structure validity and frame validity. In the case of structure validity, the result follows easily from the well-known 0-1 law for first-order logic. However, our proof gives considerably more information. It leads to an elegant axiomatization for almost-sure structure validity and to sharper complexity bounds. Since frame validity can be reduced to a Π_1^1 formula, the 0-1 law for frame validity helps delineate when 0-1 laws exist for second-order logics.

*A preliminary version of this paper appears in *Proceedings of the Seventh Annual IEEE Symposium on Logic in Computer Science*, 1992. This version is almost identical to one that appears in a special issue of *Annals of Pure and Applied Logic* (vol. 69, 1994, pp. 157–193) devoted to the papers of this conference.

†Part of the work of the first author was performed while he was on sabbatical at the University of Toronto.

‡The work of the second author was completed while at Carnegie Mellon University and the University of Toronto

1 Introduction

Glebskii *et al.* [GKLT69] and, independently, Fagin [Fag76] established a fascinating connection between asymptotic probability and logical definability. They showed that every property P expressible in first-order logic without function symbols is either almost-surely true or almost-surely false in finite structures: more precisely, if $\mu_n(P)$ is the fraction of structures with domain $\{1, \ldots, n\}$ in which P is true, then $\mu(P) = \lim_{n\to\infty} \mu_n(P)$ is either 0 or 1. This remarkable property is known as a *0-1 law*. Grandjean [Gra83] showed that the problem of deciding whether a formula is almost-surely true is PSPACE-complete for bounded underlying vocabularies, that is, vocabularies with an *a priori* bound on the arities of the predicates in the vocabulary. This forms a sharp contrast to Trakhtenbrot's classical theorem that says that the set of formulas which are valid in all finite structures is co-r.e., assuming that the vocabulary contains at least one binary predicate.

It is well known that first-order logic has rather limited expressive power (cf. [AU79, Fag75]). Thus, researchers have investigated asymptotic probabilities in logical languages that go beyond first-order. (See [Com88] for an overview and references.) Of most interest to us here are results for existential second-order logic (Σ^1_1). The interest in Σ^1_1 stems in part from a result of Fagin [Fag74] showing that a property is Σ^1_1 definable if and only if it is NP-computable. Full Σ^1_1 does not have a 0-1 law [Fag76]; in fact, neither does monadic Σ^1_1, where the existential quantification is over monadic predicates [Kau87]. A 0-1 law does hold for certain fragments of existential second-order logic, whose structure is characterized by the pattern of first-order quantifiers. If Ψ is a class of first-order formulas, let $\Sigma^1_1(\Psi)$ consist of the set of Σ^1_1 sentences where the first-order part is in Ψ. Kolaitis and Vardi considered first-order formulas Ψ defined by their quantifier prefix. There are exactly two *prefix classes* of first-order formulas with equality for which the validity problem is decidable [DG79]: the *Bernays-Schönfinkel class*, consisting of formulas with quantifier prefixes of the form $\exists^*\forall^*$ (i.e., a possibly empty string of existential quantifiers followed by a possibly empty string of universal quantifiers) and the *Ackerman class*, consisting of formulas with quantifier prefix $\exists^*\forall\exists^*$. The results of [KV87, KV90a, PS89] show that a 0-1 law holds for $\Sigma^1_1(\Psi)$, where Ψ is the set of first-order formulas defined by some prefix class, iff Ψ is either the Bernays-Schönfinkel class or the Ackermann class. In addition, Kolaitis and Vardi show that if Ψ is either the Bernays-Schönfinkel class or the Ackermann class, the problem of deciding whether a formula in $\Sigma^1_1(\Psi)$ is almost-surely true is NEXPTIME-complete if we restrict to bounded vocabularies [KV87, KV90a].

We focus here on 0-1 laws for (propositional) modal logic. Modal logic is a natural logic to investigate, given the attention it has received in the philosophical literature and the fact that various modal logics have been shown to be of great relevance to computer science, including temporal logic [MP81] and epistemic logic (i.e., reasoning about knowledge) [Hal87]. In order to explain our results, we briefly review the syntax and semantics of modal logic. The syntax is quite simple: we start with primitive propositions and close off under negation, conjunction, and application of the modal operator $\Box$. The standard semantics for modal logic is *possible-worlds* semantics. A *frame* F is a pair $(S, \mathcal{R})$, consisting of a set of possible worlds (or states) and a binary relation $\mathcal{R}$ (called the *possibility relation*) on S. A *(Kripke) structure* M is a tuple $(S, \mathcal{R}, \pi)$ consisting of a frame $(S, \mathcal{R})$ and a truth assignment π, which assigns a truth value to each primitive proposition in each state in S. We say that the structure $(S, \mathcal{R}, \pi)$ is *based on* the frame $(S, \mathcal{R})$. $(M, s) \models \varphi$ (φ is true in state s of structure M) is defined in a straightforward way by induction on the structure of φ. (We use the relation $\mathcal{R}$ to define the semantics of $\Box$ formulas). Modal logicians have historically been interested in properties of both frames and structures [Ben85, HC84]. A formula φ is said to be *valid in structure* $M = (S, \mathcal{R}, \pi)$ if $(M, s) \models \varphi$ for every state $s \in S$. We say φ is *valid in frame* F if φ is valid in every structure M based on F. Finally, we say that φ is *structure* (resp., *frame*) *valid* if φ is valid in every structure (resp., frame). It is immediate from the definitions that a formula is structure valid if and only if it is frame valid. It is also well-known that deciding structure/frame validity is PSPACE-complete for K and S4, and co-NP-complete for S5 [Lad77].

When it comes to 0-1 laws, there are two questions we can investigate: almost-sure structure validity and almost-sure frame validity. That is, we can consider all structures with state space $\{1, \ldots, n\}$ and consider in what fraction of them a formula φ is valid, or we can consider all frames with state space $\{1, \ldots, n\}$ and ask in what fraction of them φ is valid. In both cases a 0-1 law holds: that is, a formula is valid in almost all structures (resp., frames) with state space $\{1, \ldots, n\}$ or almost none of them. However, although structure validity and frame validity coincide, almost-sure structure validity and almost-sure frame validity do not.

There is a well-known translation from a modal logic formula φ to a first-order logic formula φ^{fo} with one free variable x. (See, for example, [Ben85] for an exposition.) This translation has the property that the fraction of structures with state space $\{1, \ldots, n\}$ for which φ is valid is precisely the same as the fraction of relational structures with domain $\{1, \ldots, n\}$ for which $\forall x \varphi^{fo}$ is true. For future reference, we note that φ^{fo} has one unary predicate P corresponding to each primitive proposition p in φ and one binary predicate R corresponding to the possibility relation $\mathcal{R}$. The 0-1 law for structure validity thus follows immediately from the 0-1 law for first-order logic in light of this translation. Our proof of the 0-1 law for structure validity does not proceed via this translation; instead, it uses the relatively straightforward observation that if φ is a consistent propositional formula, then $\Diamond\varphi$ is almost-surely structure valid (where $\Diamond$ is the dual of $\Box$). Using this observation, we can show that deciding if a formula is almost-surely structure valid is in Δ_2^p ($\Delta_2^P =_{\text{def}} P^{NP}$, i.e., P with an NP oracle, and is in the second level of the polynomial time hierarchy [Sto77]). This suggests that almost-sure modal validity is easier than both modal validity and the problem of deciding if an arbitrary first-order formula is almost-surely true. Finally, we show that we can axiomatize the set of formulas that are almost-surely structure valid in a straightforward way.

The proof of the 0-1 law in the case of frame validity is far more difficult. An argument analagous to that used in the case of structure validity shows that for any modal formula φ which uses the propositional letters $p_1, \ldots, p_k$, the fraction of frames with state space $\{1, \ldots, n\}$ for which φ is valid is precisely the same as the fraction of relational structures with state space $\{1, \ldots, n\}$ for which the Π_1^1 formula $\forall P_1 \ldots P_k \forall x \varphi^{fo}$ is true. Recasting this in terms of satisfiability, the fraction of frames with state space $\{1, \ldots, n\}$ for which φ is satisfiable is precisely the same as the fraction of relational structures with domain $\{1, \ldots, n\}$ in which the Σ_1^1 formula $\exists P_1 \ldots P_k \exists x \varphi^{fo}$ is true. Let MDL be the set of first-order formulas that arise as the translation of modal formulas. We take $\exists x MDL$ to consist of all formulas of the form $\exists x \varphi$, with $\varphi \in MDL$; $\forall x MDL$ is defined analogously. Our results can thus be interpreted as showing that the class $\Sigma_1^1(\exists x MDL)$ has a 0-1 law. It is easy to show that $\exists x MDL$ is incomparable in expressive power to both the Ackermann class and the Bernays-Schönfinkel class. We conjecture that $\Sigma_1^1(\exists x MDL)$ is incomparable in expressive power to both Σ_1^1(Ackermann) and Σ_1^1(Bernays-

Schönfinkel), although we have not proved this. We can show that $\Sigma_1^1(\exists x MDL)$ can capture NP-complete properties. The techniques that we use to prove that a 0-1 law holds for frame validity involve rather delicate combinatorial arguments, and are quite different from those used by Kolaitis and Vardi. Note that $\Sigma_1^1(\exists x MDL)$ is actually a fragment of monadic Σ_1^1. Thus, our results help delineate when 0-1 laws exist for second-order logics.

We also show that the problem of deciding whether a formula is almost-surely frame valid is hard for deterministic exponential time, and thus is harder than the frame validity problem (assuming PSPACE $\neq$ EXPTIME). Notice that the vocabulary for *MDL* is bounded, since it involves only unary and binary predicates. To the best of our knowledge, this is the first time that deciding if a formula is almost-surely valid with respect to a class of structures has been shown to be *harder* than showing it is valid with respect to that class.

The rest of the paper is organized is follows. In the next section, we give the necessary technical preliminaries on modal logic and measures. In Section 3, we examine the expressive power of $\Sigma_1^1(\exists x MDL)$, and show that it can capture NP-complete properties. In Section 4, we consider almost-sure structure validity, and in Section 5, we consider almost-sure frame validity.

2 Preliminaries

As we mentioned in the introduction, the formulas of propositional modal logic are those obtained by starting with primitive propositions in some set Φ and closing off under negation, conjunction, and application of the modal operator $\Box$. We call the resulting language $\mathcal{L}(\Phi)$. As usual, we write $\varphi \vee \psi$ for $\neg(\neg\varphi \wedge \neg\psi)$, $\varphi \Rightarrow \psi$ for $\neg\varphi \vee \psi$, and $\Diamond\varphi$ for $\neg\Box\neg\varphi$. We give semantics to these formulas via Kripke structures. A *Kripke structure M over Φ* is a tuple $(S, \mathcal{R}, \pi)$, as defined in the introduction. We use π to give the semantics for primitive propositions in Φ; the semantics of the Boolean connectives is as in propositional logic; finally, we define $\Box\varphi$ to be true at a state s if φ is true in all worlds reachable from s via the $\mathcal{R}$ relation. Thus, we have

- $(M, s) \models p$ for a $p \in \Phi$ iff $\pi(s)(p) = \mathbf{true}$.
- $(M, s) \models \neg\varphi$ iff $(M, s) \not\models \varphi$
- $(M, s) \models \varphi \wedge \psi$ iff $(M, s) \models \varphi$ and $(M, s) \models \psi$.
- $(M, s) \models \Box\varphi$ iff $(M, t) \models \varphi$ for all t such that $(s, t) \in \mathcal{R}$.

As usual, we say a formula φ is *valid* (resp., *satisfiable*) in model $M = (S, \mathcal{R}, \pi)$ if $M, s \models \varphi$ for all (resp., some) $s \in S$. We write $M \models \varphi$ if φ is valid in M We say that φ is *structure valid* if it is valid in all structures, and *structure satisfiable* if it is satisfiable in some structure. A formula φ is valid in frame F if it is valid in all models based on F; φ is satisfiable in F if it is satisfiable in some model based on F. Finally, we say φ is *frame valid* if it is valid in all frames, and *frame satisfiable* if it is satisfiable in some frame.

The logic just defined, known as K, can be axiomatized as follows [HC68]:

A1. All instances of tautologies of propositional calculus

A2. $(\Box\varphi \wedge \Box(\varphi \Rightarrow \psi)) \Rightarrow \Box\psi$

R1. From φ and $\varphi \Rightarrow \psi$ infer ψ (Modus ponens)

R2. From φ infer $\Box\varphi$ (Generalization)

Modal logicians have considered numerous modal logics other than K. The ones of most interest to us here are those that have been called T, S4, and S5. All these logics satisfy the axioms of K. T is characterized by the axioms of K together with

A3. $\Box\varphi \Rightarrow \varphi$

S4 is characterized by the axioms of T together with:

A4. $\Box\varphi \Rightarrow \Box\Box\varphi$

Finally, S5 is characterized by the axioms of S4 together with:

A5. $\neg\Box\varphi \Rightarrow \Box\neg\Box\varphi$

Let $\mathcal{M}$ consist of all Kripke structures, and let $\mathcal{M}^r$ (resp., $\mathcal{M}^{rt}$; $\mathcal{M}^{rst}$) consist of all Kripke structures where the $\mathcal{R}$ relation is reflexive (resp., reflexive and transitive; reflexive, symmetric, and transitive, i.e., an equivalence relation). The following result is well known (see, for example, [HC68] for a proof).

Theorem 2.1: *K (resp., T; S4; S5) is sound and complete with respect to the structures in $\mathcal{M}$ (resp., $\mathcal{M}^r$; $\mathcal{M}^{rt}$; $\mathcal{M}^{rst}$).*

We can similarly define $\mathcal{F}$ to consist of all frames, and $\mathcal{F}^r$ (resp., $\mathcal{F}^{rt}$; $\mathcal{F}^{rst}$) to consist of all frames where the $\mathcal{R}$ relation is reflexive (resp., reflexive and transitive; and equivalence relation). It is trivial to check that structure validity and frame validity coincide, thus K (resp., T; S4; S5) is also sound and complete with respect to the frames in $\mathcal{F}$ (resp., $\mathcal{F}^r$; $\mathcal{F}^{rt}$; $\mathcal{F}^{rst}$).

Let Φ be a set of primitive propositions and let $\mathcal{M}_{n,\Phi}$ (resp., $\mathcal{F}_{n,\Phi}$) be the set of Kripke structures (resp., frames) over Φ with state space $\{1,\ldots,n\}$. Notice that $\mathcal{M}_{n,\Phi}$ and $\mathcal{F}_{n,\Phi}$ are finite if Φ is finite. If Φ is finite, then we take $\nu_{n,\Phi}$ to be the uniform probability distribution on $\mathcal{M}_{n,\Phi}$ and take $\mu_{n,\Phi}$ to be the uniform probability distribution on $\mathcal{F}_{n,\Phi}$. Although the main interest in 0-1 laws has been for finite structures, for technical reasons, we also allow Φ to be infinite. There are a number of ways to proceed in this case, all of which turn out to be equivalent for our purposes (see [GHK92] for further discussion of this issue). If Φ is infinite, we consider the σ-algebra over $\mathcal{M}_{n,\Phi}$ generated by $\mathcal{M}_{n,\Phi'}$ for all finite subsets Φ' of Φ. That is, given a structure $M \in \mathcal{M}_{n,\Phi'}$, we consider the subset A_M of $\mathcal{M}_{n,\Phi'}$ consisting of structures that agree with M on the propositions in Φ', and consider the σ-algebra generated by all sets of the form A_M. We define $\nu_{n,\Phi}$ on this σ-algebra so that $\nu_{n,\Phi}(A_M) = \nu_{n,\Phi'}(A_M)$. It is easy to check that this is a well-defined measure. We similarly define a measure $\mu_{n,\Phi}$ on $\mathcal{F}_{n,\Phi}$. For a formula $\varphi \in \mathcal{L}(\Phi)$, we write $\nu_{n,\Phi}(\varphi)$ as an abbreviation for $\nu_{n,\Phi}(\{M \in \mathcal{M}_{n,\Phi} : M \models \varphi\})$, and similarly for $\mu_n(\varphi)$. It is easy to see that if $\varphi \in \mathcal{L}(\Phi)$ and $\Phi' \supset \Phi$, then $\mu_{n,\Phi}(\varphi) = \mu_{n,\Phi'}(\varphi)$, and similarly $\nu_{n,\Phi}(\varphi) = \nu_{n,\Phi'}(\varphi)$. Thus, without loss of generality, we need to consider only finite sets Φ when computing asymptotic probabilities. We omit the subscript Φ in the rest of the paper if its role is unimportant.

Let $\nu(\varphi) = \lim_{n\to\infty} \nu_n(\varphi)$ and $\mu(\varphi) = \lim_{n\to\infty} \mu_n(\varphi)$. We say that a 0-1 law holds for structure validity if for all modal formulas φ, we have $\nu(\varphi) = 0$ or $\nu(\varphi) = 1$; we say that φ is *almost-surely structure valid* if $\nu(\varphi) = 1$. Similar definitions can be made for frame validity.

Although we are mainly interested in computing $\nu(\varphi)$ and $\mu(\varphi)$, in the process we need to apply μ and ν to events other than those defined by formulas. We are also interested in computing the asymptotic limits when we restrict to structures in $\mathcal{M}^r$, $\mathcal{M}^{rt}$, and $\mathcal{M}^{rst}$, and similarly for frames. We can make the obvious analogous definitions, for example, taking $\mathcal{F}_n^r$ to be the set of frames with state space $\{1, \ldots, n\}$ in which the $\mathcal{R}$ relation is reflexive, defining $\mu_n^r(\varphi)$ to be the fraction of frames in $\mathcal{F}_n^r$ in which φ is valid and defining $\mu^r(\varphi) = \lim_{n\to\infty} \mu_n^r(\varphi)$.

3 The expressive power of modal formulas

We begin this section by reviewing the translation from modal logic to first-order logic mentioned in the introduction. We then show that $\Sigma_1^1(\exists x MDL)$ can capture some NP-complete properties, in particular satisfiability of propositional formulas.

Suppose the primitive propositions in the modal language are $p_1, p_2, \ldots$. Consider the first-order vocabulary Φ consisting of the unary predicates $P_1, P_2, \ldots$ and the binary predicate R. We now show how to translate a modal formula φ to a first-order formula $\varphi^{fo}(x)$ with one free variable x over the vocabulary Φ. We proceed by induction on structure:

- $p^{fo} = P(x)$ if p is a primitive proposition
- $(\varphi \wedge \psi)^{fo} = \varphi^{fo} \wedge \psi^{fo}$
- $(\neg\varphi)^{fo} = \neg(\varphi^{fo})$
- $(\Box\varphi)^{fo} = \forall y(R(x, y) \Rightarrow \varphi^{fo}[x/y])$,

where $\varphi^{fo}[x/y]$ is the result of replacing all free occurences of x in φ^{fo} by y. Let *MDL* be the set of first-order formulas that are of the form φ^{fo} for some modal formula φ. It is easy to see that when formulas in *MDL* are put into prenex form, we can have arbitrarily deep alternation of quantifiers. Thus, *MDL* is syntactically distinct from the Ackermann class and the Bernays-Schönfinkel class. Although we do not go into details here, we remark that the results of van Benthem [Ben85] characterizing *MDL* show that in fact it is inequivalent in expressive power to both of these classes.

Given a Kripke structure $M = (S, \mathcal{R}, \pi)$, let M^{fo} be the relational structure over Φ with domain S, where the interpretation of P_i is the set of states in S where p_i is true according to π and the interpretation of R is $\mathcal{R}$. As we said in the introduction, the following result is well known (see [Ben85] for a proof):

Proposition 3.1: *φ is valid in M iff $\forall x\varphi^{fo}$ is true in M^{fo}.*

The translation from modal formulas to *MDL* uses an unbounded number of distinct variables in the quantification: For each occurrence of $\Box$, we have to quantify over a fresh variable y. There has been interest recently in restricted languages where only a bounded number of distinct variables appear (e.g., [IK89, KV90b]). Taking Φ as above, let $\mathcal{L}^2_{\omega\omega}(\Phi)$ consist of all first-order formulas over the vocabulary Φ where at most 2 variables are used. As van Benthem has observed [Ben85], we can actually translate modal formulas into $\mathcal{L}^2_{\omega\omega}(\Phi)$, by cleverly reusing variables. Using $\varphi^{fo'}$ to denote the new translation, the only different clause is in the translation of $\Box$ formulas:

- $(\Box\varphi)^{fo'} = \forall y(R(x,y) \Rightarrow \forall x(x = y \Rightarrow \varphi^{fo'}))$

For example, while

$$(\Box\Box p)^{fo} = \forall z(R(x,z) \Rightarrow \forall y(R(z,y) \Rightarrow P(y))),$$

we have

$$(\Box\Box p)^{fo'} = \forall y(R(x,y) \Rightarrow \forall x(x = y \Rightarrow \forall y(R(x,y) \Rightarrow P(y)))).$$

Although we do not pursue this issue further here, this observation shows at least one way in which modal formulas are less expressive than full first-order formulas.

We take $\Pi^1_1(\forall x MDL)$ (resp., $\Sigma^1_1(\exists x MDL)$) to consist of formulas of the form $\forall\mathbf{P}\,\forall x\varphi$ (resp., $\exists\mathbf{P}\,\exists x\varphi$), where φ is a first-order formula in MDL with unary predicates in $\mathbf{P}$ and binary predicate R. Given a frame $F = (S, \mathcal{R})$, let F^{fo} be the relational structure over R with domain S, where the interpretation of R is $\mathcal{R}$. It immediately follows from Proposition 3.1 that

Proposition 3.2: *φ is valid in F iff $\forall\mathbf{P}\forall x\varphi^{fo}$ is true in F^{fo}, where $\mathbf{P}$ includes the unary predicates that appear in φ^{fo}.*

Thus, frame validity can be expressed by formulas in $\Pi^1_1(\forall x MDL)$; analogously, frame satisfiability can be expressed by formulas in $\Sigma^1_1(\exists x MDL)$. This leads us to consider the expressive power of $\Sigma^1_1(\exists x MDL)$. It is well-known that $\Sigma^1_1(\exists x MDL)$ is incomparable in expressive to first-order logic [Ben85]. We conjecture that $\Sigma^1_1(\exists x MDL)$ is incomparable in expressive power to both Σ^1_1(Ackermann) and Σ^1_1(Schönfinkel), but have no proof of this. Of more interest to us here is that, just like Σ^1_1(Schönfinkel) [KV87] and Σ^1_1(Ackermann) [KV90a], $\Sigma^1_1(\exists x MDL)$ can express NP-complete properties. In particular, we now give a construction (due to Moshe Vardi) showing that $\Sigma^1_1(\exists x MDL)$ can express satisfiability of CNF formulas.

With every propositional formula α in CNF, we construct a frame F_α; we then define a modal formula φ_{SAT} such that φ_{SAT} is satisfiable in F_α iff α is a satisfiable propositional formula. This gives us the result we want.

Given α, we think of F_α as a rooted dag. From the root, we construct one successor for each clause in α. We also have a leaf node for each primitive proposition that appears in α. Suppose that β is one of the clauses in α. If the primitive proposition p is one the disjuncts that appears in β, then there is a path of length one to the node representing p. If $\neg p$ is one the disjuncts in β, then there is a path of length two from the node representing β to the node representing p. Finally, we add a path of length 3 starting at the root. (This will allow us to distinguish the root from all other nodes in F_α, none of which are at the beginning of paths of length longer than 2.) This completes the description of F_α. Thus, for example, if α is the formula $(p_1 \vee \neg p_2 \vee p_3) \wedge (p_2 \vee \neg p_3 \vee p_4)$, the frame F_α is shown in Figure 1 below. We take φ_{SAT} to be $\Diamond\Diamond\Diamond \mathit{true} \wedge \Box((\Diamond q \wedge \Box \mathit{false}) \vee \Diamond\Diamond\neg q)$.

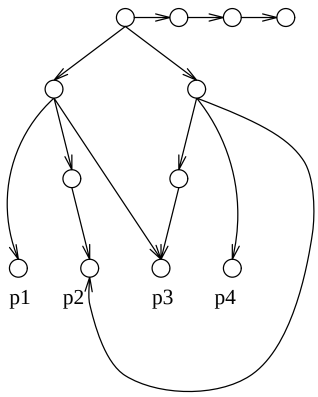

Figure 1: The frame F_α

Theorem 3.3: *If α is a propositional formula in CNF, then φ_{SAT} is satisfiable in F_α iff the CNF formula α is satisfiable.*

Proof: Suppose that α is satisfiable. Let v be a truth assignment satisfying α. Consider the structure $M = (S_\alpha, \mathcal{R}_\alpha, \pi_\alpha)$ based on F_α, where π_α is defined so that, for each primitive proposition p that appears in α, if $s \in S_\alpha$ is a leaf node representing p, then $\pi_\alpha(s)(q) = v(p)$. That is, q is true at the state s according to π_α iff p is true according to v. The truth value that π_α assigns to q at non-leaf nodes is irrelevant. It is easy to check that, if s_0 is the root of F_α, then $(M_\alpha, s_0) \models \varphi_{SAT}$; thus φ_{SAT} is satisfiable in F_α.

Conversely, suppose that φ_{SAT} is satisfiable in F_α. Thus, there is a model $M_\alpha = (S_\alpha, \mathcal{R}_\alpha, \pi_\alpha)$ and a state $s \in S_\alpha$ such that $(M_\alpha, s) \models \varphi_{SAT}$. In particular, that means that $(M_\alpha, s) \models \Diamond\Diamond\Diamond true$. It is easy to see that this forces s to be the root. Let v be the truth assignment to the primitive propositions in α such that $v(p) = \mathbf{true}$ iff q is true according at π_α at the node in S_α corresponding to p. We leave it to the reader to check that α must be true under truth assignment v, and hence that α is satisfiable. ▮

This shows that satisfiability of CNF formulas is expressible in $\Sigma_1^1(\exists x MDL)$.

4 0-1 laws for structure validity

It is easy to see that the mapping $M \rightarrow M^{fo}$ gives a one-to-one correspondence between Kripke structures with state space $\{1, \ldots, n\}$ and relational structures over Φ with domain $\{1, \ldots, n\}$. Thus, the following corollary to Theorem 3.1 is immediate.

Corollary 4.1: *The fraction of Kripke structures with state space $\{1, \ldots, n\}$ for which φ is valid is the same as the fraction of relational structures over Φ for which $\forall x \varphi^{fo}$ is true.*

Putting this together with the 0-1 law for first-order logic, we get

Corollary 4.2: *There is a 0-1 law for structure validity.*

This translation does not give us the other results claimed in our introduction. These all follow from the following simple observation. Recall that $\Diamond$ is the dual of $\Box$, so that $\Diamond\varphi$ is an abbreviation for $\neg\Box\neg\varphi$. Thus, $(M,s) \models \Diamond\varphi$ if there is some state t such that $(s,t) \in \mathcal{R}$ and $(M,t) \models \varphi$.

Proposition 4.3: *If φ is a consistent propositional formula, then $\Diamond\varphi$ is valid in almost all structures.*

Proof: Suppose that φ mentions k primitive propositions. There are 2^k possible assignments of truth values to these primitive propositions. Since φ is consistent, then at least one of these truth assignments makes φ true. Thus, given states s and t in a Kripke structure, the probability that t is a successor of s satisfying φ is at least $1/2^{k+1}$. The probability that a given state in a structure with state space $\{1,\ldots,n\}$ does not have any $\mathcal{R}$-successors where φ is true is thus at most $(1-1/2^{k+1})^n$. Hence, the probability that some state in such a structure does not have any $\mathcal{R}$ successors where φ is true is at most $\alpha(n) = n(1-1/2^{k+1})^n$. It is easy to see that $\lim_{n\to\infty}\alpha(n) = 0$. Thus, for almost all structures, $\Diamond\varphi$ is valid. ∎

We now provide a translation from an arbitrary modal formula φ to a propositional formula φ^r, with the property that $\varphi \Leftrightarrow \varphi^r$ is almost-surely valid. We proceed by induction on the structure of formulas:

- $p^r = p$ for a primitive proposition p
- $(\varphi \wedge \psi)^r = \varphi^r \wedge \psi^r$
- $(\neg\varphi)^r = \neg\varphi^r$
- $(\Box\varphi)^r = \begin{cases} \mathit{true} & \text{if } \varphi^r \text{ is valid} \\ \mathit{false} & \text{otherwise.} \end{cases}$

Proposition 4.4: *The formula $\varphi \Leftrightarrow \varphi^r$ is valid in almost all structures.*

Proof: The only nontrivial case is if φ is of the form $\Box\psi$. By the inductive hypothesis, we know that $\psi \Leftrightarrow \psi^r$ is valid in almost all structures. If ψ^r is valid, it follows that ψ is valid in almost all structures, and hence $\Box\psi$ is valid in almost all structures. Thus, $\Box\psi \Leftrightarrow \mathit{true}$ is valid in almost all structures. But $(\Box\psi)^r =_{\mathrm{def}} \mathit{true}$ in this case, so $\Box\psi \Leftrightarrow (\Box\psi)^r$ is valid in almost all structures. If ψ^r is not valid, then $\neg\psi^r$ is satisfiable. By Proposition 4.3, we know that $\Diamond\neg\psi^r$ is valid in almost all structures. From the inductive hypothesis, it follows that $\Diamond\neg\psi$ is valid in almost all structures, and hence that $\Box\psi \Leftrightarrow \mathit{false}$ is valid in almost all structures. Since $(\Box\psi)^r =_{\mathrm{def}} \mathit{false}$ in this case, again we get that $\Box\psi \Leftrightarrow (\Box\psi)^r$ is valid in almost all structures. ∎

We now immediately get:

Theorem 4.5: *For all modal formulas φ, we have $\nu(\varphi) = 1$ iff the propositional formula φ^r is valid; otherwise $\nu(\varphi) = 0$.*

We next consider the complexity of computing whether a formula is almost-surely valid. The situation is surprisingly subtle. For one thing, it turns out to matter if we take Φ to be finite or infinite. Notice that if we take Φ to be finite, the complexity of computing satisfiability for propositional formulas over Φ is linear time. We get to NP only by allowing an unbounded number of propositions. An analogous situation occurs here (which is precisely why we allowed Φ to be infinite in general).

There is another subtlety involving how we represent formulas. Typically, when we compute upper or lower bounds on complexity for the satisfiability problem, bounds are given as functions of the length of the formula, represented as a string of symbols. Of course, there are other ways of representing the formula. We could represent it as a tree, with the leaves labeled by primitive propositions and the interior nodes labeled by operations such as conjunction, negation, or $\Box$. With each interior node we can associate the formula that results from applying the operation labeling the node to the formulas represented by the nodes of its successors. It is easy to see that the size of the tree (i.e., the number of nodes in the tree) is proportional to the length of the original formula. Thus, choosing between these two representations is a matter of taste.

Rather than representing the formula as a tree, we could represent it as a dag (directed acyclic graph), so that a node can be the successor of more than one node. The dag representation can be exponentially more succinct than the tree representation. For example, if φ is a complex formula, then the representation of $\psi = \varphi \wedge \neg\Box\varphi$ as a dag requires only two more nodes than the representation of φ, since the node representing φ can be "reused", although the length of ψ is more than twice the length of φ. Because the dag representation is more succinct than the tree representation, a lower bound is stronger if it is proved for the tree representation, while an upper bound is stronger if it is proved for the dag representation. To distinguish the two representations, we use $||\varphi||$ to denote the length of φ under the tree representation and $|\varphi|$ to denote the length of φ under the dag representation.

Typically not much issue is made of the representation of a formula. This is because for all logics that we are aware of, the complexity of validity is independent of whether we use a tree or dag representation. In particular, it is easy to see that this is true for propositional logic and all standard modal logics. Essentially, any upper bound for complexity that is based on considering subformulas will typically be independent of the representation. The situation is different if we consider the complexity of evaluating the truth of a propositional formula. This is known to be complete for polynomial time if we take the dag representation [Lad75] and complete for alternating logarithmic time if we use the tree representation [Bus87].

If Φ is finite, it is easy to show that deciding almost-sure structure validity for formulas in Φ is in polynomial time. (Of course, the constants are exponential in $|\Phi|$.) If Φ is infinite, then it is easy to show that the problem of deciding almost-sure structure validity is in $\Delta_2^p = P^{NP}$, at the second level of the polynomial hierarchy [Sto77]. This is true whether we use the tree or dag representation. Moshe Vardi has proved a matching Δ_2^p lower bound for the dag representation; techniques independently developed by Gottlob [Got95] can also be used to prove that for the dag representation, the problem of deciding almost-sure structure validity is Δ_2^p-complete. On the other hand, using Gottlob's techniques, it can be shown that for the tree representation, the problem of deciding almost-sure structure validity is $\Delta_2^{p,\log(n)}$-complete. (The complexity class $\Delta_2^{p,\log(n)}$ corresponds to languages where on input size n, we are allowed to ask only $\log(n)$ queries of the NP oracle.) Thus, there is almost surely a gap between the complexity of deciding almost-sure structure validity for the the tree representation and the dag representation.

Theorem 4.6: *If Φ is finite, then deciding almost-sure structure validity for formulas in $\mathcal{L}(\Phi)$ is in polynomial time (for both the dag and tree representations). If Φ is infinite, then deciding almost-sure structure validity is Δ_2^p-complete for the dag representation of formulas, and is $\Delta_2^{p,\log(n)}$-complete for the tree representation.*

Proof: We can reduce the formula φ to φ^r by querying an oracle for satisfiability no more than $|\varphi|$ times. One more query will determine if φ^r is valid. These are polynomial time queries if Φ is finite, whether φ is represented as a tree or a dag; they are NP queries if Φ is infinite. Thus, it follows that almost-sure validity is in polynomial time if Φ is finite and in Δ_2^p if Φ is infinite, for both representations.

We now present a modification of Vardi's proof of the Δ_2^p lower bound for the dag representation. Consider a pair (α, Φ') consisting of a propositional formula α and a sequence $\Phi' = \langle p_1, \ldots, p_n \rangle$ of primitive propositions such that all the primitive propositions that appear in α are contained in Φ'. We can order the truth assignments to the propositions in Φ' in lexicographic order, where we write $v < v'$ for two valuations if for some i, we have $v'(p_i) = \mathit{true}$, $v(p_i) = \mathit{false}$, and $v(p_j) = v'(p_j)$ for $j < i$. Let the language L consist of all pairs (α, Φ') such that α is satisfiable, and if v is the maximum satisfying assignment for α (with respect to the lexicographic order just defined), we have $v(p_n) = \mathit{true}$. This language is known to be Δ_2^p-complete [Kre88]. We now show how to reduce checking membership in this language to checking whether a modal formula is almost-surely structure valid.

Given $(\alpha, \langle p_1, \ldots, p_n \rangle)$, we define modal formulas $\alpha_0, \ldots, \alpha_n$, $q_1, \ldots, q_n$, inductively. The goal is to define q_m so that q_m is almost-surely structure valid iff α is satisfiable and the maximum satisfying assignment for α makes p_m true. We take $\alpha_0 = \alpha$. Suppose we have defined $\alpha_0, \ldots, \alpha_m$ and $q_1, \ldots, q_m$, for $m < n$. We define $q_{m+1} = \Diamond(p_{m+1} \wedge \alpha_m)$ and α_{m+1} to be α with all occurences of p_j, $j \leq m+1$, replaced by q_j. If we use the tree representation of α, then it is not hard to show that, in the worst case, $||\alpha_m||$ can grow exponentially large. As we now show, there is a succinct dag representation of these formulas.

We can assume without loss of generality that all the p_i's actually appear in α (for if p_i does not appear, we can always add a conjunct of the form $p_i \vee \neg p_i$ to α). It is thus easy to see from the definition of α_m and q_m that if $m < n$, then the dag representation of both q_{m+1} and α_m contain as subdags representations of $q_1, \ldots, q_m$. Given a dag representation for α_m, there is clearly a dag representation of q_{m+1} such that $|q_{m+1}| = |\alpha_m| + 3$: we simply take the dag representation for α_m and add nodes for p_{m+1}, $\wedge$, and $\Diamond$. There is also clearly a dag representation of α_{m+1} such that $|\alpha_{m+1}| \leq |\alpha| + |q_{m+1}|$. We simply write down the dag representation of α and q_{m+1}, and then replace all edges in the dag for α leading to p_j, for $j \leq m+1$, with edges leading to the node representing q_j in the dag representation for q_{m+1}. Now an easy inductive argument shows that, with this representation, we have $|q_m| \leq m(|\alpha|+3)$ and $|\alpha_m| \leq (m+1)|\alpha| + 3m$. In particular, it follows that $|q_n| \leq n(|\alpha| + 3)$.

Finally, we show by induction on m that if $m \geq 1$ then $p_m \wedge \alpha_{m-1}^r$ is satisfiable iff α is satisfiable and the maximum satisfying assignment for α makes p_m true (where the superscript r on α_{m-1} denotes the reduction of Proposition 4.4).

First suppose $m = 1$. Observe $\alpha_0 = \alpha$ is a propositional formula, so $\alpha_0^r = \alpha_0$. Clearly $p_1 \wedge \alpha$ is satisfiable iff α is satisfiable and the maximum satisfying truth assignment for α makes p_1

true.

For the general case, suppose that $p_m \wedge \alpha^r_{m-1}$ is satisfiable. It is easy to see from the definition of α_{m-1} that α^r_{m-1} is α with p_j replaced by q^r_j, $j = 1, \ldots, m-1$. It is immediate that if α^r_{m-1} is satisfiable, then so is α. By the definition of the reduction relation, q^r_j is *true* if $p_j \wedge \alpha_{j-1}$ is satisfiable, and *false* otherwise. Since α is satisfiable, from the induction hypothesis it follows that q^r_j is true iff the maximum satisfying assignment for α makes p_j true. Thus, q^r_j is the truth value of p_j under the maximum satisfying assignment to α for $j < m$. It follows that any truth assignment to $p_m, \ldots, p_n$ that satisfies α^r_{m-1} can be extended to a truth assignment satisfying α that agrees with the maximum truth assignment satisfying α on the truth values of $p_1, \ldots, p_{m-1}$. This means that $p_m \wedge \alpha^r_{m-1}$ is satisfiable iff there is a truth assignment satisfying α that agrees with the maximum truth assignment satisfying α on the truth values of $p_1, \ldots, p_{m-1}$, and makes p_m true. It follows that $p_m \wedge \alpha^r_{m-1}$ is satisfiable iff the maximum truth assignment to α makes p_m true. For the converse, suppose that the maximum truth assignment satisfying α makes p_m true. Similar arguments to those just used show that this truth assignment must satisfy $p_m \wedge \alpha^r_{m-1}$. This completes the inductive step of the proof.

Notice that, by Proposition 4.4, q_n is almost-surely structure valid iff $p_n \wedge \alpha^r_{n-1}$ is satisfiable. By what we have just shown, it follows that q_n is almost-surely structure valid iff $(\alpha, \langle p_1, \ldots, p_n \rangle) \in L$. Thus, deciding almost-sure structure validity is Δ^p_2 hard.

To prove the $\Delta_2^{p,\log(n)}$ lower bound for the tree representation, we use an argument due to Larry Stockemeyer: Given a Turing machine **A** with an oracle for SAT that runs in polynomial time and asks only $\log(n)$ queries, we can describe its computation by a tree with polynomially many branches, each of polynomial length. (Each branch corresponds to one possible sequence of outcomes of queries to the oracle.) Using standard techniques, we can easily encode this tree in a modal formula, using $\Diamond$ formulas to represent queries to the oracle. Thus, given **A** and an input x, we can effectively find a modal formula $\varphi_{\mathbf{A},x}$ such that φ is almost-surely satisfiable (i.e., $\nu(\neg\varphi_{\mathbf{A},x}) = 0$) iff **A** accepts input x. This gives us the lower bound. Note for future reference that $\varphi_{\mathbf{A},x}$ has no nested occurrences of $\Box$.

The $\Delta_2^{p,\log(n)}$ upper bound for the tree representation follows from Gottlob's results; we refer the reader to [Got95] for further details. ∎

Finally, we can use our techniques to get a complete axiomatization for almost-sure validity. Consider the following axiom:

C. $\Diamond\varphi$, if φ is a consistent propositional formula.[1]

Let K^C be the axiom system resulting from adding axiom C to K. It turns out that the logic characterized by K^C was introduced by Carnap [Car47]. It is not a "logic" in the traditional sense, in that it is not closed under uniform substitutions. For example, $\Diamond p$ is provable in K^C, where p is a primitive proposition, but if we substitute $q \wedge \neg q$ for p, the resulting formula,

[1] Of course, checking whether a given formula is an instance of this axiom scheme is NP-complete. We can get an axiom that is simpler to check (and also gives us completeness, with a little extra work) as follows. As usual, we say that a *literal* is either p or $\neg p$, where p is a primitive proposition. A *consistent conjunction of literal* is a conjunction of literals that does not contain both p and $\neg p$ as conjuncts for some primitive proposition p. Rather than considering $\Diamond\varphi$ for any consistent propositional formula φ, it is not to hard to show that it suffices to consider $\Diamond\varphi$ where φ is a consistent conjunction of literals.

$\Diamond(q\wedge\neg q)$, is not provable. Nevertheless, as we now show, K^C characterizes almost-sure structure validity.

Theorem 4.7: *K^C is a sound and complete axiomatization for almost-sure structure validity.*

Proof: The soundness of axiom C follows immediately from Proposition 4.3. For completeness, it suffices to show that the validity $\varphi \Leftrightarrow \varphi^r$ is provable in K^C. We proceed, as usual, by induction on the structure of φ. The only nontrivial case is if φ is of the form $\Box\psi$. By the induction hypothesis, we can assume that $\psi \Leftrightarrow \psi^r$ is provable. Using Axiom A2 and straightforward modal reasoning, we can show that $\Box\psi \Leftrightarrow \Box\psi^r$ is provable. Now there are two cases to consider. If ψ^r is valid, then ψ^r is provable (by A1), and hence (by R1) so is $\Box\psi^r$. It follows that $\Box\psi^r \Leftrightarrow \mathit{true}$ is provable as well. Since $(\Box\psi)^r = \mathit{true}$ in this case, we are done. If ψ^r is not valid, then $\neg\psi^r$ is satisfiable. By axiom C, $\Diamond\neg\psi^r$ is provable. But this is just an abbreviation for $\neg\Box\neg\neg\psi^r$. Again, using straightforward modal reasoning, it follows that $\neg\Box\psi^r$ is provable. Thus, $\Box\psi^r \Leftrightarrow \mathit{false}$ is provable. Since $(\Box\psi)^r = \mathit{false}$ in this case, we are done. ∎

As Fagin showed [Fag76], there is one (infinite) relational structure U_∞ with the property that a first-order formula (without constant or function symbols) is true in U_∞ iff it has asymptotic probability 1. From Proposition 3.1, a similar result holds for structure validity. The following result characterizes this structure, and gives further information.

Given a set Φ of primitive propositions, we define the *canonical asymptotic Kripke structure over* Φ, M_Φ, as follows: Let Π_Φ consist of all the truth assignments to the propositions in Φ which make only finitely many propositions true. Let $M_\Phi = (\Pi_\Phi, \mathcal{R}, \pi)$, where $\mathcal{R}$ is the universal relation, and if $v \in \Pi_\Phi$, then $\pi(v) = v$.

Theorem 4.8: *For all formulas $\varphi \in \mathcal{L}(\Phi)$, we have $\nu(\varphi) = 1$ iff φ is valid in M_Φ.*

Proof: Left to the reader. (We remark that that we could have taken Π_Φ to consist of all the truth assignments to the primitive propositions in Φ, and the same construction would have worked. Our construction shows that if Φ is countable, then we can take M_Φ to be countable.) ∎

We have now settled the questions regarding 0-1 laws for structure validity for the modal logic K. We can ask the same questions for the modal logics T, S4, and S5; that is, we can consider limiting probabilities with respect to $\mathcal{M}^r$, $\mathcal{M}^{rt}$, or $\mathcal{M}^{rst}$.

It is easy to see that the 0-1 law for $\mathcal{M}^r$ coincides with that for $\mathcal{M}$. This follows immediately from the fact that Propositions 4.3 and 4.4 hold (with essentially no change in proof) even if we restrict to structures in $\mathcal{M}^r$. Thus, we get

Theorem 4.9: *For all modal formulas φ, we have $\nu^r(\varphi) = 1$ iff the propositional formula φ^r is valid; otherwise $\nu^r(\varphi) = 0$. Moreover, K^C is a sound and complete axiomatization for almost-sure validity with respect to $\mathcal{M}^r$.*

Things change significantly if we consider $\mathcal{M}^{rt}$ and $\mathcal{M}^{rst}$.[2] We start with $\mathcal{M}^{rst}$. Since there are fewer structures in $\mathcal{M}^{rst}$ than in $\mathcal{M}$, there are more formulas valid when we restrict to $\mathcal{M}^{rst}$

[2]In a preliminary version of this paper, which appears in the Proceedings of the Seventh Annual IEEE Symposium on Logic in Computer Science, 1992, we claimed that K^C is also a sound axiomatization for almost-sure validity with respect to $\mathcal{M}^{rt}$ and $\mathcal{M}^{rst}$. As the material below shows, this claim is false. We thank Moshe Vardi for pointing out the potential problems in our earlier proof.

than $\mathcal{M}$. On an axiomatic level, there are more axioms in S5 than in K. We might expect that more formulas (or, at least, no fewer) would be almost-surely valid when we restrict to $\mathcal{M}^{rst}$ than if we consider $\mathcal{M}$. As we now show, this is false.

First observe that if ψ is an axiom of S5, then $\nu(\psi) = 1$. For example, consider the axiom $\neg\Box\varphi \Rightarrow \Box\neg\Box\varphi$. By definition, we have that either $(\Box\varphi)^r = \mathit{true}$ or $(\Box\varphi)^r = \mathit{false}$. It is easy to check that, in either case, we have $(\neg\Box\varphi \Rightarrow \Box\neg\Box\varphi)^r = \mathit{true}$. Similarly, it is easy to show that, for any formula φ, we have $(\Box\varphi \Rightarrow \varphi)^r = \mathit{true}$ and $(\Box\varphi \Rightarrow \Box\Box\varphi)^r = \mathit{true}$. The fact that all the axioms of S5 hold with probability 1 now follows immediately from Proposition 4.4. This is true despite the fact that, in almost all structures of $\mathcal{M}$, the relation $\mathcal{R}$ is *not* an equivalence relation.

Clearly the formulas provable in S5 are valid in all (and hence almost all) structures in $\mathcal{M}^{rst}$. We now show that $\nu^{rst}(\varphi) = 1$ iff φ is provable in S5. We need the following result, which is an easy consequence of a more general result due to Compton [Com87]. Compton shows that if a class of relational structures is closed under disjoint unions and components and satisfies some other properties, then, for any given component type and any ℓ, the probability that in a random structure there are at least ℓ components of this type approaches 1. The components in the case of equivalence relations are the equivalence classes. For each k, the size k equivalence classes form a component type. Equivalence relations are easily seen to satisfy all of Compton's conditions. Thus, in particular, we get

Theorem 4.10: *For all k and ℓ, we have*

$$\lim_{n\to\infty} \nu^{rst}(\{M = (S, \mathcal{R}, \pi) \in \mathcal{M}_n^{rst} : \textit{there are at least } \ell \ \mathcal{R}\textit{-equivalence classes of size } k\}) = 1.$$

Theorem 4.11: *For all modal formulas φ, we have $\nu^{rst}(\varphi) = 1$ iff φ is provable in S5; otherwise $\nu^{rst}(\varphi) = 0$.*

Proof: Clearly if φ is provable in S5, then $\nu^{rst}(\varphi) = 1$. For the converse, suppose that φ is not provable in S5. Thus, $\neg\varphi$ is consistent with S5. By a result of Ladner [Lad77], it follows that $\neg\varphi$ is satisfiable in a frame $M = (S, \mathcal{R}, \pi) \in \mathcal{M}^{rst}$ such that $|S| = k \leq |\neg\varphi|$ and $\mathcal{R}$ is the universal relation on S. Fix $\epsilon > 0$. Clearly there is some $\ell > 0$ so that if we define the truth assignment at random in ℓ frames in $\mathcal{F}^{rst}$ of size k, then the probability that at least one of them will result in a structure isomorphic to M, and hence satisfying $\neg\varphi$, is at least $1-\epsilon$. From Theorem 4.10, it follows that $\lim_{n\to\infty} \nu_n^{rst}(\{M \in \mathcal{M}_n^{rst} : \neg\varphi \text{ is satisfied in } M\}) > 1-\epsilon$. Since this is true for all $\epsilon > 0$, we have that $\nu^{rst}(\varphi) = 0$. ∎

It immediately follows that S5 is a sound and complete axiomatization for almost-sure structure validity with respect to $\mathcal{M}^{rst}$. In particular, that means that a formula such as $\Diamond p$ (where p is a primitive proposition) which is almost-surely valid with respect to $\mathcal{M}$, is *not* almost-surely valid with respect to $\mathcal{M}^{rst}$.

The following complexity results are also immediate from the result of [Lad77] mentioned above.

Corollary 4.12: *If Φ is finite, then deciding almost-sure validity with respect to $\mathcal{M}^{rst}$ for formulas in $\mathcal{L}(\Phi)$ is in polynomial time; if Φ is infinite, it is co-NP-complete (for both the dag and tree representations).*

We now turn our attention to $\mathcal{M}^{rt}$. To characterize almost-sure structure validity with respect to $\mathcal{M}^{rt}$, we need to obtain asymptotic properties of structures where the possibility relation is reflexive and transitive. While there does not seem to be too much known about this case, a great deal is known about the case where the possibility relation is a partial order. In particular, we have the following result, due to Kleitman and Rothschild [KR75]. Given a partial order $\leq$ on a set S, we say that an element $s \in S$ is an *immediate successor* of an element $s' \in S$ if $s > s'$, and for all t in S, if $s > t \geq s'$, then $t = s'$.

Theorem 4.13: [KR75] *There are $2^{(n^2/4)+(3n/2)+O(\log(n))}$ partial orders on a set of n elements. In addition, with asymptotic probability 1, they can be partitioned into 3 levels: L_0, the set of "maximal" elements which have no immediate successors, L_1, the set of elements all of whose immediate successors are elements in L_0, and L_2, the set of elements all of whose immediate successors are elements in L_1. Moreover, $|L_0| = |L_2| = n/4 + o(n)$, $|L_1| = n/2 + o(n)$, and each element in L_i, $i = 1, 2$, has as immediate successors (asymptotically) half the elements in L_{i-1}.*

We now show that, almost surely, every reflexive transitive relation is in fact a partial order, so that the results of Kleitman and Rothschild apply to reflexive transitive relations as well.

Theorem 4.14: $\lim_{n\to\infty} \nu_n^{rt}(\{M = (S, \mathcal{R}, \pi) \in \mathcal{M}^{rt} : \mathcal{R}$ *is a partial order on* $S\} = 1$.

Proof: Given a reflexive transitive relation $\mathcal{R}$ on S, define the equivalence relation $\sim$ via $s \sim t$ iff both $(s,t) \in \mathcal{R}$ and $(t,s) \in \mathcal{R}$. If $\sim$ partitions S into k equivalence classes, then the quotient relation $\mathcal{R}/\sim$ is a partial order on these k equivalence classes. Clearly $\mathcal{R}$ is a partial order iff $\sim$ is the trivial relation, where all the equivalence classes are singletons.

Let P_k be the number of partial orders on a set of k elements and let $\left\{ {n \atop k} \right\}$ be the number of ways of partioning n elements into exactly k equivalence classes. ($\left\{ {n \atop k} \right\}$ is the Stirling number of the second kind; see [GKP89]). Thus, the number of reflexive transitive relations which are partial orders is P_n, while the number of reflexive transitive relations which are not partial orders is $\sum_{k<n} P_k \cdot \left\{ {n \atop k} \right\}$. To prove the result, it suffices to show

$$\lim_{n\to\infty} \frac{\sum_{k<n} P_k \cdot \left\{ {n \atop k} \right\}}{P_n} = 0.$$

In order to do this, we need a good estimate on $\left\{ {n \atop k} \right\}$. We begin by showing that $\binom{n}{k} n!$ is an overestimate for $\left\{ {n \atop k} \right\}$. To see this, consider any partition, and order the equivalence classes by the minimal elements appearing in them, and order the elements in an equivalence class in increasing order. This gives us an ordering of the n elements in the domain. Suppose the equivalence classes (listed in this order) have size $n_1, \ldots, n_k$. This corresponds to choosing elements $n_1, n_1 + n_2, \ldots, n_1 + \cdots + n_k$ from the domain. Thus, with each partition into k equivalence classes, we can associate a unique pair consisting of a permutation and a choice of k elements out of n.

This estimate suffices for values of k which are smaller than $n - 4\log(n)$. We use a finer estimate for $\left\{ {n \atop k} \right\}$ if $k \geq n - 4\log(n)$. In this case, at least $k - 4\log(n) \geq n - 8\log(n)$ equivalence classes must have size 1. The remaining $4\log(n)$ equivalence classes come from $n - (k - 4\log(n)) \leq 8\log(n)$ elements. Thus, using our earlier estimate, a bound on $\left\{ {n \atop k} \right\}$ in this case is given by

$$
\begin{aligned}
\binom{n}{k-4\log(n)}\left\{ {n-(k-4\log(n)) \atop 4\log(n)} \right\} &\le \binom{n}{n-8\log(n)}\left\{ {8\log(n) \atop 4\log(n)} \right\} \\
&\le \binom{n}{n-8\log(n)}\binom{8\log(n)}{4\log(n)}(8\log(n))! \\
&\le \binom{n}{n-8\log(n)}\, 2^{8\log(n)}(8\log(n))! \\
&= \frac{n!}{(n-8\log(n))!}n^8 \\
&\le n^{8\log(n)}n^8 \\
&= 2^{8\log(n)(\log(n)+1)} .
\end{aligned}
$$

By Theorem 4.13, we can safely approximate P_k by $2^{k^2/4}$ in our asymptotic estimates. Using our estimates for $\left\{ {n \atop k} \right\}$, we obtain

$$
\begin{aligned}
\sum_{k=1}^{n-1}\left\{ {n \atop k} \right\} \cdot 2^{k^2/4} &= \sum_{k=1}^{n-4\log(n)}\left\{ {n \atop k} \right\} \cdot 2^{k^2/4} + \sum_{k=n-4\log(n)+1}^{n-1}\left\{ {n \atop k} \right\} \cdot 2^{k^2/4} \\
&\le n!\; 2^{(n-4\log(n))^2/4}\left(\sum_{k=1}^{n-4\log(n)}\binom{n}{k}\right) + 2^{8\log(n)(\log(n)+1)}\sum_{k=n-4\log(n)+1}^{n-1} 2^{k^2/4} \\
&\le n!\; 2^{(n-4\log(n))^2/4}2^n + 2^{8\log(n)(\log(n)+1)}2^{((n-1)^2/4)+1} \\
&\le 2^{(n^2/4)-n\log(n)+n+4\log^2 n} + 2^{(n^2/4)-(n/2)+16\log^2 n+8\log(n)+2} .
\end{aligned}
$$

The theorem now immediately follows. ∎

Using Theorems 4.13 and 4.14, we can prove a 0-1 law for structure validity with respect to $\mathcal{M}^{rt}$ and characterize those formulas that are almost-surely structure valid. Our first step is to get an analogue to Theorem 4.8.

We define the *canonical po-structure over* Φ to be the structure $M_\Phi^{po} = (S, \mathcal{R}, \pi)$ defined somewhat analogously to the canonical asymptotic Kripke structure over Φ. Rather than having one state correspond to each truth assignment in Π_Φ, we have three states corresponding to each truth assignment. Thus, we take $S = \{s_v, t_v, u_v : v \in \Pi_\Phi\}$. We define π so that $\pi(s_v) = \pi(t_v) = \pi(u_v) = v$. Finally, we define $\mathcal{R}$ so that for all $v \in \Pi_\Phi$, the only $\mathcal{R}$-successor of u_v is u_v, the $\mathcal{R}$-successors of t_v are t_v itself and $u_{v'}$, for $v' \in \Pi_\Phi$, and the $\mathcal{R}$-successors of s_v are s_v itself, and $t_{v'}$, $u_{v'}$ for $v' \in \Pi_\Phi$. If we think of a partial order on S defined via $s \le t$ if $(s,t) \in \mathcal{R}$ then, in terms of the partition described in Theorem 4.13, the nodes s_v, $v \in \Pi_\Phi$, are in L_2 (we henceforth call these *root nodes*), the nodes t_v, $v \in \Pi_\Phi$, are in L_1 (we call these *intermediate nodes*), and the nodes u_v, $v \in \Pi_\Phi$, are in L_0 (we call these *leaf nodes*).

Theorem 4.15: *For all modal formulas $\varphi \in \mathcal{L}(\Phi)$, we have $\nu_\Phi^{rt}(\varphi) = 1$ iff φ is valid in M_Φ^{po}, and $\nu_\Phi^{rt}(\varphi) = 0$ otherwise (i.e., $\nu_\Phi^{rt}(\varphi) = 0$ iff $\neg\varphi$ is satisfiable in M_Φ^{po}).*

Proof: By Theorems 4.13 and 4.14, it suffices to show that φ is valid (resp. satisfiable) in M^{po}_{Φ} iff φ is almost-surely valid (resp. almost-surely satisfiable) in structures $M = (S, \mathcal{R}, \pi)$ such that $\mathcal{R}$ is a partial order satisfying the properties described in Theorem 4.13. These properties guarantee, among other things, that there are $O(n)$ states in each of L_0, L_1, and L_2, and that the states in L_1 and L_2 have $O(n)$ $\mathcal{R}$-successors. Suppose Φ is finite. Given such a structure $M = (S, \mathcal{R}, \pi)$, it is almost surely the case that for each pair of truth assignments v, v' to the primitive propositions in Φ, there is a state s such that $\pi(s) = v$, and if s is not in L_0, then there is a state t such that $(s,t) \in \mathcal{R}$ and $\pi(t) = v'$. With these obervations, the result is almost immediate. We leave details to the reader.

If Φ is infinite, given a formula $\varphi \in \mathcal{L}(\Phi)$, let Φ' be a finite subset of Φ such that $\varphi \in \mathcal{L}(\Phi')$. It is easy to see that $\lim_{n\to\infty} \nu_{n,\Phi}(\varphi) = \lim_{n\to\infty} \nu_{n,\Phi'}(\varphi)$. By the arguments above, $\lim_{n\to\infty} \nu_{n,\Phi'}(\varphi) = 1$ iff φ is valid in $M^{po}_{\Phi'}$, and $\lim_{n\to\infty} \nu_{n,\Phi'}(\varphi) = 0$ otherwise. Finally, it is easy to see that φ is valid (resp. satisfiable) in $M^{po}_{\Phi'}$ iff φ is valid (resp. satisfiable) in M^{po}_{Φ}. The result now follows. ∎

Theorem 4.15 not only shows that there is a 0-1 law for structure validity with respect to $\mathcal{M}^{rt}$, but gives us the necessary tools to get a complete axiomatization for almost-sure validity.

Consider the following axioms:

DEP2. $\neg(\varphi_1 \wedge \Diamond(\neg\varphi_1 \wedge \varphi_2 \wedge \Diamond(\neg\varphi_2 \wedge \varphi_3 \wedge \Diamond(\neg\varphi_3))))$

FULL. $(\varphi_1 \wedge \Diamond(\neg\varphi_1 \wedge \varphi_2 \wedge \Diamond(\neg\varphi_2)) \Rightarrow \Diamond(\varphi_4 \wedge \Diamond\varphi_5)$, if φ_4 and φ_5 are consistent propositional formulas.

C′. $(\psi \Rightarrow \Box\psi) \vee \Diamond\varphi$ if φ is a consistent propositional formula.

The axiom DEP2 (which stands for *depth 2*) captures the fact that there cannot be "paths" of length 3 in the canonical po-structure. The axiom FULL captures the fact that all paths starting at root nodes of the canonical po-structure have length 2. Note that the antecedent of FULL holds only at root nodes; the conclusion clearly holds at root nodes as well. Axiom C′, a weakening of axiom C, says that either a state is a leaf of the canonical po-structure, in which case $\psi \Rightarrow \Box\psi$ holds, or every satisfiable propositional formula is satisfied in one of its successors. of them. Let S4$^+$ consist of S4 together with the axioms DEP2, FULL, and C′.

Theorem 4.16: *S4$^+$ is a sound and complete axiomatization for almost-sure structure validity with respect to $\mathcal{M}^{rt}$.*

Proof: Since every formula φ is in $\mathcal{L}(\Phi)$ for some finite Φ, soundness is immediate from Theorems 4.15. Completeness follows using Theorem 4.15 and a standard "canonical model" construction, which goes back to [Mak66] (see, for example, [HM92] for examples of its application in modal logic). Indeed, for finite Φ, the canonical model construction can be shown to give precisely the canonical model M^{po}_{Φ}. We omit details here. ∎

Finally, we consider complexity.

Theorem 4.17: *If Φ is finite, then deciding almost-sure validity with respect to $\mathcal{M}^{rt}$ for formulas in $\mathcal{L}(\Phi)$ is in polynomial time; if Φ is infinite, it is $\Delta_2^{p,\log(n)}$-complete for the tree representation, $\Delta_2^{p,\log(n)}$-hard for the dag representation and in Δ_2^p for the dag representation.*

Proof: The result is immediate for the case that Φ is finite, since then M_Φ^{po} is finite and it can easily be checked whether a given formula φ is valid in M_Φ^{po}. Suppose that Φ is infinite.

For the upper bound, we show that, given a formula φ, we can effectively find a formula φ^* whose length is polynomial in that of φ such that φ is almost-surely structure valid with respect to $\mathcal{M}^{rt}$ iff φ^* is almost-surely structure valid with respect to $\mathcal{M}$. The upper bound then follows from Theorem 4.6.

Given a formula φ, we actually construct three formulas, φ^0, φ^1, and φ^2, with the property that φ^0 is valid iff φ is true at the leaves of the canonical po-structure, φ^2 is valid iff φ is true at all the root nodes of the canonical po-structure, and φ^1 is valid iff φ is true at all the intermediate nodes of the canonical po-structure. We can then take $\varphi^* = \varphi^0 \wedge \varphi^1 \wedge \varphi^2$.

We define the mapping $\varphi \rightarrow \varphi^i$, $i = 0, 1, 2$ by induction on structure, with the only interesting clause being the one involving $\Box$:

- $p^i = p$ for a primitive proposition p
- $(\varphi \wedge \psi)^i = \varphi^i \wedge \psi^i$
- $(\neg\varphi)^i = \neg\varphi^i$
- $(\Box\varphi)^i = \begin{cases} \varphi^0 & \text{if } i = 0 \\ \varphi^i \wedge \Box\varphi^{i-1} & \text{if } i = 1, 2. \end{cases}$

The following facts are now easy to prove:

1. (a) φ^0 is a propositional formula, (b) $|\varphi^0| \leq |\varphi|$, and (c) if u is a leaf node in $\mathcal{M}_\Phi^{po}$, then $M_\Phi^{po}, u \models \varphi \equiv \varphi^0$.
2. (a) φ^1 has no nested occurrences of $\Box$, (b) if there are k occurrences of $\Box$ in φ, then $|\varphi^1| \leq |\varphi| + k|\varphi^0|$ (the proof is by induction on k); it follows that $|\varphi^1| \leq |\varphi|^2$, and (c) if t is an intermediate node in $\mathcal{M}_\Phi^{po}$, then $M_\Phi^{po}, t \models \varphi \equiv \varphi^1$.
3. (a) φ^2 has depth of nesting of $\Box$ of at most two, (b) if there are k occurrences of $\Box$ in φ, then $|\varphi^2| \leq |\varphi| + k|\varphi^1|$; it follows that $|\varphi^2| \leq |\varphi|^3$, and (c) if s is a root node in $\mathcal{M}_\Phi^{po}$, then $M_\Phi^{po}, s \models \varphi \equiv \varphi^2$.

It is also easy to see that

4. if φ is a propositional formula, then $M_\Phi, v \models \varphi$ iff $M_\Phi^{po}, u_v \models \varphi$.
5. if there are no nested occurrences of $\Box$ in φ, then $M_\Phi, v \models \varphi$ iff $M_\Phi^{po}, t_v \models \varphi$.
6. if the depth of nesting of $\Box$ in φ is at most 2, then $M_\Phi, v \models \varphi$ iff $M_\Phi^{po}, s_v \models \varphi$.

Putting these facts together, we see that φ is valid in M_Φ^{po} iff $\varphi^0 \wedge \varphi^1 \wedge \varphi^2$ is valid in M_Φ. From Theorems 4.7 and 4.16, it follows that $K^C \vdash \varphi^0 \wedge \varphi^1 \wedge \varphi^2$ iff S4$^+ \vdash \varphi$. From Theorem 4.6, it follows that deciding almost-sure validity with respect to $\mathcal{M}^{rt}$ is in Δ_2^p for the dag representation and in $\Delta_2^{p,\log(n)}$ for the tree representation.

For the lower bound in the case of the tree representation, recall that in the proof of the corresponding lower bound in Theorem 4.6, given an oracle Turing machine $\mathbf{A}$ that, on input of size n, asks only $\log(n)$ queries of the NP-oracle, and an input x, we constructed a formula $\varphi_{\mathbf{A},x}$ such that $\mathbf{A}$ accepts x iff $\varphi_{\mathbf{A},x}$ is almost-surely satisfiable with respect to $\mathcal{M}$. Moreover, $\varphi_{\mathbf{A},x}$ had no nested occurrences of $\Box$. Let q be a primitive proposition not appearing in $\varphi_{\mathbf{A},x}$. Notice that $q \wedge \Diamond\neg q$ cannot be satisfied at a leaf node in M_Φ^{po}. From facts (5) and (6) above, it follows that $\varphi_{\mathbf{A},x} \wedge q \wedge \Diamond\neg q$ is satisfiable in M_Φ^{po} iff $\varphi_{\mathbf{A},x} \wedge q \wedge \Diamond\neg q$ is satisfiable in M_Φ. It is also easy to see that $\varphi_{\mathbf{A},x} \wedge q \wedge \Diamond\neg q$ is satisfiable in M_Φ iff $\varphi_{\mathbf{A},x}$ is satisfiable in M_Φ. By Theorem 4.8, $\varphi_{\mathbf{A},x}$ is satisfiable in M_Φ iff $\varphi_{\mathbf{A},x}$ is almost-surely satisfiable with respect to $\mathcal{M}$. The lower bound now follows. Clearly the same lower bound holds for the dag representation. ∎

Our proof shows that checking for almost-sure validity with respect to $\mathcal{M}^{rt}$ reduces to checking for almost-sure validity of formulas where $\Box$ is nested to depth 2. We do not know if this is any easier than the general problem. In particular, we have not been able to close the gap between $\Delta_2^{p,\log(n)}$ and Δ_2^p in the case of almost-sure validity with respect to $\mathcal{M}^{rt}$.

5 0-1 laws for frame validity

Our main goal in this section is to prove the 0-1 law for frame validity.

Theorem 5.1: *For every modal formula φ, either $\mu(\varphi) = 0$ or $\mu(\varphi) = 1$.*

Our approach to proving Theorem 5.1 is similar to the standard tableau technique for modal satisfiability [HC68]. We define a class of frames called the *special* frames, and reduce almost-sure frame satisfiability to satisfiability in special frames. This is made precise in Theorem 5.5 below. In order to define special frames, we first need to define a few other notions.

Definition 5.2: Given a frame $F = (S, \mathcal{R})$, $s \in S$ and $A \subseteq S$, define $\mathcal{R}(s) = \{t : (s,t) \in \mathcal{R}\}$ and $\mathcal{R}(A) = \cup_{t\in A}\mathcal{R}(t)$. Similarly, define $\mathcal{R}^{-1}(s) = \{t : (t,s) \in \mathcal{R}\}$ and $\mathcal{R}^{-1}(A) = \cup_{t\in A}\mathcal{R}^{-1}(t)$. If $B \subseteq S$, we say B *$\mathcal{R}$-covers* A if $A \subseteq \mathcal{R}^{-1}(B)$. ∎

Definition 5.3: A *labeling* of a frame $(S, \mathcal{R})$ is a function f that assigns each state in S a non-negative real number. The labeling f is *ϵ-safe* for $\epsilon \geq 0$ if for every subset S' of states such that $\min_{s\in S'} f(s) > \epsilon$ we have

$$\sum_{s\in S'} f(s) > \sum_{(s,s')\in((S'\times S')-\mathcal{R})} f(s)\cdot f(s'). \quad ∎$$

Definition 5.4: A frame $F = (S, \mathcal{R})$ is *ϵ-special (for $\epsilon \geq 0$) with respect to $S_0 \subseteq S$ and labeling* f if

SP1. f is ϵ-safe.

SP2. For all $T \subseteq S - S_0$, if $\sum_{t\in((S-S_0)-T)} f(t) < 1-\epsilon$ then $\mathcal{R}(s) \cap (S - S_0) = T$ for some $s \in S_0$.

SP3. For all $T \subseteq S - S_0$, if $\sum_{t \in T} f(t) \geq 1 + \epsilon$ then T $\mathcal{R}$-covers S_0.

A structure $M = (S, \mathcal{R}, \pi)$ is *ϵ-special for φ with respect to $S_0 \subseteq S$ and f* if (a) φ is satisfiable in M, (b) the underlying frame $(S, \mathcal{R})$ is ϵ-special with respect to S_0 and f, and (c) for all subformulas of φ of the form $\Box\psi$ and all $s \in S$, we have:

SP4. If $(M, s) \models \neg\Box\psi$, then $(M, t) \models \neg\psi$ for some $t \in S - S_0$ such $(s, t) \in \mathcal{R}$.

SP5. If $(M, s) \models \Box\psi$, then $(M, t) \models \psi$ for all $t \in S_0$.

A frame (resp., structure) is *ϵ-special* if it is ϵ-special with respect to some subset S_0 and labeling f. A frame (resp., structure) is *special (with respect to S_0 and f)* if it is 0-special (with respect to S_0 and f). Similarly, we say that a labeling is *safe* if it is 0-safe. ∎

Our interest in special structures is motivated by the following result, from which Theorem 5.1 immediately follows.

Theorem 5.5: *For any modal formula φ,*

(a) if φ is not satisfied in a finite special structure, then $\mu(\varphi) = 0$,

(b) if φ is satisfied in a finite special structure, then $\mu(\varphi) = 1$.

Most of the rest of this section is devoted to proving Theorem 5.5. Before we get into the details of the proof, let us consider more carefully the definition of special structures. Unfortunately, we cannot provide much intuition here; the details of the definition are best motivated by the proofs we are about to present. The set S_0 in a special structure can be thought of as the set where all subformulas of φ of the form $\Box\psi$ are satisfied. As we shall see, S_0 corresponds in a precise sense to a set of size $O(n)$ in almost every frame satisfying φ. Now suppose that there is a finite set of formulas $\neg\Box\psi_1, \ldots, \neg\Box\psi_k$ such that at least one of these formulas is true in every state in S_0. Let B_i be the set of states $S - S_0$ where $\neg\psi_i$ is true, $i = 1, \ldots, k$. It is easy to see (using SP4) that $\cup_{i=1}^{k} B_i$ must cover S_0. Morever, we can show that any set that covers S_0 must have size at least $\log(n) - o(\log(n))$. (We use log to represent logarithm base 2; later we use ln to represent the natural logarithm.) Thus, if $|B_i| = b_i \log(n)$, then $\sum_i b_i \geq 1$. We think of a node with label b according to the safe labeling as corresponding to a set of size $b \log(n)$, a set where a formula of the form $\neg\Box\psi$ which is true at some subset of states in S_0 is satisfied. Under this correspondence, it turns out that properties SP1–SP3 correspond to three properties that hold with probability 1 in almost all frames. We hope that further details of the definition of special structures will become clearer in the course of the proof.

Fix an integer $k > 0$ and $\delta \in (0, 1]$. Consider the following properties of a frame $F = (S, \mathcal{R})$:

F1(k, δ). For all disjoint sets $B_1, \ldots, B_l \subseteq S$ such that $l \leq k$ and $|B_i| \geq \delta \log(n)$, we have

$$\log(n) \sum_{1 \leq i \leq l} |B_i| > \sum_{\mathcal{R}(B_i) \cap B_j = \emptyset} |B_i| \cdot |B_j|.$$

F2(k, δ). For all states $u_1, \ldots, u_{k_1} \in S$ and all nonempty subsets $T_1, \ldots, T_{k_2}, B, C \subseteq S$ such that $k_1, k_2 \leq k$, $T_i \cap B = \emptyset$ for $1 \leq i \leq k_2$, $|B| \leq (1-\delta)\log(n)$, and $|C| \geq n - k\log(n)$, we have

$$|(C \cap \mathcal{R}(u_1) \cap \ldots \cap \mathcal{R}(u_{k_1}) \cap \mathcal{R}^{-1}(T_1) \cap \ldots \cap \mathcal{R}^{-1}(T_{k_2})) - \mathcal{R}^{-1}(B))| \geq k.$$

F3(k, δ). For all $C \subseteq S$ with $|C| \geq (1+\delta)\log(n)$, it is the case that C $\mathcal{R}$-covers S.

Lemma 5.6: *For all $k > 0$ and $\delta \in (0, 1]$,*

$$\lim_{n\to\infty} \mu_n(F \in \mathcal{F}_n : F \textit{ satisfies F1}(k,\delta),\ k = 1,2,3\ ) = 1.$$

Proof: We first consider F1. For each $l < k$ and each set $J \subseteq \{1,\ldots,l\} \times \{1,\ldots,l\}$, let $E_n^1(l, J, \delta)$ be the expected number of ways of choosing $B_1, \ldots, B_l$ such that $|B_i| \geq \delta\log(n)$ for $i = 1, \ldots, l$, $\mathcal{R}(B_i) \cap B_j = \emptyset$ for all $(i,j) \in J$, and

$$\log(n) \sum_{1\leq i\leq l} |B_i| \leq \sum_{(i,j)\in J} |B_i| \cdot |B_j|.$$

It suffices to show that $\lim_{n\to\infty} E_n^1(l, J, \delta) = 0$, for each $l \leq k$ and choice of J. Notice that if $|B_i| = b_i$ for $i = 1, \ldots, l$, then the number of ways of choosing the sets $B_1, \ldots, B_l$ is bounded by $\Pi_{i=1}^l \binom{n}{b_i}$. For each fixed choice of B_i and B_j, the probability that $\mathcal{R}(B_i) \cap B_j = \emptyset$ is $(1/2)^{b_i b_j}$. Let $\mathcal{B}_l = \{(b_1, \ldots, b_l) : \delta\log(n) \leq b_i \leq \log(n),\ i = 1, \ldots, l,\ \log(n)\sum_{i=1}^l b_i \leq \sum_{(i,j)\in J} b_i b_j\}$. Since $\binom{n}{m} \leq n^m/m!$, it is straightforward to check that

$$\begin{aligned}
E_n^1(l,J,\delta) &\leq \sum_{(b_1,\ldots,b_l)\in\mathcal{B}_l} \left(\prod_{1\leq i\leq l} \binom{n}{b_i}\right) \left(\sum_{(i,j)\in J} (\tfrac{1}{2})^{b_i b_j}\right) \\
&\leq \sum_{(b_1,\ldots,b_l)\in\mathcal{B}_l} (n^{b_1+\cdots+b_l}/(b_1)!\cdots(b_l)!) \left(\sum_{(i,j)\in J} (\tfrac{1}{2})^{b_i b_j}\right) \\
&\leq \sum_{(b_1,\ldots,b_l)\in\mathcal{B}_l} 2^{\log(n)\sum_{i=1}^l b_i - \sum_{(i,j)\in J} b_i b_j} / ((\lceil \delta\log(n)\rceil)!)^l \\
&\leq n^l/((\lceil\delta\log(n)\rceil)!)^l.
\end{aligned}$$

It easily follows that $\lim_{n\to\infty} E_n^1(l, J, \delta) = 0$, as desired.

For F2, we first note that if $t \in T$ then $\mathcal{R}^{-1}(t) \subseteq \mathcal{R}^{-1}(T)$, so it suffices to prove the result for singleton T_i's. For $k_1, k_2 \leq k$ let $E_n^2(k_1, k_2, \delta)$ be the expected number of ways of choosing $u_1, \ldots, u_{k_1}$, $t_1, \ldots, t_{k_2}$, and $B, C \subseteq S$ such that $|B| \leq (1-\delta)\log(n)$, $|C| \geq n - k\log(n)$, $t_i \notin B$ for $1 \leq i \leq k_2$, and

$$|(C \cap \mathcal{R}(u_1) \cap \ldots \cap \mathcal{R}(u_{k_1}) \cap \mathcal{R}^{-1}(T_1) \cap \ldots \cap R^{-1}(T_{k_2})) - \mathcal{R}^{-1}(B)| < k.$$

If $|B| = b$ and $|C| = c$, then the number of ways of choosing B, C, $u_1, \ldots u_{k_1}, t_1, \ldots, t_{k_2}$ satisfying these conditions is bounded by

$$\binom{n}{k_1}\binom{n}{k_2}\binom{n}{b}\binom{n}{c} \leq n^{k_1+k_2+b+(n-c)} \leq n^{k_1+k_2+(1-\delta+k)\log(n)}.$$

For fixed B, C, $u_1, \ldots, u_{k_1}, t_1, \ldots, t_{k_2}$, the probability that a given element is the $\mathcal{R}$-successor of each of $u_1, \ldots, u_{k_1}$, is the $\mathcal{R}$-predecessor of $t_1, \ldots, t_{k_2}$, and is not the $\mathcal{R}$-predecessor of any element in B is $(\frac{1}{2})^{k_1+k_2+b}$. Thus, the probability that all but at most k elements in C satisfy this property is

$$(1-(\tfrac{1}{2})^{k_1+k_2+b})^{c-k} \leq (1-(\tfrac{1}{2})^{2k+(1-\delta)\log(n)})^{n-k\log(n)-k}.$$

Recall that $x^y = e^{y\ln(x)}$ and $\ln(1-x) = -x-x^2/2-x^3/3-\cdots$. It follows that $\ln(1-x) < -x$ and, for sufficiently small x, $\ln(1-x) > -3x/2$. This means that an upper bound for the probability above is $e^{-(n-k\log(n)-k)/2^{2k+(1-\delta)\log(n)}}$. For sufficiently large n, we have that $n-k\log(n)-k > n/2$ and this probability is at most $e^{-n^\delta/2^{2k+1}}$. Thus, for sufficiently large n, we get that

$$\begin{aligned} E_n^2(k_1,k_2,\delta) &\leq \sum_{b=0}^{(1-\delta)\log(n)} \sum_{c=n-k\log(n)}^{n} n^{2k+(1-\delta+k)\log(n)} e^{-n^\delta/2^{2k+1}} \\ &\leq (1+(1-\delta)\log(n))(1+k\log(n))n^{2k+(1-\delta+k)\log(n)} e^{-n^\delta/2^{2k+1}}. \end{aligned}$$

Since $\delta > 0$ it follows that $\lim_{n\to\infty} E_n^2(k_1,k_2,\delta) = 0$.

For F3, it is easy to see that if $|C| \geq (1+\delta)\log(n)$, then the probability that C $\mathcal{R}$-covers S is at least $(1-1/n^{(1+\delta)})^n$. By the arguments above, this is at least $e^{-3/2n^\delta}$ for sufficiently large n. Since $\delta > 0$, this value approaches 1 as $n \to \infty$. ∎

Lemma 5.7: *Given $\delta > 0$ and a modal formula φ, let $k = 2^{|\varphi|}$ and let $F \in \mathcal{F}_n$ be a frame satisfying F1(k,δ), F2(k,δ), F3(k,δ), and the formula φ. Then we can construct a structure $M^\varphi = (S^\varphi, \mathcal{R}^\varphi, \pi^\varphi)$ which is δ-special for φ with respect to $S_2 \subseteq S^\varphi$ such that $|S^\varphi| \leq 2^{2^{|\varphi|}+|\varphi|}$ and $|S^\varphi - S_2| \leq 2^{|\varphi|}$.*

Proof: Suppose that F satisfies the hypotheses of the lemma and let $M = (S, \mathcal{R}, \pi)$ be a structure based on F in which φ is satisfiable. Roughly speaking, the idea is that we can partition S into N subsets, where $N \leq 2^{2^{|\varphi|}+|\varphi|}$. All the states in each subset agree on the truth values that they assign to subformulas of φ. Each of these subsets of states will correspond to a node in a special structure $M^\varphi = (S^\varphi, \mathcal{R}^\varphi, \pi^\varphi)$ for φ. We proceed as follows.

We define the *closure* of φ, written $cl(\varphi)$, to be the set of subformulas of φ and their negations. We say that states s and t in S are *equivalent* with respect to $cl(\varphi)$, written $s \equiv_\varphi t$, if, for every formula $\psi \in cl(\varphi)$, we have $(M,s) \models \psi$ iff $(M,t) \models \psi$. We use $[s]$ to denote the equivalence class $\{t : s \equiv_\varphi t\}$. Let S_1 be the set of equivalence classes. Note that $|S_1| \leq 2^{|\varphi|} = k$.

Suppose $|S_1| = k' \leq k$ and let $u_1, \ldots, u_{k'}$ be representatives of each equivalence class. For future reference, we call these the *canonical representatives*. Note that each equivalence class $[s] \in S_1$ contains a unique canonical representative. Define $A = \mathcal{R}(u_1) \cap \ldots \cap \mathcal{R}(u_{k'})$. From F2($k,\delta$) (taking $k_2 = 0$ and $B = \emptyset$), it follows that $A \neq \emptyset$. We partition A as follows: For each nonempty subset $[T]$ of S_1 and equivalence class $[s] \in S_1$, let $A_{[s],[T]}$ denote the set of all states in $[s] \cap A$ whose successors consist of precisely the states in $[T]$; that is

$$A_{[s],[T]} = \{s' : s' \in [s] \cap A \cap [(\cap_{[t]\in[T]}\mathcal{R}^{-1}([t])) - (\cup_{[t]\notin[T]}\mathcal{R}^{-1}([t]))]\}.$$

Define

$$S_2 = \{([s],[T]) : A_{[s],[T]} \neq \emptyset\}.$$

We take $S^\varphi = S_1 \cup S_2$. Clearly $|S^\varphi - S_2| = |S_1| \leq 2^{|\varphi|}$ and $|S_2| \leq 2^{|\varphi|}(2^{2^{|\varphi|}} - 1)$, so $|S^\varphi| \leq 2^{2^{|\varphi|}+|\varphi|}$. Let

$$\mathcal{R}^\varphi = \{([s],[t]) : [s],[t] \in S_1,\ (s,t) \in \mathcal{R}\} \cup \{(([s],[T]),[u]) : [u] \in [T]\}.$$

Finally, we define $\pi^\varphi([s]) = \pi^\varphi([s],[T]) = \pi(s)$. This completes the description of M^φ.

We next show, by induction on the structure of formulas, that if $\psi \in cl(\varphi)$ and $s \in S$, then

$(*)$ $(M,s) \models \psi$ iff $(M^\varphi,[s]) \models \psi$, and

$(**)$ if $([s],[T]) \in S_2$, then $(M,s) \models \psi$ iff $(M^\varphi,([s],[T])) \models \psi$.

The only nontrivial case is if ψ is of the form $\Box\psi'$. Suppose $(M,s) \models \Box\psi'$. Thus, $(M,s') \models \Box\psi'$ for all $s' \in [s]$. Then $(M,t) \models \psi'$ for all t such that $(s',t) \in \mathcal{R}$ for some $s' \in [s]$. By the inductive hypothesis, it follows that $(M^\varphi,[t]) \models \psi'$ for all t such that $(s',t) \in \mathcal{R}$ for some $s' \in [s]$. This means that $(M^\varphi,[t]) \models \psi'$ for all $[t]$ such that $([s],[t]) \in \mathcal{R}^\varphi$ and, if $([s],[T]) \in S_2$, that $(M^\varphi,[t]) \models \psi'$ for all $[t] \in [T]$. Thus, $(M^\varphi,[s]) \models \Box\psi'$ and, if $([s],[T]) \in S_2$, then $(M^\varphi,([s],[T])) \models \Box\psi'$.

Now suppose $(M^\varphi,[s]) \models \Box\psi'$. Thus, $(M^\varphi,[t]) \models \psi'$ for all $[t]$ such that $([s],[t]) \in \mathcal{R}^\varphi$. From the inductive hypothesis and the definition of $\mathcal{R}^\varphi$ it follows that $(M,t) \models \psi'$ for all t such that $(s,t) \in \mathcal{R}$, and hence $(M,s) \models \Box\psi'$.

Finally, suppose that $([s],[T]) \in S_2$ and $(M^\varphi,([s],[T])) \models \Box\psi'$. It follows that $(M^\varphi,[t]) \models \psi'$ for all $[t] \in [T]$. Since $A_{[s],[T]} \neq \emptyset$, there is some state $s' \in [s] \cap A$ such that $(s',t') \in \mathcal{R}$ implies that $[t'] \in [T]$. By the inductive hypothesis, it follows that $(M,t') \models \psi'$ for all t' such that $(s',t') \in \mathcal{R}$. Thus, $(M,s') \models \Box\psi'$. Since $s' \in [s]$, it follows that $(M,s) \models \Box\psi'$.

We can now show that M^φ is a $(k+1)\delta$-special structure for φ with respect to S_2. The fact that φ is satisfiable in M^φ is immediate from $(*)$ and the fact that φ is satisfiable in M. For SP4, suppose that $(M^\varphi,[s]) \models \neg\Box\psi$. By $(*)$, it follows that $(M,s) \models \neg\Box\psi$. Thus, for some t such that $(s,t) \in \mathcal{R}$, we have $(M,t) \models \neg\psi$. By the definition of $\mathcal{R}^\varphi$, it follows that $([s],[t]) \in \mathcal{R}^\varphi$, and by $(*)$ again, we have that $(M^\varphi,[t]) \models \neg\psi$. Now suppose that $(M^\varphi,([s],[T])) \models \neg\Box\psi$. By construction, there is some $s' \in [s] \cap A$ such that $(s',t') \in \mathcal{R}$ implies that $[t'] \in [T]$. Since $[s'] = [s]$, by $(**)$, we have that $(M,s') \models \neg\Box\psi$. Thus, for some t' such that $(s',t') \in \mathcal{R}$, we must have $(M,t') \models \neg\psi$. From $(*)$, we have that $(M^\varphi,[t']) \models \neg\psi$; since $[t'] \in [T]$, the definition of $\mathcal{R}^\varphi$ guarantees that $(([s],[T]),[t']) \in \mathcal{R}^\varphi$. This shows that SP4 holds.

For SP5, suppose that $(M^\varphi,[s]) \models \Box\psi$. Let u be the canonical representative in $[s]$. By construction of A, we know that $(u,t) \in \mathcal{R}$ for all $t \in A$. Thus, $(M,t) \models \psi$ for all $t \in A$. By $(**)$, it follows that for all states $([t],[T]) \in S_2$, we have $(M^\varphi,([t],[T])) \models \psi$. If $(M^\varphi,([s],[T]) \models \Box\psi$, by $(*)$ and $(**)$, it follows that $(M^\varphi,[s]) \models \Box\psi$, and again we get that for all states $([t],[T]) \in S_2$, we have $(M^\varphi,([t],[T])) \models \psi$. This proves SP5.

We now must prove SP1–SP3. Define the function f on S^φ by

$$\begin{cases} f([s]) = |[s]|/\log(n) & \text{if } [s] \in S_1 \\ f(([s],[T])) = 0 & \text{if } ([s],[T]) \in S_2. \end{cases}$$

We claim that f is δ-safe. For suppose $S' \subseteq S^\varphi$ is such that $\min_{t \in S'} f(t) > \delta$. We want to show that $\sum_{t \in S'} f(t) > \sum_{(t,t') \in ((S' \times S') - \mathcal{R}^\varphi)} f(t) \cdot f(t')$. The definition of f guarantees that $S' \subseteq S_1$. Suppose $S' = \{[s_1], \ldots, [s_l]\}$. By construction, $||[s_i]|| \geq \delta \log(n)$ for $i = 1, \ldots, l$. From $\mathrm{F1}(k, \delta)$, it follows that $\log(n) \sum_{i=1}^{l} ||[s_i]|| > \sum_{\mathcal{R}([s_i]) \cap [s_j] = \emptyset} ||[s_i]|| \cdot ||[s_j]||$. Note that $([s_i], [s_j]) \notin \mathcal{R}^\varphi$ iff $\mathcal{R}([s_i]) \cap [s_j] = \emptyset$. Thus, $\log(n) \sum_{i=1}^{l} ||[s_i]|| > \sum_{([s_i],[s_j]) \notin \mathcal{R}^\varphi} ||[s_i]|| \cdot ||[s_j]||$. Dividing both sides of this inequality by $\log(n)^2$ and using the fact that $f([s_i]) = ||[s_i]|| / \log(n)$, we get the desired result. Thus, f is δ-safe, proving SP1.

For SP2, suppose that $[T] \subseteq S_1$ and $\sum_{[s] \in S_1 - [T]} f([s]) < 1 - \delta$. Let $B = \cup_{[s] \in (S_1 - [T])} [s]$. From the definition of f, we have that $|B| < (1 - \delta) \log(n)$. From $\mathrm{F2}(k, \delta)$, it follows that

$$(\mathcal{R}(u_1) \cap \ldots \cap \mathcal{R}(u_{k'}) \cap (\cap_{[t] \in [T]} \mathcal{R}^{-1}([t]))) - \mathcal{R}^{-1}(B) \neq \emptyset,$$

where $u_1, \ldots, u_{k'}$ are the canonical representatives, as chosen above. But this means that for some $s \in A$, we have $A_{[s],[T]} \neq \emptyset$. Thus, $([s], [T]) \in S_3$. By definition, $\mathcal{R}^\varphi(([s], [T]) = [T]$. This proves SP2.

For SP3, suppose that $[T] \subseteq S_1$ and $\sum_{[s] \in [T]} f([s]) \geq 1 + \delta$. Let $C = \cup_{[t] \in [T]} [t]$. From the definition of f we have that $|C| \geq (1 + \delta) \log(n)$. Thus, from $\mathrm{F3}(k, \delta)$, we get that C $\mathcal{R}$-covers S. It easily follows that $[T]$ $\mathcal{R}^\varphi$-covers S_2. This proves SP3.

Thus, we have shown that M^φ is a δ-special structure for φ. ∎

We have just shown that under appropriate assumptions, there exists a δ-special structure for φ. Now we want to strengthen this to get a special (i.e., a 0-special) structure for φ. We first need a technical result about safe labelings.

Given an ϵ-safe labeling f of $(S, \mathcal{R})$ and $T \subseteq S$, define

$$\delta_{f,T} = \sum_{t \in T} f(t) - \sum_{(t,t') \in ((T \times T) - \mathcal{R})} f(t) f(t').$$

Let $\mathcal{T}_f = \{T \subseteq S : \min_{t \in T} f(t) > \epsilon\}$ and let $\delta_f = \min_{T \in \mathcal{T}_f} \delta_{f,T}$. Finally, let $\gamma_f = \max(0, \{f(s) : (s,s) \notin \mathcal{R}\})$. Note that $\gamma_f < 1$, for if $f(s) = 1$ and $(s,s) \notin \mathcal{R}$, then $\{s\}$ provides a counterexample to the fact that f is ϵ-safe.

Lemma 5.8: *If $\epsilon \geq 0$, f is an ϵ-safe labeling of $(S, \mathcal{R})$ and $f' \leq f$ (so that, for all $s \in S$, we have $f'(s) \leq f(s)$), then f' is an ϵ-safe labeling of $(S, \mathcal{R})$. Moreover, for all $T \in \mathcal{T}_{f'}$, we have*

$$\delta_{f',T} \geq \min\left(\delta_f, \frac{(1 - \gamma_f)^2}{8}, \frac{1 - \gamma_f}{2} \sum_{t \in T} f'(t)\right).$$

Proof: Suppose that f is ϵ-safe and $S = \{s_1, \ldots, s_m\}$. For $i = 0, \ldots, m$, define

$$f_i(s_j) = \begin{cases} f'(s_j) & \text{if } j \leq i \\ f(s_j) & \text{if } j > i. \end{cases}$$

Clearly $f_i \leq f$ for $i = 0, \ldots, m$, $f_0 = f$, and $f_m = f'$. We show that the conclusions of the lemma hold for f_i by induction on i. If $i = 0$, the result is immediate, since $f_0 = f$. Suppose the result holds for f_i and $i < m$. We now show that it holds for f_{i+1}. So, suppose that $S' \in \mathcal{T}_{f_{i+1}}$.

We want to show that $\delta_{f_{i+1},S'} \geq \min(\delta_f, \frac{(1-\gamma_f)^2}{8}, \frac{1-\gamma_f}{2}\sum_{s\in S'} f_{i+1}(s))$. If $s_{i+1} \notin S'$, then f_{i+1} and f_i agree on S', so the result follows immediately from the inductive hypothesis. If $s_{i+1} \in S'$, let $T = S' - \{s_{i+1}\}$ and let

$$K = \sum_{(s_{i+1},t)\in((\{s_{i+1}\}\times T)-\mathcal{R})} f_i(t) + \sum_{(t,s_{i+1})\in((S'\times\{s_{i+1}\})-\mathcal{R})} f_i(t).$$

Notice that $\delta_{f_i,S'} = \delta_{f_i,T} + (1-K)f_i(s_{i+1})$. Since f_i and f_{i+1} agree on T, it follows that $\delta_{f_{i+1},S'} \geq \delta_{f_i,T} + (1-K)f_{i+1}(s_{i+1})$. (The reason we write $\geq$ rather than $=$ in this last expression is that if $(s_{i+1}, s_{i+1}) \notin \mathcal{R}$, then $f_i(s_{i+1})$ is one of the terms in K, whereas for equality this term should be $f_{i+1}(s_{i+1})$.) If $K \geq 1$ then, since $f_{i+1}(s_{i+1}) \leq f_i(s_{i+1})$, we get that $\delta_{f_{i+1},S'} \geq \delta_{f_i,S'}$, and the result follows from the induction hypothesis. On the other hand, if $K < 1$, then $\delta_{f_{i+1},S} \geq \delta_{f_i,T}$. If $T \neq \emptyset$, then it is easy to see that $T \in \mathcal{T}_{f_i}$, since $S' \in \mathcal{T}_{f_{i+1}}$. In this case, if $\delta_{f_i,T} \geq \min(\delta_f, \frac{(1-\gamma_f)^2}{8})$, then the result follows immediately from the inductive hypothesis. If not, then by the inductive hypothesis, we have that $\frac{(1-\gamma_f)^2}{8} > \delta_{f_i,T} \geq \frac{1-\gamma_f}{2}\sum_{t\in T} f_i(t)$, so that $\sum_{t\in T} f_i(t) < (1-\gamma_f)/4$. Clearly $K < 2\sum_{t\in T} f_i(t) + x$, where $x = 0$ if $(s_{i+1}, s_{i+1}) \in \mathcal{R}$ and $x = f_i(s_{i+1})$ if $(s_{i+1}, s_{i+1}) \notin \mathcal{R}$. The definition of γ_f guarantees that $x \leq \gamma_f$, so $K < (1-\gamma_f)/2 + \gamma_f$. Thus, $1 - K > \frac{1-\gamma_f}{2}$. It follows that $\delta_{f_{i+1},S'} \geq \frac{1-\gamma_f}{2}\sum_{t\in T} f_i(t) + (1-K)f_{i+1}(s_{i+1}) > \frac{1-\gamma_f}{2}\sum_{s\in S'} f_{i+1}(s)$. This gives us the desired result in this case.

It remains only to check the case that $T = \emptyset$. But in this case, $S' = \{s_{i+1}\}$. If $(s_{i+1}, s_{i+1}) \in \mathcal{R}$, then $\delta_{f_{i+1},S'} = f_{i+1}(s_{i+1})$. If $(s_{i+1}, s_{i+1}) \notin \mathcal{R}$, then $f_{i+1}(s_{i+1}) \leq \gamma_f$, so $\delta_{f_{i+1},S'} = f_{i+1}(s_{i+1}) - (f_{i+1}(s_{i+1}))^2 \geq (1-\gamma_f)f_{i+1}(s_{i+1})$. ∎

Lemma 5.9: *If F is ϵ-special with respect to S_0 and f, then F is also ϵ-special with respect to S and f', where $f'(s) = \min(f(s), 1)$ for $s \in S - S_0$ and $f'(s) = 0$ for $s \in S_0$.*

Proof: It follows immediately from Lemma 5.8 that f' is safe. We leave to the reader the easy verification that properties SP2 and SP3 still hold using f'. ∎

Part (a) of Theorem 5.5 now follows immediately from the following result.

Proposition 5.10: *If $\mu(\varphi) \neq 0$, then there is a special structure $M = (S, \mathcal{R})$ for φ with respect to a set $S_0 \subseteq S$ such $|S| \leq 2^{2^{|\varphi|}+|\varphi|}$ and $|S - S_0| \leq 2^{|\varphi|}$.*

Proof: Suppose $\mu(\varphi) \neq 0$. Then there exist infinitely many n such that

$$\mu_n(\{F \in \mathcal{F}_n : \text{ some structure based on } F \text{ satisfies } \varphi\})$$

is strictly greater than 0. From Lemma 5.6 and the hypotheses of the proposition, it follows that there exists an increasing sequence $n_1, n_2, \ldots$ such that for all m, there exists a frame with n_m states such that the hypotheses of Lemma 5.7 hold with $\delta = 1/m$. Thus, corresponding to each n_m there exists a $(1/m)$-special structure $M_m = (S_m, \mathcal{R}_m, \pi_m)$ for φ with respect to a subset $S'_m \subseteq S_m$ and a safe labeling f_m such that $|S_m| \leq 2^{2^{|\varphi|}+|\varphi|}$ and $|S'_m - S_m| \leq 2^{|\varphi|}$. Since there are only finitely many structures satisfying φ with at most $2^{2^{|\varphi|}+|\varphi|}$ states, there must exist one structure $M = (S, \mathcal{R}, \pi)$ and a subset $S_0 \subseteq S$ such that $M = M_m$ and $S_0 = S'_m$ for infinitely many m. Thus, M is a $(1/m)$-special structure for φ with respect to S_0 and f_m for all m. We want to show that M is in fact special.

By Lemma 5.9, we can assume without loss of generality that $f_m(s) \leq 1$ for all $s \in S$. Suppose that $S = \{s_1, \ldots, s_N\}$. The sequence of tuples $(f_0(s_1), \ldots, f_0(s_N)), (f_1(s_1), \ldots, f_1(s_N)), \ldots$ is a sequence in the compact space $[0,1]^N$. Thus, the sequence has an accumulation point $(a_1, \ldots, a_N)$; i.e., a subsequence of this sequence converges to $(a_1, \ldots, a_N)$. Now consider the labeling defined by $f(s_i) = a_i$. Straightforward continuity arguments show that M is a special structure of φ with respect to f. We leave details to the reader. ∎

In order to prove Part (b) of Theorem 5.5, we show that a special structure can be embedded in almost every frame in such a way as to preserve satisfiability.

Suppose that $F = (S, \mathcal{R})$ and $F' = (S', \mathcal{R}')$ are two frames such that $|S| \leq |S'|$, and suppose $S_0 \subseteq S$. We say that F is S_0-*embeddable in* F' if there is an onto mapping $\gamma : S' \rightarrow S$ such that

P1. if $(s,t) \in \mathcal{R}$ and $t \notin S_0$, then $\gamma^{-1}(t)$ $\mathcal{R}$-covers $\gamma^{-1}(s)$

P2. if $(s,t) \notin \mathcal{R}$ and $t \notin S_0$, then $\mathcal{R}'(\gamma^{-1}(s)) \cap \gamma^{-1}(t) = \emptyset$.

Lemma 5.11: *If $F = (S, \mathcal{R})$, $S_0 \subseteq S$, M is a special structure for φ with respect to S_0 based on F, and F is S_0-embeddable in F', then φ is satisfied in F'.*

Proof: Suppose the hypotheses of the theorem hold and $\mathcal{F}' = (S', \mathcal{R}')$. Let $M' = (S', \mathcal{R}', \pi')$, where $\pi'(s')(p) = \pi(\gamma(s'))(p)$. We show, by induction on the structure of ψ, that $(M', s') \models \psi$ iff $(M, \gamma(s')) \models \psi$, for all subformulas ψ of φ. The case where ψ is a primitive proposition, conjunction, or negation are straightforward and left to the reader. We consider the case that ψ is of the form $\Box\psi'$. Suppose $(M', s') \models \Box\psi'$. If $(M, \gamma(s')) \not\models \Box\psi'$, then by SP4, there is some state $t' \in S - S_0$ such that $(\gamma(s'), t) \in \mathcal{R}$ and $(M, t) \not\models \psi$. By P1 there is some $t' \in \gamma^{-1}(t)$ such that $(s', t') \in \mathcal{R}'$. It follows by the induction hypothesis that $(M', t') \not\models \psi'$, which is a contradiction. Thus, $(M, \gamma(s)) \models \Box\psi'$, as desired. For the converse, suppose $(M, \gamma(s')) \models \Box\psi'$ and $(s', t') \in \mathcal{R}'$. If $\gamma(t') \in S_0$, then $(M, \gamma(t')) \models \psi'$ by SP5. Thus, by the induction hypothesis, $(M', t') \models \psi'$. If $\gamma(t') \notin S_0$, then from P2 it follows that $(\gamma(s'), \gamma(t')) \in \mathcal{R}$. Thus, we must have that $(M, \gamma(t')) \models \psi$ and by the induction hypothesis, $(M', t') \models \psi$. It now follows that $(M, s') \models \Box\psi$, as desired. ∎

Part (b) of Theorem 5.5 now follows immediately from the following result.

Proposition 5.12: *If F is a finite special frame with respect to S_0, then*

$$\lim_{n\to\infty} \mu_n(F' \in \mathcal{F}_n : F \textit{ is } S_0\textit{-embeddable in } F') = 1.$$

Proof: Suppose $F = (S, \mathcal{R})$ is special with respect to $S_0 \subseteq S$ and the labeling f. By Lemma 5.9, without loss of generality, we can assume that $f(s) \leq 1$ for all $s \in S$. Let $S_1 = S - S_0$. Our first step is to show that for almost all frames $F' = (S', \mathcal{R}')$ we can find an onto function $\gamma : S' \rightarrow S$ such that

P1′. if $(s,t) \in ((S_1 \times S_1) \cap \mathcal{R})$, then $\gamma^{-1}(t)$ $\mathcal{R}$-covers $\gamma^{-1}(s)$

P2$'$. if $(s,t) \in ((S_1 \times S_1) - \mathcal{R})$, then $\mathcal{R}'(\gamma^{-1}(s)) \cap \gamma^{-1}(t) = \emptyset$

P3. if $s \in S_1$ and $f(s) > 0$, then $|\gamma^{-1}(s)| = \lfloor f(s)\log(n) \rfloor$

P4. if $f(s) = 0$ then $|\gamma^{-1}(s)| = 1$

P5. if $T \subseteq S_1$ and $\sum_{t \in T} f(t) \geq 1$, then $\gamma^{-1}(T)$ $\mathcal{R}'$-covers $\gamma^{-1}(S_0)$.

Notice that P1$'$ and P2$'$ are weaker variants of P1 and P2, respectively, where we only focus on pairs (s,t) in $S_1 \times S_1$.

To prove this we use the *second moment method*, a standard technique in random graph theory [Bol85]. Let X be a random variable on $\mathcal{F}$ such that $X(F')$ is the number of mappings γ from F' to F satisfying P1$'$, P2$'$, P3, P4, and P5. We want to show

($\dagger$) $\lim_{n\to\infty} \mu_n(\{F' \in \mathcal{F}_n : X(F') > 0\}) = 1$.

Let $E_n(X)$ be the expected value of $X(F')$ in $\mathcal{F}_n$. According to the second moment method, to prove ($\dagger$), it suffices to show that $\lim_{n\to\infty} E_n(X) = \infty$ and $\lim_{n\to\infty} E_n(X^2)/E_n(X)^2 = 1$.

To compute $E_n(X)$, we must count the number of ways of choosing the sets $\gamma^{-1}(s)$ for $s \in S_1$ satisfying the constraints P3 and P4, and for each such way, compute the probability that it satisfies P1$'$, P2$'$, and P5. Suppose $S_1 = \{s_1, \ldots, s_m\}$. Let $K = \{k : f(s_k) > 0\}$ and let $J = \{(i,j) \in K \times K : (s_i, s_j) \notin \mathcal{R}\}$. It turns out to be convenient to split many of our calculations into two parts, one for the case of elements in K and one for the $m - |K|$ elements not in K. Let $d_i = |\gamma^{-1}(s_i)|$ and let $d = \sum_{i=1}^m d_i$. Notice that if $i \in K$, then $d_i = \lfloor f(s_i)\log(n) \rfloor$.

Clearly, a lower bound on the number of ways of choosing γ so that it satisfies P3 and P4 in a structure of size n is $(n-d)^d/d!$, since this is a lower bound on $\binom{n}{d}$, the number of ways of choosing the d elements in $\gamma^{-1}(S_1)$.

Suppose γ satisfies P3 and P4; we want to compute the probability that it satisfies P1$'$, P2$'$, and P5. Let p_n be the probability that γ satisfies P1$'$, P2$'$, and P5. The properties are easily seen to be independent, so $p_n = p_n^1 p_n^2 p_n^5$, where p_n^1 (resp., p_n^2, p_n^5) is the probability that γ satisfies P1$'$ (resp., P2$'$, P5).

We start with P5. Let $T_1, \ldots T_k$ be all the subsets of S_1 such that $\sum_{s \in T_j} f(s) \geq 1$. The probability that $\gamma^{-1}(T_j)$ $\mathcal{R}'$-covers $\gamma^{-1}(S_0)$ is $(1 - (\frac{1}{2})^{|\gamma^{-1}(T_j)|})^{|\gamma^{-1}(S_0)|}$. Since $|\gamma^{-1}(S_0)| \leq n$ and (by P3) $|\gamma^{-1}(T_j)| \geq \log(n) - m$, this probability is at least $(1 - 2^m/n)^n$. Now using arguments similar to those of Lemma 5.6, we can see that this probability is $e^{n\ln(1-2^m/n)} > 2^{-2^{m+1}}$ for n sufficiently large. Since there are at most 2^m subsets T_j to consider, we have that $p_n^5 \geq (1/2)^{2^{2m+1}}$ for sufficiently large n.

We next consider P1$'$. If $(s_i, s_j) \in \mathcal{R}$, then we want $\gamma^{-1}(s_j)$ to cover $\gamma^{-1}(s_i)$. The probability of that is easily seen to be $(1 - (1/2)^{d_j})^{d_i}$. If $s_j \notin K$, then $d_j = 1$, and this probability is $(1/2)^{d_i}$. If $s_j \in K$ then $\lim_{n\to\infty}(1 - (1/2)^{d_j})^{d_i} = \lim_{n\to\infty}(e^{-d_i/2^{d_j}}) = 1$ (since d_j is $O(\log(n))$). Thus, $(1 - (1/2)^{d_j})^{d_i} \geq 1/2$ for sufficiently large n. It follows that $p_n^1 \geq (1/2)^{(m-|K|)d + m|K|}$ for sufficiently large n.

Finally, for P2$'$, suppose that $(s_i, s_j) \notin \mathcal{R}$. We want to compute the probability that $\mathcal{R}(\gamma^{-1}(s_i)) \cap \gamma^{-1}(s_j) = \emptyset$. It is easy to see that this probability $(1/2)^{d_i d_j}$. It follows that

$p_n^2 = (1/2)^{\sum_{\{(i,j):(s_i,s_j)\notin\mathcal{R}\}} d_i d_j}$. Since $d_i = 1$ if $i \notin K$, we have

$$\begin{aligned}\sum_{\{(i,j):(s_i,s_j)\notin\mathcal{R}\}} d_i d_j &\leq \sum_{\{(i,j):i\notin K\}} d_i d_j + \sum_{\{(i,j):j\notin K\}} d_i d_j + \sum_{\{(i,j)\in J\}} d_i d_j \\ &\leq 2(m-|K|)d + \sum_{\{(i,j)\in J\}} d_i d_j.\end{aligned}$$

Thus, $p_n^2 \geq (1/2)^{2(m-|K|)d+\sum_{(i,j)\in J} d_i d_j}$.

Putting all this together, it follows that

$$E_n(X) \geq ((n-d)^d/d!)(1/2)^{2^{2m+1}+3(m-|K|)d+m|K|+\sum_{(i,j)\in J} d_i d_j}$$

for sufficiently large n.

There are now two cases to consider. If $|K| = 0$, then $|J| = 0$ and $d = m$. In this case, we get that $E_n(X) \geq ((n-m)^m/m!)(1/2)^{2^{2m+1}+3m^2}$. Since m is a constant, we clearly have $\lim_{n\to\infty} E_n(X) = \infty$.

Now suppose $|K| > 0$. Since d is $O(\log(n))$, for sufficiently large n, we have $n - d > n/2$. Thus, for sufficiently large n,

$$E_n(X) \geq (n^d/d!)(1/2)^{d+2^{2m+1}+3(m-|K|)d+m|K|+\sum_{(i,j)\in J} d_i d_j}.$$

Since $d_i = \lfloor f(s_i)\log(n)\rfloor$ for $i \in J$, we get that $d \geq (\log(n)\sum_{i\in K} f(s_i)) - m$. Thus, using the notation $\delta_{f,K}$ introduced just prior to the statement of Lemma 5.8, we have

$$\begin{aligned}E_n(X) &\geq 2^{\log(n)d-(d+2^{2m+1}+3(m-|K|)d+m|K|+\sum_{(i,j)\in J} d_i d_j)}/d! \\ &\geq 2^{\log(n)^2\left(\sum_{i\in K} f(s_i)-\sum_{(i,j)\in J} f(s_i)f(s_j)\right)-(m\log(n)+d+2^{2m+1}+3d(m-|K|)+m|K|)}/d! \\ &= 2^{\delta_{f,K}\log(n)^2-(m\log(n)+d+2^{2m+1}+3d(m-|K|)+m|K|)}/d!\end{aligned}$$

Since F is special, f is 0-safe, and hence $\delta_{f,K} > 0$. Since d is $O(\log(n))$, it is easy to see that $\lim_{n\to\infty} E_n(X) = \infty$, as desired.

We now show that that $E_n(X^2)/E_n(X)^2 - 1 \to 0$. It is easy to see that $X^2(F')$ is just the number of ordered pairs of mappings (γ,γ') from F' to F such that both γ and γ' satisfy P1$'$, P2$'$, P3–P5. Let $Y_{d'}(F')$ be the number of such ordered pairs (γ,γ') satisfying these properties such that $|\gamma^{-1}(S_1)\cap\gamma'^{-1}(S_1)| = d'$; in this case we say that γ and γ' have *overlap* d'. Clearly $X^2(F') = \sum_{d'=0}^{d} Y_{d'}(F')$. Arguments along the same lines as those used to compute $E_n(X)$ show that $E_n(Y_0) \sim E_n(X)^2$, where, for two functions $F(n)$ and $G(n)$, we write $F(n) \sim G(n)$ if $\lim_{n\to\infty} F(n)/G(n) = 1$. We leave details to the reader. Thus, it remains to show that $\lim_{n\to\infty}\sum_{d'=1}^{d}(E_n(Y_{d'})/E_n(Y_0)) = 0$. Since d is $O(\log(n))$, it suffices to show that if $1 \leq d' \leq d$, we have $\lim_{n\to\infty} E_n(Y_{d'})\log(n)/E_n(Y_0) = 0$.

To compute $E_n(Y_{d'})$, we must again count the number of ways of choosing pairs (γ,γ') satisfying the constraints P3 and P4 and having overlap d', and for each such way, compute the probability that it satisfies P1$'$, P2$'$, and P5. Since we actually want to compare $E_n(Y_{d'})$ to $E_n(Y_0)$, it is more useful to compute the ratio R_n of the number of ways of choosing pairs (γ,γ') satisfying P3 and P4 having overlap d' to the number of ways of choosing such pairs with overlap 0 in a frame of size n, and the ratio q_n of the probability that a given pair (γ,γ')

with overlap d' satisfies P1$'$, P2$'$, and P5, to the probability that a pair with overlap 0 satisfies these properties. It is easy to see that $E_n(Y_{d'})/E_n(Y_0) = R_n q_n$.

There are clearly more ways of choosing pairs with no overlap then there are of choosing pairs with overlap d'; straightforward counting arguments of the type used above show that $R_n \leq d^{2d'}/(n-2d)^{d'}$. To see this, let $d'_i = |\gamma_1^{-1}(s_i) \cap \gamma_2^{-1}(s_i)|$, for $1 \leq i \leq m$. Then $R_n = A_n/B_n$, where

$$A_n = \frac{n!}{\prod_{i=1}^m d'_i! \prod_{i=1}^m (d_i - d'_i)!^2 (n - 2d + d')!}$$

and

$$B_n = \frac{n!}{\prod_{i=1}^m d_i!^2 (n - 2d)!}.$$

The bound given from R_n then follows from simple manipulations, using the fact that $d_i \leq d$, $1 \leq i \leq m$.

While there are fewer ways of choosing pairs with overlap d than with overlap 0, the probability of such a pair satisfying P1$'$, P2$'$, and P5 is higher. We need to compute by how much. Again, since the properties are independent, we have $q_n = q_n^1 q_n^2 q_n^5$, where q_n^1 (resp., q_n^2, q_n^5) is the ratio of the probabilities that these pairs satisfy P1$'$ (resp., P2$'$, P5$'$).

Suppose that (γ_1, γ_2) is a pair with overlap d' satisfying P3 and P4, and (γ_3, γ_4) is a pair with overlap 0 satisfying P3 and P4. We start by computing the possible increase in P5. We saw above that the probability that P5 holds for a particular choice of γ is at least $1/2^{2^{2m+2}}$. Thus, the probability that P5 holds for the pair (γ_3, γ_4) is at least $1/2^{2^{2m+2}}$. The probability that it holds for the pair (γ_1, γ_2) is clearly at most 1. Thus, q_n^5 is at most $2^{2^{2m+2}}$. We now consider P1$'$. Given a pair $(s_i, s_j) \in \mathcal{R}'$, then P1$'$ requires that $\gamma_h^{-1}(s_j)$ $\mathcal{R}'$-covers $\gamma_h^{-1}(s_i)$, for $h = 1, \ldots, 4$. We want to compute the ratio of the probability that this holds for the pair (γ_1, γ_2) to the probability that this holds for the pair (γ_3, γ_4). It is clear that this ratio is maximized if $\gamma_1^{-1}(s_j) = \gamma_2^{-1}(s_j)$. Since, by assumption, $\gamma_3^{-1}(s_i)$, $\gamma_4^{-1}(s_i)$, $\gamma_3^{-1}(s_j)$, and $\gamma_4^{-1}(s_j)$ are all disjoint, it is easy to check that the ratio at most $1/(1-(1/2)^{d_j})^{d'_i}$. If $s_j \notin K$, then the ratio is at most $2^{d'_i}$, while if $s_j \in K$, then similar arguments to those used above show that the ratio is at most 2, for sufficiently large n. It follows that $q_n^1 \leq 2^{(m-|K|)d'+|K|}$ for n sufficiently large.

Finally, we consider P2$'$. Suppse that $(s_i, s_j) \notin \mathcal{R}$. Then P2$'$ requires that $\mathcal{R}'(\gamma_h^{-1}(s_i))$ and $\gamma_h^{-1}(s_j)$ are disjoint, for $h = 1, \ldots, 4$. We want to compute the ratio of the probability that this holds for the pair (γ_1, γ_2) to the probability that this holds for the pair (γ_3, γ_4). Straightforward calculations show that the ratio is exactly $2^{d'_i d'_j}$. Thus, $q_n^2 = 2^{\sum_{\{(i,j):(s_i,s_j)\notin\mathcal{R}\}} d'_i d'_j}$. Using arguments similar to those used in calculating p_n^2, we can show that $q_n^2 \leq 2^{2(m-|K|)d' + \sum_{(i,j)\in J} d'_i d'_j}$.

Putting this together, we see that for n sufficiently large,

$$E_n(Y_d)/E_n(Y_0) = R_n q_n^1 q_n^2 q_n^5 \leq (d^{2d'}/(n-2d)^{d'}) 2^{3(m-|K|)d'+|K|+2^{2m+2}+\sum_{(i,j)\in J} d'_i d'_j}.$$

Since $n - 2d \geq n/2$ for sufficiently large n, we get that for n sufficiently large,

$$E_n(Y_d)/E_n(Y_0) \leq 2^{3(m-|K|)d'+d'+|K|+2^{2m+2}+\sum_{(i,j)\in J} d'_i d'_j} d^{2d'}/n^{d'}.$$

Again, we first consider the case where $|K| = 0$. In this case, since $J = \emptyset$ and $d', d \leq m$, we get that $E_n(Y_{d'})/E_n(Y_0) \leq 2^{3m^2+m+2^{2m+2}} m^{2m}/n^{d'}$ for sufficiently large n. It follows that $\lim_{n\to\infty} E_n(Y_{d'}) \log(n)/E_n(Y_0) = 0$ in this case.

Now consider the case that $|K| > 0$. Let f' be the labeling such that $f'(s_i) = d'_i/\log(n)$ if $i \in K$ and $f'(s_i) = 0$ if $i \notin K$. Since $d'_i \leq |\gamma_1^{-1}(s_i)| = \lfloor f(s_i)\log(n)\rfloor$ if $i \in K$, it immediately follows that $f' \leq f$. Thus, by Lemma 5.8, f' is a safe mapping. Moreover, if we set $d'' = \sum_{i \notin K} d'_i$, then

$$\delta_{f',K} \geq \min\left(\delta_f, \frac{(1-\gamma_f)^2}{8}, \frac{(1-\gamma_f)(d'-d'')}{2\log(n)}\right).$$

Straightforward manipulations show that, for n sufficiently large,

$$\begin{aligned}
& E_n(Y_{d'})/E_n(Y_0) \\
\leq\ & 2^{3(m-|K|)d'+d'+|K|+2^{2m+2}+\sum_{(i,j)\in J} d'_i d'_j} d^{2d'} / n^{d''+(\sum_{i\in K} d'_i)} \\
=\ & 2^{3(m-|K|)d'+d'+|K|+2^{2m+2}+2d'\log(d)-d''\log(n)-\log(n)\sum_{i\in K} d'_i+\sum_{(i,j)\in J} d'_i d'_j} \\
=\ & 2^{3(m-|K|)d'+d'+|K|+2^{2m+2}+2d'\log(d)-d''\log(n)-\log(n)^2\left(\sum_{i\in K} f'(s_i)-\sum_{(i,j)\in J} f'(s_i)f'(s_j)\right)} \\
=\ & 2^{3(m-|K|)d'+d'+|K|+2^{2m+2}+2d'\log(d)-d''\log(n)-\log(n)^2\delta_{f',K}}.
\end{aligned}$$

Since d' is $O(\log(n))$, it easily follows from the lower bound on $\delta_{f',K}$ that

$$\lim_{n\to\infty} E_n(Y_d)\log(n)^2/E_n(Y_0) = 0,$$

as desired. Thus, by the second moment method, we can conclude that, with probability approaching 1, we can find a mapping γ satisfying P1$'$, P2$'$, P3, P4, and P5.

We are now almost done. Choose ϵ so that for all $T \subseteq S_1$, if $\sum_{t\in T} f(t) < 1$, then in fact $\sum_{t\in T} f(t) < 1-\epsilon$. Let $N = |S_0|2^{|S_1|}$. By Lemma 5.6, the asymptotic probability that a frame satisfies F2(N,ϵ) is 1. Consider a frame $F' = (S', \mathcal{R}')$ satisfying F2(N,ϵ) such that there is a mapping $\gamma : F' \to F$ satisfying P1$'$, P2$'$, P3, P4, and P5. Let $S'_0 = \gamma^{-1}(S_0)$ and let $S'_1 = \gamma^{-1}(S_1)$. Notice that $S'_0 = S' = S'_1$. We now show that, in fact, by possibly redefining γ on S'_0, we can get a map $\gamma' : F' \to F$ satisfying P1 and P2. This shows that F is embeddable in F'.

For each $T \subseteq S_1$, let S_T consist of all the states in S_0 with $\mathcal{R}$-successors in T and no $\mathcal{R}$ successors in $S_1 - T$; similarly, let S'_T consist of all the states in S'_0 with $\mathcal{R}'$-successors in $\gamma^{-1}(t)$ for $t \in T$ and no $\mathcal{R}'$ successors in $\gamma^{-1}(t)$ for $t \in S_1 - T$. That is,

$$S_T = (S_0 \cap (\cap_{t\in T}\mathcal{R}^{-1}(t))) - \cup_{t\in S_1-T}\mathcal{R}^{-1}(t)$$

and

$$S'_T = (S'_0 \cap (\cap_{t\in T}\mathcal{R}'^{-1}(\gamma^{-1}(t)))) - \cup_{t\in S_1-T}\mathcal{R}'^{-1}(\gamma^{-1}(t)).$$

If $\sum_{t\in S_1-T} f(t) < 1$, then by SP2, $S_T \neq \emptyset$, and by F2(N,ϵ) and the choice of N, we have $|S'_T| \geq N \geq |S_0|$. If $\sum_{t\in S_1-T} f(t) \geq 1$, then by SP3, $S_T = \emptyset$, and by P5, $S'_T = \emptyset$.

It is straightforward to redefine γ on S'_0 to get an onto map $\gamma' : F' \to F$ that agrees with γ on S'_1 such that $\gamma'^{-1}(S_T) = S'_T$. We now show that γ' satisfies P1 and P2. We start with P1. If $(s,t) \in \mathcal{R}$ and both $s, t \in S_1$, since γ' agrees with γ on S'_1, it follows from P1$'$ that $\gamma'^{-1}(t)$ covers $\gamma'^{-1}(s)$. Suppose that $s \in S_0$. Then $s \in S_T$ for some $T \subseteq S_1$ such that $t \in T$. By construction, $\gamma'^{-1}(s) \in S'_T$ and $\gamma'^{-1}(t)$ covers $\gamma'^{-1}(s)$. This shows that P1 holds.

For P2, suppose that $(s,t) \notin \mathcal{R}$. If both $s,t \in S_1$, then it follows from P2$'$ that $\mathcal{R}(\gamma'^{-1}(s)) \cap \mathcal{R}(\gamma'^{-1}(t)) = \emptyset$. If $s \in S_0$, then $s \in S_T$ for some $T \subseteq S_1$ such that $t \notin T$. By construction, $\gamma'^{-1}(s) \in S'_T$, and so $\mathcal{R}'(\gamma'^{-1}(s)) \cap \gamma'^{-1}(t) = \emptyset$. This shows that P2 holds.

Thus, we can embed F into a frame that satisfies F2(N,ϵ) for which there is a mapping γ satisfying P1$'$, P2$'$, P3, P4, and P5. Since these are both properties that hold with asymptotic probability 1, it follows that $\lim_{n\to\infty} \mu_n(\{F' \in \mathcal{F}_n : F \text{ is } S_0\text{-embeddable in } F'\}) = 1$. ∎

We have now completed the proof of Theorem 5.5. The theorem and its proof gives us a great deal of information, which we can now exploit. For one thing, we get an analogue of Theorem 4.8 for frames:

Theorem 5.13: *Given Φ, there is an infinite frame F_∞ such that for all formulas $\varphi \in \mathcal{L}(\Phi)$, $\mu(\varphi) = 1$ iff φ is valid in F_∞.*

Proof: Just take F_∞ to be the disjoint union of all special frames. Note that F_∞ is infinite, even if Φ is finite. ∎

Turning our attention to complexity, we can show

Theorem 5.14: *For both the dag and the tree representations and for both finite and infinite sets of propositions Φ, deciding almost-sure frame-validity of formulas in $\mathcal{L}(\Phi)$ is in double-exponential space and is exponential-time hard.*

Proof: The lower bound follows much the same lines as the exponential time lower bound of Fischer and Ladner [FL79] for one-letter PDL. In their proof, Fischer and Ladner show how, given a polynomial-space alternating Turing machine $\mathbf{A}$ and an input x, there is a formula $\varphi_{\mathbf{A},x}$ in one-letter PDL such that $\varphi_{\mathbf{A},x}$ is satisfiable iff $\mathbf{A}$ accepts x. The Fischer-Ladner argument requires Φ to be infinite, since they use the primitive propositions to represent the states of $\mathbf{A}$ and there is no bound on the number of states. We return to this point below. We can replace all occurrences of $[a]$ in their formula with $\Box$, all occurrences of $\langle a \rangle$ by $\Diamond$, and all occurrences of $[a^*]$ by $\Box\Box$, giving us a modal formula $\varphi'_{\mathbf{A},x}$. Let $\mathcal{R}^2$ be the result of composing $\mathcal{R}$ with itself, so $\mathcal{R}^2 = \{(s,t) : \exists u((s,u) \in \mathcal{R}, (u,t) \in \mathcal{R}\}$. A straightforward argument shows that $\mu(\{F = (S,\mathcal{R}) : \mathcal{R}^2 \text{ is the universal relation on } S\}) = 1$; with asymptotic probability 1, all states are connected by a path of length two. It follows that, with asymptotic probability 1, if $\Box\Box\varphi$ is true at some state, then φ is true at all states. Thus $\Box\Box$ essentially acts like a^* in PDL. A straightforward argument now shows that $\varphi_{\mathbf{A},x}$ is satisfiable iff $\varphi'_{\mathbf{A},x}$ is satisfiable in a special structure iff $\varphi'_{\mathbf{A},x}$ is satisfiable in almost all frames. Thus, deciding if a formula is satisfiable (or valid) in almost all frames is exponential-time hard provided Φ is infinite. It is not hard to show that we can find an unbounded collection of independent formulas using only primitive proposition (and unbounded nesting of $\Box$ and $\Diamond$), and use thus prove the same result even for finite Φ. We leave details to the reader.

For the upper bound, the problem reduces to deciding whether there is a special structure for φ. We know that if there is one at all, then there is a special structure $M = (S,\mathcal{R},\pi)$ for φ with respect to S_0 such that $|S| \le 2^{2^{|\varphi|}+|\varphi|}$ and $|S - S_0| \le 2^{|\varphi|}$. For each structure $M = (S,\mathcal{R},\pi)$ and subset $S_0 \subseteq S$ satisfying these constraints, we can easily check (in double-exponential time) if φ is satisfiable in M and properties SP4 and SP5 hold. We now need to check properties SP1–SP3. This amounts to checking whether there is a safe labeling satisfying SP2 and SP3. Without loss of generality (using Lemma 5.9), we can assume that the safe labeling assigns value 0 to all the states in S_0. Thus, all that matters is the value assigned to the (at most exponential number of) states in $S - S_0$. We can find a formula in the language of arithmetic (i.e., over $+, \times, 0, 1$) whose length is at most double-exponential in $|\varphi|$ that is valid in the theory of real closed fields iff such a safe mapping exists: If $S - S_0 = \{s_1, \ldots, s_N\}$ (where $N \leq 2^{|\varphi|}$), then we simply say there exist numbers $x_1, \ldots, x_N$ such that the appropriate properties hold, where the "appropriate properties" can easily be expressed by a double-exponential length quantifier-free formula in $x_1, \ldots, x_N$ (that depends on the $\mathcal{R}$ relation in M). Since this formula has only existential quantifiers, by a result of Canny [Can88], we can check whether it is true in double-exponential space. Thus, in double-exponential space, we can check whether a special structure for φ exists. ∎

Just as for structure validity, we can also ask whether a 0-1 law holds for frame validity if we consider frames in $\mathcal{F}^r$, $\mathcal{F}^{rt}$, or $\mathcal{F}^{rst}$. The answer in all cases is yes. Define a *depth-2* frame to be one whose longest paths have length at most 2. Thus, $F = (S, \mathcal{R})$ is a depth-2 frame if there do not exist states s_0, s_1, s_2, s_3 such that $s_i \neq s_{i+1}$ for $i \in \{0, 1, 2\}$ and $(s_0, s_1), (s_1, s_2), (s_2, s_3) \in \mathcal{R}$. Notice that Theorems 4.13 and 4.14 guarantee that almost all frames where $\mathcal{R}$ is reflexive and transitive are actually depth-2 frames.

Theorem 5.15: *For every modal formula φ*

(a) $\mu^r(\varphi) = 1$ if φ if there is a special modal structure $M = (S, \mathcal{R}, \pi)$ for φ such that $\mathcal{R}$ is reflexive; otherwise $\mu^r(\varphi) = 0$.

(b) $\mu^{rt}(\varphi) = 1$ if φ is valid in all reflexive, transitive depth-2 frames; otherwise $\mu^{rt}(\varphi) = 0$.

(c) $\mu^{rst}(\varphi) = 1$ if φ is S5-valid; otherwise $\mu^{rst}(\varphi) = 0$.

Proof: The proof for part (a) follows similar lines to that of the proof of Theorem 5.5; we omit details here.

For part (b), since from Theorems 4.13 and 4.14 it follows that almost all frames where $\mathcal{R}$ is reflexive and transitive are actually reflexive, transitive, depth-2 frames, we have that if φ is valid in all reflexive, transitive, depth-2 frames, then $\mu^{rt}(\varphi) = 1$. If φ is not valid in all reflexive, transitive, depth-2 frames, then there must be some structure $M = (S, \mathcal{R}, \pi)$ such that $(S, \mathcal{R})$ is a depth-2 frame and $M, s_0 \models \neg\varphi$ for some $s_0 \in S$. It is easy to see that we can find a set S' of states in S including s_0 such that each state in S' has less than $|\varphi|$ immediate successors and for all subformulas ψ of φ and all $s \in S'$, we have $(M', s) \models \psi$ iff $(M, s) \models \psi$, where $M' = (S', \mathcal{R}', \pi')$, and $\mathcal{R}'$ and π' are the restrictions of $\mathcal{R}$ and π, respectively, to S'. Intuitively, each state $s \in S'$ has enough $\mathcal{R}'$-successors to ensure that all subformulas of the form $\Diamond\psi$ that are satisfied at state s in M are also satisfied at state s in M'. In particular, note that $(M', s_0) \models \varphi$. Note for future reference that $|S'| \leq |\varphi|^2$. Now suppose that $F = (S'', \mathcal{R}'')$ is a depth-2 frame in $\mathcal{F}_n^{rt}$ such that each non-leaf state in S'' has at least k successors. By Theorem 4.13, if n is sufficiently large, almost all frames in $\mathcal{F}_n^{rt}$ will satisfy this property. We can construct an onto function $\gamma : S'' \to S'$ such that $(s', t') \in \mathcal{R}''$ iff $(\gamma(s'), \gamma'(t')) \in \mathcal{R}'$. Moreover, we can define a function π'' such that $\pi''(s') = \pi'(\gamma(s'))$. Let $M'' = (S'', \mathcal{R}'', \pi'')$. An easy induction on structure shows that for all formulas ψ, we have $(M'', s) \models \psi$ iff $(M', \gamma(s)) \models \psi$. In particular, it follows that $\neg\varphi$ is satisfiable in F''. Thus, $\neg\varphi$ is satisfied in almost all frames in $\mathcal{F}^{rt}$, so $\mu^{rt}(\varphi) = 0$.

For part (c), clearly if φ is provable in S5, then $\mu^{rst}(\varphi) = 1$. If φ is not provable in S5 then, as we have already observed, by results of Ladner [Lad77], there is some structure $M = (S, \mathcal{R}, \pi)$ such that $\mathcal{R}$ is the universal relation on S, $\neg\varphi$ is satisfiable in M, and $|S| = k \leq |\neg\varphi|$. By Theorem 4.10, almost every frame $F = (S', \mathcal{R}') \in \mathcal{F}^{rst}$ contains an equivalence class of size k. Clearly we can define a truth assignment π' such that $\neg\varphi$ is satisfiable in that equivalence class in $(S', \mathcal{R}', \pi')$. Hence, $\neg\varphi$ is satisfied in almost all frames in $\mathcal{F}^{rst}$, so $\mu^{rst}(\varphi) = 0$. ∎

We next consider axiomatizability. Although the set of formulas that are almost-surely frame valid with respect to $\mathcal{F}$ is decidable, and thus does admit a recursive axiomatization, it appears that there is no elegant axiomatization for almost-sure frame validity in this cases. It is clear from the previous theorem that we can obtain an axiomatization for almost-sure frame validity with respect to $\mathcal{F}^r$ by adding the axiom $\Box\varphi \Rightarrow \varphi$ to a complete axiomatization for almost-sure frame validity with respect to $\mathcal{F}$. Of course, the previous theorem shows that S5 is a complete axiomatization for almost-sure frame validity with respect to $\mathcal{F}^{rst}$. Finally, for $\mathcal{F}^{rt}$, it is easy to see that the following axiom, a weakening of the axiom DEP2, characterizes depth-2 frames:

DEP2$'$. $\neg(p \wedge \Diamond(\neg p \wedge \Diamond(p \wedge \Diamond\neg p)))$

Let S4* consist of the axioms of S4 together with DEP2$'$. From the previous theorem we immediately obtain:

Theorem 5.16: *S4* is a sound and complete axiomatization for almost-sure frame validity with respect to $\mathcal{F}^{rt}$.*

Finally, we consider complexity issues. Deciding almost-sure frame validity with respect to $\mathcal{F}^r$ is easily seen to satisfy the same complexity bounds as almost-sure frame validity with respect to $\mathcal{F}$. Since S5 is a complete axiomatization for almost-sure frame validity with respect to $\mathcal{F}^{rst}$, the problem of deciding if a formula is almost-surely frame valid in this case is complete for co-NP if Φ is infinite and is in polynomial time if Φ is finite. As we now show, this is also the case for almost-sure frame validity with respect to $\mathcal{F}^{rt}$.

Theorem 5.17: *If Φ is finite, then deciding almost-sure validity with respect to $\mathcal{F}^{rt}$ for formulas in $\mathcal{L}(\Phi)$ is in polynomial time; if Φ is infinite, it is co-NP-complete (for both the dag and tree representations).*

Proof: We consider the satisfiability problem. As we saw in the proof of Theorem 5.15, given a formula φ, if it is satisfiable in a reflexive, transitive, depth-2 frame, it is satisfiable in one with at most $|\varphi|^2$ states. Thus, if Φ is infinite, we can simply guess a satisfying structure of the right type and verify that it does indeed satisfy φ. If Φ is finite, it is easy to check that there are only finitely many inequivalent reflexive, transitive, depth-2 frames. We can simply check each one of them to see if any satisfy φ. ∎

Acknowledgements: We would like to thank Moshe Vardi for his many useful comments on the paper and for allowing us to include his result on Δ_p^2-hardness (Theorem 4.6), his proof that frame satisfiability can express SAT (Theorem 3.3), and his observation that we can translate from modal logic to first-order formulas in $\mathcal{L}^2_{\omega\omega}$. Ron Fagin, Grisha Schwarz, and Rineke Verbrugge also provided useful comments on a draft of the paper. Kevin Compton pointed out the theorem in [Com87] from which Theorem 4.10 follows. We thank Larry Stockmeyer for his proof of the $\Delta_2^{p,\log(n)}$ lower bound in Theorem 4.6 and for pointing out the reference [Kre88]. Finally, we thank Georg Gottlob for pointing out that the logic K^C was originally defined by Carnap and for discussions on the material in Theorem 4.6.

References

[AU79] A. V. Aho and J. D. Ullman. Universality of data retrieval languages. In *Proc. 6th ACM Symp. on Principles of Programming Languages*, pages 110–117, 1979.

[Ben85] J. F. A. K. van Benthem. *Modal Logic and Classical Logic.* Bibliopolis, Naples, 1985.

[Bol85] B. Bollob'as. *Random Graphs.* Academic Press, New York, 1985.

[Bus87] S. R. Buss. The Boolean formula value problem is in ALOGTIME. In *Proc. 19th ACM Symp. on Theory of Computing*, pages 123–131, 1987.

[Can88] J. F. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th ACM Symp. on Theory of Computing*, pages 460–467, 1988.

[Car47] R. Carnap. *Meaning and Necessity.* University of Chicago Press, Chicago, 1947.

[Com87] K. J. Compton. A logical approach to asymptotic combinatorics I: First-order properties. *Advances in Mathematics*, 65:65–96, 1987.

[Com88] K. Compton. 0-1 laws in logic and combinatorics. In I. Rival, editor, *Proc. 1987 NATO Adv. Study Inst. on algorithms and order*, pages 353–383. Reidel, Dordrecht, Netherlands, 1988.

[DG79] B. Dreben and W. D. Goldfarb. *The Decision Problem: Solvable Classes of Quantificational Formulas.* Addison-Wesley, Reading, Mass., 1979.

[Fag74] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. In R. M. Karp, editor, *Complexity of Computation, SIAM-AMS Proceedings, Vol. 7*, pages 43–73, 1974.

[Fag75] R. Fagin. Monadic generalized spectra. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 21:89–96, 1975.

[Fag76] R. Fagin. Probabilities on finite models. *Journal of Symbolic Logic*, 41(1):50–58, 1976.

[FL79] M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Sciences*, 18(2):194–211, 1979.

[GHK92] A. J. Grove, J. Y. Halpern, and D. Koller. Asymptotic conditional probabilities for first-order logic. In *Proc. 24th ACM Symp. on Theory of Computing*, pages 294–305, 1992.

[GKLT69] Y. V. Glebskiĭ, D. I. Kogan, M. I. Liogon'kiĭ, and V. A. Talanov. Range and degree of realizability of formulas in the restricted predicate calculus. *Kibernetika*, 2:17–28, 1969.

[GKP89] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics—A Foundation for Computer Science*. Addison-Wesley, Reading, Mass., 1989.

[Got95] G. Gottlob. NP trees and Carnap's modal logic. *Journal of the ACM*, 42(2):421–457, 1995.

[Gra83] E. Grandjean. Complexity of the first–order theory of almost all structures. *Information and Control*, 52:180–204, 1983.

[Hal87] J. Y. Halpern. Using reasoning about knowledge to analyze distributed systems. In J. F. Traub, B. J. Grosz, B. W. Lampson, and N. J. Nilsson, editors, *Annual Review of Computer Science, Vol. 2*, pages 37–68. Annual Reviews Inc., Palo Alto, Calif., 1987.

[HC68] G. E. Hughes and M. J. Cresswell. *An Introduction to Modal Logic*. Methuen, London, 1968.

[HC84] G. E. Hughes and M. J. Cresswell. *A Companion to Modal Logic*. Methuen, London, 1984.

[HM92] J. Y. Halpern and Y. Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54:319–379, 1992.

[IK89] N. Immerman and D. Kozen. Definability with bounded number of bound variables. *Information and Computation*, 83:121–139, 1989.

[Kau87] M. Kaufmann. Counterexample to the 0-1 law for existential monadic second-order logic. CLI Internal Note 32, Computational Logic Inc., December 1987.

[KR75] D. J. Kleitman and B. L. Rothschild. Asymptotic enumeration of partial orders on a finite set. *Transactions of the AMS*, 205:205–220, 1975.

[Kre88] M. W. Krentel. The complexity of optimization problems. *Journal of Computer and System Sciences*, 36(3):490–509, 1988.

[KV87] Ph. G. Kolaitis and M. Y. Vardi. The decision problem for the probabilities of higher-order properties. In *Proc. 19th ACM Symp. on Theory of Computing*, pages 425–435, 1987.

[KV90a] Ph. G. Kolaitis and M. Y. Vardi. 0-1 laws and decision problems for fragments of second-order logic. *Information and Computation*, 87:302–338, 1990.

[KV90b] Ph. G. Kolaitis and M. Y. Vardi. 0-1 laws for infinitary logics. In *Proc. 5th IEEE Symp. on Logic in Computer Science*, pages 156–167, 1990.

[Lad75] R. E. Ladner. The circuit value problem is log-space complete for *P*. *SIGACT News*, 6(2):18–20, 1975.

[Lad77] R. E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.

[Mak66] D. Makinson. On some completeness theorems in modal logic. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 12:379–384, 1966.

[MP81] Z. Manna and A. Pnueli. Verification of temporal programs: the temporal framework. In R. S. Boyer and J. S. Moore, editors, *The Correctness Problem in Computer Science*. Academic Press, New York, 1981.

[PS89] L. Pacholski and W. Szwast. The 0-1 law fails for the class of existential second-order Gödel sentences with equality. In *Proc. 30th IEEE Symp. on Foundations of Computer Science*, pages 280–285, 1989.

[Sto77] L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.