A Logic for Reasoning about Probabilities*

Ronald Fagin
Joseph Y. Halpern
Nimrod Megiddo

IBM Almaden Research Center
San Jose, CA 95120
email: fagin@ibm.com, halpern@ibm.com, megiddo@ibm.com

Abstract: We consider a language for reasoning about probability which allows us to make statements such as "the probability of E_1 is less than 1/3" and "the probability of E_1 is at least twice the probability of E_2", where E_1 and E_2 are arbitrary events. We consider the case where all events are measurable (i.e., represent measurable sets) and the more general case, which is also of interest in practice, where they may not be measurable. The measurable case is essentially a formalization of (the propositional fragment of) Nilsson's probabilistic logic. As we show in a companion paper, the general (nonmeasurable) case corresponds precisely to replacing probability measures by Dempster-Shafer belief functions. In both cases, we provide a complete axiomatization and show that the problem of deciding satisfiability is NP-complete, no worse than that of propositional logic. As a tool for proving our complete axiomatizations, we give a complete axiomatization for reasoning about Boolean combinations of linear inequalities, which is of independent interest. This proof and others make crucial use of results from the theory of linear programming. We then extend the language to allow reasoning about conditional probability, and show that the resulting logic is decidable and completely axiomatizable, by making use of the theory of real closed fields.

*This paper is essentially the same as one that appears in *Information and Computation* **87**:1,2, 1990, pp. 78–128. A preliminary version appears in *Proceedings of the Third Symposium on Logic in Computer Science*, 1988, pp. 277-291.

1 Introduction

The need for reasoning about probability arises in many areas of research. In computer science we must analyze probabilistic programs, reason about the behavior of a program under probabilistic assumptions about the input, or reason about uncertain information in an expert system. While probability theory is a well-studied branch of mathematics, in order to carry out formal reasoning about probability, it is helpful to have a logic for reasoning about probability with a well-defined syntax and semantics. Having such a logic might also clarify the role of probability in the analysis. It is all too easy to lose track of precisely which events it is that are being assigned a probability, and how that probability should be assigned (see [HT93] for a discussion of the situation in the context of distributed systems). There is a fairly extensive literature on reasoning about probability (see for example [Bac90, Car50, Gai64, GKP88, GF87, HF87, Hoo78, Kav89, Kei85, Luk70, Nil86, Nut87, Sha76] and the references in [Nil86]), but remarkably few attempts at constructing a logic to reason explicitly about probabilities.

We start by considering a language that allows linear inequalities involving probabilities. Thus, typical formulas include $3w(\varphi) < 1$ and $w(\varphi) \geq 2w(\psi)$. We consider two variants of the logic. In the first, φ and ψ represent measurable events, which have a well-defined probability. In this case, these formulas can be read "three times the probability of φ is less than one" (i.e., φ has probability less than 1/3) and "φ is at least twice as probable as ψ". However, there are times we want to be able to discuss in the language events that are not measurable. In such cases, we view $w(\varphi)$ as representing the inner measure (induced by the probability measure) of the set corresponding to φ. The letter w is chosen to stand for "weight"; w will sometimes represent a (probability) measure and sometimes an inner measure induced by a probability measure.

The usual reason that mathematicians deal with nonmeasurable sets is out of mathematical necessity: for example, it is well known that if the set of points in the probability space consists of all numbers in the real interval $[0, 1]$, then we cannot allow every set to be measurable if (like Lebesgue measure) the measure is to be translation-invariant (see [Roy64, page 54]). However, in this paper we allow nonmeasurable sets out of choice, rather than out of mathematical necessity. Our original motivation for allowing nonmeasurable sets came from distributed systems, where they arise naturally, particularly in asynchronous sytems (see [HT93] for details). It seems that allowing nonmeasurability might also provide a useful way of reasoning about uncertainty, a topic of great interest in AI. (This point is discussed in detail in [FH91].) Moreover, as is shown in [FH91], in a precise sense inner measures induced by probability measures correspond to Dempster-Shafer belief functions [Dem68, Sha76], the key tool in the Dempster-Shafer theory of evidence (which in turn is one of the major techniques for dealing with uncertainty in AI). Hence, reasoning about inner measures induced by probability measures corresponds to one important method of reasoning about uncertainty in AI. We shall discuss belief functions more in Section 7.

We expect our logic to be used for reasoning *about* probabilities. All formulas are either true or false. They do not have probabilistic truth values. We give a complete axiomatization of the logic for both the measurable and general (nonmeasurable) cases. In both cases, we show that the problem of deciding satisfiability is NP-complete, no worse than that of propositional logic. The key ingredient in our proofs is the observation that the validity problem can be reduced to a linear programming problem, which allows us to apply techniques from linear programming.

The logic just described does not allow for general reasoning about conditional probabilities. If we think of a formula such as $w(p_1 \mid p_2) \geq 1/2$ as saying "the probability of p_1 given p_2 is at least 1/2", then we can express this in the logic described above by rewriting $w(p_1 \mid p_2)$ as $w(p_1 \wedge p_2)/w(p_2)$ and then clearing the denominators to get $w(p_1 \wedge p_2) - 2w(p_2) \geq 0$. However, we cannot express more complicated expressions such as $w(p_2 \mid p_1) + w(p_1 \mid p_2) \geq 1/2$ in our logic, because clearing the denominator in this case leaves us with a nonlinear combination of terms. In order to deal with conditional probabilities, we can extend our logic to allow expressions with products of probability terms, such as $2w(p_1 \wedge p_2)w(p_2) + 2w(p_1 \wedge p_2)w(p_1) \geq w(p_1)w(p_2)$ (this is what we get when we clear the denominators in the conditional expression above). Because we have products of terms, we can no longer apply techniques from linear programming to get decision procedures and axiomatizations. However, the decision problem for the resulting logic can be reduced to the decision problem for the theory of *real closed fields* [Sho67]. By combining a recent result of Canny [Can88] with some of the techniques we develop in the linear case, we can obtain a polynomial space decision procedure for both the measurable case and the general case of the logic. We can further extend the logic to allow first-order quantification over real numbers. The decision problem for the resulting logic is still reducible to the decision problem for the theory of real closed fields. This observation lets us derive complete axiomatizations and decision procedures for the extended language, for both the measurable and general case. In this case, combining our techniques with results of Ben-Or, Kozen, and Reif [BKR86], we get an exponential space decision procedure. Thus, allowing nonlinear terms in the logic seems to have a high cost in terms of complexity, and further allowing quantifiers an even higher cost.

The measurable case of our first logic (with only linear terms) is essentially a formalization of (the propositional fragment of) the logic discussed by Nilsson in [Nil86].[1] The question of providing a complete axiomatization and decision procedure for Nilsson's logic has attracted the attention of other researchers before. Haddawy and Frisch [HF87] provide some sound axioms (which they observe are not complete), and show how interesting consequences can be deduced using their axioms. Georgakopoulos, Kavvadias, and Papadimitriou [GKP88] show that a less expressive logic than ours (where formulas have the form $(w(\varphi_1) = c_1) \wedge \ldots \wedge (w(\varphi_m) = c_m)$, and each φ_i is a disjunction of primitive propositions and their negations) is also NP-complete. Since their logic is weaker than ours, their lower bound implies ours; their upper bound techniques (which were developed independently of ours) can be extended in a straightforward way to the

[1] Nilsson does not give an explicit syntax for his logic, but it seems from his examples that he wants to allow linear combinations of terms.

language of our first logic.

The measurable case of our richer logic bears some similarities to the first-order logic of probabilities considered by Bacchus [Bac90]. There are also some significant technical differences; we compare our work with that of Bacchus and the more recent results on first-order logics of probability in [AH94, Hal90] in more detail in Section 6.

The measurable case of the richer logic can also be viewed as a fragment of the probabilistic propositional dynamic logic considered by Feldman [Fel84]. Feldman provides a double-exponential space decision procedure for his logic, also by reduction to the decision problem for the theory of real closed fields. (The extra complexity in his logic arises from the presence of program operators.) Kozen [Koz85] too considers a probabilistic propositional dynamic logic (which is a fragment of Feldman's logic) for which he shows that the decision problem is PSPACE-complete. While a formula such as $w(\varphi) \geq 2w(\psi)$ can be viewed as a formula in Kozen's logic, conjunctions of such formulas cannot be so viewed (since Kozen's logic is not closed under Boolean combination). Kozen also does not allow nonlinear combinations.

None of the papers mentioned above consider the nonmeasurable case. Hoover [Hoo78] and Keisler [Kei85] provide complete axiomatizations for their logics (their language is quite different from ours, in that they allow infinite conjunctions, and do not allow sums of probabilities). Other papers (for example [LS82, HR87]) consider modal logics that allow more qualitative reasoning. In [LS82] there are modal operators that allow one to say "with probability one" or "with probability greater than zero"; in [HR87] there is a modal operator which says "it is likely that". Decision procedures and complete axiomatizations are obtained for these logics. However, neither of them allows explicit manipulation of probabilities.

In order to prove our results on reasoning about probabilities for our first logic, which allows only linear terms, we derive results on reasoning about Boolean combinations of linear inequalities. These results are of interest in their own right. It is here that we make our main use of results from linear programming. Our complete axiomatizations of the logic for reasoning about probabilities, in both the measurable and nonmeasurable case, divide neatly into three parts, which deal respectively with propositional reasoning, reasoning about linear inequalities, and reasoning about probabilities.

The rest of this paper is organized as follows. Section 2 defines the first logic for reasoning about probabilities, which allows only linear combinations, and deals with the measurable case of the logic: we give the syntax and semantics, provide an axiomatization, which we prove is sound and complete, prove a small model theorem, and show that the decision procedure is NP-complete. In Section 3, we extend these results to the nonmeasurable case. Section 4 deals with reasoning about Boolean combinations of linear inequalities: again we give the syntax and semantics, provide a sound and complete axiomatization, prove a small model theorem, and show that the decision procedure is NP-complete. In Section 5, we extend the logic for reasoning about probabilities to allow nonlinear combinations of terms, thus allowing us to reason about conditional probabilities. In Section 6, we extend the logic further to allow first-order quantification over real numbers. We show that the techniques of the previous sections can be extended to obtain decision procedures and complete axiomatizations for the richer logic. In Section 7, we discuss Dempster-Shafer belief functions and their relationship to inner measures induced by probability measures. We give our conclusions in Section 8.

2 The measurable case

2.1 Syntax and semantics

The syntax for our first logic for reasoning about probabilities is quite simple. We start with a fixed infinite set $\Phi = \{p_1, p_2, \ldots\}$ of *primitive propositions* or *basic events*. For convenience, we define *true* to be an abbreviation for the formula $p \vee \neg p$, where p is a fixed primitive proposition. We abbreviate $\neg$*true* by *false*. The set of *propositional formulas* or *events* is the closure of Φ under the Boolean operations $\wedge$ and $\neg$. We use p, possibly subscripted or primed, to represent primitive propositions, and φ and ψ, again possibly subscripted or primed, to represent propositional formulas. A *primitive weight term* is an expression of the form $w(\varphi)$, where φ is a propositional formula. A *weight term*, or just *term*, is an expression of the form $a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k)$, where $a_1, \ldots, a_k$ are integers and $k \geq 1$. A *basic weight formula* is a statement of the form $t \geq c$, where t is a term and c is an integer.[2] For example, $2w(p_1 \wedge p_2) + 7w(p_1 \vee \neg p_3) \geq 3$ is a basic weight formula. A *weight formula* is a Boolean combination of basic weight formulas. We now use f and g, again possibly subscripted or primed, to refer to weight formulas. When we refer to a "formula", without saying whether it is a propositional formula or a weight formula, we mean "weight formula". We shall use obvious abbreviations, such as $w(\varphi) - w(\psi) \geq a$ for $w(\varphi) + (-1)w(\psi) \geq a$, $w(\varphi) \geq w(\psi)$ for $w(\varphi) - w(\psi) \geq 0$, $w(\varphi) \leq c$ for $-w(\varphi) \geq -c$, $w(\varphi) < c$ for $\neg(w(\varphi) \geq c)$, and $w(\varphi) = c$ for $(w(\varphi) \geq c) \wedge (w(\varphi) \leq c)$. A formula such as $w(\varphi) \geq 1/3$ can be viewed as an abbreviation for $3w(\varphi) \geq 1$; we can always allow rational numbers in our formulas as abbreviations for the formula that would be obtained by clearing the denominators.

In order to give semantics to such formulas, we first need to review briefly some probability theory (see, for example, [Fel57, Hal50] for more details). A *probability space* is a tuple $(S, \mathcal{X}, \mu)$ where S is a set (we think of S as a set of *states* or *possible worlds*, for reasons to be explained below), $\mathcal{X}$ is a σ-algebra of subsets of S (i.e., a set of subsets of S containing the empty set and closed under complementation and countable union)

[2] In an earlier version of this paper [FHM88], we allowed c and the coefficients that appear in terms to be arbitrary real numbers, rather than requiring them to be integers as we do here. There is no problem giving semantics to formulas with real coefficients, and we can still obtain the same complete axiomatization by precisely the same techniques as described below. However, when we go to richer languages later, we need the restriction to integers in order to make use of results from the theory of real closed fields. We remark that we have deliberately chosen to be sloppy and use a for both the symbol in the language that represents the integer a, and for the integer itself.

whose elements are called *measurable sets*, and μ is a *probability measure* defined on the measurable sets. Thus $\mu: \mathcal{X} \rightarrow [0,1]$ satisfies the following properties:

P1. $\mu(X) \geq 0$ for all $X \in \mathcal{X}$

P2. $\mu(S) = 1$

P3. $\mu(\cup_{i=1}^{\infty} X_i) = \Sigma_{i=1}^{\infty} \mu(X_i)$, if the X_i's are pairwise disjoint members of $\mathcal{X}$

Property P3 is called *countable additivity*. Of course, the fact that $\mathcal{X}$ is closed under countable union guarantees that if each $X_i \in \mathcal{X}$, then so is $\cup_{i=1}^{\infty} X_i$. If $\mathcal{X}$ is a finite set, then we can simplify property P3 to

P3$'$. $\mu(X \cup Y) = \mu(X) + \mu(Y)$, if X and Y are disjoint members of $\mathcal{X}$

This property is called *finite additivity*. Properties P1, P2, and P3$'$ characterize probability measures in finite spaces. Observe that from P2 and P3$'$ it follows (taking $Y = \overline{X}$, the complement of X) that $\mu(\overline{X}) = 1 - \mu(X)$. Taking $X = S$, we also get that $\mu(\emptyset) = 0$. We remark for future reference that it is easy to show that P3$'$ is equivalent to the following axiom:

P3$''$. $\mu(X) = \mu(X \cap Y) + \mu(X \cap \overline{Y})$

Given a probability space $(S, \mathcal{X}, \mu)$, we can give semantics to weight formulas by associating with every basic event (primitive proposition) a measurable set, extending this association to all events in a straightforward way, and then computing the probability of these events using μ. More formally, a *probability structure* is a tuple $M = (S, \mathcal{X}, \mu, \pi)$, where $(S, \mathcal{X}, \mu)$ is a probability space, and π associates with each state in S a truth assignment on the primitive propositions in Φ. Thus $\pi(s)(p) \in \{\mathbf{true}, \mathbf{false}\}$ for each $s \in S$ and $p \in \Phi$. Define $p^M = \{s \in S \mid \pi(s)(p) = \mathbf{true}\}$. We say that a probability structure M is *measurable* if for each primitive proposition p, the set p^M is measurable. We restrict attention in this section to measurable probability structures. The set p^M can be thought of as the possible worlds where p is true, or the states at which the event p occurs. We can extend $\pi(s)$ to a truth assignment on all propositional formulas in the standard way, and then associate with each propositional formula φ the set $\varphi^M = \{s \in S \mid \pi(s)(\varphi) = \mathbf{true}\}$. An easy induction on the structure of formulas shows that φ^M is a measurable set. If $M = (S, \mathcal{X}, \mu, \pi)$, we define

$$M \models a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) \geq c \text{ iff } a_1 \mu(\varphi_1^M) + \cdots + a_k \mu(\varphi_k^M) \geq c.$$

We then extend $\models$ ("satisfies") to arbitrary weight formulas, which are just Boolean combinations of basic weight formulas, in the obvious way, namely

$$\begin{array}{rcl} M \models \neg f & \text{iff} & M \not\models f \\ M \models f \wedge g & \text{iff} & M \models f \text{ and } M \models g. \end{array}$$

There are two other approaches we could have taken to assigning semantics, both of which are easily seen to be equivalent to this one. One is to have π associate a measurable set p^M directly with a primitive proposition p, rather than going through truth assignments as we have done. The second (which was taken in [Nil86]) is to have S consist of one state for each of the 2^n different truth assignments to the primitive propositions of Φ and have $\mathcal{X}$ consist of all subsets of S. We choose our approach because it extends more easily to the nonmeasurable case considered in Section 3, to the first-order case, and to the case considered in [FH94] where we extend the language to allow statements about an agent's knowledge. (See [FH91] for more discussion about the relationship between our approach and Nilsson's approach.)

As before, we say a weight formula f is *valid* if $M \models f$ for all probability structures M, and is *satisfiable* if $M \models f$ for some probability structure M. We may then say that f is *satisfied in* M.

2.2 Complete axiomatization

In this subsection we characterize the valid formulas for the measurable case by a sound and complete axiomatization. A formula f is said to be *provable* in an axiom system if it can be proven in a finite sequence of steps, each of which is an axiom of the system or follows from previous steps by an application of an inference rule. It is said to be *inconsistent* if its negation $\neg f$ is provable, and otherwise f is said to be *consistent*. An axiom system is *sound* if every provable formula is valid and all the inference rules preserve validity. It is *complete* if every valid formula is provable (or, equivalently, if every consistent formula is satisfiable).

The system we now present, which we call AX_{MEAS}, divides nicely into three parts, which deal respectively with propositional reasoning, reasoning about linear inequalities, and reasoning about probability.

Propositional reasoning:

Taut. All instances of propositional tautologies

MP. From f and $f \Rightarrow g$ infer g (modus ponens)

Reasoning about linear inequalities:

Ineq. All instances of valid formulas about linear inequalities (we explain this in more detail below)

Reasoning about probabilities:

W1. $w(\varphi) \geq 0$ (nonnegativity)

W2. $w(true) = 1$ (the probability of the event *true* is 1)

W3. $w(\varphi \wedge \psi) + w(\varphi \wedge \neg\psi) = w(\varphi)$ (additivity)

W4. $w(\varphi) = w(\psi)$ if $\varphi \equiv \psi$ is a propositional tautology (distributivity)

Before we prove the soundness and completeness of AX_{MEAS}, we briefly discuss the axioms and rules in the system.

First note that axioms W1, W2, and W3 correspond precisely to P1, P2, and P3$''$, the axioms that characterize probability measures in finite spaces. We have no axiom that says that the probability measure is countably additive. Indeed, we can easily construct a "nonstandard" model $M = (S, \mathcal{X}, \mu, \pi)$ satisfying all these axioms where μ is finitely additive, but not countably additive, and thus not a probability measure. (An example can be obtained by letting S be countably infinite, letting $\mathcal{X}$ consist of the finite and co-finite sets, and letting $\mu(T) = 0$ if T is finite, and $\mu(T) = 1$ if T is co-finite, for each $T \in \mathcal{X}$.) Nevertheless, as we shall show in Theorem 2.2, the axiom system above completely characterizes the properties of weight formulas in probability structures. This is consistent with the observation that our axiom system does not imply countable additivity, since countable additivity cannot be expressed by a formula in our language.

Instances of Taut include formulas such as $f \vee \neg f$, where f is a weight formula. However, note that if p is a primitive proposition, then $p \vee \neg p$ is not an instance of Taut, since $p \vee \neg p$ is not a weight formula, and all of our axioms are, of course, weight formulas. We remark that we could replace Taut by a simple collection of axioms that characterize propositional tautologies (see for example [Men64]). We have not done so here because we want to focus here on the axioms for probability.

The axiom Ineq includes "all valid formulas about linear inequalities." To make this precise, assume that we start with a fixed infinite set of *variables*. Let an *inequality term* (or just *term*, if there is no danger of confusion) be an expression of the form $a_1x_1 + \cdots + a_kx_k$, where $a_1, \ldots, a_k$ are integers and $k \geq 1$. A *basic inequality formula* is a statement of the form $t \geq c$, where t is a term and c is an integer. For example, $2x_3 + 7x_2 \geq 3$ is a basic inequality formula. An *inequality formula* is a Boolean combination of basic inequality formulas. We use f and g, again possibly subscripted or primed, to refer to inequality formulas. An *assignment to variables* is a function A that assigns a real number to every variable. We define

$$A \models a_1x_1 + \cdots + a_kx_k \geq c \text{ iff } a_1A(x_1) + \cdots + a_kA(x_k) \geq c.$$

We then extend $\models$ to arbitrary inequality formulas, which are just Boolean combinations of basic inequality formulas, in the obvious way, namely

$$\begin{array}{rcl} A \models \neg f & \text{iff} & A \not\models f \\ A \models f \wedge g & \text{iff} & A \models f \text{ and } A \models g. \end{array}$$

As usual we say an inequality formula f is *valid* if $A \models f$ for all A that are assignments to variables, and is *satisfiable* if $A \models f$ for some such A.

A typical valid inequality formula is

$$\begin{aligned}(a_1 x_1 + \cdots + a_k x_k \geq c) \wedge (a'_1 x_1 + \cdots + a'_k x_k \geq c') \Rightarrow \\ (a_1 + a'_1)x_1 + \cdots + (a_k + a'_k)x_k \geq (c + c').\end{aligned} \tag{1}$$

To get an instance of Ineq, we simply replace each variable x_i that occurs in a valid formula about linear inequalities by a primitive weight term $w(\varphi_i)$ (of course, each occurrence of the variable x_i must be replaced by the same primitive weight term $w(\varphi_i)$). Thus, the following weight formula, which results from replacing each occurrence of x_i in (1) by $w(\varphi_i)$, is an instance of Ineq:

$$\begin{aligned}(a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) \geq c) \wedge (a'_1 w(\varphi_1) + \cdots + a'_k w(\varphi_k) \geq c') \Rightarrow \\ (a_1 + a'_1)w(\varphi_1) + \cdots + (a_k + a'_k)w(\varphi_k) \geq (c + c').\end{aligned} \tag{2}$$

We give a particular sound and complete axiomatization for Boolean combinations of linear inequalities (which, for example, has (1) as an axiom) in Section 4. Other axiomatizations are also possible; the details don't matter here.

Finally, we note that just as for Taut and Ineq, we could make use of a complete axiomatization for propositional equivalences to create a collection of elementary axioms that could replace W4.

In order to see an example of how the axioms operate, we show that $w(false) = 0$ is provable. Note that this formula is easily seen to be valid, since it corresponds to the fact that $\mu(\emptyset) = 0$, which we already observed follows from the other axioms of probability.

Lemma 2.1: *The formula $w(false) = 0$ is provable from AX_{MEAS}.*

Proof: In the semi-formal proof below, PR is an abbreviation for "propositional reasoning", i.e., using a combination of Taut and MP.

1. $w(\mathit{true} \wedge \mathit{true}) + w(\mathit{true} \wedge \mathit{false}) = w(\mathit{true})$ (W3, taking φ and ψ both to be *true*)
2. $w(\mathit{true} \wedge \mathit{true}) = w(\mathit{true})$ (W4)
3. $w(\mathit{true} \wedge \mathit{false}) = w(\mathit{false})$ (W4)
4. $((w(\mathit{true} \wedge \mathit{true}) + w(\mathit{true} \wedge \mathit{false}) = w(\mathit{true})) \wedge (w(\mathit{true} \wedge \mathit{true}) = w(\mathit{true})) \wedge (w(\mathit{true} \wedge \mathit{false}) = w(\mathit{false}))) \Rightarrow (w(\mathit{false}) = 0)$ (Ineq, since this is an instance of the valid inequality $((x_1 + x_2 = x_3) \wedge (x_1 = x_3) \wedge (x_2 = x_4)) \Rightarrow (x_4 = 0)$)
5. $w(\mathit{false}) = 0$ (1, 2, 3, 4, PR) ∎

Theorem 2.2: *AX_{MEAS} is sound and complete with respect to measurable probability structures.*

Proof: It is easy to see that each axiom is valid in measurable probability structures. To prove completeness, we show that if f is consistent then f is satisfiable. So suppose that f is consistent. We construct a measurable probability structure satisfying f by reducing satisfiability of f to satisfiability of a set of linear inequalities, and then making use of the axiom Ineq.

Our first step is to reduce f to a canonical form. Let $g_1 \vee \cdots \vee g_r$ be a disjunctive normal form expression for f (where each g_i is a conjunction of basic weight formulas and their negations). Using propositional reasoning, we can show that f is provably equivalent to this disjunction. Since f is consistent, so is some g_i; this is because if $\neg g_i$ is provable for each i, then so is $\neg(g_1 \vee \cdots \vee g_r)$. Moreover, any structure satisfying g_i also satisfies f. Thus, without loss of generality, we can restrict attention to a formula f that is a conjunction of basic weight formulas and their negations.

An *n-atom* is a formula of the form $p'_1 \wedge \ldots \wedge p'_n$, where p'_i is either p_i or $\neg p_i$ for each i. If n is understood or not important, we may refer to n-atoms as simply *atoms*.

Lemma 2.3: *Let φ be a propositional formula. Assume that $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in φ. Let $At_n(\varphi)$ consist of all the n-atoms δ such that $\delta \Rightarrow \varphi$ is a propositional tautology. Then $w(\varphi) = \sum_{\delta \in At_n(\varphi)} w(\delta)$ is provable.*[3]

Proof: While the formula $w(\varphi) = \sum_{\delta \in At_n(\varphi)} w(\delta)$ is clearly valid, showing it is provable requires some care. We now show by induction on $j \geq 1$, that if $\psi_1, \ldots, \psi_{2^j}$ are all of the j-atoms (in some fixed but arbitrary order), then $w(\varphi) = w(\varphi \wedge \psi_1) + \cdots + w(\varphi \wedge \psi_{2^j})$ is provable. If $j = 1$, this follows by finite additivity (axiom W3), possibly along with Ineq and propositional reasoning (to permute the order of the 1-atoms, if necessary). Assume inductively that we have shown that

$$w(\varphi) = w(\varphi \wedge \psi_1) + \cdots + w(\varphi \wedge \psi_{2^j}) \tag{3}$$

is provable. By W3, $w(\varphi \wedge \psi_1 \wedge p_{j+1}) + w(\varphi \wedge \psi_1 \wedge \neg p_{j+1}) = w(\varphi \wedge \psi_1)$ is provable. By Ineq and propositional reasoning, we can replace each $w(\varphi \wedge \psi_r)$ in (3) by $w(\varphi \wedge \psi_r \wedge p_{j+1}) + w(\varphi \wedge \psi_r \wedge \neg p_{j+1})$. This proves the inductive step.

In particular,

$$w(\varphi) = w(\varphi \wedge \delta_1) + \cdots + w(\varphi \wedge \delta_{2^n}) \tag{4}$$

is provable. Since $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in φ, it is clear that if $\delta_r \in At_n(\varphi)$, then $\varphi \wedge \delta_r$ is equivalent to δ_r, and if $\delta_r \notin At_n(\varphi)$, then $\varphi \wedge \delta_r$ is equivalent to *false*. So by W4, we see that if $\delta_r \in At_n(\varphi)$, then $w(\varphi \wedge \delta_r) = w(\delta_r)$

[3] Here $\sum_{\delta \in At_n(\varphi)} w(\delta)$ represents $w(\delta_1) + \cdots + w(\delta_r)$, where $\delta_1, \ldots, \delta_r$ are the distinct members of $At_n(\varphi)$ in some arbitrary order. By Ineq, the particular order chosen does not matter.

is provable, and if $\delta_r \notin At_n(\varphi)$, then $w(\varphi \wedge \delta_r) = w(\mathit{false})$ is provable. Therefore, as before, we can replace each $w(\varphi \wedge \delta_r)$ in (4) by either $w(\delta_r)$ or $w(\mathit{false})$ (as appropriate). Also, we can drop the $w(\mathit{false})$ terms, since $w(\mathit{false}) = 0$ is provable by Lemma 2.1. The lemma now follows. ∎

Using Lemma 2.3 we can find a formula f' provably equivalent to f where f' is obtained from f by replacing each term in f by a term of the form $a_1 w(\delta_1) + \cdots + a_{2^n} w(\delta_{2^n})$, where $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in f, and where $\{\delta_1, \ldots, \delta_{2^n}\}$ are the n-atoms. For example, the term $2w(p_1 \vee p_2) + 3w(\neg p_2)$ can be replaced by $2w(p_1 \wedge p_2) + 2w(\neg p_1 \wedge p_2) + 5w(p_1 \wedge \neg p_2) + 3w(\neg p_1 \wedge \neg p_2)$ (the reader can easily verify the validity of this replacement with a Venn diagram). Let f'' be obtained from f' by adding as conjuncts to f' all of the weight formulas $w(\delta_j) \geq 0$, for $1 \leq j \leq 2^n$, along with weight formulas $w(\delta_1) + \cdots + w(\delta_{2^n}) \geq 1$ and $-w(\delta_1) - \cdots - w(\delta_{2^n}) \geq -1$ (which together say that the sum of the probabilities of the n-atoms is 1). Then f'' is provably equivalent to f', and hence to f. (The fact that the formulas that say "the sum of the probabilities of the n-atoms is 1" are provable follow from Lemma 2.3, where we let φ be *true*.) So we need only show that f'' is satisfiable.

The negation of a basic weight formula $a_1 w(\delta_1) + \cdots + a_{2^n} w(\delta_{2^n}) \geq c$ can be written $-a_1 w(\delta_1) - \cdots - a_{2^n} w(\delta_{2^n}) > -c$. Thus, without loss of generality, we can assume that f'' is the conjunction of the following $2^n + r + s + 2$ formulas:

$$\begin{array}{rcl}
w(\delta_1) + \cdots + w(\delta_{2^n}) & \geq & 1 \\
-w(\delta_1) - \cdots - w(\delta_{2^n}) & \geq & -1 \\
w(\delta_1) & \geq & 0 \\
 & \cdots & \\
w(\delta_{2^n}) & \geq & 0 \\
a_{1,1} w(\delta_1) + \cdots + a_{1,2^n} w(\delta_{2^n}) & \geq & c_1 \\
 & \cdots & \\
a_{r,1} w(\delta_1) + \cdots + a_{r,2^n} w(\delta_{2^n}) & \geq & c_r \\
-a'_{1,1} w(\delta_1) - \cdots - a'_{1,2^n} w(\delta_{2^n}) & > & -c'_1 \\
 & \cdots & \\
-a'_{s,1} w(\delta_1) - \cdots - a'_{s,2^n} w(\delta_{2^n}) & > & -c'_s
\end{array} \tag{5}$$

Here the $a_{i,j}$'s and $a'_{i,j}$'s are some integers.

Since probabilities can be assigned independently to n-atoms (subject to the constraint that the sum of the probabilities equals one), it follows that f'' is satisfiable iff the following system of linear inequalities is satisfiable:

$$\begin{array}{rcl}
x_1 + \cdots + x_{2^n} & \geq & 1 \\
-x_1 - \cdots - x_{2^n} & \geq & -1 \\
x_1 & \geq & 0
\end{array}$$

$$
\begin{array}{rcl}
& \cdots & \\
x_{2^n} & \geq & 0 \\
a_{1,1}x_1 + \cdots + a_{1,2^n}x_{2^n} & \geq & c_1 \\
& \cdots & \\
a_{r,1}x_1 + \cdots + a_{r,2^n}x_{2^n} & \geq & c_r \\
-a'_{1,1}x_1 - \cdots - a'_{1,2^n}x_{2^n} & > & -c'_1 \\
& \cdots & \\
-a'_{s,1}x_1 - \cdots - a'_{s,2^n}x_{2^n} & > & -c'_s
\end{array}
\tag{6}
$$

As we have shown, the proof is concluded if we can show that f'' is satisfiable. Assume that f'' is unsatisfiable. Then the set of inequalities in (6) is unsatisfiable. So $\neg f''$ is an instance of the axiom Ineq. Since f'' is provably equivalent to f, it follows that $\neg f$ is provable, that is, f is inconsistent. This is a contradiction. ∎

Remark: When we originally started this investigation, we considered a language with weight formulas of the form $w(\varphi) \geq c$, without linear combinations. We extended to allow linear combinations for two reasons. The first is that the greater expressive power of linear combinations seems to be quite useful in practice (to say that φ is twice as probable as ψ, for example). The second is that we do not know a complete axiomatization for the weaker language. The fact that we can express linear combinations is crucial to the proof given above. ∎

2.3 Small model theorem

The proof of completeness presented in the previous subsection gives us a great deal of information. As we now show, the ideas of the proof let us also prove that a satisfiable formula is satisfiable in a small model.

Let us define the *length* $|f|$ of the weight formula f to be the number of symbols required to write f, where we count the length of each coefficient as 1. We have the following small model theorem.

Theorem 2.4: *Suppose f is a weight formula that is satisfied in some measurable probability structure. Then f is satisfied in a structure $(S, \mathcal{X}, \mu, \pi)$ with at most $|f|$ states where every set of states is measurable.*

Proof: We make use of the following lemma [Chv83, page 145].

Lemma 2.5: *If a system of r linear equalities and/or inequalities has a nonnegative solution, then it has a nonnegative solution with at most r entries positive.*

(This lemma is actually stated in [Chv83] in terms of equalities only, but the case stated above easily follows: if $x_1^*, \ldots, x_k^*$ is a solution to the system of inequalities, then we pass to the system where we replace each inequality $h(x_1, \ldots, x_k) \geq c$ or $h(x_1, \ldots, x_k) > c$ by the equality $h(x_1, \ldots, x_k) = h(x_1^*, \ldots, x_k^*)$.)

Returning to the proof of the small model theorem, as in the completeness proof, we can write f in disjunctive normal form. It is easy to show that each disjunct is a conjunction of at most $|f|-1$ basic weight formulas and their negations. Clearly, since f is satisfiable, one of the disjuncts, call it g, is satisfiable. Suppose that g is the conjunction of r basic weight formulas and s negations of basic weight formulas. Then just as in the completeness proof, we can find a system of equalities and inequalities of the following form, corresponding to g, which has a nonnegative solution.

$$\begin{array}{rcl} x_1 + \cdots + x_{2^n} & = & 1 \\ a_{1,1}x_1 + \cdots + a_{1,2^n}x_{2^n} & \geq & c_1 \\ & \ldots & \\ a_{r,1}x_1 + \cdots + a_{r,2^n}x_{2^n} & \geq & c_r \\ -a'_{1,1}x_1 - \cdots - a'_{1,2^n}x_{2^n} & > & -c'_1 \\ & \ldots & \\ -a'_{s,1}x_1 - \cdots - a'_{s,2^n}x_{2^n} & > & -c'_s \end{array} \qquad (7)$$

So by Lemma 2.5, we know that (7) has a solution x^*, where x^* is a vector with at most $r+s+1$ entries positive. Suppose $x_{i_1}^*, \ldots, x_{i_t}^*$ are the positive entries of the vector x^*, where $t \leq r+s+1$. We can now use this solution to construct a small structure satisfying f. Let $M = (S, \mathcal{X}, \mu, \pi)$ where S has t states, say $s_1, \ldots, s_t$, and $\mathcal{X}$ consists of all subsets of S. Let $\pi(s_j)$ be the truth assignment corresponding to the n-atom δ_{i_j} (and where $\pi(s_j)(p) = \mathbf{false}$ for every primitive proposition p not appearing in f). The measure μ is defined by letting $\mu(\{s_j\}) = x_{i_j}^*$, and extending μ by additivity. We leave it to the reader to check that $M \models f$. Since $t \leq r+s+1 \leq |f|$, the theorem follows. ∎

2.4 Decision procedure

When we consider decision procedures, we must take into account the length of coefficients. We define $\|f\|$ to be the length of the longest coefficient appearing in f, when written in binary. The *size* of a rational number a/b, where a and b are relatively prime, is defined to be the sum of lengths of a and b, when written in binary. We can then extend the small model theorem above as follows:

Theorem 2.6: *Suppose f is a weight formula that is satisfied in some measurable probability structure. Then f is satisfied in a structure $(S, \mathcal{X}, \mu, \pi)$ with at most $|f|$ states where every set of states is measurable, and where the probability assigned to each state is a rational number with size $O(|f|\,\|f\| + |f|\log(|f|))$.*

Theorem 2.6 follows from the proof of Theorem 2.4 and the following variation of Lemma 2.5, which can be proven using Cramer's rule and simple estimates on the size of the determinant.

Lemma 2.7: *If a system of r linear equalities and/or inequalities with integer coefficients each of length at most ℓ has a nonnegative solution, then it has a nonnegative solution with at most r entries positive, and where the size of each member of the solution is $O(r\ell + r\log(r))$.*

We need one more lemma, which says that in deciding whether a weight formula f is satisfied in a probability structure, we can ignore the primitive propositions that do not appear in f.

Lemma 2.8: *Let f be a weight formula. Let $M = (S, \mathcal{X}, \mu, \pi)$ and $M' = (S, \mathcal{X}, \mu, \pi')$ be probability structures with the same underlying probability space $(S, \mathcal{X}, \mu)$. Assume that $\pi(s)(p) = \pi'(s)(p)$ for every state s and every primitive proposition p that appears in f. Then $M \models f$ iff $M' \models f$.*

Proof: If f is a basic weight formula, then the result follows immediately from the definitions. Furthermore, this property is clearly preserved under Boolean combinations of formulas. ∎

We can now show that the problem of deciding satisfiability is NP-complete.

Theorem 2.9: *The problem of deciding whether a weight formula is satisfiable in a measurable probability structure is NP-complete.*

Proof: For the lower bound, observe that the propositional formula φ is satisfiable iff the weight formula $w(\varphi) > 0$ is satisfiable. For the upper bound, given a weight formula f, we guess a satisfying structure $M = (S, \mathcal{X}, \mu, \pi)$ for f with at most $|f|$ states such that the probability of each state is a rational number with size $O(|f|\,\|f\| + |f|\log(|f|))$, and where $\pi(s)(p) = \mathbf{false}$ for every state s and every primitive proposition p not appearing in f (by Lemma 2.8, the selection of $\pi(s)(p)$ when p does not appear in f is irrelevant). We verify that $M \models f$ as follows. For each term $w(\psi)$ of f, we create the set $Z_\psi \subseteq S$ of states that are in ψ^M by checking the truth assignment of each $s \in S$ and seeing whether this truth assignment makes ψ true; if so, then $s \in \psi^M$. We then replace each occurrence of $w(\psi)$ in f by $\sum_{s \in Z_\psi} \mu(s)$, and verify that the the resulting expression is true. ∎

3 The general (nonmeasurable) case

3.1 Semantics

In general, we may not want to assume that the set φ^M associated with the event φ is a measurable set. For example, as shown in [HT93], in an asynchronous system, the most natural set associated with an event such as "the most recent coin toss landed heads" will not in general be measurable. More generally, as discussed in [FH91], we may not want to assign a probability to all sets. The fact that we do not assign a probability to a set then becomes a measure of our uncertainty as to its precise probability; as we show below, all we can do is bound the probability from above and below.

If φ^M is not a measurable set, then $\mu(\varphi^M)$ is not well-defined. Therefore, we must give a different semantics to weight formulas than we did in the measurable case, where $\mu(\varphi^M)$ is well-defined for each formula φ. One natural semantics is obtained by considering the inner measure induced by the probability measure rather than the probability measure itself. Given a probability space $(S, \mathcal{X}, \mu)$ and an arbitrary subset A of S, define $\mu_*(A) = \sup\{\mu(B) \mid B \subseteq A \text{ and } B \in \mathcal{X}\}$. Then μ_* is called the *inner measure induced by* μ [Hal50]. Clearly μ_* is defined on all subsets of S, and $\mu_*(A) = \mu(A)$ if A is measurable. We now define

$$M \models a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) \geq c \text{ iff } a_1 \mu_*(\varphi_1^M) + \cdots + a_k \mu_*(\varphi_k^M) \geq c, \tag{8}$$

and extend this definition to all weight formulas just as before. Note that M satisfies $w(\varphi) \geq c$ iff there is a measurable set contained in φ^M whose probability is at least c. Of course, if M is a measurable probability structure, then $\mu_*(\varphi^M) = \mu(\varphi^M)$ for every formula φ, so this definition extends the one of the previous section.

We could just as easily have considered outer measures instead of inner measures. Given a probability space $(S, \mathcal{X}, \mu)$ and an arbitrary subset A of S, define $\mu^*(A) = \inf\{\mu(B) \mid A \subseteq B \text{ and } B \in \mathcal{X}\}$. Then μ^* is called the *outer measure induced by* μ [Hal50]. As with the innner measure, the outer measure is defined on all subsets of S. It is easy to show that $\mu_*(A) \leq \mu^*(A)$ for all $A \subseteq S$; moreover, if A is measurable, then $\mu^*(A) = \mu(A)$ if A is measurable. We can view the inner and outer measures as providing the best approximations from below and above to the probability of A. (See [FH91] for more discussion of this point.)

Since $\mu^*(A) = 1 - \mu_*(\overline{A})$, where as before, $\overline{A}$ is the complement of A, it follows that the inner and outer measures are expressible in terms of the other. We would get essentially the same results in this paper if we were to replace the inner measure μ_* in (8) by the outer measure μ^*.

If $M = (S, \mathcal{X}, \mu, \pi)$ is a probability structure, and if $\mathcal{X}'$ is a set of nonempty, disjoint subsets of S such that $\mathcal{X}$ consists precisely of all countable unions of members of $\mathcal{X}'$, then let us call $\mathcal{X}'$ a *basis* of M. We can think of $\mathcal{X}'$ as a "description" of the measurable sets. It is easy to see that if $\mathcal{X}$ is finite, then there is a basis. Moreover, whenever $\mathcal{X}$ has a basis, it is unique: it consists precisely of the minimal elements of $\mathcal{X}$ (the nonempty sets in $\mathcal{X}$ none of whose proper nonempty subsets are in $\mathcal{X}$). Note that if $\mathcal{X}$ has a basis, once we know the probability of every set in the basis, we can compute the probability of every measurable set by using countable additivity. Furthermore, the inner and outer measures can be defined in terms of the basis: the inner measure of A is the sum of the measures of the basis elements that are subsets of A, and the outer measure of A is the sum of the measures of the basis elements that intersect A.

3.2 Complete axiomatization

Allowing p^M to be nonmeasurable adds a number of complexities to both the axiomatization and decision procedure. Of the axioms for reasoning about weights, while W1 and W2 are still sound, it is easy to see that W3 is not. Finite additivity does not hold for inner measures. It is easy to see that we do not get a complete axiomatization simply by dropping W3. For one thing, we can no longer prove $w(false) = 0$. Thus, we add it as a new axiom:

W5. $w(false) = 0$

But even this is not enough. For example, superadditivity is sound for inner measures. That is, the following axiom is valid in all probability structures:

$$w(\varphi \wedge \psi) + w(\varphi \wedge \neg\psi) \leq w(\varphi). \tag{9}$$

But adding this axiom still does not give us completeness. For example, let $\delta_1, \delta_2, \delta_3$ be any three of the four distinct 2-atoms $p_1 \wedge p_2$, $p_1 \wedge \neg p_2$, $\neg p_1 \wedge p_2$, and $\neg p_1 \wedge \neg p_2$. Consider the following formula:

$$w(\delta_1 \vee \delta_2 \vee \delta_3) - w(\delta_1 \vee \delta_2) - w(\delta_1 \vee \delta_3) - w(\delta_2 \vee \delta_3) + w(\delta_1) + w(\delta_2) + w(\delta_3) \geq 0. \tag{10}$$

Although it is not obvious, we shall show that (10) is valid in probability structures. It also turns out that (10) does not follow from the other axioms and rules we just mentioned above; we demonstrate this after giving a few more definitions.

As before, we assume that $\delta_1, \ldots, \delta_{2^n}$ is a list of all the n-atoms in some fixed order. Define an *n-region* to be a disjunction of n-atoms where the n-atoms appear in the disjunct in order. For example, $\delta_2 \vee \delta_3$ is an n-region, while $\delta_3 \vee \delta_2$ is not. By insisting on this order, we ensure that there are exactly 2^{2^n} distinct n-regions (one corresponding to each subset of the n-atoms). We identify the empty disjunction with the formula *false*. As before, if n is understood or not important, we may refer to n-regions as simply *regions*. Note that every propositional formula all of whose primitive propositions are in $\{p_1, \ldots, p_n\}$ is equivalent to some n-region. Define a *size r region* to be a region that consists of precisely r disjuncts. We say that ρ' is a *subregion* of ρ if ρ and ρ' are n-regions, and each disjunct of ρ' is a disjunct of ρ. Thus, ρ' is a subregion of ρ iff $\rho' \Rightarrow \rho$ is a propositional tautology. We shall often write $\rho' \Rightarrow \rho$ for "ρ' is a subregion of ρ". A *size r subregion* of a region ρ is a size r region that is a subregion of ρ.

Remark: We can now show that (10) (where $\delta_1, \delta_2, \delta_3$ are distinct 2-atoms) does not follow from AX_{MEAS} with W3 replaced by W5 and the superadditivity axiom (9). Define a function ν whose domain is the set of propositional formulas, by letting $\nu(\varphi) = 1$ when at least one of the 2-regions $\delta_1 \vee \delta_2$, $\delta_1 \vee \delta_3$, or $\delta_2 \vee \delta_2$ logically implies φ. Let F be the set of basic weight formulas that are satisfied when ν plays the role of w (for example, a basic weight formula $a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) \geq c$ is in F iff $a_1 \nu(\varphi_1) + \cdots + a_k \nu(\varphi_k) \geq c$). Now (10) is not in F, since the left-hand side of (10) is $1 - 1 - 1 - 1 + 0 + 0 + 0$, which is

-2. However, it is easy to see that F contains every instance of every axiom of AX_{MEAS} other than W3, as well as W5 and every instance of the superadditivity axiom (9), and is closed under modus ponens. (The fact that every instance of (9) is in F follows from the fact that both $\varphi \wedge \psi$ and $\varphi \wedge \neg\psi$ cannot simultaneously be implied by 2-regions where two of $\delta_1, \delta_2, \delta_3$ are disjuncts.) Therefore, (10) does not follow from the system that results when we replace W3 by W5 and the superadditivity axiom. ∎

Now (10) is just one instance of the following new axiom:

W6. $\sum_{t=1}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t} w(\rho') \geq 0$, if ρ is a size r region and $r \geq 1$.

There is one such axiom for each n, each n-region ρ, and each r with $1 \leq r \leq 2^{2^n}$. It is instructive to look at a few special cases of W6. Let the size r region ρ be the disjunction $\delta_1 \vee \cdots \vee \delta_r$. If $r = 1$, then W6 says that $w(\delta_1) \geq 0$, which is a special case of axiom W1 (nonnegativity). If $r = 2$, then W6 says

$$w(\delta_1 \vee \delta_2) - w(\delta_1) - w(\delta_2) \geq 0,$$

which is a special case of superadditivity. If $r = 3$, we obtain (10) above.

3.2.1 Soundness of W6

In order to prove soundness of W6, we need to develop some machinery (which will prove to be useful again later for both our proof of completeness and for our decision procedure).

Let $M = (S, \mathcal{X}, \mu, \pi)$ be a probability structure. We shall find it useful to have a fixed standard ordering $\rho_1, \ldots, \rho_{2^{2^n}}$ of the n-regions, where every size r' region precedes every size r region if $r' < r$. In particular, if $\rho_{k'}$ is a proper subregion of ρ_k, then $k' < k$. We have identified ρ_1 with *false*; similarly, we can identify $\rho_{2^{2^n}}$ with *true*.

We now show that for every n-region ρ there is a measurable set $h(\rho) \subseteq \rho^M$ such that all of the $h(\rho)$'s are disjoint, and such that the inner measure of ρ^M is the sum of the measures of the sets $h(\rho')$ where ρ' is a subregion of ρ. In the measurable case (where each ρ^M is measurable), it is easy to see that we can take $h(\rho) = \rho^M$ if ρ is an n-atom, and $h(\rho) = \emptyset$ otherwise. Let $\mathcal{R}$ be the set of all 2^{2^n} distinct n-regions.

Proposition 3.1: *Let $M = (S, \mathcal{X}, \mu, \pi)$ be a probability structure. There is a function $h : \mathcal{R} \to \mathcal{X}$ such that if ρ is an n-region, then*

1. *$h(\rho) \subseteq \rho^M$.*
2. *If ρ and ρ' are distinct n-regions, then $h(\rho)$ and $h(\rho')$ are disjoint.*
3. *If $h(\rho) \subseteq (\rho')^M$ for some proper subregion ρ' of ρ, then $h(\rho) = \emptyset$.*

4. $\mu_*(\rho^M) = \sum_{\rho' \Rightarrow \rho} \mu(h(\rho'))$.

Proof: If M has a basis, then the proof is easy: We define $h(\rho)$ to be the union of all members of the basis that are subsets of ρ^M, but not of $(\rho')^M$ for any proper subregion ρ' of ρ. It is then easy to verify that the four conditions of the proposition hold.

We now give the proof in the general case (where M does not necessarily have a basis). This proof is more complicated.

We define $h(\rho_j)$ by induction on j, in such a way that

1. $h(\rho_j) \subseteq \rho_j^M$.
2. If $j' < j$, then $h(\rho_{j'})$ and $h(\rho_j)$ are disjoint.
3. If $j' < j$, and $h(\rho_j) \subseteq \rho_{j'}^M$, then $h(\rho_j) = \emptyset$.
4. $\mu_*(\rho_j^M) = \sum_{\rho' \Rightarrow \rho_j} \mu(h(\rho'))$.

Because our ordering ensures that if $\rho_{j'}$ is a subregion of ρ_j then $j' \leq j$, this is enough to prove the proposition.

To begin the induction, let us define $h(\rho_1)$ (that is, $h(\mathit{false})$) to be $\emptyset$. For the inductive step, assume that $h(\rho_j)$ has been defined whenever $j < k$, and that each of the four conditions above hold whenever $j < k$. We now define $h(\rho_k)$ so that the four conditions hold when $j = k$. Clearly $\mu_*(\rho_k^M) \geq \sum_{\rho' \Rightarrow \rho_k \text{ and } \rho' \neq \rho_k} \mu(h(\rho'))$, since $\cup_{\rho' \Rightarrow \rho_k \text{ and } \rho' \neq \rho_k} h(\rho')$ is a measurable set contained in ρ_k^M (because $h(\rho') \subseteq (\rho')^M \subseteq \rho_k^M$), with measure $\sum_{\rho' \Rightarrow \rho_k \text{ and } \rho' \neq \rho_k} \mu(h(\rho'))$ (because by inductive assumption the sets $h(\rho')$ where $\mu(h(\rho'))$ goes into this sum are pairwise disjoint). If $\mu_*(\rho_k^M) = \sum_{\rho' \Rightarrow \rho_k \text{ and } \rho' \neq \rho_k} \mu(h(\rho'))$, then we define $h(\rho_k)$ to be $\emptyset$. In this case, the four conditions clearly hold when $j = k$. If not, let W be a measurable subset of ρ_k^M such that $\mu_*(\rho_k^M) = \mu(W)$. Let $W' = W - \cup_{\rho' \Rightarrow \rho_k \text{ and } \rho' \neq \rho_k} h(\rho')$. Since by inductive assumption the sets $h(\rho')$ that go into this union are pairwise disjoint and are each subsets of ρ_k^M (because $h(\rho') \subseteq (\rho')^M \subseteq \rho_k^M$), it follows that $\mu_*(\rho_k^M) = \mu(W') + \sum_{\rho' \Rightarrow \rho_k} \mu(h(\rho'))$, and in particular $\mu(W') > 0$. Let $W'' = W' - \cup_{k' < k} h(\rho_{k'})$. Suppose we can show $\mu(W'') = \mu(W')$. It then follows that $\mu_*(\rho_k^M) = \mu(W'') + \sum_{\rho' \Rightarrow \rho_k} \mu(h(\rho'))$. We define $h(\rho_k)$ to be W''. Thus, condition (4) holds when $j = k$, and by construction, so do conditions (1) and (2). We now show that condition (3) holds. If not, find $k' < k$ such that $h(\rho_k) \subseteq \rho_{k'}^M$ and $h(\rho_k) \neq \emptyset$. By our construction, since $h(\rho_k) \neq \emptyset$, it follows that $h(\rho_k)$ has positive measure. By inductive assumption, $\mu_*(\rho_{k'}^M) = \sum_{\rho' \Rightarrow \rho_{k'}} \mu(h(\rho'))$. Now when $\rho' \Rightarrow \rho_{k'}$, it follows that $h(\rho') \subseteq (\rho')^M \subseteq \rho_{k'}^M$. Hence, if $T = \cup_{\rho' \Rightarrow \rho_{k'}} h(\rho')$, then T is a measurable set contained in $\rho_{k'}^M$ with measure equal to the inner measure of $\rho_{k'}^M$. However, $h(\rho_k)$ is a measurable set contained in $\rho_{k'}^M$ with positive measure, and which is disjoint from T. This is clearly impossible.

Thus it only remains to show that $\mu(W'') = \mu(W')$. If not, then $\mu(W' \cap h(\rho_{k'})) > 0$ for some $k' < k$. Let $Z = W' \cap h(\rho_{k'})$ (thus, $\mu(Z) > 0$), and let $\rho_{k''}$ be the n-region logically equivalent to $\rho_k \wedge \rho_{k'}$. Since $k' < k$, it follows that $\rho_{k''}$ is a proper subregion of ρ_k, and hence $k'' < k$. Since $W' \subseteq W \subseteq \rho_k^M$, and since $h(\rho_{k'}) \subseteq \rho_{k'}^M$, it follows that $Z = W' \cap h(\rho_{k'}) \subseteq \rho_k^M \cap \rho_{k'}^M = \rho_{k''}^M$ (where the final equality follows from the fact that $\rho_{k''}$ is logically equivalent to $\rho_k \wedge \rho_{k'}$). By construction, W' is disjoint from $h(\rho')$ for every subregion ρ' of ρ_k, and in particular for every subregion ρ' of $\rho_{k''}$ (since $\rho_{k''} \Rightarrow \rho_k$). Z is disjoint from $h(\rho')$ for every subregion ρ' of $\rho_{k''}$, since $Z \subseteq W'$. So Z is a subset of $\rho_{k''}^M$ with positive measure which is disjoint from $h(\rho')$ for every subregion ρ' of $\rho_{k''}$. But this contradicts our inductive assumption that $\mu_*(\rho_{k''}^M) = \sum_{\rho' \Rightarrow \rho_{k''}} \mu(h(\rho'))$. Thus we have shown that $\mu(W'') = \mu(W')$. ∎

In the fourth part of Proposition 3.1, we expressed inner measures of n-regions in terms of measures of certain measurable sets $h(\rho)$. We now show how to invert, to give the measure of a set $h(\rho)$ in terms of inner measures of various n-regions. We thereby obtain a formula expressing $\mu(h(\rho))$ in terms of the inner measure. As we shall see, axiom W6 says precisely that $\mu(h(\rho))$ is nonnegative. So W6 is sound, since probabilities are nonnegative. Since we shall "re-use" this inversion later, we shall state the next proposition abstractly, where we assume that we have vectors $(x_{\rho_1}, \ldots, x_{\rho_{2^{2^n}}})$ and $(y_{\rho_1}, \ldots, y_{\rho_{2^{2^n}}})$, each indexed by the n-regions. In our case of interest, y_ρ is $\mu(h(\rho))$, and x_ρ is $\mu_*(\rho^M)$.

Proposition 3.2: *Assume that $x_\rho = \sum_{\rho' \Rightarrow \rho} y_{\rho'}$, for each n-region ρ. Let ρ be a size r region. Then*

$$y_\rho = \sum_{t=0}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t} x_{\rho'}.$$

Proof: This proposition is simply a special case of Möbius inversion [Rot64] (see [Hal67, pp. 14–18]). Since the proof of Proposition 3.2 is fairly short, we now give it.

Replace each $x_{\rho'}$ in the right-hand side of the equality in the statement of the proposition by $\sum_{\rho'' \Rightarrow \rho'} y_{\rho''}$. We need only show that the result is precisely y_ρ (in particular, every other y_τ "cancels out"). Note that for every y_τ that is involved in this replacement, τ is a subregion of ρ (since it is a subregion of some ρ' that is a subregion of ρ).

First, y_ρ is contributed to the right-hand side precisely once, when $t = r$, by x_ρ. Now let τ be a size s subregion of ρ, where $0 \leq s \leq r-1$. We shall show that the total of the contributions of y_τ is zero (that is, the sum of the positive coefficients of the times it is added in plus the sum of the negative coefficients is zero). Thus, we count how many times y_τ is contributed by

$$\sum_{t=0}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t} x_{\rho'}. \tag{11}$$

If $t < s$, then y_τ is not contributed by the tth summand of (11). If $t \geq s$, then it is straightforward to see that τ is a subregion of $\binom{r-s}{t-s}$ distinct size t subregions of ρ, and so the total contribution by the tth summand of (11) is $(-1)^{r-t}\left(\begin{array}{c} r-s \\ t-s \end{array}\right)$. Therefore, the total contribution is

$$\sum_{t=s}^{r}(-1)^{r-t}\left(\begin{array}{c} r-s \\ t-s \end{array}\right). \tag{12}$$

This last expression is easily seen to be equal to $(-1)^{r-s}\sum_{u=0}^{r-s}(-1)^{u}\left(\begin{array}{c} r-s \\ u \end{array}\right)$. But this is $(-1)^{r-s}$ times the binomial expansion of $(1-1)^{r-s}$, and so is 0. ∎

Corollary 3.3: *Let ρ be a size r region. Then*

$$\mu(h(\rho)) = \sum_{t=0}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t}\mu_*((\rho')^M).$$

Proof: Let y_ρ be $\mu(h(\rho)$, and let x_ρ be $\mu_*(\rho^M)$. The corollary then follows from part (4) of Proposition 3.1, and Proposition 3.2. ∎

Corollary 3.4: *Let ρ be a size r region. Then*

$$\sum_{t=0}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t}\mu_*((\rho')^M) \geq 0.$$

Proof: This follows from Corollary 3.3 and from the fact that measures are nonnegative. ∎

Proposition 3.5: *Axiom W6 is sound.*

Proof: This follows from Corollary 3.4, where we ignore the $t=0$ term since $\mu_*(\emptyset)=0$. ∎

3.2.2 Completeness

Let AX be the axiom system that results when we replace W3 by W5 and W6. We now prove that AX is a complete axiomatization in the general case, where we allow nonmeasurable events. Thus we want to show that if a formula f is consistent, then f is satisfiable. As in the measurable case, we can easily reduce to the case that f is a conjunction of basic weight formulas and their negations. However, now we cannot rewrite subformulas of f in terms of subformulas involving atoms over the primitive propositions that appear in f, since this requires W3, which does not hold if we consider inner measures. Instead, we proceed as follows.

Let $p_1, \ldots, p_n$ include all of the primitive propositions that appear in f. Since every propositional formula using only the primitive propositions $p_1, \ldots, p_n$ is provably equivalent to some n-region ρ_i, it follows that f is provably equivalent to a formula f' where each conjunct of f' is of the form $a_1 w(\rho_1) + \cdots + a_{2^{2^n}} w(\rho_{2^{2^n}})$. As before, f' corresponds in a natural way to a system $Ax \geq b$, $A'x > b'$ of inequalities, where $x = (x_1, \ldots, x_{2^{2^n}})$ is a column vector whose entries correspond to the inner measures of the n-regions $\rho_1, \ldots, \rho_{2^{2^n}}$. If f is satisfiable in a probability structure (when w is interpreted as an inner measure induced by a probability measure), then $Ax \geq b, A'x > b'$ clearly has a solution. However, the converse is false. For example, if this system consists of a single formula, namely $-w(p) > 0$, then of course the inequality has a solution (such as $w(p) = -1$), but f is not satisfiable. Clearly, we need to add constraints that say that the inner measure of each n-region is nonnegative, and the inner measure of the region equivalent to the formula *false* (respectively *true*) is 0 (respectively 1).[4] But even this is not enough. For example, we can construct an example of a formula inconsistent with W6 (namely, the negation of (10)), where the corresponding system is satisfiable. We now show that by adding inequalities corresponding to W6, we can force the solution to act like the inner measure induced by some probability measure. Thus, we can still reduce satisfiability of f to the satisfiability of a system of linear inequalities.

Let P be the $2^{2^n} \times 2^{2^n}$ matrix of 0's and 1's such that if $x = (x_{\rho_1}, \ldots, x_{\rho_{2^{2^n}}})$ and $y = (y_{\rho_1}, \ldots, y_{\rho_{2^{2^n}}})$, then $x = Py$ describes the hypotheses of Proposition 3.2, that is, such that $x = Py$ "says" that $x_\rho = \sum_{\rho' \Rightarrow \rho} y_{\rho'}$, for each n-region ρ. Similarly, let N be the $2^{2^n} \times 2^{2^n}$ matrix of 0's, 1's, and -1's such that $y = Nx$ describes the conclusions of Proposition 3.2, that is, such that $y = Nx$ "says" that

$$y_\rho = \sum_{t=0}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t} x_{\rho'},$$

for each n-region ρ. We shall make use of the following technical properties of the matrix N:

Lemma 3.6:

1. *The matrix N is invertible.*

2. $\sum_{i=1}^{2^{2^n}} (Nx)_i = x_{2^{2^n}}$ *for each vector x of length 2^{2^n}.*

Proof: The proof of Proposition 3.2 shows that whenever x and y are vectors where $x = Py$, then $y = Nx$. Therefore, P is invertible, with inverse N. Hence, N is invertible. This proves part (1). As for part (2), let x be an arbitrary vector of length 2^{2^n}, and let $y = Nx$. Since N and P are inverses, it follows that $x = Py$. Now $\sum_{i=1}^{2^{2^n}} (Nx)_i =$

[4] Actually, when we speak about the inner measure of an n-region ρ, we really mean the inner measure of the set ρ^M that corresponds to the n-region ρ.

$\sum_{i=1}^{2^{2^n}} y_i$. But it is easy to see that the last row of $x = Py$ says that $x_{2^{2^n}} = \sum_{i=1}^{2^{2^n}} y_i$. So $\sum_{i=1}^{2^{2^n}} (Nx)_i = x_{2^{2^n}}$, as desired. ∎

We can now show how to reduce satisfiability of f to the satisfiability of a system of linear inequalities. Assume that f is a conjunction of basic weight formulas and negations of basic weight formulas. Define $\widehat{f}$ to be the system $Ax \geq b, A'x > b'$ of inequalities that correspond to f.

Theorem 3.7: *Let f be a conjunction of basic weight formulas and negations of basic weight formulas. Then f is satisfied in some probability structure iff there is a solution to the system $\widehat{f}, x_1 = 0, x_{2^{2^n}} = 1, Nx \geq 0$.*

Proof: Assume first that f is satisfiable. Thus, assume that $(S, \mathcal{X}, \mu, \pi) \models f$. Define x^* by letting $x_i^* = \mu_*(\rho_i^M)$, for $1 \leq i \leq 2^{2^n}$. Clearly x^* is a solution to the system given in the statement of the theorem, where $x_1^* = 0$ holds since $\mu_*(\emptyset) = 0$, $x_{2^{2^n}}^* = 1$ holds since $\mu_*(S) = 1$, and $Nx^* \geq 0$ holds by Corollary 3.4.

Conversely, let x^* satisfy the system given in the statement of the theorem. We now construct a probability structure $M = (S, \mathcal{X}, \mu, \pi)$ such that $M \models f$. This, of course, is sufficient to prove the theorem. Assume that $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in f. For each of the 2^n n-atoms δ and each of the 2^{2^n} n-regions ρ, if $\delta \Rightarrow \rho$ (that is, if δ is one of the n-atoms whose disjunction is ρ), then let $s_{\delta,\rho}$ be a distinct state. We let S consist of these states $s_{\delta,\rho}$ (of which there are less than $2^n 2^{2^n}$). Intuitively, $s_{\delta,\rho}$ will turn out to be a member of $h(\rho)$ where the atom δ is satisfied. For each n-region ρ, let H_ρ be the set of all states $s_{\delta,\rho}$. Note that H_ρ and $H_{\rho'}$ are disjoint if ρ and ρ' are distinct. The measurable sets (the members of $\mathcal{X}$) are defined to be all possible unions of subsets of $\{H_{\rho_1}, \ldots, H_{\rho_{2^{2^n}}}\}$. If J is a subset of $\{1, \ldots, 2^{2^n}\}$, then the complement of $\cup_{j \in J} H_j$ is $\cup_{j \notin J} H_j$. Thus, $\mathcal{X}$ is closed under complementation. Since also $\mathcal{X}$ clearly contains the empty set and is closed under union, it follows that $\mathcal{X}$ is a σ-algebra of sets. As we shall see, H_ρ will play the role of $h(\rho)$ in Proposition 3.1. The measure μ is defined by first letting $\mu(H_{\rho_i})$ (where ρ_i is the ith n-region) be the ith entry of Nx^* (which is nonnegative by assumption), and then extending μ to $\mathcal{X}$ by additivity. Note that the only H_{ρ_i} that is empty is H_{ρ_1}, and that $\mu(H_{\rho_1})$ is correctly assigned the value 0, since the first entry of Nx^* is x_1^*, which equals 0, since $x_1 = 0$ is an equality of the system that x^* is a solution to. By additivity, $\mu(S)$ (where S is the whole space) is assigned the value $\sum_{i=1}^{2^{2^n}} \mu(H_{\rho_i}) = \sum_{i=1}^{2^{2^n}} (Nx^*)_i$, which equals $x_{2^{2^n}}^*$ by Lemma 3.6, which equals 1, since $x_{2^{2^n}} = 1$ is an equality of the system that x^* is a solution to. Thus, μ is indeed a probability measure.

We define π by letting $\pi(s_{\delta,\rho})(p_i) = \textbf{true}$ iff $\delta \Rightarrow p_i$, for each primitive proposition p_i. It is straightforward to verify that if δ is an n-atom, then δ^M is the set of all states $s_{\delta,\rho}$, and if ρ is an n-region, then ρ^M is the set of all states $s_{\delta,\rho'}$ where $\delta \Rightarrow \rho$.

Recall that $\mathcal{R}$ is the set of all n-regions. For each $\rho \in \mathcal{R}$, define $h(\rho) = H_\rho$. We now show that the four conditions of Proposition 3.1 hold.

1. $h(\rho) \subseteq \rho^M$: This holds because $h(\rho) = H_\rho = \{s_{\delta,\rho} | \delta \Rightarrow \rho\} \subseteq \{s_{\delta,\rho'} | \delta \Rightarrow \rho\} = \rho^M$.

2. If ρ and ρ' are distinct n-regions, then $h(\rho)$ and $h(\rho')$ are disjoint: This holds because if ρ and ρ' are distinct, then $h(\rho) = \{s_{\delta,\rho} | \delta \Rightarrow \rho\}$, which is disjoint from $h(\rho') = \{s_{\delta,\rho'} | \delta \Rightarrow \rho'\}$.

3. If $h(\rho) \subseteq (\rho')^M$ for some proper subregion ρ' of ρ, then $h(\rho) = \emptyset$: We shall actually prove the stronger result that if $h(\rho) \subseteq (\rho')^M$, then $\rho \Rightarrow \rho'$. If $\rho \not\Rightarrow \rho'$, then let δ be an n-atom of ρ that is not an n-atom of ρ'. Then $s_{\delta,\rho} \in h(\rho)$, but $s_{\delta,\rho} \notin (\rho')^M$. So $h(\rho) \not\subseteq (\rho')^M$.

4. $\mu_*(\rho^M) = \sum_{\rho' \Rightarrow \rho} \mu(h(\rho'))$: We just showed (with the roles of ρ and ρ' reversed) that if $h(\rho') \subseteq \rho^M$, then $\rho' \Rightarrow \rho$. Also, if $\rho' \Rightarrow \rho$, then $h(\rho') \subseteq \rho'^M$ by condition (1) above, so $h(\rho') \subseteq \rho^M$. Therefore, the sets $h(\rho')$ that are subsets of ρ^M are precisely those where $\rho' \Rightarrow \rho$. By construction, every measurable set is the disjoint union of sets of the form $h(\rho')$. Hence, $\cup_{\rho' \Rightarrow \rho} h(\rho')$ is the largest measurable set contained in ρ^M. Therefore, by disjointness of the sets $h(\rho')$, it follows that $\mu_*(\rho^M) = \sum_{\rho' \Rightarrow \rho} \mu(h(\rho'))$.

Let $y^* = Nx^*$. Then, by construction, the ith entry of y^* is $\mu(H_{\rho_i}) = \mu(h(\rho_i))$, for $i = 1, \ldots, 2^{2^n}$. Define a vector z^* of length 2^{2^n} by letting the ith entry be $\mu_*(\rho_i^M)$. Since, as we just showed, $\mu_*(\rho^M) = \sum_{\rho' \Rightarrow \rho} \mu(h(\rho'))$, it follows from Proposition 3.2 that $y^* = Nz^*$. By Lemma 3.6, the matrix N is invertible. So, since $y^* = Nx^*$ and $y^* = Nz^*$, it follows that $x^* = z^*$. But x^* satisfies the inequalities $\widehat{f}$. Since $x^* = z^*$, it follows that x^* is the vector of inner measures. So $M \models f$, as desired. ∎

Theorem 3.8: *AX is a sound and complete axiom system with respect to probability structures.*

Proof: We proved soundness of W6 in Proposition 3.5 (the other axioms are clearly sound). As for completeness, assume that formula f is unsatisfiable; we must show that f is inconsistent. As we noted, we reduce as before to the case that f is a conjunction of basic weight formulas and their negations. By Theorem 3.7, since f is unsatisfiable, the system $Ax \geq b, A'x > b', x_1 = 0, x_{2^{2^n}} = 1, Nx \geq 0$ of Theorem 3.7 has no solution. Now the formulas corresponding to $x_1 = 0, x_{2^{2^n}} = 1$, and $Nx \geq 0$ are provable; this is because the formulas corresponding to $x_1 = 0$ and $x_{2^{2^n}} = 1$ are axioms W5 and W2, and because the formulas corresponding to $Nx \geq 0$ follow from axiom W6. We now conclude by making use of Ineq as before. ∎

The observant reader may have noticed that the proof of Theorem 3.8 does not make use of axiom W1. Hence, the axiom system that results by removing axiom W1 from AX is still complete. This is perhaps not too surprising. We noted earlier that W1 in the case of atoms (i.e., $w(\delta) \geq 0$ for δ an atom) is a special case of W6. With a little more work, we can prove W1 for all formulas φ from the other axioms.

3.3 Small model theorem

It follows from the construction in the proof of Theorem 3.7 that a small model theorem again holds. In particular, it follows that if f is a weight formula and if f is satisfiable in the nonmeasurable case, then f is satisfied in a structure with less than $2^n 2^{2^n}$ states. Indeed, it is easy to see from our proof that if f involves only k primitive propositions, and f is satisfiable in the nonmeasurable case, then f is satisfied in a structure with less than $2^k 2^{2^k}$ states. However, we can do much better than this, as we shall show.

The remaining results of Section 3 were obtained jointly with Moshe Vardi.

Theorem 3.9: *Let f be a weight formula that is satisfied in some probability structure. Then it is satisfied in a structure with at most $|f|^2$ states, with a basis of size at most $|f|$.*

Proof: By considering a disjunct of the disjunctive normal form of f, we can assume as before that f is a conjunction of basic weight formulas and their negations. Let us assume that f is a conjunction of r such inequalities altogether.

If $M = (S, \mathcal{X}, \mu, \pi)$ is a probability structure, let us define an *extension of M* to be a tuple $E = (S, \mathcal{X}, \mu, \pi, h)$ where h is a function as in Proposition 3.1. In particular, $h(\rho)$ is a measurable set for each $\rho \in \mathcal{R}$. We call E an *extended probability structure*. By Proposition 3.1, for every probability structure M there is an extended probability structure E that is an extension of M. If $\rho \in \mathcal{R}$ and E is an extension of M, then we may write ρ^E for ρ^M. Define an *h-term* to be an expression of the form $a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) + a'_1 H(\varphi'_1) + \cdots + a'_{k'} H(\varphi_{k'})$, where $\varphi_1, \ldots, \varphi_k, \varphi'_1, \ldots, \varphi'_{k'}$ are propositional formulas, $a_1, \ldots, a_k, a'_1, \ldots, a'_{k'}$ are integers, and $k + k' \geq 1$. An *h-basic weight formula* is a statement of the form $t \geq c$, where t is an h-term and c is an integer. If $E = (S, \mathcal{X}, \mu, \pi, h)$ is an extension of M we define

$$
\begin{aligned}
&E \models a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) + a'_1 H(\varphi'_1) + \cdots + a'_{k'} H(\varphi_{k'}) \geq c \text{ iff} \\
&a_1 \mu_*(\varphi_1^M) + \cdots + a_k \mu_*(\varphi_k^M) + a'_1 \mu(h(\varphi_1)) + \cdots + a'_{k'} \mu(h(\varphi_k)) \geq c.
\end{aligned}
$$

Thus, $H(\rho)$ represents $\mu(h(\rho))$. We construct *h-weight formulas* from h-basic weight formulas, and make the same conventions on abbreviations ("$>$", etc.), as we did with weight formulas.

Again, assume that $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in f. Let f' be obtained from f by replacing each "$w(\varphi)$" that appears in f by "$w(\rho)$", where ρ is the n-region equivalent to φ. Then f and f' are equivalent. By part (4) of Proposition 3.1, we can "substitute" $\sum_{\rho' \Rightarrow \rho} H(\rho')$ for $w(\rho)$ in f' for each n-region ρ, to obtain an equivalent h-weight formula f'' (which is a conjunction of basic h-weight formulas and their negations). Since f is a conjunction of r inequalities, so is f''.

Consider now the system corresponding to the r inequalities that are the conjuncts of f'', along with the equality $\sum_\rho H(\rho) = 1$. Since f, and hence f'', is satisfiable, this system has a nonnegative solution. Therefore, we see from Lemma 2.5 that this system has a nonnegative solution with at most $r+1$ of the $H(\rho)$'s positive. Let $\mathcal{N}$ be the set of n-regions $\rho \in \mathcal{R}$ such that $H(\rho)$ is positive in this solution; thus, $|\mathcal{N}| \leq r+1$. Assume that the solution is given by $H(\rho) = c_\rho$ for $\rho \in \mathcal{N}$, and $H(\rho) = 0$ if $\rho \notin \mathcal{N}$. Note in particular that $\sum_{\rho \in \mathcal{N}} c_\rho = 1$, and that each c_ρ is nonnegative.

Let $\mathcal{T}$ be the set of all n-regions ρ such that $w(\rho)$ appears in f. Note that $r+|\mathcal{T}|+1 \leq |f|$. Recall that $At_n(\rho)$ consists of all the n-atoms δ such that $\delta \Rightarrow \rho$ is a propositional tautology. Thus ρ is equivalent to the disjunction of the n-atoms in $At_n(\rho)$. For each n-region $\rho \in \mathcal{N}$ and each n-region $\tau \in \mathcal{N} \cup \mathcal{T}$ such that $At_n(\rho) \not\subseteq At_n(\tau)$, select an n-atom $\omega_{\rho,\tau}$ such that $\omega_{\rho,\tau} \Rightarrow \rho$ but $\omega_{\rho,\tau} \not\Rightarrow \tau$. For each n-region $\rho \in \mathcal{N}$, let ρ^* be the n-region whose n-atoms are precisely all such n-atoms $\omega_{\rho,\tau}$. So ρ^* is a subregion of ρ; moreover, if ρ^* is a subregion of $\tau \in \mathcal{N} \cup \mathcal{T}$, then ρ is a subregion of τ. Let $\mathcal{N}^* = \{\rho^* | \rho \in \mathcal{N}\}$. By construction, if ρ and ρ' are distinct members of $\mathcal{N}$, then $\rho^* \neq (\rho')^*$. Now $\mathcal{N}^*$ contains $|\mathcal{N}| \leq r+1 \leq |f|$ members, and if $\rho^* \in \mathcal{N}^*$, then ρ^* contains at most $r + |\mathcal{T}| \leq |f|$ n-atoms.

We know from part (4) of Proposition 3.1 that in each extended probability structure it is the case that $w(\rho) = \sum_{\rho' \Rightarrow \rho} H(\rho')$ is satisfied. Let $d_\rho = \sum_{\{\rho' \,|\, \rho' \Rightarrow \rho \text{ and } \rho' \in \mathcal{N}\}} c_{\rho'}$, for each n-region $\rho \in \mathcal{T}$. Now f'', and hence f, is satisfied when $H(\rho) = c_\rho$ for $\rho \in \mathcal{N}$ and $H(\rho) = 0$ if $\rho \notin \mathcal{N}$. Therefore, f is satisfied when $w(\rho) = d_\rho$ for each $\rho \in \mathcal{T}$.

We now show that if $\rho \in \mathcal{T}$, then $\{\rho' \,|\, \rho' \Rightarrow \rho \text{ and } \rho' \in \mathcal{N}\} = \{\rho' \,|\, (\rho')^* \Rightarrow \rho \text{ and } (\rho')^* \in \mathcal{N}^*\}$. First, $\rho' \in \mathcal{N}$ iff $(\rho')^* \in \mathcal{N}^*$, by definition. We then have $\{\rho' \,|\, \rho' \Rightarrow \rho \text{ and } \rho' \in \mathcal{N}\} \subseteq \{\rho' \,|\, (\rho')^* \Rightarrow \rho \text{ and } (\rho')^* \in \mathcal{N}^*\}$ since if ρ' is a subregion of ρ (i.e., $\rho' \Rightarrow \rho$), then $(\rho')^*$ is a subregion of ρ, because $(\rho')^*$ is a subregion of ρ', which is a subregion of ρ. Conversely, if $(\rho')^*$ is a subregion of ρ, then ρ' is a subregion of ρ because $\rho \in \mathcal{T}$ (this was shown above).

We now prove that if an extended probability structure satisfies $H(\rho^*) = c_\rho$ if $\rho^* \in \mathcal{N}^*$, and $H(\tau) = 0$ if $\tau \notin \mathcal{N}^*$, then it also satisfies f. In such an extended probability structure, $w(\rho)$ takes on the value $\sum_{\{(\rho')^* | (\rho')^* \Rightarrow \rho \text{ and } (\rho')^* \in \mathcal{N}^*\}} c_{\rho'}$, which equals $\sum_{\{\rho' | (\rho')^* \Rightarrow \rho \text{ and } (\rho')^* \in \mathcal{N}^*\}} c_{\rho'}$ (since * gives a 1-1 correspondence between $\mathcal{N}$ and $\mathcal{N}^*$), which, from what we just showed, equals $\sum_{\{\rho' | \rho' \Rightarrow \rho \text{ and } \rho' \in \mathcal{N}\}} c_{\rho'}$, which by definition equals d_ρ. But we showed that f is satisfied when $w(\rho) = d_\rho$ for each $\rho \in \mathcal{T}$.

Therefore, we need only construct an extended probability structure $E = (S, \mathcal{X}, \mu, \pi, h)$ (which extends a structure M) that satisfies $H(\rho^*) = c_\rho$ if $\rho^* \in \mathcal{N}^*$, and $H(\tau) = 0$ if $\tau \notin \mathcal{N}^*$, such that E has at most $|f|^2$ states and has a basis of size at most $|f|$. Our construction is similar to that in the proof of Theorem 3.7. For each $\rho^* \in \mathcal{N}^*$ and each $\delta \in At_n(\rho^*)$, let s_{δ,ρ^*} be a distinct state. Let S, the set of states of E, be the set of all such states s_{δ,ρ^*}. Since $\mathcal{N}^*$ contains at most $|f|$ members and $At_n(\rho^*)$ contains at most $|f|$ n-atoms for each $\rho^* \in \mathcal{N}^*$, it follows that S contains at most $|f|^2$ states. We shall define π and h in such a way that s_{δ,ρ^*} is a state in δ^M and in $h(\rho^*)$. Define π by letting $\pi(s_{\delta,\rho^*})(p) = \textbf{true}$ iff $\delta \Rightarrow p$ (intuitively, iff the primitive proposition p is true in the n-atom δ). Similarly to before, it is straightforward to verify that if δ is an n-atom, then δ^M is the set of all states s_{δ,ρ^*}, and if τ is an n-region, then τ^M is the set of all states

s_{δ,ρ^*} where $\delta \in At_n(\tau)$. For each n-region $\tau \in \mathcal{R}$, define h by letting $h(\tau)$ be the set of all states $s_{\delta,\tau}$ (in particular, if $\tau \notin \mathcal{N}^*$, then $h(\tau) = \emptyset$). The measurable sets (the members of $\mathcal{X}$) are defined to be all disjoint unions of sets $h(\tau)$. (It is easy to verify that the sets $h(\tau)$ and $h(\tau')$ are disjoint if τ and τ' are distinct, and that the union of all sets $h(\tau)$ is the whole space S.) Finally, μ is defined by letting $\mu(h(\rho^*)) = c_\rho$, and extending μ by additivity. It is easy to see that μ is a measure, because the $h(\rho^*)$'s are nonempty, disjoint sets whose union is all of S, and $\sum_{\rho^* \in \mathcal{N}^*} \mu(h(\rho^*)) = \sum_{\rho \in \mathcal{N}} c_\rho = 1$. The collection of sets $h(\rho^*)$, of which there are $|\mathcal{N}^*| \leq |f|$, is a basis. Clearly, this construction has the desired properties. ∎

3.4 Decision procedure

As before, we can modify the proof of the small model theorem to obtain the following:

Theorem 3.10: *Let f be a weight formula that is satisfied in some probability structure. Then f is satisfied in a structure with at most $|f|^2$ states, with a basis of size at most $|f|$, where the probability assigned to each member of the basis is a rational number with size $O(|f|\,\|f\| + |f|\,\log(|f|))$.*

Once again, this gives us a decision procedure. Somewhat surprisingly, the complexity is no worse than it is in the measurable case.

Theorem 3.11: *The problem of deciding whether a weight formula is satisfiable with respect to general probability structures case is NP-complete.*

Proof: For the lower bound, again the propositional formula φ is satisfiable iff the weight formula $w(\varphi) > 0$ is satisfiable. For the upper bound, given a weight formula f, we guess a satisfying structure M for f as in Theorem 3.10, where the way we represent the measurable sets and the measure in our guess is through a basis and a measure on each member of the basis. Thus, we guess a structure $M = (S, \mathcal{X}, \mu, \pi)$ with at most $|f|^2$ states and a basis B of size at most $|f|$, such that the probability of each member of B is a rational number with size $O(|f|\,\|f\| + |f|\log(|f|))$, and where $\pi(s)(p) = \textbf{false}$ for every state s and every primitive proposition p not appearing in f (again, by Lemma 2.8, the selection of $\pi(s)(p)$ when p does not appear in f is irrelevant). We verify that $M \models f$ as follows. Let $w(\psi)$ be an arbitrary term of f. We define $B_\psi \subseteq B$, by letting B_ψ consist of all $W \in B$ such that the truth assignment $\pi(w)$ of each $w \in W$ makes ψ true. We then replace each occurrence of $w(\psi)$ in f by $\sum_{W \in B_\psi} \mu(W)$, and verify that the resulting expression is true. ∎

4 Reasoning about linear inequalities

In this section, we consider more carefully the logic for reasoning about linear inequalities. We provide a sound and complete axiomatization, and consider decision procedures. The reader interested only in reasoning about probability can skip this section with no loss of continuity.

4.1 Complete axiomatization

In this subsection we give a sound and complete axiomatization for reasoning about linear inequalities, where now the language consists of inequality formulas (as defined in the discussion of the axiom Ineq in Section 2). The system has two parts, the first of which deals with propositional reasoning, and the second of which deals directly with reasoning about linear inequalities.

Propositional reasoning:

Taut. All instances of propositional tautologies[5]

MP. From f and $f \Rightarrow g$ infer g (modus ponens)

Reasoning about linear inequalities:

I1. $x \geq x$ (identity)

I2. $(a_1x_1 + \cdots + a_kx_k \geq c) \Leftrightarrow (a_1x_1 + \cdots + a_kx_k + 0x_{k+1} \geq c)$ (adding and deleting 0 terms)

I3. $(a_1x_1 + \cdots + a_kx_k \geq c) \Rightarrow (a_{j_1}x_{j_1} + \cdots + a_{j_k}x_{j_k} \geq c)$, if $j_1, \ldots, j_k$ is a permutation of $1, \ldots, k$ (permutation)

I4. $(a_1x_1 + \cdots + a_kx_k \geq c) \wedge (a'_1x_1 + \cdots + a'_kx_k \geq c') \Rightarrow (a_1 + a'_1)x_1 + \cdots + (a_k + a'_k)x_k \geq (c + c')$ (addition of coefficients)

I5. $(a_1x_1 + \cdots + a_kx_k \geq c) \Leftrightarrow (da_1x_1 + \cdots + da_kx_k \geq dc)$ if $d > 0$ (multiplication and division of nonzero coefficients)

I6. $(t \geq c) \vee (t \leq c)$ if t is a term (dichotomy)

I7. $(t \geq c) \Rightarrow (t > d)$ if t is a term and $c > d$ (monotonicity)

[5] For example, if f is an inequality formula, then $f \vee \neg f$ is an instance.

It is helpful to clarify what we mean when we say that we can replace the axiom Ineq by this axiom system in our axiomatizations AX and AX_{MEAS} of the previous sections. We of course already have the axiom and rule for propositional reasoning (Taut and MP) in AX and AX_{MEAS}, so we can simply replace Ineq by axioms I1-I7. As we noted earlier, this means that we replace each variable x_i by $w(\varphi_i)$, where φ_i is an arbitrary propositional formula. For example, the axiom I3 would become:

$$(a_1 w(\varphi_1) + \cdots + a_k w(\varphi_k) \geq c) \wedge (a_1' w(\varphi_1) + \cdots + a_k' w(\varphi_k) \geq c') \Rightarrow \\ (a_1 + a_1')w(\varphi_1) + \cdots + (a_k + a_k')w(\varphi_k) \geq (c + c').$$

We note also that the axiom I1 (which becomes $w(\varphi) \geq w(\varphi)$) is redundant in AX and AX_{MEAS}, because it is a special case of axiom W4 (which says that $w(\varphi) = w(\psi)$ if $\varphi \equiv \psi$ is a propositional tautology).

We call the axiom system described above AX_{INEQ}. In this section, we show that AX_{INEQ} is sound and complete.

In order to see an example of how the axioms operate, we show that the following formula is provable:

$$(a_1 x_1 + a_1' x_1 + a_2 x_2 + \cdots + a_n x_n \geq c) \Leftrightarrow ((a_1 + a_1')x_1 + a_2 x_2 + \cdots + a_n x_n \geq c). \quad (13)$$

This formula, which is clearly valid, tells us that it is possible to add coefficients corresponding to a single variable, and thereby reduce each inequality to one where no variable appears twice. We give the proof in fairly painful detail, since we shall want to make use of some techniques from the proof again later. We shall make use of the provability of (13) in our proof of completeness of AX_{INEQ}.

Lemma 4.1: *The formula (13) is provable from AX_{INEQ}.*

Proof: In the semi-formal proof below, we again write PR as an abbreviation for "propositional reasoning", i.e., using a combination of Taut and MP. We shall show that the right implication (the formula that results by replacing "$\Leftrightarrow$" in formula (13) by "$\Rightarrow$") is provable from AX_{INEQ}. The proof that the left implication holds is very similar, and is left to the reader. By putting these proofs together and using PR, it follows that formula (13) is provable.

If the coefficient $a_1 = 0$ in (13), then the result follows from I2, I3, and propositional reasoning. Thus, we assume $a_1 \neq 0$ in our proof.

1. $x_1 - x_1 \geq 0$ (I1)
2. $a_1 x_1 - a_1 x_1 \geq 0$ (this follows from 1, I5 and PR if $a_1 > 0$; if $a_1 < 0$, then instead of multiplying by a_1, we multiply by $-a_1$, and get the same result after using the permutation axiom I3 and PR)
3. $a_1 x_1 - a_1 x_1 + 0x_1 \geq 0$ (2, I2, PR)

4. $a'_1x_1 - a'_1x_1 + 0x_1 \geq 0$ (by the same derivation as for 3)

5. $a'_1x_1 + 0x_1 - a'_1x_1 \geq 0$ (4, I3, PR)

6. $(a_1 + a'_1)x_1 - a_1x_1 - a'_1x_1 \geq 0$ (3, 5, I4, PR)

7. $-a_1x_1 - a'_1x_1 + (a_1 + a'_1)x_1 + 0x_2 + \cdots + 0x_n \geq 0$ (6, I2, I3, PR)

8. $(a_1x_1 + a'_1x_1 + a_2x_2 + \cdots + a_nx_n \geq c) \Rightarrow (a_1x_1 + a'_1x_1 + 0x_1 + a_2x_2 + \cdots + a_nx_n \geq c)$ (I2, I3, PR)

9. $(a_1x_1 + a'_1x_1 + 0x_1 + a_2x_2 + \cdots + a_nx_n \geq c) \wedge (-a_1x_1 - a'_1x_1 + (a_1 + a'_1)x_1 + 0x_2 + \cdots + 0x_n \geq 0) \Rightarrow (0x_1 + 0x_1 + (a_1 + a'_1)x_1 + a_2x_2 + \cdots + a_nx_n \geq c)$ (I4)

10. $(0x_1 + 0x_1 + (a_1 + a'_1)x_1 + a_2x_2 + \cdots + a_nx_n \geq c) \Rightarrow ((a_1 + a'_1)x_1 + a_2x_2 + \cdots + a_nx_n \geq c)$ (I2, I3, PR)

11. $(a_1x_1 + a'_1x_1 + a_2x_2 + \cdots + a_nx_n \geq c) \Rightarrow ((a_1 + a'_1)x_1 + a_2x_2 + \cdots + a_nx_n \geq c)$ (7, 8, 9, 10, PR) ∎

For the sake of our proof of completeness of AX$_{INEQ}$, we need also to show that the following formula is provable:

$$0x_1 + \cdots + 0x_n \geq 0 \tag{14}$$

This formula can be viewed as saying that the right implication of axiom I5 holds when $d = 0$.

Lemma 4.2: *The formula (14) is provable from AX_{INEQ}.*

Proof: This time we shall give a more informal proof of provability. From I1, we obtain $x_1 \geq x_1$, that is, $x_1 - x_1 \geq 0$. By permutation (axiom I3), we obtain also $-x_1 + x_1 \geq 0$. If we add these latter two inequalities by I4, and delete a 0 term by I2, we obtain $0x_1 \geq 0$. By using I2 to add 0 terms, we obtain $0x_1 + \cdots + 0x_n \geq 0$, as desired. ∎

Theorem 4.3: *AX_{INEQ} is sound and complete.*

Proof: It is easy to see that each axiom is valid. To prove completeness, we show that if f is consistent then f is satisfiable. So suppose that f is consistent.

As in the proof of Theorem 2.2, we first reduce f to a canonical form. Let $g_1 \vee \cdots \vee g_r$ be a disjunctive normal form expression for f (where each g_i is a conjunction of basic inequality formulas and their negations). Using propositional reasoning, we can show that f is provably equivalent to this disjunction. As in the proof of Theorem 2.2, since f is consistent, so is some g_i. Moreover, any assignment satisfying g_i also satisfies f. Thus, without loss of generality, we can restrict attention to a formula f that is a conjunction of basic inequality formulas and their negations. The negation of a basic inequality formula $a_1x_1 + \cdots + a_nx_n \geq c$ can be written $-a_1x_1 - \cdots - a_nx_n > -c$. Thus, we can think of both basic inequality formulas and their negations as inequalities. By making use of Lemma 4.1, we can assume that no variable appears twice in any inequality. By making use of axiom I2 to add 0 terms and I3 to permute if necessary, we can assume that all of the inequalities contain the same variables, in the same order, with no variable repeated in any given inequality. Thus, without loss of generality, we can assume that f is the conjunction of the following $r + s$ formulas, where $x_1, \ldots, x_n$ are distinct variables:

$$\begin{array}{rcl} a_{1,1}x_1 + \cdots + a_{1,n}x_n & \geq & c_1 \\ & \cdots & \\ a_{r,1}x_1 + \cdots + a_{r,n}x_n & \geq & c_r \\ -a'_{1,1}x_1 - \cdots - a'_{1,n}x_n & > & -c'_1 \\ & \cdots & \\ -a'_{s,1}x_1 - \cdots - a'_{s,n}x_n & > & -c'_s \end{array} \tag{15}$$

The argument now splits into two cases, depending on whether s (the number of strict inequalities in the system above or, equivalently, the number of negations of basic inequality formulas in f) is zero or greater than zero.

We first assume $s = 0$. We make use of the following variant of Farkas' lemma [Far02] (see [Sch86, page 89]) from linear programming, where A is a matrix, b is a column vector, and x is a column vector of distinct variables:

Lemma 4.4: *If $Ax \geq b$ is unsatisfiable, then there exists a row vector α such that*

1. $\alpha \geq 0$
2. $\alpha A = 0$
3. $\alpha b > 0$

Intuitively, α is a "witness" or "blatant proof" of the fact that $Ax \geq b$ is unsatisfiable. This is because if there were a vector x satisfying $Ax \geq b$, then $0 = (\alpha A)x = \alpha(Ax) \geq \alpha b > 0$, a contradiction.

Note that if $s = 0$, then we can write (15) in matrix form as $Ax \geq b$, where A is the $r \times n$ matrix of coefficients on the left-hand side, x is the column vector $(x_1, \ldots, x_n)$, and b is the column vector of the right-hand sides.

Suppose, by way of contradiction, that f and hence $Ax \geq b$ is unsatisfiable. We now show that f must be inconsistent, contradicting our assumption that f is consistent. Let $\alpha = (\alpha_1, \ldots, \alpha_r)$ be the row vector guaranteed to us by Lemma 4.4. Either by I5 or by Lemma 4.2 (depending on whether $\alpha_j > 0$ or $\alpha_j = 0$), we can multiply the j^{th} inequality formula in (15) (i.e., the j^{th} conjunct of f) by α_j (for $1 \leq j \leq r$), and then use I4 to add the resulting inequality formulas together. The net result (after deleting some 0 terms by I2) is the formula $(0x_1 \geq c)$, where $c = \alpha b > 0$. From this formula, by I7, we can conclude $(0x_1 > 0)$, which is an abbreviation for $\neg(0x_1 \leq 0)$, which is in turn an abbreviation for $\neg(-0x_1 \geq -0)$, i.e. $\neg((0x_1 \geq 0)$. Thus $f \Rightarrow \neg(0x_1 \geq 0)$ is provable.

However, by Lemma 4.2, $(0x_1 \geq 0)$ is also provable. It follows by propositional reasoning that $\neg f$ is provable, that is, f is inconsistent. Thus the assumption that f is unsatisfiable leads to the conclusion that f is inconsistent, a contradiction.

We now consider the case where $s > 0$. Farkas' lemma does not apply, but a variant of it, called Motzkin's transposition theorem, which is due to Fourier [Fou26], Kuhn [Kuh56], and Motzkin [Mot56] (see [Sch86, page 94]), does. A and A' are matrices, b and b' are column vectors, and x is a column vector of distinct variables.

Lemma 4.5: *If the system $Ax \geq b, A'x > b'$ is unsatisfiable, then there exist row vectors α, α' such that*

1. *$\alpha \geq 0$ and $\alpha' \geq 0$*
2. *$\alpha A + \alpha' A' = 0$*
3. *Either*
   (a) *$\alpha b + \alpha' b' > 0$, or*
   (b) *some entry of α' is strictly positive, and $\alpha b + \alpha' b' \geq 0$*

We now show that α and α' together form a witness to the fact that the system $Ax \geq b, A'x > b'$ is unsatisfiable. Assume that there were x satisfying $Ax \geq b$ and $A'x > b'$. In case (3a) of Lemma 4.5 ($\alpha b + \alpha' b' > 0$), we are in precisely the same situation as in Farkas' lemma, and the argument after Lemma 4.4 applies. In case (3b) of Lemma 4.5, let $\Delta = (A'x) - b'$; thus, Δ is a column vector and $\Delta > 0$. Then $0 = (\alpha A + \alpha' A')x = (\alpha A)x + (\alpha' A')x = \alpha(Ax) + \alpha'(A'x) \geq \alpha b + \alpha'(b' + \Delta) = (\alpha b + \alpha' b') + \alpha' \Delta \geq \alpha' \Delta > 0$, where the last inequality holds since every α'_j is nonnegative, some α'_j is strictly positive, and every entry of Δ is strictly positive. This is a contradiction.

In order to apply Motzkin's transposition theorem, we write (15) as two matrix inequalities: $Ax \geq b$, where A is the $r \times n$ matrix of coefficients on the left-hand side of the first r inequalities (those involving "$\geq$"), x is the column vector $(x_1, \ldots, x_n)$, and b is the column vector of the right-hand sides of the first r inequalities; and $A'x > b'$, where A' is the $s \times n$ matrix of coefficients on the left-hand side of the last s inequalities (those involving "$>$"), and b' is the column vector of the right-hand sides of the last s inequalities.

Again assume that f is unsatisfiable. Let $\alpha = (\alpha_1, \ldots, \alpha_r)$ and $\alpha' = (\alpha'_1, \ldots, \alpha'_s)$ be the row vectors guaranteed to us by Lemma 4.5. In case (3a) of Lemma 4.5, we replace every "$>$" in (15) by "$\geq$" and proceed to derive a contradiction as in the case that $s = 0$. Note that we can do this replacement by I6, since $t > c$ is an abbreviation for $\neg(t \leq c)$.

In order to deal with case (3b) of Lemma 4.5, we need one preliminary lemma, which shows that a variation of axiom I5 holds.

Lemma 4.6: *$(a_1x_1 + \cdots + a_kx_k > c) \Leftrightarrow (da_1x_1 + \cdots + da_kx_k > dc)$ is provable, if $d > 0$.*

Proof: The following formula is an instance of axiom I5:

$$(d(-a_1)x_1 + \cdots + d(-a_k)x_k \geq d(-c)) \Leftrightarrow ((-a_1)x_1 + \cdots + (-a_k)x_k \geq -c).$$

By taking the contrapositive and using the fact that $t > c$ is an abbreviation for $\neg(-t \geq -c)$, we see that the desired formula is provable. ∎

Since we are considering case (3b) of Lemma 4.5, we know that some α'_j is strictly positive; without loss of generality, assume that α'_s is strictly positive. For $1 \leq j \leq s-1$, let us replace the "$>$" in the jth inequality involving "$>$" in (15) by "$\geq$". Again, this is legal by I6. As before, either by axiom I5 or by Lemma 4.2, we can multiply the j^{th} inequality formula in the system (15) by α_j (for $1 \leq j \leq r$), and multiply each of the next $s-1$ inequalities that result when we replace $>$ by $\geq$ by α'_j, $j = 1, \ldots, s-1$, respectively. Finally, by Lemma 4.6, we can multiply the last inequality in (15) by α_s (which is strictly positive, by assumption). This results in the following system of inequalities:

$$\begin{array}{rcl} \alpha_1 a_{1,1}x_1 + \cdots + \alpha_1 a_{1,n}x_n & \geq & \alpha_1 c_1 \\ & \cdots & \\ \alpha_r a_{r,1}x_1 + \cdots + \alpha_r a_{r,n}x_n & \geq & \alpha_r c_r \\ -\alpha'_1 a'_{1,1}x_1 - \cdots - \alpha'_1 a'_{1,n}x_n & \geq & -\alpha'_1 c'_1 \\ & \cdots & \\ -\alpha'_{s-1} a'_{s-1,1}x_1 - \cdots - \alpha'_{s-1} a'_{s-1,n}x_n & \geq & -\alpha'_{s-1} c'_{s-1} \\ -\alpha'_s a'_{s,1}x_1 - \cdots - \alpha'_s a'_{s,n}x_n & > & -\alpha'_s c'_s \end{array} \tag{16}$$

Let us denote the last inequality (the inequality involving "$>$") in (16) by g. Let $a''_1x_1 + \cdots + a''_nx_n \geq d$ be the result of "adding" all the inequalities in (16) except g. This inequality is provable from f using I4. Since $\alpha A + \alpha' A' = 0$, we must have that $\alpha'_s a'_{s,j} = a''_j$, for $j = 1, \ldots, n$. So the inequality g is $(-a''_1x_1 - \cdots - a''_nx_n > -\alpha'_s c'_s)$. Since $\alpha b + \alpha' b' \geq 0$, it follows that $-\alpha'_s c'_s \geq -d$. Hence, the formula $g \Rightarrow (-a''_1x_1 - \cdots - a''_nx_n > -d)$ is provable using I7 and propositional reasoning (there are two case, depending on whether $-\alpha'_s c'_s = -d$ or $-\alpha'_s c'_s > -d$). Now $-a''_1x_1 - \cdots - a''_nx_n > -d$ is equivalent to $a''_1x_1 + \cdots + a''_nx_n < d$. But this contradicts $a''_1x_1 + \cdots + a''_nx_n \geq d$, which we already showed is provable from f. It follows by propositional reasoning that $\neg f$ is provable, that is, f is inconsistent, as desired.

Since we have shown that assuming f is unsatisfiable leads to the conclusion that f is inconsistent, it follows that if f is consistent then f is satisfiable. ∎

4.2 Small model theorem

A "model" for an inequality formula is simply an assignment to variables. We think of an assignment to variables as "small" if it assigns a nonzero value to only a small number of variables. We now show that a satisfiable formula is satisfiable by a small assignment to variables.

As we did with weight formulas, let us define the *length* $|f|$ of an inequality formula f to be the number of symbols required to write f, where we count the length of each coefficient as 1. We have the following "small model theorem".

Theorem 4.7: *Suppose f is a satisfiable inequality formula. Then f is satisfied by an assignment to variables where at most $|f|$ variables are assigned a nonzero value.*

Proof: As in the completeness proof, we can write f in disjunctive normal form. It is easy to show that each disjunct is a conjunction of at most $|f|$ basic inequality formulas and their negations. Clearly, since f is satisfiable, one of the disjuncts is satisfiable. The result then follows from Lemma 4.8 below, which is closely related to Lemma 2.5. Lemma 2.5 says that if a system of r linear equalities and/or inequalities has a nonnegative solution, then it has a nonnegative solution with at most r entries positive. Lemma 4.8 below, by contrast, says that if the system has a solution (not necessarily nonnegative), then there is a solution with at most r variables assigned a nonzero (not necessarily positive) value.

Lemma 4.8: *If a system of r linear equalities and/or inequalities has a solution, then it has a solution with at most r variables assigned a nonzero value.*

Proof: By the comment after Lemma 2.5, we can pass to a system of equalities only.

Hence, let $Ax = b$ represent a satisfiable system of linear equalities, where A has r rows; we must show that there is a solution where at most r of the variables are assigned a nonzero value. Since $Ax = b$ is satisfiable, it follows that b is in the vector space V spanned by the columns of A. Since each column is of length r, it follows from standard results of linear algebra that V is spanned by some subset of at most r columns of A. So b is the linear combination of at most r columns of A. Thus, there is a vector y^* with at most r nonzero entries where $Ay^* = b$. This proves the lemma. ∎

4.3 Decision procedure

As before, when we consider decision procedures, we must take into account the length of coefficients. Again, we define $\|f\|$ to be the length of the longest coefficient appearing in f, when written in binary, and we define the size of a rational number a/b, where a and b are relatively prime, to be the sum of lengths of a and b, when written in binary. We can then extend the small model theorem above as follows:

Theorem 4.9: *Suppose f is a satisfiable inequality formula. Then f is satisfied by an assignment to variables where at most $|f|$ variables are assigned a nonzero value, and where the value assigned to each variable is a rational number with size $O(|f|\,\|f\| + |f|\,\log(|f|))$.*

Theorem 4.9 follows from the proof of Theorem 4.7 and the following simple variation of Lemma 4.8, which can be proven using Cramer's rule and simple estimates on the size of the determinant.

Lemma 4.10: *If a system of r linear equalities and/or inequalities with integer coefficients each of length at most ℓ has a solution, then it has a solution with at most r variables assigned a nonzero value, and where the size of each member of the solution is $O(r\ell + r\log(r))$.*

As a result, we get

Theorem 4.11: *The problem of deciding whether an inequality formula is satisfiable in a measurable probability structure is NP-complete.*

Proof: For the lower bound, a propositional formula φ is satisfiable iff the inequality formula that is the result of replacing each propositional variable p_i by the inequality $x_i \geq 0$ is satisfiable. For the upper bound, given an inequality formula f, we guess a satisfying assignment to variables for f with at most $|f|$ variables being assigned a nonzero value, such that each nonzero value assigned to a variable is a rational number with size $O(|f|\,\|f\| + |f|\log(|f|))$. We then verify that the assignment satisfies the inequality formula. ∎

5 Reasoning about conditional probability

We now turn our attention to reasoning about conditional probability. As we pointed out in the introduction, the language we have been considering is not sufficiently expressive to allow us to express statements such as $2w(p_2 \mid p_1) + w(p_1 \mid p_2) \geq 1$. Suppose we extend our language to allow products of terms, so that formulas such as $2w(p_1)w(p_2) \geq 1$ are allowed. We call such formulas *polynomial weight formulas*. To help make the contrast clearer, let us now refer to the formulas we have been calling "weight formulas" as "linear weight formulas". We leave it to the reader to provide a formal syntax for polynomial weight formulas. Notice that by clearing the denominators, we can rewrite the formula involving conditional probabilities to $2w(p_1 \wedge p_2)w(p_2) + 2w(p_1 \wedge p_2)w(p_1) \geq w(p_1)w(p_2)$, which is a polynomial weight formula.[6]

[6] Actually, it might be better to express it as the polynomial weight formula $w(p_1) \neq 0 \wedge w(p_2) \neq 0 \Rightarrow (2w(p_1 \wedge p_2)w(p_2) + 2w(p_1 \wedge p_2)w(p_1) \geq w(p_1)w(p_2))$, to take care of the case where the denominator is 0.

In order to discuss decision procedures and axiomatizations for polynomial weight formulas, we need to consider the theory of real closed fields. We now define a real closed field. All of our definitions are fairly standard (see, for example, [Sho67]). An *ordered field* is a field with a linear ordering $<$, where the field operations $+$ (plus) and $\cdot$ (times) respect the ordering: that is, (1) $x < y$ implies that $x + z < y + z$, and (2) if x and y are positive, then so is $x \cdot y$. A *real closed field* is an ordered field where every positive element has a square root and every polynomial of odd degree has a root. Tarski showed [Tar51, Sho67] that the theory of real closed fields coincides with the theory of the reals (under $+, \cdot, <$ and constants $0, 1, -1$). That is, any first-order formula that involves only $+, \cdot, <, 0, 1, -1$ is true about the real numbers if and only if it is true of every real closed field.

Tarski [Tar51] showed that the decision problem for this theory is decidable. Ben-Or, Kozen, and Reif [BKR86] have shown that the decision problem is decidable in exponential space. Fischer and Rabin [FR74] prove a nondeterministic exponential time lower bound for the complexity of the decision problem. In fact, Fischer and Rabin's lower bound holds even if the only nonlogical symbol is $+$ (plus). Berman [Ber80] gives a slightly sharper lower bound in terms of alternation. Canny [Can88] has recently shown that the quantifier-free fragment is decidable in polynomial space.

We do not know a sound and complete axiomatization for polynomial weight formulas. For this reason, we shall extend later to allow first-order quantification, which will enable us to obtain a complete axiomatization in a larger language. However, we do have small model theorems and decision procedures, which we now describe.

5.1 Small model theorems

Despite the added expressive power of the language, we can still prove small model theorems along much the same lines as we proved them in the case of linear weight formulas.

Theorem 5.1: *Suppose f is a polynomial weight formula that is satisfied in some measurable probability structure. Then f is satisfied in a structure with at most $|f|$ states where every set of states is measurable.*

Proof: Let f be a polynomial weight formula which is satisfied in some measurable probability structure, say $M = (S, \mathcal{X}, \mu, \pi)$. Let $\varphi_1, \ldots, \varphi_k$ be the propositional formulas that appear in f. Clearly $k \leq ||f||$. Let $c_i = \mu(\varphi_i^M)$, for $1 \leq i \leq k$. As before, assume that $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in f, and let $\delta_1, \ldots, \delta_{2^n}$ be the n-atoms. Let F be the following set of equalities and inequalities, where we think of each $w(\delta)$ as a variable:

$$w(\delta_1) + \cdots + w(\delta_{2^n}) \quad = \quad 1$$

$$\begin{aligned}
\sum_{\delta \in At_n(\varphi_1)} w(\delta) &= c_1 \\
&\cdots \\
\sum_{\delta \in At_n(\varphi_k)} w(\delta) &= c_k
\end{aligned}$$

Since f is satisfiable in a measurable probability structure, this system F has a nonnegative solution. Hence, by Lemma 2.5, there is a solution with at most $k+1$ of the $w(\delta)$'s positive. As in the proof of Theorem 2.4, this gives us a structure that satisfies f with at most $|f|$ states where every set of states is measurable. ∎

Note: We could have proven Theorem 2.4 with the same proof we just gave. However, the proof would not generalize immediately to proving Theorem 2.6.

Theorem 5.2: *Let f be a polynomial weight formula that is satisfied in some probability structure. Then it is satisfied in a structure with at most $|f|^2$ states, and with a basis of size at most $|f|$.*

Proof: The proof of this theorem is obtained by modifying the proof of Theorem 3.9 in the same way as the proof of Theorem 5.1 is obtained by modifying the proof of Theorem 2.4. ∎

5.2 Decision procedures

In Sections 2 and 3, we were able to obtain decision procedures for linear weight formulas by extending the small model theorems to show that not only are there small models, but there are small models where the probabilities have a "small" length. Such a result is false for polynomial weight formulas (consider $2w(p)w(p) = 1$). Hence, in order to obtain a decision procedure in this case, we use a different technique for deciding satisfiability: We reduce the problem to a problem in the quantifier-free theory of real closed fields, and then apply Canny's decision procedure.

Theorem 5.3: *There is a procedure that runs in polynomial space for deciding if a polynomial weight formula is satisfiable in a measurable probability structure.*

Proof: Let f be a polynomial weight formula, where the distinct primitive propositions that appear in f are $p_1, \ldots, p_n$. Let $\delta_1, \ldots, \delta_{2^n}$ be the n-atoms, and let T be a subset of the n-atoms, with at most $|f|$ members. Assume that the members of T are precisely $\delta_{i_1}, \ldots, \delta_{i_t}$, where $i_1 < \cdots < i_t$. Let $x_1, \ldots, x_t$ be variables (as many variables as the cardinality of T), where intuitively, x_j will correspond to $w(\delta_{i_j})$). Let f_T be the conjunction of $x_1 + \cdots + x_t = 1$ with the result of replacing each term $w(\varphi)$ of f by $\sum_{\delta_{i_j} \in At_n(\varphi)} x_j$. By Theorem 5.1, it is easy to see that f is satisfiable in a measurable probability structure iff for some T with at most $|f|$ members, f_T is satisfiable over the real numbers (that is, iff there are real numbers $x_1^*, \dots, x_t^*$ such that the result of replacing each variable x_i by x_i^* is true about the real numbers). It is straightforward to verify that $|f_T|$ is polynomial in $|f|$, where $|f_T|$ is the length of f_T, and again we count the length of each coefficient as 1.

We would now like to apply Canny's decision procedure for checking if f_T is satisfiable, but there is one small problem. The formula f_T has arbitrary integer coefficients, whereas the language of real closed fields allows only the constants 0, 1, and -1. Now we could replace a constant like 17 by $1 + \cdots + 1$ (17 times). This would result in a formula f_T' that is in the language of real closed fields, but $|f_T'|$ might be exponential in $||f||$. The solution is to express 17 as $2^4 + 1$, and then write this in the language of real closed fields as $(1+1)\cdot(1+1)\cdot(1+1)\cdot(1+1)+1$. Using this technique we can clearly represent any coefficient whose length is k when written in binary by an expression in the language of real closed fields of length $O(k^2)$. Let f_T' be the formula that results by representing the coefficients of f_T in this way. Thus $|f_T'|$ is polynomial in $|f| \cdot ||f||$.

The PSPACE decision procedure for satisfiability of f proceeds by systematically cycling through each candidate for T, and using Canny's PSPACE algorithm to decide if f_T' is satisfiable over the real numbers. Our algorithm says that f is satisfiable iff f_T' is satisfiable over the real numbers for some T. ∎

Theorem 5.4: *There is a procedure that runs in polynomial space for deciding whether a polynomial weight formula is satisfiable in a (general) probability structure.*

Proof: Let f be a polynomial weight formula. Assume that $\{p_1, \dots, p_n\}$ includes all of the primitive propositions that appear in f. Define a *partial probability structure* to be a tuple $Q = (S, B, \pi)$, where S is a set (thought of as a set of states); $B = \{T_1, \dots, T_t\}$ gives a partition of S, that is, the T_i's are nonempty and pairwise disjoint, and their union is S (we think of B as being a basis); and $\pi(s)$ is a truth assignment for every state in S, where we assume that $\pi(s)(p) =$ **false** for every primitive proposition p that does not appear in f (note: the analog to Lemma 2.8 holds, so we do not care about primitive propositions that do not appear in f). Intuitively, a partial probability structure gives all the information about a probability structure except the measure of the basis elements. For each propositional formula φ over $\{p_1, \dots, p_n\}$, define $V(\varphi) \subseteq \{1, \dots, t\}$ by letting $i \in V(\varphi)$ iff φ is true under the truth assignment $\pi(b)$ for every $b \in T_i$. Intuitively, if we expanded Q to a probability structure M by defining the measure of each basis element, then the inner measure of φ^M would be obtained by adding the measures of each T_i where $i \in V(\varphi)$. Let $x_1, \dots, x_t$ be variables (as many variables as the cardinality of B), where intuitively, x_i corresponds to the measure of T_i. Let f_Q be the conjunction of $x_1 + \cdots + x_t = 1$ with the result of replacing each term $w(\varphi)$ of f by $\sum_{i \in V(\varphi)} x_i$ (and by 0 if $V(\varphi)$ is empty) and replacing each integer coefficient of f by the appropriate representation as discussed in the proof of Theorem 5.3. By Theorem 5.2, it is easy to see that f is satisfiable in a probability structure iff for some "small" partial probability structure Q (that is, a partial probability structure $Q = (S, B, \pi)$ where S has at most $|f|^2$ members and B has at most $|f|$ members), f_Q is satisfiable over the real numbers. It is easy to see that if Q is small, then the size of f_Q is polynomial in $|f|\cdot||f||$. The PSPACE decision procedure for satisfiability of f proceeds by systematically cycling through each small partial probability structure Q, and using Canny's PSPACE algorithm to decide if f_Q is satisfiable over the real numbers. Our algorithm says that f is satisfiable iff one of these f_Q's is satisfiable over the real numbers. ∎

6 First-order weight formulas

The basic idea in proving completeness for linear weight formulas was to use the axioms W1–W4 to reduce the problem to checking validity of a set of linear inequalities, and then apply the axiom Ineq. In the case of polynomial weight formulas we want to use a similar technique. In this case, we use W1–W4 to reduce the problem to checking validity of a formula in the language of real closed fields, and then apply a sound and complete axiomatization for real closed fields. There is only one difficulty in carrying out this program: the theory of real closed fields allows first-order quantification over the reals. Thus, in order to carry out our program, we have to extend the language yet again to allow such quantification.

We define a *basic first-order weight formula* to be like a basic polynomial weight formula, except that now we allow variables (intended to range over the reals) in expressions. Thus, a typical basic first-order weight formula is:

$$(3 + x) \cdot w(\varphi) \cdot w(\psi \wedge \varphi) + 2 \cdot w(\psi) \geq z.$$

The set of *first-order weight formulas* is obtained by closing off the basic first-order weight formulas under conjunction, negation, and first-order quantification (where the quantification is over the reals). In order to ascribe semantics to first-order weight formulas, we now need a pair consisting of a probability structure M and a *valuation* v, where a valuation is a function from variables to the reals that gives meaning to the free variables in the formula. Thus, for example, if $M = (S, \mathcal{X}, \mu, \pi)$, then

$$\begin{array}{l}(M, v) \models (3 + x) \cdot w(\varphi) \cdot w(\psi \wedge \varphi) + 2 \cdot w(\psi) \geq z \text{ iff} \\ (3 + v(x))\mu_*(\varphi^M)\mu_*(\psi \wedge \varphi) + 2\mu_*(\psi^M) \geq v(z).\end{array}$$

We deal with quantification as usual, so that $(M, v) \models \forall x\varphi$ iff $(M, v') \models \varphi$ for all v' that agree with v except possibly in the value that they assign to x. We leave the remaining details to the reader. It would be quite natural to restrict attention to *sentences*, i.e., formulas with no free variables. Note that the truth or falsity of a sentence is independent of the valuation. We shall usually not bother to do so. Thus, when we say that a first-order weight formula is satisfiable, we mean that there is a probability structure M and a valuation v such that $(M, v) \models f$. Note that a formula f with free variables

$x_1, \ldots, x_k$ is satisfiable iff the sentence $\exists x_1 \ldots \exists x_k f$ is satisfiable. Similarly, f is valid iff the sentence $\forall x_1 \ldots \forall x_k f$ is valid.

We can prove a small model theorem for first-order weight formulas using techniques identical to those used in Theorems 5.1 and 5.2.

Theorem 6.1: *Let f be a first-order weight formula that is satisfied in some measurable probability structure. Then f is satisfied in a structure with at most $|f|$ states where every set of states is measurable.*

Theorem 6.2: *Let f be a first-order weight formula that is satisfied in some probability structure. Then f is satisfied in a structure with at most $|f|^2$ states, and with a basis of size at most $|f|$.*

We can also obtain decision procedures for first-order weight formulas by appropriately modifying Theorems 5.3 and 5.4, except that instead of using Canny's PSPACE algorithm, we use Ben-Or, Kozen, and Reif's exponential space algorithm (since the first-order formulas f'_T and f_Q of the proofs are no longer necessarily quantifier-free).

Theorem 6.3: *There is a procedure that runs in exponential space for deciding whether a first-order weight formula is satisfiable in a measurable probability structure.*

Theorem 6.4: *There is a procedure that runs in exponential space for deciding whether a first-order weight formula is satisfiable in a (general) probability structure.*

In order to get a complete axiomatization for first-order weight formulas, we begin by giving a sound and complete axiomatization for real closed fields, which Tarski [Tar51] proved is complete for the reals. The version we give is a minor modification of that appearing in [Sho67]. The nonlogical symbols are $+, \cdot, <, 0, 1, -1$.

First-order reasoning:

FO-Taut. All instances of valid formulas of first-order logic with equality (see, for example, [End72, Sho67])

MP. From f and $f \Rightarrow g$ infer g (modus ponens)

Reasoning about real closed fields:

F1. $\forall x \forall y \forall z((x + y) + z = x + (y + z))$

F2. $\forall x(x + 0 = x)$

F3. $\forall x(x + (-1 \cdot x) = 0)$

F4. $\forall x \forall y(x + y = y + x)$

F5. $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$

F6. $\forall x(x \cdot 1 = x)$

F7. $\forall x(x \neq 0 \Rightarrow \exists y(x \cdot y = 1))$

F8. $\forall x \forall y(x \cdot y = y \cdot x)$

F9. $\forall x \forall y \forall z(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$

F10. $0 \neq 1$

F11. $\forall x(\neg(x < x))$

F12. $\forall x \forall y \forall z((x < y) \wedge (y < z) \Rightarrow (x < z))$

F13. $\forall x \forall y((x < y) \vee (x = y) \vee (y < x))$

F14. $\forall x \forall y \forall z((x < y) \Rightarrow ((x + z) < (y + z)))$

F15. $\forall x \forall y(((0 < x) \wedge (0 < y)) \Rightarrow (0 < x \cdot y))$

F16. $\forall x((0 < x) \Rightarrow \exists y(y \cdot y = x))$

F17. Every polynomial of odd degree has a root

An instance of axiom F17, which would say that every polynomial of degree 3 has a root, would be

$$\forall y_0 \forall y_1 \forall y_2 \forall y_3((y_0 \neq 0) \Rightarrow \exists x(y_0 \cdot x \cdot x \cdot x + y_1 \cdot x \cdot x + y_2 \cdot x + y_3 = 0))$$

Axioms F1–F10 are the field axioms, axioms F11–F13 are the axioms for linear orders, axioms F14–F15 are the additional axioms for ordered fields, and axioms F16–F17 are the additional axioms for real closed fields. Let us denote the axiom system above by AX_{RCF}. Then AX_{RCF} is a sound and complete axiomatization for real closed fields [Tar51, Sho67]. Let us denote by $\mathrm{AX}_{FO\text{-}MEAS}$ the result of taking AX_{RCF} along with our axioms W1–W4 and one more axiom, F18 below, that lets us replace the integer coefficients that appear in weight formulas by an expression in the language of real closed fields:

F18. $k = 1 + \cdots + 1$ (k times)

(We remark that there is no need to use an efficient representation of integer coefficients here, as there was, say, in Theorem 5.3, since complexity issues do not arise.) Let us denote by AX_{FO} the result of replacing W3 in $\mathrm{AX}_{FO\text{-}MEAS}$ by W5 and W6.[7] We now show

[7]The occurrences of $\geq$ in an expression such as $t_1 \geq t_2$ in W1–W6 can be viewed as an abbreviation for $(t_2 < t_1) \vee (t_1 = t_2)$, which is a formula in the language of real closed fields.

that $\mathrm{AX}_{FO\text{-}MEAS}$ is a sound and complete axiomatization for first-order weight formulas with respect to measurable probability structures, and AX_{FO} is a sound and complete axiomatization for first-order weight formulas with respect to (general) probability structures.

Theorem 6.5: *$AX_{FO\text{-}MEAS}$ is a sound and complete axiomatization for first-order weight formulas with respect to measurable probability structures.*

Proof: From what we have said, it is clear that $\mathrm{AX}_{FO\text{-}MEAS}$ is sound. To show completeness, we carry out the ideas sketched at the beginning of this section: namely, we reduce a first-order weight formula to an equivalent formula in the language of real closed fields. Assume that f is a first-order weight formula that is unsatisfiable with respect to measurable probability structures (that is, there is no measurable probability structure that satisfies it). Let $p_1, \ldots, p_n$ include all of the primitive propositions that appear in f, and let $\delta_1, \ldots, \delta_{2^n}$ be the n-atoms. Let $x_1, \ldots, x_{2^n}$ be new variables, where intuitively, x_i represents $w(\delta_i)$. Let f' be $\exists x_1 \ldots \exists x_{2^n} g$, where g is the conjunction of:

$$\begin{array}{rcl} x_1 + \cdots + x_{2^n} & = & 1 \\ x_1 & \geq & 0 \\ & \cdots & \\ x_{2^n} & \geq & 0 \end{array} \tag{17}$$

along with the result of replacing each $w(\varphi)$ in f by $\sum_{\delta_i \Rightarrow \varphi} x_i$ (and by 0 if φ is equivalent to $false$) and replacing each integer coefficient k in f by $1 + \cdots + 1$ (k times). It is easy to see that since f is unsatisfiable with respect to measurable probability structures, it follows that f' is false about the real numbers. By Tarski's result on the completeness of AX_{RCF}, it follows that $\neg f'$ is provable in AX_{RCF}. By making use of Lemma 2.3 (which again holds, by essentially the same proof), it is not hard to see that $\neg f$ is provable in $\mathrm{AX}_{FO\text{-}MEAS}$. The straightforward details are omitted. ∎

To prove completeness of AX_{FO} in the general (nonmeasurable) case, we need a lemma, which is completely analogous to Theorem 3.7. Let f be a first-order weight formula, where $\{p_1, \ldots, p_n\}$ includes all of the primitive propositions that appear in f, and let $\rho_1, \ldots, \rho_{2^{2^n}}$ be the n-regions. Let $x_1, \ldots, x_{2^{2^n}}$ be new variables (one new variable for each n-region), where intuitively, x_i corresponds to $w(\rho_i)$. Let $\widehat{f}$ be the result of replacing each $w(\varphi)$ in f by x_i, where ρ_i is the n-region equivalent to φ. Let $\widetilde{f}$ be $\widehat{f} \wedge (x_1 = 0) \wedge (x_{2^{2^n}} = 1) \wedge$ "$Nx \geq 0$", where "$Nx \geq 0$" is the conjunction of the inequalities $Nx \geq 0$.

Lemma 6.6: *Let f be a first-order weight formula. Then f is satisfied in some probability structure iff $\widetilde{f}$ is satisfiable over the real numbers.*

Proof: The proof is virtually identical to that of Theorem 3.7. For example, if $\widetilde{f}$ is satisfiable over the real numbers, then let $x^* = x_1^*, \ldots, x_{2^{2^n}}^*$ be real numbers such that the result of replacing each x_i in $\widetilde{f}$ by x_i^* is true about the real numbers. The proof of Theorem 3.7 shows how to use x^* to build a probability structure that satisfies f. ∎

Theorem 6.7: *AX_{FO} is a sound and complete axiomatization for first-order weight formulas with respect to (general) probability structures.*

Proof: Again, it is clear that AX_{FO} is sound. To show completeness, assume that f is an unsatisfiable first-order weight formula (that is, there is no probability structure that satisfies it). Let f' be $\exists x_1 \ldots \exists x_{2^{2^n}} \widetilde{f}$. By Lemma 6.6, f' is false about the real numbers. By Tarski's result again on the completeness of AX_{RCF}, it follows that $\neg f'$ is provable in AX_{RCF}. As before, it is therefore not hard to see that $\neg f$ is provable in AX_{FO}. Again, the straightforward details are omitted. ∎

We close this section with a few remarks on how these results relate to those obtained in [Bac90] and [AH94, Hal90]. In Bacchus' language it is possible to represent probabilities of first-order formulas. However, while we place probabilities on possible worlds here, Bacchus instead places the probability on the domain. Thus, (using our notation), he would allow a formula such as $\forall x(w_y(P(x,y)) \geq 1/3)$, which should be read "for all x, the probability that a random y satisfies $P(x,y)$ is at least 1/3." In addition, first-order quantification over probabilities is allowed, as in a formula of the form $\exists r \forall y(w_y(P(x,y)) \geq r)$. Thus we can view Bacchus' language as an extension of first-order weight formulas, where the arguments of the weight function are first-order formulas rather than just propositional formulas. There is an additional technical difference between our approach and that of Bacchus. Bacchus' "probabilities" do not have to be real valued; they can take values in arbitrary ordered fields. Moreover, Bacchus requires his probability measures to be only finitely additive rather than countably additive; thus they are not true probability measures. Bacchus does provide a complete axiomatization for his language. However, a formula that is valid when the probabilities take on real values is not necessarily provable in his system, since it may not be valid when probabilities are allowed to take values in arbitrary ordered fields. On the other hand, Bacchus' axioms are all sound when probability is interpreted in the more standard way and, as Bacchus shows, they do enable us to prove many facts of interest regarding the probability of first-order sentences.

More recently, in [Hal90], two first-order logics of probability are presented. One, in the spirit of Bacchus, puts probability on the domain while the other, more in the spririt of our approach here, puts probability on the possible worlds. It is shown that these ideas can be combined to allow a logic where we can reason simultaneously about probabilities on the domain and on possible worlds. In all cases, the probabilities are countably additive and take values in the reals. In [AH94] it is shown that in general the decision problem for these logics is wildly undecidable (technically, it is Π_1^2-complete).

However, in some special cases, the logic is decidable; complete axiomatizations for these cases are provided in [Hal90].

7 Dempster-Shafer belief functions

The Dempster-Shafer theory of evidence [Sha76] provides one approach to attaching likelihoods to events. This theory starts out with a *belief function* (sometimes called a *support function*). For every event A, the belief in A, denoted $Bel(A)$, is a number in the interval $[0,1]$ that places a lower bound on likelihood of A. Shafer [Sha76] defines a belief function (over S) to be a function $Bel: 2^S \rightarrow [0,1]$ (where, as usual, 2^S is the set of subsets of S), that satisfies the following conditions:

B1. $Bel(\emptyset) = 0$

B2. $Bel(S) = 1$

B3. $Bel(A_1 \cup \ldots \cup A_r) \geq \sum_{I \subseteq \{1,\ldots,r\}, I \neq \emptyset} (-1)^{|I|+1} Bel(\bigcap_{i \in I} A_i)$.

Property B3 may seem unmotivated. Perhaps the best way to understand it is as an analogue to the usual inclusion-exclusion rule for probabilities [Fel57, p. 89], which is obtained by replacing the inequality by equality (and the belief function Bel by a probability function μ). In particular, B3 holds for probability functions. In [FH91] it is shown to hold for all inner measures induced by probability functions. Thus, every inner measure is a belief function. The converse is almost true, but not quite. It turns out that roughly speaking, the converse would be true if the domain of belief functions and inner measures were formulas, rather than sets. We now give a precise version of this informal statement.

By analogy with probability structures, let us define a *DS structure* (where, of course, "DS" stands for Dempster-Shafer) to be a tuple $D = (S, Bel, \pi)$, where Bel is a belief function over S, and as before, π associates with each state in S a truth assignment on the primitive propositions in Φ. For each propositional formula φ, we define φ^D just as we defined φ^M for probability structures M. Let $M = (S, \mathcal{X}, \mu, \pi)$ be a probability structure. Following [FH91], we say that D and M are *equivalent* if $Bel(\varphi^D) = \mu_*(\varphi^M)$ for every propositional formula φ.

For the purposes of the next theorem, we wish to consider probability structures and DS structures where there are effectively only a finite number of propositional variables. Let us say that a probability structure $M = (S, \mathcal{X}, \mu, \pi)$ or a DS structure $D = (S, Bel, \pi)$ is *special* if $\pi(s)(p) =$ **false** for all but finitely many primitive propositions p and for every state s.

Theorem 7.1: [FH91]

1. For every special probability structure there is an equivalent special DS structure.

2. For every special DS structure there is an equivalent special probability structure.

It follows immediately that AX is a sound and complete axiomatization for linear weight formulas with respect to DS structures (i.e., where $w(\varphi)$ is interpreted as the belief in φ).[8] Similarly, AX_{FO} is a sound and complete axiomatization for first-order weight formulas with respect to DS structures. All of our decision procedures carry over immediately. Thus, for linear weight formulas, the complexity of the decision problem with respect to DS structures is NP-complete; for polynomial weight formulas, there is a polynomial space procedure for deciding satisfiability (and validity), and for first-order weight formulas, there is an exponential space procedure for deciding satisfiability (and validity). Let W6′ be the following axiom, which is obtained directly from Shafer's condition B3 above in the obvious way.

W6′. $w(\varphi_1 \vee \ldots \vee \varphi_r) \geq \sum_{I \subseteq \{1,\ldots,r\},\, I \neq \emptyset} (-1)^{|I|+1} w(\bigwedge_{i \in I} \varphi_i)$.

In the remainder of this section, we show that we could just as well have used W6′ as W6 throughout this paper. Let AX′ (respectively, AX'_{FO}) be the axiom system that results when we replace W6 in AX (respectively, AX_{FO}) by W6′.

Theorem 7.2: *The axiom system AX (respectively, AX_{FO}) is equivalent to the axiom system AX′ (respectively, AX'_{FO}).*

Proof: For convenience, we restrict attention to AX, since the proof is essentially identical in the case of AX_{FO}. We first show that if f is an instance of axiom W6′, then f is provable in AX. Assume not. Then $\neg f$ is consistent with AX. By completeness (Theorem 3.8), there is a probability structure that satisfies $\neg f$. So by Theorem 7.1, there is a DS structure that satisfies $\neg f$. However, this is impossible, since it is easy to see that every DS structure satisfies every instance of axiom W6′.

Now let f be an instance of axiom W6; we must show that f is provable in AX′. Let f be

$$\sum_{t=1}^{r} \sum_{\rho' \text{ a size } t \text{ subregion of } \rho} (-1)^{r-t} w(\rho') \geq 0, \tag{18}$$

where ρ is the size r region $\delta_1 \vee \cdots \vee \delta_r$, and $r \geq 1$. If $r = 1$, then (18) says $w(\delta_1) \geq 0$, which is a special case of axiom W1. Assume now that $r \geq 2$. Define φ_i, for $1 \leq i \leq r$, to be the disjunction of each of $\delta_1, \ldots, \delta_r$ *except* δ_i. Rewrite W6′ as

$$w(\varphi_1 \vee \ldots \vee \varphi_r) + \sum_{I \subseteq \{1,\ldots,r\},\, I \neq \emptyset} (-1)^{|I|} w(\bigwedge_{i \in I} \varphi_i) \geq 0. \tag{19}$$

[8] We can restrict attention to special structures because of Lemma 2.8, which implies that if we are concerned with the validity of a formula f, then we can restrict attention without loss of generality to the finitely many primitive propositions that appear in f. In [FH91], attention was restricted to structures where there are only a finite number of primitive propositions, which is equivalent to considering special structures.

We now show that (18) and (19) are equal, term by term. First, the $w(\varphi_1 \vee \ldots \vee \varphi_r)$ term of (19) is equal to $w(\rho)$, since $\varphi_1 \vee \ldots \vee \varphi_r$ is equivalent to ρ. This corresponds to the term of (18) where $t = r$ and $\rho' = \rho$. Now consider the term of (19) where the distinct members of I are precisely $i_1, \ldots, i_s$. It is straightforward to verify that $\bigwedge_{i \in I} \varphi_i$ is equivalent to the t-subregion ρ' of ρ which is the disjunction of each of $\delta_1, \ldots, \delta_r$ except $\delta_{i_1}, \ldots, \delta_{i_s}$, where $t = r - s$. So the term $(-1)^{|I|} w(\bigwedge_{i \in I} \varphi_i)$ equals $(-1)^s w(\rho')$, which equals $(-1)^{r-t} w(\rho')$, a term of (18). The only term of (19) that does not match up with a term of (18) occurs when $I = \{1, \ldots, r\}$; but then $\bigwedge_{i \in I} \varphi_i$ is equivalent to *false*, so $w(\bigwedge_{i \in I} \varphi_i) = 0$. Otherwise, there is a perfect matching between the terms of (18) and (19). It follows easily that (18) is provable in AX$'$. ∎

8 Conclusions

We have investigated a logic for reasoning about probability, both for cases where propositions necessarily represent measurable sets and for the general case. We have provided complete axiomatizations and decision procedures for a number of variants of the logic.

We were surprised both to be able to get fairly elegant complete axiomatizations for so rich a logic, and to be able to prove that the satisfiability problem for the linear case is in NP. This is certainly the best we could have hoped for, since clearly the satisfiability problem for our logic is at least as hard as that of propositional logic. We remark that in [GKP88, Kav89] there is some discussion of subcases of the decision procedure for the measurable case that can be handled efficiently. It would be of interest to have further results on easily decidable subcases of the logic, or on good heuristics for checking validity.

While the focus of this paper is on technical issues—axiomatizations and decision procedures—it is part of a more general effort to understand reasoning about knowledge and probability. In [FH91] we consider the issue of appropriate models for reasoning about uncertainty in more detail, and compare the probabilistic approach to the Dempster-Shafer approach. In [FH94], we consider a logic of knowledge and probability that allows arbitrary nesting of knowledge and probability operators. In particular, we allow higher-order weight formulas such as $w(w(\varphi) \geq 1/2) \geq 1/3$. (See also [Gai86] for discussion and further references on the subject of higher-order probabilities.) We are again able to prove technical results about complete axiomatizations and decision procedures for the resulting logics extending those of this paper. There is also a general look at the interaction between knowledge and probability. The paper [HT93] focuses on knowledge and probability in distributed systems. Finally, [AH94, Hal90] consider issues of reasoning about probability in a first-order context.

We feel that there is far more work to be done in this area though, particularly in understanding how to model real-world phenomena appropriately. We expect that our formalization will help provide that understanding.

Acknowledgments: We are grateful to Moshe Vardi for his valuable suggestion that led to a dramatic improvement in the complexity of the decision procedure in the nonmeasurable case, and for his other comments and constructive criticisms. We thank Martín Abadi for a careful reading of the paper, and for numerous helpful suggestions. Finally, we thank Dexter Kozen for bringing Canny's work on real closed fields to our attention.

References

[AH94] M. Abadi and J.Y. Halpern. Decidability and expressiveness for first-order logics of probability. *Information and Computation*, 112(1):1–36, 1994.

[Bac90] F. Bacchus. *Representing and Reasoning with Probabilistic Knowledge.* MIT Press, Cambridge, Mass., 1990.

[Ber80] L. Berman. The complexity of logical theories. *Theoretical Computer Science*, 11:71–77, 1980.

[BKR86] M. Ben-Or, D. Kozen, and J. H. Reif. The complexity of elementary algebra and geometry. *Journal of Computer and System Sciences*, 32(1):251–264, 1986.

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

[Car50] R. Carnap. *Logical Foundations of Probability.* University of Chicago Press, Chicago, 1950.

[Chv83] V. Chvátal. *Linear Programming.* W. Freeman and Co., San Francisco, Calif., 1983.

[Dem68] A. P. Dempster. A generalization of Bayesian inference. *Journal of the Royal Statistical Society, Series B*, 30:205–247, 1968.

[End72] H. B. Enderton. *A Mathematical Introduction to Logic.* Academic Press, New York, 1972.

[Far02] J. Farkas. Theorie der enfachen ungleichungen. *J. Reine und Angewandte Math.*, 124:1–27, 1902.

[Fel57] W. Feller. *An Introduction to Probability Theory and its Applications*, volume 1. John Wiley & Sons, New York, 2nd edition, 1957.

[Fel84] Y. Feldman. A decidable propositional probabilistic dynamic logic with explicit probabilities. *Information and Control*, 63:11–38, 1984.

[FH91] R. Fagin and J. Y. Halpern. Uncertainty, belief, and probability. *Computational Intelligence*, 7(3):160–173, 1991.

[FH94] R. Fagin and J. Y. Halpern. Reasoning about knowledge and probability. *Journal of the ACM*, 41(2):340–367, 1994.

[FHM88] R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. In *Proc. 3rd IEEE Symp. on Logic in Computer Science*, pages 277–291, 1988.

[Fou26] J. B. J. Fourier. Solution d'une question particulière du calcul des inégalités. *Nouveau Bulletin des Sciences par la Société philomathique de Paris*, pages 99–100, 1826.

[FR74] M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. In R. M. Karp, editor, *Complexity of Computation, SIAM-AMS Proceedings, Vol. 7*, pages 27–42, 1974.

[Gai64] H. Gaifman. Concerning measures in first order calculi. *Israel Journal of Mathematics*, 2:1–18, 1964.

[Gai86] H. Gaifman. A theory of higher order probabilities. In J. Y. Halpern, editor, *Theoretical Aspects of Reasoning about Knowledge: Proc. 1986 Conference*, pages 275–292. Morgan Kaufmann, San Francisco, Calif., 1986.

[GF87] H. Guggenheimer and R. S. Freedman. Foundations of probabilistic logic. In *Proc. Tenth International Joint Conference on Artificial Intelligence (IJCAI '87)*, pages 939–941, 1987.

[GKP88] G. Georgakopoulos, D. Kavvadias, and C. H. Papadimitriou. Probabilistic satisfiability. *Journal of Complexity*, 4(1):1–11, 1988.

[Hal50] P. Halmos. *Measure Theory*. Van Nostrand, 1950.

[Hal67] M. Hall, Jr. *Combinatorial Theory*. Blaisdell, 1967.

[Hal90] J. Y. Halpern. An analysis of first-order logics of probability. *Artificial Intelligence*, 46:311–350, 1990.

[HF87] P. Haddawy and A. M. Frisch. Convergent deduction for probabilistic logic. In *Proc. Third AAAI Uncertainty in Artificial Intelligence Workshop*, 1987.

[Hoo78] D. N. Hoover. Probability logic. *Annals of Mathematical Logic*, 14:287–313, 1978.

[HR87] J. Y. Halpern and M. O. Rabin. A logic to reason about likelihood. *Artificial Intelligence*, 32(3):379–405, 1987.

[HT93] J. Y. Halpern and M. R. Tuttle. Knowledge, probability, and adversaries. *Journal of the ACM*, 40(4):917–962, 1993.

[Kav89] D. Kavvadias. *Complexity of Probabilistic Logic*. PhD thesis, Patras University, 1989. (In Greek.).

[Kei85] H. J. Keisler. Probability quantifiers. In J. Barwise and S. Feferman, editors, *Model-Theoretic Logics*, pages 509–556. Springer-Verlag, Berlin/New York, 1985.

[Koz85] D. Kozen. Probabilistic PDL. *Journal of Computer and System Sciences*, 30:162–178, 1985.

[Kuh56] H. W. Kuhn. Solvability and consistency for linear equations and inequalities. *American Mathematical Monthly*, 63:217–232, 1956.

[LS82] D. Lehmann and S. Shelah. Reasoning about time and chance. *Information and Control*, 53:165–198, 1982.

[Luk70] J. Lukasiewicz. Logical foundations of probability theory. In L. Berkowski, editor, *Jan Lukasiewicz Selected Works*, pages 16–43. North-Holland, Amsterdam, 1970.

[Men64] E. Mendelson. *Introduction to Mathematical Logic*. Van Nostrand, New York, 1964.

[Mot56] T. S. Motzkin. The assignment problem. In J. H. Curtiss, editor, *Numerical Analysis*, Proc. Symposia in Applied Mathematics, Vol. VI, pages 109–125. McGraw-Hill, New York, 1956.

[Nil86] N. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28:71–87, 1986.

[Nut87] J. T. Nutter. Uncertainty and probability. In *Proc. Tenth International Joint Conference on Artificial Intelligence (IJCAI '87)*, pages 373–379, 1987.

[Rot64] G. C. Rota. On the foundations of combinatorial theory, I. Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 2:340–368, 1964.

[Roy64] H. L. Royden. *Real Analysis*. Macmillan, 1964.

[Sch86] A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, New York, 1986.

[Sha76] G. Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, Princeton, N.J., 1976.

[Sho67] J. R. Shoenfield. *Mathematical Logic*. Addison-Wesley, Reading, Mass., 1967.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. Univ. of California Press, 2nd edition, 1951.