REASONING ABOUT KNOWLEDGE AND PROBABILITY:

Preliminary Report

Ronald Fagin
Joseph Y. Halpern

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

Abstract: We provide a model for reasoning about knowledge and probability together. We allow explicit mention of probabilities in formulas, so that our language has formulas that essentially say "according to agent i, formula φ holds with probability at least α." The language is powerful enough to allow reasoning about higher-order probabilities, as well as allowing explicit comparisons of the probabilities an agent places on distinct events. We present a general framework for interpreting such formulas, and consider various properties that might hold of the interrelationship between agents' subjective probability spaces at different states. We provide a complete axiomatization for reasoning about knowledge and probability, prove a small model property, and obtain decision procedures. We then consider the effects of adding common knowledge and a probabilistic variant of common knowledge to the language.

1 Introduction

Reasoning about knowledge has become an active topic of investigation for researchers in such diverse fields as philosophy [Hin62], economics [Aum76], and artificial intelligence [Moo85]. Recently the interest of theoretical computer scientists has been sparked, since reasoning about knowledge has been shown to be a useful tool in analyzing distributed systems (see [Hal87] for an overview and further references).

In many of the application areas for reasoning about knowledge, it is important to be able to reason about the probability of certain events as well as the knowledge of agents. In particular, this arises in distributed systems applications when we want to analyze randomized or probabilistic programs. Not surprisingly, researchers have considered knowledge and probability before. Indeed, all the works in economics on reasoning about knowledge, going back to Aumann's seminal paper [Aum76], have probability built into the model. However, they do not consider a logical language that explicitly allows reasoning about probability. In this paper we consider a language which extends the traditional logic of knowledge by allowing explicit reasoning about probability along the lines discussed in a companion paper [FHM88].

In the standard possible-worlds model of knowledge (which we briefly review in the next section), agent *i knows* a fact φ, written $K_i\varphi$, in a *world* or *state* s if φ is true in all the worlds the agent considers possible in world s. We want to reason not only about an agent's knowledge, but also about the subjective probability he places on certain events. In order to do this, we extend the language considered in [FHM88], which is essentially a formalization of Nilsson's probability logic [Nil86]. Typical formulas in the logic of [FHM88] include $m(\varphi) \geq 2m(\psi)$ and $m(\varphi) < 1/3$, where φ and ψ are propositional formulas. These formulas can be viewed as saying "φ is twice as probable as ψ" and "φ has probability less than 1/3", respectively. Since we want to reason about agent i's subjective probability, we modify their language to allow formulas such as $m_i(\varphi) \geq 2m_i(\psi)$. We also allow φ and ψ here to be arbitrary formulas (which may themselves contain nested occurences of the modal operators m_j and K_j) rather than just propositional formulas. This gives us the power to reason about higher-order probabilities (see [Gai86] for more discussion on this subject, as well as added references) and to reason about the probability that an agent knows a certain fact.

In order to give semantics to such a language in the possible-worlds framework, roughly speaking, we assume that at each state each agent has a probability on the worlds he considers possible. Then a formula such as $m_i(\varphi) \geq 2m_i(\psi)$ is true at state s if, according to agent i's subjective probability at state s, the event φ is twice as probable as ψ. For technical and philosophical reasons, we find it convenient to view the probability in general as being placed on a subset of the worlds that the agents considers possible, rather than the set of all worlds that the agent considers possible in a given state. As we shall show by example, different choices for the probability space seem to correspond to different assumptions about the background context.

Despite the richness of the resulting language, we can combine the the well-known techniques for reasoning about knowledge with the techniques for reasoning about probability introduced in [FHM88] to obtain an elegant complete axiomatization for the resulting language. Just as there are different assumptions we can make about the relationship between the worlds that agent i considers possible, leading to different axioms for knowledge (see [HM85] for an overview), there are also different assumptions about the interrelationships between agents' subjective probability spaces at different states, which also can be captured axiomatically. We discuss these assumptions and their appropriateness, and show how these assumptions can effect the complexity of the decision procedure for the language.

This paper is closely related to a number of other works. Propositional probabilistic variants of temporal logic [HS84,LS82] and dynamic logic [Fel84, Koz85] have also been studied, with the goal of analyzing probabilistic programs. Probabilistic temporal logic papers have traditionally limited the language so that the only probabilistic statements that can be made are Boolean combinations of formulas of the form "φ occurs with probability one." The logics studied in [Fel84,Koz85] do bear some superficial resemblance to ours in that explicit probability statements are allowed, as well as linear combinations of statements. Indeed, the probability logic considered in [FHM88], where the only formulas in the scope of the modal operator m are propositional formulas, is a fragment of Feldman's logic. However, there are some fundamental differences as well, which arise from the fact that the main object of interest in these other logics are programs. As a result, our language and those used in [Fel84,Koz85] are incomparable. The languages used in [Fel84,Koz85] are richer than the one we consider here in that they allow explicit reasoning about programs, but poorer in that they can talk about the probability of only a restricted class of formulas. Moreover, there are significant technical differences in the semantics of knowledge operators (our K_i's) and the program operators of [Fel84,Koz85].

There are two other papers that consider reasoning about knowledge and uncertainty in a possible worlds framework somewhat similar to our own. Halpern and McAllester [HM84a] consider a language that allows reasoning about knowledge and likelihood, but their notion of likelihood, based on the logic of likelihood of [HR87], considers only a qualitative notion of likelihood, rather than explicit probabilities. While this may be appropriate for some applications, it is not useful for an analysis of protocols. Ruspini [Rus87] discusses certain relations that hold between knowledge and probability in the one-agent case, and relates this in turn to Dempster-Shafer *belief functions* [Sha79].

The rest of this paper is organized as follows. The next section contains a brief review of the classical possible-worlds semantics for knowledge and a discussion of how knowledge can be ascribed to processes in a distributed system. In Section 3 we describe the extended language for knowledge and probability and discuss some assumptions that can be placed on the interrelationships between agents' subjective probability spaces at different states. In section 4 we state our results on complete axiomatizations and decision procedures (detailed proofs are left to the full paper). In Section 5 we extend the language to allow common knowledge and probabilistic common knowledge. In Section 6 we give our conclusions.

2 The standard Kripke model for knowledge

In this section we briefly review the standard S5 possible-worlds semantics for knowledge. The reader is referred to [HM85] for more details.

In order to reason formally about knowledge we need a language. Suppose we consider a system with n agents, say $1, \ldots, n$, and we have a set Φ_0 of primitive propositions about which we wish to reason. (For distributed systems applications these will typically represent statements such as "the value of variable x is 0"; in natural language situations they might represent statements of the form "It is raining in San Francisco.") We construct more complicated formulas by closing off Φ_0 under conjunction, negation, and the modal operators K_i, $i = 1, \ldots, n$ (where $K_i\varphi$ is read "agent i knows φ").

We give semantics to these formulas by means of *Kripke structures* [Kri63], which formalize the intuitions behind possible worlds. A *Kripke structure for knowledge* (for n agents) is a tuple $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$, where S is a set of *states* (thought of as states of affairs or possible worlds), $\pi(s)$ is a truth assignment to the primitive propositions of Φ_0 for each state $s \in S$ (i.e., $\pi(s)(p) \in \{\mathbf{true}, \mathbf{false}\}$ for each primitive proposition $p \in \Phi_0$ and state $s \in S$), and $\mathcal{K}_i$ is an equivalence relation on the states of S, for $i = 1, \ldots, n$. The $\mathcal{K}_i$ relation is intended to capture the possibility relation according to agent i: $(s, t) \in \mathcal{K}_i$ if in world s agent i considers t a possible world.[1] We define $\mathcal{K}_i(s) = \{s' \mid (s, s') \in \mathcal{K}_i\}$.

We now assign truth values to formulas at a state in a structure. We write $(M, s) \models \varphi$ if the formula φ is true at state s in Kripke structure M.

$(M, s) \models p$ (for $p \in \Phi_0$) iff $\pi(s)(p) = \mathbf{true}$
$(M, s) \models \varphi \wedge \psi$ iff $(M, s) \models \varphi$ and $(M, s) \models \psi$
$(M, s) \models \neg\varphi$ iff $(M, s) \not\models \varphi$
$(M, s) \models K_i\varphi$ iff $(M, t) \models \varphi$ for all $t \in \mathcal{K}_i(s)$.

The last clause in this definition captures the intuition that agent i knows φ in world (M, s) exactly if φ is true in all worlds that i considers possible.

Given a structure $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$, we say a formula is φ is *valid in M*, and write $M \models \varphi$, if $(M, s) \models \varphi$ for every state s in S, and say that φ is *satisfiable in M* if $(M, s) \models \varphi$ for some state s in S. We say a formula φ is *valid* if it is valid in all structures, and it is *satisfiable* if it is satisfiable in some structure. It is easy to check that a formula φ is valid in M (resp. valid) if and only if $\neg\varphi$ is not satisfiable in M (resp. not satisfiable).

It is well known that the following set of axioms and inference rules, which goes back to Hintikka [Hin62], provides a complete axiomatization for the notion of knowledge that we are considering. That is, each of the axioms below is valid, the inference rules preserve validity, and all valid formulas can be proved from these axioms and rules (see [HM85] for a proof):

K1. All instances of propositional tautologies
K2. $(K_i\varphi \wedge K_i(\varphi \Rightarrow \psi)) \Rightarrow K_i\psi$
K3. $K_i\varphi \Rightarrow \varphi$
K4. $K_i\varphi \Rightarrow K_iK_i\varphi$
K5. $\neg K_i\varphi \Rightarrow K_i\neg K_i\varphi$

R1. From φ and $\varphi \Rightarrow \psi$ infer ψ (modus ponens)
R2. From φ infer $K_i\varphi$ (knowledge generalization)

While philosophers have spent years debating the appropriateness of this approach for capturing the notion of knowledge as applied to human reasoning (see [Len78] for a review of the pertinent literature), there are many applications in distributed systems where it has proved

---

[1] We could take $\mathcal{K}_i$ to be an arbitrary binary relation, but for distributed systems applications, taking it to be an equivalence relation seems most appropriate (see [Hal86] for further discussion of this point).

quite useful (see [Hal87] for an overview). We now briefly review how knowledge is ascribed to processes in distributed systems. More details on the model can be found in [Hal86].

A distributed system consists of a collection of processes, say $1, \ldots, n$, connected by a communication network. We think of these processes as running some protocol. At any time in the execution of such a protocol, the system is in some *global state*, which is a tuple of the form $\langle e, l_1, \ldots, l_n \rangle$, where l_i is the local state of process i, and e is the state of the *environment*. We think of the global state as providing a "snapshot" of the state of the system at any time. The environment includes everything that we consider relevant to the system that is not described in the state of the processes. A *run* of a system is just a function from the natural numbers to global states. Intuitively, a run describes a possible execution of a system over time (where we think of time as ranging over natural numbers). We identify a system with a set of runs (these can be thought of as the possible runs of the system when running a particular protocol). We often speak of a pair (r, m), consisting of a run r and a time m, as a *point*. Associated with any point (r, m) we have $r(m)$, the global state of the system at this point. We can define equivalence relations $\sim_i$, for $i = 1, \ldots, n$, on points via $(r, m) \sim_i (r', m')$ iff process i has the same local state at the global states $r(m)$ and $r'(m')$.

Suppose we fix a set Φ_0 of primitive propositions. We define an interpreted system $\mathcal{I}$ to be a pair $(\mathcal{R}, \pi)$, where $\mathcal{R}$ is a system (set of runs), and π is a truth assignment to the primitive propositions of Φ_0 at every point in $\mathcal{R}$. With this definition, it is easy to view an interpreted system as a Kripke structure, where the points play the role of states and the $\mathcal{K}_i$ relation is given by $\sim_i$. In particular, we have

$$(\mathcal{I}, r, m) \models K_i\varphi \text{ iff } (\mathcal{I}, r', m') \models \varphi \text{ for all } (r', m') \text{ such that } (r', m') \sim_i (r, m).$$

3 Adding probability

The formula $K_i\varphi$ says that φ is true at all the worlds that agent i considers possible. We want to extend our language to allows formulas such as $m_i(\varphi) \geq \alpha$, which intuitively says that "according to agent i, formula φ holds with probability at least α." In fact, it turns out to be convenient to extend the language even further. Specifically, if $\varphi_1, \ldots, \varphi_k$ are formulas, then so is $\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha$, where $\theta_1, \ldots, \theta_k, \alpha$ are arbitrary real numbers, and $k \geq 1$. We call such a formula an *i-probability formula*. An expression of the form $\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k)$ is called a *term*. Allowing arbitrary linear combinations of terms in i-probability formulas gives us a great deal of flexibility in expressing relationships between probabilities of events. Notice we do not allow mixed formulas such as $m_i(\varphi) + m_j(\psi) \geq \alpha$.[2]

We use a number of abbreviations throughout the paper for readability. For example, we use $m_i(\varphi) \geq m_i(\psi)$ as an abbreviation for $m_i(\varphi) - m_i(\psi) \geq 0$, $m_i(\varphi) \leq \alpha$ for $-m_i(\varphi) \geq -\alpha$, $m_i(\varphi) < \alpha$ for $\neg(m_i(\varphi) \geq \alpha)$, and $m_i(\varphi) = \alpha$ for $(m_i(\varphi) \geq \alpha) \wedge (m_i(\varphi) \leq \alpha)$. We also use $K_i^\alpha(\varphi)$ as an abbreviation for $K_i(m_i(\varphi) \geq \alpha)$. Intuitively, this says that "agent i knows that the probability of φ is greater than or equal to α."

---

[2] There would be no difficulty giving semantics to such formulas, but some of our results on decision procedures and axiomatizations seem to require that we not allow such mixed formulas. We return to this point in the next section.

The language used here extends that considered in [FHM88] in two ways. First, rather than have just one "probability modality" m, we have a modality m_i for each agent i, to capture the idea of subjective probability. Secondly, rather than restricting the formulas that appear in the scope of the probability modality to be propositional, we allow them to be arbitrary. In particular, we allow higher-order probability formulas such as $m_i(m_j(\varphi) \geq \alpha)) \geq \beta$.

Before we give formal semantics to this language, we briefly review some material from probability theory (see [Fel57] or any other basic text on probability theory for more details). A ***probability space*** is a tuple (Ω, X, μ) where Ω is a set, X is a σ-algebra of subsets of Ω (i.e., a set of subsets containing Ω and closed under complementation and countable union), whose elements are called the ***measurable sets***, and a probability measure μ defined on the elements of X. Note that μ does not assign a probability to all subsets of Ω, but only to the measurable sets. The ***inner measure*** μ_* corresponding to μ is defined on all subsets of Ω; if $A \subseteq \Omega$, we have

$$\mu_*(A) = \sup\{\mu(B) \mid B \subseteq A \text{ and } B \in X\}.$$

Thus, the inner measure of A is essentially the measure of the largest measurable set contained in A. The properties of probability spaces guarantee that μ_* is well defined, and that if A is measurable, then $\mu_*(A) = \mu(A)$.

Given a structure $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$, in order to decide whether a probability formula is true at a state s in M, we need to associate with each state s a probability space. Thus we take a ***Kripke structure for knowledge and probability*** (for n agents) to be a tuple $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$, where $\mathcal{P}$ is a function that assigns to each agent $i \in \{1, \ldots, n\}$ and state $s \in S$ a probability space $\mathcal{P}(i, s)$. We shall usually write $\mathcal{P}(i, s)$ as $\mathcal{P}_{i,s} = (S_{i,s}, X_{i,s}, \mu_{i,s})$. Intuitively, the probability space $\mathcal{P}_{i,s}$ describes agent i's subjective probability distribution at state s. It seems unreasonable for agent i to assume that there is any positive probability on a subset of worlds that he does not consider possible; thus we assume in the remainder of the paper that $S_{i,s} \subseteq \mathcal{K}_i(s)$. It might seem reasonable to take $S_{i,s} = \mathcal{K}_i(s)$, but, as we shall see below, there are good technical and philosophical reasons to allow $S_{i,s}$ to be a proper subset.[3]

We can give semantics to formulas not involving probability just as before. To give semantics to i-probability formulas, assume inductively we have defined $(M, s) \models \varphi$ for each state $s \in S$. Define $S_{i,s}(\varphi) = \{s' \in S_{i,s} \mid (M, s') \models \varphi\}$. Then the obvious way to define the semantics of a formula such as $\mu_i(\varphi) \geq \alpha$ is

$$(M, s) \models m_i(\varphi) \geq \alpha \text{ iff } \mu_{i,s}(S_{i,s}(\varphi)) \geq \alpha.$$

The only problem with this definition is that the set $S_{i,s}(\varphi)$ might not be measurable (i.e., not in $X_{i,s}$), so that $\mu_{i,s}(S_{i,s}(\varphi))$ might not be well defined. We discuss this issue in more detail below (and, in fact, provide sufficient conditions to guarantee that this set is measurable), but in order to deal with this problem in general, we use the inner measures $(\mu_{i,s})_*$ rather than $\mu_{i,s}$. Thus $m_i(\varphi) \geq \alpha$ is true at the state s if there is some measurable set (according to agent i) contained in $S_{i,s}(\varphi)$ whose measure is at least α. More generally, we have

$$(M, s) \models \theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha \text{ iff } \theta_1(\mu_{i,s})_*(S_{i,s}(\varphi_1)) + \cdots + \theta_k(\mu_{i,s})_*(S_{i,s}(\varphi_k)) \geq \alpha.$$

---

[3] It is easy to extend $\mu_{i,s}$ to a measure on any superset T of $S_{i,s}$ by simply taking $T - S_{i,s}$ to be a measurable set with measure 0. Thus we always can, if we like, think of the measure as really being defined on $\mathcal{K}_i(s)$.

This completes the semantic definition for the whole language.

Before we discuss the properties of this language, it is helpful to consider a detailed example. This example illustrates some of the subtleties involved in choosing the probability spaces at each state.

Suppose we have two agents. Agent 2 has an input bit, either 0 or 1. He then tosses a fair coin, and performs an action a if the coin toss agrees with the input bit, i.e., if the coin toss lands heads and the input bit is 1, or if the coin lands tails and the input bit is 0. We assume that agent 1 never learns agent 2's input bit or the outcome of his coin toss. From agent 1's viewpoint, if agent 2's input bit is 0, then the probability that agent 2 performs action a is 1/2 (since the probability of the coin landing heads is 1/2); similarly, if agent 2's input bit is 1, then the probability of agent 2 performing action a is 1/2. Thus, it seems reasonable to say that agent 1 knows that the *a priori* probability of agent 2 performing action a is 1/2. Note that we do not need to assume a probability distribution on the input bits for this argument to hold. Indeed, it holds independent of the probability distribution, and even if there is no probability distribution on the input bit.

Now suppose we want to capture this argument in our formal system. From agent 1's point of view, there are four possibilities: $(1,h),(1,t),(0,h),(0,t)$ (the input bit was 1 and the coin landed heads, the input bit was 1 and the coin landed tails, etc.). We can view these as the possible worlds or states in a Kripke structure. Call them s_1, s_2, s_3, and s_4 respectively; let S be the set consisting of all four states. Assume that we have primitive propositions A, H, T, B_0, and B_1 in the language, denoting the events that action a is performed, the coin landed heads, the coin landed tails, agent 2's input bit is 0, and agent 2's input bit is 1. Thus H is true at states s_1 and s_3, A is true at states s_1 and s_4, and so on. To simplify the discussion, suppose that somehow we have decided what agent 2's subjective probability space is at each state. What should agent 1's subjective probability space be? We now describe three plausible answers to this question.

1. We can associate with each state the probability space consisting of all four states, i.e., all the possible worlds. In this case, the only candidates for measurable sets (besides the whole space and the empty set) are $\{s_1, s_3\}$ (which corresponds to the event "the coin landed heads") and $\{s_2, s_4\}$. Each of these sets has probability 1/2. Call the resulting Kripke structure M_0. Note that we cannot take $\{s_1\}$ to be a measurable set, since we have no probability on the input bit being 1. We also cannot take $\{s_1, s_4\}$, which corresponds to the event "action a is performed", to be measurable. This is because if it were measurable, then, since the set of measurable sets is closed under finite intersection, we would have to take $\{s_1\}$ to be measurable.
2. We can associate with states s_1 and s_2, where the input bit is 1, the probability space consisting only of s_1 and s_2, with $\{s_1\}$ and $\{s_2\}$ both being measurable and having measure 1/2. Similarly, we can associate with states s_3 and s_4 the probability space consisting only of s_3 and s_4, with $\{s_3\}$ having measure 1/2. Thus, when the input bit is 1, we take the probability space to consist of only those states where input bit is 1, with the obvious probability on that space; similarly for when the input bit is 0. Call this Kripke structure M_1.
3. Finally, we can make the trivial choice of associating with each state the probability space consisting of that state alone, and giving it measure 1. Call the resulting Kripke structure

M_2.

Of the three Kripke structures above, it is easy to see that only M_1 supports the informal reasoning above. It is easy to check that we have $(M_1, s) \models K_1^{1/2} A$, for every state $s \in S$. On the other hand, in every state of M_2, we have either $m_1(A) = 1$ (in states s_1 and s_4) or $m_1(A) = 0$ (in states s_2 and s_3). Thus, for every state $s \in S$, we have $(M_2, s) \models K_1(m_1(A) = 1 \vee m_1(A) = 0)$ and $(M_2, s) \models \neg K_1^{1/2} A$. Finally, in M_0, the event A is not measurable, nor does it contain any non-empty measurable sets. Thus, we have $(M_0, s) \models K_1(m_1(A) = 0)$ (where now m_1 represents the inner measure, since A is not measurable).

Does this mean that M_1 is somehow the "right" Kripke structure for this situation? Not necessarily. A better understanding can be attained if we think of this as a two-step process developing over time. At the first step, "nature" (nondeterministically) selects agent 2's input bit. Then agent 2 tosses the coin. We can think of M_2 as describing the situation after the coin has landed. It does not make sense to say that the probability of heads is 1/2 at this time (although it does make sense to say that the *a priori* probability of heads is 1/2), nor does it make sense to say that the probability of performing action a is 1/2. After the coin has landed, either it landed heads or it didn't; either a was performed or it wasn't. This is the intuitive explanation for why the formula $K_1((m_1(A) = 1) \vee (m_1(A) = 0))$ is valid in M_2. M_1 describes the situation after nature has made her decision, but before the coin is tossed. Thus, agent 1 knows that either the input bit is 1 or the input bit is 0 (although he doesn't know which one). As expected, the formula $K_1((m_1(B_0) = 1) \vee (m_1(B_1) = 0))$ holds in this situation. M_0 can be viewed as describing the initial situation, before nature has made her decision. At this point the event "the input bit is 0" is not measurable and we cannot attach a probability to it.

We can capture these intuitions nicely using runs. There are four runs, say r_1, r_2, r_3, r_4, corresponding to the four states above. There are three relevant times: 0 (before nature has decided on the input bit), 1 (after nature has decided, but before the coin is tossed), and 2 (after the coin is tossed). Agent 1's local state contains only the time (since agent 1 never learns anything about the coin or the input bit); agent 2's local state contains the time, the input bit (at times 1 and 2), and the outcome of the coin toss (at time 2). We can omit the environment from the global state; everything relevant is already captured by the states of the agents. Thus, for example, $r_3(1) = \langle 1, (1, 0) \rangle$ and $r_3(2) = \langle 2, (2, 0, h) \rangle$. We now interpret the propositons A, H, etc. to mean that the action a has been or eventually will be performed, heads has been or eventually will be tossed, etc. Thus, proposition A is true at the point (r_j, k) if the action a is performed at $(r_j, 3)$. Similarly, H is true at (r_j, k) if heads is tossed in run r_j, and so on.

Clearly at each time $k = 0, 1, 2$, agent 1 considers the four points (r_j, k), $j = 1, 2, 3, 4$, possible. At time 0 we can add on a probability structure to make this look like M_0. At time 1, defining the probability spaces so that we get Kripke structure M_1 seems to be appropriate, while at time 2, Kripke structure M_2 seems appropriate. Thus, although it seems that in some sense agent 1's knowledge about the input bit and the outcome of the coin toss does not change over time, the subjective probability spaces used by agent 1 may change (for example, to reflect the fact that the coin has been tossed).

Even in this simple example we can already see that the decision of how to assign the probability spaces is not completely straightforward. In general, it seems that it will depend in more detail on the form of the analysis. This example already shows that in general at a state

s, we do not want to take $S_{i,s} = \mathcal{K}_i(s)$. Note that $S_{i,s} = \mathcal{K}_i(s)$ only in M_0 above; in particular, in M_1, where we can carry out the informal reasoning which says that action a occurs with probability 1/2, we have $S_{i,s}$ as a strict subset of $\mathcal{K}_i(s)$.[4]

Observe that in our example, at every point (r, k), we took the probability space to consist of all (r', k) such that $r(k) = r'(k)$; i.e., all the points with the same global state. Moreover, if we had included agent 2 in the discussion, we would have assigned agent 2 exactly the same subjective probability space as agent 1 at every point.

In fact, the probability here is not subjective at all. It is an *objective* probability, generated by the toss of the coin. Although the agents have different sets of points they consider possible, they agree on what the probability space is at each point. This is a quite natural assumption in distributed systems. Intuitively, if the agents had complete information about the global state of the system, they would agree on what the appropriate probability space should be.[5]

In the context of a Kripke structure for knowledge and probability where $\mathcal{P}_{i,s}$ is agent i's probability space at state s, objective probability corresponds to the condition:

OBJ. $\mathcal{P}_{i,s} = \mathcal{P}_{j,s}$ for all s and all agents i, j.

Because of our assumption that $S_{i,s} \subseteq \mathcal{K}_i(s)$, it follows that OBJ implies that $S_{i,s} \subseteq \mathcal{K}_j(s)$ for all states s and agents i and j. Thus, if we had required that $S_{i,s} = \mathcal{K}_i(s)$ for each agent i, then OBJ could hold only in Kripke structures where $\mathcal{K}_i(s) = \mathcal{K}_j(s)$ for all states s and agents i and j.

We now consider some other assumptions about the interrelationship between an agent's subjective probability spaces at different states. A rather natural assumption to make on the choice of probability space is that it is the same in all worlds the agent considers possible. In the context of distributed systems, this would mean that an agent's probability space is determined by his local state. We call this property SDP (*state-determined probability*). Formally, we have:

SDP. $(s, s') \in \mathcal{K}_i$ implies $\mathcal{P}_{i,s} = \mathcal{P}_{i,s'}$.

Of the three Kripke structures we considered above, only M_0 satisfies SDP. It seems that SDP is most natural where there are no nondeterministic choices that have been made by "nature". SDP is an assumption that has often been made. Indeed, it is implicitly assumed in much of the economists' work (e.g. [Aum76,Cav83]). In these papers it is assumed that each agent views the set S of all worlds as a probability space. Thus, for each agent i we have a probability space $\mathcal{P}_i = (S, X_i, \mu_i)$.[6] Agent i's subjective probability of an event e at a state s is taken to be the conditional probability of e given agent i's set of possible worlds. More formally, we have $\mathcal{P}_{i,s} = (\mathcal{K}_i(s), X_{i,s}, \mu_{i,s})$, where $X_{i,s} = \{A \cap \mathcal{K}_i(s) \mid A \in X_i\}$, and $\mu_{i,s}(A \cap \mathcal{K}_i(s)) = \mu_i(A)/\mu_i(\mathcal{K}_i(s))$.[7] Note that the resulting Kripke structure has the SDP property.

---

[4] The example presented here is a simplification of one given by Mark Tuttle. It was Mark who first pointed out to us the need to allow $S_{i,s}$ to be a proper subset of $\mathcal{K}_i(s)$.

[5] Mark Tuttle and Yoram Moses first pointed out to us that in distributed systems applications, an appropriate choice is often an objective probability with the probability space consisting of all the points with the same global state. This approach was first taken in [HMT88].

[6] Aumann actually assumes that there is an objective probability on the whole space, so that $\mathcal{P}_i = \mathcal{P}_j$ for all agents i and j. This corresponds to the agents having a common prior distribution.

[7] This approach runs into slight technical difficulties if $\mathcal{K}_i(s)$ is not measurable, or has measure 0. However, it is always assumed that this is not the case.

While M_1 and M_2 in our example above do not satisfy SDP, they do satisfy a weaker property which we call *uniformity*. Roughly speaking, uniformity holds if we can partition $\mathcal{K}_i(s)$ into subsets such that at every point in a given subset T, the probability is placed on T. More formally, uniformity holds if:

UNIF. For all i, s, and t, if $\mathcal{P}_{i,s} = (S_{i,s}, X_{i,s}, \mu_{i,s})$ and $t \in S_{i,s}$, then $\mathcal{P}_{i,t} = \mathcal{P}_{i,s}$.

Again, note that SDP is a special case of UNIF, and that all the structures in our example above satisfy UNIF.

There is one last property of interest to us, which seems to have been assumed in all previous papers involving reasoning about probability, and that is that all formulas define measurable sets. As shown in [FHM88] (and as we shall see again below), reasoning about probability is simplified if we assume that all formulas define measurable sets. More precisely, we say formulas define measurable sets in M if

MEAS. For every formula φ, the set $S_{i,s}(\varphi) \in X_{i,s}$.

Clearly if primitive propositions define measurable sets, then all propositional formulas define measurable sets. However, there is no particular reason to expect that a probability formula such as $m_i(p) + m_i(q) \geq 1/2$ will define a measurable set (in fact, it is easy to show in general it will not). Let PMEAS be the property which says that all primitive propositions define measurable sets. (Note that PMEAS does not holds in M_0, but does hold in M_1 and M_2). The following lemma describes sufficient conditions for MEAS to hold.

Lemma 3.1: *If M is a structure satisfying OBJ, UNIF, and PMEAS, then M satisfies MEAS.*

Proof: A straightforward induction on the structure of formulas φ shows that $S_{i,s}(\varphi)$ is measurable for all formulas φ. The assumption OBJ implies that for all agents i and j, the set $S_{i,s} \subseteq \mathcal{K}_j(s)$, so it is easy to see that $S_{i,s}(K_j(\varphi))$ is either $S_{i,s}$ or $\emptyset$. In either case it is measurable. Similarly, we can show that OBJ and UNIF together imply that for any probability formula φ, we have that $S_{i,s}(\varphi)$ is either $S_{i,s}$ or $\emptyset$. ∎

It seems that OBJ, UNIF, and PMEAS are often reasonable assumptions in distributed systems applications, so this lemma is of more than just pure technical interest.

4 Complete axiomatizations and decision procedures

We now describe a natural complete axiomatization for the logic of probability and knowledge. The axiom system can be modularized into several components:

I. Axiom and rule for propositional reasoning

Axiom K1 and rule R1 from section 2

II. Axioms and rule for reasoning about knowledge

Axioms K2-K5 and rule R2 from section 2

III. Axioms and rule for reasoning about probability

Any set of axioms that allow us to prove all valid i-probability formulas will do. In the measurable case (that is, where MEAS holds), the axioms below (taken from [FHM88]), together with axiom K1 and rule R1 suffice:

P1. $m_i(true) = 1$ (the probability of the event *true* is 1)
P2. $m_i(false) = 0$ (the probability of the event *false* is 0)
P3. $(\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha) \Leftrightarrow (\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) + 0 m_i(\varphi_{k+1}) \geq \alpha)$ (adding and deleting 0 terms)
P4. $(\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha) \Rightarrow (\theta_{j_1} m_i(\varphi_{j_1}) \cdots + \theta_{j_k} m_i(\varphi_{j_k}) \geq \alpha)$, if $j_1, \ldots, j_k$ is a permutation of $1, \ldots, k$ (permutation)
P5. $(\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha) \wedge (\theta'_1 m_i(\varphi_1) + \cdots + \theta'_k m_i(\varphi_k) \geq \alpha') \Rightarrow$ $(\theta_1 + \theta'_1) m_i(\varphi_1) + \cdots + (\theta_k + \theta'_k) m_i(\varphi_k) \geq (\alpha + \alpha')$ (addition of coefficients)
P6. $(\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha) \Rightarrow (\gamma\theta_1 m_i(\varphi_1) + \cdots + \gamma\theta_k m_i(\varphi_k) \geq \gamma\alpha)$ if $\gamma \geq 0$ (multiplication of coefficients)
P7. $(t \geq \alpha) \vee (t \leq \alpha)$ if t is a term (dichotomy)
P8. $(t \geq \alpha) \Rightarrow (t > \beta)$ if t is a term and $\alpha > \beta$ (monotonicity)
P9. $m_i(\varphi \wedge \psi) + m_i(\varphi \wedge \neg\psi) = m_i(\varphi)$ (measurability)
RP1. From $\varphi \Rightarrow \psi$ infer $m_i(\psi) \geq m_i(\varphi)$ (distributivity)

Things get more complicated if we drop the measurability assumption. It is easy to check that P9 is no longer sound. As shown in [FHM88], there is another axiom that we can replace P9 by to get a complete axiomatization. Fortunately, the analogue to this axiom also does the trick even in our setting. To even state the new axiom we need to introduce some notation.

Let $\mathcal{T} = \{\varphi_1, \ldots, \varphi_n\}$ be a set of formulas. Define an *atom (over $\mathcal{T}$)* to be a formula of the form $\varphi'_1 \wedge \ldots \wedge \varphi'_n$, where φ'_i is either φ_i or $\neg\varphi_i$ for each i. Define a *region (over $\mathcal{T}$)* to be a disjunction of atoms, and an *r-region (over $\mathcal{T}$)* to be a disjunction of r inequivalent atoms. Note that there are 2^{2^n} inequivalent regions. We say that R' is a *subregion* of R if R and R' are regions, and each disjunct of R' is a disjunct of R. An r-subregion of a region R is an r-region that is a subregion of R. Consider now the following axiom:

P9′. $\sum_{m=1}^{r}(-1)^{r-m}\left(\sum_{\varphi' \text{ an } m\text{-subregion of } \varphi} m(\varphi')\right) \geq 0$, if φ is an r-region.

It turns out that if we replace P9 by P9′, we get a complete axiomatization for i-probability formulas in the non-measurable case. (See [FHM88] for more details, as well as proofs of soundness and completeness).

Because we have knowledge in the picture, we need one more axiom to describe the interrelationship between knowledge and probability.

IV. Axiom relating knowledge and probability

P10. $K_i\varphi \Rightarrow (m_i(\varphi) = 1)$

Essentially, P10 captures the fact that $S_{i,s} \subseteq \mathcal{K}_i(s)$. (In particular, if we wanted to drop this assumption, we would get a complete axiomatization by dropping P10.)

Let AX_{MEAS} consist of K1-K5, P1-P10, R1, R2, and RP1, and let AX be the result of replacing P9 in AX_{MEAS} by P9′.

Theorem 4.1: *AX (resp. AX_{MEAS}) is a sound and complete axiomatization for the logic of knowledge and probability (resp. for structures satisfying MEAS).*

Proof: Soundness is straightforward, as usual, so we focus on completeness. We sketch the proof for the measurable case; the non-measurable case follows the same lines.

In order to prove completeness, we need only show that if the formula φ is consistent with AX_{MEAS}, then φ is satisfiable in a Kripke structure for knowledge and probability satisfying MEAS. Let $\mathrm{Sub}^+(\varphi)$ be the set of subformulas of φ and their negations.

Following Makinson [Mak66] (see also [HM85]), we first construct a Kripke structure for knowledge (but not probability) by letting the states be maximal consistent subsets of $\mathrm{Sub}^+(\varphi)$, where if s and t are states, then $(s,t) \in \mathcal{K}_i$ precisely if s and t contain the same formulas of the form $K_i\psi$. By the completeness of axioms K1, P1-P9 and rules R1, RP1 for reasoning about probability alone (as shown in [FHM88]), it follows that for each state s, there is a probability space that satisfies the probability formulas and negations of probability formulas of s. Furthermore, because of the axiom P10, it is possible to let the states of the probability space be $\mathcal{K}_i(s)$, in such a way that the probability of each $\psi \in \mathrm{Sub}^+(\varphi)$ is the probability of the set of states that contain ψ. Let us call the resulting Kripke structure for knowledge and probability M. As usual in Makinson-style proofs, we can then show, by induction on the structure of formulas ψ, that for each formula $\psi \in \mathrm{Sub}^+(\varphi)$, we have $\psi \in s$ iff $(M,s) \models \psi$. Since every consistent formula $\psi \in \mathrm{Sub}^+(\varphi)$ is contained in some state, it follows immediately that there is a state s (namely, a state that contains ψ) such that $(M,s) \models \psi$. This is sufficient to prove completeness, since in particular this holds when ψ is φ. The proof in the non-measurable case is essentially the same, except that now we construct an inner measure. ∎

We can also capture some of the assumptions we made about systems axiomatically. In a precise sense, OBJ corresponds to the axiom

P11. $(\theta_1 m_i(\varphi_1) + \cdots + \theta_k m_i(\varphi_k) \geq \alpha) \Rightarrow (\theta_1 m_j(\varphi_1) + \cdots + \theta_k m_j(\varphi_k) \geq \alpha)$

Axiom P11 says that each i-probability formula implies the corresponding j-probability formula. This is clearly sound if we have an objective probability distribution.

UNIF corresponds to the axiom

P12. $\varphi \Rightarrow (m_i(\varphi) = 1)$ if φ is an i-probability formula or the negation of an i-probability formula,

while SDP corresponds to the axiom

P13. $\varphi \Rightarrow K_i\varphi$ if φ is an i-probability formula or the negation of an i-probability formula.

From axiom P10 it follows that P13 implies P12, which is reasonable since SDP is a special case of UNIF. Since SDP says that agent i knows the probability space (in that it is the same for all states in $\mathcal{K}_i(s)$), it is easy to see that agent i knows all i-probability formulas. Since a given i-probability formula has the same truth value at all states where agent i's subjective probability space is the same, the soundness of P12 in structures satisfying UNIF is also easy to verify.

The same techniques used to prove Theorem 4.1 can be extended to prove

Theorem 4.2: *Let $\mathcal{A}$ be a subset of $\{OBJ, UNIF, SDP\}$, and let A be the corresponding subset of $\{P11, P12, P13\}$. Then $AX \cup A$ (resp. $AX_{MEAS} \cup A$) is a sound and complete axiomatization for the logic of knowledge and probability for structures satisfying $\mathcal{A}$ (resp. $MEAS \cup \mathcal{A}$).*[8]

As is often the case in modal logics, the ideas in our completeness proof can be extended to get a small model property and a decision procedure. In order to state our results here, we need a few definitions. Let Sub(φ) be the set of all subformulas of φ. It is easy to see that an upper bound on the size $|\mathrm{Sub}(\varphi)|$ of Sub(φ) is the number of symbols in φ, where we treat a real number as a single symbol. We also define the *size* of a Kripke structure $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$ to be the number of states in S. (Note that the size of a Kripke structure may be infinite.)

Theorem 4.3: *Let $\mathcal{A}$ be any subset of $\{MEAS, OBJ, UNIF, SDP\}$. The formula φ is satisfiable in a Kripke structure satisfying $\mathcal{A}$ iff it is satisfiable in a Kripke structure satisfying $\mathcal{A}$ of size at most $|Sub(\varphi)|2^{|Sub(\varphi)|}$ (or just $2^{|Sub(\varphi)|}$ if $MEAS \in \mathcal{A}$).*

It can be shown that this result is essentially optimal, in that there is a sequence of formulas $\varphi_1, \varphi_2, \ldots$ and a constant $c > 0$ such that (1) $|Sub(\varphi_k)| \leq ck$, (2) φ_k is satisfiable, and (3) φ_k is satisfiable only in a structure of size at least 2^n. Indeed, this exponential lower bound holds even when there is only one agent. However, if we assume that either UNIF or SDP hold, then we can get polynomial-sized models in the case of one agent.

Theorem 4.4: *If the formula φ just talks about the knowledge and probabilities of one agent and $\mathcal{A}$ is a subset of $\{MEAS, OBJ, UNIF, SDP\}$ containing either UNIF or SDP, then φ is satisfiable in a structure satisying $\mathcal{A}$ iff φ is is satisfiable in a structure of size polynomial in $|Sub(\varphi)|$ satisfying $\mathcal{A}$.*

In order to discuss the complexity of decision procedures, we must restrict attention to the case where the coefficients appearing in probability formulas are rational (since the decision procedure will involve doing rational arithmetic). In this case, all the coefficients can be represented as fractions where the numerator and denominator are both integers, so it makes sense to talk about the length of the coefficients and the length of the formula, viewed as a string of symbols. Let $|\varphi|$ be the length of the formula φ.

Theorem 4.5: *Let $\mathcal{A}$ be a subset of $\{MEAS, OBJ, UNIF, SDP\}$. If it is not the case that UNIF or SDP is in $\mathcal{A}$, then the validity problem with respect to structures satisfying $\mathcal{A}$ is complete for exponential time (i.e., there is an algorithm that decides if a formula φ is valid in all structures satisfying $\mathcal{A}$ that runs in time exponential in $|\varphi|$, and every exponential time problem can be reduced to the validity problem). If UNIF or SDP is in $\mathcal{A}$, then the validity problem with respect to structures satisfying $\mathcal{A}$ is complete for polynomial space.*

Again, if we restrict attention to the case of one agent and structures satisfying either UNIF or SDP, then we can do better.

---

[8] While it is straightforward to extend Theorem 4.1 to the case where we have mixed formulas of the form $m_i(\varphi) + m_j(\psi) \geq \alpha$ (with appropriate modifications to axioms P3, P4, P5, and P6), the situation seems much more complicated in the presence of the properties UNIF and SDP. It is due to these complexities that we did not allow such mixed formulas in our language.

Theorem 4.6: *Let $\mathcal{A}$ be a subset of $\{MEAS, OBJ, UNIF, SDP\}$ containing UNIF or SDP. For the case of one agent, the validity problem with respect to structures satisfying $\mathcal{A}$ is NP-complete.*

5 Adding common knowledge

For many of our applications, we need to reason not only about what an individual process knows, but about what everyone in a group knows, or what everyone in a group knows that everyone else in the group knows knows. *Common knowledge* can be viewed as the state of knowledge where everyone knows, everyone knows that everyone knows, everyone knows that everyone knows that everyone knows, etc.

It is easy to extend our language so that we can reason about common knowledge. We add modal operators E_G (where G is a subset of $\{1,\ldots,n\}$) and C_G, where $E_G\varphi$ and $C_G\varphi$ are read "everyone in the group G knows φ" and "φ is common knowledge among the group G", respectively.

$(M,s) \models E_G\varphi$ iff $(M,s) \models K_i\varphi$ for all $i \in G$

$(M,s) \models C_G\varphi$ iff $(M,s) \models E_G^k\varphi$ for all $k \geq 1$, where $E_G^1\varphi$ is an abbreviation for $E_G\varphi$, and $E_G^{k+1}\varphi$ is an abbreviation for $E_G E_G^k\varphi$.

It is well known (again, see [HM85]) that we can get a complete axiomatization for the language of knowledge and common knowledge by adding the following axioms and rule of inference to the axiom system described in Section 2:

C1. $E_G\varphi \equiv \bigwedge_{i\in G} K_i\varphi$
C2. $(C_G\varphi \wedge C_G(\varphi \Rightarrow \psi)) \Rightarrow C_G\psi$
C3. $C_G\varphi \equiv E_G(\varphi \wedge C_G\varphi)$
RC1. From $\varphi \Rightarrow E_G\varphi$ infer $\varphi \Rightarrow C_G\varphi$.

Axiom C3, called the *fixed point axiom*, says that $C_G\varphi$ can be viewed as a fixed point of the equation $X \equiv E_G(\varphi \wedge X)$. In fact, with a little work it can be shown to be the greatest fixed point of this equation, that is, it is implied by all other fixed points. For most of our applications, it is the fixed point characterization of common knowledge that is essential to us (see [HM84b] for a discussion of fixed points). The rule of inference RC1 is called the induction rule. The reason is that from the fact that $\varphi \Rightarrow E_G\varphi$ is valid, we can easily show by induction on k that $\varphi \Rightarrow E_G^k\varphi$ is valid for all k. It follows that $\varphi \Rightarrow C_G\varphi$ is valid.

It is perhaps not surprising that if we augment AX_{MEAS} with the axioms for common knowledge, we get a complete axiomatization for the language of knowledge, common knowledge, and probability for structures satisfying MEAS. If we want to deal with non-measurable structures, we must use the axiom system AX rather than AX_{MEAS}. And again we get small model theorems and an exponential-time complete decision procedure (regardless of what additional assumptions among MEAS, OBJ, UNIF, and SDP we make). The proofs involve a combination of the techniques for dealing with common knowledge, and the techniques for probability introduced in [FHM88] and the previous section. We omit details here.

In [HM84b] it was observed that common knowledge is often not attainable in practical distributed systems, but weaker variants of it are. One obvious variant to consider is a probabilistic variant (indeed, this was already mentioned as something to consider in [HM84b]). Recall that we defined $K_i^\alpha \varphi$ to be an abbreviation for $K_i(m_i(\varphi) \geq \alpha)$. We now extend our syntax to allow modal operators of the form E_G^α and C_G^α. We define

$(M, s) \models E_G^\alpha \varphi$ iff $(M, s) \models K_i^\alpha \varphi$ for all $i \in G$.

By analogy to $C_G\varphi$, we want $C_G^\alpha \varphi$ to be the greatest fixed point of the equation $X \equiv E_G^\alpha(\varphi \wedge X)$. The obvious analogue to the definition of $C_G\varphi$, namely, $E_G^\alpha \varphi \wedge (E_G^\alpha)^2 \varphi \wedge \ldots$ does not work. (We give a counterexample in the full paper.) However, a slight variation does work. Define $(F_G^\alpha)^0 \varphi = \mathit{true}$ and $(F_G^\alpha)^{k+1} \varphi = E_G^\alpha(\varphi \wedge (F_G^\alpha)^k \varphi)$. Then we take

$$(M, s) \models C_G^\alpha \varphi \text{ iff } (M, s) \models (F_G^\alpha)^k \varphi \text{ for all } k \geq 1.$$

We remark that this actually is a generalization of the non-probabilistic case. The reason is that if we define $F_G^0 \varphi = \mathit{true}$ and $F_G^{k+1} \varphi = E_G(\varphi \wedge F_G^k \varphi)$, then we get $F_G^k \varphi \equiv E_G^k \varphi$. This is because $E_G(\varphi \wedge \psi) \equiv E_G\varphi \wedge E_G\psi$ and $E_G\varphi \Rightarrow \varphi$. The analogous facts do not hold once we add probabilities, as we have already observed.

The following lemma shows that this definition indeed does have the right properties:

Lemma 5.1: *$C_G^\alpha \varphi$ is the greatest fixed point solution of the equation $X \equiv E_G^\alpha(\varphi \wedge X)$.*

It is now easy to check that we have the following analogues to the axioms for E_G and C_G.

CP1. $E_G^\alpha \varphi \equiv \bigwedge_{i \in G} K_i^\alpha \varphi$.
CP2. $C_G^\alpha \varphi \equiv E_G^\alpha(\varphi \wedge C_G^\alpha \varphi)$
RCP1. From $\psi \Rightarrow E_G^\alpha(\psi \wedge \varphi)$ infer $\psi \Rightarrow C_G^\alpha \varphi$.

We remark that these axioms and rule of inference are sound for all types of structures we have considered.

We believe we can show that these axioms and inference rule, together with the axioms and inference rules C1-C3 and RC1 for common knowledge discussed above and AX_{MEAS} (resp. AX) gives us a sound and complete axiomatization for this extended language in the measurable case (resp. in the general case). Moreover, we believe we can prove a small model theorem, and show that the validity problem for all variants of the logic is in double exponential time. We are currently working out the details of the proof.

6 Conclusions

We have investigated a logic of knowledge and probability that allows explicit reasoning about probability. We have been able to obtain complete axiomatizations and decision procedures for our logic, and hope to extend these results to the language with common knowledge. We have also identified some important properties that might hold of the interrelationship between agents' subjective probability spaces at different states.

It seems to us that the most important area for further research lies in understanding better what the appropriate choice of probability space is. Using the ideas in this paper together with Moses' recent work on resource-bounded reasoning [Mos88], Yoram Moses, Mark Tuttle, and the second author have made progress on capturing *interactive proofs* and *zero knowledge* [GMR85] in the framework of knowledge and probability discussed in this paper. These results appear in [HMT88]. Interestingly, the appropriate choice of probability space in [HMT88] seems to be that generated on all the points with the same global state, as in our examples in Section 3. Thus the probability space satisfies OBJ and UNIF, but not SDP. We have plausible arguments for at least two distinct choices of probability space in analyzing probabilistic variants of the coordinated attack problem (see [HM84b] for a discussion of the coordinated attack problem, and a knowledge-based analysis of it). However, we need to have a larger body of examples in which to test our ideas.

Acknowledgements: The foundations of this paper were greatly influenced by discussions the second author had with Yoram Moses and Mark Tuttle in the context of their joint work on capturing interactive proofs [HMT88]. In particular, their observation that it was necessary to allow $S_{i,s} \subset \mathcal{K}_i(s)$ caused us to rethink many of our ideas. They also suggested taking $K_i^\alpha \varphi$ to be an abbreviation for $K_i(m_i(\varphi) \geq \alpha)$ rather than $m_i(\varphi) \geq \alpha$, as was done in an early draft of this paper. As usual, Moshe Vardi's comments helped improve both the style and content of the paper. Finally, we would like to thank Nimrod Megiddo for his patient and enlightening discussions on linear programming.

References

[Aum76] R. J. Aumann, Agreeing to disagree, *Annals of Statistics* **4**:6, 1976, pp. 1236–1239.

[Cav83] J. Cave, Learning to agree, *Economics Letters* **12**, 1983, pp. 147–152.

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

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

[FHM88] R. Fagin, J. Y. Halpern, and N. Megiddo, A logic for reasoning about probabilities, to appear, 1988.

[Gai86] H. Gaifman, A theory of higher order probabilities, *Theoretical Aspects of Reasoning about Knowledge: Proceedings of the 1986 Conference* (J. Y. Halpern, ed.), Morgan Kaufmann, 1986, pp. 275–292.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof-systems, *Proc. 17th ACM Symp. on Theory of Computing*, 1985, pp. 291–304.

[Hal86] J. Y. Halpern, Reasoning about knowledge: an overview, *Theoretical Aspects of Reasoning about Knowledge: Proceedings of the 1986 Conference* (J. Y. Halpern, ed.), Morgan Kaufmann, 1986, pp. 1–17.

[Hal87] J. Y. Halpern, Using reasoning about knowledge to analyze distributed systems, *Annual Review of Computer Science, Vol. 2*, Annual Reviews Inc., 1987, pp. 37–68.

[Hin62] J. Hintikka, *Knowledge and Belief*, Cornell University Press, 1962.

[HM84a] J. Y. Halpern and D. A. McAllester, Knowledge, likelihood, and probability, *Proc. of AAAI-84*, 1984, pp. 137–141.

[HM84b] J. Y. Halpern and Y. Moses, Knowledge and common knowledge in a distributed environment, *Proc. 3rd ACM Symp. on Principles of Distributed Computing*, 1984, pp. 50–61. A revised version appears as *IBM Research Report RJ 4421*, Aug., 1987.

[HM85] J. Y. Halpern and Y. Moses, A guide to the modal logics of knowledge and belief, *Proc. of the 9th IJCAI*, 1985, pp. 480–490.

[HMT88] J. Y. Halpern, Y. Moses, and M. Tuttle, A knowledge-based analysis of zero knowledge, to appear, *Proc. 20th ACM Symp. on Theory of Computing*, 1988.

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

[HS84] S. Hart and M. Sharir, Probabilistic temporal logics for finite and bounded models, *Proc. 16th ACM Symp. on Theory of Computing*, 1984, pp. 1–13.

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

[Kri63] S. Kripke, A semantical analysis of modal logic, *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* **9**, 1963, pp. 67–96.

[Len78] W. Lenzen, Recent work in epistemic logic, *Acta Philosophica Fennica* **30**, 1978, pp. 1–219.

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

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

[Moo85] R. C. Moore, A formal theory of knowledge and action, *Formal Theories of the Commonsense World* (J. Hobbs and R. C. Moore, eds.), Ablex Publishing Corp., 1985.

[Mos88] Y. Moses, Resource-bounded knowledge and belief, *Proceedings of the Second Conference on Theoretical Aspects of Reasoning about Knowledge* (M. Y. Vardi, ed.), Morgan Kaufmann, 1988.

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

[Rus87] E. H. Ruspini, Epistemic logics, probability, and the calculus of evidence, *Proc. of the 10th IJCAI*, 1987, pp. 924–931.

[Sha79] G. A. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, 1979.