Reasoning with Time and Chance
(Extended abstract)

by

Daniel Lehmann and Saharon Shelah

Institute of Mathematics and Computer Science,
Hebrew University, Jerusalem 9104 (Israel)

Abstract:

The temporal propositional logic of linear time is generalized to an uncertain world, in which random events may occur. The formulas do not mention probabilities explicitly, i.e. the only probability appearing explicitly in formulas is probability one. This logic is claimed to be useful for stating and proving properties of probabilistic programs. It is convenient for proving those properties that do not depend on the specific distribution of probabilities used in the program's random draws. The formulas describe properties of execution sequences. The models are stochastic systems, with state transition probabilities. Three different axiomatic systems are proposed and shown complete for general models, finite models and models with bounded transition probabilities respectively. All three systems are decidable, by the results of Rabin [Ra1].

1. Introduction

Probabilistic algorithms have recently been advocated for solving problems in different areas, and especially for enforcing efficient cooperation between asynchronous parts of a large system. Some of those algorithms exhibit efficiency, elegance and robustness but proofs of correctness were often delicate. This had not been considered surprising since such proofs must combine the difficulties of both parallel programming and probability theory.

Since the framework of temporal logic has proved itself useful to analyze parallel programs, we extend it to deal with chance on top of time and present a decidable logic in which a great many interesting properties of probabilistic parallel programs can be expressed. We hope that this work will lead to automatic or semi-automatic proof systems that will help the designer of simple probabilistic algorithms for distributed systems.

Our logic is a strict extension of the temporal logic of linear time advocated and described in [Pn]: all formulas of the temporal logic of linear time are formulas of our system, they describe the same sets of execution sequences in both systems and such a formula is valid in our system if and only if it is valid in the logic of linear time. Therefore a user of our system may use all he knows about classical temporal logic without any change; all he has to do is to express the aspects of his program that depend on chance. It is a

fundamental and striking feature of our system that it deals with probabilistic programs in the framework of linear time. In this respect our work differs from recent efforts to use branching time (see for example [La], [BMP], [CE], [EH]). We think that, for probabilistic processes, *sometimes* should be *not never* ([La]). A finer analysis of the relation between linear and branching time logics may be found in section 14.

This work also differs from previous attempts to tackle probabilistic programs by quantitative methods, for example [Ko], [Re], [HSP], [FH] and [MT]. Our basic claim is that there is a large family of useful probabilistic algorithms that may be analyzed by purely qualitative methods. Clearly, some sophisticated probabilistic algorithms require a quantitative analysis. A similar effort to develop qualitative and not quantitative techniques, for a different class of problems, has been pursued by [HR].

2. Probabilistic algorithms

The analysis of asynchronous systems of programs (parallel programs) is known to be more difficult than that of sequential programs by one order of magnitude. The analysis of probabilistic asynchronous systems has, so far, been considered as another order of magnitude harder (see, in particular [LR]). We think that this first evaluation could have been too pessimistic, and that the problems encountered arose more from the novelty of the tool than from some intrinsic complexity. Together with the effort towards clarifying the concepts that can be found, for example, in [HSP], the framework proposed here should prove that, for at least a class of probabilistic asynchronous systems, probabilistic systems are not much harder than deterministic asynchronous systems.

The authors of [LR] and [CLP] quickly realized two things:
1) the properties they wanted to prove about their algorithms did not explicitly involve numeric probabilities, except probability one, and
2) the algorithms studied satisfied those properties independently of the exact numeric distribution used to implement the random draws.

A case in point is [LR] where the basic claim is that the system is, with probability one, free of deadlock, and this is true whatever the positive probabilities α and β, with which the two sides are chosen, may be. The algorithms of [CLP], [Ra3] and [Ra4] exhibit similar properties.

Noticeable exceptions are the algorithms for testing primality of [SS], [Ra2] and [Le] for which the interesting properties to be shown are of the type: if n is composite then a witness to that fact will be found with a probability greater than $f(n)$. Some finer properties of the solution described in [Ra3] also demand explicit mention of numeric probabilities.

If one divides the probabilistic algorithms in two broad classes:
(1) algorithms that are guaranteed to give correct results with probability one, and
(2) algorithms that may make mistakes with a probability smaller than any ε fixed in advance

one may say that the method proposed here is suited to prove the correctness of algorithms of the first class and not of the second.

Since so many interesting properties could be expressed without explicit mention of probabilities, and did not depend on the exact probability distribution used, we set to ourselves to provide a logical system for the analysis of those properties. In our system numerical probabilities cannot be expressed at all. Chance appears as a modality qualifying those assertions that are certainly true, i.e. true whatever the results of the random draws could be. The modality expressing that an assertion is possibly true, i.e. that it holds with a strictly positive probability, is the dual of the previous one.

Our system is therefore very rudimentary and simple and well in line with the feelings of those who have dealt with the algorithms mentioned above, that only very basic facts about probability theory are required to prove the needed properties. Essentially one does not need anything more than: "if I throw a coin an infinite number of times then it *will* fall an

infinite number of times on heads". The completeness result below gives a precise meaning to this claim.

3. The models

We begin by describing the models we shall be dealing with. We suppose that a set **Pvar** of propositional variables is given. If one wants to study the truth of propositions that say something about the passing of time, it is natural to consider, as models, linear sequences of "instantaneous states of affairs" (in short states), where a state is (or is labelled by) a subset of **Pvar**. This is the class of models proposed in [Pn]. Since we want to study the truth of propositions that describe the passing of time in an uncertain universe, i.e. a universe in which the moves from one state to the next one are probabilistic in nature, we shall consider models that are essentially Markov chains.

In the case of deterministic parallel programs, each possible execution of the program defines a model. A program, therefore, defines a set of models. This set may be characterized by a formula. To prove that a given program enjoys a property, one shows that each one of the models corresponding to a possible execution satisfies the formula expressing the desired property. Similarly, in the case of probabilistic parallel programs, a program defines a set of models. This set is definable by a formula and to prove that a given program enjoys a property, one shows that all models of the set satisfy the formula corresponding to the property of interest.

We shall now define three classes of models and, later on, the notion of validity of a formula in those models. In a word, our models are Markov systems, i.e. states and transition probabilities (see [KSK], for example, for a reference on Markov chains). Similar models for different, richer, languages have been proposed in [FH], [Ko], [MT] and [Re].

A word on notation first. If A is a set, $A^{\mathbb{N}}$ is the set of all infinite sequences over A. If $\sigma \in A^{\mathbb{N}}$ and $n \in \mathbb{N}$, we denote $\sigma(n)$ by σ_n and we shall use σ^n to denote the sequence defined by : $\sigma^n_m = \sigma_{m+n}$ for all $m \in \mathbb{N}$.

Definition 1: A g-model (where g stands for *general*) is a quadruple $\langle \mathcal{S}, u, l, p \rangle$, where the following holds.
1) $\mathcal{S}$ is an arbitrary (non-empty) denumerable set. Elements of $\mathcal{S}$ are called states and denoted by: $s, t, \cdots$.
2) $u \in \mathcal{S}$ is called the initial state
3) $l : \mathcal{S} \to 2^{\mathbf{Pvar}}$ is a labelling function, associating to every state the set of propositional variables that hold in that state ($2^{\mathbf{Pvar}}$ denotes the set of all subsets of **Pvar**)
4) $p : \mathcal{S} \times \mathcal{S} \to [0,1]$ associates with every possible transition a probability, in such a way that for every $s \in \mathcal{S}$, we have $\sum_{t \in \mathcal{S}} p(s,t) = 1$. The sum is finite or infinite. We use here real probabilities but could as well, without affecting theorems or proofs, have used rational probabilities.

Definition 2: A g-model $\mathcal{U}$ is said to be a b-model (bounded), if there is a $\alpha \in \mathbb{R}$, $\alpha > 0$ such that for every $s, t \in \mathcal{S}$, if $p(s,t) > 0$ then $p(s,t) > \alpha$.

Definition 3: A g-model $\mathcal{U}$ is said to be an f-model (finite), if its state set $\mathcal{S}$ is finite.

An f-model is clearly a b-model. As in the theory of Markov chains (see [KSK] or any text on the subject for a formal definition), in a model $\mathcal{U}$, the transition function p yields, for any state s, a probability distribution on the set P_s of all sequences σ of $\mathcal{S}^{\mathbb{N}}$ that begin at s, i.e. such that $\sigma_0 = s$. We shall denote this probability distribution by $\tilde{p}_s$. It suffices to know that the set Q of all sequences σ of $\mathcal{S}^{\mathbb{N}}$, satisfying $\sigma_0 = s_0$, $\sigma_1 = s_1$, $\cdots$, $\sigma_n = s_n$, $(0 \leq n)$, is measurable and such that :

$$\tilde{p}_{s_0}(Q) = p(s_0,s_1) \times p(s_1,s_2) \times \cdots \times p(s_{n-1},s_n).$$

4. The language

Our formulas are built-out of propositional variables, classical connectives, temporal connectives and modal connectives.

We define formally the set of all formulas Γ. We shall denote propositional variables by p , q , $\cdots$. Formulas will be denoted by a , b , $\cdots$. They are defined by the following rules.

1) A propositional variable $p \in$ **Pvar** is a formula. A propositional variable denotes a basic proposition, that does not mention time.
2) If a and b are formulas, then:
   a) $\neg a$ is a formula. The symbol $\neg$ denotes logical negation and is read **not**.
   b) $a \vee b$ is a formula. The symbol $\vee$ denotes logical disjunction and is read **or**.
   c) $\bigcirc a$ is a formula. The symbol $\bigcirc$ is read **next** and denotes the next instant of time.
   d) $\Box a$ is a formula. The symbol $\Box$ is read **always** and denotes all the instants of times from the present (included) and on.
   e) $a \,\mathcal{U}\, b$ **until** is a formula. The symbol $\mathcal{U}$ **until** is read **until**. It was introduced in [GPSS]. The formula $a \,\mathcal{U}\, b$ **until** b denotes the fact that, there is a instant of time in the future when b is true and until the first such instant of time, say t, a stays continuously true at all intermediate instants of time (t not necessarily included).
   f) ∇a is a formula. The symbol ∇ is read **certainly** and denotes a probability of one. It has been chosen for its typographical proximity to the universal quantifier symbol $\forall$.

One may look at our language as a generalization of the one proposed by [EH], if one identifies our modal connective **certainly** (∇) and their **for all** ($\forall$). Our language is an extension of theirs since we allow the application of any connective to any formula, where they make a distinction between state and path formulas and enforce certain restrictions in the way one may build formulas related to that distinction. Their semantics is different from ours, though. More on the relation between the system presented here and that of [EH] is to be found in section 14.

We shall use the classical abbreviations: $a \wedge b$ for $\neg(\neg a \vee \neg b)$, **true** for $p \vee \neg p$, **false** for $\neg$**true**, $a \rightarrow b$ for $\neg a \vee b$ and $a \leftrightarrow b$ for $(a \rightarrow b) \wedge (b \rightarrow a)$. We shall also use two other abbreviations: $\Diamond a$ is read **sometime a** and stands for $\neg\Box\neg a$, Δa is read **possibly a** and stands for $\neg\nabla\neg a$. The usual rules of precedence are assumed. We assume also that $\rightarrow$ associates to the right.

5. The semantics

We shall now attach a truth-value ***true*** or ***false*** , to every formula and every sequence of states of a model. All formulas are path formulas, in the terminology of [EH].

Definition 4: Let $\mathcal{U}$ be a g-model $\langle \mathcal{S} , u , l , p \rangle$, $\sigma \in \mathcal{S}^{\mathbb{N}}$ a sequence of states and $a \in \Gamma$ a formula:

$p \,|^{\sigma}_{\mathcal{U}} =$ ***true*** $\iff p \in l(\sigma_0)$

Notice that the truth value of a propositional variable, relative to a sequence σ, depends only on the first state of the sequence: σ_0.

$\neg a \,|^{\sigma}_{\mathcal{U}} =$ ***true*** $\iff a \,|^{\sigma}_{\mathcal{U}} =$ ***false***

$a \vee b \,|^{\sigma}_{\mathcal{U}} =$ ***true*** $\iff a \,|^{\sigma}_{\mathcal{U}} =$ ***true*** or $b \,|^{\sigma}_{\mathcal{U}} =$ ***true***

$\bigcirc a \,|^{\sigma}_{\mathcal{U}} = \mathit{true} \iff a \,|^{\sigma^1}_{\mathcal{U}} = \mathit{true}$

$\Box a \,|^{\sigma}_{\mathcal{U}} = \mathit{true} \iff \forall n \in \mathbb{N} \;\; a \,|^{\sigma^n}_{\mathcal{U}} = \mathit{true}$

$a \;\mathcal{U}\mathbf{ntil}\; b \,|^{\sigma}_{\mathcal{U}} = \mathit{true} \iff$

$\exists n \in \mathbb{N}$ such that $b \,|^{\sigma^n}_{\mathcal{U}} = \mathit{true}$ and $\forall k < n$, $a \,|^{\sigma^k}_{\mathcal{U}} = \mathit{true}$

$\nabla a \,|^{\sigma}_{\mathcal{U}} = \mathit{true} \iff \tilde{P}_{\sigma_0}(\{\tau \mid \tau \in P_{\sigma_0},\; a \,|^{\tau}_{\mathcal{U}} = \mathit{true}\}) = 1$

One may readily check that the set of paths considered above is indeed measurable. Notice now that the truth of a formula of the type ∇a at a sequence σ in a model $\mathcal{U}$ depends only on the state σ_0 and the model $\mathcal{U}$, i.e. ∇a is really a state formula.

With the assumptions above, we shall denote $\tilde{P}_s(\{\tau \mid \tau \in P_s,\; a \,|^{\tau}_{\mathcal{U}} = \mathit{true}\})$ by $\tilde{P}_s(a)$.

6. Satisfaction and Validity

We shall now propose a notion of satisfiability that, in essence, says that a model satisfies a formula a if a holds for **almost** all paths beginning at the initial state. Our choice of definition expresses our view that there is no practical difference between satisfaction and satisfaction with probability one. This definition expresses our belief that a formula that holds with probability one does, really, holds. Anybody who does not share this belief will find an alternative approach in section 12.

Definition 5: Let $\mathcal{U}$ be a g-model and $a \in \Gamma$ a formula. We say that $\mathcal{U}$ satisfies a and write $\mathcal{U} \models a$, if $\tilde{P}_u(\{\tau \mid \tau \in P_u \;,\; a \,|^{\tau}_{\mathcal{U}} = \mathit{true}\}) = 1$.

One immediately sees that: $\mathcal{U} \models a \iff \mathcal{U} \models \nabla a$. One should also notice that it may happen that $\mathcal{U} \not\models a$ and $\mathcal{U} \not\models \neg a$.

In the next definition, and from now on, γ may be any one of {g, b, f}.

Definition 6: If $a \in \Gamma$, we say that a is γ-valid if every γ-model $\mathcal{U}$ satisfies a. We shall denote γ-validity by $\underset{\gamma}{\models}$.

7. The logical system

Three different logical systems: TCg, TCb and TCf will be proposed now, each one of them corresponding to one of the notions of γ-validity defined above. The logical systems we propose contain schemata for axioms and rules of inference. An axiom schema denotes all formulas obtained from it by consistent substitution of arbitrary formulas for the formula variables (a ,b ,c) appearing in it, and consistent substitution of arbitrary propositional variables for the variables (p ,q ,..) that stand up for propositional variables. We do not allow the replacement of a propositional variable by an arbitrary formula. The symbol $\underset{\gamma}{\vdash}$ denotes provability in the system corresponding to γ. Most of the axioms and all of the inference rules are common to all three systems. When something is claimed to hold in any one of our three systems we use $\vdash$. In other words $\vdash$ may be replaced *consistently* by any one of our three deducibility symbols.

Our systems are best viewed as composed of a number of levels.

The first level concerns classical propositional calculus.

A0) A suitable axiomatization of the propositiónal calculus

R0) (Modus Ponens) If $\vdash a$ and $\vdash a \to b$ then $\vdash b$.

The second level concerns the temporal logic of linear time, as found in [GPSS]. The axiomatization presented here is not the most economical.

A1) $\bigcirc(a \to b) \to \bigcirc a \to \bigcirc b$

A2) $\neg\bigcirc a \leftrightarrow \bigcirc\neg a$

A3) $\Box(a \to b) \to \Box a \to \Box b$

A4) $a\ \mathcal{U}\ b \to \Diamond b$

A5) $\Box a \leftrightarrow a \wedge \bigcirc\Box a$

A6) $a\ \mathcal{U}\ b \leftrightarrow b \vee a \wedge \bigcirc(a\ \mathcal{U}\ b)$

A7) $\Box(a \to \bigcirc a) \to a \to \Box a$

R1) ($\Box$generalization) If $\vdash a$ then $\vdash \Box a$.

The third level concerns general truths about certainty.

A8) $\nabla(a \to b) \to \nabla a \to \nabla b$

A9) $\Delta\nabla a \leftrightarrow \nabla a$

A10) $\nabla a \to a$

R2) (∇ generalization) If $\vdash a$ then $\vdash \nabla a$.

This third level amounts to the modal system S5, that is well known and well suited for the notion of certainty if we accept that there is no difference between satisfaction and satisfaction with probability one.

The fourth level expresses the fact that propositional variables denote *state* propositions, i.e. propositions that do not mention future instants of time. For this reason, if the propositional variable p is true for some path σ it is true for all paths τ of P_{σ_0}.

A11) $p \to \nabla p$

In A11 p stands for a propositional variable and cannot be replaced by an arbitrary formula. Because of A11, our system does not enjoy the substitution property.

The last and most interesting level describes the interrelation between time and chance. The following axiom expresses a general property, and is part of all three systems we propose.

A12) $\nabla\bigcirc a \to \bigcirc\nabla a$

Axiom A12 expresses the fact that the passing of time can only reduce the span of the possible, as can be seen on its contrapositive.

$$\bigcirc\Delta a \to \Delta\bigcirc a \qquad (1)$$

The schema we shall consider next is suitable for b-models, i.e. models in which the

probabilities of the basic transitions that are not zero are bounded from below, by some positive number. Since the final formulation of the axiom for this case is slightly intricate, let us introduce first some special case of the axiom. In a system with bounded probabilities, any transition that is possible an infinite number of times will eventually be taken (with probability one). We may express the above remark by the following schema.

$$\Box\Diamond\,\Delta O\nabla a \rightarrow \Diamond\, a \tag{2}$$

Notice that we need the ∇ in the hypothesis to ensure that the formula a has, an infinite number of times, a probability at least α (α is the number that bounds from below the probabilities of the basic transitions) to be true at the next instant of time. Notice also that the schema above implies both:

$$\Box\Diamond\,\Delta O\nabla a \rightarrow \Box\Diamond\,\nabla a \tag{3}$$

(Hint: $\Box$-generalize (2), use A3 and T1 below, next section) and

$$\Box\Diamond\,\Delta O a \rightarrow \Box\Diamond\,\Delta a \tag{4}$$

(Hint: replace a by Δa in (2), use the contrapositive of A9 in the hypothesis to get rid of ∇ and the contrapositive of A10 to get rid of the inner Δ)

Schema (2) is not strong enough, since it does not allow to speak about a specific subset of instants of time at which $\Delta O\nabla a$ holds. Formula (5) remedies this defect.

$$\Box\Diamond\,(\nabla a \wedge \Delta O\nabla b) \rightarrow \Diamond\,(a \wedge O b) \tag{5}$$

The reader is now ready for the final form of the axiom. It really should be considered as a sequence of schemata. It is a k-steps unfolding of the previous schema and expresses the fact that successive random draws are independent.

A13) $$\Box\Diamond\left[\nabla a_0 \wedge \Delta O(\nabla a_1 \wedge \Delta O(\nabla a_2 \wedge \Delta O(\cdots \wedge \Delta O\nabla a_k)))\right] \rightarrow$$
$$\Diamond\,(a_0 \wedge O a_1 \wedge OO a_2 \wedge \cdots \wedge O^{(k)} a_k)$$

The following (6), is equivalent to A13, and more concise.

$$\Box\Diamond\,\Delta\left[\bigwedge_{l=0}^{k} O^{(l)}\nabla a_l\right] \rightarrow \Diamond\left[\bigwedge_{l=0}^{k} O^{(l)}\nabla a_l\right] \tag{6}$$

To see the equivalence, notice first that one may as well precede each a_i of the conclusion of A13 by ∇, and then use

$$\left[\nabla a_0 \wedge \Delta O(\nabla a_1 \wedge \Delta O(\cdots \Delta O\nabla a_k))\right] \leftrightarrow \Delta\left[\bigwedge_{l=0}^{k} O^{(l)}\nabla a_l\right]$$

One may not do with Axiom A13 restricted to a finite subset of indexes k. It is indeed possible, for any k, to build a model (unbounded) that satisfies A13 for k but does not satisfies it for $k+1$. The construction is too lengthy to be included here. It is however possible that one (other) single schema may imply the whole sequence A13.

The algorithm presented in Section 5 of [Ra4] is a good example of a system with bounded transition probabilities but an infinite state set. It will be shown in section 9 that most real life systems should be treated as having an infinite state set, even when they seem to be "finite".

Our last axiom is suitable only for finite systems, is stronger than A13 and expresses the fact

that, in a finite system, if something has, an infinite number of times, a positive chance of happening, it certainly happens sometime.

A14) $\Box\Diamond\Delta a \rightarrow \Diamond a$

It is useful to record also the contrapositive of A14.

$$\Box a \rightarrow \Diamond\Box\nabla a \tag{7}$$

We define three different systems, from the weakest to the strongest:
1) TCg: A0-A12 and R0-R2
2) TCb: A0-A13 and R0-R2
3) TCf: A0-A12, A14 and R0-R2.

8. An example

We shall use the system above to express and prove an interesting property on a toy program. For reasons of space economy, we satisfy ourselves with a very simple example. Nevertheless we expect that our example is telling enough to suggest how our system can be used to prove properties about parallel probabilistic programs. But, for sure, much additional work is needed before the feasibility of using our system can be assessed.

Suppose we consider a system of two processes P_1 and P_2. The system has three states s_i, for $i=1,..,3$. The initial state is s_1. If process P_1 is activated while the system is in s_1, it leaves it in s_1. If it is activated while the system is in s_2, with probability $\frac{1}{2}$ it leaves it in the same state and with the same probability it moves it to s_3. If process P_2 is activated in state s_1, with probability $\frac{1}{2}$ it leaves it in s_1 and with the same probability it moves the system to s_2. If it is activated in s_2, then with probability $\frac{1}{10}$, it moves the system to s_3 and with probability $\frac{9}{10}$ it moves it to s_1. The diagrams of Fig. 1 are an equivalent description of the system.

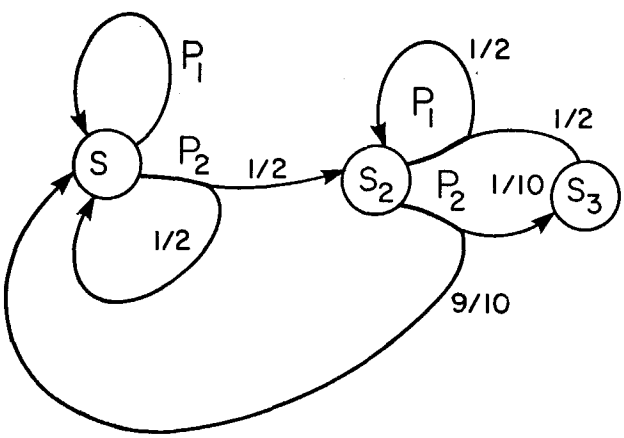

Figure 1

We claim that, with probability one, the system will, sometime, enter state s_3, under the hypothesis of fairness (all three notions of impartiality, justice and fairness of [LPS] are equivalent here).

The basic assertions we shall use are $at\ s_i$. The claim we want to make about the system may be formalized in the following proposition.

$$(C) \quad at\ s_1 \rightarrow \Diamond\ at\ s_3$$

Notice that the proposition does not mention probabilities explicitly, though we expect (C) to be correct only with probability one.

The following propositions will describe our system. Our first formula (E) has only a technical role. It expresses the fact that the system cannot be at the same time in two different states.

$$(E) \quad \Box\left[\bigwedge_{\substack{i,j=1,3 \\ i\neq j}} at\ s_i \rightarrow \neg at\ s_j\right]$$

Our next formula (M1) will describe the possible moves from state s_1. It says that, when at state s_1, one of two things must occur: either P_1 operates and then the next state is s_1, or P_2 operates and then the next state is either s_1 or s_2, but both states have a strictly positive probability of occurring.

$$(M1) \quad \Box\left[at\ s_1 \rightarrow O at\ s_1 \vee O\left(at\ s_1 \vee at\ s_2\right) \wedge \Delta O at\ s_1 \wedge \Delta O at\ s_2\right]$$

Similarly (M2) describes the possible moves from s_2.

$$(M2) \quad \Box\left[at\ s_2 \rightarrow O\left(at\ s_2 \vee at\ s_3\right) \wedge \Delta O at\ s_2 \wedge \Delta O at\ s_3 \right.$$
$$\left. \vee O\left(at\ s_1 \vee at\ s_3\right) \wedge \Delta O at\ s_1 \wedge \Delta O at\ s_3\right]$$

Two more propositions are needed, that express the assumption of impartiality: each one of the processes operates an infinite number of times.

$$(B1) \quad \Box\Diamond\left[at\ s_1 \wedge O at\ s_1 \vee at\ s_2 \wedge \Delta O at\ s_2 \wedge \Delta O at\ s_3 \vee at\ s_3\right]$$

$$(B2) \quad \Box\Diamond\left[at\ s_1 \wedge \Delta O at\ s_1 \wedge \Delta O at\ s_2 \vee at\ s_2 \wedge \Delta O at\ s_1 \wedge \Delta O at\ s_3 \vee at\ s_3\right]$$

In general, a formula expressing that the execution sequence is a possible execution in which process i is activated an infinite number of times may always be build by writing that, in the execution sequence, there is an infinite number of states in which all possible results of activating process i are indeed possible tomorrow. The careful reader noticed that we do not care to insist that process i has been activated an infinite number of times, but only that the execution sequence is identical with one in which it has been executed an infinite number of times (the execution sequence must not reveal, in general, which process has been activated at every step, though the name of the process activated last could be made part of the state).

Our claim about the system is that the proposition

$$E \wedge M1 \wedge M2 \wedge B1 \wedge B2 \rightarrow C \tag{9}$$

is valid in any b-model. Our proof proceeds the following way. First, classical temporal logic shows that proposition (10) is g-valid.

$$M1 \wedge M2 \rightarrow at\ s_1 \rightarrow \Diamond\Box at\ s_1 \vee \Box\Diamond\ at\ s_2 \vee \Diamond\ at\ s_3 \tag{10}$$

Indeed, if the system is in state s_1 and never attains s_3, it must stay forever in s_i, for $i=1,2$, since it cannot move to any other state unless it passes through s_3. Then it either ends up continuously in s_1, after some time, or is an infinite number of times in s_2.

Then, again classical temporal logic would show proposition (11) is g-valid.

$$E \wedge B2 \wedge \Diamond\Box at\, s_1 \rightarrow \Box\Diamond \Delta\bigcirc at\, s_2 \qquad (11)$$

Now, we should notice that (12) is b-valid.

$$\Box\Diamond \Delta\bigcirc at\, s_2 \rightarrow \Box\Diamond \bigcirc at\, s_2 \qquad (12)$$

To prove (12), use A11 to prove $at\, s_2 \rightarrow \nabla at\, s_2$, and then A13 to prove that $\Box\Diamond \Delta\bigcirc\nabla at\, s_2 \rightarrow \Diamond at\, s_2$. Now, putting all together, we see that (13) is b-valid.

$$E \wedge M1 \wedge M2 \wedge B2 \wedge at\, s_1 \rightarrow \Box\Diamond at\, s_2 \vee \Diamond at\, s_3 \qquad (13)$$

But clearly (14) is g-valid.

$$M2 \wedge \Box\Diamond at\, s_2 \rightarrow \Box\Diamond \Delta\bigcirc at\, s_3 \qquad (14)$$

Notice that the conclusion does not depend on the assumption of impartiality. Now, by a reasoning similar to the one that lead us to (12), we see that (15) is b-valid.

$$\Box\Diamond \Delta\bigcirc at\, s_3 \rightarrow \Diamond\bigcirc at\, s_3 \qquad (15)$$

We conclude that (9) is b-valid.

Is it enough to convince us that the system enjoys the desired property? The answer is yes, since any possible (fair) execution of our program must result in a b-model that satisfies E, M1, M2, B1 and B2. It would have been slightly simpler to show that (9) is f-valid. Would that be enough to convince us that the system enjoys the desired property? The answer is no. In spite of the fact that the system can be in only a finite number of states, it is possible that some of its possible executions cannot be described as a finite model, since the schedule may be inherently "infinite", e.g. remember an amount of the past history of the system that cannot be bounded a priori and base its decision as to which process to schedule on that history. To be fully satisfied we must show that formula (9) is b-valid.

9. Soundness and Completeness

Theorem 1: For any $\gamma \in \{g,b,f\}$ and for any $\alpha \in \Gamma$, $\underset{\gamma}{\vdash} \alpha \Leftrightarrow \underset{\gamma}{\models} \alpha$.

The proof of theorem 1 will appear in the full paper. It proceeds by the method known as *selective filtration*. It also provides a write-up and an extension of the completeness proof of [GPSS]. It is smooth and uniform enough to allow similar proofs for similar logics. We consider selective filtration to be more elegant and clearer than the tableau method that essentially amounts to brute force.

10. Alternative systems for unbelievers

Anybody who does not believe that formulas that hold with probability one *really* hold should, instead of Definition 5, use the following definition of satisfiability.

Definition 21: Let $\mathcal{U}$ be a g-model and $\alpha \in \Gamma$ a formula. We say that $\mathcal{U}$ satisfies α and write $\mathcal{U} \models \alpha$, iff for any $\tau \in P_u$, $\alpha\,|^{\tau}_{\mathcal{U}} = true$.

The definition of validity stays unchanged. The logical system should be changed in the following way. Essentially, instead of basing our system on S5, we should base it on *deontic* S5 (see [Ch]). More specifically, one notices that the rules R0-R2 are still sound and that, except A10, A12, A13 and A14, all axioms are still valid. Therefore we keep the rules R0-R2 and the axioms A0-A9 and A11. For the other axioms, we just prefix them by $\nabla\Box$. Instead of A10 use the following A10'.

A10') $\nabla\Box[\nabla\alpha \rightarrow \alpha]$

Instead of A12, use the following A12'.

A12') $\nabla\Box[\nabla\bigcirc\alpha \rightarrow \bigcirc\nabla\alpha]$

Instead of A13 and A14, use the following A13' and A14'.

A13') $\nabla\Box[A13]$

A14') $\nabla\Box[A14]$

We think that the resulting systems NTCγ are sound and complete for the stricter notion of validity of Definition 21. The proof should be very similar to the one presented above, the only basic difference being that the relation $\equiv$ behaves slightly differently and that theories T that do not satisfy $T \equiv T$ must be treated as a special case. The relation $\equiv$ is transitive (by T10) but not reflexive or symmetric. It, nevertheless, satisfies the property: if $T \equiv T'$, then $\nabla\alpha \in T$ iff $\nabla\alpha \in T'$.

11. Linear time versus branching time

One may remark that our language is also suitable for interpretation in non-probabilistic models. Indeed it may be interpreted on tree models similar to those used in branching time temporal logic, the symbol ∇ being taken to mean ***for all paths***. With this interpretation our language contains branching time logic as it is defined in [BMP] and [EH]. If one takes the natural definition of satifiability that says that a model satisfies a formula if the formula holds for all the branches that begin at the initial state, one immediately notices that our system TCg is sound also for those models. It is not complete, though. Notice, for example, that the formula $p \wedge \nabla\Box\Delta\bigcirc p \rightarrow \Delta\Box p$ is valid for our new non-probabilistic interpretation, but is not valid in our probabilistic interpretation. To find the additional axioms needed to obtain a complete axiomatization of this non-probabilistic interpretation is an open problem.

Another non-probabilistic interpretation of our connective ∇ has been suggested by M. Magidor. Interpret ∇ as : for a "co-meagre" family of paths, where the term "co-meagre" refers to a set whose complement is of the first category in Baire's classification, assuming the natural topology for paths in models of arbitrary size. Perhaps surprisingly, our system TCf is sound and complete for this interpretation, showing that arbitrary categorical models behave exactly as finite probabilistic models. The proof of this result is outside the scope of this paper.

12. Conclusion and open problems

The main practical conclusion of this work is that there is a large class of probabilistic programs for which a qualitative analysis is sufficient, and that this analysis may be completed without any need to use sophisticated probability theory.

The three systems we presented are decidable by reduction to SωS and the results of Rabin [Ra1]. The reduction is standard and extremely inefficient as a practical decision method and therefore we shall not describe the reduction in detail.

The question of the complexity of decision procedures for our systems is interesting and open. It follows from the results of [SC] that satisfiability is Pspace-hard. Our conjecture is that the three systems above are in Pspace.

References

[BMP] Ben-Ari, M., Manna, Z. and Pnueli, A. The temporal logic of branching time, Conf. Record 8th Annual ACM Symposium on Principles of Programming Languages, Williamsburg, Va. (Jan. 1981), pp. 164-176.
[CE] Clarke, E.M. and Emerson, E.A. Design and synthesis of synchronization skeletons using branching time temporal logic, Proc. Workshop on Logics of Programs, Kozen ed., Springer-Verlag (1982) (to appear).
[Ch] Chellas, B. F. Modal logic, an introduction, Cambridge University Press, Cambridge (1980).
[CLP] Cohen, S., Lehmann D. and Pnueli, A. Symmetric and economical solutions to the mutual exclusion problem in a distributed system (in preparation).
[EH] Emerson, E. A. and Halpern, J. Y. Decision procedures and expressiveness in the temporal logic of branching time, Conf. Record 14th Annual ACM Symposium on Theory of Computing, San Francisco, CA (May 1982), pp. 169-179.
[FH] Feldman, Y. A. and Harel, D. A probabilistic dynamic logic, Conf. Record 14th Annual ACM Symposium on Theory of Computing, San Francisco, CA (May 1982), pp. 181-195. (also Tech. Report CS82-07, Dept. of Applied Mathematics, the Weizmann Institute of Science).
[GPSS] Gabbay, D., Pnueli, A., Shelah, S. and Stavi, J. On the temporal analysis of fairness, Conf. Record of 7th Annual ACM Symposium on Principles of Programming Languages, Las Vegas, Nevada (Jan. 1980), pp. 163-173.
[HC] Hughes, G. E. and Cresswell, M. J., An introduction to modal logic, Methuen, London (1972).
[HR] Halpern, J. Y. and Rabin, M. O., A logic to reason about likelihood, Proc. 15th Annual ACM Symposium on Theory of Computing (April 1983).
[HSP] Hart, S., Sharir, M. and Pnueli, A. Termination of probabilistic concurrent programs, Conf. Record 9th Annual ACM Symposium on Principles of Programming Languages, Albuquerque, New Mexico (1982), pp.1-6.
[Ko] Kozen, D. Semantics of probabilistic programs, J. of Computer and System Sciences Vol. 22 (1981), pp. 328-350.
[KSK] Kemeny, J.G., Snell, J.L. and Knapp, A.W., Denumerable Markov chains, Van Nostrand, Princeton, NJ (1966).
[La] Lamport, L. "Sometimes" is sometimes "not never", Conf. Record of 7th Annual ACM Symposium on Principles of Programming Languages, Las Vegas, Nevada (Jan. 1980), pp. 174-183.
[Le] Lehmann, D. On primality tests, SIAM Journal on Computing Vol. 11 (1982), pp. 374-375.
[LPS] Lehmann, D., Pnueli, A. and Stavi, J. Impartiality, Justice and Fairness: the ethics of concurrent termination, Proceedings of 8th International Colloquium on Automata, Languages and Programming, July 1981, Acco, Israel, pp. 264-277.
[LR] Lehmann, D. and Rabin, M. O. On the advantages of free choice: a symmetric and fully distributed solution to the dining philosophers problem (extended abstract), Conf. Record of 8th Annual ACM Symposium on Principles of Programming Languages, Williamsburg, Va. (Jan. 1981), pp. 133-138.
[MT] Makowski, J.A. and Tiomkin, M. A probabilistic propositional dynamic logic (Extended Abstract), manuscript 1982.
[Pn] Pnueli, A. The temporal semantics of concurrent programs, Theoretical Computer Science Vol. 13 (1981), pp. 45-60.
[Ra1] Rabin, M. O. Decidability of second order theories and automata on infinite trees, Trans. AMS Vol. 141 (1969), pp. 1-35.
[Ra2] Rabin, M.O. Probabilistic algorithms, in Algorithms and Complexity, New Directions and Recent Results, J.F. Traub, ed., Academic Press, New York, 1976.
[Ra3] Rabin, M.O. N-process mutual exclusion with bounded waiting by 4.log N-valued shared variable, Journal of Computer and System Sciences Vol.25 (1982) pp. 66-75.
[Ra4] Rabin, M.O. The choice coordination problem, Acta Informatica Vol. 17 (1982), pp. 121-134.
[Re] Reif, J. H. Logics for probabilistic programming, Proc. 12th ACM Symposium on Theory of

Computing,

Los Angeles, CA (April 1980), pp. 8-13.
[SC] Sisla, A. P. and Clarke, E. M. The complexity of propositional linear temporal logics, Proc. 14th Annual ACM Symposium on Theory of Computing, San Francisco, CA (May 1982), pp. 159-168.
[SS] Solovay, R. and Strassen V., A fast Monte-Carlo test for primality, SIAM Journal on Computing Vol. 6 (1977), pp. 84-85; erratum Vol. 7 (1978), pp. 118.