INFORMATION AND CONTROL 53, 165–198 (1982)

Reasoning with Time and Chance

DANIEL LEHMANN AND SAHARON SHELAH

Institute of Mathematics and Computer Science,
Hebrew University, Jerusalem 91904, Israel

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 (*Trans. Amer. Math. Soc.* **141** (1969), 1–35).

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 Pnueli (1981): 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

0019-9958/82 $2.00

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, Lamport, 1980; Ben-Ari, Manna, and Pnueli, 1981; Clarke and Emerson, 1982; and Emerson and Halpern, 1982). We think that, for probabilistic processes, *sometimes* should be *not never* (Lamport, 1980). 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, Kozen (1981), Reif (1980), Hart, Sharir, and Pnueli (1982), Feldman and Harel (1982), and Makowski and Tiomkin (1982). 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 Halpern and Rabin (1983).

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 Lehmann and Rabin, 1981). 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 Hart *et al.* (1982), the framework proposed here should prove that, for at least a class of asynchronous systems, probabilistic systems are not much harder than deterministic systems.

The authors of Lehmann and Rabin (1981) and Cohen, Lehmann, and Pnueli (1983) 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 Lehmann and Rabin (1981) 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 Cohen *et al.* (1983), Rabin (1982a, 1982b) exhibit similar properties.

Noticeable exceptions are the algorithms for testing primality of Solovay and Strassen (1977), Rabin (1976), and Lehmann (1982) 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 Rabin (1982a) 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 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 properties needed. 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 Pnueli (1981). 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 Kemeny *et al.*, 1966, for example, for a reference on Markov chains). Similar models for different, richer, languages have been proposed in Feldman and Harel (1982), Kozen (1981), Makowski and Tiomkin (1982) and Reif (1980).

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 $\langle S, u, l, p \rangle$, where the following hold:

(1) S is an arbitrary (nonempty) denumerable set. Elements of S are called states and denoted by: $s, t, \ldots,$

(2) $u \in S$ is called the initial state,

(3) $l\colon S \rightarrow 2^{\mathbf{Pvar}}$ 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) $p\colon S \times S \rightarrow [0, 1]$ associates with every possible transition a probability, in such a way that for every $s \in S$, we have $\sum_{t \in S} p(s, t) = 1$. 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 U is said to be a b-model (bounded), if there is an $\alpha \in \mathbb{R}$, $\alpha > 0$ such that for every $s, t \in S$, if $p(s, t) > 0$, then $p(s, t) > \alpha$.

Definition 3. A g-model U is said to be an f-model (finite), if its state set 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 U, the transition function p yields, for any state s, a probability distribution on the set P_s of all sequences σ of $S^{\mathbb{N}}$ 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 $S^{\mathbb{N}}$, satisfying $\sigma_0 = s_0$, $\sigma_1 = s_1, \dots, \sigma_n = s_n$ $(0 \leqslant n)$, 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.

As we define formally the set of all formulas Γ, we shall also define the size ($\#$) and the depth (Ω) of a formula. By depth we mean the depth in the connective $\bigcirc$. We shall denote propositional variables by $p, q, \dots$. Formulas will be denote by $a, b, \dots$. They are defined by the following rules:

(1) A propositional variable $p \in \mathbf{Pvar}$ is a formula and $\#(p) = 1$, $\Omega(p) = 0$. 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 and $\#(\neg a) = \#(a) + 1$, $\Omega(\neg a) = \Omega(a)$. The symbol $\neg$ denotes logical negation and is read **not**.

(b) $a \vee b$ is a formula and $\#(a \vee b) = \#(a) + \#(b) + 1$, $\Omega(a \vee b) = \text{maximum}(\Omega(a), \Omega(b))$. The symbol $\vee$ denotes logical disjunction and is read **or**.

(c) $\bigcirc a$ is a formula and $\#(\bigcirc a) = \#(a) + 1$, $\Omega(\bigcirc a) = \Omega(a) + 1$. The symbol $\bigcirc$ is read **next** and denotes the next instant of time.

(d) $\Box a$ is a formula and $\#(\Box a) = \#(a) + 1$, $\Omega(\Box a) = \Omega(a)$. The symbol $\Box$ is read **always** and denotes all the instants of times from the present (included) and on.

(e) $a\mathbf{Until}b$ is a formula and $\#(a\mathbf{Until}b) = \#(a) + \#(b) + 3$ (we need $\#(a\mathbf{Until}b) > \#(\Box(a \vee b))$), $\Omega(a\mathbf{Until}b) = \text{maximum}(\Omega(a), \Omega(b))$. The symbol **Until** is read **until**. It was introduced in [GPSS]. The formula $a\mathbf{Until}b$ 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 and $\#(\nabla a) = \#(a) + 1$, $\Omega(\nabla a) = \Omega(a)$. 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. We shall denote the set of all formulas of size less or equal to n by Γ_n.

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 Emerson and Halpern (1982).

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

$$p\,|_U^\sigma = \mathbf{true} \Leftrightarrow p \in l(\sigma_0).$$

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.

$$\neg a\,|_U^\sigma = \mathbf{true} \Leftrightarrow a\,|_U^\sigma = \mathbf{false},$$
$$a \vee b\,|_U^\sigma = \mathbf{true} \Leftrightarrow a\,|_U^\sigma = \mathbf{true} \text{ or } b\,|_U^\sigma = \mathbf{true}$$
$$\bigcirc a\,|_U^\sigma = \mathbf{true} \Leftrightarrow a\,|_U^{\sigma^1} = \mathbf{true},$$
$$\Box a\,|_U^\sigma = \mathbf{true} \Leftrightarrow \forall n \in \mathbb{N}\ a\,|_U^{\sigma^n} = \mathbf{true},$$
$$a\mathbf{Until}b\,|_U^\sigma = \mathbf{true} \Leftrightarrow \exists n \in \mathbb{N} \text{ such that } b\,|_U^{\sigma^n} = \mathbf{true} \text{ and } \forall k < n,\ a\,|_U^{\sigma^k} = \mathbf{true},$$
$$\nabla a\,|_U^\sigma = \mathbf{true} \Leftrightarrow \tilde{p}_{\sigma_0}(\{\tau \mid \tau \in P_{\sigma_0}, a\,|_U^\tau = \mathbf{true}\}) = 1.$$

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 U depends only on the state σ_0 and the model U, i.e., ∇a is really a state formula.

With the assumptions above, we shall denote $\tilde{p}_s(\{\tau \mid \tau \in P_s,\ a\,|_U^\tau = \textbf{true}\})$ 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 U be a g-model $\langle S, u, l, p\rangle$ and $a \in \Gamma$ a formula. We say that U satisfies a and write $U \models a$, if $\tilde{p}_u(\{\tau \mid \tau \in P_u,\ a\,|_U^\tau = \textbf{true}\}) = 1$.

One immediately sees that $U \models a \Leftrightarrow U \models \nabla a$. One should also notice that it may happen that $U \not\models a$ and $U \not\models \neg a$.

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 U satisfies a. We shall denote γ-validity by $\models_\gamma$.

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 $(p, q, \ldots)$ that stand up for propositional variables. We do not allow the replacement of a propositional variable by an arbitrary formula. The symbol $\vdash_\gamma$ 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 propositional calculus.

(A0) A suitable axiomatization of the propositional 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 Gabbay, Pnueli, Shelah, and Stavi (1980). 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) $a\mathbf{Until}b \to \Diamond b$,

(A5) $\Box a \to a \wedge \bigcirc \Box a \wedge \bigcirc a$,

(A6) $a\mathbf{Until}b \leftrightarrow b \vee a \wedge \bigcirc(a\mathbf{Until}b)$,

(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) $\triangle \nabla a \leftrightarrow \nabla a$,

(A10) $\nabla a \to a$,

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

This third level amounts to the model 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:

$$\bigcirc\triangle a \rightarrow \triangle\bigcirc a. \tag{1}$$

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 cases 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.

$$\Box\Diamond\triangle\bigcirc\nabla a \rightarrow \Diamond a. \tag{2}$$

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

$$\Box\Diamond\triangle\bigcirc\nabla a \rightarrow \Box\Diamond\nabla a \tag{3}$$

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

$$\Box\Diamond\triangle\bigcirc a \rightarrow \Box\Diamond\triangle a \tag{4}$$

(hint: replace a by $\triangle a$ in (3), use the contrapositive of (A9) in the hypothesis to get rid of ∇ and the contrapositive of (A10) to get rid of the inner $\triangle$).

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

$$\Box\Diamond(\nabla a \wedge \triangle\bigcirc\nabla b) \rightarrow \Diamond(a \wedge \bigcirc b). \tag{5}$$

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:

$$\text{(A13)}\quad \Box\Diamond(\nabla a_0 \wedge \triangle\bigcirc(\nabla a_1 \wedge \triangle\bigcirc(\nabla a_2 \wedge \triangle\bigcirc(\cdots \wedge \triangle\bigcirc\nabla a_k))))$$
$$\rightarrow \Diamond(a_0 \wedge \bigcirc a_1 \wedge \bigcirc\bigcirc a_2 \wedge \cdots \wedge \bigcirc^{(k)} a_k).$$

Schema (6), is equivalent to (A13) and more concise

$$\Box\Diamond\triangle\left[\bigwedge_{l=0}^{k} \bigcirc^{(l)}\nabla a_l\right] \rightarrow \Diamond\left[\bigwedge_{l=0}^{k} \bigcirc^{(l)}\nabla a_l\right]. \tag{6}$$

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

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

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) $\Box \Diamond \triangle a \rightarrow \Diamond a$.

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. Some Theorems

We list, with minimal justification, theorems that will be of use later.

$$\vdash \Box \Box a \leftrightarrow \Box a, \tag{T1}$$

$$\vdash \nabla \nabla a \leftrightarrow \nabla a. \tag{T2}$$

Proof. The implication from left to right follows from (A10). Let us prove the opposite implication. $\nabla a \rightarrow \triangle \nabla a$ by (A9). $\triangle \nabla \neg \nabla a \rightarrow \nabla \neg \nabla a$, by (A9). $\triangle \nabla a \rightarrow \nabla \triangle \nabla a$, is the contrapositive of the previous formula. But $\nabla \triangle \nabla a \rightarrow \nabla \nabla a$, by (A9), (R2), and (A8).

$$\vdash \Diamond a \leftrightarrow a \vee \bigcirc \Diamond a, \tag{T3}$$

$$\vdash \Diamond \Box (a \wedge b) \leftrightarrow \Diamond \Box a \wedge \Diamond \Box b, \tag{T4}$$

$$\vdash \bigcirc (a \wedge b) \leftrightarrow \bigcirc a \wedge \bigcirc b, \tag{T5}$$

$$\vdash \nabla (a \wedge b) \leftrightarrow \nabla a \wedge \nabla b, \tag{T6}$$

$$\vdash \neg (a \textit{U}\mathbf{ntil} b) \leftrightarrow \Box \neg b \vee [\neg b \textit{U}\mathbf{ntil}(\neg a \wedge \neg b)]. \tag{T7}$$

Theorems (T1), (T3)–(T5), and (T7) are theorems of the logic of linear time and their proofs may be found in Gabbay *et al.* (1980). Theorems (T2) and (T6) are theorems of (S5) and their proofs may be found in Hughes and Cresswell (1972) or Chellas (1980).

9. 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.

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 Lehmann *et al.*, 1981 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) $\textit{at}\ s_1 \rightarrow \Diamond\ \textit{at}\ s_3$.

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)

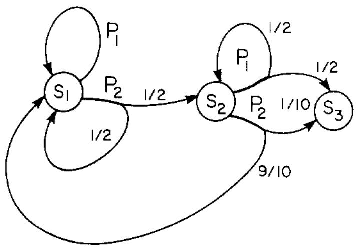

FIGURE 1

has only a technical role. It expresses the fact that the system cannot be at the same time in two different states:

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

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:

$$\text{(M1)}\quad \Box[at\ s_1 \rightarrow \bigcirc at\ s_1 \vee \bigcirc(at\ s_1 \vee at\ s_2) \wedge \triangle\bigcirc at\ s_1 \wedge \triangle\bigcirc at\ s_2].$$

Similarly (M2) describes the possible moves from s_2:

$$\begin{aligned}\text{(M2)}\quad \Box[at\ s_2 \rightarrow\ & \bigcirc(at\ s_2 \vee at\ s_3) \wedge \triangle\bigcirc at\ s_2 \wedge \triangle\bigcirc at\ s_3\\ & \vee \bigcirc(at\ s_1 \vee at\ s_3) \wedge \triangle\bigcirc at\ s_1 \wedge \triangle\bigcirc at\ s_3].\end{aligned}$$

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

$$\text{(B1)}\quad \Box\Diamond[at\ s_1 \wedge \bigcirc at\ s_1 \vee at\ s_2 \wedge \triangle\bigcirc at\ s_2 \wedge \triangle\bigcirc at\ s_3 \vee at\ s_3],$$

$$\text{(B2)}\quad \Box\Diamond[at\ s_1 \wedge \triangle\bigcirc at\ s_1 \wedge \triangle\bigcirc at\ s_2 \vee at\ s_2 \wedge \triangle\bigcirc at\ s_1 \wedge \triangle\bigcirc at\ s_3 \vee at\ s_3].$$

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 built 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:

$$E \wedge B2 \wedge \Diamond\Box at\, s_1 \rightarrow \Box\Diamond\triangle\bigcirc at\, s_2. \tag{11}$$

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

$$\Box\Diamond\triangle\bigcirc at\, s_2 \rightarrow \Box\Diamond\bigcirc at\, s_2. \tag{12}$$

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

$$E \wedge M1 \wedge M2 \wedge B2 \wedge at\, s_1 \rightarrow \Box\Diamond at\, s_2 \vee \Diamond at\, s_3. \tag{13}$$

But clearly (14) is *g*-valid:

$$M2 \wedge \Box\Diamond at\, s_2 \rightarrow \Box\Diamond\triangle\bigcirc at\, s_3. \tag{14}$$

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:

$$\Box\Diamond\triangle\bigcirc at\, s_3 \rightarrow \Diamond\bigcirc at\, s_3. \tag{15}$$

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.

10. Soundness

We shall now prove the soundness of the three logical systems TCg, TCb, and TCf.

THEOREM 1. *For any $\gamma \in \{g, b, f\}$ and for any $a \in \Gamma$, if $\vdash_\gamma a$, then $\vDash_\gamma a$.*

Proof. The proof is almost obvious. Indeed, we claim that, if $\vdash_\gamma a$, then for any γ-model U and any state s, $\tilde{p}_s(a) = 1$.

Axioms (A0)–(A7) clearly hold for all sequences of states in all models. Axiom (A8) holds for all sequences (i.e., at all states) in all models, because $\tilde{p}_s(b) \geqslant \tilde{p}_s(a \wedge (a \rightarrow b))$ and if both $\tilde{p}_s(c) = 1$ and $\tilde{p}_s(d) = 1$, then $\tilde{p}_s(c \wedge d) = 1$. Notice, now, that $\tilde{p}_s(\nabla a)$ and $\tilde{p}_s(\Delta a)$ may only be 0 or 1, and also that $\tilde{p}_s(\nabla a) = 1 \Leftrightarrow \tilde{p}_s(a) = 1$. Axiom (A9), then, holds for all sequences in all models, since $\tilde{p}_s(\Delta \nabla a) = 1 \Leftrightarrow \tilde{p}_s(\nabla \neg \nabla a) = 0 \Leftrightarrow \tilde{p}_s(\neg \nabla a) \neq 1 \Leftrightarrow \tilde{p}_s(\nabla a) \neq 0 \Leftrightarrow \tilde{p}_s(\nabla a) = 1$. Axiom (A10) need not hold for all sequences. But let us show that $\tilde{p}_s(\nabla a \rightarrow a) = 1$. We see that $\tilde{p}_s(\neg \nabla a \vee a) \geqslant \tilde{p}_s(\neg \nabla a)$ and $\tilde{p}_s(\neg \nabla a \vee a) \geqslant \tilde{p}_s(a)$. If $\tilde{p}_s(\neg \nabla a) = 1$, we are through. Otherwise, $\tilde{p}_s(\neg \nabla a) = 0$ and $\tilde{p}_s(a) = 1$. Axiom (A11) clearly holds for every sequence. Axiom (A12) does not hold for every sequence, but only for those sequences whose first transition has a positive probability, but those sequences have measure one. Indeed let σ be such that $p(\sigma_0, \sigma_1) > 0$, $\tilde{p}_{\sigma_0}(\bigcirc a) = \sum_{t \in S} p(\sigma_0, t) \times \tilde{p}_t(a)$. Therefore, $\tilde{p}_{\sigma_0}(\bigcirc a) = 1 \Rightarrow \tilde{p}_{\sigma_1}(a) = 1$.

Let now U be a b-model, with transition probabilities bounded by α. Axiom (A13) need not hold for all sequences. Let a denote the formula

$$a = \nabla a_0 \wedge \Delta \bigcirc (\nabla a_1 \wedge \Delta \bigcirc (\nabla a_2 \wedge \Delta \bigcirc (\cdots \wedge \Delta \bigcirc \nabla a_k))).$$

Notice that a is a *state* formula, i.e., its truth value depends only on the first state of the path at which it is evaluated. Consider, now, a state s at which a holds. There are states $s_0, s_1, \ldots, s_k$ such that $s_0 = s$, at s_i the formula ∇a_i holds, for any $i \leqslant k$ and $p(s_i, s_{i+1}) > 0$, for any $i < k$. But since our model is bounded, the set of sequences, out of s, that begin by $s_0, s_1, \ldots, s_k$ has a weight of at least α^k. A sequence σ that does not satisfy (A13) must therefore visit an infinite number of such states (possibly all different) but never takes the corresponding sequence $s_0, \ldots, s_n$, that has a bounded probability. The set of those sequences has weight zero.

Now let U be an f-model and let us show that U satisfies (A14). We shall show that the set Q of sequences of P_u that do not satisfy (A14) has measure zero. Let $T =^{\text{def}} \{s \in S \mid \tilde{p}_s(a) > 0\}$. Since S is finite, for any sequence $\sigma \in Q$ there is a state $s \in T$ that appears in σ an infinite number of times. For $s \in T$, let Q_s be the set of sequences of P_u that visit s an infinite number of times but no tail of which satisfy a. We have $Q = \bigcup_{s \in T} Q_s$. It is therefore enough to show that $\tilde{p}_u(Q_s) = 0$, for any $s \in T$. Elementary measure theory (without relying on the finiteness of S or the language Γ) shows that for all $s \in T$ and $\beta < 1$, there exists $n \in \mathbb{N}$ and $t_0, \dots, t_n \in S$ such that $t_0 = s$, $p(t_i, t_{i+1}) > 0$, for all $i < n$ and $\tilde{p}_{t_0}(a \mid [t_0, \dots, t_n]) > \beta$, where this last probability is a conditional probability and denotes the weight of all those sequences of P_{t_0} that satisfy a and begin by $t_0, \dots, t_n$ relative to the weight of all the sequences that begin in this way. But almost all sequences of Q_s contain the sequence $[t_0, \dots, t_n]$ at least once (as a subsequence) and therefore the probability of a tail that satisfies a is at least β. We conclude that, for $s \in T$, $\tilde{p}_u(Q_s) < \varepsilon$ for any $\varepsilon > 0$. Therefore $\tilde{p}_u(Q_s) = 0$.

The three inference rules (R0)–(R2) are obviously sound.

11. Completeness

THEOREM 2. *For any* $\gamma \in \{g, b, f\}$ *and for any* $a \in \Gamma$, *if* $\models_\gamma a$, *then* $\vdash_\gamma a$.

Theorem 2 is the main technical result of this paper and the remainder of this section is devoted to its proof. The proof proceeds by the method known as *selective filtration*. Our proof may also be used as a write-up and an extension of the completeness proof of Gabbay *et al.* (1980). The reader should notice the uniform treatment of all modalities. This uniformity guarantees that similar completeness proofs may be obtained for similar logics. We consider selective filtration to be more elegant and clearer than the tableau method that essentially amounts to brute force.

11.1. *Theories*

Since the basic results of this subsection are standard, they will not be proved. We define a theory to be any subset of Γ.

DEFINITION 7. A theory T is said to be γ-inconsistent if there is a $n \in \mathbb{N}$ and formulas $a_0, a_1, \dots, a_n \in T$ such that

$$\vdash_\gamma a_1 \wedge \cdots \wedge a_n \rightarrow \neg a_0.$$

If T is not γ-inconsistent, it is said to be γ-consistent.

DEFINITION 8. A theory T is said to be complete, if for any formula $a \in \Gamma$, either $a \in T$ or $\neg a \in T$.

LEMMA 1. *If T is a γ-consistent and complete theory, then*

(a) *if $a \in T$ and $\vdash_\gamma a \rightarrow b$, then $b \in T$,*

(b) $a \in T \Leftrightarrow \neg a \notin T$,

(c) $a \vee b \in T \Leftrightarrow a \in T$ *or* $b \in T$,

(d) *if T' is a γ-consistent theory (not necessarily complete), then there is a γ-consistent and complete theory T such that $T' \subseteq T$,*

(e) $\nvdash_\gamma a \Leftrightarrow$ *there is a γ-consistent and complete theory T such that $\neg a \in T$.*

11.2. *Relations Among Theories*

We pursue our study of consistent and complete theories, by defining relations among such theories. We define one relation per nonclassical connective, and prove some simple results about them.

11.2.1. *The Successor Relation*

DEFINITION 9. Let T_1 and T_2 be two theories, we say that T_2 is a successor of T_1 and write $T_1 \rho T_2$ if $\forall a \in \Gamma$ such that $\bigcirc a \in T_1$, we have $a \in T_2$.

LEMMA 2. *If T is a γ-consistent and complete theory, there is a unique γ-consistent and complete theory T^+ such that $T \rho T^+$. It is characterized by $a \in T^+ \Leftrightarrow \bigcirc a \in T$.*

11.2.2. *The Future Relation*

DEFINITION 10. We say that T_2 is a future of T_1 and write $T_1 \leqslant T_2$ if $\forall a \in \Gamma$ such that $\Box a \in T_1$, we have $a \in T_2$.

LEMMA 3. *Among γ-consistent and complete theories the relation $\leqslant$ is reflexive and transitive, it contains the relation ρ.*

Notice that $\leqslant$ contains the reflexive and transitive closure of ρ. Indeed the inclusion is strict. Hint: consider a consistent theory that contains $\bigcirc^{(k)} a$ for all k's, but contains also $\neg \Box a$, and use Lemma 4.

LEMMA 4. *Let T be a γ-consistent and complete theory and $a \in \Gamma$ a formula with $\neg \Box a \in T$. There is a γ-consistent and complete theory T', such that $T \leqslant T'$ and $\neg a \in T'$.*

11.2.3. *The Alternative Relation*

DEFINITION 11. We say that T_2 is an alternative for T_1 and write $T_1 \equiv T_2$ if $\forall a \in \Gamma$ such that $\nabla a \in T_1$, we have $a \in T_2$.

LEMMA 5. *Among γ-consistent and complete theories the relation $\equiv$ is an equivalence relation.*

Proof. The relation $\equiv$ is reflexive by Axiom (A10). It is transitive by (T2). Let us show that it is symmetric. Suppose $T \equiv T'$ and $\nabla a \in T'$ and $a \notin T$. Then $\neg a \in T$, $\Delta \neg a \in T$ by (A10)'s contrapositive, $\nabla \Delta \neg a \in T$ by (A9)'s contrapositive and $\Delta \neg a \in T'$. But $\nabla a \in T'$, $\Delta \neg a \in T'$ and T' is γ-consistent. A contradiction. Q.E.D.

A consequence is that, if $T \equiv T'$, then $\nabla a \in T$ iff $\nabla a \in T'$.

LEMMA 6. *Let T be a γ-consistent and complete theory and $a \in \Gamma$ a formula with $\neg \nabla a \in T$. There is a γ-consistent and complete theory T', such that $T \equiv T'$ and $\neg a \in T'$.*

Proof. If the theory $R =^{\mathrm{def}} \{b \mid \nabla b \in T\} \cup \{\neg a\}$ is γ-consistent, then it may be completed to a satisfactory T' by Lemma 1(d). Suppose that R is γ-inconsistent. Then there are formulas b_i, $i = 1,\ldots, n$ such that $\nabla b_i \in T$ for $i = 1,\ldots, n$ and $\vdash_\gamma b_1 \wedge b_2 \wedge \cdots \wedge b_n \rightarrow a$. It follows that $\vdash_\gamma \nabla[b_1 \wedge \cdots \wedge b_n \rightarrow a]$, by (R2). Then $\vdash_\gamma \nabla[b_1 \wedge \cdots \wedge b_n] \rightarrow \nabla a$, by (A8). $\vdash_\gamma \nabla b_1 \wedge \cdots \wedge \nabla b_n \rightarrow \nabla a$, by (T6). Therefore $\nabla a \in T$, a contradiction. Q.E.D.

The next lemma exactly translates Axiom (A12) in terms of theories.

LEMMA 7. *Let T_1, T_2, and T_3 be γ-consistent and complete theories, such that $T_1 \rho T_2$ and $T_2 \equiv T_3$, then there is a γ-consistent and complete theory T' such that $T_1 \equiv T'$ and $T' \rho T_3$.*

Proof. Consider $R =^{\mathrm{def}} \{a \mid \nabla a \in T_1\} \cup \{\bigcirc b \mid \in T_3\}$. If the theory R is γ-consistent, take T' to be any γ-consistent complete extension of R (there exists one by Lemma 1(d)). Suppose R is not γ-consistent. There are formulas $a_i, i = 1,\ldots, m$ and b_j, $j = 1,\ldots, n$, such that $\nabla a_i \in T_1$, $b_j \in T_3$ and $\vdash_\gamma\ a_1 \wedge \cdots \wedge a_m \rightarrow \neg[\bigcirc b_1 \wedge \cdots \wedge \bigcirc b_n]$. Then, by (R2), (T5), and (A8), $\vdash_\gamma \nabla[a_1 \wedge \cdots \wedge a_m] \rightarrow \nabla \neg \bigcirc [b_1 \wedge \cdots \wedge b_n]$. Therefore, by (T6), (A2), (A8), and (A12) $\vdash_\gamma \nabla a_1 \wedge \cdots \wedge \nabla a_m \rightarrow \bigcirc \nabla \neg [b_1 \wedge \cdots \wedge b_n]$. Then $\bigcirc \nabla \neg [b_1 \wedge \cdots \wedge b_n] \in T_1$ and $\nabla \neg [b_1 \wedge \cdots \wedge b_n] \in T_2$. Therefore $\neg [b_1 \wedge \cdots \wedge b_n] \in T_3$. A contradiction. Q.E.D.

Whenever R_1 and R_2 are relations, we shall use $R_1 R_2$ to denote the composition of the two relations (R_1 first, and then R_2). With this notation, Lemma 7 states that, for γ-consistent and complete theories, $(\rho\equiv) \subseteq (\equiv\rho)$.

The next lemma is an easy consequence of the previous one, but it is, with its variations for the bounded and the finite case, of central importance.

LEMMA 8. *Let $k \geqslant 0$ and $T_0, T_1, ..., T_k$ be γ-consistent and complete theories such that $\forall i$, $0 \leqslant i < k$, $T_i \equiv \rho T_{i+1}$. There are γ-consistent and complete theories S_i, for $i = 0, ..., k$, such that*

(1) $S_i \equiv T_i, \forall i, 0 \leqslant i \leqslant k,$

(2) $S_i \rho S_{i+1}, \forall i, 0 \leqslant i < k.$

Proof. By induction on k. For $k = 0$, take $S_0 = T_0$. For $k > 0$, use the induction hypothesis to find S_i, for $1 \leqslant i \leqslant k$. Now $T_0 \equiv \rho T_1 \equiv S_1$. There is a γ-consistent and complete theory U, such that $T_0 \doteq U$, and $U\rho \equiv S_1$. By Lemma 7, then there is an S_0, with $U \equiv S_0$ and $S_0 \rho S_1$. Q.E.D.

11.3. *Terminal Theories and Terminal Relations*

11.3.1. *Terminal Theories*

The relations described above are fine for studying the system TCg. For studying TCb and TCf we also need a refinement of some of the notions above. First, since Axioms (A13) and (A14) express the fact that certain propositions are only true after a certain time, we need to capture the notion of a theory that is far enough in the future for anything that must become true from a certain time on to have already become true. Our notion of a terminal theory is a technical innovation of this work. It exemplifies the advantage that may be taken of consistent theories that have no model.

DEFINITION 12. A g-consistent and complete theory T is said to be terminal *iff* it satisfies any one of the two equivalent properties:

(1) $\forall a, a \in \Gamma \ \Diamond\Box a \in T \Rightarrow a \in T,$

(2) $\forall a, a \in \Gamma \ \Diamond a \in T \Rightarrow \Box\Diamond a \in T.$

The proof of the equivalence of the two propositions above is the following:

Proof. Suppose (1) and $\Diamond a \in T$. If $\Box\Diamond a \notin T$, then $\Diamond\Box\neg a \in T$ and $\Diamond\Box\Box\neg a \in T$. Then $\Box\neg a \in T$. A contradiction. Suppose (2) and $\Diamond\Box a \in T$. Then $\Box\Diamond\neg a \notin T$ and $\Diamond\neg a \notin T$, $\Box a \in T$ and $a \in T$. Q.E.D.

The interest of terminal theories is contained in Lemmas 9 and 10.

LEMMA 9. (1) *Let T and T' be γ-consistent and complete theories, such that $T \leqslant T'$, then, if T is terminal, so is T'.*

(2) *Let T be a γ-consistent, complete and terminal theory, then $T^+ \leqslant T$.*

LEMMA 10. *Let T be a γ-consistent and complete theory, then there is a γ-consistent and complete terminal theory T', such that $T \leqslant T'$.*

Proof. Consider $\{a \mid \Diamond\Box a \in T\}$, which is γ-consistent by (T4), and complete it to obtain T'. Let $\Box a \in T$, then $\Diamond\Box a \in T$ and by construction $a \in T'$. Therefore $T \leqslant T'$. Let now $\Diamond\Box a \in T'$, then $\Diamond\Box a \in T$, by the previous remark, and therefore $a \in T'$. We conclude that T' is terminal.

Q.E.D.

11.3.2. *Terminal Relations*

We also need a refinement of the alternative relation.

DEFINITION 13. Let T_1 and T_2 be g-consistent and complete, we say that T_2 is a terminal alternative for T_1 and write $T_1 \approx T_2$ iff

(1) $T_1 \equiv T_2$,
(2) $T_1 \leqslant T_2$,
(3) $T_2 \leqslant T_1$.

Conditions (2) and (3) (together) are equivalent to: $\forall a \in \Gamma$, $\Box a \in T_1 \Leftrightarrow \Box a \in T_2$.

LEMMA 11. *Among g-consistent and complete theories, the relation $\approx$ is an equivalence relation: it is contained in the relation $\equiv$.*

11.4. *Basic Lemmas for the Bounded Case*

LEMMA 12. *Let $k \geqslant 0$ and $T_0, T_1, \ldots, T_k$ be b-consistent and complete theories such that $\forall i$, $0 \leqslant i < k$, $T_i \equiv \rho T_{i+1}$. If T_0 is terminal, there are b-consistent and complete theories S_i, for $i = 0, \ldots, k$ such that*

(1) $S_0 \approx T_0$,
(2) $S_i \equiv T_i$, $\forall i$, $0 < i \leqslant k$,
(3) $S_i \rho S_{i+1}$, $\forall i$, $0 \leqslant i < k$.

Proof. Let R be the following theory:

$$\{a_0 \mid \nabla a_0 \in T_0\} \cup \{\Box b \mid \Box b \in T_0\} \cup \{\Diamond c \mid \Diamond c \in T_0\} \cup \{\bigcirc a_1 \mid \nabla a_1 \in T_1\}$$
$$\cup \{\bigcirc\bigcirc a_2 \mid \nabla a_2 \in T_2\} \cup \cdots \cup \{\bigcirc^{(k)} a_k \mid \nabla a_k \in T_k\}.$$

First we want to show that R is b-consistent. Suppose not. By using (T5) and

(T6), one may group together formulas of the same summand of R and may find formulas, as above, such that

$$\underset{b}{\vdash} \Box b_1 \wedge \Box b_2 \wedge \cdots \wedge \Box b_l \wedge \Diamond c_1 \wedge \cdots \wedge \Diamond c_m \rightarrow \neg(a_0 \wedge \bigcirc a_1 \wedge \cdots \wedge \bigcirc^{(k)} a_k).$$

By (R1) and some obvious manipulations,

$$\underset{b}{\vdash} \Box b_1 \wedge \Box b_2 \wedge \cdots \wedge \Box b_l \wedge \Box\Diamond c_1 \wedge \cdots \wedge \Box\Diamond c_m$$
$$\rightarrow \Box\neg(a_0 \wedge \bigcirc a_1 \wedge \cdots \wedge \bigcirc^{(k)} a_k).$$

Therefore, since T_0 is terminal, $\Box\neg(a_0 \wedge \bigcirc a_1 \wedge \cdots \wedge \bigcirc^{(k)} a_k)$ must be in T_0. But $\nabla a_k \in T_k$, and therefore $\Delta\bigcirc\nabla a_k \in T_{k-1}$. Then $\nabla a_{k-1} \wedge \Delta\bigcirc\nabla a_k \in T_{k-1}$. In this way we can see that $\nabla a_0 \wedge \Delta\bigcirc(\nabla a_1 \wedge (\cdots \wedge \Delta\bigcirc\nabla a_k \cdots))$ is in T_0. But T_0 is terminal and the antecedent of Axiom (13) is in T_0. Therefore $\Diamond(a_0 \wedge \bigcirc a_1 \wedge \cdots \wedge \bigcirc^{(k)} a_k)$ must be in T_0. Contradiction. We showed that R is b-consistent. By Lemma 1(d), there is a b-consistent and complete theory S_0 that contains R. Clearly $S_0 \approx T_0$. Take S_i to be $S_0^{+(i)}$, for $i = 1, ..., k$. We are left to show that, $\forall i$, $1 \leqslant i \leqslant k$, we have $S_i \equiv T_i$. Suppose $\nabla e \in T_i$, by construction $\bigcirc^{(k)} e \in S_0$ and $e \in S_i$. Q.E.D.

The next lemma is a corollary of Lemma 12.

Lemma 13. *Let $k \geqslant 0$, S and T be b-consistent and complete theories, and suppose that T is terminal and that $T \equiv S$. There are b-consistent and complete theories $T_0, T_1, ..., T_k$ and $S_0, S_1, ..., S_k$ such that $T_i \equiv S_i$, $\forall i = 0, ..., k$, $T_0 = T$, $S_0 = S$, $T_i \approx \rho T_{i+1}$* and *$S_i \rho S_{i+1}$, $\forall i = 0, ..., k-1$.*

Proof. By induction on k. For $k = 0$, the result is clear. Suppose $k > 0$. By the induction hypothesis, we build T_i and S_i for $i = 0, ..., k-1$. Now we have $T_{k-1} \equiv \rho S^+_{k-1}$. By Lemma 12 (with $k = 1$), there is a theory U such that $U \approx T_{k-1}$ and $U^+ \equiv S^{+(k)}$. Take $T_k = U^+$. Q.E.D.

11.5. *Basic Lemmas for the Finite Case*

The first basic lemma for the finite case is fundamental.

Lemma 14. *Let T and S be f-consistent and complete theories, such that $T \equiv S$. If T is terminal, then $T \approx S$.*

Proof. Let us show that $T \leqslant S$. Suppose $\Box a \in T$. By (7) then, $\Diamond\Box\nabla a$ is in T. Since T is terminal, $\nabla a \in T$ and $a \in S$. Let us show now that $S \leqslant T$. We show that $\Diamond a \in T \Rightarrow \Diamond a \in S$. Suppose that $\Diamond a \in T$. Since T is terminal $\Box\Diamond a \in T$. By (7) then, $\Diamond\Box\nabla\Diamond a \in T$. Since T is terminal, $\nabla\Diamond a \in T$ and $\Diamond a \in S$. Q.E.D.

From Lemma 6, now follows:

LEMMA 15. *Let T be an f-consistent complete terminal theory and $a \in \Gamma$ a formula with $\neg\nabla a \in T$. There is an f-consistent and complete theory T', such that $T \approx T'$ and $\neg a \in T'$. The theory T' is terminal.*

Lemmas 7 and 8 have similar refinements that the reader may easily find.

11.6. *Traces and Relations Among Them*

Since not every consistent theory has a model, we need to restrict ourselves to a finite set of formulas.The first thing to do, then, is to restrict our attention to those propositional variables that appear in the formulas of interest. Without loss of generality, we shall, from now on, suppose that **Pvar** is a finite set. Therefore, for any n, Γ_n is finite. For the remainder of the proof, let $n \in \mathbb{N}$ be a fixed number. We are interested only in the formulas of Γ_n, but since we need to consider, for the proof, also some slightly larger formulas, we define n' to be slightly larger than n. For example, we may take $n' =^{\text{def}} n + 7$. We shall define traces of theories over $\Gamma_{n'}$, but we shall claim only about formulas of Γ_n.

DEFINITION 14. A γ-trace D of size n (we shall not mention n any more) is the intersection of some γ-consistent and complete theory T with $\Gamma_{n'}$.

Notice we use n' not n. There is only a finite number of traces of size n. Let $\mathscr{D}_n$ be the set of all traces of size n (the γ in question will be clear from the context). A trace is a finite set of formulas and may therefore be charactecterized by a formula.

DEFINITION 15. If $D \in \mathscr{D}_n$ is a γ-trace of size n, we define the characteristic formula of D by $\chi_D =^{\text{def}} \bigwedge_{a \in D} a \wedge \bigwedge_{a \in \Gamma_{n'} - D} \neg a$.

The characteristic formula χ_D is not in general in D. The next lemma summarizes the properties of characteristic formulas.

LEMMA 16. *Let D be a γ-trace and T a γ-theory, then $D = T \cap \Gamma_{n'} \Leftrightarrow \chi_D \in T$.*

We define between traces all the relations that have been defined between theories: ρ, $\leqslant$, $\equiv$, $\equiv\rho$, $\approx\rho$, and $\approx$, in the following way: $D \mathrel{\mathrm{R}} D' \Leftrightarrow$ there are theories T and T' such that $D = T \cap \Gamma_{n'}$, $D' = T' \cap \Gamma_{n'}$ and $T \mathrel{\mathrm{R}} T'$. Notice that $\equiv\rho$ and $\approx\rho$ are the projections of the composition of relations, **not** the composition of the projections.

Similarly, terminal traces are traces of terminal theories. A word of caution is in order here: the relations defined above among traces do not enjoy all the nice properties that they enjoy over theories (e.g., $\geqslant$ need not be transitive). We take care not to use any of those properties, by proving everything we need on the theories themselves, and only then project the property on the traces.

We define ρ_γ^* to be the reflexive and transitive closure of the relation ρ on the γ-traces. Notice that ρ_γ^* is the reflexive and transitive closure of the projection, **not** the projection of the reflexive and transitive closure. We offer the following explanation to the difference in our treatment between ρ_γ^* and the other relations. All other relations really live on the level of theories and everything concerning them should be done at this higher level and projected downwards on the level of traces only at the last instant. On the other hand the interest of ρ_γ^* lies only at the level of traces, i.e., we have no reason to consider this relation among theories since it does not correspond to any connective of our logic.

Lemmas 17 and 18 explain the interest of considering traces, their proofs are as in Gabbay *et al.* (1980).

LEMMA 17. *Let D be a γ-trace and $E_1,..., E_m$ the ρ-successors of D, then* $\vdash_\gamma \chi_D \rightarrow \bigcirc(\chi_{E_1} \vee \cdots \vee \chi_{E_m})$.

Proof. Suppose not. There is a γ-consistent and complete theory T that contains χ_D and $\neg\bigcirc(\chi_{E_1} \vee \cdots \vee \chi_{E_m})$. By Lemma 16, $T \cap \Gamma_{n'} = D$. But T contains $\bigcirc\neg(\chi_{E_1} \vee \cdots \vee \chi_{E_m})$, and therefore T^+ contains $\neg\chi_{E_i}$ for any $i = 1,..., m$. By Lemma 16, $T^+ \cap \Gamma_{n'}$ is not one of the E_i, $i = 1,..., m$. Contradiction. Q.E.D.

LEMMA 18. *Let D and D' be γ-traces. If $D \leqslant D'$, then $D\rho_\gamma^* D'$.*

Proof. Let $D \leqslant D'$. By definition of the relation $\leqslant$ on traces, there are γ-consistent and complete theories T and T' such that $T \leqslant T'$, $D = T \cap \Gamma_{n'}$ and $D' = T' \cap \Gamma_{n'}$. By Lemma 16, we have $\chi_D \in T$ and $\chi_{D'} \in T'$. Let $E_1,..., E_m$ be all the traces that are in the relation ρ_γ^* with D (D is one of them). Let $\chi =^{\text{def}} \chi_{E_1} \vee \cdots \vee \chi_{E_m}$. By Lemma 17, $\vdash_\gamma \chi_{E_i} \rightarrow \bigcirc\chi$, for any $i = 1,..., m$, since all ρ-successors of E_i are contained in the list: $E_k, k = 1,..., m$. Therefore $\vdash_\gamma \chi \rightarrow \bigcirc\chi$. By (R1): $\vdash_\gamma \Box(\chi \rightarrow \bigcirc\chi)$. By (A7): $\vdash_\gamma \chi \rightarrow \Box\chi$. Therefore $\Box\chi \in T$ and $\chi \in T'$. By Lemma 16, D' is one of the E_i, $i = 1,..., m$. Q.E.D.

All three proofs of completeness begin the same way. Suppose that $\nvdash_\gamma a$, we shall build a γ-model that does not satisfy a. First, by Lemma 1(e), there is a γ-consistent and complete theory T_a, that contains $\neg a$. Now take $n = \#(a)$. We shall look at γ-traces of size n. Let $D_a =^{\text{def}} T_a \cap \Gamma_{n'}$. It is a γ-trace of size n, that contains $\neg a$.

11.7. *Completeness of* TCg

The model $U = \langle S, u, l, p \rangle$, that does not satisfy a, is defined the following way:

(1) $S = \mathbb{N} \times \mathscr{D}_n$.

(2) $u = \langle 0, D_a \rangle$.

(3) $l(\langle i, D \rangle) = \{p \mid p \in D\}$.

(4) Let us say, first, that the only transitions with nonzero probability are those that increase the first coordinate by one and use $\equiv\rho$ to move along the second coordinate. In other terms, $p(\langle i, D \rangle, \langle j, E \rangle) \neq 0 \Leftrightarrow j = i + 1$ and $D \equiv\rho E$. If $D\rho E$ let us call the transition from $\langle i, D \rangle$ to $\langle i+1, E \rangle$ a standard transition. A transition of positive probability that is not standard, will be called nonstandard. Our goal is to give increasing (with the first coordinate) weight to the standard transitions, and ensure that, with probability one, after a certain time, only standard transitions occur. Therefore we choose a sequence α_i of real numbers between 0 and 1, such that $\prod_{i=0}^{\infty} \alpha_i > 0$. From state $\langle i, D \rangle$, we give equal probability to all standard transitions, so as to give them total weight α_i, and equal probability to all nonstandard transitions, so as to give them total weight $1 - \alpha_i$.

Our goal is to show that in U, $\tilde{p}_u(\neg a) > 0$ and therefore the model U does not satisfy a. We shall call a sequence of states standard if it is a sequence of standard transitions. A sequence of states is called ultimately standard, if it is a sequence of transitions of positive probability and some tail of it is a standard sequence (i.e., the sequence is standard after a certain point). First we notice

LEMMA 19. *Let s be a state of U. The weight of all standard sequences from s (under $\tilde{p}_s$) is strictly positive and the weight of all ultimately standard sequences from s is* 1. *Formally,* $\tilde{p}_s(\{\sigma \mid \sigma \in P_s, \sigma \textit{ is standard}\}) > 0$, *and* $\tilde{p}_s(\{\sigma \mid \sigma \in P_s, \sigma \textit{ is ultimately standard}\}) = 1$.

Proof. Let Q_k be the set of all sequences σ of P_s that begin by k standard moves, i.e., such that $\sigma_j \rho \sigma_{j+1}$, for all $j, 0 \leqslant j < k$. By construction $\tilde{p}_s(Q_k) \geqslant \prod_{j=0}^{k-1} \alpha_j$. Therefore $\tilde{p}_s(\{\sigma \mid \sigma \in P_s, \sigma \text{ is standard}\}) \geqslant \prod_{j=0}^{\infty} \alpha_j > 0$. Let R_k be the set of all sequences σ of P_s that are standard after index k, i.e., such that $\sigma_j \rho \sigma_{j+1}$, for all $j, k \leqslant j$. By construction $\tilde{p}_s(R_k) \geqslant \prod_{j=k}^{\infty} \alpha_j$. Therefore $\tilde{p}_s(\{\sigma \mid \sigma \in P_s, \sigma \text{ is ultimately standard}\}) \geqslant \lim_{k \to \infty} \prod_{j=k}^{\infty} \alpha_j = 1$. Q.E.D.

DEFINITION 16. If $\sigma = \{\langle k_i, D_i \rangle\}$ and $\tau = \{\langle j_i, E_i \rangle\}$ are sequences of states, we say that σ and τ are equivalent and write $\sigma \equiv \tau$ iff for every $i \in \mathbb{N}$, $D_i \equiv E_i$.

Definition 17 captures the essential (for us, now) property of random sequences, i.e., the property that almost all sequences satisfy. In the completeness proofs of the other systems we shall need a stronger property.

Definition 17. Let σ be a sequence of states of U, σ is said to be generic iff for any trace D that appears an infinite number of times (as a second component) in σ, any trace E such that $D\rho E$ appears (as a second component) in σ an infinite number of times.

Lemma 20. *At any state, the weight of generic sequences is one, i.e., for any state s, $\tilde{p}_s(\{\tau \mid \tau \in P_s, \tau \text{ is generic}\}) = 1$.*

Proof. Suppose that $D\rho E$ and that, on the whole, D has exactly n ρ-successors. Let Q_k be the set of all sequences σ of P_s that contain D at least k times but do not contain E even once. Clearly $\tilde{p}_s(Q_k) \leqslant \prod_{j=0}^{k-1} (1-\alpha_k)$. It follows that for any state s, $\tilde{p}_s(\{\tau \mid \tau \in P_s, \tau \text{ is not generic}\})$

$$\leqslant \prod_{k=0}^{\infty} (1-\alpha_k) = 0. \qquad \text{Q.E.D.}$$

Notice that, if a sequence of states $\sigma = \{\langle k_i, D_i \rangle\}$ is generic and if a trace E appears an infinite number of times in the sequence (as a second component), then every trace F such that $E\rho^*F$ also appears an infinite number of times. Our basic result concerning U is

Lemma 21. *Let $b \in \Gamma_n$, σ a generic standard sequence of states (of U), and τ and τ' two equivalent sequences of states, then*

(a) $b\,|_U^{\sigma} = \textbf{true} \Leftrightarrow b \in D_0$, *where* $\sigma_i = \langle k_i, D_i \rangle$,

(b) $b\,|_U^{\tau} = b\,|_U^{\tau'}$.

Proof. The proof is by induction on the size of b, i.e., $\#(b)$, at each induction step, we prove (a) first, and then (b).

$b = p$. (a) $p\,|_U^{\sigma} = \textbf{true} \Leftrightarrow p \in l(\sigma_0) \Leftrightarrow p \in D_0$,

(b) $p\,|_U^{\tau} = \textbf{true} \Leftrightarrow p \in E$, where $\tau_0 = \langle i, E \rangle \Leftrightarrow \nabla p \in E$, by (A11) and because $n' \geqslant n+1 \Leftrightarrow \nabla p \in E'$, where $\tau'_0 = \langle i, E' \rangle$, since $E \equiv E' \Leftrightarrow p \in E' \Leftrightarrow p\,|_U^{\tau'} = \textbf{true}$.

$b = \neg c$. Obvious.

$b = c \vee d$. Obvious.

$b = \bigcirc c$. (a) $\bigcirc c\,|_U^{\sigma} = \textbf{true} \Leftrightarrow c\,|_U^{\sigma^1} = \textbf{true} \Leftrightarrow c \in D_1 \Leftrightarrow \bigcirc c \in D_0$, since $D_0 \rho D_1$ (since σ is a standard sequence).

(b) Obvious.

$b = \Box c$. (a) $\Box c \in D_0 \Rightarrow \forall i \in \mathbb{N}$, $\Box c \in D_i$, (by induction on i, using (A5)) since σ is a standard sequence $\Rightarrow \forall i \in \mathbb{N}$, $c \in D_i \Rightarrow \forall i \in \mathbb{N}$, $c\,|_U^{\sigma^i} = \textbf{true}$, by the induction hypothesis and since the end part of a generic sequence is generic $\Rightarrow \Box c\,|_U^{\sigma} = \textbf{true}$.

Suppose now that $\Box c \notin D_0$. Then $\Diamond\neg c \in D_0$. It follows that $\exists i \in \mathbb{N}$, $\neg c \in D_i$ or $\forall i \in \mathbb{N}$, $\Diamond\neg c \in D_i$ (by (T3)). We want to show that the first alternative is true. In the last case, there is a trace E, that appears an infinite number of times, and $\neg\Box c \in E$. Since the sequence σ is generic, all traces F such that $E\rho^*F$ appear an infinite number of times in the sequence. By Lemmas 4 and 18 then, there is an $i \in \mathbb{N}$, for which $\neg c \in D_i$. We conclude that $\exists i \in \mathbb{N}$ such that $c \notin D_i$ and by the induction hypothesis $c\,|_U^{\sigma^i} =$ **false** and $\Box c\,|_U^{\sigma} =$ **false.**

(b) Obvious.

$b = c$**Until**d. (a) Suppose c**Until**$d \in D_0$. Then, by (A4), $\Box\neg d \notin D_0$ and by the induction hypothesis there exists an index k, for which $d \in D_k$. Let i be the smallest such k. Now using (A6), one may show that for any $j < i$, $c \in D_j$. Now by (A6) and the induction hypothesis part (a), one sees that c**Until**$d\,|_U^{\sigma} =$ **true.**

Suppose now that c**Until**$d \notin D_0$. Then, by (T7), either $\Box\neg d \in D_0$, and we conclude by the induction hypothesis part (a), or, by (T7) and (A4), $\Box(c \vee d) \notin D_0$. By the induction hypothesis part (a), there is an index k, for which $c \notin D_k$ and $d \notin D_k$. Let i be the smallest such k. Now, by using (A6) and the induction hypothesis, one may show, by induction on i, that c**Until**$d\,|_U^{\sigma} =$ **false.**

(b) Obvious.

$b = \nabla c$. (a) Suppose $\nabla c \in D_0$. We want to show that, for almost all sequences $\tau \in P_{\sigma_0}$, we have $c\,|_U^{\tau} =$ **true.** Since almost all sequences of P_{σ_0} are generic (by Lemma 20), it is enough, by Lemma 19 to show that if τ is generic and ultimately standard, then $c\,|_U^{\tau} =$ **true.** Let τ be standard from index i on. By Lemma 8, there are g-consistent and complete theories: S_m, $0 \leqslant m < i$ such that $S_m \equiv D_m$, $\forall m$ $0 \leqslant m < i$ and $S_m \rho S_{m+1}$, $\forall m$, $0 \leqslant m < i - 1$. Let us define the sequence τ' by: $\tau'_m = \langle k_m, S_m \rangle$ $\forall m$, $0 \leqslant m < i$ and $\tau'_m = \tau_m$, $\forall m$, $i \leqslant m$. The sequence τ' is equivalent to τ. Therefore, by the induction hypothesis, part (b), $c\,|_U^{\tau} = c\,|_U^{\tau'}$. It is generic since it is identical with τ from index i on an since τ is generic. It is also standard. Since τ' is standard and generic, we conclude, by the induction hypothesis part (a), that $c\,|_U^{\tau'} =$ **true** $\Leftrightarrow c \in D'$, where $\tau'_0 = \langle k, D' \rangle$. But since $\tau \equiv \tau'$, and $\nabla c \in D_0$, we conclude that $c \in D'$.

Suppose now that $\neg\nabla c \in D_0$. We must find a set Q of sequences that begin at σ_0 and do not satisfy c, such that Q has a positive measure. Remember that $\sigma_0 = \langle k_0, D_0 \rangle$. By Lemma 6, there is a trace E such that $D_0 \equiv E$ and $c \notin E$. Let E' be any trace such that $E\rho E'$. Lemma 2 ensures the existence of such an E'. We have $D_0 \equiv\rho E'$, and by the definition of our model $p(\langle k_0, D_0 \rangle, \langle k_0 + 1, E' \rangle) > 0$. Let us define Q as the set of all sequences τ such that: $\tau_0 = \sigma_0$, $\tau_1 = \langle k_1, E' \rangle$ and the sequence τ^1 is standard and generic. By Lemma 19, we have $\tilde{p}_{\sigma_0}(Q) > 0$. It is left to us to show that no sequence of Q satisfies c. Let τ be any sequence of Q. Let τ' be the sequence $\langle k_0, E \rangle$, $\tau_1, \tau_2, \ldots$. It is a generic standard sequence. By the induction hypothesis, part (a) we have $c \,|_U^{\tau'} =$ **false**. But since $D_0 \equiv E$, $\tau \equiv \tau'$. We conclude, by the induction hypothesis, part (b), that $c \,|_U^{\tau} =$ **false**.

(b) Let σ be any generic standard sequence starting at τ_0. Since the truth value of ∇c depends only on the first state of the sequence we have $\nabla c \,|_U^{\tau} = \nabla c \,|_U^{\sigma}$. By the induction hypothesis, part (a) just above: $\nabla c \,|_U^{\sigma} =$ **true** $\Leftrightarrow \nabla c \in D$, where $\tau_0 = \sigma_0 = \langle k_0, D \rangle$. Similarly $\nabla c \,|_U^{\tau'} =$ **true** $\Leftrightarrow \nabla c \in D'$, where $\tau'_0 = \langle k_0, D' \rangle$. But, since $D \equiv D'$, $\nabla c \in D \Leftrightarrow \nabla c \in D'$. Q.E.D.

We may now conclude the proof of completeness. Since $\neg a \in D_a$ and D_a is the initial state of our model U, we conclude from Lemmas 19 and 21 that $\tilde{p}_u(\neg a) > 0$ and therefore $U \not\models a$.

11.8. *Completeness of* TCb

There are many ways to build a satisfactory model, we choose a model that may be described concisely. The model $U = \langle S, u, l, p \rangle$, that does not satisfy a, is defined the followed way:

(1) $S = \mathbb{N} \times \mathscr{D}_n$.

(2) $u = \langle 0, D_a \rangle$.

(3) $l(\langle i, D \rangle = \{p \mid p \in D\}$.

(4) Choose some number α: $\frac{1}{2} < \alpha < 1$. We distinguish here between the states of first coordinate 0 and the other ones. For states whose first coordinate is zero, we give a positive probability to a move from $\langle 0, D \rangle$ to $\langle 0, D' \rangle$ iff $D \equiv \rho D'$. We give a positive probability to a move from $\langle 0, D \rangle$ to $\langle 1, D' \rangle$ iff D is terminal and $D \approx \rho D'$. All other transitions from $\langle 0, D \rangle$ have probability zero. We give equal probabilities to all moves of positive probability. For states whose first coordinate is positive, we allow to increase or decrease by one the first coordinate. If $i > 0$, we give a positive probability to a transition from $\langle i, D \rangle$ to $\langle j, D' \rangle$ iff $D \approx \rho D'$ and either $j = i - 1$ or $j = i + 1$. Moreover, we give a combined weight of α ($\alpha > \frac{1}{2}$) to those moves that increase the first coordinate.

Notice that states $\langle k, D \rangle$ with $k > 0$ and D not terminal cannot be reached from the initial state by transitions of positive probability. We may as well exclude those states from our consideration. From now on, if $\langle k, D \rangle$ is a state such that $k > 0$, then D is terminal.

Let σ be a sequence and let $\sigma_i = \langle k_i, D_i \rangle$. Let m be a natural number. We define σ to be m-standard iff there exists a j, such that D_j is terminal, for all i

such that $j + m \leqslant i$, we have $D_i \approx\rho D_{i+1}$ and for all i such that, $i \leqslant j + m - 1$ we have $D_i \rho D_{i+1}$. Notice that in this case D_i is terminal for any $i \geqslant j$.

A sequence is said to be m-ultimately standard if it has a tail that is m-standard.

The definition of equivalent sequences is unchanged. We shall now need a stronger definition of generic sequences (it is needed in the $\Diamond$ case below).

DEFINITION 18. Let σ be a sequence of states of U, σ is said to be generic iff for any trace D_0 that appears an infinite number of times (as a second component) in σ and for any finite sequence of traces $D_0, D_1, \ldots, D_m$ such that $D_i \rho D_{i+1}$, for every i such that $0 \leqslant i < m$ the sequence above appears (as second components) in σ (in this order) an infinite number of times.

Lemma 20 stays true, since, in our model, ρ-transitions always have a positive bounded probability.

Our next task is to prove a strengthened version of Lemma 19.

LEMMA 22. *Let s be a state of U. The weight of all m-standard sequences from s (under $\tilde{p}_s$) is strictly positive and the weight of all ultimately m-standard sequences from s is* 1.

Proof. A classical result of the theory of Markov chains (see, for example, Proposition 5–18 of Kemeny *et al.*, 1966) ensures that, if $s = \langle i, D \rangle$ is a state such that $i > 0$, the set of sequences beginning at s that contain only states with a first coordinate $k > i$ (except the first state of the sequence, obviously) has a positive weight and that the set of sequences beginning at s that contain an infinite number of states with a first coordinate of i has weight zero. This property depends crucially on the fact that $\alpha > \frac{1}{2}$. Then, using also Lemmas 10 and 20, we see that, if s is any state, the set of m-standard sequences beginning at s has a positive weight and the set of m-ultimately standard sequences beginning at s has weight one. Q.E.D.

Our basic result concerning U is

LEMMA 23. *Let $b \in \Gamma_n$, σ a generic $\Omega(b)$-standard sequence of states (of U) and τ and τ' two equivalent sequences of states, then*

(a) $b \,|^{\sigma}_{U} = \textbf{true} \Leftrightarrow b \in D_0$, *where* $\sigma_i = \langle k_i, D_i \rangle$,

(b) $b \,|^{\tau}_{U} = b \,|^{\tau'}_{U}$.

Proof. The proof is very similar to the proof of Lemma 21, and therefore we shall only highlight the changes to be made.

$b = \bigcirc c$. (a) $\bigcirc c \,|^{\sigma}_{U} = \textbf{true} \Leftrightarrow c \,|^{\sigma^1}_{U} = \textbf{true}$. The sequence σ^1 is generic since σ is. Since σ is $\Omega(b)$-standard, σ^1 is $(\Omega(b) - 1)$-standard. But

$\Omega(b) - 1 = \Omega(c)$. Therefore, by the induction hypothesis: $c\,|_U^{\sigma^1} = \mathbf{true} \Leftrightarrow c \in D_1$. Since $\Omega(b) \geqslant 1$, the first transition of σ is a ρ-transition and $D_0 \rho D_1$. We conclude that $c \in D_1 \Leftrightarrow \bigcirc c \in D_0$.

$b = \Box c$. (a) Suppose $\Box c \in D_0$. Since σ is standard, we have , $\forall i \in \mathbb{N}$, $D_i \approx\rho D_{i+1}$. Therefore one can show, by induction on i, that $\forall i \in \mathbb{N}$, $\Box c \in D_i$. Our goal is to use the induction hypothesis on c. We notice that $\forall i \in \mathbb{N}$, σ^i is generic. Let i be given. In general σ^i is not $\Omega(c)$-standard. Let $m = \Omega(c)$. Now we have to distinguish between two cases following whether D_i is terminal or not. If D_i is not terminal, then $k_i = 0$ and we may essentially reason as in Lemma 21. More precisely, since σ is m-standard, there is an index j such that D_j is terminal and for all n such that $j + m \leqslant n$, we have $D_n \approx\rho D_{n+1}$ and for all n such that $0 \leqslant n < j + m$ we have $D_n \rho D_{n+1}$. If D_i is not terminal it must be that $i < j$. Therefore the sequence σ^i is m-standard and we may use the induction hypothesis part (a) to conclude: $c\,|_U^{\sigma^i} = \mathbf{true}$. On the other hand, suppose that D_i is terminal. By Lemma 12 (and this is the only time we use the full force of Axiom (A13)), we may find traces E_n, for $n = i,\ldots,j + m - 1$, such that $E_i \approx D_i$, for all n such that $i < n \leqslant j + m - 1$ we have $E_n \equiv D_n$ and for all n such that $i \leqslant n < j + m - 1$ we have $E_n \rho E_{n+1}$. Let the sequence τ be defined by: $\tau_n = \sigma_n$, $\forall n, j + m \leqslant n$ and $\tau_n = \langle 0, E_n \rangle$, $\forall n, n \leqslant j + m - 1$. By construction σ^i and τ are equivalent and therefore by the induction hypothesis (b) $c\,|_U^{\sigma^i} = c\,|_U^{\tau}$. But τ is a generic m-standard sequence and by the induction hypothesis (a) $c\,|_U^{\tau} = \mathbf{true} \Leftrightarrow c \in E_i$. To conclude, notice that $\Box c \in D_i \Rightarrow \Box c \in E_i$ since $D_i \approx E_i$. We conclude that $\Box c\,|_U^{\sigma} = \mathbf{true}$.

$\Box c \notin D_0$. Following the line of reasoning used in Lemma 21 one may see that $\exists i \in \mathbb{N}$ such that $c \notin D_i$. Now, as just above, we must distinguish two cases. If D_i is not terminal, σ^i must be m-standard and one may use the induction hypothesis part(a). If D_i is terminal, the proof is more delicate. If D_i is terminal and does not contain c, it must contain $\Box \neg \Box c$ (here we need $n' \geqslant n + 2$). We may then show that for all indexes j such that $j \geqslant i$, $\Box \neg \Box c \in D_j$. Therefore there is a terminal trace E that contains $\neg \Box c$ and appears an infinite number of times in σ. Since σ is generic, we conclude, using Lemma 18, that there is a terminal trace F that does not contain c and that appears an infinite number of times in σ. Since σ is generic, the trace F must appear in σ an infinite number of times followed by at least $\Omega(c)$ ρ-transitions. Let j be such a point in σ, with $j \geqslant i$. At j, we may apply the induction hypothesis part (a) and see that $c\,|_U^{\sigma^j} = \mathbf{false}$. We conclude that $\Box c\,|_U^{\sigma^i} = \mathbf{false}$.

$b = \nabla c$. (a) Suppose $\nabla c \in D_0$. We want to show that, for almost all sequences $\tau \in P_{\sigma_0}$, we have $c\,|_U^{\tau} = \mathbf{true}$. Since almost all sequences of P_{σ_0} are generic (by Lemma 20), and $\Omega(c)$-ultimately standard (by Lemma 22) it is enough to show that if τ is generic and $\Omega(c)$-ultimately standard, then

$c\,|^{\tau}_{U}=$ **true**. Let $m=\Omega(c)$. Since τ is m-ultimately standard it has an m-standard tail. Using Lemma 8 as we did in the corresponding part of Lemma 21, we may build a sequence τ' that is equivalent to τ, generic and m-standard. By the induction hypothesis, part (b), $c\,|^{\tau}_{U}=c\,|^{\tau'}_{U}$. We conclude by using the induction hypothesis, part (a).

Suppose now that $\neg\nabla c \in D_0$. We must find a set Q of sequences that begin at σ_0 and do not satisfy c, such that Q has a positive measure. Remember that $\sigma_0=\langle k_0, D_0\rangle$. We have to distinguish two cases, following whether k_0 is zero or positive. If $k_0=0$, we reason essentially as in the corresponding part of Lemma 21. By Lemma 6, there is a trace E such that $D_0 \equiv E$ and $c \notin E$. Let E' be any trace such that $E\rho E'$. Lemma 2 ensures the existence of such an E'. We have $D_0 \equiv\rho E'$, and by the definition of our model $p(\langle 0, D_0\rangle, \langle 0, E'\rangle)>0$. Let us define Q as the set of all sequences τ such that: $\tau_0=\sigma_0$, $\tau_1=\langle 0, E'\rangle$ and the sequence τ^1 is generic and $\Omega(c)$-standard. By Lemmas 20 and 22, we have $\tilde{p}_{\sigma_0}(Q)>0$. It is left to us to show that no sequence of Q satisfies c. Let τ be any sequence of Q. Let τ' be the sequence $\langle 0, E\rangle, \tau_1, \tau_2, \ldots$. It is a generic $\Omega(c)$-standard sequence. By the induction hypothesis, part (a) we have $c\,|^{\tau'}_{U}=$ **false**. But since $D_0 \equiv E$, $\tau \equiv \tau'$. We conclude, by the induction hypothesis, part (b), that $c\,|^{\tau}_{U}=$ **false**.

If $k_0>0$, we may not reason in the same way since the first move of the sequences of Q above may have probability zero (in the case D_0 does not stand in the relation $\approx\rho$ to E'). But notice that, in this case, we know that D_0 is terminal. By Lemma 6, there is a trace E such that $D_0 \equiv E$ and $c \notin E$. Let $m=\Omega(c)$. By Lemma 13, there are traces $E_0, \ldots, E_m$ and $F_0, \ldots, F_m$ such that $E_0=E$ and $F_0=D_0$, $E_i \equiv F_i$ for $0 \leqslant i \leqslant m$, $E_i \rho E_{i+1}$ for $0 \leqslant i < m$ and $F_i \approx\rho F_{i+1}$ for $0 \leqslant i < m$. Notice that the traces F_i are all terminal. Let Q be the set of all sequences τ such that: $\tau_i=\langle k_i, F_i\rangle$ $\forall i\, 0 \leqslant i \leqslant m$ and τ^m is generic and 0-standard. By construction and Lemmas 20 and 22, the set Q has a positive measure. It is left to us to show that no sequence of Q satisfies c. Let τ be a sequence of the set Q. Define the sequence τ' by: $\tau'_i=\tau_i$ for $m<i$ and $\tau'_i=\langle 0, E_i\rangle$ for $0 \leqslant i \leqslant m$. By construction $\tau \equiv \tau'$ and therefore, by the induction hypothesis part (b) $c\,|^{\tau}_{U}=c\,|^{\tau'}_{U}$. But the sequence τ' is generic since it has a generic tail. It is also m-standard since it consists of a prefix of m ρ-transitions and a 0-standard tail. By the induction hypothesis part (a) we conclude $c\,|^{\tau'}_{U}=$ **false**. Q.E.D.

The proof of completeness is completed as in the previous case.

11.9. *Completeness of* TCf

The model $U=\langle S, u, l, p\rangle$, that does not satisfy a, is defined the following way:

(1) $S=\mathscr{D}_n$.

(2) $u = D_a$.

(3) $l(D) = \{p \mid p \in D\}$.

(4) If D is not terminal, then we decide that $p(D, E) \neq 0$ iff $D \equiv \rho E$ and that all transitions of positive probability from D have equal probabilities. On the other hand, if D is terminal $p(D, E) \neq 0$ iff $D \approx \rho E$ and all transitions from D have equal probabilities.

Notice that if D is terminal and the transition $D \rightarrow E$ has a positive probability, then E is terminal.

If $D \rho E$ let us call the transition from D to E a ρ-transition. Let m be a natural number. Let σ be a sequence of states of U. If there exists an $n \in \mathbb{N}$ such that: σ_n is terminal, for all i such that $0 \leqslant i < n + m$, we have $\sigma_i \rho \sigma_{i+1}$ and for all i such that $n + m \leqslant i$, we have $\sigma_i \approx \rho \sigma_{i+1}$ we shall say that σ is an m-standard sequence. We define ultimately m-standard sequences as above.

We see, using Lemmas 9, 10, and 18, that the set of m-standard sequences beginning at a trace s has positive weight and that the set of ultimately m-standard sequences beginning at a trace s has weight 1.

DEFINITION 19. Two sequences of states τ and τ' are said to be equivalent ($\tau \equiv \tau'$) if $\forall i \in \mathbb{N}$, $\tau_i \equiv \tau'_i$.

DEFINITION 20. Let σ be a sequence of states of U, σ is said to be generic iff for any trace D_0 that appears an infinite number of times in σ and for any finite sequence of traces $D_0, D_1, ..., D_m$ such that $D_i \rho D_{i+1}$, for every i such that $0 \leqslant i < m$ the sequence above appears in σ (in this order) an infinite number of times.

The weight of generic sequences is one, i.e., for any state s, $\tilde{p}_s(\{\tau \mid \tau \in P_s, \tau$ generic$\}) = 1$.

Our goal is to show that in U, $\tilde{p}_u(\neg a) > 0$ and therefore the model U does not satisfy a. Our basic result concerning U is

LEMMA 24. *Let $b \in \Gamma_n$, σ an $\Omega(b)$-standard generic sequence of states (of U) and τ and τ' two equivalent sequences of states, then*

(a) $b \,|^{\sigma}_{U} = \mathbf{true} \Leftrightarrow b \in \sigma_0$,

(b) $b \,|^{\tau}_{U} = b \,|^{\tau'}_{U}$.

Proof. The proof is very similar to that of Lemma 23, and we signal only the differences.

$b = \nabla c$. (a) In the first half of the proof reason as in Lemma 23.

Suppose now that $\neg \nabla c \in D_0$. We must find a set Q of sequences that begin at σ_0 and do not satisfy c, such that Q has a positive measure. We have to distinguish two cases, following whether σ_0 is terminal or not. If σ_0 is not terminal then we use Lemma 6 to build a trace E such that $\sigma_0 \equiv E$ and $c \notin E$. If, on the contrary, σ_0 is terminal we use Lemma 15 to build a trace E such that $\sigma_0 \approx E$ and $c \notin E$. Let E' be any trace such that EpE'. Lemma 2 ensures the existence of such an E'. Notice that, by definition of our model, whether σ_0 is terminal or not, we have $p(\sigma_0, E') > 0$. Let us define Q as the set of all sequences τ such that: $\tau_0 = \sigma_0$, $\tau_1 = E'$ and the sequence τ^1 is generic and $\Omega(c)$-standard. We have $\tilde{p}_{\sigma_0}(Q) > 0$. It is left to us to show that no sequence of Q satisfies c. Let τ be any sequence of Q. Let τ' be the sequence E, τ_1, τ_2,.... It is a generic $\Omega(c)$-standard sequence. By the induction hypothesis, part (a) we have $c\,|_U^{\tau'} =$ **false**. But since $\sigma_0 \equiv E$, $\tau \equiv \tau'$. We conclude, by the induction hypothesis, part (b), that $c\,|_U^{\tau} =$ **false**. Q.E.D.

We may now conclude the proof of completeness, as in the previous cases.

12. Alternative Systems for Unbelievers

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

Definition 21. Let U be a g-model and $a \in \Gamma$ a formula. We say that U satisfies a and write $U \models a$, iff for any $\tau \in P_u$, $a\,|_U^{\tau} =$ **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 Chellas, 1980). More specifically, one notices that rules (R0)–(R2) are still sound and that, except (A10), (A12)–(A14), all axioms are still valid. Therefore we keep rules (R0)–(R2) and Axioms (A0)–(A9) and (A11). For the other axioms, we just prefix them by $\nabla\Box$. Instead of (A10) use

(A10′) $\nabla\Box[\Box a \rightarrow a]$.

Instead of (A12), use

(A12′) $\nabla\Box[\nabla\bigcirc a \rightarrow \bigcirc\nabla a]$.

Instead of (A13) and (A14), use

(A13′) $\nabla\Box[\text{A13}]$.

(A14′) $\nabla\Box[\text{A14}]$.

13. Some Theorems for Unbelievers

We shall now list, with minimal justification, some theorems of the system consisting of Axioms (A0)–(A9), (A10′), (A11), (A12′) and rules (R0)–(R2). We omit writing the deducibility symbol.

$$\neg\nabla\mathbf{false}. \tag{T8}$$

Proof. $\mathbf{true} \Rightarrow \nabla\mathbf{true} \Rightarrow \triangle\nabla\mathbf{true}$, by $(A9) \Rightarrow \neg\nabla\triangle\mathbf{false}$. But $\mathbf{false} \to \triangle\mathbf{false} \Rightarrow \nabla\mathbf{false} \to \nabla\triangle\mathbf{false} \Rightarrow$ whose contrapositive is $\neg\nabla\triangle\mathbf{false} \to \neg\nabla\mathbf{false}$.

$$\nabla a \to \triangle a. \tag{T9}$$

The proof goes the following way: $\neg\nabla\mathbf{false} \Leftrightarrow \neg\nabla(a \wedge \neg a) \Leftrightarrow \neg(\nabla a \wedge \nabla\neg a) \Leftrightarrow \neg\nabla a \vee \neg\nabla\neg a \Rightarrow \nabla a \to \triangle a$.

$$\nabla a \leftrightarrow \nabla\nabla a. \tag{T10}$$

The implication from right to left follows easily from (A.10′). The implication from left to right is proved as in (T2).

$$\nabla[\triangle a \vee b] \leftrightarrow \triangle a \vee \nabla b, \tag{T11}$$

$$\nabla\Box\nabla a \to \nabla\Box a. \tag{T12}$$

Follows from (A10′).

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 $\nabla a \in T$ iff $\nabla a \in T'$.

14. Linear Time versus Branching Time

One may remark that our language is also suitable for interpretation in nonprobabilistic 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 Ben-Ari *et al.* (1981) and Emerson and Halpern (1982). If one takes the natural definition of satisfiability 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 $p \wedge \nabla\Box\triangle\bigcirc p \to \triangle\Box p$ is valid for our new nonprobabilistic interpretation, but is not valid in our probabilistic interpretation. To find the additional axioms needed to obtain a complete axiomatization of this nonprobabilistic interpretation is an open problem.

Another nonprobabilistic 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.

15. 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 $S\omega S$ and the results of Rabin (1969). 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 Sisla and Clarke (1982) that satisfiability is Pspace-hard. Our conjecture is that the three systems above are in Pspace.

Note added in proof. S. Kraus and D. Lehmann have shown that all three systems require exponential time and may be decided in nondeterministic exponential time.

Acknowledgments

Amir Pnueli is not only responsible for having pioneered the use of temporal logic in proofs of correctness, he also took a deep interest in many previous versions of the system presented here. His help is gratefully acknowledged. Remarks from David Harel, Rivkah Sherman, and Sergiu Hart on a first draft were also useful. A very detailed, accurate, and thoughtful referee report of Yishai Feldman contributed to the final version.

References

Ben-Ari, M., Manna, Z., and Pnueli, A. (1981), The temporal logic of branching time, in "Conf. Record, 8th Annual ACM Symposium on Principles of Programming Languages," Williamsburg, Va., pp. 164–176, January.

Clarke, E. M., and Emerson, E. A. (1982), Design and synthesis of synchronization skeletons using branching time temporal logic, in "Proceedings, Workshop on Logics of Programs" (Kozen, Ed.), Lecture Notes in Computer Science **131**, pp. 52–71, Springer–Verlag, Berlin.

Chellas, B. F. (1980), "Modal Logic: An Introduction," Cambridge Univ. Press, Cambridge, 1980.

COHEN, S., LEHMANN, D., AND PNUELI, A. (1983), Symmetric and economical solutions to the mutual exclusion problem in a distributed system, *in* "Proceedings, 10th International Colloquium on Automata, Languages and Programming," Barcelona, Spain, July.

EMERSON, E. A., AND HALPERN, J. Y. (1982), Decision procedures and expressiveness in the temporal logic of branching time, *in* "Conf. Record, 14th Annual ACM Symposium on Theory of Computing," San Francisco, Calif., pp. 169–179, May.

FELDMAN, Y. A., AND HAREL, D. (1982), A probabilistic dynamic logic, in "Conf. Record, 14th Annual ACM Symposium on Theory of Computing," San Francisco, Calif., pp. 181–195, May; Tech. Report CS82-07, Dept. of Applied Mathematics, the Weizmann Institute of Science.

GABBAY, D., PNUELI, A., SHELAH, S., AND STAVI, J. (1980), On the temporal analysis of fairness, *in* "Conf. Record, 7th Annual ACM Symposium on Principles of Programming Languages," Las Vegas, Nev., pp. 163–173, January.

HUGHES, G. E., AND CRESSWELL, M. J., (1972), "An Introduction to Modal Logic," Methuen, London.

HALPERN, J. Y., AND RABIN, M. O. (1983), A logic to reason about likelihood, *in* "Proceedings, 15thAnnual ACM Symposium on Theory of Computing," April.

HART, S., SHARIR, M., AND PNUELI, A. (1982), Termination of probabilistic concurrent programs, *in* "Conf. Record, 9th Annual ACM Symposium on Principles of Programming Languages," Albuquerque, N. M., pp. 1–6.

KOZEN, D. (1981), Semantics of probabilistic programs, *J. Comput. System Sci.* **22**, 328–350.

KEMENY, J. G., SHELL, J. L., AND KNAPP, A. W. (1966), "Denumerable Markov Chains," Van Nostrand, Princeton, N.J.

LAMPORT, L. (1980), "Sometimes" is sometimes "not never," *in* "Conf. Record, 7th Annual ACM Symposium on Principles of Programming Languages," Las Vegas, Nev., pp. 174–183, January.

LEHMANN, D. (1982), On primality tests, *SIAM J. Comput.* **11**, 374–375.

LEHMANN, D., PNUELI, A., AND STAVI, J. (1981), Impartiality, Justice, and Fairness: The ethics of concurrent termination, *in* "Proceedings, 8th International Colloquium on Automata, Languages, and Programming," Acco, Israel, pp. 264–277, July.

LEHMANN, D., AND RABIN, M. O. (1981), On the advantages of free choice: A symmetric and fully distributed solution to the dining philosophers problem (extended abstract), *in* "Conf. Record, Annual ACM Symposium on Principles of Programming Languages," Williamsburg, Va, pp. 133–138, January.

MAKOWSKI, J. A., AND TIOMKIN, M. (1982), A probabilistic propositional dynamic logic (extended abstract), manuscript.

PNUELI, A. (1981), The temporal semantics of concurrent programs, *Theoret. Comput. Sci.* **13**, 45–60.

RABIN, M. O. (1969), Decidability of second order theories and automata on infinite trees, *Trans. Amer. Math. Soc.* **141**, 1–35.

RABIN, M. O. (1976), Probabilistic algorithms, *in* "Algorithms and Complexity, New Directions and Recent Results" (J. F. Traub, Ed.), Academic Press, N.Y.

RABIN, M. O. (1982), N-process mutual exclusion with bounded waiting by $4 \log N$-valued shared variable. *J. Comput. System Sci.* **25**, 66–75.

RABIN, M. O. (1982), The choice coordination problem, *Acta Inform.* **17**, 121–134.

REIF, J. H. (1980), Logics for probabilistic programming, *in* "Proceedings, 12th ACM Symposium on Theory of Computing," Los Angeles, Calif., pp. 8–13, April.

SISLA, A. P., AND CLARKE, E. M. (1982), The complexity of propositional linear temporal logics, *in* "Proceedings, 14th Annual ACM Symposium on Theory of Computing," San Francisco, Calif., pp. 159–168, May.

SOLOVAY, R., AND STRASSEN V. (1977), A fast Monte Carlo test for primality, *SIAM J. Comput.* **6**, 84–85; Erratum, **7** (1978), 118.