Reprinted from INFORMATION AND CONTROL
All Rights Reserved by Academic Press, New York and London

Vol. 70, No. 2/3, August/September 1986
Printed in Belgium

Probabilistic Propositional Temporal Logics*

SERGIU HART AND MICHA SHARIR†

School of Mathematical Sciences, Tel Aviv University,
Tel Aviv 69978, Israel

We present two (closely-related) propositional probabilistic temporal logics based on temporal logics of branching time as introduced by Ben-Ari, Pnueli, and Manna (*Acta Inform.* **20** (1983), 207–226), Emerson and Halpern ("Proceedings, 14th ACM Sympos. Theory of Comput.," 1982, pp. 169–179, and Emerson and Clarke (*Sci. Comput. Program.* **2** (1982), 241–266). The first logic, PTL_f, is interpreted over finite models, while the second logic, PTL_b, which is an extension of the first one, is interpreted over infinite models with transition probabilities bounded away from 0. The logic PTL_f allows us to reason about finite-state sequential probabilistic programs, and the logic PTL_b allows us to reason about (finite-state) concurrent probabilistic programs, without any explicit reference to the actual values of their state-transition probabilities. A generalization of the tableau method yields deterministic single-exponential time decision procedures for our logics, and complete axiomatizations of them are given. Several meta-results, including the absence of a finite-model property for PTL_b, and the connection between satisfiable formulae of PTL_b and finite state concurrent probabilistic programs, are also discussed.

1. INTRODUCTION

Recent progress in the theory of probabilistic programs (Sharir, Pnueli, and Hart, 1984; Hart, Sharir, and Pnueli, 1983; Hart and Sharir, 1985) has yielded relatively simple methods for verification of certain properties of such programs. Sequential probabilistic programs have been represented in Sharir, Pnueli, and Hart (1984) as discrete Markov chains, whereas concurrent probabilistic programs have been represented in Hart, Sharir, and Pnueli (1983) and Hart and Sharir (1985) as processes involving cooperation of several Markov chains (with a common state space) obeying certain "fairness" constraints. In both cases, if one assumes that the state space of the programs in question is finite, then one can obtain simple

* A preliminary version of this paper has appeared in "Proceedings 16th Sympos. on Theory of Computing," 1984, pp. 1–13.

(†) Work by the second author has been partly supported by a grant from the Bat-Sheva Fund.

0019-9958/86 $3.00

algorithmic techniques for analyzing and proving *termination* of such programs. For sequential programs these techniques are essentially classical results in Markov chain theory, whereas for concurrent programs new techniques had to be developed. In both cases, the actual values of the state-transition probabilities proved to be irrelevant for the properties in question.

These encouraging results have motivated the study of logics for probabilistic programs, as presented in this paper. These logics allow us to express various properties of such programs, including invariant and liveness properties, without explicit reference to the values of the transition probabilities. The first logic, which we call PTL_f, is intended for reasoning about sequential programs, whereas the second logic, called PTL_b, extends the first one and is intended for reasoning about concurrent programs. Both logics are based (at least syntactically) on existing temporal logics for branching time (Ben-Ari, Pnueli, and Manna 1983; Emerson and Halpern, 1982; Emerson and Clarke, 1982). These logics are interpreted over models which can simulate the execution of probabilistic programs; for PTL_f these are essentially finite Markov chains, whereas for PTL_b they are infinite stochastic processes whose state-transition probabilities are bounded away from 0 (this assumption holds for finite-state concurrent probabilistic programs since there are only finitely many different state-transitions).

It turns out that satisfiability of formulae in both logics is decidable, in one-exponential time, by decision procedures based on the tableau technique which generalize similar procedures for the nonprobabilistic logics of Ben-Ari, Pnueli and Manna (1983) and Emerson and Clarke (1982). The probabilistic context of our logics makes these procedures more complicated than their nonprobabilistic counterparts, and introduces into them some special techniques which are variants of the techniques used in Hart, Sharir, and Pnueli (1983) for analyzing termination of concurrent probabilistic programs.

Together with these decision procedures, we also provide complete axiomatizations for both logics, and show that the same decision procedures can be used to construct a proof of the negation of any unsatisfiable formula.

Moreover, by inspection of the decision procedure for PTL_b, we see that for many (satisfiable) formulae of that logic the model constructed by that procedure can be replaced by a finite model. This establishes a connection between satisfiability of a formula in PTL_b and its satisfiability in PTL_f, when certain conditions hold. Some additional properties of the models of formulae in these logics are also discussed.

Several additional probabilistic logics have been proposed by Lehmann and Shelach (1982), Pnueli (1983), Feldman (1983), Feldman and Harel (1982), and Kozen (1983), in order to reason about probabilistic programs.

Of these logics, the last three logics are extended dynamic logics, rather than temporal ones, and moreover make explicit reference to the actual values of the transition probabilities involved. The logic in Pnueli (1983) is incomplete, and its semantic interpretation leads to a rather complicated probabilistic analysis.

The logics TC_f and TC_b of Lehman and Shelah (1982), developed about the same time as ours, are the closest in spirit to our logics. The semantic interpretation of PTL_f is very similar to that of TC_f, whereas the semantic interpretation of PTL_b is similar to that of TC_b. The difference between these logics is that the logics TC have richer syntax allowing arbitrary linear temporal formula to follow the path quantifiers, rather than just a single linear temporal operator as in our logics. As a consequence, the logics in Lehmann and Shelach (1982), although also decidable, have less efficient decision procedures. (This is analogous to the difference between the more restricted non-probabilistic branching-time logic CTL of Emerson and Halpern (1982) and the more general logic CTL^* of Emerson and Halpern (1983).) See also related work by Kraus (1985) and by Kraus and Lehmenn (1983).

The paper is organized as follows. In Section 2 we define the syntax and semantics of our logics, and make a few basic observations concerning these notions. In Section 3 we give axiomatic systems for both logics, and prove a few theorems which are needed later on. Section 4 describes the decision procedures for our logics, and shows how to construct a model for a satisfiable formula in either logic. Section 5 proves the completeness of the systems of both logics, in the sense that the proof of any formula p for which $\sim p$ is unsatisfiable, can be mechanically obtained from the tableau constructed for $\sim p$. Section 6 discusses some meta-results concerning properties of formulae and their models.

The decision procedures for PTL_b and PTL_f have been programmed in SETL and have been tested on several formulae. Appendix A gives a few examples of the output of this procedure.

2. Syntax and Semantics

In this section we introduce our two logic systems, denoted PTL_f and PTL_b, which are almost identical syntactically, but differ in the interpretation of their formulae. Formally, (an austere version of) the syntax of our logics is defined as follows.

Definition. Syntactically valid formulas in the logics PTL_f and PTL_b are defined recursively as follows:

(1) Every formula in the propositional calculus is a formula in these logics.

(2) If p and q are formulas in PTL_f or PTL_b then so are $\sim p$, $p \vee q$, $\forall \mathbf{X}p$, $\forall \mathbf{F}p$, and $p \; \forall \mathbf{U} q$.

As will shortly be seen, the operator $\forall \mathbf{F}$ in PTL_f is redundant, and can be defined in terms of the other two operators. These logics can be augmented by additional operators as will be detailed below.

PTL_f and PTL_b are interpreted as follows. A model of PTL_b is a (discrete) Markov chain, possibly having infinitely many states, for which there exists $\alpha > 0$ such that all nonzero transition probabilities of the chain are $\geqslant \alpha$. A specified initial state is associated with the model; in addition, there is an assignment of truth values to all propositions appearing in a given formula at each state of the chain. Formally,

DEFINITION. A model M of PTL_b is a quadruple (S, P, s_0, ρ), where S is a set of states, $s_0 \in S$ is the initial state, P is a transition probability matrix (i.e., a nonnegative mapping on $S \times S$ with $\sum_{t \in S} P(s, t) = 1$ for each $s \in S$) each of whose entries is either 0 or $\geqslant \alpha$, where α is some positive constant, and ρ is a mapping on S assigning to each $s \in S$ the set of true propositions at that state. For convenience, we abbreviate $p \in \rho(s)$ as $p \in s$.

A model of PTL_f is defined similarly, with the additional requirement that the set S be *finite* (the requirement of the boundedness of the transition probabilities clearly holds here).

Each model M induces in a standard manner a probability measure μ_M on the space Ω_M of all infinite paths $\omega = (s_n)_{n=0}^{\infty}$ in S starting at s_0. The measure μ_M is defined on the σ-field generated by the cylindrical sets of the form

$$\Omega(s_0, \ldots, s_n) \equiv \{\omega \in \Omega_M \mid \omega_i = s_i, \; i = 0, \ldots, n\}$$

and the μ_M-measure of each such set is the product

$$P(s_0, s_1) \cdot P(s_1, s_2) \cdot \cdots \cdot P(s_{n-1}, s_n)$$

of the transition probabilities along the edges of the common initial prefix $(s_0, \ldots, s_n)$ of all paths in this set.

Truth of a formula p of either logic, in an appropriate model M, denoted $\models_M p$, is defined inductively as follows:

(i) If p is a proposition, then $\models_M p \Leftrightarrow p \in s_0$.

(ii) If $q = \sim p$, then $\models_M q \Leftrightarrow \not\models_M p$.

(iii) If $r = p \vee q$, then $\models_M r \Leftrightarrow \models_M p$ or $\models_M q$, and similarly for all other logical connectives.

(iv) If $q = \forall \mathbf{X} p$, then $\models_M q \Leftrightarrow \models_{M_1} p$ for all $s_1 \in S$ such that $P(s_0, s_1) > 0$, where M_1 is the model M with initial state s_1, instead of s_0.

(v) If $r = p \, \forall \mathbf{U} q$, then $\models_M r \Leftrightarrow \mu_M(A_{p,q}) = 1$, where

$$A_{p,q} = \{\omega = (s_n) \in \Omega_M \mid \inf\{n \mid \not\models_{M_n} p\} \geqslant \inf\{n \mid \models_{M_n} q\}\}$$

and M_n is the model M with initial state s_n. I.e., $A_{p,q}$ consists of paths along which either p always holds, or else p holds until the first time q holds.

(vi) If $q = \forall \mathbf{F} p$, then $\models_M q$ iff the set of paths starting at s_0 along which p eventually holds is of measure 1. Following standard terminology in probability theory, this is equivalent to the existence of a stopping time N on Ω_M which is μ_M-almost surely finite, such that $\models_{M_N} p$ for each ω with $N(\omega) < \infty$. (A stopping time is a function N defined on Ω_M whose values are either nonnegative integers or $+\infty$, having the property that whenever $N(\omega) = n$ then $N(\omega') = n$ for each path ω' having the same first n states as ω.)

We now discuss some important features of our logics:

(1) Using negations of the modal operators $\forall \mathbf{X}$, $\forall \mathbf{U}$, and $\forall \mathbf{F}$, we define additional operators as follows:

$$\exists \mathbf{X} p \equiv \sim (\forall \mathbf{X} \sim p)$$

$$p \exists \mathbf{U} q \equiv \sim ((\sim q) \, \forall \mathbf{U} (\sim p))$$

$$\exists \mathbf{G} p \equiv \sim \forall \mathbf{F} \sim p.$$

Note that $\forall \mathbf{U}$ and the $\exists \mathbf{U}$ operators describe different notions of the "until" operator. In $p \, \forall \mathbf{U} q$, $\mathbf{U}$ denotes the "weak" until (in which p holds either indefinitely or until q becomes true, but q need not ever become true), whereas in $p \, \exists \mathbf{U} q$, $\mathbf{U}$ denotes (a variant of) the "strong" until (in which p holds until q becomes true, including the state at which q is true, and q does indeed become true). The reader should keep this difference in mind in what follows.

(2) Intuitively, $\models_M \forall \mathbf{X} p$ means that p holds at all immediate successors (sons) of the initial state of M. Similarly, $\models_M \exists \mathbf{X} p$ means that p is valid in at least one son of the initial state of M. $\models_M p \, \forall \mathbf{U} q$ means that along all paths ω starting at s_0 and consisting only of transitions with non-zero probability, p holds at all states of ω up to the first state, if any, at which q holds. Note that "p until q for all paths" is equivalent to "p until q for *almost* all paths:" Indeed, "p until q" not being satisfied on some path means that the first time p is not true q is not true also; this is therefore a property of *finite* paths; if it happens at all, its probability must therefore be positive. Similarly, $\models_M p \exists \mathbf{U} q$ if there exists a *finite* path ω of states

reachable from s_0 via transitions having nonzero probabilities, such that p holds at all states of ω, and q holds at the final state of ω. These observations imply that the $\forall\mathbf{U}$ and $\exists\mathbf{U}$ operators are actually nonprobabilistic, a property that we will use later in discussing PTL_f. Also, $\models_M \forall\mathbf{F}p$ if p eventually holds on μ_M-almost every path. In the same manner, $\models_M \exists\mathbf{G}p$ if the μ_M-measure of the set of paths along which p always holds (i.e., the set $A_{p,\text{false}}$), is positive.

(3) The modal operators $\forall\mathbf{G}p$ and $\exists\mathbf{F}p$ of Ben-Ari, Pnueli, and Manna (1983) can be defined in both logics PTL_f and PTL_b in the following usual way:

$$\exists\mathbf{F}p \equiv \mathbf{true}\ \exists\mathbf{U}p$$

$$\forall\mathbf{G}p \equiv p\ \forall\mathbf{U}\ \mathbf{false}.$$

$\models_M \exists\mathbf{F}p$ if p holds on at least one state of the model, and $\models_M \forall\mathbf{G}p$ if p holds at all states of the model.

(4) In PTL_f, the operator $\forall\mathbf{F}$ and its dual $\exists\mathbf{G}$ can be defined in terms of the other operators, as follows:

$$\exists\mathbf{G}p \equiv p\ \exists\mathbf{U}(\forall\mathbf{G}p) \equiv p\ \exists\mathbf{U}(p\forall\mathbf{U}\ \mathbf{false})$$

$$\forall\mathbf{F}p \equiv (\exists\mathbf{F}p)\ \forall\mathbf{U}p \equiv (\mathbf{true}\ \exists\mathbf{U}p)\ \forall\mathbf{U}p.$$

These two definitions are quite nonobvious, and are special to the finite model interpretation of PTL_f. $\models_M \forall\mathbf{F}p$ if on μ_M-almost every path p holds eventually. However, in the case of finite models (i.e., finite Markov chains), this is equivalent to requiring that on every path ω and every state s_n along ω before the first time (if any) p holds on ω, there exists a path from s_n on which p eventually holds. This latter property is always implied by the interpretation of $\models_M \forall\mathbf{F}p$ as defined above (including infinite Markov chains); the reverse implication can be proved for *finite* Markov chains using standard "0–1 law" arguments, similar to those in Hart, Sharir, and Pnueli (1983) (e.g., see Theorem 2.2 there). (Such a 0–1 law states that, in a finite Markov chain, if there is a positive probability of eventually reaching a certain set of states from every state in the chain, then this probability is 1 for all starting states.) The definition of $\exists\mathbf{G}p$ follows by negation. However, this will not work for PTL_b: as is well known, in a denumerable Markov chain, even if every state has an eventual successor where p holds, p need not occur eventually almost surely (since this successor may be reached only after arbitrarily many steps, its probability may be arbitrarily small—even if all positive single-step transition probabilities in the chain are bounded away from zero).

After reducing formulas in PTL_f as above, we obtain equivalent formulas which are expressed using only the operators $\forall\mathbf{X}$, $\exists\mathbf{X}$, $\forall\mathbf{U}$, and $\exists\mathbf{U}$. Let p be

such a reduced formula, and let M be a model of PTL_f. It is plain that the same model, viewed as a *non-deterministic* structure M' (i.e., where state transitions denote non-deterministic, rather than probabilistic, choices), is also a model of, say, CTL, and vice versa, each model of CTL can also be regarded as a probabilistic model for PTL_f, by assigning appropriate probabilities to its state transtitions. Moreover, since each of the operators $\forall\mathbf{X}$, $\exists\mathbf{X}$, $\forall\mathbf{U}$, and $\exists\mathbf{U}$ is nonprobabilistic, it can be easily shown, by induction on the structure of (the reduced) p, that p is satisfiable by a model M of PTL_f if and only if p is also satisfiable, as a formula of CTL, by the corresponding non-deterministic structure M'. These observations will be used in the following section to show that PTL_f is decidable and has complete axiomatization, using similar properties of CTL.

(5) Consider a finite-state probabilistic *sequential* program; its execution history can clearly be modelled in PTL_f (such that the model states become program states, and the propositions contained in each such state are considered as properties holding at that program state).

(6) In contrast, consider a finite-state probabilistic *concurrent* program, with finitely many processes (we will refer to such a program in short as a *finite* probabilistic concurrent program); it turns out that to model its execution requires the use of PTL_b. Indeed, as in Hart, Sharir, and Pnueli (1983), such a finite concurrent program is specified in terms of a finite common state space I and a finite collection K of processes, such that at each state $i \in I$, if the next process to execute an atomic step is some $k \in K$, then the program will reach after execution of that step a state $j \in I$ with probability P_{ij}^k (thus, in particular, $\sum_{j \in I} P_{ij}^k = 1$).

Note that we cannot model such a concurrent probabilistic program in PTL_b, because at any given program state i, the choice of the next process k to execute an atomic step is nondeterministic and cannot be determined from the program description as specified above; at different points in the execution of the program, different choices may be made.

However, we can model any specific *execution* of such a program in PTL_b. It is specified in terms of a *schedule* σ which determines at each execution step the process $k \in K$ to execute the next step. We assume (as in Hart, Sharir, and Pnueli, 1983) that σ's decision is a function of the entire execution history, i.e., the sequence of states $(i_0, i_1, \ldots, i_m)$ reached during execution, where i_m is the present program state. This execution can be modeled in PTL_b by a model M defined as follows. The states of M are all finite execution histories as defined above. For each such history $h = (i_0, i_1, \ldots, i_m)$, let $k = \sigma(h)$ be the next process to execute; then M contains transitions from h to all histories of the form $h \| (i_{m+1})$ such that $P_{i_m i_{m+1}}^k > 0$, and the probability of that transition in M is the same $P_{i_m i_{m+1}}^k$. The starting state h_0 of M is the singleton history (i_0), where $i_0 \in I$ is the

initial program state. Finally, each state h in M may contain propositions which reflect properties of the last program state in h, or which describe the last process scheduled along h, etc. Since our program has only finitely many positive transition probabilities, it is clear that all transition probabilities in M are bounded away from zero.

We will say that the program execution as determined by the schedule σ satisfies a formula p of PTL_b (whose atomic subformulae consist of propositions describing properties of individual program states or of the processes about to be scheduled), if the corresponding model M as defined above satisfies p. Intuitively this is an appropriate definition because M is defined so as to model all possible (infinite) execution sequences of the program under σ. Indeed, these execution sequences are precisely the infinite paths in M, and the probability measure μ_M as defined above is precisely the probability distribution induced on the space of all program execution paths by σ and by the individual program transition probabilities. (In other words, the μ_M-measure of any cylinder $\Omega(i_0,..., i_m)$ is the probability that the first $m+1$ program states reached during program execution under σ will be $i_0,..., i_m$.)

As an illustration, consider the following type of formula p of PTL_b which specifies the structure of some (finite-state) concurrent probabilistic program and also asserts that during execution of this program a certain property t will hold eventually almost surely.

$$\begin{aligned}
&(at_s_1 \wedge activ_k_1 \supset \exists \mathbf{X} at_s_1') \forall \mathbf{U}\ \mathbf{false} \wedge \cdots \\
&\wedge (at_s_m \wedge activ_k_m \supset \exists \mathbf{X} at_s_m') \forall \mathbf{U}\ \mathbf{false} \\
&\wedge (\forall \mathbf{F} activ_k_1) \forall \mathbf{U}\ \mathbf{false} \wedge \cdots \wedge (\forall \mathbf{F} activ_k_r) \forall \mathbf{U}\ \mathbf{false} \\
&\wedge at_s_0 \supset \forall \mathbf{F} t;
\end{aligned} \tag{2.1}$$

here the first group of conjuncts describe the state-transitions of the program, the second group of conjuncts specify that the program execution must be fair, and the last line asserts that if execution starts at s_0 then t will hold eventually almost surely. Note that any execution of the program starting at s_0 for which t holds eventually almost surely corresponds to a model of PTL_b which satisfies p. Conversely, the results of Section 4 and the subsequent discussion in Section 6 imply that if p is satisfiable by some model of PTL_b then it is also satisfiable by a model that corresponds to some specific execution of the underlying concurrent probabilistic program.

Finally, note that the execution of a finite state concurrent program (involving more than one process) in general cannot be modeled by a *finite* Markov chain (and thus by a model of PTL_f). For example, suppose that the program consists of three states s_1, s_2, and s_3, and of two processes k_1, k_2, such that under k_1 the transitions having nonzero probability are

(s_1, s_1), (s_1, s_2), (s_2, s_1), (s_2, s_2), (s_3, s_3), and under k_2 they are (s_1, s_3), (s_2, s_3), (s_3, s_3). Consider the schedule σ starting at s_1 and defined by the rule: Schedule k_1 repeatedly until the first time at which the number of visits at s_2 is equal to the number of visits at s_1; in this case schedule k_2, and thereafter schedule k_1 and k_2 alternately. The execution of this program under σ cannot be modeled by a finite-state Markov chain; in fact this execution is identical to the behavior of a random walk on 0, 1, 2,..., with absorption at 0. Moreover, the fairness of σ *does* depend on the transition probabilities of k_1 at s_1 and s_2 (e.g., σ is fair if $P^{k_1}_{s_1,s_2}$, $P^{k_1}_{s_2,s_2} \geqslant \frac{1}{2}$, and is unfair if both these probabilities are $< \frac{1}{2}$.)

The problem with this σ is that it is not *finitary*. Roughly speaking, a schedule is finitary if it is a finite automaton acting on the execution history, whose scheduling decisions depend on its current state. That is, there exists a finite partition A of the set of all finite histories (i.e., each finite history belongs to exactly one element of A) such that, if h and h' belong to the same element of A, then (i) $\sigma(h) = \sigma(h')$; and (ii) for any next state i, $h\|i$ and $h'\|i$ belong to the same element of A. It is easily seen that for finite-state concurrent programs, their execution under a schedule σ can be modeled by a finite-state Markov chain if and only if σ is finitary.

Fair schedules need not be finitary. However, it can be shown from Theorem 2.1 of Hart, Sharir, and Pnueli (1983) that almost-sure termination by any fair schedule can be effectively decided by essentially considering only finitary (fair) schedules, and therefore is a property that can be stated and verified in PTL_f. This interplay between PTL_b and PTL_f will be studied in more generality in Section 6. We will obtain there the property just noted as a special case of a more general rule, which gives sufficient conditions for formulae of PTL_b to be equivalently represented (and checked) in PTL_f. In particular, we will show that if formulae such as p in (2.1) are satisfiable by a model corresponding to some execution of the concurrent program, then p is also satisfied by a similar execution under a finitary schedule.

3. Axiomatic Systems

We next present sound and complete deductive systems for PTL_f and PTL_b which are similar to the systems for *UB* of Ben-Ari, Pnueli, and Manna (1983) and *CTL* of Emerson and Halpern (1982).

Axioms and Rules Common to Both Logics

Axioms.

(A0) *Axioms of the propositional calculus*

(A1) $\forall \mathbf{X}(p \supset q) \supset (\forall \mathbf{X} p \supset \forall \mathbf{X} q)$

(A2) $p \forall \mathbf{U} q \supset q \vee (p \wedge \forall \mathbf{X}(p \forall \mathbf{U} q))$.

INFERENCE RULES.

(R0) *Modus ponens; propositional reasoning*

(R1) $\vdash p \Rightarrow \vdash \forall \mathbf{X} p$

(R2) $\vdash r \supset q \vee (p \wedge \forall \mathbf{X} r) \Rightarrow \vdash r \supset p \forall \mathbf{U} q$

(R3) $\vdash p \Rightarrow \vdash \sim (\forall \mathbf{F} \sim p)$.

Additional Axioms for PTL_f

(A3) $\forall \mathbf{F} p \equiv (\mathbf{true}\ \exists \mathbf{U} p)\ \forall \mathbf{U} p$.

Additional Axioms and Rules for PTL_b

(A4) $\forall \mathbf{F} p \equiv p \vee \forall \mathbf{X} \forall \mathbf{F} p$

(A5) $\forall \mathbf{F} \forall \mathbf{F} p \supset \forall \mathbf{F} p$

(A6) $(p \forall \mathbf{U} q) \wedge \forall \mathbf{F}(\sim p) \supset \forall \mathbf{F} q$

(R4) $\vdash r \supset p \vee (\forall \mathbf{X} \forall \mathbf{F} r \wedge \exists \mathbf{X} p) \Rightarrow \vdash r \supset \forall \mathbf{F} p$.

We now justify the soundness of our axioms and rules. Axioms (A1) and (A2) and rules (R1) and (R2) are nonprobabilistic and are sound in our interpretations, as well as in the interpretations of the nonprobabilistic logic *CTL*. (It has been pointed out by Pnueli that these axioms and rules can be used to simplify existing axiomatizations for that logic.) The axiom (A1) and the rule (R1) are taken from Ben-Ari, Pnueli, and Manna (1983), and their soundness follows from the definition of $\forall \mathbf{X}$, as in Ben-Ari, Pnueli, and Manna (1983). Axiom (A2) states that $r = p \forall \mathbf{U} q$ satisfies the implication $r \supset q \vee (p \wedge \forall \mathbf{X} r)$, which again is obvious from the definitions of the operators $\forall \mathbf{U}$ and $\forall \mathbf{X}$; whereas rule (R2) states that $p \forall \mathbf{U} q$ is the "largest" solution to that implication, in the sense that it is implied by any other solution. The soundness of this rule can be proved by a simple inductive argument.

The soundness of the rule (R3) is also easy to establish from the definitions. As noted in (4) in the preceding section, axiom (A3) is sound under finite-model interpretations.

The soundness of axioms (A4)–(A6), in our interpretation of PTL_b, follows from probabilistic arguments (which apply also in the general unbounded case). Moreover, they are also sound for non-probabilistic logics, such as *CTL* or *UB* (under their standard non-probabilistic interpretation). Specifically, (A4) states that an event p happens eventually almost surely if and only if it either happens now, or else it happens eventually almost surely from any next instance on. Axiom (A5) states that if

there exists an almost surely finite stopping time N such that for each path ω with $N=N(\omega)<\infty$, the event p will happen eventually almost surely after reaching ω_N, then p will happen eventually almost surely. (In other words, the composition of a family of almost-surely finite stopping times on an almost-surely finite stopping time yields an almost-surely finite stopping time.) Axiom (A6) states that if p holds continuously until the first time (if any) at which q holds, and if there exists an almost surely finite stopping time N at which p does not hold, then there exists another almost surely finite stopping time $N' \leqslant N$ which q holds. The soundness of this axiom is immediate from the definitions.

Finally, the rule (R4) states that for r to imply that p will eventually hold (almost surely), it is sufficient to require that r implies that either p holds now, or that at least one succeeding state satisfies p, and at the same time r will hold once more eventually a.s. after every succeeding state. To prove the soundness of this rule, we argue as follows. Let S_0 denote the set of all states s in S at which r holds, and which are reachable from the initial state s_0 via paths along which p did not hold yet (except possibly at s itself). Assume $s_0 \in S_0$ (for otherwise there is nothing to prove). For each $s \in S_0$ let β_s denote the probability that p will hold eventually, given that we have reached s. The premise of (R4) implies that $\beta_s \geqslant \alpha > 0$ (the lower bound for the positive transition probabilities) for each $s \in S_0$. Let $\gamma \equiv \inf_{s \in S_0} \beta_s \geqslant \alpha$. For every $s \in S_0$ we have

$$\beta_s \geqslant \alpha \cdot 1 + (1-\alpha) \cdot \gamma$$

(with probability at least α, p holds next, and otherwise p will hold eventually with probability at least γ). Thus $\gamma \geqslant \alpha + (1-\alpha)\gamma$, implying $\gamma = 1$, or $\beta_s = 1$ for all $s \in S_0$.

Remark. It would be tempting to replace (R4) by the simpler sound rule

$$(\text{R4}') \quad \vdash r \supset p \vee (\forall \mathbf{X} r \wedge \exists \mathbf{X} p) \Rightarrow \vdash r \supset \forall \mathbf{F} p.$$

However, the resulting axiomatic system will not be complete. In fact, (R4) cannot be deduced from the modified axiomatic system. We will show this indirectly, by exhibiting an alternative interpretation for the modified axiomatic system, with (R4) replaced by (R4'), for which (R4) does not hold.

Consider the interpretation of the modified system under models M which are defined as in PTL_b, except that their associated transition probabilities are not required to be bounded away from 0. Instead we require that for each state s at the ith level of M we have $P(s, t) \geqslant 1/i$, for each nonzero transition probability $P(s, t)$. It is easy to see that all axioms and rules of the modified system are sound under this interpretation. Indeed, everything except (R4') is either nonprobabilistic or holds in

general unbounded models. Concerning (R4′), suppose that a model M satisfies the premise of (R4′), and that r holds at the initial state of M. Then the probability that p still does not hold after n levels of M is at most $\prod_{i=2}^{n}(1-1/i) \to 0$ as $n \to \infty$. Nevertheless, it is easy to construct a model M of this new kind for which the antecedent of (R4) holds, whereas its consequent does not. To obtain M, take a sequence $\{i_t\}$ of levels for which $\prod_{t=1}^{\infty}(1-1/i_t) > 0$, and define M so that r holds at the root and at each node in each of the levels i_t. For each node n at the i_t level, p holds at exactly one son m of n, with $P(n, m) = 1/i_t$. It is then easy to check that M satisfies the antecedent of (R4) but not its consequent.

Hence, the "essence" of the bounded-model interpretation of PTL_b is captured by the rule (R4).

Returning to PTL_f, the discussion in (4) of the preceding section implies that the above axiomatic system is complete for PTL_f. This follows from the fact that each valid formula p of PTL_f can be reduced, using (A3), to another valid formula involving only logical connectives and the operators $\forall\mathbf{X}$, $\exists\mathbf{X}$, $\forall\mathbf{U}$, and $\exists\mathbf{U}$. This reduced formula, considered as a formula of *CTL*, is also valid, and, since *CTL* is complete (Emerson and Halpern, 1982; Emerson and Clarke, 1982), the reduced p is provable from the corresponding axiomatic system of *CTL*, hence also from the remainder of the above system for PTL_f. Similar arguments show that PTL_f is decidable, by first reducing a given formula p of PTL_f by (A3) and then by applying a decision procedure for *CTL* (cf. Emerson and Halpern, 1982; Emerson and Clarke, 1982) to the reduced formula. These properties of PTL_f will also follow as special cases of the completeness and decidability of PTL_b, which will be established in the two following sections.

Theorems Common to PTL_f and PTL_b

We next list a few basic theorems provable from the core set of axioms and inference rules common to both logics. Some of these will be used in the sequel (in particular, see Sect. 5), while others are provided so as to illustrate the properties of the various operators of our logics:

(T1) $\forall\mathbf{X}(p \wedge q) \equiv \forall\mathbf{X}p \wedge \forall\mathbf{X}q$

(T2) $\forall\mathbf{X}p \vee \forall\mathbf{X}q \supset \forall\mathbf{X}(p \vee q)$

(T3) $p\forall\mathbf{U}q \equiv q \vee (p \wedge \forall\mathbf{X}(p\forall\mathbf{U}q))$

(T4) $p\forall\mathbf{U}q \wedge ((\sim q)\,\forall\mathbf{U}r) \supset p\forall\mathbf{U}r$

(T5) $(p \vee q)\,\forall\mathbf{U}r \supset p\forall\mathbf{U}(q \vee r)$

(T6) $(p\forall\mathbf{U}r) \wedge (q\forall\mathbf{U}r) \equiv (p \wedge q)\,\forall\mathbf{U}r$

(T7) $(p \supset \forall\mathbf{X}p)\,\forall\mathbf{U}q \supset (p \supset (p\forall\mathbf{U}q))$

(T8) $\forall\mathbf{F}p \supset \mathbf{true}\,\exists\mathbf{U}p$

(T9) $\forall\mathbf{X}p \supset \forall\mathbf{F}p$.

We can also deduce a few additional inference rules:

(R1′) $\vdash p \supset q \Rightarrow \vdash \forall \mathbf{X} p \supset \forall \mathbf{X} q$

(R2′) $\vdash p \Rightarrow \vdash p \forall \mathbf{U} q$ for any q

(R5′) $\vdash p \Rightarrow \vdash \forall \mathbf{F} p$

(R6) $\vdash p \supset q \Rightarrow \vdash \forall \mathbf{F} p \supset \forall \mathbf{F} q$

(R7) $\vdash r \supset \forall \mathbf{F}(p \vee (\forall \mathbf{X} \forall \mathbf{F} r \wedge \exists \mathbf{X} p)) \Rightarrow \vdash r \supset \forall \mathbf{F} p$.

Here are the proofs of these theorems and rules:

Proof of (R1′). By (R1) we have $\vdash \forall \mathbf{X}(p \supset q)$, so that by (A1) and (R0) we have $\vdash \forall \mathbf{X} p \supset \forall \mathbf{X} q$. Q.E.D.

Proof of (R2′) By (A0) we have $\vdash$ **true**, so that by (R1) $\vdash \forall \mathbf{X}$ **true**. Since $\vdash p$ is given, we have also $\vdash p \wedge \forall \mathbf{X}$ **true**. It follows by (R0) that

$$\vdash \mathbf{true} \supset q \vee (p \wedge \forall \mathbf{X} \mathbf{true})$$

so that by (R2) we have $\vdash$ **true** $\supset p \forall \mathbf{U} q$, or $\vdash p \forall \mathbf{U} q$. Q.E.D.

Proof of (T1). That the left-hand side implies the right-hand side follows from (R1′). To prove the other implication, we begin with the tautology

$$\vdash p \supset (q \supset (p \wedge q)).$$

From it we obtain by (R1′)

$$\vdash \forall \mathbf{X} p \supset \forall \mathbf{X}(q \supset (p \wedge q)).$$

Now (A1) gives

$$\vdash \forall \mathbf{X}(q \supset (p \wedge q)) \supset (\forall \mathbf{X} q \supset \forall \mathbf{X}(p \wedge q)).$$

Hence, using (R0),

$$\vdash \forall \mathbf{X} p \wedge \forall \mathbf{X} q \supset \forall \mathbf{X}(p \wedge q).$$ Q.E.D.

Proof of (T2). From the tautology $\vdash p \supset p \vee q$, we deduce, using (R1′),

$$\vdash \forall \mathbf{X} p \supset \forall \mathbf{X}(p \vee q)$$

and symmetrically

$$\vdash \forall \mathbf{X} q \supset \forall \mathbf{X}(p \vee q)$$

from which two statements the theorem follows immediately. Q.E.D.

Proof of (T3). The left-hand side implies the right-hand side by (A2). To prove the converse implication, let r denote the right-hand side of (T3). Thus we have

$$\vdash p\forall \mathbf{U} q \supset r$$

so that, by (R1′),

$$\vdash \forall \mathbf{X}(p\forall \mathbf{U} q) \supset \forall \mathbf{X} r$$

or

$$\vdash q \vee (p \wedge \forall \mathbf{X}(p\forall \mathbf{U} q)) \supset q \vee (p \wedge \forall \mathbf{X} r)$$

which is to say,

$$\vdash r \supset q \vee (p \wedge \forall \mathbf{X} r)$$

so that, by (R2), we conclude

$$\vdash r \supset p\, \forall \mathbf{U} q$$

which is what we wanted to show. Q.E.D.

Proof of (T4). Put $s = p\forall \mathbf{U} q$, $t = (\sim q)\forall \mathbf{U} r$, and $w = s \wedge t$. Then we have by (T3)

$$\vdash w \equiv (q \vee (p \wedge \forall \mathbf{X} s)) \wedge (r \vee (\sim q \wedge \forall \mathbf{X} t))$$

or

$$\vdash w \equiv (q \wedge r) \vee (p \wedge \forall \mathbf{X} s \wedge r) \vee (p \wedge \sim q \wedge \forall \mathbf{X} s \wedge \forall \mathbf{X} t).$$

Hence (recall (T1)),

$$\vdash w \supset r \vee r \vee (p \wedge \sim q \wedge \forall \mathbf{X}(s \wedge t))$$

or

$$\vdash w \supset r \vee (p \wedge \forall \mathbf{X} w)$$

so that, by (R2), we deduce the required implication

$$\vdash w \supset p\forall \mathbf{U} r.$$ Q.E.D.

Proof of (T5). Put $w = (p \vee q)\, \forall \mathbf{U} r$. Then by (A2)

$$\vdash w \supset r \vee ((p \vee q) \wedge \forall \mathbf{X} w)$$

so that, by (R0),

$$\vdash w \supset r \vee (q \wedge \forall \mathbf{X} w) \vee (p \wedge \forall \mathbf{X} w)$$

or

$$\vdash w \supset (r \vee q) \vee (p \wedge \forall \mathbf{X} w)$$

so that, by (R2), we conclude

$$\vdash w \supset p \forall \mathbf{U}(q \vee r). \qquad \text{Q.E.D.}$$

Proof of (T6). Put $w = (p \forall \mathbf{U} r) \wedge (q \forall \mathbf{U} r)$. By (A2) we have

$$\vdash w \supset (r \vee (p \wedge \forall \mathbf{X}(p \forall \mathbf{U} r)) \wedge (r \vee (q \wedge \forall \mathbf{X}(q \forall \mathbf{U} r))$$

so that, by (R0)),

$$\vdash w \supset r \vee (p \wedge q \wedge \forall \mathbf{X}(p \forall \mathbf{U} r) \wedge \forall \mathbf{X}(q \forall \mathbf{U} r)).$$

Hence, by (T1) and (R0),

$$\vdash w \supset r \vee ((p \wedge q) \wedge \forall \mathbf{X} w)$$

which implies, using (R2),

$$\vdash w \supset (p \wedge q) \forall \mathbf{U} r.$$

For the converse implication, put $z = (p \wedge q) \forall \mathbf{U} r$. Then, by (A2),

$$\vdash z \supset r \vee ((p \wedge q) \wedge \forall \mathbf{X} z)$$

so that, by (R0),

$$\vdash z \supset r \vee (p \wedge \forall \mathbf{X} z).$$

Thus, by (R2), we have $\vdash z \supset p \forall \mathbf{U} r$, and in a completely symmetric fashion, we also have $\vdash z \supset q \forall \mathbf{U} r$, from which the desired implication readily follows by (R0). Q.E.D.

Proof of (T7). Put $w = p \wedge ((p \supset \forall \mathbf{X} p) \forall \mathbf{U} q)$. By (A2), we have

$$\vdash w \supset p \wedge (q \vee ((p \supset \forall \mathbf{X} p) \wedge \forall \mathbf{X}((p \supset \forall \mathbf{X} p) \forall \mathbf{U} q)))$$

so that, by (R0),

$$\vdash w \supset q \vee (p \wedge \forall \mathbf{X} p \wedge \forall \mathbf{X}((p \supset \forall \mathbf{X} p) \forall \mathbf{U} q))).$$

Hence, using (T1),

$$\vdash w \supset q \vee (p \wedge \forall \mathbf{X} w)$$

from which we conclude, using (R2), that $\vdash w \supset p \, \forall \mathbf{U} q$. Q.E.D.

Proof of (T8). By (A6), with $\sim p$ instead of p and **false** instead of q, we have

$$\vdash ((\sim p) \, \forall \mathbf{U} \, \mathbf{false}) \wedge \forall \mathbf{F} p \supset \forall \mathbf{F} \, \mathbf{false},$$

or

$$\vdash \forall \mathbf{F} p \wedge (\sim (\forall \mathbf{F} \, \mathbf{false})) \supset \mathbf{true} \exists \mathbf{U} p.$$

From $\vdash$**true** we have by (R3) $\vdash \sim (\forall \mathbf{F} \, \mathbf{false})$, which completes the proof by (R0). Q.E.D.

Proof of (T9). By (A4),

$$\vdash p \supset \forall \mathbf{F} p,$$

and

$$\vdash \forall \mathbf{X} \forall \mathbf{F} p \supset \forall \mathbf{F} p.$$

Applying (R1′) to the first implication, we obtain

$$\vdash \forall \mathbf{X} p \supset \forall \mathbf{X} \forall \mathbf{F} p,$$

and (R0) completes the proof. Q.E.D.

Proof of (R5). Immediate by (A4) and (R0).

Proof of (R6). $\vdash p \supset q$, or $\vdash \sim p \vee q$, implies by (R2′)

$$\vdash (\sim p \vee q) \forall \mathbf{U} \, \mathbf{false}.$$

By (T5), we have

$$\vdash (\sim p \vee q) \, \forall \mathbf{U} \, \mathbf{false} \supset \sim p \forall \mathbf{U} q,$$

hence (R0) gives

$$\vdash \sim p \forall \mathbf{U} q.$$

By (A6),

$$\vdash (\sim p \forall \mathbf{U} q) \wedge \forall \mathbf{F} p \supset \forall \mathbf{F} q,$$

and (R0) again gives

$$\vdash \forall \mathbf{F} p \supset \forall \mathbf{F} q. \qquad \text{Q.E.D.}$$

Remark. Note that the statement

$$\forall \mathbf{F}(p \supset q) \supset (\forall \mathbf{F} p \supset \forall \mathbf{F} q)$$

is not valid in our logics!

Proof of (R7). Put $s \equiv p \vee (\forall \mathbf{X} \forall \mathbf{F} r \wedge \exists \mathbf{X} p)$. The premise of (R7) is $\vdash r \supset \forall \mathbf{F} s$. Hence, by (R6), $\vdash \forall \mathbf{F} r \supset \forall \mathbf{F} \forall \mathbf{F} s$, and by (A5) and (R0) we obtain $\vdash \forall \mathbf{F} r \supset \forall \mathbf{F} s$. Using (R1′) and (R0), we obtain

$$\vdash s \supset p \vee (\forall \mathbf{X} \forall \mathbf{F} s \wedge \exists \mathbf{X} p),$$

so that (R4) gives $\vdash s \supset \forall \mathbf{F} p$. Arguing as above, this implies

$$\vdash \forall \mathbf{F} s \supset \forall \mathbf{F} p,$$

and together with the premise $\vdash r \supset \forall \mathbf{F} s$ of (R7), we obtain

$$\vdash r \supset \forall \mathbf{F} p. \qquad \text{Q.E.D.}$$

4. The Tableau Method

In this section we modify the tableau method of Ben–Ari, Pnueli, and Manna (1983) and Emerson and Clarke (1982) to obtain a deterministic, exponential time-decision procedure for testing satisfiablity in PTL_b. The same technique also applies to PTL_f, as will be noted at the end of this section. The construction presented below is similar to that of Ben–Ari, Pnueli, and Manna (1983) and Emerson and Clarke (1982), but differs in certain aspects with reflect the probabilistic context of our interpretation.

(Note that another competing technique for testing satisfiability is the *maximal model* technique (cf. Emerson and Halpern, 1982). We have not checked whether this technique can also be modified to yield a probabilistic model of the form required by our interpretation, although we believe that this is indeed possible.)

Given a formula p_0 of PTL_b which we wish to test for satisfiability, we construct from it a finite directed graph $\mathbf{T}$ called *tableau*, each of whose nodes n is labeled by a set F_n of formulae (intuitively, formulae that are true at n), some of which have already been "expanded," while others are still "unexpanded." Initially $\mathbf{T}$ contains a single node n_0 (the root), and $F_{n_0} = \{p_0\}$, with p_0 unexpanded. $\mathbf{T}$ is then constructed inductively as follows. At each step we pick a node n having no successors, and a formula

TABLE I

α-expansions

r	r_1	r_2	r_3
$p \wedge q$	p	q	
$\exists \mathbf{G} p$	p	$\exists \mathbf{X} \exists \mathbf{G} p$	$\forall \mathbf{X}$ (**true** $\vee \exists \mathbf{G} p$)
$\sim (p \vee q)$	$\sim p$	$\sim q$	
$\sim (p \forall \mathbf{U} q)$	$(\sim q) \exists \mathbf{U} (\sim p)$		
$\sim (p \exists \mathbf{U} p)$	$(\sim q) \forall \mathbf{U} (\sim p)$		
$\sim (\forall \mathbf{F} p)$	$\exists \mathbf{G} \sim p$		
$\sim (\exists \mathbf{G} p)$	$\forall \mathbf{F} \sim p$		
$\sim (\forall \mathbf{X} p)$	$\exists \mathbf{X} \sim p$		
$\sim (\exists \mathbf{X} p)$	$\forall \mathbf{X} \sim p$		
$\forall \mathbf{G} p$	p	$\forall \mathbf{X} \forall \mathbf{G} p$	

$p \in F_n$ which has not yet been expanded. We then expand p by one of the rules stated below, thereby creating outgoing edges from n, some of which may lead to newly created nodes of **T** while others may point back at nodes already present in **T**.

Let n be a node of **T** and p an unexpanded formula in F_n; n can be expanded by one of the following rules:

α-expansion. If F_n contains a formula r having one of the forms in the first column of Table I, then we create one successor n_1 of n and put $F_{n_1} = F_n \cup \{r_1, r_2, \ldots\}$, where $r_1, r_2, \ldots$ are the corresponding formulae in the other columns of the table.

β-expansion. If F_n contains a formula r having one of the forms in the first column of Table II, then we create two successors n_1 and n_2 of n, and put $F_{n_1} = F_n \cup \{r_1\}$, and $F_{n_2} = F_n \cup \{r_2\}$, where r_1 and r_2 are the corresponding formulae in the other two columns of the table.

TABLE II

β-Expansions

r	r_1	r_2
$p \vee q$	p	q
$\forall \mathbf{F} p$	p	$\forall \mathbf{X} \forall \mathbf{F} p \wedge \exists \mathbf{X} \forall \mathbf{F} p$
$\sim (p \wedge q)$	$\sim p$	$\sim q$
$\exists \mathbf{F} p$	p	$\exists \mathbf{X} \exists \mathbf{F} p$
$p \forall \mathbf{U} q$	q	$p \wedge \forall \mathbf{X} (p \forall \mathbf{U} q)$
$p \exists \mathbf{U} q$	$p \wedge q$	$p \wedge \exists \mathbf{X} (p \exists \mathbf{U} q)$

X-expansion. If none of the preceding rules apply to n, then n is called a *state*; each unexpanded formula in F_n is either a proposition, the negation of a proposition, or a formula preceded by $\forall\mathbf{X}$ or $\exists\mathbf{X}$. The following X-expansion rule is then applied to node n. Let $\forall\mathbf{X}p_1,\ldots,\forall\mathbf{X}p_a$ be all the formulae in F_n preceded by $\forall\mathbf{X}$, and let $\exists\mathbf{X}q_1,\ldots,\exists\mathbf{X}q_b$ be all the formulae in F_n preceded by $\exists\mathbf{X}$. Then we create b sons $n_1,\ldots,n_b$ of n with

$$F_{n_k}=\{p_1,\ldots,p_a,q_k\}$$

for each $k=1,\ldots,b$; the kth son will be identified as the q_k-*son* of n. (If $b=0$, we create one son n_0 of n and put

$$F_{n_0}=\{p,\ldots,p_a\}.)$$

Each successor of n under this expansion is called a *pre-state* (since from it a new state will be eventually reached). The root n_0 of the tableau is also called a pre-state.

Remarks. (1) Comparing the expansion rules listed in Tables I and II with the corresponding expansion rules used in the nonprobabilistic cases, we see that the only rules which have changed are those corresponding to formulae of the form $\forall\mathbf{F}p$ and $\exists\mathbf{G}p$. The expansion rules that we use for these formulae involve clauses which are logically redundant; they are needed however to ensure proper development of the tableau, as will become apparent from the foregoing analysis and from the examples given in Appendix A. Note also that since the connectives of our logic are not independent of one another, some of the expansion rules given in Tables I and II are redundant, but are given there for exposition sake.

(2) The β-expansion rules concerning formulae of the forms $p\exists\mathbf{U}q$ or $\forall\mathbf{F}p$ are given special treatment in portions of the sequel. To prepare for this treatment we call the edge from n to n_1 an *essential* $\exists\mathbf{U}$ (resp. $\forall\mathbf{F}$)-*edge*, and n_1 the *essential* $\exists\mathbf{U}$ (resp. $\forall\mathbf{F}$)-*son* of n.

The construction of $\mathbf{T}$ is terminated by using the following termination rules (cf. Ben–Ari, Pnueli, and Manna, 1983):

(1) We do not expand any further nodes n for which F_n contains both a proposition and its negation. Such nodes are called *closed* meaning that they represent an inconsistent set of conjuncts; these nodes will be erased from the final form of the tableau by the marking rule (M1) given below.

(2) At an X-expansion of a state n, we do not create new succeeding prestates if their set of formulae is identical to the set of formulae of some ancestor pre-state m of n; in this case the corresponding outgoing edge from n points back to m.

These termination rules ensure that the resulting graph **T** is finite, and as a matter of fact, its size is singly exponential in the size of the given formula p_0.

Having thus created **T** we proceed to mark some of its nodes using several marking rules (some coincide with similar rules of Ben-Ari, Pnueli, and Manna, 1983, while others are special to the probabilistic case). Roughly speaking, a node is marked if its set of formulae cannot be satisfied by a model that can be obtained from "unwinding" the tableau from that node. Such nodes will eventually be deleted from the tableau. Before stating these rules, we need certain technical preparations.

Let S denote the set of *states* in **T** and let Π denote the set of *pre-states* in **T**. For every $s \in S$, let $X(s)$ be the set of al successor pre-states of s (obtained by the X-expansion rule); for each pre-state $\xi \in \Pi$, let $T(\xi)$ denote the set of all states in S which are reachable from ξ via paths consisting of α and β-expansions only. We will also use the inverse relations: $X^{-1}(\xi)$ denotes the set of all predecessor states of ξ (there may be more than one such state according to rule (2) for terminating the tableau construction), and $T^{-1}(s)$ is the (unique) pre-state preceding s. Essentially, all intermediate nodes of **T** which are neither states nor pre-states are ignored in the sequel. See Fig. 1 for an example illustrating these notions.

We now deal with formulae of the form $\exists \mathbf{G}p$, whose treatment require a certain structural decomposition of the tableau, which we now proceed to describe. Given $r = \exists \mathbf{G}p$ and $n \in S$ with $r \in F_n$, let $S_r = \{s \in S: r \in F_s\}$, and let $Y \subset \Pi$ be the set of all pre-states ξ which are reachable from n along paths whose states all belong to S_r. We will obtain a decomposition of Y which is closely related to the decomposition of the state-space of a (finite-state) concurrent probabilistic program given in Hart, Sharir, and Pnueli (1983). The purpose of this decomposition is to find *ergodic* sets E of states, all of which contain r, and for which there exists an "unwinding" of the

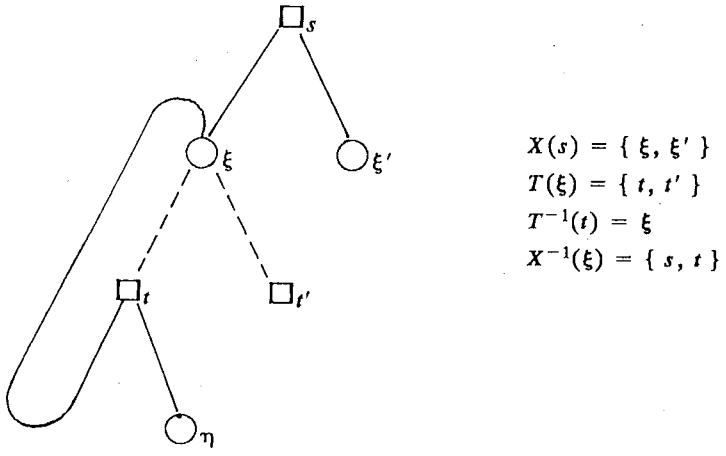

FIG. 1. A fragmentary tableau and the X and T relations.

tableau starting at any $s \in E$ and visiting from then on only states of E. Such an unwinding will enable us to show that r is satisfied in a model constructed from this unwinding and whose initial state is either in E or from which E can be reached via some finite path of states in S.

More precisely, define

$$I_0 = \{s \in T(Y): r \notin F_s\}.$$

We will construct inductively a sequence of (disjoint) subsets $\{H_m\}_{m \geq 1}$ of Y, as follows. We begin by constructing a directed graph G, whose nodes are the pre-states of Y, and whose edges are given by the relation $v \equiv X \circ T$ restricted to Y (i.e., $\eta \in v(\xi)$ if there exists $s \in S_r$ such that $s \in T(\xi)$ and $\eta \in X(s)$; it is helpful to label each such edge by the corresponding state s); note that G may contain loops (i.e., edges of the form (ξ, ξ)) and multiple edges. Let H_1 be a terminal strongly connected component of G, including the degenerate case of a singleton $H_1 = \{\xi\}$, in which case it is not required that (ξ, ξ) be an edge of G. Thus, for each $\xi \in H_1$ and each $t \in T(\xi)$, either $X(t) \subset H_1$ or $t \in I_0$. Next, suppose that $H_1, \ldots, H_{m-1}$ have already been defined, and put $K_{m-1} = \bigcup_{i<m} H_i$. We first update G by erasing all nodes $\xi \in H_{m-1}$, together with all edges (η, η') for which there exists $s \in T(\eta)$ such that both ξ and η' belong to $X(s)$ (thus, besides edges (η, ξ) we also erase edges (η, η') with the same label s as (η, ξ)). H_m is then defined to be a terminal strongly connected component of the (updated) graph G (including the degenerate case of a singleton, as above). Thus, H_m has the following property: For each $\xi \in H_m$ and each $t \in T(\xi)$, either

(1) $t \in I_0$; or

(2) $X(t) \cap K_{m-1} \neq \varnothing$; or

(3) $X(t) \subset H_m$.

(Note that this holds for $m = 1$ too.) We continue with this process until G becomes empty.

Having obtained this decomposition, we next define, for each $m \geq 1$,

$$I_m \equiv \{s \in S: T^{-1}(s) \in H_m \text{ and } X(s) \subset H_m\}.$$

$$L_m \equiv \{s \in S: T^{-1}(s) \in H_m, s \notin I_0 \text{ and } X(s) \not\subset H_m\}.$$

LEMMA 4.1. *If $\xi, \eta \in H_m$ and $\eta \in v(\xi)$ via the state t (i.e., $t \in T(\xi) \cap X^{-1}(\eta)$) then $t \in I_m$.*

Proof. The edge (ξ, η) has not been erased at the time H_m was constructed, and thus we must have $X(t) \subset H_m$, i.e., $t \in I_m$ by definition.

COROLLARY 4.2. *$I_m = \varnothing$ if and only if H_m is not strongly connected (and*

thus H_m is a singleton, say $H_m = \{\xi\}$, and each $t \in T(\xi)$ is either in I_0 or satisfies $X(t) \cap K_{m-1} \neq \varnothing$).

COROLLARY 4.3. *If $I_m \neq \varnothing$ then:*

(E1) *$T(\xi) \cap I_m \neq \varnothing$, for each $t \in I_m$ and each $\xi \in X(t)$.*

(E2) *For each $s, t \in I_m$, $s \neq t$, there exists a chain $s = s_0, s_1, \ldots, s_j = t$ of states in I_m, such that $s_{i+1} \in N(s_i)$ for $i = 0, 1, \ldots, j-1$, where $N \equiv T \circ X$.*

Proof. (E1) $\xi \in H_m$ which is strongly connected, thus there exists an edge (ξ, η) with $\eta \in H_m$ too; the corresponding state s through which this edge materializes then belongs to $T(\xi) \cap I_m$.

(E2) Let $\eta = T^{-1}(t)$, and let ξ be an arbitrary pre-state in $X(s)$. Since both $\xi, \eta \in H_m$ and H_m is strongly connected, there exists a chain $\xi = \xi_0, \xi_1, \ldots, \xi_{j-1} = \eta$ of pre-states in H_m such that $\xi_{i+1} \in \nu(\xi_i)$ for all $i = 0, 1, \ldots, j-2$. Let s_{i+1} be the state corresponding to the edge (ξ_i, ξ_{i+1}); then $s_{i+1} \in I_m$ by Lemma 4.1, and $s = s_0, s_1, \ldots, s_{j-1}, s_j = t$ is the required chain of states. Q.E.D.

COROLLARY 4.4. *If $I_m \neq \varnothing$ then for each $\xi \in H_m$ we have $X^{-1}(\xi) \cap I_m \neq \varnothing$.*

Proof. By Corollary 4.2, H_m is strongly connected, thus ξ is connected to itself via a nonempty chain of edges $(\tau_1, \tau_2), (\tau_2, \tau_3), \ldots, (\tau_{n-1}, \tau_n)$, where $\tau_1 = \tau_n = \xi$. But then it follows from Lemma 4.1 that the state through which the last edge (τ_{n-1}, ξ) has materialized belongs to $X^{-1}(\xi) \cap I_m$. Q.E.D.

Suppose that $I_m \neq \varnothing$. Intuitively, this means that, starting at some $s \in I_m$, one can "unwind" the tableau into an infinite tree which consists only of states in I_m, by choosing at each pre-state $\xi \in H_m$ a state $t \in T(\xi) \cap I_m$, and by noting that all successor pre-states of t are contained in H_m. Since the formula $\exists \mathbf{G} p$ is contained in F_s, we could potentially use such an unwinding of $\mathbf{T}$ as a model for the satisfiability of $\exists \mathbf{G} p$. This, however, depends on our ability to satisfy other formulae of F_s by that same unwinding. As will be seen below, it suffices to require from I_m that its unwinding can satisfy every formula of the form $\forall \mathbf{F} q$ which appears at some of its states.

DEFINITION. A set E of states in S is called an **ergodic set** if it satisfies the following properties (the first two of which are as in Corollary 4.3):

(E1) $T(\xi) \cap E \neq \varnothing$, for each $t \in E$ and each $\xi \in X(t)$.

(E2) For each $s, t \in E$, $s \neq t$, there exists a chain $s = s_0, s_1, \ldots, s_j = t$ of states in E, such that $s_{i+1} \in N(s_i)$ for $i = 0, 1, \ldots, j-1$, where $N \equiv T \circ X$.

(E3) For each formula of the form $\forall \mathbf{F} q$ which appears in F_s for some $s \in E$, there exists $t \in E$ such that $q \in F_t$.

Consequently, we distinguish between three subcases:

(I) $I_m = \varnothing$.

(II) $I_m \neq \varnothing$ is not ergodic. That is, there exists $s \in I_m$ and a formula $(\forall \mathbf{F} q) \in F_s$ such that $q \notin F_t$ for all $t \in I_m$. (It is easily seen, by the rule of $\forall \mathbf{F}$-expansion, that in this case the formula $\forall \mathbf{F} q$ belongs to F_t for every $t \in I_m$.)

(III) $I_m \neq \varnothing$ is ergodic (we will call it an *ergodic set for the formula* r, or an *r-ergodic set* for short).

Marking Rules

We are now in a position to state our marking rules:

(M1) Mark every closed node (i.e., a node containing both a proposition and its negation).

(M2) If n is a node at which an α-expansion has been applied and its son n_1 has been marked then mark n.

(M3) If n is a node at which a β-expansion has been applied and both its sons n_1 and n_2 have been marked then mark n.

(M4) If n is a state and one of its succeeding pre-states has been marked then mark n.

(M5) Let $r = p\ \exists \mathbf{U} q$ or $r = \forall \mathbf{F} p$, and let N_r denote the set of all unmarked nodes n of $\mathbf{T}$ whose set of formulae F_n contains r; assume this set is nonempty. A path π in $\mathbf{T}$ is *r-acceptable* if it visits only nodes in N_r, and at every state s along π (at which an X-expansion takes place), π continues with that son of s generated by the formula $\exists \mathbf{X} r$ in F_s.

A node $n \in N_r$ will be marked if there exists no r-acceptable path from n to a node $m \in N_r$ with $p, q \in F_m$ if $r = p\ \exists \mathbf{U} q$ or with $p \in F_m$ if $r = \forall \mathbf{F} p$. (The intuitive meaning of this rule is clear for $r = p\ \exists \mathbf{U} q$; as for $r = \forall \mathbf{F} q$ this rule is justified by yet another application of the 0–1 law—see below for details.)

To implement this rule, one may use a straightforward backwards propagation technique, starting from those nodes where r is "fulfilled" (i.e., contains p, q in the case $r = p\ \exists \mathbf{U} q$ or p in the case $r = \forall \mathbf{F} p$).

We come now to the last and most complex marking rule (M6), which uses the machinery of ergodic sets developed above:

(M6) Let $r = \exists \mathbf{G} p$ be a formula appearing in the set F_n of some unmarked state n. Without loss of generality, assume all marked nodes have been deleted from $\mathbf{T}$. As above, let $S_r = \{s \in S: r \in F_s\}$, and let $Y \subset \Pi$ be the set of all pre-states ξ which are reachable from n along paths whose states all belong to S_r. Decompose Y into sets $\{H_m\}_{m \geq 1}$ as above, from

which the sets $\{I_m\}_{m \geq 1}$ are obtained. If all non-empty I_m are not ergodic (i.e., for each m either case (I) or case (II) above holds), then mark n. Otherwise, n remains unmarked.

Remark. For efficiency, we could mark all nodes of S_r simultaneously if its decomposition contains no ergodic set. Better still, even if an ergodic set exists, we can still mark all nodes m of S_r for which there does not exist a path contained in S_r and leading from m to such an ergodic set.

The marking process proceeds in phases; in each such phase we either apply one of the rules (M1)–(M4) to a single node of **T** or apply rule (M5) to a formula $\forall \mathbf{F}p$ or $p \exists \mathbf{U} q$ at some node of **T** which may cause several nodes of **T** to be marked simultaneously, or apply rule (M6) to a formula $\exists \mathbf{G}p$ and a node containing it, which again can result in marking more than one node. This marking process terminates when no new nodes can be marked.

As to the complexity of the marking procedure just described, note that each marking phase marks at least one additional node of the tableau. Moreover, each such phase requires time polynomial in the size of the tableau. Indeed, phases involving rules (M1)–(M4) are performed by straightforward linear-time scanning of **T**; phases involving (M5) are performed by a linear-time graph propagation procedure. Finally, phases involving (M6) apply the procedure described above for decomposition of the tableau into the sets H_m. This procedure is based on repeated graph decomposition into strongly connected components. Since each such decomposition requires linear time, and removes at least one node from the tableau, the overall procedure runs in time quadratic in the size of the tableau. Overall we conclude that the marking procedure runs in time polynomial in the size of the tableau, hence singly exponential in the size of the given formula.

The main result of this paper is

THEOREM 4.5. *p_0 is satisfiable if and only if the root n_0 of* **T** *has not been marked. Moreover, if the root has been marked then $\sim p_0$ is provable in PTL_b (i.e., the axiomatization of PTL_b given in Sect. 3 is complete). In this latter case the proof of $\sim p_0$ can be obtained mechanically off the tableau* **T**.

Proof. The proof of completeness of the axiomatic system of Section 3 is postponed to the following section. Here we show that if n_0 has not been marked, then we can construct a model of PTL_b for p_0 from the unmarked nodes of **T**. This is achieved by first constructing from the unmarked nodes of **T** a *Hintikka structure* (defined below), and then transforming this structure into a model for p_0.

DEFINITION. A *Hintikka structure* H for a formula p_0 of PTL_b is an

infinite tree with a root s_0 such that the number of sons of any node in H is bounded, and such that with each node $s \in H$ there is associated a set F_s of formulae of PTL_b. Given such a tree H, we can associate with each edge (m, n) of H a *transition probability* equal to $1/d$, where d is the out-going degree of m (note that these probabilities are bounded away from 0). This probability assignment allows us to regard H as a stochastic process, and induces, for each node $s \in H$, a probability measure $\mu_{s,H}$ on the set Ω_s of all infinite paths in H starting at s, in the standard manner as in Section 2. In addition, H must have the following properties ($p \in F_s$ is abbreviated as $p \in s$):

(H0) $p_0 \in s_0$.

(H1) $\sim p \in s$ implies $p \notin s$ (i.e., H is consistent).

(H2) Let r be a formula to which an α-expansion is applicable (see Table I); then $r \in s$ implies $r_j \in s$ for all corresponding subconjuncts r_j of r (appearing in the other columns of the table).

(H3) Let r be a formula to which a β-expansion is applicable (see Table II); then $r \in s$ implies $r_1 \in s$ or $r_2 \in s$ (where r_1, r_2 are the two corresponding disjuncts appearing in the other columns of the table).

(H4a) If $\forall \mathbf{X} p \in s$ then $p \in t$ for all succeeding nodes t of s in H.

(H4b) If $\exists \mathbf{X} p \in s$ then $p \in t$ for at least one succeeding node t of s in H.

(H4c) If $p \exists \mathbf{U} q \in s$ then there exists a path from s all of whose nodes contain p, and its last node also contains q.

(H4d) If $p \forall \mathbf{U} q \in s$ then every path starting at s either contains p in all its nodes, or contains p at all its initial nodes (possibly none) before reaching a node which contains q.

(H4e) If $\forall \mathbf{F} p \in s$ then there exists a stopping time N, defined on Ω_s (the subtree of H rooted at s), which is $\mu_{s,H}$-almost-surely finite, and for which $p \in \omega_{N(\omega)}$, for each $\omega \in \Omega_s$ with $N(\omega) < \infty$.

(H4f) If $\exists \mathbf{G} p \in s$ then

$$\mu_{s,H}\{\omega \in \Omega_s : p \in \omega_n \text{ for all } n \geqslant 1\} > 0.$$

LEMMA 4.6. *If p_0 has a Hintikka structure, then it has a model, i.e., it is satisfiable.*

Proof. Let H be a Hintikka structure for p_0. We construct from H a model $M = (S, P, s_0, \rho)$, where S is the set of nodes of H, P is the probability mapping defined above on the set of edges of H, and ρ is defined as follows: for a proposition a and a node s, $a \in \rho(s)$ if $a \in F_s$ or $\sim a \notin F_s$, whereas $a \notin \rho(s)$ if $\sim a \in F_s$.

M is clearly a PTL_b-model. To show that it is a model for p_0, we prove, using simultaneous induction on the length of formulae r appearing in F_s, that

$$r \in s \in S \Rightarrow \models_{M_s} r;$$
$$\sim r \in s \in S \Rightarrow \models_{M_s} \sim r,$$

where M_s is the model M with initial state s.

The proof of this claim proceeds as in Ben–Ari, Pnueli, and Manna (1983), except for the treatment of formulae involving $\forall\mathbf{U}$, $\exists\mathbf{U}$, $\forall\mathbf{F}$, and $\exists\mathbf{G}$, which are handled as follows:

Suppose that $p\exists\mathbf{U}q \in s$. Then by (H4c) there exists a (simple) path $\omega = (\omega_1 = s, \omega_2, \ldots, \omega_n)$, such that $p \in \omega_j$ for all $j = 1, \ldots, n$ and $q \in \omega_n$. It follows by induction that $\models_{M_{\omega_j}} p$, $j = 1, \ldots, n$, and that $\models_{M_{\omega_n}} q$, thus $\models_{M_s} p\exists\mathbf{U}q$.

Similarly, if $p\forall\mathbf{U}q \in s$, then every path from s contains p at all its nodes until the first occurrence of q, if any. Again, by induction, it follows from the definition of $\forall\mathbf{U}$ that $\models_{M_s} p\forall\mathbf{U}q$.

Next, suppose that $\exists\mathbf{G}p \in s$. Then by (H4f) the $\mu_{s,H}$ measure of paths $\omega \in \Omega_s$ for which $p \in \omega_n$ for each $n \geq 1$, is positive. By induction hypothesis, for each such ω, and each $n \geq 1$, we have $\models_{M_{\omega_n}} p$, so that by definition of validity of $\exists\mathbf{G}p$ it follows immediately that $\models_{M_s} \exists\mathbf{G}p$.

Finally, suppose that $\forall\mathbf{F}p \in s$. Then there exists a $\mu_{s,H}$-almost surely finite stopping time N on Ω_s such that $p \in \omega_{N(\omega)}$ for every $\omega \in \Omega_s$, for which $N(\omega) < \infty$. Again, by induction hypothesis, this implies that $\models_{M_{\omega_{N(\omega)}}} p$ for each such ω, so that, by definition of validity of $\forall\mathbf{F}p$, we conclude that $\models_{M_s} \forall\mathbf{F}p$.

These inductive arguments imply in particular that $\models_M p_0$, so that p_0 is satisfiable. Q.E.D.

It therefore remains to construct a Hintikka structure H for p_0 from the unmarked nodes of $\mathbf{T}$. For this, we use the following construction, in which we assume, for simplicity, that all nodes of $\mathbf{T}$ are unmarked. The following observations, which have already appeared implicity in the marking rule (M6), will be useful in motivating and explaining the construction of the required Hintikka structure. As before, we let S (resp. Π) denote the set of all (unmarked) states (resp. pre-states) of $\mathbf{T}$. The nodes of the Hintikka structure H we are about to construct from $\mathbf{T}$ will be states in S. The number of sons of a node $s \in H$ is the same as the number of pre-states in $X(s)$. For each such $\xi \in X(s)$ there will correspond a son of s in H which will be an element of $T(\xi)$. The decisions as to which state in $T(\xi)$ to choose as the corresponding son of s can be thought of as being taken by some "scheduler," and we will refer to them as a *schedule* of $\mathbf{T}$. This notation is very similar to the modelling of the execution of a concurrent probabilistic program, as described, e.g., in Hart, Sharir, and Pnueli (1983). In this

analogy, the "program states" are our pre-states Π; at each such $\xi \in \Pi$, the schedule assigns a process to execute the next program state, which, in our case, corresponds to choosing a state $t \in T(\xi)$, and then "execute" the **X**-transitions from t to new pre-states (i.e., new program states). Thus "program execution" corresponds to the construction of H, in which we just record the states in S chosen by the scheduler.

It is instructive to note that, unlike the finite-model interpretation of PTL_f, in the case of bounded models we can let the schedule be quite arbitrary, and depend upon the entire path in H from the root to the current node. In contrast, in the case of PTL_f, in order to ensure that the resulting structure be finite, we have to require that the schedule be "finitary," i.e., use only finite memory in determining the next state to be chosen at the current pre-state.

The preceding remarks imply that to construct H it suffices to define the corresponding schedule σ. σ is a function defined on the set of all *finite execution histories*, each such history being a sequence of the form

$$h_n = (\xi_0, s_1, \xi_1, s_2, \ldots, s_n, \xi_n)$$

with ξ_0 the root of **T** and where for each $i = 1, \ldots, n$ we have $s_i \in T(\xi_{i-1})$ and $\xi_i \in X(s_i)$. (Thus, for convenience, we label each node of H also by the pre-state ξ of its corresponding state s. Each such h_n corresponds to a path ω of length n in H in which the schedule's decisions at the first $n-1$ nodes are already recorded; $\sigma(h_n)$ is to be the state s_{n+1} in $T(\xi_n)$ that the schedule will choose at the terminal node of ω.) Figure 2 illustrates these notations.

Before defining σ, we first modify **T** slightly to eliminate any partial overlapping between ergodic sets. Let $E_1, \ldots, E_d$ be the ergodic sets of **T** (for all formulae). Suppose that $s \in S$ belongs to more than one ergodic set, say $s \in E_1 \cap E_2 \cap \cdots \cap E_e$. We then replace s by e new nodes $(s, 1)$, $(s, 2), \ldots,$ (s, e) such that, for $j = 1, 2, \ldots, e$ we have

$$F_{(s,j)} = F_s; \qquad X((s,j)) = X(s); \qquad T^{-1}((s,j)) = T^{-1}(s).$$

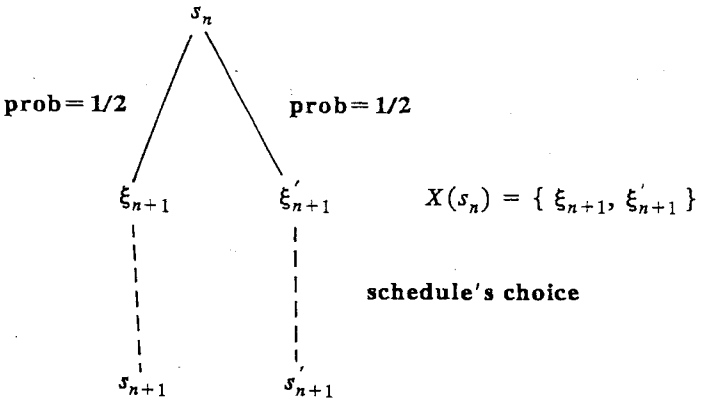

FIG. 2. Tableau unwinding by a schedule.

Define

$$E'_j = (E_j - \{s\}) \cup \{(s, j)\},$$

for $j = 1, 2, \ldots, e$. Since the internal structure of E'_j is isomorphic to the structure of E_j for $j = 1, 2, \ldots, e$, it follows that all these new sets are ergodic. Furthermore, if we apply the marking procedure to the new tableau obtained by this splitting, then no new nodes will be marked because the duplication of states in the above manner cannot cause any of the marking rules (M1)–(M6) to become applicable if it were not applicable before.

Repeating the splitting procedure just described for each original $s \in S$ as needed, we obtain an equivalent but larger tableau $\mathbf{T}'$ together with associated ergodic sets $E'_1, E'_2, \ldots, E'_d$, with each state belonging to at most one of these ergodic sets. Without loss of generality, we will assume that the original ergodic sets $E_1, \ldots, E_d$ in $\mathbf{T}$ itself already have this property. Then each set $s \in S$ either belongs to a unique ergodic set E_e, or else is "transient," i.e., belongs to $E_0 \equiv (\bigcup_{e=1}^{d} E_e)^c$.

For every $s \in S$ and $\xi \in X(s)$, we define

$$V(s, \xi) = \begin{cases} T(\xi) \cap E_e & \text{if } s \in E_e,\ e > 0, \\ T(\xi) & \text{if } s \in E_0. \end{cases}$$

Note that $V(s, \xi)$ is always nonempty. For each such s and ξ let $(t^1_\xi, \ldots, t^k_\xi)$ be a fixed enumeration of the elements of $T(\xi)$, and let $(v^1_{(s,\xi)}, \ldots, v^l_{(s,\xi)})$ be a fixed enumeration of the elements of $V(s, \xi)$ (note that $k \equiv k(\xi)$ and $l \equiv l(s, \xi)$). Let

$$h_n = (\xi_0, s_1, \xi_1, s_2, \ldots, s_n, \xi_n)$$

be a finite history in H; we will define $\sigma(h_n) = s_{n+1}$ as follows. Let r be the number of occurrences of $s \equiv s_n$ in h_n (up to and including n) i.e., $r = |\{i: 1 \leqslant i \leqslant n,\ s_i = s_n\}|$. Two possible cases can arise:

(a) All the following three conditions hold:

(i) $r = v^2$ for some $v \geqslant 3$.

(ii) $|X(s)| > 1$.

(iii) $\xi_{m_1} = \xi_{m_2} = \cdots = \xi_{m_v}$, where $n > m_1 > m_2 > \cdots > m_v$ are the places in h_n of the last v occurrences of s (before the nth place).

(b) At least one of these conditions does not hold.

If case (a) occurs, let $j \equiv v \pmod{k(\xi_n)}$ and define $\sigma(h_n) = t^j_{\xi_n}$. If case (b) occurs, let $j \equiv (r - \lfloor \sqrt{r} \rfloor) \pmod{l(s, \xi_n)}$ and define $\sigma(h_n) = v^j_{(s_n, \xi_n)}$.

Let us call a visit at s for which r is a perfect square $\geqslant 9$ a *square* visit. Thus case (a) occurs only at pre-states ξ following a square visit (of order

v^2) at a state s which has more than one succeeding pre-state, and for which s is followed in h_n by the same pre-state ξ at each of the last v visits at s. When this case applies, the schedule iterates through $T(\xi)$ in a round robin fashion (stepping through the elements of $T(\xi)$ once per each such special square visit). Similarly, case (b) occurs when the visit at the last state s in h_n is either non-square, or is square but not all last $\sqrt{r}$ visits at s have been followed by the same succeeding pre-state. In these cases the schedule iterates through $V(s, \xi)$ in a round robin fashion, in which the square visits at s are not counted.

The reason(s) for the peculiar definition of this schedule will become apparent below. Intuitively, it is due to the fact that one has to make sure that ergodic sets which are entered are also eventually exited when needed.

We next show that the unwinding of the tableau **T** by the schedule σ just defined yields a Hintikka structure H for p_0. The proof that H satisfies conditions (H4c), (H4e), and (H4f) is somewhat involved and technical. We have to show the existence of a path (or, in the case of (H4f), a set of paths having positive measure) passing only through nodes containing the corresponding subformula $r = q\exists \mathbf{U}p$, $\forall \mathbf{F}p$ or $\exists \mathbf{G}p$ and (in the cases of (H4c) and (H4e)) ending at a node containing p; in showing this, difficulties can arise because as such a path is being constructed, it can enter various ergodic sets, some of which may be irrelevant to the "fulfillment" of r, and so must be exited in order for r to be fulfilled. We construct a path by choosing at each state along the way a corresponding succeeding pre-state; the schedule then chooses which state will follow (according to the definition above).

DEFINITION. A function ρ defined on a subset $S_\rho \subset S$ and having non-negative integer values, is called an *existential ranking function* if the following conditions hold:

(i) $S_\rho^0 \equiv \rho^{-1}(0) \neq \varnothing$.

(ii) For each $s \in S_\rho - S_\rho^0$ there exists $\eta \in X(s)$ such that $T(\eta) \subset S_\rho$.

(iii) For each $s \in S_\rho - S_\rho^0$ there exists $t \in T(X(s))$ such that $\rho(t) < \rho(s)$.

(iii′) For each $s \in S_\rho - S_\rho^0$ with $|X(s)| = 1$ there exists $t \in V(s, \xi)$ such that $\rho(t) < \rho(s)$, where $X(s) = \{\xi\}$.

DEFINITION. A function ρ defined on a subset $S_\rho \subset S$ and having a non-negative integer values, is called a *universal ranking function* if the following conditions hold:

(i) $S_\rho^0 \equiv \rho^{-1}(0) \neq \varnothing$.

(iv) For each $s \in S_\rho - S_\rho^0$ and for each $\xi \in X(s)$ we have $V(s, \xi) \subset S_\rho$.

(v) For each $s \in S_\rho - S_\rho^0$ there exists $\xi \in X(s)$ and $t \in V(s, \xi)$ such that $\rho(t) < \rho(s)$.

Note an essential difference between the two definitions: "there exists a son in $X(s)$" in (ii) vs. "for all sons in $X(s)$" in (iv); this explains our choice of names.

PROPOSITION 4.7. *Let ρ be an existential ranking function, and let h_n be a history (which we take, here and in the sequel, as $h_n = (\xi_0, s_1, \ldots, \xi_{n-1}, s_n)$) with $s_n \in S_\rho$. Then there exists a finite path in H from s_n to some state in S_ρ^0, which visits only states in S_ρ.*

Proof. Assume the contrary, and construct inductively the following infinite path ω in H, starting at s_n, which stays forever in S_ρ. For each $m \geqslant n$, let s_m be the current state, which we assume to belong to S_ρ. If there exists $\xi \in X(s_m)$ such that $t \equiv \sigma(h_{m-1}, s_m, \xi)$ satisfies $\rho(t) < \rho(s)$, then continue the path ω with any such ξ as the following ξ_m. Otherwise choose $\xi_m = \eta$, where η is one of the pre-states in $X(s)$ as given by condition (ii) for $s = s_m$ (if there is more than one such η, fix one and *always* choose it). In all cases, $s_{m+1} \in S_\rho$. (Note that in order to define the path ω, we have to choose for each (h_{m-1}, s_m) the next $\xi_m \in X(s_m)$, i.e., the outcome of the randomization at s_m; σ will then define s_{m+1}.)

We have thus defined an infinite path ω in S_ρ. Let ρ_0 be the minimal value of ρ appearing along ω infinitely often, and let s be a state which appears infinitely often along ω with $\rho(s) = \rho_0$. Note that $\rho_0 > 0$ by assumption, so that by condition (iii) there exists some $\xi \in X(s)$ and some $t \in T(\xi)$ such that $\rho(t) < \rho(s)$. Since ρ_0 is minimal, t cannot be visited infinitely often in ω, so that, for some $m \geqslant n$, the path never visits t after the mth place.

Let r be the number of visits at s in h_m (i.e., up to and including the mth place on the path). Let $v \geqslant 3$ be the smallest integer satisfying $v^2 > r$. Suppose first that $|X(s)| > 1$, and consider the sequence of visits at s along ω numbered $(v+1)^2$, $(v+2)^2$, etc. Then at each one of these visits at s, case (a) applies to the scheduler, since at all preceding visits the succeeding pre-state of s is η by definition of ω. Therefore, after at most $|T(\xi)|$ of these visits we would have reached a visit at s, with a preceding history h, such that $\sigma(h, s, \xi) = t$, so that t should follow s after that visit, by definition of ω—a contradiction. Finally, if $|X(s)| = 1$, then condition (iii′) implies that the state $t \in T(X(s))$ with $\rho(t) < \rho(s)$ belongs to the appropriate $V(s, \xi)$. Here only case (b) applies, and after at most $|V(s, \xi)|$ non-square visits at s the schedule would have to choose t after the pre-state ξ, so that ω would contain t after the mth place, again a contradiction. This establishes the proposition. Q.E.D.

PROPOSITION 4.8. *There exists $\alpha > 0$ (depending only on $|S|$), such that for every universal ranking function ρ, and for each finite history h_n with $s_n \in S_\rho$, the probability of reaching S_ρ^0 from s_n via states in S_ρ only, is $\geqslant \alpha$.*

Proof. Consider the following path ω (which is defined inductively, as in the preceding proposition, by specifying the pre-state which follows each state along the path): At each state $s \in \omega$, let r be the total number of visits at s, and assume $|X(s)| > 1$ (otherwise ω must continue with the sole successor pre-state of s). If $r \neq v^2 - 1$, for all $v \geqslant 3$, then choose the pre-state ξ given by condition (v) (if there is more than one such ξ, fix one and *always* choose it); if $r = v^2 - 1$, choose any $\eta \in X(s)$ which is different from the pre-state chosen at visit number $r - 1 = v^2 - 2$ (this is possible since $|X(s)| > 1$; it guarantees that condition (a)(iii) in the definition of the scheduler will not be satisfied at $r = v^2$). Note that by condition (iv), ω never leaves S_ρ. Indeed, the only possibility of leaving S_ρ is at square visits for which case (a) applies; but our choice of pre-states along ω guarantees that this never happens (this also holds for states s with $|X(s)| = 1$, by definition). Hence ω visits only states in S_ρ, and at each such state on ω, the schedule operates according to case (b). For each $s \in S_\rho - S_\rho^0$ appearing along ω, let $\xi \in X(s)$ be the chosen pre-state given by (v), and let $t \in V(s, \xi)$ be a state for which $\rho(t) < \rho(s)$. Since at each visit at s along ω case (b) applies, it follows that if we disregard square visits at s and also visits numbered $v^2 - 1$, then by definition of σ, after every $|V(s, \xi)|$ consecutive visits at s, ω would contain one visit at t (following one of those visits at s). If we also take into account the disregarded visits at s, then a visit at t would be guaranteed during every sequence of at least $|V(s, \xi)| + 2\sqrt{|V(s, \xi)|} \leqslant 3|S|$ consecutive visits at s. If t is not yet in S_ρ^0, we can repeat this argument with $\xi' \in X(t)$ and $t' \in V(s, \xi')$ for which $\rho(t') < \rho(t)$. We would then conclude that during every sequence of at least

$$3|S| \cdot 3|S| = 9|S|^2$$

consecutive visits at s, at least one visit at t' is guaranteed along ω.

Continuing in this manner, we conclude that every $(3|S|)^{\rho(s)}$ consecutive visits at s along ω generate at least one visit at some state $u \in S_\rho^0$. Thus, if we terminate ω at the first time it reaches S_ρ^0, it follows that the total length of ω is at most

$$\sum_{s \in S_\rho} (3|S|)^{\rho(s)} \leqslant \sum_{s \in S_\rho} (3|S|)^{\max\rho} \leqslant (3|S|)^{\max\rho} \cdot |S| \leqslant (3|S|)^{\max\rho + 1}.$$

It therefore follows that the probability of ω is at least

$$((1/|S|)^{((3|S|)^{\max\rho + 1})}$$

(here we have used the very crude estimate that the probability of a single edge in H is at least $1/|S|$). We can even sharpen the bound just obtained, by noting that any ranking function ρ can have at most $|S|-1$ different nonzero values. We can therefore use the preceding inductive argument at most $|S|-1$ times, and thus we can replace $\max \rho + 1$ in the above formula by $|S|$. Thus, if we define

$$\alpha = |S|^{(-(3|S|)^{|S|})} > 0,$$

it follows that, for any universal ranking function ρ, the probability of reaching S_ρ^0 from any ρ-ranked state in H, is at least α, as asserted. Q.E.D.

The two preceding propositions 4.7 and 4.8 will next be used to show that the tree H generated by our schedule σ is indeed a Hintikka structure for the formula p_0. This will be a consequence of the following sequence of lemmas:

LEMMA 4.9. *Let h_n be a finite history in H such that $r \equiv p\exists \mathbf{U} q \in s_n$. Then there exists a finite path from s_n to some state t with $q \in t$ which visits only states s with $r \in s$ (and thus also $p \in s$).*

Proof. Define an existential ranking function ρ on the set $S_\rho = \{s \in S: r \in s\}$ as follows. If $q \in s$ then put $\rho(s) = 0$; otherwise, for each $s \in S_\rho$, let $\rho(s)$ be the length of the shortest path from s to S_ρ^0 which contains only states in S_ρ (by the length of such a path we mean the number of states lying on it, excluding the last such state). Note that all states $s \in S_\rho$ will get a finite rank, for otherwise they would have been marked by rule (M5). It is easily checked that ρ is indeed an existential ranking function. Indeed, condition (i) is trivial. To satisfy condition (ii), note that if $s \in S_\rho - S_\rho^0$, then $q \notin s$, so that s must contain the formula $\exists \mathbf{X} r$ and consequently $X(s)$ will contain a pre-state η inheriting r. It follows that this η satisfies condition (ii). Condition (iii) is immediate (because all states in S_ρ have finite rank). Concerning (iii'), note that if $s \in S_\rho$ and $|X(s)| = 1$ then the only $\exists \mathbf{X}$ formula in s is $\exists \mathbf{X} r$, hence in particular no formula of the form $\exists \mathbf{G} w$ belongs to s; thus $s \in E_0$, which implies that for the sole member $\xi \in X(s)$ we have $V(s, \xi) = T(\xi)$, so that (iii') holds. The lemma is then an immediate corollary of Proposition 4.7. Q.E.D.

LEMMA 4.10. *Let h_n be a finite history in H such that $r \equiv \exists \mathbf{G} p \in s_n$. Then there exists a finite path ω from s_n to some state $t \in E(r) \equiv U\{E_e: E_e$ an r-ergodic set$\}$, which visits only states s with $r \in s$ (and thus also $p \in s$).*

Proof. As in the preceding lemma, we define an existential ranking function ρ on the set $S_\rho = \{s \in S: r \in s\}$, so that, for each such s, $\rho(s)$ is the length of the shortest path which never leaves S_ρ, from s to some state

$t \in E(r)$ (in particular all states in $E(r)$ get rank 0). As in the preceding lemma, one easily checks that conditions (i), (ii), and (iii) are satisfied. Concerning condition (iii'), note that if $s \in S_\rho$ is such that $X(s)$ contains a single pre-state ξ, then either $s \in E_0$, in which case $V(s, \xi) = T(\xi)$, or s belongs to some r-ergodic set, in which case $\rho(s) = 0$, or s belongs to some E_e which is w-ergodic for some $w \neq r$ but not r-ergodic. But then s contains the two $\exists\mathbf{G}$ formulae r and w, so that it must have at least two succeeding pre-states, contrary to assumption. As before, the lemma now follows immediately from Proposition 4.7. Q.E.D.

LEMMA 4.11. *Let h_n be a finite history in H such that $r \equiv \exists\mathbf{G}p \in s_n$. Then there exists a finite path ω from s_n to some state $t \in E_e$, where E_e is some r-ergodic set, which visits only states s with $r \in s$ (and thus also $p \in s$), and such that the probability of never leaving E_e after t is positive.*

Proof. Consider the set Λ of all paths ω starting at s_n and satisfying

(1) If ω has reached a state t following a case (a) action of the schedule, such that t does not belong to an r-ergodic set, apply the preceding Lemma 4.10 to obtain a path ω' leading from t to some r-ergodic set and visiting only states containing r. Then ω continues after t as ω', until such an ergodic set is reached.

(2) If ω has reached some state $t \in E_e$, for some r-ergodic set E_e, such that the visit at t is the *first* square visit after s_n, then ω continues with the prestate in $X(t)$ corresponding to $\exists\mathbf{X}r$. Call this visit the "special" visit at t.

(3) For each state t as in (2) which also satisfies $|X(t)| > 1$, and at each *subsequent* square visit (of order τ^2) at t following the "special" visit, the last τ preceding visits at t along ω are such that they are not all followed by the same pre-state.

Note that Λ is not empty (in cases (1) and (2), the continuation after t is explicitly stated; in case (3) choose, for example, at visit number v at t the pre-state number $v \pmod 2$ in $X(t)$). Moreover, each path $\omega \in \Lambda$ never leaves the set $R = \{s \in S: r \in s\}$. Indeed, suppose that for some $m \geqslant n$, $s_m \in \omega$ belongs to R. Assume first that $s_m \in E_e$ for some r-ergodic set E_e. If the schedule choice of a state at the pre-state following s_m along ω is of type (b), then by definition s_{m+1} will also belong to E_e, hence to R. If, on the other hand, the schedule's choice at ξ is of type (a), then condition (2) above ensures that $s_{m+1} \in R$ if the current visit at s_m is the first visit (i.e., the special one), and condition (3) above ensures that a case (a) choice cannot occur later on along ω for the pair s, ξ. Finally, if s_m does not belong to any r-ergodic set, then it must lie on a subpath ω' as in condition (1) above, and the preceding Lemma 4.10 guarantees that s_{m+1} belongs to R too.

(The reason for distinguishing the first (special) square visit at a state s from subsequent square visits, is that the schedule's choice at the pre-state following the special visit may depend on part of the past history h_n (i.e., before reaching s_n), over which we have no control. We therefore choose a "safe" pre-state following the special visit, thus ensuring that we remain in R. After that special visit we are in full control over the construction of a path in Λ, as reflected in condition (3)).

The number of special visits as in condition (2) is at most $|S|$ (at most one such visit per state), so that there exists $\omega \in \Lambda$ containing the maximal number of such special visits. Thus, after advancing some finite number of steps along ω, we reach a state u such that all paths in Λ which continue from u onwards do not contain a special visit beyong that point. Let t be the first state along one of these paths which belongs to some r-ergodic set E_e (which exists by condition (1)). Then, after reaching that t, we have, for each $s \in E_e$:

$$\textbf{Prob}\,(E_e \text{ is left (immediately) following a visit at } s)$$

$$\leqslant \sum_{v=v_0+1}^{\infty} \textbf{Prob}\,(E_e \text{ is left immediately after visit number } v^2 \text{ at } s)$$

(where $v_0^2 \geqslant 9$ is the special visit at s after s_n)

$$\leqslant \sum_{v=4}^{\infty} d \cdot \left(\frac{1}{d}\right)^v$$

(where $d = |X(s)|$; note that $(1/d)^v$ is the probability that the same pre-state in $X(s)$ has been chosen at the last v preceding visits at s)

$$= \sum_{v=4}^{\infty} \left(\frac{1}{d}\right)^{v-1} \leqslant \sum_{v=4}^{\infty} \left(\frac{1}{2}\right)^{v-1} = \frac{1}{4}.$$

(The last inequality follows since $d \geqslant 2$, because only at states having more than one succeeding pre-state can E_e be left.) The estimate just given is valid because the only way to exit E_e after t is to choose at some state $s \in E_e$ the same pre-state for v consecutive visits preceding a square visit of order v^2 at s; this is because no special visits of type (2) can occur after t.

Thus, after reaching t, the probability of never leaving E_e immediately after a particular $s \in E_e$ is at least $\frac{3}{4}$. Moreover, the events of leaving E_e immediately after visits at different states $s \in E_e$ are independent, because they depend on disjoint sets of randomizations, thus their complementing events are also independent, leading to

$$\textbf{Prob}\,(E_e \text{ never left after } t) \geqslant (\tfrac{3}{4})^{|E_e|} \geqslant (\tfrac{3}{4})^{|S|} > 0$$

and this proves the lemma. Q.E.D.

LEMMA 4.12. *Let h_n be a finite history in H such that $r \equiv \forall \mathbf{F} p \in s_n$. Then the probability of reaching after s_n a state in $R \equiv \{s \in S: p \in s\} \cup E_0^c$ is $\geqslant \alpha$, where α is the positive constant given in Proposition* 4.8.

Proof. We define a universal ranking function ρ on the set $S_\rho = \{s \in S: r \in s\}$, so that, for each $s \in S_\rho$ we let $\rho(s)$ be the length of the shortest path from s to a state in R which visits only states in S_ρ (such a path exists since rule (M5) did not mark s). To see that ρ is indeed a universal ranking function, note that $S_\rho - S_\rho^0 \subset E_0$, hence for all $s \in S_\rho - S_\rho^0$ and all $\xi \in X(s)$ we have $r \in F_\xi$ and $V(s, \xi) = T(\xi) \subset S_\rho$. The lemma now follows immediately from Proposition 4.8. Q.E.D.

LEMMA 4.13. *Let h_n be a finite history in H such that $r \equiv \forall \mathbf{F} p \in s_n$, and suppose that $s_n \in E_e$ for some $e > 0$. Then the probability of reaching after s_n a state in E_e containing p is $\geqslant \alpha$.*

Proof. As in the preceding lemma, we define a universal ranking function ρ on the set $S_\rho = \{s \in E_e: r \in s\}$, so that, for each $s \in S_\rho$ we let $\rho(s)$ be the length of the shortest path from s to a state containing p which only visits states in E_e (recall condition (E3) in the definition of ergodic sets). The definition of $V(s, \xi) = T(\xi) \cap E_e$ together with the fact that E_e is an ergodic set, readily imply that ρ is indeed a universal ranking function. The lemma then follows from Proposition 4.8. Q.E.D.

LEMMA 4.14. *Let h_n be a finite history in H such that $r \equiv \forall \mathbf{F} p \in s_n$. Then the probability of reaching after s_n a state in $Q = \{s \in S: p \in s\}$ is at least α^2.*

Proof. Let α_1 be the probability of reaching after s_n an ergodic set before reaching Q. Now

$$\begin{aligned}&\textbf{Prob}\ (Q \text{ reached})\\ &\quad = \textbf{Prob}\ (Q \text{ reached before an ergodic set})\\ &\qquad + \textbf{Prob}\ (Q \text{ reached after an ergodic set}).\end{aligned}$$

By Lemma 4.12, the first term is at least $\alpha - \alpha_1$, and by Lemma 4.13, the second term is at least $\alpha_1 \alpha$. Thus the total probability is $\geqslant (\alpha - \alpha_1) + \alpha_1 \alpha \geqslant \alpha^2$. Q.E.D.

COROLLARY 4.15. *Let h_n be a finite history in H such that $t \equiv \forall \mathbf{F} p \in s_n$. Then the probability of reaching after s_n a state in $Q = \{s \in S: p \in s\}$ is* 1.

Proof. This is a direct consequence of the zero-one law applied to the preceding Lemma 4.14 (see, e.g., Theorem 2.3 in Hart and Sharir, 1985). We will sketch the argument here. Let $0 < \beta < \alpha^2$; Lemma 4.14 implies that

there exists an integer m (depending on h_n) such that a state in Q is reached within no more than m steps from h_n, with probability at least β. The current state after these m steps, if Q has not been reached, must contain our formula r; we can continue from it by applying the same argument, and so on. The total probability of reaching Q will thus be no less than

$$\beta + (1-\beta)\,\beta + (1-\beta)^2\,\beta + \cdots$$

which equals 1. Q.E.D.

As a result of the preceding sequence of lemmas, we finally conclude

THEOREM 4.16. *H is a Hintikka structure for p_0. Thus p_0 is satisfiable.*

Proof. It is easily seen that H satisfies conditions (H0)–(H3), (H4a), (H4b), and (H4d). Lemma 4.9 implies that it satisfies condition (H4c); Corollary 4.15 implies that it satisfies condition (H4e); and Lemma 4.11 implies that H satisfies condition (H4f). Q.E.D.

We have thus shown that if the root of **T** has not been marked then p is satisfiable. The converse statement is proven in the following section.

Remark. The tableau construction and its associated decision procedure described in this section is for the more complex logic PTL_b. As argued in Sections 2 and 3, we can obtain a decision procedure for formulae p_0 of PTL_f, by first rewriting p_0 as a nonprobabilistic formula, replacing all terms of p_0 of the form $\forall\mathbf{F}p$ and $\exists\mathbf{G}p$ by the appropriate right-hand side of the axiom (A3) or of its contrapositive form, and continuing this process until p_0 is reduced to an equivalent formula p_1 involving only the modalities $\forall\mathbf{X}$, $\exists\mathbf{X}$, $\forall\mathbf{U}$, and $\exists\mathbf{U}$. Then, to decide satisfiability of p_1, use the tableau method described above (which in this case would essentially coincide with the tableau techniques for the non-probabilistic logics *CTL* and *UB*).

5. COMPLETENESS

In this section we prove the second part of Theorem 4.5, namely that if the root n_0 of the tableau **T** constructed for a formula p_0 of PTL_b is marked by the procedure described in the preceding section, then $\sim p_0$ is provable from the axioms of PTL_b given in Section 3. This, together with the proof of the first part of Theorem 4.5, will establish the completeness of our deductive system. In the case of PTL_f, the same arguments to be used below still apply (they become simpler, since one does not have to deal with $\forall\mathbf{F}$ and $\exists\mathbf{G}$). Of course, as noted above, an alternative proof of com-

pleteness will follow from the fact that formulas of PTL_f may be re-expressed in terms of the non-probabilistic logics *CTL*, *UB*, and from the corresponding completeness proofs for these logics.

As in Ben–Ari, Pnueli, and Manna (1983) we define, for each node $n \in T$, the *associated formula* af_n of n to be $\vee.\{\sim p: p \in F_n\}$; note that $af_{n_0} = \sim p_0$. The proof proceeds by showing, using induction on the phases of the marking procedure, that if n is a marked node, then af_n is provable. Since we assume that n_0 is marked, it follows that $\sim p_0$ is provable.

The basis for our induction are phases which mark nodes n using the rule (M1). In these cases we obtain, using "dilution" as in Lemma 5.1 of Ben–Ari, Pnueli, and Manna (1983), that $\vdash af_n$. Similarly, for phases which mark nodes n using one of the rules (M2)–(M4), we can show, as in Lemma 5.2 of Ben–Ari, Pnueli, and Manna (1983), that $\vdash af_n$. For the rules (M2) and (M3) (corresponding respectively to α and β expansions) this follows from simple propositional reasoning and from the fact that each of the expansions listed in Tables I and II of Section 4 is a theorem of PTL_b. For the rule (M4) (corresponding to X-expansions) the proof proceeds exactly as in Ben–Ari, Pnueli, and Manna (1983), using rule (R1′) and theorem (T1).

Next consider a marking phase which has applied rule (M5) to a formula $r = p\exists \mathbf{U} q$. Let t be a state in $\mathbf{T}$ which has been marked by (M5). (Note that it suffices to consider states only. Indeed, let n be any node which is marked by this application of (M5). Suppose first that n is a node where r is expanded. Then the non-essential son of n must have already been previously marked—otherwise (M5) would not apply to n. It therefore follows that every state t reachable from n by α and β expansions only must also have been marked by the present application of (M5). But then, assuming we have already shown $\vdash af_t$ for each such state t, then the properties of rules (M1)–(M3) stated above make it plain that one also has $\vdash af_n$. This remark also applies to the remaining cases of marking by (M5) and by (M6).)

In what follows we will ignore the marked portion of $\mathbf{T}$ (before the current application of (M5)), and assume that each node we refer to is presently unmarked. Let us introduce the following terminology: For each state $u \in S$ such that $r \in F_u$, denote the r-son of u by η_u, and put $R(u) = T(\eta_u)$ (i.e., the *states* following η_u). Also put $R^* = R^*(t) = \bigcup_{m=0}^{\infty} R^m(t)$; in other words, $R^*(t)$ is the set of all states reachable from t along an r-acceptable path. Note that each state in R^* will be marked by the current application of (M5) (otherwise t would not have been marked either); the same argument also shows that we have $\exists \mathbf{X} r \in F_u$ for each state u in R^*, and thus η_u is well defined. For each $u \in R^*$ define $V(u)$ to be the set of (presently unmarked) nodes at which r is expanded, which are reachable from η_u by α and β expansions only (i.e., before a state in $R(u)$).

Note that the essential son v_1 of any $v \in V(u)$ has already been marked, for otherwise v, and consequently also u and t, would not have been marked by (M5). For each $v \in V(u)$, define $Q(v)$ to be the set of unmarked states reachable from v (or from the nonessential son v_2 of v) by α and β expansions only. Note that $Q \circ V = R$ for all $u \in R^*$. Also denote, for each state $u \in R^*$,

$$Y_u = \{k: \forall \mathbf{X} k \in F_u\}$$

and

$$W^t = \bigvee_{u \in R^*} \left(\bigwedge Y_u\right),$$

where we will always write $\bigwedge Y = \bigwedge \{k: k \in Y\}$ for any set of formulas Y. These formulae have the following properties, generalizing Lemmas 5.3 and 5.4 of Ben-Ari, Pnueli, and Manna (1983):

LEMMA 5.1. $\vdash W^t \supset \sim p \vee \sim q$.

Proof. Let $u \in R^*$. Note that $F_{\eta_u} = \{r\} \cup Y_u$. Let $v \in V(u)$. Since none of the α or β expansions performed between η_u and v did involve r, we can write $F_v = \{r\} \cup Z_v$, where Z_v is the set of formulae in F_v into which formulae in Y_u have expanded. Moreover, since each of these expansions corresponds to a theorem of PTL_b, it follows that

$$\vdash \bigwedge Y_u \supset \bigvee_{v \in V(u)} \left(\bigwedge Z_v\right). \tag{U1}$$

However, as already noted, for each $v \in V(u)$, the essential $\exists\mathbf{U}$-son v_1 of v must have been marked by a previous marking phase, so that, by our induction on the marking steps, it follows that $\vdash af_{v_1}$, or

$$\vdash (\sim p) \vee (\sim q) \vee \left(\sim \bigwedge Z_v\right)$$

or

$$\vdash \bigwedge Z_v \supset (\sim p) \vee (\sim q),$$

for each $v \in V(u)$. Thus also

$$\vdash \bigvee_{v \in V(u)} \left(\bigwedge Z_v\right) \supset (\sim p) \vee (\sim q),$$

and by (U1) we obtain that

$$\vdash \bigwedge Y_u \supset (\sim p) \vee (\sim q)$$

holds for each $u \in R^*$, thus

$$\vdash \bigvee_{u \in R^*} \left(\bigwedge Y_u \right) \supset (\sim p) \vee (\sim q),$$

as asserted. Q.E.D.

LEMMA 5.2. $\vdash p \wedge W^t \supset \forall \mathbf{X} W^t$.

Proof. Let $u \in R^*$. By the implication (U1) given in the preceding proof, we have

$$\vdash p \wedge \left(\bigwedge Y_u \right) \supset p \wedge \left(\bigvee_{v \in V(u)} \left(\bigwedge Z_v \right) \right) \tag{U2}$$

that is,

$$\vdash p \wedge \left(\bigwedge Y_u \right) \supset \bigvee_{v \in V(u)} \left(p \wedge \left(\bigwedge Z_v \right) \right). \tag{U2'}$$

Let $v \in V(u)$. The nonessential $\exists \mathbf{U}$-son v_2 of v satisfies

$$F_{v_2} = \{ p, \exists \mathbf{X} r \} \cup Z_v.$$

Since $\exists \mathbf{X} r$ is not expanded at any of the nodes connecting v_2 to $Q(v)$, it follows, as in (U1), that

$$\vdash p \wedge \left(\bigwedge Z_v \right) \supset \bigvee_{w \in Q(v)} \left(\bigwedge_{k \in Y_w} \forall \mathbf{X} k \right),$$

because these formulae are part of F_w. Hence

$$\vdash \bigvee_{v \in V(u)} \left(p \wedge \left(\bigwedge Z_v \right) \right) \supset \bigvee_{w \in R(u)} \left(\bigwedge_{k \in Y_w} \forall \mathbf{X} k \right)$$

so that, by (T1) and (R0), we have

$$\vdash \bigvee_{v \in V(u)} \left(p \wedge \left(\bigwedge Z_v \right) \right) \supset \bigvee_{w \in R(u)} \forall \mathbf{X} \left(\bigwedge Y_w \right).$$

Combining this with (U2'), we get

$$\vdash p \wedge \left(\bigwedge Y_u \right) \supset \bigvee_{w \in R(u)} \left(\forall \mathbf{X} \left(\bigwedge Y_w \right) \right).$$

Since this holds for each $y \in R^*$, we obtain

$$\vdash p \wedge \left(\bigvee_{u \in R^*} \left(\bigwedge Y_u \right) \right) \supset \bigvee_{\substack{u \in R^* \\ w \in R(u)}} \left(\forall \mathbf{X} \left(\bigwedge Y_w \right) \right)$$

$$\supset \bigvee_{w \in R^*} \left(\forall \mathbf{X} \left(\bigwedge Y_w \right) \right) \supset \forall \mathbf{X} \left(\bigvee_{w \in R^*} \left(\bigwedge Y_w \right) \right)$$

(the final implication being a consequence of (T2)). We have thus shown

$$\vdash p \wedge W^t \supset \forall \mathbf{X} W^t$$

as asserted. Q.E.D.

We can now show that $\vdash af_t$, as follows. Note that $F_{\eta_t} = \{r\} \cup Y_t$. Thus $af_{\eta_t} = \sim r \vee \sim (\wedge Y_t)$. We have, by Lemmas 5.1 and 5.2,

$$\vdash W^t \supset \sim p \vee \sim q,$$

$$\vdash W^t \supset \sim p \vee (\forall \mathbf{X} W^t).$$

Hence

$$\vdash W^t \supset \sim p \vee (\sim q \wedge \forall \mathbf{X} W^t),$$

or, using (R2),

$$\vdash W^t \supset (\sim q) \, \forall \mathbf{U} (\sim p).$$

Hence we also have

$$\vdash \bigwedge Y_t \supset \sim (p \exists \mathbf{U} q)$$

or

$$\vdash \sim \left(\bigwedge Y_t \right) \vee \sim r$$

that is, $\vdash af_{\eta_t}$. Hence af_t too, as follows from the inductive step of our proof corresponding to the marking rule (M4).

Next consider a marking phase which has applied rule (M5) to a formula $r = \forall \mathbf{F} p$, and let t be a state which has been marked by this phase. In a similar manner to what we did above for formulae involving $\exists \mathbf{U}$, we denote by $R^* = R^*(t)$ the set of all (presently unmarked) states reachable from t along r-acceptable paths (i.e., by choosing at each state u the r-son of u, also to be denoted as η_u). Again, since t has been marked at this phase, no

state in R^* has been ranked, so that it must contain both $\forall \mathbf{X} r$ and $\exists \mathbf{X} r$. In other words, at each node v where r has been expanded, the essential $\forall \mathbf{F}$-son of v must have been previously marked. We will also use the notations $R(u)$, $V(u)$, $Q(v)$ as above, each of which is defined in an obviously modified manner. Also put

$$Y_u = \{k: \forall \mathbf{X} k \in F_u \text{ and } k \neq r\}$$

$$W^t = \bigvee_{u \in R^*} \left(\bigwedge Y_u \right)$$

These formulae have the following properties:

LEMMA 5.3. $\vdash W^t \supset \sim p$.

Proof. Let $u \in R^*$. Note that $F_{\eta_u} = \{r\} \cup Y_u$. As before, for each $v \in V(u)$ we can write $F_v = \{r\} \cup Z_v$, where Z_v is the set of formulae in F_v into which formulae in Y_u have expanded. Moreover, since each of the expansions performed along the path from η_u to v corresponds to a theorem of PTL_b, it follows that

$$\vdash \bigwedge Y_u \supset \bigvee_{v \in V_u} \left(\bigwedge Z_v \right). \tag{F1}$$

However, at each $v \in V(u)$, the formula r was expanded. Since the essential $\forall \mathbf{F}$-son v_1 of v has been marked by a previous marking phase, it follows from our induction on the marking steps that $\vdash af_{v_1}$, or

$$\vdash (\sim p) \vee \left(\sim \bigwedge Z_v \right)$$

or

$$\vdash \bigwedge Z_v \supset \sim p,$$

for each $v \in V_u$. Thus also

$$\vdash \bigvee_{v \in V(u)} \left(\bigwedge Z_v \right) \supset \sim p,$$

or, using (F1),

$$\vdash \bigwedge Y_u \supset \sim p.$$

This however implies that

$$\vdash \bigvee_{u \in R^*} \left(\bigwedge Y_u \right) \supset \sim p$$

from which we obtain

$$\vdash W^t \supset \sim p$$

as asserted. Q.E.D.

LEMMA 5.4. $\vdash W^t \supset \forall \mathbf{X} W^t$.

Proof. Let $u \in R^*$. At each $v \in V(u)$ the formula r is expanded, and the essential $\forall \mathbf{F}$-son v_1 of v has been marked in a previous stage, but v is yet unmarked. Thus its nonessential son v_2 is unmarked, and we have

$$F_{v_2} = Z_v \cup \{\forall \mathbf{X} r, \exists \mathbf{X} r\}.$$

Continuing with these expansions until we reach a state w (in $Q(v) \subset R(u)$), and observing that $\forall \mathbf{X} r$ and $\exists \mathbf{X} r$ will not be expanded any more, we obtain, using (F1),

$$\vdash \bigwedge Y_u \supset \bigvee_{w \in R(u)} \left(\bigwedge (F_w - \{\forall \mathbf{X} r, \exists \mathbf{X} r\}) \right).$$

But

$$\vdash \bigwedge (F_w - \{\forall \mathbf{X} r, \exists \mathbf{X} r\}) \supset \bigwedge_{k \in Y_w} \forall \mathbf{X} k.$$

Hence, using (T1),

$$\vdash \bigwedge (F_w - \{\forall \mathbf{X} r, \exists \mathbf{X} r\}) \supset \forall \mathbf{X} \left(\bigwedge Y_w \right).$$

Thus

$$\vdash \bigwedge Y_u \supset \bigvee_{w \in R(u)} \forall \mathbf{X} \left(\bigwedge Y_w \right)$$

or, taking disjunction,

$$\vdash W^t \supset \bigvee_{w \in R^*} \forall \mathbf{X} \left(\bigwedge Y_w \right)$$

and finally, using (T2), we obtain

$$\vdash W^t \supset \forall \mathbf{X}\left(\bigvee_{w \in R^*}\left(\bigwedge Y_w\right)\right) \supset \forall \mathbf{X} W^t$$

as asserted. Q.E.D.

Lemmas 5.3 and 5.4 together imply

$$\vdash W^t \supset (\sim p) \wedge \forall \mathbf{X} W^t$$

which, using (R2), imply that

$$\vdash W^t \supset (\sim p)\, \forall \mathbf{U}\, \mathbf{false}$$

which in turn implies (using the contrapositive form of (T8) and (R0))

$$\vdash W^t \supset \exists \mathbf{G} \sim p$$

that is

$$\vdash \sim\left(\left(\bigwedge Y_t\right) \wedge \forall \mathbf{F} p\right).$$

In other words, we have shown that $\vdash af_{\eta_t}$, from which, using the argument corresponding to the marking rule (M4), it follows also that $\vdash af_t$, which is what was to be shown.

Finally, we need to consider nodes at which the marking rule (M6) has been applied to some formula $r = \exists \mathbf{G} p$. This portion of the proof is the most complex, and is special to PTL_b, in the sense that all the other related logics (UB, CTL, PTL_f) have no similar marking rule for $\exists \mathbf{G} p$.

Let $t \in S$ be a state that has been marked by (M6) for the formula r. Let $\Gamma(t)$ denote the set of all pre-states reachable from t along paths each of whose *states* contain r. Let $R^*(t) = \{t\} \cup T[\Gamma(t)]$. (Recall the notations introduced when (M6) was defined at Section 4; for a state s, $X(s)$ is the set of its sons (pre-states); for a pre-state ξ, $T(\xi)$ is the set of states reachable from ξ by α and β expansions only.)

Applying rule (M6) for t and r, we decompose $\Gamma(t)$ into finitely many disjoint sets $H_1 \cup H_2 \cdots \cup H_m$, and obtain a similar decomposition of $R^*(t)$ into $I_0 \cup I_1 \cup \cdots \cup I_m \cup L_1 \cdots \cup L_m$ where I_0 is the set of all states in $R^*(t)$ which do not contain r, where each of the sets $I_1, \ldots, I_m$ is either empty or a communicating but nonergodic set of states (i.e., satisfies (E1) and (E2), but not (E3)), and where $L_1, \ldots, L_m$ are "transition sets" of states satisfying

$$s \in L_j \Leftrightarrow T^{-1}(s) \in H_j, \qquad s \notin I_0, \qquad \text{and} \qquad X(s) \cap K_{j-1} \neq \varnothing$$

(recall that $L_1 = \varnothing$).

As already noted, since t has been marked by (M6), we must have, for each $j=1,\ldots,m$ either

(I) $I_j=\varnothing$; or

(II) $I_j\neq\varnothing$ and there exists some formula q such that for each $s\in I_j$, $\forall\mathbf{F}q\in F_s$ but $q\notin F_s$.

Before investigating both these cases, we begin with a few general observations and notations. For each $\xi\in\Gamma(t)$ we denote

$$Z_\xi=\bigwedge F_\xi$$

and for each $s\in R^*(t)$ we denote

$$Q_s=\bigwedge F_s.$$

Let $X(s)=\{\eta_1,\ldots,\eta_k\}$, and $Y_s=\{\gamma\colon \forall\mathbf{X}\gamma\in F_s\}$. This means that Q_s is a conjunction involving, among others, formulae of the form $\exists\mathbf{X}\beta_{\eta_1},\ldots,\exists\mathbf{X}\beta_{\eta_k}$, and also formulae of the form $\forall\mathbf{X}\gamma$, where $\gamma\in Y_s$, in the sense that for each $j=1,\ldots,k$ we have

$$F_{\eta_j}=Y_s\cup\{\beta_{\eta_j}\}.$$

Note also that we must have one j for which $\beta_{\eta_j}=\exists\mathbf{G}p$; we may assume $j=1$. We have

$$\vdash Q_s\supset\forall\mathbf{X}\left(\bigwedge Y_s\right)\wedge\exists\mathbf{X}\beta_{\eta_1}\wedge\cdots\wedge\exists\mathbf{X}\beta_{\eta_k}\tag{G1}$$

which leads to (using (A1))

$$\begin{aligned}\vdash Q_s\supset\forall\mathbf{X}\Big[&\left(\left(\bigwedge Y_s\right)\wedge\beta_{\eta_1}\right)\vee\left(\left(\bigwedge Y_s\right)\wedge\beta_{\eta_2}\right)\vee\cdots\\&\vee\left(\left(\bigwedge Y_s\right)\wedge\beta_{\eta_k}\right)\vee\left(\left(\bigwedge Y_s\right)\wedge\sim\beta_{\eta_1}\wedge\cdots\wedge\sim\beta_{\eta_k}\right)\Big]\\&\vee\exists\mathbf{X}\left(\left(\bigwedge Y_s\right)\wedge\beta_{\eta_k}\right).\end{aligned}\tag{G2}$$

But $\sim\beta_{\eta_1}\equiv\sim\exists\mathbf{G}p$, so that we can write (G2) as

$$\vdash Q_s\supset\forall\mathbf{X}(Z_{\eta_1}\vee Z_{\eta_2}\cdots\vee Z_{\eta_k}\vee\exists\mathbf{G}p)\wedge\exists\mathbf{X}Z_{\eta_1}\cdots\wedge\exists\mathbf{X}Z_{\eta_k}.\tag{G3}$$

Let us define, for each $j=1,\ldots,m$,

$$A_j=\bigvee_{\xi\in H_j}Z_\xi;\qquad B_j=\bigvee_{i\leqslant j}A_i.$$

Let us fix some $j = 1,..., m$, and consider both cases (I) and (II) listed above:

(I) $I_j = \varnothing$. In this case H_j must contain a single element ξ, and $T(\xi) \subset I_0 \cup L_j$.

LEMMA 5.5. *If I_j satisfies condition* (I) *then*

$$\vdash A_j = Z_\xi \supset \bigvee_{s \in T(\xi) \cap L_j} Q_s \vee \left[\bigvee_{s \in T(\xi) \cap I_0} (Q_s \wedge \sim \exists \mathbf{G} p) \right]. \qquad \text{(G4)}$$

Proof. Consider any node n lying between ξ and $T(\xi)$. If F_n contains $\exists \mathbf{G}p$, then all nodes following n up to $T(\xi)$ must contain $\exists \mathbf{G}p$, so that all states in $T(\xi)$ following n must belong to L_j. By construction of $\Gamma(t)$, F_ξ must contain either $\exists \mathbf{G}p$ itself, or else the disjunction $\mathbf{true} \vee \exists \mathbf{G}p$. In the first case, $T(\xi) \cap I_0$ is empty, so that (G4) follows from the fact that each α or β expansion done between ξ and $T(\xi)$ corresponds to a theorem of PTL_b. In the second case, for each node n between ξ and $T(\xi)$ at which $(\mathbf{true} \vee \exists \mathbf{G}p)$ has been expanded, let n_1 be the son of n which "inherits" $\exists \mathbf{G}p$ and let n_2 be the other son of n. It follows that $\wedge F_{n_1} = (\wedge F_n) \wedge \exists \mathbf{G}p$, and $\wedge F_{n_2} = (\wedge F_n) \wedge \mathbf{true} = \wedge F_n$, thus

$$\vdash \wedge F_n \supset \left(\bigwedge F_{n_1} \right) \vee \left(\left(\bigwedge F_{n_2} \right) \wedge \sim \exists \mathbf{G}p \right);$$

these implications are then easily seen to imply (G4). Q.E.D.

Remark. The above proof is the main place in which the redundant expansion rule for $\exists \mathbf{G}p$ is used. The intuitive reason for this redundancy is to make sure that for each pre-state ξ in the tableau which contains $\exists \mathbf{G}p$, this subformula is propagated to *all* its succeeding pre-states, so that each of them "gets a chance" to fulfill $\exists \mathbf{G}p$. Without this provision, we could run into situations in which the unwinding of the tableau from ξ may not generate a set of paths having *positive* probability on which p is always satisfied (although this set will not be empty). This case is illustrated in Example 3 given in Appendix A below.

For each $s \in T(\xi) \cap L_j$ there exists $\eta \in X(s) \cap K_{j-1}$, and moreover, by definition of $\Gamma(t)$ we have $X(s) \subset \Gamma(t)$. Thus, using (G3), we can write

$$\vdash Q_s \supset \forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G}p) \wedge \exists \mathbf{X} B_{j-1}. \qquad \text{(G5)}$$

It therefore follows from (G4) and (G5) that for I_j's satisfying (I) we have

$$\vdash A_j \supset [\forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G}p) \wedge \exists \mathbf{X} B_{j-1}] \vee \sim \exists \mathbf{G}p. \qquad \text{(G6)}$$

(II) $I_j \neq \varnothing$ and there exists a formula q for which $\forall \mathbf{F}q \in F_s$ and $q \notin F_s$ for each $s \in I_j$.

Let $\xi \in H_j$ be any pre-state. As in case (I) we claim

LEMMA 5.6. *If I_j satisfies condition* (II) *then*

$$\vdash Z_\xi \supset \bigvee_{s \in T(\xi) \cap I_j} (Q_s \wedge \sim q) \vee \left(\bigvee_{s \in T(\xi) \cap L_j} Q_s \right) \vee \left(\bigvee_{s \in T(\xi) \cap I_0} (Q_s \wedge \sim \exists \mathbf{G} p) \right). \tag{G7}$$

This is shown as in the proof of (G4). The appearance of $\sim q$ in conjunction with Q_s for $s \in I_j$ follows from the fact that at the node n along the path from ξ to s at which the $\forall\mathbf{F}$-expansion of $\forall\mathbf{F}q$ has taken place, q was inherited by the other son of n. Since one has $\forall\mathbf{F}q \supset q \vee (\sim q \wedge \forall\mathbf{X}\forall\mathbf{F}q)$, it follows that it is logically consistent to add $\sim q$ to the nonessential F-son of n, and hence eventually also to s (by a similar argument to that used for $\sim \exists \mathbf{G} p$ in the proof of Lemma 5.5).

It follows from (G7) that

$$\vdash A_j \supset \bigvee_{s \in I_j} (Q_s \wedge \sim q) \vee \left(\bigvee_{s \in L_j} Q_s \right) \vee (\sim \exists \mathbf{G} p). \tag{G8}$$

Using (G5), we can write this as

$$\vdash A_j \supset \bigvee_{s \in I_j} (Q_s \wedge \sim q) \vee w \tag{G9}$$

where

$$w = [\forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G} p) \wedge \exists \mathbf{X} B_{j-1}] \vee \sim \exists \mathbf{G} p.$$

(Note that the term in square brackets drops out for $j = 1$, since $L_1 = \varnothing$ by definition.) Moreover, for each $s \in I_j$ we have $X(s) \subset H_j$, so that by (G3) we have for each such s

$$\vdash Q_s \supset \forall \mathbf{X}(A_j \vee \sim \exists \mathbf{G} p). \tag{G10}$$

By the definition of w, we have $\sim \exists \mathbf{G} p \supset w$; from (G10),

$$\vdash Q_s \supset \forall \mathbf{X}(A_j \vee w)$$

for all $s \in I_j$. Substituting in (G9), we get

$$\vdash A_j \supset w \vee (\forall \mathbf{X}(A_j \vee w) \wedge \sim q) \tag{G11}$$

from which, using (R2), it is easy to obtain

$$\vdash A_j \vee w \supset (\sim q)\, \forall \mathbf{U} w$$

so that, in particular,

$$\vdash A_j \supset (\sim q)\,\forall \mathbf{U} w. \tag{G12}$$

However, since $\forall \mathbf{X}\forall \mathbf{F} q \in F_s$ for each $s \in I_j$, and since each $\xi \in H_j$ satisfies $X^{-1}(\xi) \cap I_j \neq \varnothing$ (cf. Corollary 4.4), it follows that $\forall \mathbf{F} q \in F_\xi$ for each $\xi \in H_j$, hence

$$\vdash A_j \supset \forall \mathbf{F} q \tag{G13}$$

which, together with (G12), implies by (A6)

$$\vdash A_j \supset \forall \mathbf{F}(\sim \exists \mathbf{G} p \vee [\forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G} p) \wedge \exists \mathbf{X} B_{j-1}]). \tag{G14}$$

Finally, since (G6) is a special case of (G14) by (A4), we conclude that (G14) holds for each $j = 1,..., m$. This implies

$$\vdash B_j \supset \bigvee_{i=1}^{j} \{\forall \mathbf{F}(\sim \exists \mathbf{G} p \vee [\forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G} p) \wedge \exists \mathbf{X} B_{i-1}])\}. \tag{G15}$$

But for each $i \leqslant j$ we have $\vdash B_{i-1} \supset B_{j-1}$. It follows from the contrapositive form of rule (R1′) and from rule (R6) that

$$\vdash B_j \supset \forall \mathbf{F}(\sim \exists \mathbf{G} p \vee [\forall \mathbf{X}(B_m \vee \sim \exists \mathbf{G} p) \wedge \exists \mathbf{X} B_{j-1}]) \tag{G16}$$

for each $1 < j \leqslant m$. For $j = 1$, the term in square brackets disappears, because L_1 is empty; in this case (G16) reduces to

$$\vdash B_1 \supset \forall \mathbf{F}(\sim \exists \mathbf{G} p) = \forall \mathbf{F} \forall \mathbf{F}(\sim p) \supset \forall \mathbf{F}(\sim p) \tag{G17}$$

by (A5).

LEMMA 5.7.

$$\vdash B_m \supset \forall \mathbf{F}(\sim p). \tag{G18}$$

Proof. Put $v = \sim \exists \mathbf{G} p$ and for each $j = 1,..., m$ put $C_j = B_j \vee v$. Since $B_j \supset C_j$ it follows from (G16) that

$$\vdash C_j \supset \forall \mathbf{F}(C_{j-1} \vee [\forall \mathbf{X} C_m \wedge \exists \mathbf{X} C_{j-1}]). \tag{G19}$$

We will show, using induction on j, that

$$\vdash C_j \supset \forall \mathbf{F} C_{j-1} \tag{G20}$$

from which, by repeated applications of (A5) and finally (G17), we easily obtain (G18). We begin to prove (G20) for $j = m$. From (G19) we obtain

$$\vdash C_m \supset \forall \mathbf{F}(C_{m-1} \vee [\forall \mathbf{X} C_m \wedge \exists \mathbf{X} C_{m-1}])$$

which, by (R7), yields (G20) for $j=m$. Suppose next that (G20) has already been established for all $k>j$; then it follows from (A5) that $C_m \supset \forall \mathbf{F} C_j$, so that (G19) becomes

$$\vdash C_j \supset \forall \mathbf{F}(C_{j-1} \vee [\forall \mathbf{X} \forall \mathbf{F} C_j \wedge \exists \mathbf{X} C_{j-1}])$$

from which we obtain, using (R7) again, that $C_j \supset \forall \mathbf{F} C_{j-1}$, as required. This proves our lemma. Q.E.D.

Having established (G18), let us next choose any pre-state $\xi \in T(t)$ such that $\exists \mathbf{G} p \in F_\xi$ (there are many such pre-states: for example, for each $s \in R'(t) = R(t) - I_0$, the son η_s of s corresponding to $\exists \mathbf{X} \exists \mathbf{G} p \in F_s$ is such a pre-state). For each such ξ we have

$$\vdash Z_\xi \supset B_m \supset \forall \mathbf{F}(\sim p)$$

and also

$$\vdash Z_\xi \supset \exists \mathbf{G} p$$

both of which formulae imply that

$$\vdash \sim Z_\xi$$

so that, by dilution,

$$\vdash af_\xi .$$

Thus, by the portion of the completeness proof corresponding to the marking rule (M4), it follows that $\vdash af_s$ for each $s \in R'(t)$, and in particular

$$\vdash af_t . \qquad \text{Q.E.D.}$$

This concludes our proof of completeness, for we have shown that the associated formula of each marked node is provable, and in particular $af_{n_0} \equiv \sim p_0$ is provable, which is what we wanted to show. Q.E.D.

6. Discussion

We have presented a probabilistic temporal logic for bounded models which, syntactically, is quite similar to nonprobabilistic temporal logics for branching time (*UB*, *CTL*). We have also given a deterministic single-exponential decision procedure for satisfiability in PTL_b, and have presented a complete axiomatization of this logic. Several additional consequences of our results deserve comment:

First, the arguments of Section 4 actually imply that PTL_b has the

FINITE PRE-MODEL PROPERTY: If a formula p of PTL_b is satisfiable, then there exists a finite set of states I (actually pre-states of the associated tableau), and for each $s \in I$ there is a finite collection $K(s)$ of probability distributions over I (one for each tableau state in $T(s)$) such that a model for p can be obtained by some "strategy" of choosing at each model state s, one of the distributions in $K(s)$; this adds all states (in I) in the support of that distribution as successors of s in the model.

This observation implies

PROPOSITION 6.1. *Let p be a formula of PTL_b. If p is satisfiable, then there exists an execution of a finite probabilistic concurrent program (i.e., having a finite state space and finitely many processes) which serves as a model for p (in the sense described in remark (6) of Sect. 2).*

Proof. Consider the tableau for p: For each pre-state ξ, let $l(\xi)$ be the number of states in $T(\xi)$; put $l = \max_\xi l(\xi)$, and $K = \{1, 2, ..., l\}$. For each ξ, let $\phi_\xi : K \to T(\xi)$ be an arbitrary map onto $T(\xi)$ (thus, with each $1 \leqslant k \leqslant l$ we associate one transition from ξ to a state $t \in T(\xi)$). The program is now defined as follows. The program states are the pre-states of the tableau; and there are l processes; for each process $k \in K$ and each program state ξ, execution of k at ξ results in the randomization (i.e., X-transitions) at the tableau state $\phi_\xi(k)$. The specific execution of this program which satisfies p is obtained in a manner similar to the unwinding of the tableau into a Hintikka structure for p in Section 4—whenever the tableau scheduler in Section 4 chooses a state s in $T(\xi)$ for some pre-state ξ, the corresponding program scheduler chooses a process $k \in K$ for which $\phi_\xi(k) = s$. It is clear that the resulting finite concurrent probabilistic program and its schedule yield an execution of the program which serves as a model for p. Q.E.D.

Together with the remarks made in Section 2 (see (6) there), this result implies that PTL_b serves as a proper tool to argue about executions of finite concurrent probabilistic programs. Indeed, it p is a formula of PTL_b which asserts some property about concurrent probabilistic programs, then either p is indeed provable in PTL_b, or else, by Proposition 6.1 applied to $\sim p$, we can construct a finite concurrent probabilistic program and produce a certain scheduling of its processes for which execution p does not hold. This observation also implies the following

COROLLARY. *Consider the class of concurrent probabilistic programs with (possibly) infinitely many states, finitely many processes and positive transition probabilities bounded away from zero. Let p be a property of an execution of such a program. If p is expressible in PTL_b and is satisfied by an execution of such a program, then p must also be satisfied by an execution of a finite (i.e., finite-state) program in this class.*

A second observation is that PTL_b does not have the *finite model* property. By this we mean that there exist satisfiable formulas of PTL_b, which however are not satisfied by any model of PTL_f. An example of such a formula is

$$r_3 = \forall \mathbf{G} \exists \mathbf{F} p \wedge \exists \mathbf{G} \sim p,$$

which is analyzed in the Appendix (see Example 3 there for the tableau construction and a proof of satisfiability of r_3 in PTL_b). In contrast, if one expands r_3 in PTL_f (using axiom (A3)), then it is easily checked that r_3 becomes unsatisfiable (in PTL_f, or, equivalently, in the corresponding nonprobabilistic logics *CTL* and *UB*).

A third observation on the results developed so far concerns the structure of the "schedule" used in Section 4 to construct a model from the tableau of a satisfiable formula p of PTL_b. As noted there, that schedule is generally not finitary. However, a close inspection of its definition shows that it needs to be nonfinitary only in cases where it enters some ergodic set E corresponding to some formula $\exists \mathbf{G} r$, and it has to ensure that it gets out of E at every possible "exit" from E with positive probability. However, the schedule really needs to exit E only if some states in E contain formulae of the form $\exists \mathbf{G} q$ (resp. $p \exists \mathbf{U} q$) which are not fulfilled inside E. In these cases the schedule must make sure that for each occurrence of such a node in the model there exists a path from that occurrence which reaches an ergodic set for $\exists \mathbf{G} q$ (resp. a state fulfilling q). In all other cases, there is no need for the schedule to leave E once it had been entered, and the schedule can then be replaced by a finitary schedule. When this is the case, the model that results from unwinding the tableau of p in this finitary fashion is equivalent to a finite Markov chain, so that although p is a formula of PTL_b, it is also satisfiable by a model of PTL_f.

The precise condition that p has to satisfy for this property to hold is somewhat complicated to state, since it depends on properties of the tableau of p. Nevertheless, a simple sufficient condition can be given:

DEFINITION. (a) A formula of PTL_b is said to be written in *canonical form* if it is either a proposition, the negation of a proposition, or has one of the forms $q \vee r$, $q \wedge r$, $\exists \mathbf{X} q$, $\forall \mathbf{X} q$, $q \exists \mathbf{U} r$, $q \forall \mathbf{U} r$, $\forall \mathbf{F} q$, $\exists \mathbf{G} q$, where q and r themselves are written in canonical form (in other words, negations are "pushed" inside arguments of logical operators as much as possible).

(b) A formula p of PTL_b is said to be *finitary*, if, when written in canonical form, it contains at most one subformula of the form $\exists \mathbf{G} q$, and, if it contains such a subformula, then it contains no subformulae of the form $r \exists \mathbf{U} s$.

Note that any formula p of PTL_b can be written in equivalent canonical

form, using some of the expansion rules given in Tables I and II of Section 4.

THEOREM 6.2. *Let p be a finitary formula of PTL_b. Then the following are equivalent:*

(a) *p is satisfiable by a model of PTL_b;*

(b) *p is satisfiable by a model of PTL_f;*

(c) *$\sim p$ is not provable in PTL_b;*

(d) *$\sim p$ is not provable in PTL_f.*

Proof. From the completeness of PTL_b and of PTL_f it follows that (a) $\Leftrightarrow$ (c), and (b) $\Leftrightarrow$ (d). It is also always the case that (d) $\Rightarrow$ (a). If p is finitary, then it is easily seen that only subformulae of the form $\exists \mathbf{G} q$ or $q\, \exists \mathbf{U} r$ which appear in the canonical form of p, can appear in nodes of the tableau. It then follows from the preceding remarks that if p is PTL_b-satisfiable, then one can construct a PTL_f-model for p from its tableau, which shows that (a) $\Rightarrow$ (b). Q.E.D.

As an application of this theorem, consider an assertion p about the termination of a finite probabilistic concurrent program. It will generally have the form (2.1) given in Section 2. It is easy to check that the negation of p contains in canonical form only one occurrence of an $\exists \mathbf{G}$ subformula, and no $\exists \mathbf{U}$ subformulae. Hence, Theorem 6.2 applies to $\sim p$, and implies that p is provable in PTL_b iff it is provable in PTL_f. This in turn implies that the program terminates almost surely under any fair schedule iff it terminates almost surely under any fair and finitary schedule. Although this property could be deduced directly from the results of Hart, Sharir, and Pnueli (1983), it is interesting to obtain it as a special case of a purely syntactic condition on formulae of our logics.

APPENDIX A: EXAMPLES

In this Appendix we present four examples of the application of our decision procedures to formulae of PTL_b. To display the corresponding tableaux in more compact and readable form, we use the following conventions and shortcuts: Only unexpanded formulae are shown at each node of the tableau; several successive α expansions are combined into a single expansion; closing of nodes is marked by X; pre-states are given numerical labels enclosed in circles, and states are given alphabetical labels enclosed in boxes; α and β expansions are denoted by dashed edges, while X expansions are denoted by solid edges (we use the convention that an essential

son is drawn as the left son). Several intermediate nodes are also given labels, when their associated set of formulae coincides with a set of a previously constructed node. In this case further expansion of the tableau past such a node is not shown, since it completely parellels the expansion of the preceding node. A node whose set of formulae coincides with that of a preceeding node is given a label of the form a', where a is the label given

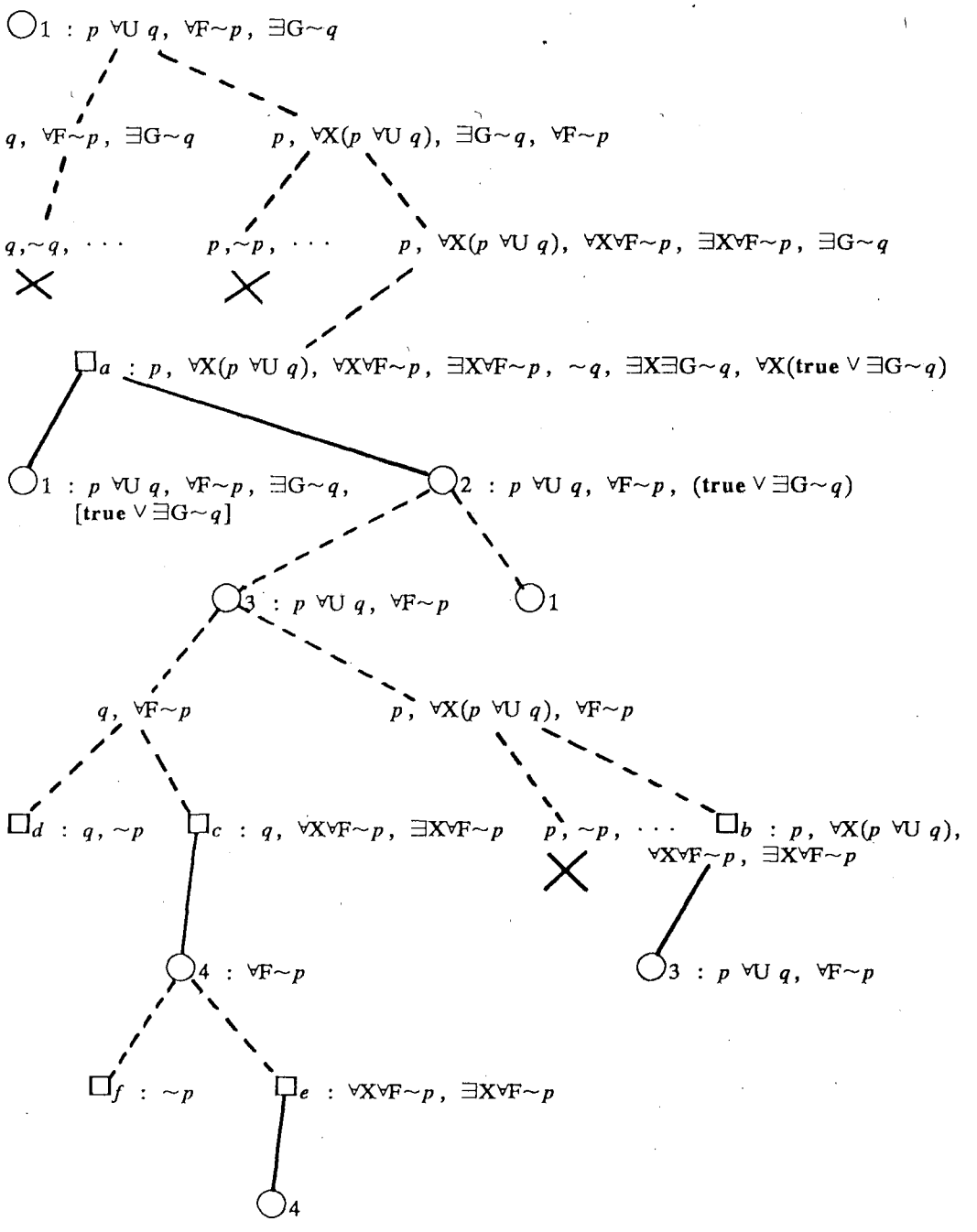

FIG. A.1. Construction of T_1.

to that preceeding node. Finally each tableau is displayed in two figures, the first of which gives the full construction, whereas the second figure gives a condensed form of the tableau, involving only pre-states and states and their X and T-relationships. (For convenience, we will label states s in this second compact representation of the tableau by propositions and their negations appearing in F_s, and also by $\forall\mathbf{F}$ and $\exists\mathbf{G}$ subformulae appearing in F_s.)

EXAMPLE 1. $r_1 = (p\ \forall\mathbf{U}q) \wedge \forall\mathbf{F} \sim p \wedge \exists\mathbf{G} \sim q$. This is the negation of the axiom (A6), and will be shown indeed to be unsatisfiable. The construction of the tableau $\mathbf{T}_1$ for r_1 is shown in Fig. A.1, and the condensed form of $\mathbf{T}_1$ is shown in Fig. A.2. Applying the marking rule (M5) to $\forall\mathbf{F} \sim p$, we note that this formula is "fulfilled" at states d, d', and f, and that from any other node of $\mathbf{T}_1$ one of these states can be reached. Hence, no node is marked by this rule. Next we apply rule (M6) to $k = \exists\mathbf{G} \sim q$. The relevant nodes are $S_k = \{a, a'\}$ and $Y = \{1, 2\}$. The decomposition yields

$$I_0 = \{b, c, d\}; \qquad H_1 = \{1, 2\}; \qquad I_1 = \{a, a'\}.$$

However, I_1 is not ergodic, because $\forall\mathbf{F} \sim p$ is contained in $F_a = F_{a'}$, but $\sim p$ is not contained in these sets. Hence, (M6) will mark the nodes a, a', 1, 2. Since the root of $\mathbf{T}_1$ has been marked, we conclude that r_1 is unsatisfiable.

EXAMPLE 2. $r_2 = \forall\mathbf{F}\forall p \wedge \exists\mathbf{G} \sim p$. This is the negation of axiom (A5), and will be shown to be unsatisfiable. The construction of the

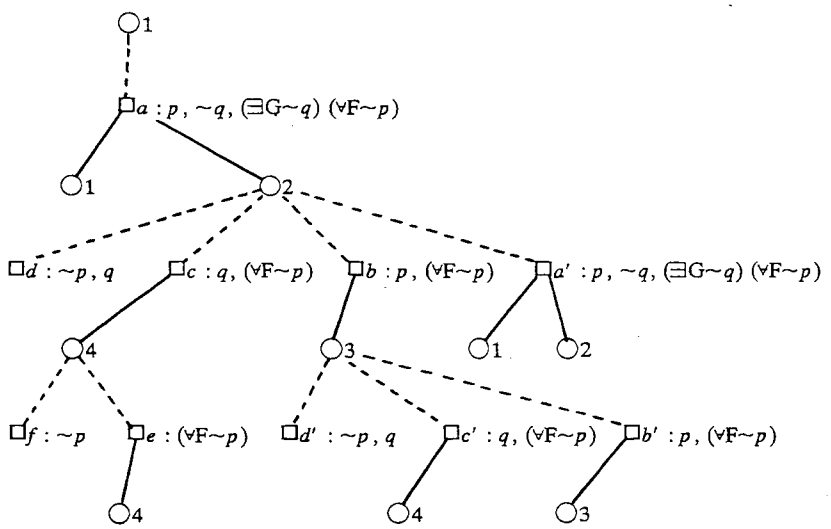

FIG. A.2. Compact form of $\mathbf{T}_1$.

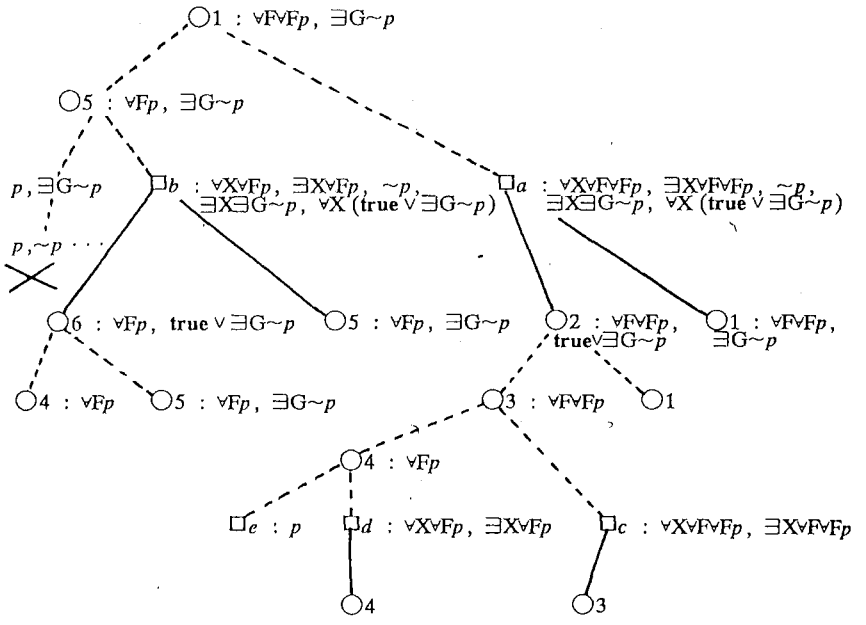

FIG. A.3. Construction of $\mathbf{T}_2$.

corresponding tableau $\mathbf{T}_2$ is shown in Fig. A.3, and its condensed form is shown in Fig. A.4. The subformula $\forall\mathbf{F}p$ is contained in nodes

$$4, 5, 6, b, b_1, b', b'_1, d, d_1, d_2, d', e, e_1, e_2, e'$$

and is fulfilled at states e, e_1, e_2, e'. It easily follows that rule (M5) applied to $\forall\mathbf{F}p$ does not result in any marking. Similarly, the subformula $\forall\mathbf{F}\forall\mathbf{F}p$ is fulfilled at all the states of the b, d, or e "type." Again, no node is marked from application of (M5) to this subformula.

Finally, consider rule (M6) applied to $k = \exists\mathbf{G} \sim p$. It is contained in the nodes

$$1, 2, 5, 6, a, a_1, b, b_1, b', b'_1.$$

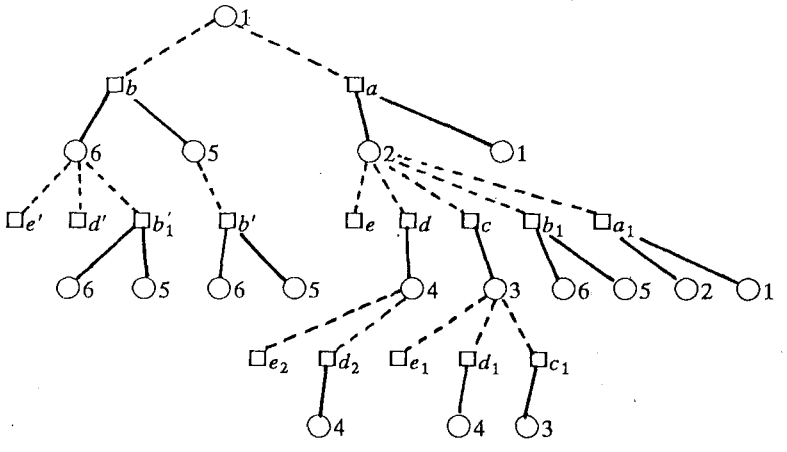

FIG. A.4. Compact form of $\mathbf{T}_2$.

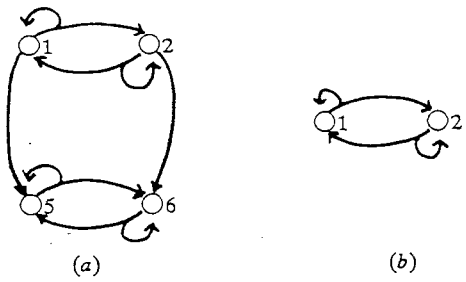

FIG. A.5. The transitions graphs used in (M6).

We first have

$$I_0 = \{c, d, d', e, e'\}.$$

The initial value of the transition graph used by the decomposition algorithm of (M6) is shown in Fig. A.5(a). It follows that

$$H_1 = \{5, 6\}; \qquad I_1 = \{b', b_1'\}.$$

The reduced transition graph used in the second decomposition step is shown in Fig. A.5(b), from which it follows that

$$H_2 = \{1, 2\}; \qquad I_2 = \{a, a_1\}; \qquad L_2 = \{b, b_1\}.$$

But neither of I_1, I_2 is ergodic, the first because of the nonfulfillment of $\forall \mathbf{F}p$, and the second because of the nonfulfillment of $\forall \mathbf{F} \forall \mathbf{F}p$. Hence, (M6) causes the root 1 to be marked, so that r_2 is unsatisfiable.

EXAMPLE 3. $r_3 = \forall \mathbf{G} \exists \mathbf{F}p \wedge \exists \mathbf{G} \sim p$ (for simplicity we shall use the auxiliary operators $\forall \mathbf{G}$, $\exists \mathbf{F}$ explicitly, instead of their implicit represen-

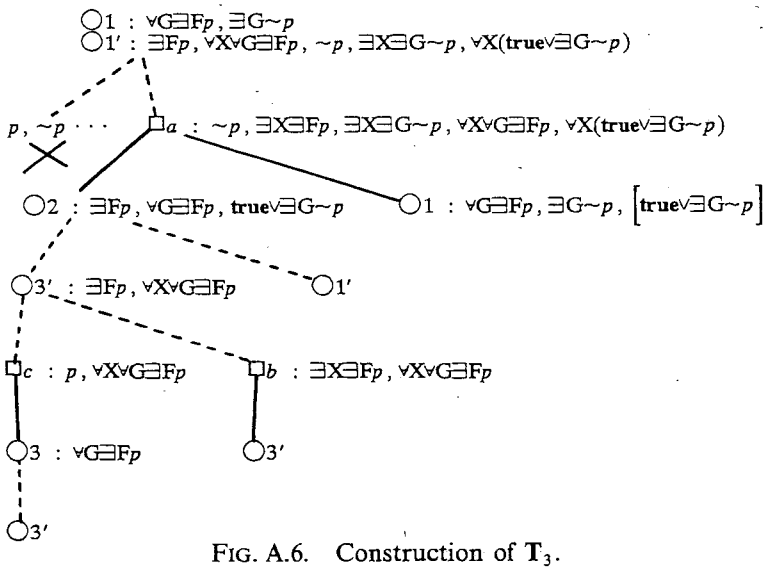

FIG. A.6. Construction of $\mathbf{T}_3$.

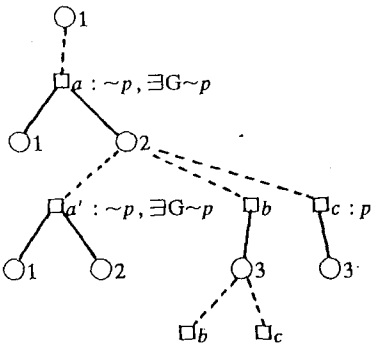

FIG. A.7. Compact form of $\mathbf{T}_3$.

tations by means of the operators $\forall\mathbf{U}$, $\exists\mathbf{U}$). The construction of the corresponding tableau $\mathbf{T}_3$ is given in Fig. A.6, and the condensed form of $\mathbf{T}_3$ is given in Fig. A.7. Since the subformula $\exists\mathbf{F}p$ is "fulfilled" at state c, and since c is reachable from any other node of $\mathbf{T}_3$, application of the marking rule (M5) results in no marking. Application of the rule (M6) to the subformula $q = \exists\mathbf{G} \sim p$ proceeds as follows: The set of relevant nodes is $\{1, 2, a, a'\}$. The decomposition as specified in (M6) gives

$$I_0 = \{b, c\}; \qquad H_1 = \{1, 2\}; \qquad I_1 = \{a, a'\}.$$

Since no subformulae of the form $\forall\mathbf{F}$ appear in r_3, the set I_1 is ergodic, and so no node needs to be marked by this rule. Hence r_3 is satisfiable. To obtain a model for r_3 from $\mathbf{T}_3$ we can use the following "scheduling" strategy for the unwinding of $\mathbf{T}_3$ (this scheduling is simpler than that given in Sect. 4, but has the disadvantage that it requires assignment of unequal probabilities to edges emerging from a common state):

At the pre-state 1, schedule the (only possible) state a.

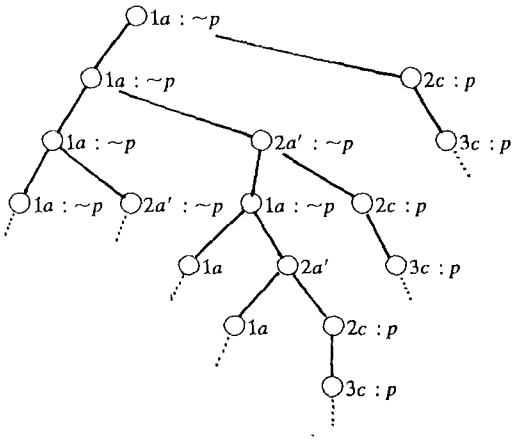

FIG. A.8. Unwinding $\mathbf{T}_3$ into a model for r_3.

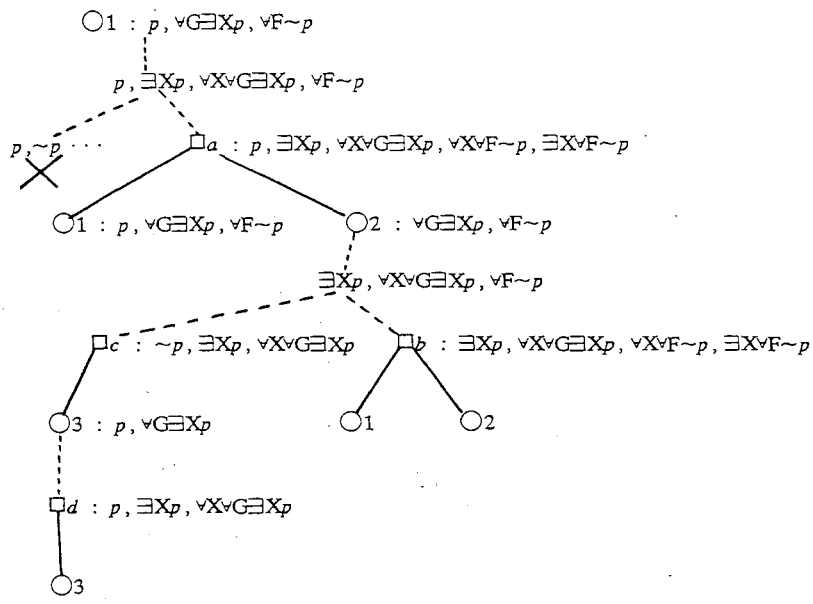

FIG. A.9. Construction of $\mathbf{T}_4$.

At the pre-state 2, schedule the state a' until the first time in which the number of visits at the pre-state 2 equals the number of visits at the pre-state 1, in which case schedule the state c.

At the pre-state 3 always schedule the state c.

The resulting model is shown in Fig. A.8. It essentially coincides with the behavior of a random walk on the non-negative integers with absorption at 0. This model will satisfy r_3 provided that we assign a probability $> \frac{1}{2}$ to the edges from a to 1 and from a' to 1. The reader is invited to check that if one expands subformulae of the form $\exists \mathbf{G} q$ as in the nonprobabilistic case (Ben–Ari, Pnueli, and Manna, 1983) as $q \wedge \exists \mathbf{X} \exists \mathbf{G} q$, then the modified tableau for r_3 would be such that no model for r_3 could be obtained by its unwinding.

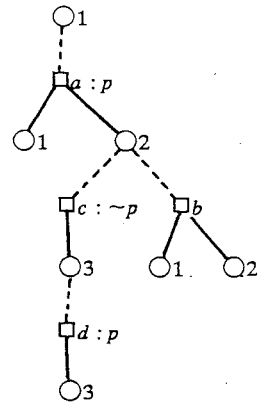

FIG. A.10. Compact form of $\mathbf{T}_4$.

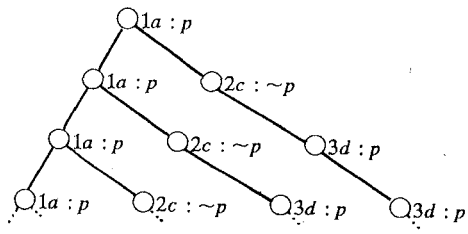

FIG. A.11. Unwinding $\mathbf{T}_4$ into a model for r_4.

Remark. The formula r_3 is also satisfiable in the nonprobabilistic logic *UB* of Ben-Ari, Pnueli, and Manna (1983) (with the standard nonprobabilistic interpretation of the operator $\exists\mathbf{G}$) by a smaller and simpler tableau. However, as noted in Section 6, r_3 is unsatisfiable in PTL_f. Thus, rewriting it using axiom (A3), we obtain a formula which is unsatisfiable in any of the logics PTL_f, *CTL*, *UB*.

EXAMPLE 4. $r_4 = p \wedge \forall\mathbf{G}\exists\mathbf{X}p \wedge \forall\mathbf{F} \sim p$. This formula is chosen to demonstrate the different treatment of $\forall\mathbf{F}$ formulae in our logic PTL_b and in the nonprobabilistic logics *UB*, *CTL*. In fact r_4 is shown below to be satisfiable as a formula of PTL_b, but is unsatisfiable as a formula of *UB*. The construction of the corresponding tableau $\mathbf{T}_4$ is shown in Fig. A.9, and the condensed form of $\mathbf{T}_4$ is shown in Fig. A.10. The formula $\forall\mathbf{F} \sim p$ is fulfilled at state c, and every node containing $\forall\mathbf{F} \sim p$ can reach c. Hence, the rule (M5) does not cause any node to be marked, and r_4 is consequently satisfiable. To obtain a model for r_4 from $\mathbf{T}_4$ simply choose at the pre-state 2 always the state c (again, this is a simpler schedule than the general one given in Sect. 4). The resulting model is shown in Fig. A.11 (note that it certainly does not satisfy r_4 as a model of *UB*).

ACKNOWLEDGMENT

The authors would like to thank Amir Pnueli for suggesting the problem, and for several useful discussions concerning our logics. In particular, certain simplifications of the axiomatic systems of Section 3 are due to him. We also wish to thank our anonymous referees whose critical comments were very helpful in improving the presentation of this paper.

RECEIVED June 27, 1983; ACCEPTED April 18, 1985

REFERENCES

BEN-ARI, M., PNUELI, A., AND MANNA, Z. (1983), The temporal logic of branching time, *Acta Inform.* **20**, 207–226.

EMERSON, E. A., AND CLARKE, E. M. (1982), Using branching time logic to synthesize synchronization skeletons, *Sci. Comput. Program.* **2**, 241–266.

EMERSON, E. A., AND HALPERN, J. Y. (1982), Decision procedures and expressiveness in the temporal logic of branching time, *in* "Proceedings 14th ACM Sympos. Theory of Comput.," pp. 169–179.

EMERSON, E. A., AND HALPERN, J. Y. (1983), "Sometimes" and "not never" revisited: On branching vs. linear time, *in* "Proceedings 10th ACM Sympos. Principles of Program. Lang," pp. 127–140.

FELDMAN, Y., AND HAREL, D. (1982). A probabilistic dynamic logic, *in* "Proceedings, 14th ACM Sympos. Theory of Comput.," pp. 181–195.

FELDMAN, Y. (1983), A decidable propositional probabilistic dynamic logic, *in* "Proceedings 15th ACM Sympos. Theory of Comput.," pp. 298–309.

HART, S., SHARIR, M., AND PNUELI, A. (1983), Termination of concurrent probabilistic programs, *ACM Trans. Program. Lang. Systems* **5**, 356–380.

HART, S., AND SHARIR, M. (1985), Concurrent probabilistic programs, or: How to Schedule if You Must, *SIAM J. Comput.* **14**, 991–1012; *in* "Proceedings, 10th Int. Colloq. Automata, Lang. & Program.," 1983, pp. 304–318, Lecture Notes in Computer Science Vol. 154, Springer–Verlag, New York/Berlin, 1983.

KOZEN, D. (1983), A probabilistic PDL, *in* "Proceedings 15th ACM Sympos. Theory of Comput.," pp. 291–297.

KRAUS, S. (1983), M. Sc. thesis, Computer Science Dept., Hebrew University, Jerusalem.

KRAUS, S., AND LEHMANN, D. (1983), Decision procedures for time and chance, *in* "Proceedings 24th IEEE Sympos. on Found. Comput. Sci.," pp. 202–209.

LEHMANN, D., AND SHELACH, S. (1982), Reasoning with time and chance, *Inform. Control* **53**, pp. 165–198.

PNUELI, A. (1983), On the extremely fair treatment of probabilistic algorithms, *in* "Proceedings 15th ACM Sympos. Theory of Comput.," pp. 278–290.

SHARIR, M., PNUELI, A., AND HART, S. (1984), The verification of probabilistic programs, *Siam J. Comput.* **13**, 292–314.

Printed by the St. Catherine Press Ltd., Tempelhof 41, Bruges, Belgium