A Logic of Probability with Decidable Model Checking*

DANIÉLE BEAUQUIER, *University Paris 12, France*
E-mail: beauquier@univ-paris12.fr

ALEXANDER RABINOVICH, *Tel-Aviv University, Israel*
E-mail: rabino@math.tau.ac.il

ANATOL SLISSENKO, *University Paris 12, France*
E-mail: slissenko@univ-paris12.fr

Abstract

A predicate logic of probability, close to the logics of probability of Halpern *et al*., is introduced. Our main result concerns the following model-checking problem: deciding whether a given formula holds on the structure defined by a given finite probabilistic process. We show that this model-checking problem is decidable for a rather large subclass of formulas of a second-order monadic logic of probability. We discuss also the decidability of satisfiability and compare our logic of probability with the probabilistic temporal logic *pCTL**.

Keywords: Predicate logic of probability, model checking, decidability, finite Markov chain.

1 Introduction

Logics with probabilities were considered in different contexts; on the one hand, in artificial intelligence for reasoning about uncertainty in expert systems, and on the other hand, for specification and verification of systems which exhibit some uncertainty, such as fault-tolerant or randomized systems.

One can distinguish two families of logical approaches for reasoning about probabilities: (i) the first one extends the predicate logics and (ii) the second one extends temporal logics.

A fundamental contribution to the study of predicate logics of probability was made in [6, 9], mainly motivated by the problems of artificial intelligence. Reference [9] contains an excellent survey and analysis of previous works on predicate logics of probability. There have been very interesting works on extensions of predicate logic by probability quantifiers in model theory (see survey in [14]). The models considered there are different from the one considered in this article, and these works seem to be unrelated to our.

Most of the work related to the verification uses probabilistic extensions of temporal logics. The first applications of temporal logic to probabilistic systems were considered while studying which temporal properties are satisfied with probability 1 by systems modeled as finite Markov chains [17]. Later, references [12, 2] introduced *pCTL* and *pCTL** logics that can express quantitative bounds on the probability of system evolutions. This approach is

* Partially supported by French-Israeli Arc-en-ciel/Keshet project No. 30 and No. 15.

Published online 26 July 2006 doi:10.1093/logcom/exl004

surveyed, e.g., in [11, 4, 19]. One of the main problems addressed in these works is the model-checking problem, to decide whether a given formula holds on the structure defined by a given finite Markov chain.

In this article we are interested in the verification of probabilistic systems. However, unlike previous works on verification, we take as a specification formalism a probabilistic extension of predicate logics. Predicate logics offer some advantages (over modal and temporal logics) because of their expressiveness and convenience for formalization of complicated properties.

We follow the general setting of [6, 9, 1] to introduce a rather expressive predicate logic of probability. The main syntactical mechanism of extension of the predicate logic to predicate logic of probability (used in [6, 9]) is by introducing formulas of the form $\mathbf{Prob}_{>x}(\varphi)$ with the intended meaning 'the probability of φ is greater than x'. Here x is a real value variable that ranges over the interval $[0, 1]$. In these works it is allowed to quantify both over-the-domain variables and the real-value variables; moreover, the standard addition and multiplication functions can be applied to the real-value variables. Our probabilistic logic is much weaker. It extends the predicate logic by formulas of the form $\mathbf{Prob}_{>q}(\varphi)$, where q is a rational number (and not a variable); we do not allow to apply arithmetic operations or predicates to the rationals. The property 'φ_1 and φ_2 have the same probability' is easily expressible in the logics considered in [9, 1]; however, it cannot be expressed in our probabilistic logic.

Abadi and Halpern [1] extensively studied the complexity of the satifiability problem for the logic of probability and demonstrated that it takes very little to make reasoning about probability highly undecidable. It turns out that the satisfiabilty problem for this logic with only one constant symbol is at least as hard as that of elementary analysis. We will show that our (much weaker) logic is undecidable for the language that contains only unary predicates.

Our main result shows that the model checking problem is decidable for the logic of probability. The technique used to prove this result significantly extends the technique developed for the proofs of decidability of the model checking problem for probabilistic temporal logics [4]. The expressive power of our logic is incomparable to the expressive power of probabilistic temporal logics. The property 'there is a moment at which Q holds with probability one' is easily formalized in our logic of probability, yet we will show that it cannot be expressed in probabilistic temporal logics. On the other hand, our logic cannot express 'branching properties' which are easily formalized in probabilistic temporal logics.

The article is organized as follows. In Section 2 the syntax and semantics of our logic of probability is presented. In Section 3 we show that monadic predicate logic of probability is undecidable and does not have finite model property. Section 4 contains the statement of our main results about a fragment of probabilistic monadic logic of order with decidable model checking. Section 5 is devoted to the proof of these results. In Section 6 we extend decidable model checking to formulas with nested probabilistic operators. Section 7 provides a detailed comparison of our logic with probabilistic temporal logic *pCTL**. In the last section we describe some extensions of the main results and list open problems.

2 Logic of probability

We follow Halpern's presentation of logic of probability [9]. There, arithmetic operations on probabilities are allowed. Probabilities may be variables that are quantified. In our setting,

we only compare probabilities with rational constants. However, we consider second-order logics, while [9] confines itself to first-order ones.

We consider a language that consists of a collection Σ of predicate symbols of various arities. We also have a collection of predicate variables of various arities. Given formulas φ and ψ in the logic, we allow formulas of the form $\mathbf{Prob}_{>q}(\varphi)$ and $\mathbf{Prob}_{>q}(\varphi|\psi)$, where q is a rational number that can be read as 'the probability of φ is greater than q' and 'the probability of φ under the condition ψ is greater than q', respectively in the two formulas.

2.1 Syntax

More formally, we define the syntax as follows. The vocabulary consists of a set of deterministic predicate symbols, a set of probabilistic predicate symbols, predicate variables and individual variables. We also assume that for every rational number there is a constant in the vocabulary.

Formulas:

- *Atomic formulas* are of the form $\mathcal{P}(x_1, \ldots, x_k)$, where $\mathcal{P}$ is a (deterministic or probabilistic) predicate symbol of arity k and $x_1, \ldots, x_k$ are individual variables; or of the form $X(x_1, \ldots, x_k)$, where X is a deterministic predicate variable of arity k and $x_1, \ldots, x_k$ are individual variables.
- If φ_1 and φ_2 are formulas then $(\varphi_1 \vee \varphi_2)$ and $\neg\varphi_1$ are formulas.
- If φ is a formula then $\exists x\,\varphi$ and $\exists X\,\varphi$, where x is an individual variable and X is a deterministic predicate variable, are formulas.
- If φ, ψ are formulas, and q is a rational number, then $\mathbf{Prob}_{>q}(\varphi)$ and $\mathbf{Prob}_{>q}(\varphi \mid \psi)$ are formulas.

Conjunction $(\varphi_1 \wedge \varphi_2)$, implication $(\varphi_1 \rightarrow \varphi_2)$, the first-order and second-order universal quantifications $\forall x$ and $\forall X$ are defined as usual, using disjunction, negation and the existential quantifiers. Expressions like $\mathbf{Prob}_{<q}$, $\mathbf{Prob}_{\leq q}$, $\mathbf{Prob}_{\geq q}$, $\mathbf{Prob}_{=q}$ can be also defined in terms of $\mathbf{Prob}_{>p}$ using negation and modified bounds on probability in a syntactical manner. For example, we define $\mathbf{Prob}_{<p}(\varphi)$ as $\mathbf{Prob}_{>(1-p)}(\neg\varphi)$.

2.2 Semantics

First, we recall some basic notions from probability theory.

A *measurable space* is a pair (Ω, Δ) consisting of a non-empty set Ω and a σ-algebra Δ of its subsets that are called *measurable sets* and represent random events in probability context. A *σ-algebra* over Ω contains Ω and is closed under complementation and countable union. Adding to a measurable space a *probability measure* $\mu : \Delta \rightarrow [0, 1]$ such that $\mu(\Omega) = 1$ and that is countably additive, we get a *probability space* (Ω, Δ, μ). Probabilistic predicates are interpreted as random predicates. Given a domain $\mathcal{U}$ and a probabilistic space (Ω, Δ, μ) a *random* (or *stochastic*) *predicate* P of arity k is a function from $\Omega \times \mathcal{U}^k$ to $Bool = \{true, false\}$ such that for any fixed $u_1, \ldots, u_k \in \mathcal{U}$ the set $\{\omega \in \Omega : P(\omega, u_1, \ldots, u_k)\}$ is measurable.

A *probabilistic structure* for the language described here is a tuple $(\langle \mathcal{U}, \delta \rangle, \langle \Omega, \Delta, \mu \rangle, \pi)$, where

- $\langle \mathcal{U}, \delta \rangle$ is a first-order structure with universe $\mathcal{U}$, and δ assigns a relation over $\mathcal{U}$ of the appropriate arity to each deterministic predicate symbol;

- $\langle \Omega, \Delta, \mu \rangle$ is a probabilistic space;
- π assigns to each probabilistic predicate symbol P of arity k a random predicate $\pi(P)$: $\Omega \times \mathcal{U}^k \to \mathit{Bool}$.

Define a *valuation* ν to be a function that assigns to each individual variable an element of $\mathcal{U}$, and to each deterministic predicate variable a *finite* relation over $\mathcal{U}$ of the appropriate arity ('finite' means that the set of tuples for which the deterministic predicate is true is finite).

Given a probabilistic structure $\mathcal{M} = (\langle \mathcal{U}, \delta \rangle, \langle \Omega, \Delta, \mu \rangle, \pi)$, an element $\omega \in \Omega$ and a valuation ν, we formally define when a formula φ holds at ω in $\mathcal{M}$ under a valuation ν, written $\mathcal{M}, \nu, \omega \models \varphi$, by the following inductive clauses:

(S1) $\mathcal{M}, \nu, \omega \models R(x_1, \ldots, x_k)$ for a deterministic predicate symbol R of arity k and individual variables $x_1, \ldots, x_k$ iff $\delta(R)(\nu(x_1), \ldots, \nu(x_k))$ is true.

(S2) $\mathcal{M}, \nu, \omega \models X(x_1, \ldots, x_k)$ for a deterministic predicate variable X of arity k iff $\nu(X)(\nu(x_1), \ldots, \nu(x_k))$ is true.

(S3) $\mathcal{M}, \nu, \omega \models P(x_1, \ldots, x_k)$ for a probabilistic predicate P of arity k iff $\pi(P)(\omega, \nu(x_1), \ldots, \nu(x_k))$ is true.

(S4) Quantifiers over individual variables and Boolean connectors are treated as usual.

(S5) Quantifiers over deterministic predicate variables are interpreted as quantifiers over deterministic predicate variables that range only over finite relations over $\mathcal{U}$.

(S6) $\mathcal{M}, \nu, \omega \models \mathbf{Prob}_{>q}(\varphi)$ iff $\mu(\{\omega' \in \Omega : M, \nu, \omega' \models \varphi\}) > q$, that is iff the set of all ω' for which $\mathcal{M}, \nu, \omega' \models \varphi$ holds has a measure greater than q.

(S7) $\mathcal{M}, \nu, \omega \models \mathbf{Prob}_{>q}(\varphi \mid \psi)$ iff $\mu\{\omega' \in \Omega : M, \nu, \omega' \models (\varphi \wedge \psi)\} > q \cdot \mu\{\omega' \in \Omega : M, \nu, \omega' \models \psi\}$, i.e., the conditional probability of φ under ψ is $> q$.

Remark that (S6) is a particular case of (S7) when $\psi = \mathit{true}$.

The semantics is well defined only if the sets that appear in (S6) and (S7) are measurable. From now on, we assume that the probabilistic structure satisfy the following assumption: *The domain $\mathcal{U}$ of probabilistic structures is countable* (**Countability Assumption**).

Proposition 1
Under Countability Assumption the sets that appear in (S6) and (S7) are measurable, and the semantics is well defined.

Proof. The proof proceeds by induction on the structure of formulas. The only not quite straightforward step is quantification.

To show that $\{\omega' \in \Omega : M, \nu, \omega' \models \exists x\, \varphi\}$ is measurable, we use the inductive hypothesis for φ and the fact that any σ-algebra is closed under the countable unions.

To show that $\{\omega' \in \Omega : M, \nu, \omega' \models \exists X\, \varphi\}$ is measurable, we use the inductive hypothesis for φ, i.e., the fact that the set of finite predicates over a countable domain is countable and the fact that any σ-algebra is closed under the countable unions. ■

Proposition 2
Suppose that two valuations ν_1 and ν_2 agree on the free variables of a formula φ. Then, $M, \nu_1, \omega \models \varphi$ iff $\mathcal{M}, \nu_2, \omega \models \varphi$.

Proposition 3
If every occurrence of each probabilistic predicates in a formula φ is in the scope of an operator **Prob** then $M, \nu, \omega_1 \models \varphi$ iff $\mathcal{M}, \nu, \omega_2 \models \varphi$ for every $\omega_1, \omega_2 \in \Omega$. In particular, for any formula ψ we have $M, \nu, \omega_1 \models \mathbf{Prob}_{>q}(\psi)$ iff $M, \nu, \omega_2 \models \mathbf{Prob}_{>q}(\psi)$.

Notations: We use standard notations. If the free variables of formula φ are in the set $\{x_1, \ldots, x_k\}$, we write $\mathcal{M}, a_1, \ldots, a_n, \omega \models \varphi(x_1, \ldots, x_k)$ or $\mathcal{M}, \omega \models \varphi[a_1, \ldots, a_k]$ instead of $\mathcal{M}, \nu, \omega \models \varphi$, where $\nu(x_i) = a_i$ for $i = 1, \ldots, k$.

In addition, if all occurrences of probabilistic predicates in formula φ are in the scope of an operator **Prob**, we abbreviate this to $\mathcal{M} \models \varphi[a_1, \ldots, a_k]$.

These abbreviations are justified by Proposition 2 and Proposition 3.

3 Undecidability of monadic logic of probability

The propositional fragment of our logic is decidable [5]. Moreover, if a propositional probabilistic formula is satisfiable, then it is satisfiable over a finite probabilistic space.

In this section we show that:

(1) The monadic fragment of first-order probabilistic logic is undecidable and
(2) There are satisfiable monadic first-order probabilistic formulas that are not satisfiable over finite probabilistic spaces.

For first-order logic it is well-known that the satisfiability problem is decidable if the language has only unary predicates (monadic logic) and the satisfiability problem is undecidable even for the language with one binary predicate [13]. Many undecidability results for probabilistic logics can be found in [1], where this question was investigated in detail. It was shown in [1] that the satisfiability problem of their probabilistic logic even with one unary predicate is Σ_1^2 complete. However, the logics considered there allow addition and multiplication of probabilities and quantifiers over reals and the methods of [1] are not applicable for our (much weaker) probabilistic logic.

We prove (Theorem 1) that the satisfiability/validity problem for first-order monadic logic of probability (that is a logic of probability where all predicates are monadic) is undecidable. Our proof reduces the satisfiability problem for first-order predicate logic with one binary predicate to the satisfiability problem for the monadic logic of probability.

First, we define a translation from the first-order formulas over a binary predicate to formulas of probabilistic logic with two unary predicates. Let B be a binary predicate symbol and ϕ be a formula in the signature $\{B\}$. Replace in ϕ every occurrence of $R(x, y)$ by $\mathbf{Prob}_{>0}(P(x) \wedge Q(y))$, where P and Q are unary probabilistic predicate symbols. The resulting formula $\psi(P, Q)$ is called the translation of ϕ.

PROPOSITION 4
The formula $\phi(R)$ is satisfiable iff its translation $\psi(P, Q)$ is satisfiable.

PROOF. It is clear that, if the translation of ϕ is satisfiable in a probabilistic structure $\mathcal{M}$, then ϕ is satisfiable in the structure $\langle |M|, R^* \rangle$, where $|\mathcal{M}|$ is the universe of $\mathcal{M}$ and $R^*(a, b)$ holds iff $\mathcal{M}, a, b \models \mathbf{Prob}_{>0}(P(x) \wedge Q(y))$.

Let $\mathcal{M}$ be a structure for a binary predicate name R, where the interpretation of R is a relation R^* over a countable universe $\mathcal{U} = \{a_1, a_2, \ldots, a_n, \ldots\}$. Let us define a probabilistic structure $\mathcal{M}$ as follows. Take as a probabilistic space $\Omega = \mathcal{U}$ with a discrete distribution of probabilities $\mu(\{a_n\}) = 1/2^n$ for every n if Ω is infinite, and μ is uniform if Ω is finite.

For each $a_n \in \Omega$, set $\pi(P)(a_n, t) = \mathit{true}$ iff $t = a_n$ and set $\pi(Q)(a_n, t) = \mathit{true}$ iff $R^*(a_n, t)$.

Observe that for every $a, b \in \mathcal{U}$, $R^*(a, b)$ iff $\mathcal{M}, a, b \models \mathbf{Prob}_{>0}(P(x) \wedge Q(y))$. Hence, for every sentence ϕ in the signature $\{R\}$ and its translation ψ, we have $\mathcal{M} \models \phi$ iff $\mathcal{M} \models \psi$. In particular, if ϕ is satisfiable, then its translation is satisfiable. ■

From Proposition 4 we can deduce:

THEOREM 1
The satisfiability problem for monadic logic of probability is undecidable.

We do not know the exact complexity for the satisfiability problem of monadic logic of probability, yet we believe that it is much lower than Σ_1^2.

It is well-known that the monadic logic has finite model property, i.e. every satisfiable formula has a finite model. It was shown in [5] that if a propositional probabilistic formula is satisfiable, then it is satisfiable over a finite probabilistic space. These contrast with the following property of the monadic logic of probability:

PROPOSITION 5
There exists a satisfiable formula of monadic logic of probability with equality such that all its models have an infinite probabilistic space and an infinite universe.

PROOF. There is a closed predicate formula $\phi(R)$ over a binary predicate R which is satisfiable only in structures with infinite domain. For example, take for $\phi(R)$ the conjunction of the three properties, R is transitive, irreflexive and $\forall x\, \exists y\, R(x, y)$. Consider the formula $\psi(P, Q)$ obtained as in the preceding text, replacing in $\phi(R)$ every occurrence of $R(x, y)$ by $\mathbf{Prob}_{>0}(P(x) \wedge Q(y))$. Consider the probabilistic monadic formula

$$\Psi(P, Q) = \psi(P, Q) \wedge \mathbf{Prob}_{=1}(\exists! x\, P(x)) \wedge \forall x\, \mathbf{Prob}_{>0}(P(x))$$

We claim that:

(1) $\Psi(P, Q)$ is satisfiable.
(2) Every model of $\Psi(P, Q)$ has an infinite probabilistic space.
(3) Every model of $\Psi(P, Q)$ has an infinite universe.

In order to prove (1), consider the following model $\mathcal{M}$. Take a countable infinite universe $\mathcal{U} = \{a_1, a_2, \ldots, a_n, \ldots\}$. Take as a probabilistic space $\Omega = \mathcal{U}$ with a discrete distribution of probabilities $\mu(\{a_n\}) = 1/2^n$ for every n.

For each $a_n \in \Omega$ set $\pi(P)(a_n, t) = true$ iff $t = \{a_n\}$ and $\pi(Q)(a_n, t) = true$ iff $t \in \{a_{n+1}, a_{n+2}, \ldots\}$. Then, it is clear from the construction that $\mathcal{M}$ satisfies $\Psi(P, Q)$.

Here is the proof of (2). Suppose there is a structure $\mathcal{M}$ that is a model of $\Psi(P, Q)$ with a finite probabilistic space $\Omega = \{\omega_1, \ldots, \omega_k\}$. We can suppose that $\mu(\omega_i) > 0$ for $i = 1, \ldots, k$. Thus, for $i = 1, \ldots, k$ there exists a unique $a_i \in \mathcal{U}$ such that $\pi(P)(\omega_i, a_i)$ because $\mathcal{M}$ satisfies $\mathbf{Prob}_{=1}(\exists! x\, P(x))$. Choose an element a in universe $\mathcal{U}$ different from all the a_i. Since $\mathcal{M}$ satisfies $\forall x\, \mathbf{Prob}_{>0}(P(x))$, there exists an $\omega \in \Omega$ such that $\pi(P)(\omega, a) = true$. A contradiction.

The proof of (3) is easy. Indeed the formula $\psi(P, Q)$ is satisfiable only in structures with infinite domain, as follows from its definition, the construction of ϕ and Proposition 4. ■

4 Model checking for fragments of logic of probabilities

In this section we consider a logic of probability with one binary deterministic predicate, the order $<$, all other predicates are probabilistic monadic and all its second-order variables are monadic. This logic is denoted PMLO (probabilistic monadic logic of order). Formally the syntax of probabilistic monadic logic of order has in its vocabulary *individual* (first-order) variables $t_0, t_1, \ldots, t_k$, monadic *predicate* variables (interpreted as finite sets), and unary predicate names (interpreted as probabilistic predicates) and

one binary relation $<$ (the order). We use lowercase letters t, x, y to range over individual variables and uppercase letters X, Y, Z to range over monadic variables and monadic predicate names.

Atomic formulas are of the form $X(t), t_1 < t_2$ and $t_1 = t_2$, where t, t_1, t_2 are first-order variables, and X is either monadic variable or a monadic predicate name.

Well-formed formulas of the monadic logic PMLO are obtained from atomic formulas using Boolean connectives $\neg$, $\vee$, $\wedge$, $\rightarrow$, the (first-order) quantifiers $\exists t$ and $\forall t$, second-order quantifiers $\exists X$ and $\forall X$ and probabilistic constructs $\mathbf{Prob}_{>q}(\varphi)$ and $\mathbf{Prob}_{>q}(\varphi \mid \psi)$, where q is a rational number.

The formulas without probabilistic constructs are formulas of the weak monadic logic of order (WMLO) denoted also as weak second-order logic of one successor (WS1S). WMLO is a fundamental formalism and plays an important role in automata theory; moreover, temporal logics can be translated into WMLO [20].

The probabilistic structures used in this section are defined by finite probabilistic processes. We study the following model checking problem: decide whether a given PMLO formula φ holds on the structure defined by a given finite probabilistic process. We introduce a rather large subclass $\mathcal{C}$ of formulas for which the model checking problem is 'almost always decidable'.

Subsection 4.1 explains how finite probabilistic processes define probabilistic structures. Subsection 4.2 introduces a class $\mathcal{C}$ of formulas and states the main results of this study.

4.1 Probabilistic structures defined by finite probabilistic processes

Definition 1

A finite probabilistic process is a finite labeled Markov chain [15] $\mathcal{M} = (S, M, V, \mathcal{L})$, where S is a finite set of states, $\mathcal{M}$ is a transition probability matrix: $S^2 \rightarrow [0, 1]$ such that $\mathcal{M}(i, j)$ is a rational number for all $(i, j) \in S^2$, $\sum_{j \in S} M(i, j) = 1$ for every $i \in S$, and $V : S \rightarrow 2^{\mathcal{L}}$ is a valuation function that assigns to each state a set of symbols from a finite set $\mathcal{L}$.

The pair (S, M) is called a finite Markov chain.

The subsequent lemma is a well-known fact in the theory of matrices (see, e. g. [17], 13.7.5, 13.7.1).

Lemma 1

Let (S, M) be a finite Markov chain. There exists a positive natural number d period of the Markov chain such that the following limits exist:

$$\lim_{m \rightarrow \infty} M^{r+dm} = M_r \quad (r = 0, 1, \ldots, d-1).$$

Moreover, if the elements of $\mathcal{M}$ are rational, then these limits are computable from $\mathcal{M}$ and the convergence to the limits is geometric, i.e. $|M^{r+dm}(i, j) - P_r(i, j)| < a \cdot b^m$ when $m \geq m_0$ for some positive rationals $a, b < 1$ and natural m_0; the numbers a, b and m_0 are also computable from $\mathcal{M}$.

Given a finite probabilistic process $\mathcal{M} = (S, M, V, \mathcal{L})$ and a state s, we define a probabilistic structure $\mathcal{M}_s$ as follows:

Signature: A deterministic binary predicate $<$, and monadic probabilistic predicates P for every label $P \in \mathcal{L}$.

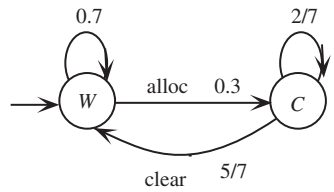

FIGURE 1. A finite probabilistic process (*W* stands for *Wait* and *C* stands for *Call*)

Interpretation:

- The universe of the structure $\mathcal{M}_s$ is the set $\mathbb{N}$ of natural numbers;
- $<$ is interpreted as the standard less relation over $\mathbb{N}$;
- Probabilistic space (Ω, Δ, μ) [16] : $\Omega = sS^{\omega}$ is the set of all infinite sequences of states starting from s, Δ is the σ-algebra generated by the basic cylindric sets $D_u = uS^{\omega}$, for every $u \in sS^*$, and the probability measure μ is defined by $\mu(D_u) = \prod_{i=0,\ldots,n-1} M(s_i, s_{i+1})$, where $u = s_0 s_1 \ldots s_n$;
- Interpretation of monadic probabilistic predicates: for each $\omega = s_0 s_1 \ldots s_n \ldots \in \Omega$, for each $n \in \mathbb{N}$ we have $\pi(P)(\omega, n)$ iff $P \in V(s_n)$ (i.e. P belongs to the label of state s_n). At this point, notice that, for every integer n, the set $\{\omega \in \Omega : \pi(P)(\omega, n)\}$ is μ-measurable since it is a finite union of basic cylinders.

EXAMPLE

Let us consider a call-establishment procedure in a simple telephone network where the capacity of simultaneous outgoing calls is less than the number of users. An abstraction of this procedure represents the behavior of a user where time is assumed to be discrete (Figure 1).

To simplify our presentation, it is assumed that a user who is not connected is continuously attempting to get a connection (state *Wait*) and at each moment he succeeds to establish, the connection with the probability 3/10. Moreover, when the call is established, the duration of the call (state *Call*) follows a geometric distribution: at each moment, the probability to finish the call is 5/7.

The set of labels here is equal to the set of states, and the label of a state is the state itself. One can write a liveness property such that:

$$\varphi =_{df} \forall t \; \mathbf{Prob}_{=1}(\exists \, t' > t \; Call(t')) \tag{1}$$

which expresses that, at every time, the probability that the user will be served later is equal to one.

One can also express some probabilistic property concerning the time the user has to wait before being served:

$$\psi =_{df} \forall t \; \mathbf{Prob}_{\geq 0.9}(\exists t' \; (t < t' \; \wedge \; t' < t + 3 \; \wedge \; Call(t'))) \tag{2}$$

One can prove that $\mathcal{M}_{Wait} \models \varphi$ and $\mathcal{M}_{Wait} \not\models \psi$.

4.2 Statement of main results

In this subsection we define some classes of formulas. Our main results (Theorems 3–5), roughly speaking, state that for these classes it is decidable whether a given formula in a class holds in the structure defined by a given finite probabilistic process $\mathcal{M}$. The proofs of these results will be provided in the following section.

All our decidability results are only for formulas that do not contain conditional probability operators. From now on we will deal only with such formulas.

DEFINITION 2
A PMLO-formula φ belongs to the class $\mathcal{C}$ iff operators $\mathbf{Prob}_{>q}$ are not nested, and for every subformula of φ of the form $\mathbf{Prob}_{>q}\psi$, the formula ψ does not contain free predicate variables. If a PMLO formula φ contains occurrences $\mathbf{Prob}_{>q}$ only with $q=0$, then φ is called a qualitative formula. If, for every subformula of the form $\mathbf{Prob}_{>q}\psi$ of a PMLO formula φ, the formula ψ contains at most one free individual variable, then φ is called a simple formula.

For example, the formula

$$\exists t \exists t' (t < t' \wedge \mathbf{Prob}_{>1/3}(P(t) \wedge P(t') \wedge \exists Q \forall t'' > t\ Q(t'')) \wedge \mathbf{Prob}_{>1/2}(\neg P(t'))), \tag{3}$$

where P is a probabilistic predicate and Q a deterministic one, belongs to $\mathcal{C}$.

The properties (1) and (2) are expressed by simple formulas; these formulas are also in the class $\mathcal{C}$.

As an example that uses a weak second-order quantification, we can mention the following property: the probability that a given probabilistic predicate has an even number of elements is greater than 0.9. It is easy to write a formula $Even(X)$ of WMLO, which says that the number of elements in X is even. Hence, in our logic the aforementioned property can be formalized as $\mathbf{Prob}_{>0.9}(Even(P))$.

A PMLO formula φ is called a *sentence* if it has no free variable and every occurrence of each probabilistic predicate is in the scope of an operator **Prob**.

If φ is a sentence, $\mathcal{M} \models \varphi$ stands for $\mathcal{M}, \omega \models \varphi$, that is well-defined and is independent from ω and an interpretation of variables due to Proposition 3.

The main results of this study, roughly speaking, say that it is decidable whether a given formula $\varphi \in \mathcal{C}$ holds in the structure defined by a given finite probabilistic process $\mathcal{M}$.

In order to express our decidability result about model checking, we need to introduce the notion of *parameterized* formula of logic of probability.

The set of *parameterized formulas* is defined similarly to the set of formulas; the only difference is that operators $\mathbf{Prob}_{>q}$ with $q \in \mathbb{Q}$ are replaced by $\mathbf{Prob}_{>p}$, where p is a parameter name.

For example,

$$\exists t \exists t' (t < t' \wedge \mathbf{Prob}_{>p_1}(P(t) \wedge P(t') \wedge\ \exists Q \forall t'' > t\ Q(t'')) \wedge \mathbf{Prob}_{>p_2}(\neg P(t')))$$

is a parameterized formula.

Let φ be a *parameterized formula* with parameters $p_1, \ldots, p_m$ and $\alpha_1, \ldots, \alpha_m$ be a sequence of rational values. We denote by $\varphi_{\alpha_1,\ldots,\alpha_m}$ the formula obtained by replacing in φ each parameter p_i by the value α_i. The set of parameterized sentences is defined exactly like the set of sentences. By abuse of terminology, we say that a parameterized formula φ belongs to $\mathcal{C}$ if all (or, equivalently, any of) its instances $\varphi_{\alpha_1,\ldots,\alpha_m}$ are in $\mathcal{C}$.

In the following text, for simplicity, we will write $\mathbf{Prob}_{M_s}(\varphi(n_1, \ldots, n_k))$ instead of $\mu\{\omega : \mathcal{M}_s, n_1, \ldots, n_k, \omega \models \varphi(t_1, \ldots, t_k)\}$ for a finite probabilistic process $\mathcal{M}$, state s of $\mathcal{M}$ and $(n_1, \ldots, n_k) \in \mathbb{N}^k$.

Now, we are ready to state the main technical theorem.

THEOREM 2
Let $\mathcal{M}$ be a finite probabilistic process, s_0 be a state of $\mathcal{M}$ and $\varphi(t_1, \ldots, t_k)$ be a parameterized formula without free predicate variables and with m parameters.

(1) If formula φ is in the class $\mathcal{C}$ and is simple, one can compute for each parameter p_i in φ $(i = 1, \ldots, m)$ a finite set H_i of rational values not containing zero such that for each tuple of rationals $\alpha = (\alpha_1, \ldots, \alpha_m)$ where $\alpha_i \in \mathbb{Q} \setminus H_i$, $i = 1, \ldots, m$, one can compute a WMLO formula $\psi(t_1, \ldots, t_k)$ such that for $n_1, \ldots, n_k \in \mathbb{N}(\mathcal{M}, s_0)$ satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi(n_1, \ldots, n_k)$.
(2) If formula φ is in the class $\mathcal{C}$, then, for each rational number $\epsilon > 0$, one can compute for each parameter p_i in φ $(i = 1, \ldots, m)$ a set H_i that is the union of a finite set of intervals not containing zero, with total length less than ϵ, such that for each tuple of rationals $\alpha = (\alpha_1, \ldots, \alpha_m)$ where $\alpha_i \in \mathbb{Q} \setminus H_i$, $i = 1, \ldots, m$, one can compute a WMLO formula $\psi(t_1, \ldots, t_k)$ such that for $n_1, \ldots, n_k \in \mathbb{N}(M, s_0)$ satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi(n_1, \ldots, n_k)$.

Remarks:

(1) The complexity of our decision procedure is mainly determined by the complexity of decision procedure for WMLO formulas (that is non-elementary in the worst case) [18].
(2) The fact that we cannot treat a set of exceptional values seems to be essential from the mathematical point of view. Once annot exclude that the model checking problem is undecidable for these exceptional values. However, for practical properties the values of probabilities can always be slightly changed without loss of its essential significance and this permits to eliminate these exceptional values of probabilities.

From Theorem 2 and from the fact that the validity problem for WMLO is decidable, one deduces immediately the following decidability results:

THEOREM 3 (Qualitative model checking)
Given a qualitative sentence φ in the class $\mathcal{C}$, a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$, it is decidable whether φ holds in the probabilistic structure $\mathcal{M}_s$.

THEOREM 4
Given a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$ and a parameterized simple sentence φ in the class $\mathcal{C}$ with m parameters, one can compute for each parameter p_i in φ a finite set H_i $(i = 1, \ldots, m)$ such that for each tuple $\alpha = (\alpha_1, \ldots, \alpha_m)$ where $\alpha_i \in \mathbb{Q} \setminus H_i$, $i = 1, \ldots, m$, it is decidable whether φ holds in the probabilistic structure $\mathcal{M}_s$.

THEOREM 5
Given a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$, a parameterized sentence φ in the class $\mathcal{C}$ with m parameters and a rational number $\epsilon > 0$, one can compute for each parameter p_i in φ $(i = 1, \ldots, m)$ a finite set H_i of intervals, not containing zero, with total length less than ϵ, such that for each tuple $\alpha = (\alpha_1, \ldots, \alpha_m)$, where $\alpha_i \in \mathbb{Q} \setminus H_i$, $i = 1, \ldots, m$, it is decidable whether φ holds in the probabilistic structure $\mathcal{M}_s$.

5 Proof of Theorem 2

Before providing the proof of Theorem 2, let us illustrate the model checking procedure on a simple example.

Assume that $\mathcal{M}$ is a finite state labelled Markov chain. Moreover, assume that (i) its matrix M is regular, i.e., $\lim_{n\to\infty} M^n$ exists and (ii) there is exactly one state s_1 labelled by a predicate P_1.

Let $\varphi(t)$ be the formula $\mathbf{Prob}_{>1/2}P_1(t)$. In order to check whether φ is satisfiable in the structure $\mathcal{M}_{s_0}$, i.e. whether there exists an integer n such that $\varphi(n)$ holds in $\mathcal{M}_{s_0}$, we can do the following. First, observe that the probability that $P_1(t)$ holds at a moment n in the structure $\mathcal{M}_{s_0}$ is $(M^n)_{0,1}$. Second, compute $\widehat{M} = \lim_{n\to\infty} M^n$; and let $\lambda = \widehat{M}_{0,1}$. (This step is computable by Lemma 1). Now we will proceed by the following cases:

Case $\lambda > 1/2$**:**
In this case $\mathbf{Prob}_{>1/2}P_1(n)$ holds in $\mathcal{M}_{s_0}$ for all n that are big. Therefore, $\mathbf{Prob}_{>1/2}P_1(t)$ is satisfiable in $\mathcal{M}_{s_0}$.

Case $\lambda < 1/2$**:**
In this case by Lemma 1 we can compute n_0 such that for all $n > n_0$ the probability that $P_1(n)$ holds will be $\sim\lambda < 1/2$. Therefore, $\mathbf{Prob}_{>1/2}P_1(t)$ is satisfiable iff it is satisfiable for $n \le n_0$. The last condition can be checked by verifying if there is $n < n_0$ such that $(M^n)_{0,1} > 1/2$.

Case $\lambda = 1/2$**:**
In this case we have to verify that there is n such that $(M^n)_{0,1} > 1/2$. We do not know how to treat this exceptional case.

From the preceding description, it is clear how to model check the parameterized formula $\mathbf{Prob}_{>r}P_1(t)$ on $\mathcal{M}_{s_0}$ for all values of the parameter r except one value λ. Moreover, the preceding arguments show that for $r \neq \lambda$ the set of n that satisfies $\mathbf{Prob}_{>r}P_1(t)$ is either finite (Case $\lambda < r$) or cofinite (case $\lambda > r$).

The procedure for model checking of arbitrary formulas is similar to the procedure described in the preceding text. The aforementioned assumption that M is regular is not essential and can be easily removed. The more difficult part of the proof is a reduction of arbitrary formulas to simpler formulas. This is done in the rest of this section.

5.1 Future and past formulas and decomposition lemma

We introduce a notation: $\mathbb{N}_{\ge a} = \{n \in \mathbb{N} \mid n \ge a\}$ and recall what are future and past WMLO formulas.

Definition 3 (Future Formulas)
A WMLO formula $\varphi(x_0, X_1, X_2, \ldots, X_m)$ with only one free first-order variable x_0 is a future formula if for every $a \in \mathbb{N}$ and every m subsets $S_1, S_2, \ldots, S_m$ of $\mathbb{N}$, the following holds: $(\mathbb{N}, a, S_1, S_2, \ldots, S_m) \models \varphi(x_0, X_1, X_2, \ldots, X_m)$ iff $(\mathbb{N}_{\ge a}, a, S'_1, S'_2, \ldots, S'_m) \models \varphi(x_0, X_1, X_2, \ldots, X_m)$, where $S'_i = S_i \cap \mathbb{N}_{\ge a}$ for $i = 1, 2, \ldots, m$.

Past WMLO formulas are defined in a symmetric way. Note that the definition of the future formulas is a semantical one.

It is convenient to extend the syntax of the monadic logic of order with the bounded existential quantifiers $\exists t_{\leq t_1}$, $\exists t_{\geq t_1}^{\leq t_2}$, $\exists t_{\geq t_1}$. Semantically, $\exists t_{\geq t_1}^{\leq t_2}\varphi$ is a shorthand for $\exists t\ t_1 \leq t \wedge t \leq t_2 \wedge \varphi$. Similarly, $\exists t_{\leq t_1}\varphi$ (respectively, $\exists t_{\geq t_1}\varphi$) is a shorthand for $\exists t\ t \leq t_1 \wedge \varphi$ (respectively, $\exists t\ t \geq t_1 \wedge \varphi$).

There is a syntactic characterization of future and past formulas.

Proposition 6
A WMLO-formula $\varphi(x_0, X_1, X_2, \ldots, X_m)$ with only one free first-order variable x_0 is a future (respectively, past) formula iff it is (semantically) equivalent to a formula where all first-order quantifiers are relativized to $\geq x_0$ (respectively, $\leq x_0$), i.e. are of the form $\exists t_{\geq x_0}$ (respectively, $\exists t_{\leq x_0}$).

Similar to Lemma 9.3.2 in [8], we have the following decomposition lemma for WMLO logic:

Lemma 2 (Decomposition Lemma)
The formula $t_1 < t_2 < \cdots < t_k \ \wedge \psi(t_1, t_2, \ldots, t_k)$, where $\psi(t_1, t_2, \ldots, t_k)$, is a WMLO formula with only free variables $t_1, \ldots, t_k$ is equivalent to a finite disjunction of formulas of the form:

$$\vee_{i\in I}\varphi_{i,\leftarrow}(t_1) \wedge \psi_{i,1}(t_1, t_2) \wedge \cdots \wedge \psi_{i,k-1}(t_{k-1}, t_k) \wedge \varphi_{i,\rightarrow}(t_k),$$

where

(1) $\varphi_{i,\leftarrow}(t_1)$ is a past formula
(2) $\varphi_{i,\rightarrow}(t_k)$ is a future formula
(3) In $\psi_{i,j}(t_j, t_{j+1})$ only t_j and t_{j+1} are free and all first-order quantifiers are of the form $\exists t_{\leq t_j}^{\geq t_{j+1}}$, for $j = 1, \ldots, k-1$.

Moreover, formulas $\varphi_{i,\leftarrow}$, $\varphi_{i,\rightarrow}$, $\psi_{i,j}$ are computable from ψ and for $i_1 \neq i_2$, the disjuncts $\varphi_{i_1,\leftarrow}(t_1) \wedge \psi_{i_1,1}(t_1, t_2) \wedge \cdots \wedge \psi_{i_1,k-1}(t_{k-1}, t_k) \wedge \varphi_{i_1,\rightarrow}(t_k)$ and $\varphi_{i_2,\leftarrow}(t_1) \wedge \psi_{i_2,1}(t_1, t_2) \wedge \cdots \wedge \psi_{i_2,k-1}(t_{k-1}, t_k) \wedge \varphi_{i_2,\rightarrow}(t_k)$ are mutually exclusive.

5.2 Ultimately periodic sets

Let d, k and h be fixed integers. We say that a set $S \subseteq \mathbb{N}^k$ is ultimately periodic with period d, dimension k and displacement h if for all $n_1, \ldots, n_k \in \mathbb{N}$:

$$\text{if } n_i \geq h \text{ then } ((n_1, \ldots, n_i, \ldots, n_k) \in S \text{ iff } (n_1, \ldots, n_i + d, \ldots, n_k) \in S).$$

Observe that in dimension one, a set is ultimately periodic with period one if and only if it is finite or cofinite. This characterization is not true in higher dimensions.

A finite set $J \subseteq \mathbb{N}^k$ is a representation of S if $(n_1, \ldots, n_i \ldots, n_k) \in S$ iff there is $(m_1, \ldots, m_i \ldots, m_k) \in J$ such that: for all $i \in \{1, \ldots, k\}$ $[(m_i = n_i < h)$ or $(m_i \geq h,\ n_i \geq h$ and $m_i = n_i \ mod\ d)]$.

Lemma 3 (Properties of Ultimately Periodic Sets)

(1) If a set is ultimately periodic, then its complement is ultimately periodic.
(2) If $S_1, S_2 \subseteq \mathbb{N}^k$ are ultimately periodic, then $S_1 \cup S_2, S_1 \cap S_2$ are ultimately periodic.
(3) Every ultimately periodic set has a finite representation.

(4) If $S \subseteq \mathbb{N}^k$ is ultimately periodic, then there exists a WMLO formula $\theta(t_1, \ldots, t_k)$ such that $(\mathbb{N}, <) \models \theta(n_1, n_1 + n_2, \ldots, n_1 + \cdots + n_k)$ iff $(n_1, n_2, \ldots, n_k) \in S$.

PROOF. The first two properties are easy to prove. We prove the last ones.

Proof of (3). If $S \subseteq \mathbb{N}^k$ is an ultimately periodic set with period d, dimension k and displacement h, then the set $\{(n_1, \ldots, n_k) : (n_1, \ldots, n_k) \in S \wedge \bigwedge_{i=1}^{k} n_i < h + d\}$ is a finite representation of S.

Proof of (4).

For $i < d \in \mathbb{N}$ let $\Theta_{i,d}(t_1, t_2)$ be a formula that says that $t_1 < t_2$ and $t_2 - t_1 = i \bmod d$. It can be written as the conjunction of

(1) $t_1 < t_2$
(2) There are predicate variables $Z_0, \ldots, Z_{d-1}$ such that

   (a) The sets $Z_0, \ldots Z_{d-1}$ partition interval $[t_1, t_2]$
   (b) $\forall t(t_1 \leq t < t_2) \rightarrow \bigwedge_{j=0}^{d-1}(t \in Z_j \leftrightarrow t + 1 \in Z_{j+1 \bmod d})$
   (c) $t_1 \in Z_{\hat{}5}$ and $t_2 \in Z_i$

From $\Theta_{i,d}$ and the finite representation J of S, which is given above, we obtain: $(n_1, n_2, n_3, \ldots, n_k) \in S$ is equivalent to:

$$\bigvee_{(m_1,\ldots,m_k)\in J} \bigwedge_{i=1}^{k} (n_i = m_i < h \vee (\Theta_{m_i,d}(0, n_i) \wedge n_i \geq h \wedge m_i \geq h).$$

Notice that if $\Theta_{m_i,d}(0, n_i)$ holds then $\Theta_{m_i,d}(n', n' + n_i)$ for every integer n'. Notice also that for every $n \in \mathbb{N}$ there is a WMLO formula $\mathrm{diff}_n(t_1, t_2)$ and a WMLO formula $\mathrm{less}_n(t_1, t_2)$ such that for all $n_1, n_2 \in N$:

$$\mathrm{diff}_n(n_1, n_2) \text{ if and only if } n_2 - n_1 = n \text{ and}$$
$$\mathrm{less}_n(n_1, n_2) \text{ if and only if } n_2 - n_1 < n.$$

Finally, the desirable formula, $\theta(t_1, \ldots, t_k)$ can be defined as:

$$\bigvee_{(m_1,\ldots,m_k)\in J} \left[C_{m_1} \wedge A_{(m_2,\ldots,m_k)} \wedge B_{(m_2,\ldots,m_k)} \right], \text{ where}$$

$$C_m \text{ is } \begin{cases} t_1 = m & \text{if } m < h \\ t_1 \geq m \wedge \Theta_{m,d}(0, t_1) & \text{otherwise} \end{cases}$$

and

$$A_{(m_2,\ldots,m_k)} \text{ is } \bigwedge_{\{i:1<i\leq k \wedge m_i<h\}} \mathrm{diff}_{m_i}(t_{i-1}, t_i)$$

and

$$B_{(m_2,\ldots,m_k)} \text{ is } \bigwedge_{\{i:1<i\leq k \wedge m_i\geq h\}} \Theta_{m_i,d}(t_{i-1}, t_i) \wedge \neg \mathrm{less}_h(t_{i-1}, t_i).$$

■

5.3 A Lemma from analysis

The next lemma is a simple lemma from analysis:

LEMMA 4
For $1 \leq i \leq k$, $1 \leq j \leq m$, let $M_{i,j}$ be probabilistic rational matrices of size $N \times N$, and $I_{i,j}$ be rational (row) vectors of the size N with all elements equal to zero, except one equal to 1; let $F_{i,j}$ be rational (column) vectors of the size N with all elements in [0, 1], and $c_j \in \mathbb{Q}^+$. Suppose that matrices $M^n_{i,j}$ have a limit when $n \to \infty$. Let $a_{i,j,n} = I_{i,j} \cdot M^n_{i,j} \cdot F_{i,j}$. Let

$$L_p = \left\{ (n_1, \ldots, n_k) \in \mathbb{N}^k : \sum_{j=1}^{m} \left(c_j \cdot \prod_{i=1}^{k} a_{i,j,n_i} \right) > p \right\}$$

(1) If $p = 0$, then L_p is ultimately periodic with period one.
(2) If $p \neq 0$, then

   (a) If $k = 1$, then there is a computable finite set H such that, for every rational $p \notin H$, the set L_p is finite or cofinite, i.e. ultimately periodic with period one.
   (b) If $k > 1$, then for every rational $\epsilon > 0$ there is a computable set H that is the union of a finite set of intervals with total length at most ϵ such that for every rational $p \notin H$ the set L_p is ultimately periodic with period one.

In all the aforementioned cases a finite representation of L_p is computable from $M_{i,j}, I_{i,j}, F_{i,j}$ and p. In 2(b), the set H is the union of a finite set $\{[a_i, b_i] : a_i, b_i \in \mathbb{Q} \text{ for } i = 1, \ldots, t\}$ of intervals; by computability of H we mean that the sequences $\langle a_i : i = 1, \ldots, t \rangle$ and $\langle b_i : i = 1, \ldots, t \rangle$ are computable from $M_{i,j}, I_{i,j}, F_{i,j}$ and p.

PROOF. Recall the following well-known fact. Let G be a graph and s, s' be its vertices. Then, the set $G_{s,s'} =_{df} \{n \in \mathbb{N} :$ there is a path from s to s' of length $n\}$ is ultimately periodic. Moreover, the set $G_{s,s'}$ has a computable finite representation, because $\{a^n : n \in G_{s.s'}\}$ is a regular language over a unary alphabet.

We study first the case when $p = 0$. In this case, $(n_1, \ldots, n_k) \in L_0$ iff there exists $j \in \{1, \ldots m\}$ such that for all $i \in \{1, \ldots, k\}$ $a_{i,j,n_i} > 0$. Let $G_{i,j}$ be the graph with vertices $1, \ldots, N$, and (s, s') is an edge iff $M_{i,j}(s, s') > 0$. Let s be the vertex such that $I_{i,j}(s) = 1$ and $F = \{s' \mid F_{i,j}(s') > 0\}$. We have $a_{i,j,n_i} > 0$ iff there exists in the graph $G_{i,j}$ a path from s to some vertex in F with length n_i. Thus, the set L_0 is ultimately periodic, and a finite representation of L_0 is computable by the well-known fact mentioned earlier.

We study now the case when $p > 0$.

Define:

$\Delta(n_1, \ldots, n_k) = \sum_{j=1}^{m} (c_j \cdot \prod_{i=1}^{k} a_{i,j,n_i})$.

Let $l = lim_{n_1 \to \infty, \ldots, n_k \to \infty} \Delta(n_1, \ldots, n_k) = \sum_{j=1}^{m} (c_j \cdot \prod_{i=1}^{k} lim_{n_i \to \infty} a_{i,j,n_i})$

$= \sum_{j=1}^{m} (c_j \cdot \prod_{i=1}^{k} I_{i,j} \cdot (lim_{n_i \to \infty} M^{n_i}_{i,j}) \cdot F_{i,j})$.

From Lemma 1 the limit l is rational and computable.

The proof of 2 is by induction on k.

Case $k = 1$ and $p > 0$:

- If $l = 0$ then $lim_{n_1 \to \infty} \Delta(n_1) = 0$ and so $L_p = \{n_1 : \Delta(n_1) > p\}$ is a finite set.
- If $l \neq 0$, let $H = \{l\}$.

If $p > l$, then L_p is finite.

If $p < l$, then L_p is cofinite, and hence L_p is ultimately periodic with period one.

In both cases, a finite representation of L_p is computable due to the exponential convergence of the matrices to the limit, as stated in Lemma 1.

Case $k > 1$ and $p > 0$:

For every rational ϵ there exists an integer N such that, if $n_1, \ldots, n_k \geq N$, then

$$|\Delta(n_1, \ldots, n_k) - l| < \epsilon/4. \tag{4}$$

Let:

$$\mathbb{N}^k_{\geq N} = \{(n_1, \ldots, n_k) \in \mathbb{N}^k \mid n_i \geq N \text{ for } i = 1, \ldots, k\}.$$

For $i \in \{1, \ldots, k\}$ and $n_i \in \{0, \ldots, N-1\}$ let:

$$\mathbb{N}^k_{i,n_i} = \mathbb{N}^{i-1}\{n_i\}\mathbb{N}^{k-i}.$$

We have $\mathbb{N}^k = \mathbb{N}^k_{\geq N} \cup (\cup_{i=1}^{i=k} \cup_{n_i=0}^{n_i=N-1} \mathbb{N}^k_{i,n_i})$.

We will prove that the intersection of L_p with each of the sets $\mathbb{N}^k_{\geq N}$, and $\mathbb{N}^k_{i,n_i}$ is ultimately periodic and a finite representation of the intersection is computable.

Firstly, from (4) we deduce that, for each p such that $|p - l| > \epsilon/4$, the set $\mathbb{N}^k_{\geq N} \cap L_p = \{(n_1, \ldots, n_k) \in \mathbb{N}^k_{\geq N} : \Delta(n_1, \ldots, n_k) > p\}$ is ultimately periodic with period one, and a finite representation of this set is computable (this set is empty, if $p > l + \epsilon/4$; it is equal to $\mathbb{N}^k_{\geq N}$, if $p < l - \epsilon/4$).

Secondly, fix $i_0 \in \{1, \ldots, k\}$ and $n_{i_0} \in \{0, \ldots, N-1\}$. A tuple $(n_1, \ldots, n_k) \in \mathbb{N}^k_{i_0,n_{i_0}}$ satisfies

$$\Delta(n_1, \ldots, n_k) > p$$

iff

$$\sum_{j=1}^{m} \left(c_j \cdot a_{i_0,j,n_{i_0}} \cdot \prod_{i \neq i_0} a_{i,j,n_i} \right) > p. \tag{5}$$

Let $C_j = c_j \cdot a_{i_0,j,n_{i_0}}$. Note that (5) can be rewritten as:

$$\sum_{j=1}^{m} \left(C_j \cdot \prod_{i \neq i_0} a_{i,j,n_i} \right) > p. \tag{6}$$

Let $\epsilon' = \epsilon/2kN$. By the induction hypothesis, there exists a computable set $H_{i_0,n_{i_0}}$, which is the union of a finite number of intervals with the sum of lengths at most ϵ' such that, if a rational $p \neq 0$ is not in $H_{i_0,n_{i_0}}$ then the set of tuples $(n_1, \ldots, n_{i_0-1}, n_{i_0+1}, \ldots, n_k)$, which satisfy (6), is ultimately periodic with period one and with a computable finite representation. Thus, for a fixed (i_0, n_{i_0}), if rational p is not in a finite number of intervals the sum of lengths of which is at most $\epsilon/2kN$, the set of tuples in $\mathbb{N}^k_{i,n_i}$ that satisfies the inequality (5) is ultimately periodic with period one and with a computable finite representation. Finally, define a set of interval H as follows:

An interval I is in H if I is the interval $[l - \epsilon/4, l + \epsilon/4]$ or I is one of the intervals in H_{i,n_i} for $i = 1, \ldots, k$ and $n_i = 1, \ldots, N$.

H is a finite set of interval, because the sets H_{i,n_i} ($i = 1, \ldots, k$ and $n_i = 1, \ldots, N$) are finite. For the same reasons, H is a computable set. Finally, the total length of the intervals in H is less than $2 \times \epsilon/4 + kN \cdot \epsilon/2kN = \epsilon$. This completes the proof. ■

5.4 Technical lemmas

In this subsection we will collect theorems and lemmas that will be used in the next subsection, where the proof of theorem 2 is completed.

The next theorem easily follows from Theorem 4.1.7 in [4].

THEOREM 6
Let $\varphi(t)$ be a future WMLO formula, $\mathcal{M}$ be a finite probabilistic process and s be a state of $\mathcal{M}$. The probability f_s that $\varphi(0)$ holds in $\mathcal{M}_s$ is computable from $\mathcal{M}$, s and φ.

Lemma 5 (Past Formulas)
Let $\varphi(t)$ be a past WMLO formula, $\mathcal{M}$ be a finite probabilistic process and s_0 be a state of $\mathcal{M}$. There is a probabilistic matrix Q and vectors u and v such that for every $n \in \mathbb{N}$ the probability that $\varphi(n)$ holds in $\mathcal{M}_{s_0}$ is equal to $uQ^n v$. Moreover, Q, u and v are computable from $\mathcal{M}$, s_0 and φ.

PROOF. Let $\varphi(t)$ be a past WMLO formula. A structure S for such a formula φ is defined as an infinite word on the alphabet $\Sigma = 2^{\mathcal{L}}$, where $\mathcal{L}$ is the set of monadic symbols of $\varphi(t)$. The property defined by $\varphi(t)$ depends only on the prefix of size $t+1$ of a model. Thus, from [3], there exists a computable finite complete deterministic automaton $\mathcal{A}$ on the alphabet Σ accepting a language of finite words $L(\mathcal{A})$ such that $S, n \models \varphi(t)$ iff the prefix of S of size $n+1$ belongs to $L(\mathcal{A})$.

Therefore, given the automaton $\mathcal{A}$ and the finite probabilistic process $\mathcal{M}$, we build a new finite probabilistic process $\mathcal{M}'$, the 'product' of $\mathcal{M}$ and $\mathcal{A}$ following the same lines as in Section 4 of [4].

States of $\mathcal{M}'$ are pairs (q, s), where q is a state of $\mathcal{A}$ and s is a state of $\mathcal{M}$. There is a transition from (q, s) to (q', s') iff (q, σ, q') is a transition in $\mathcal{A}$, where σ is the valuation of s in $\mathcal{M}$, and the probability of this transition is the same as the probability of (s, s') in $\mathcal{M}$.

At last, the set of labels $\mathcal{L}'$ of $\mathcal{M}'$ is reduced to one symbol F, and the valuation of (q, s) is $\{F\}$ if q is a final state in $\mathcal{A}$, and $\emptyset$ otherwise.

We have:

$$\mathbf{Prob}_{\mathcal{M}_{s_0}}(\varphi(n)) = \mathbf{Prob}_{\mathcal{M}'_{(q_0, s_0)}}(F(n))$$

where q_0 is the initial state of $\mathcal{A}$ and F is the monadic probabilistic symbol defined by $\mathcal{L}'$.

Let Q be the transition probability matrix of the Markov chain $\mathcal{M}'$, let u be the row vector with zero components, except $u_{(q_0, s_0)}$, which is equal to 1, and let v be the column vector with zero components, except for $v_{(q,s)}$ which are equal to 1 if $q \in F$. We have:

$$\mathbf{Prob}_{\mathcal{M}'_{(q_0, s_0)}}(F(n)) = uQ^n v.$$

So $f_{s_0} = uQ^n v$ is computable. ■

LEMMA 6
Let $\varphi(t_1, t_2)$ be a formula with all first-order quantifiers of the form $\exists t_{\geq t_1}^{\leq t_2}$, and $\psi(t_1)$ be a past formula. Let $\mathcal{M}$ be a finite probabilistic process and s_i, s_j be two of its states. For $n_1, n_2 \in \mathbb{N}$,

$$\mathbf{Prob}_{\mathcal{M}_{s_i}}(\psi(n_1) \wedge S_j(n_1) \wedge \varphi(n_1, n_1 + n_2)) = \mathbf{Prob}_{\mathcal{M}_{s_i}}(\psi(n_1) \wedge S_j(n_1)) \cdot \mathbf{Prob}_{\mathcal{M}_{s_j}}(\varphi(0, n_2)),$$

where $S_j(t)$ is a predicate which is true exactly in state s_j.

PROOF. The set of elements from the probabilistic space $\Omega = s_i S^\omega$, which satisfy $\psi(n_1) \wedge S_j(n_1) \wedge \varphi(n_1, n_1 + n_2)$, can be written as a concatenation product $\Omega_1 \cdot \Omega_2$, where Ω_1 is the set of finite paths of length n_1 starting in s_i ending in s_j and satisfying $\psi(n_1)$ and Ω_2 is the set of infinite paths starting in s_j and satisfying $\varphi(0, n_2)$. This is due to the fact that all quantifiers of φ are of the form $\exists t_{1 \geq t_1}^{\leq t_2}$. Thus,

$$\mathbf{Prob}_{\mathcal{M}_{s_i}}(\psi(n_1) \wedge S_j(n_1) \wedge \varphi(n_1, \ n_1 + n_2)) = \mathbf{Prob}_{\mathcal{M}_{s_i}}(S_j(n_1) \wedge (\psi(n_1)) \cdot \mathbf{Prob}_{\mathcal{M}_{s_j}}(\varphi(0, n_2)).$$

■

LEMMA 7
Let $k, m \in \mathbb{N}$. For $1 \leq i \leq k$, $1 \leq j \leq m$, let $\mathcal{M}_{i,j}$ be a finite probabilistic process, $s_{i,j}$ be a state of $\mathcal{M}_{i,j}$, $\varphi_{i,j}(t_i)$ be a past WMLO formula with only one free variable t_i, and $c_j \in \mathbb{Q}^+$. Let

$$L_p = \left\{ (n_1, \ldots, n_k) \in \mathbb{N}^k : \sum_{1 \leq j \leq m} c_j \cdot \mathbf{Prob}_{\mathcal{M}_{1,j}, s_{1,j}}(\varphi_{1,j}(n_1)) \cdot \cdots \cdot \mathbf{Prob}_{\mathcal{M}_{k,j}, s_{k,j}}(\varphi_{k,j}(n_k)) > p \right\}$$

(1) If $p = 0$, then L_p is ultimately periodic.
(2) If $p \neq 0$, then
   (a) If $k = 1$, then there is a computable finite set H such that, for every rational $p \notin H$, the set L_p is finite or cofinite, i.e. ultimately periodic.
   (b) If $k > 1$, then for every rational $\epsilon > 0$ there is a computable set H that is the union of a finite set of intervals with the total length at most ϵ such that for every rational $p \notin H$ the set L_p is ultimately periodic.

In all the afore mentioned cases a finite representation of L_p is computable.

PROOF. Using Lemma 5, one can compute, for each $1 \leq i \leq k$, and $1 \leq j \leq m$, a probabilistic matrix $Q_{i,j}$, and vectors $u_{i,j}, v_{i,j}$, such that the probability that $(M_{i,j,s_{i,j}}, n_i)$ satisfies $\varphi_{i,j}(t_i)$ is equal to $u_{i,j} \cdot Q_{i,j}^{n_i} \cdot v_{i,j}$.

Let d be the least common multiple of the periods of the Markov chains with the matrix $Q_{i,j}$ (for $1 \leq i \leq k$ and $1 \leq j \leq m$). By Lemma 1, $\lim_{n \to \infty} (Q_{i,j}^d)^n$ exists. Let $Q'_{i,j}$ be $Q_{i,j}^d$. If we write $n_i = r_i + dn'_i$, with $0 \leq r_i < d$, then

$$u_{i,j} \cdot Q_{i,j}^{n_i} \cdot v_{i,j} = u_{i,j} \cdot (Q_{i,j}^d)^{n'_i} \cdot (Q_{i,j}^{r_i} \cdot v_{i,j}) = u_{i,j} \cdot Q'^{n'_i}_{i,j} \cdot v'_{i,j} = a_{i,j,n'_i}.$$

Using Lemma 1, $\lim_{n \to \infty} Q'^n_{i,j}$ exists, so the hypotheses of Lemma 4 are satisfied. Therefore, L_p is an ultimately periodic set with period d, and the present Lemma is proven. ■

LEMMA 8
Let $\mathcal{M}$ be a finite probabilistic process, s be a state of $\mathcal{M}$, and $\varphi(t_1, \ldots, t_k)$ be a WMLO formula with only free variables $t_1, \ldots, t_k$. Let

$$(\mathbb{N}^k)_{\varphi,p} =_{df} \{(n_1, \ldots, n_k) \in \mathbb{N}^k \mid M_s, n_1, n_1 + n_2, \ldots, n_{k-1} + n_k \models \mathbf{Prob}_{>p}(t_1 < t_2 < \cdots < t_k \wedge \varphi(t_1, \ldots, t_k))\}$$

(1) If $p = 0$, then $(\mathbb{N}^k)_{\varphi,p}$ is ultimately periodic.
(2) If $p \neq 0$, then
   (a) If $k = 1$, then there is a computable finite set H such that, for every rational $p \notin H$, the set $(\mathbb{N}^k)_{\varphi,p}$ is finite or cofinite, i.e. ultimately periodic.
   (b) If $k > 1$, then for every rational $\epsilon > 0$ there is a computable set H that is the union of a finite set of intervals with the total length at most ϵ such that for every rational $p \notin H$ the set $(\mathbb{N}^k)_{\varphi,p}$ is ultimately periodic.

In all the aforementioned cases a finite representation of $(\mathbb{N}^k)_{\varphi,p}$ is computable.

PROOF. Using Lemma 2 the formula $t_1 < t_2 < \cdots < t_k \wedge \varphi(t_1, t_2, \ldots, t_k)$ is equivalent to a finite disjunction of formulas of the form:

$$\bigvee_{i \in I} \varphi_{i,\leftarrow}(t_1) \wedge \varphi_{i,1}(t_1, t_2) \wedge \cdots \wedge \varphi_{i,k-1}(t_{k-1}, t_k) \wedge \varphi_{i,\rightarrow}(t_k),$$

where

(1) $\varphi_{i,\leftarrow}(t_1)$ is a past formula.
(2) $\varphi_{i,\rightarrow}(t_k)$ is a future formula.
(3) In $\varphi_{i,j}(t_j, t_{j+1})$ only t_j and t_{j+1} are free and all quantifiers are relativized to between t_j and t_{j+1} (i.e. are of the form $\exists t^{\geq t_{j+1}}_{\leq t_j}$ for $j = 1, \ldots, k-1$).

Moreover, formulas $\varphi_{i,\leftarrow}$, $\varphi_{i,\rightarrow}$, $\psi_{i,j}$ are computable from ψ and for $i_1 \neq i_2$, the disjuncts $\varphi_{i_1,\leftarrow}(t_1) \wedge \psi_{i_1,1}(t_1, t_2) \wedge \cdots \wedge \psi_{i_1,k-1}(t_{k-1}, t_k) \wedge \varphi_{i_1,\rightarrow}(t_k)$ and $\varphi_{i_2,\leftarrow}(t_1) \wedge \psi_{i_2,1}(t_1, t_2) \wedge \cdots \wedge \psi_{i_2,k-1}(t_{k-1}, t_k) \wedge \varphi_{i_2,\rightarrow}(t_k)$ are mutually exclusive.

For each state j of $\mathcal{M}$ we introduce a new probabilistic predicate symbol S_j, and add S_j to the valuation of the state j. Let $\mathcal{M}'$ be the new finite probabilistic process obtained in this way.

The following equalities hold for every tuple of integers $n'_1, \ldots, n'_k$, where Q is the set of states of $\mathcal{M}$:

$$\begin{aligned}
&\mathbf{Prob}_{M_s}(n'_1 < n'_2 < \cdots < n'_k \wedge \varphi(n'_1, n'_2, \ldots, n'_k)) \\
&= \mathbf{Prob}_{M_s}\left(\bigvee_i \varphi_{i,\leftarrow}(n'_1) \wedge \psi_{i,1}(n'_1, n'_2) \wedge \cdots \wedge \psi_{i,k-1}(n'_{k-1}, t_k) \wedge \varphi_{i,\rightarrow}(n'_k)\right) \\
&= \sum_{i \in I} \mathbf{Prob}_{M_s}(\varphi_{i,\leftarrow}(n'_1) \wedge \psi_{i,1}(n'_1, n'_2) \wedge \cdots \wedge \psi_{i,k-1}(n'_{k-1}, t_k) \wedge \varphi_{i,\rightarrow}(n'_k)) \\
&= \sum_{i \in I, j_1, \ldots, j_k \in Q} \mathbf{Prob}_{M_s}(\varphi_{i,\leftarrow}(n'_1) \wedge S_{j_1}(n'_1) \wedge \psi_{i,1}(n'_1, n'_2) \wedge S_{j_2}(n'_2) \wedge \cdots \wedge S_{j_{k-1}}(n'_{k-1}) \\
&\quad \wedge \psi_{i,k-1}(n'_{k-1}, n'_k) \wedge S_{j_k}('n_k) \wedge \varphi_{i,\rightarrow}(n'_k))
\end{aligned}$$

and using Lemma 6 iteratively k times:

$$= \sum_{i\in I, j_1,\ldots j_k\in Q} \mathbf{Prob}_{M_s}(\varphi_{i,\leftarrow}(n_1') \wedge S_{j_1}(n_1')) \cdot \mathbf{Prob}_{M_{j_1}}\ (\psi_{i,1}(0, n_2' -' n_1) \wedge S_{j_2}(n_2' -' n_1)) \ldots$$

$$\ldots \mathbf{Prob}_{M_{jk-1}}(\psi_{i,k-1}(0, n_k' - n_{k-1}') \wedge S_{j_k}(n_k' - n_{k-1}')) \cdot \mathbf{Prob}_{M_{j_k}}(\varphi_{i,\rightarrow}(0)).$$

We can compute the rational constants $\mathbf{Prob}_{M_{j_k}}(\varphi_{i,\rightarrow}(0))$ using Theorem 6. Then, we apply Lemma 7 with $n_1 = n_1'$ and $n_i = n_i' - n_{i-1}'$ for $i = 2, \ldots, k$ to finish the proof.

5.5 Finishing off

Now we are ready to complete the proof of of Theorem 2.

Recall that an *ordered partition* of the set $\{1, \ldots, k\}$ is a tuple $(N_1, \ldots, N_l)$, where N_i are non-empty disjoint subsets of $\{1, \ldots, k\}$ and the union of N_i is $\{1, \ldots, k\}$.

For each $i = 1, \ldots, m$, let ψ_i be the sub-formula of φ of the form $\mathbf{Prob}_{>p_i}\varphi_i(t_1 \ldots, t_k)$. Let Π be the set of ordered partitions $(N_1, \ldots, N_l)$ $(l \leq k)$ of the set $\{1, \ldots, k\}$.

For each ordered partition $\pi = (N_1, \ldots, N_l)$ let θ_π be the formula $\wedge_{i=1,\ldots,l} Eq(N_i) \wedge t_{i_1} < t_{i_2} < \cdots < t_{i_l}$ where i_j is an element in N_j for $j = 1, \ldots, l$ and $Eq(N_i)$ expresses the fact that all the t_j for $j \in N_i$ are equal. The formulas θ_π for $\pi \in$ represent all the different orderings of the values $\{t_1, \ldots, t_k\}$.

Observe that

$$\mathbf{Prob}_{>p_i}\varphi_i(t_1, \ldots, t_k) = \mathbf{Prob}_{>p_i} \bigvee_{\pi\in\Pi} (\theta_\pi(t_1, \ldots, t_k) \wedge \varphi_i(t_1, \ldots, t_k))$$

$$= \bigvee_{\pi\in\Pi} \mathbf{Prob}_{>p_i}(\theta_\pi(t_1, \ldots, t_k) \wedge \varphi_i(t_1, \ldots, t_k))$$

since for a fixed tuple $(n_1, \ldots, n_k)$ exactly one $\theta_\pi(n_1, \ldots, n_k)$ holds.

Let us fix now a partition $\pi = (N_1, \ldots, N_l)$, and let us choose some i_j in each N_j. Let $\varphi'_{i,\pi}(t_{i_1}, \ldots, t_{i_l})$ be the formula obtained from $\varphi_i(t_1, \ldots, t_k)$ by replacing each t_n for n in N_j by t_{i_j}.

The formula

$$\mathbf{Prob}_{>p_i}(\theta_\pi(t_1, \ldots, t_k)\ \wedge\ \varphi_i(t_1, \ldots, t_k))$$

is equivalent to

$$\bigwedge_{i=1,\ldots,l} Eq(N_i) \wedge \mathbf{Prob}_{>p_i}(t_{i_1} < t_{i_2} < \cdots < t_{i_l} \wedge \varphi'_{i,\pi}(t_{i_1}, \ldots, t_{i_l})).$$

One can compute now, using Lemma 8 a set of probabilities $H_{i,\pi}$ not containing zero such that, for each value $\alpha_{i,\pi} \in \mathbb{Q} \setminus H_{i,\pi}$, the set $R_{\alpha_{i,\pi}} = \{(n_1, \ldots, n_l) : M_{s_0}, n_1, n_1 + n_2, \ldots, n_1 + \cdots + n_{l-1} + n_l \models \mathbf{Prob}_{>\alpha_i}(t_{i_1} < t_{i_2} < \cdots < t_{i_l} \wedge \varphi'_{i,\pi}(t_{i_1}, \ldots, t_{i_l}))$ is ultimately periodic with a computable finite representation. Moreover, if $k = 1$, the sets $H_{i,\pi}$ are finite. Using Lemma 3, there is a WMLO formula $\theta_{\alpha_{i,\pi}}(t_{i_l}, \ldots, t_{i_1})$ such that $\theta_{\alpha_{i,\pi}}(n_1, n_1 + n_2, \ldots n_1 + \cdots + n_l)$ holds iff

$(n_1, \ldots, n_l) \in R_{\alpha_{i,\pi}}$. Thus, the PMLO sub-formula $\mathbf{Prob}_{>\alpha_{i,\pi}}(t_{i_1} < t_{i_2} < \cdots < t_{i_l} \wedge \varphi'_{i,\pi}(t_{i_1}, \ldots, t_{i_l}))$ can be replaced by the WMLO formula $\theta_{\alpha_{i,\pi}}(t_{i_1}, \ldots, t_{i_l})$.

Let $H_i = \cup_{\pi \in \Pi} H_{i,\pi}$, and $\alpha = (\alpha_1, \ldots, \alpha_m)$ such that $\alpha_i \in \mathbb{Q} \setminus H_i$ for $i = 1, \ldots, m$. Consider the WMLO formula $\psi(t_1, \ldots, t_k)$ obtained from φ_α, eliminating in the way just described all the probabilistic operators. We have:(M, s_0) satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi(n_1, \ldots, n_k)$. ■

6 Extension of decidable model checking to nested formulas

In class $\mathcal{C}$ we disallow nesting of **Prob** operators. In the following we prove that the decidability results can be extended to formulas with nested **Prob**.

Definition 4
A PMLO formula φ belongs to the class $\mathcal{C}'$ iff in every subformula of the form $\mathbf{Prob}_{>q}\psi$, the formula ψ does not have free second-order deterministic variables.

Definition 5
Let $\epsilon > 0$ be a real number. The ϵ-thin subsets of $\mathbb{Q}^n$ are defined by the induction on n, as follows:

(1) $S \subset \mathbb{Q}$ is ϵ-thin if and only if S can be covered by a finite set of intervals of total length $< \epsilon$.
(2) $S \subset \mathbb{Q}^{d+1}$ is ϵ-thin if there is an ϵ-thin set $S_1 \subset \mathbb{Q}$ and $i \leq d+1$, such that for every $q_i \notin S_1$ the set $\{\langle q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_{d+1}\rangle : \langle q_1, \ldots, q_d, q_{d+1}\rangle \in S\}$ is an ϵ-thin subset of $\mathbb{Q}^d$.

Definition 6
The 0-thin subset of $\mathbb{Q}^n$ are defined by the induction on n as follows:

(1) $S \subset \mathbb{Q}$ is 0-thin if and only if S is finite.
(2) $S \subset \mathbb{Q}^{d+1}$ is 0-thin if there is an 0-thin set $S_1 \subset \mathbb{Q}$ and $i \leq d+1$, such that for every $q_i \notin S_1$ the set $\{\langle q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_{d+1}\rangle : \langle q_1, \ldots, q_d, q_{d+1}\rangle \in S\}$ is 0-thin subset of $\mathbb{Q}^d$.

Observe that if $S_1 \subset \mathbb{Q}^{d_1}$ and $S_2 \subset \mathbb{Q}^{d_2}$ are ϵ-thin (respectively, 0-thin) then their Cartesian product $S_1 \times S_2 \subset \mathbb{Q}^{d_1+d_2}$ is ϵ-thin (respectively, 0-thin).

We say that $H \subseteq \mathbb{Q}^m$ is *computable* if there exists an algorithm that for each m-tuple of rational numbers decides whether it is in H.

Recall that if φ is a parameterized formula with parameters $p_1, \ldots, p_m$, and $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a sequence of rational values, then we denote by φ_α the formula obtained by replacing in φ each parameter p_i by the value α_i.

Theorem 7
Let $\mathcal{M}$ be a finite probabilistic process, s_0 be a state of $\mathcal{M}$ and $\varphi(t_1, \ldots, t_k)$ be a parameterized formula in the class $\mathcal{C}'$ with m parameters.

(1) There exists a WMLO formula $\psi(t_1, \ldots, t_k)$ such that, for each $(n_1, \ldots, n_k) \in \mathbb{N}^k$, (M, s_0) satisfies $\varphi_{(0,\ldots,0)}(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi(n_1, \ldots, n_k)$.
(2) For every rational $\epsilon > 0$, there exists a computable ϵ-thin set $H \subset (\mathbb{Q}^+)^m$, such that for each tuple of (rational) values $\alpha = (\alpha_1, \ldots, \alpha_m) \notin H$ there is a WMLO formula $\psi_\alpha(t_1, \ldots, t_k)$ such that (M, s_0) satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi_\alpha(n_1, \ldots, n_k)$.

(3) If φ is simple, there exists a computable 0-thin set $H \subset (\mathbb{Q}^+)^m$ such that for each tuple of (rational) values $\alpha = (\alpha_1, \ldots, \alpha_m) \notin H$ there is a WMLO formula $\psi_\alpha(t_1, \ldots, t_k)$ such that (M, s_0) satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi_\alpha(n_1, \ldots, n_k)$.

PROOF. The proof is by induction on the depth l of the nesting of **Prob** operators.

First, let us prove Theorem 7(1). In this case the formulas are qualitative.

Inductive base $l = 1$: This case follows from Theorem 2(1).

Inductive step $l - 1 \rightarrowtail l$: Let φ be a parameterized formula of the nesting depth $l > 1$. Let φ_i be all the subformulas of $\varphi_{(0,\ldots,0)}$ of the form $\mathbf{Prob}_{>0}(\beta_i)$, where β_i are WMLO formulas.

By Theorem 2(1), the formulas φ_i are equivalent (over the probabilistic structure generated by (M, s_0)) to WMLO formulas ψ_i. When we replace the subformulas φ_i of $\varphi_{(0,\ldots,0)}$ by ψ_i, we obtain a formula φ', which is equivalent (over the probabilistic structure generated by (M, s_0)) to $\varphi_{(0,\ldots,0)}$ and has nesting depth $l - 1$. Therefore, by the inductive hypothesis, φ' is equivalent (over the probabilistic structure generated by (M, s_0)) to a WMLO formula ψ. Since $\varphi_{(0,\ldots,0)}$ and φ' are equivalent, we derive that $\varphi_{(0,\ldots,0)}$ is equivalent (over the probabilistic structure generated by (M, s_0)) to ψ. This completes the inductive step and the proof of Theorem 7(1).

The proofs for Theorem 7(2) and 7(3) are similar and follow the same arguments as the proof for Theorem 7(1).

In the following, we sketch the proof of Theorem 7(2). In the proof we use 'equivalent' for 'equivalent over the probabilistic structure generated by (M, s_0))'. We also assume that in all parameterized formulas every parameter occurs at most once (this assumption is not essential, but it slightly simplifies the proof).

Inductive base $l = 1$: This case follows from Theorem 2(2) and the observation that the Cartesian product of ϵ-thin subsets of $\mathbb{Q}$ is ϵ-thin.

Inductive step $l - 1 \rightarrowtail l$: Let φ be a parameterized formula of the nesting depth $l > 1$. Let φ_i $(i = 1, \ldots, k)$ be all the sub-formulas of φ of the form $\mathbf{Prob}_{>p_i}(\beta_i)$, where β_i are WMLO formulas.

By Theorem 2(2), there are

(1) Sets H_i $(i = 1, \ldots, k)$ such that H_i is the union of a finite set of intervals with the total length at most ϵ, and
(2) For every $\alpha_i \notin H_i$ there is WMLO formulas ψ^i (which depends on α_i) such that the WMLO formulas ψ^i are equivalent to $\varphi^i_{\alpha_i}$ ($\varphi^i_{\alpha_i}$ is the formula obtained from φ^i when the parameter p_i is replaced by the rational value α_i).

Note that the set $G =_{df} H_1 \times H_2 \times \cdots \times H_k$ is an ϵ-thin subset of $\mathbb{Q}^k$.

Fix $(\alpha_1, \ldots, \alpha_k) \in \mathbb{Q} \setminus G$. Let φ' be obtained from φ by replacing φ_i by ψ_i. Let $p_{k+1}, \ldots, p_m$ be the parameters that occur in φ'. Note that the nesting depth of φ' is $l - 1$. Therefore, by the inductive hypothesis, there is an ϵ-thin $H_{(\alpha_1,\ldots,\alpha_k)} \subset \mathbb{Q}^{m-k}$ such that for every $\widehat{\alpha} \notin H_{(\alpha_1,\ldots,\alpha_k)}$ there is a WMLO formula ψ that is equivalent to $\varphi'_{\hat{\alpha}}$. Hence, $\varphi_{(\alpha_1,\ldots,\alpha_k,\hat{\alpha})}$ is equivalent to ψ. We proved that for every $(\alpha_1, \ldots, \alpha_m) \notin H = G \times \mathbb{Q}^{m-k} \cup \cup_{(\alpha_1,\ldots,\alpha_k) \notin G}(\alpha_1, \ldots, \alpha_k) \times H_{(\alpha_1,\ldots,\alpha_k)}$ there is a WMLO formula ψ that is equivalent to $\varphi_{(\alpha_1,\ldots,\alpha_k,\alpha_m)}$. To complete the proof, it remains to show that H is an ϵ-thin subset of $\mathbb{Q}^m$. The set G is an ϵ-thin subset of $\mathbb{Q}^k$ and for every $(\alpha_1, \ldots, \alpha_k) \notin G$ the set $H_{(\alpha_1,\ldots,\alpha_k)}$ is an ϵ-thin subset of $\mathbb{Q}^{m-k}$. Therefore, H is ϵ-thin. This completes the proof of Theorem 7(2).

The proof of Theorem 7(3) is similar to the proof of Theorem 7(2). ■

As a consequence of Theorem 7, we get the following decidability results:

THEOREM 8 (Qualitative Model Checking)
Given a qualitative sentence φ in the class $\mathcal{C}'$, a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$, it is decidable whether φ holds in the probabilistic structure $\mathcal{M}_s$.

THEOREM 9
Given a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$ and a parametrized simple sentence φ in the class $\mathcal{C}'$ with m parameters, there exists a computable 0-thin set $H \subset (\mathbb{Q}^+)^m$ such that for each tuple of (rational) values $\alpha = (\alpha_1, \ldots, \alpha_m) \notin H$ one can decide whether φ_α holds in the probabilistic structure $\mathcal{M}_s$.

THEOREM 10
Given a finite probabilistic process $\mathcal{M}$, a state s of $\mathcal{M}$ and a parameterized sentence φ in the class $\mathcal{C}'$ with m parameters, for every rational $\epsilon > 0$, there exists a computable ϵ-thin set $H \subset (\mathbb{Q}^+)^m$ such that for each tuple of (rational) values $\alpha = (\alpha_1, \ldots, \alpha_m) \notin H$ one can decide whether φ_α holds in the probabilistic structure $\mathcal{M}_s$.

7 Comparison with probabilistic temporal logic *pCTL**

The logic *pCTL** is one of the most popular among probabilistic temporal logics [2]. The relationship between our logic and *pCTL** is rather complex. The semantics for logic of probability is defined over arbitrary probabilistic structures; however, *pCTL** is defined only for finite probabilistic processes. Moreover, unlike the logic of probability, the truth value of *pCTL** formula depends not only on the probabilistic structure defined by a finite probabilistic process, but also on the 'branching structure' of this process. Hence, there is no meaning preserving translation from *pCTL** to the *monadic* logic of probability. We also show in the following text that, even for the class of models restricted to finite probabilistic processes, no *pCTL** formula is equivalent to the probabilistic formula $\exists t\ \mathbf{Prob}_{\geq 1} Q(t)$, where Q is a probabilistic predicate symbol. The formula $\exists t\ \mathbf{Prob}_{\geq 1} Q(t)$ formalizes a natural property: 'there is a moment at which Q holds with probability one'.

Let us recall the syntax and the semantics of the logic *pCTL** as defined in [2]. Formulas are evaluated on a finite probabilistic process $(S, P, V, \mathcal{L})$.

There are two types of formulas in *pCTL**: state formulas (which are true or false in a specific state) and path formulas (which are true or false along a specific path).

Syntax. State formulas are defined by the following syntax:

(1) Each a in $\mathcal{L}$ is a state formula.
(2) If f_1 and f_2 are state formulas, then so are $\neg f_1$, $f_1 \vee f_2$.
(3) If g is a path formula, then $Pr_{<q}(g)$, $Pr_{>q}(g)$ are state formulas for every rational number q.

Path formulas are defined by the following syntax:

(1) A state formula is a path formula.
(2) If g_1 and g_2 are path formulas, then so are $\neg g_1$, $g_1 \vee g_2$.
(3) If g_1 and g_2 are path formulas, then so are Xg_1, $g_1 U g_2$.
(X and U are respectively the *Next* and *Until* temporal operators).

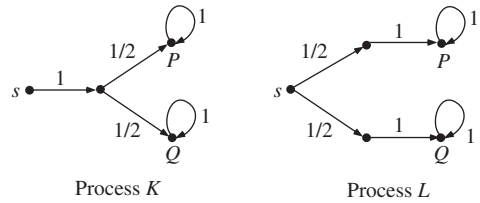

FIGURE 2. Two processes distinguishable by *pCTL** formula

Semantics. Given a finite probabilistic process $\mathcal{M} = (S, P, V, \mathcal{L})$, state formulas and path formulas are interpreted as defined below. Formulas f_1 and f_2 are state formulas and g_1 and g_2 are path formulas. Let s be a state, and Π be an arbitrary infinite path in $\mathcal{M}$. Satisfaction of a state formula is defined with respect to s, and satisfaction of a path formula with respect to Π. For each integer $k \geq 0$, we denote by Π^k the path obtained from Π when removing the first k states (thus $\Pi^0 = \Pi$), and we denote by $[\Pi]_k$ the kth state of Π.

- $\mathcal{M}, s \models Q$ iff $a \in V(Q)$,
- $\mathcal{M}, s \models \neg f_1$ iff $\mathcal{M}, s \not\models f_1$, $\mathcal{M}, s \models f_1 \vee f_2$ iff $\mathcal{M}, s \models f_1$ or $\mathcal{M}, s \models f_2$,
- $\mathcal{M}, s \models \mathbf{Prob}_{>q}(g_1)$ iff $\mu\{\sigma \in sS^\omega \mid M, \sigma \models g_1\} > q$ $\mathcal{M}, s \models \mathbf{Prob}_{<q}(g_1)$ is defined in a similar way,
- $\mathcal{M}, \Pi \models f_1$ iff $[\Pi]_0 \models f_1$,
- $\mathcal{M}, \Pi \models \neg g_1$ iff $\mathcal{M}, \Pi \not\models g_1$, $M, \Pi \models g_1 \vee g_2$ iff $\mathcal{M}, \Pi \models g_1$ or $\mathcal{M}, \Pi \models g_2$,
- $\mathcal{M}, \Pi \models Xg_1$ iff $\mathcal{M}, \Pi^1 \models g_1$,
- $\mathcal{M}, \Pi \models g_1 U g_2$ iff there exists $k \geq 0$ such that $\mathcal{M}, \Pi^k \models g_2$ and for all $0 \leq j < k$, $\mathcal{M}, \Pi^j \models g_1$.

In the following we give an example that illustrates differences between the logic of probabilities and *pCTL**. Consider the finite probabilistic processes K and L as shown in Figure 2. Let φ be the following *pCTL** formula

$$\mathbf{Prob}_{=1}\big(X(\mathbf{Prob}_{=1/2}(XP) \wedge \mathbf{Prob}_{=1/2}(XQ))\big).$$

Note that $K, s \models \varphi$ but $L, s \not\models \varphi$. However, the probabilistic structures K_s and L_s are the same. Hence, unlike the truth value of logic of probability, the truth value of *pCTL** formula depends not only on the probabilistic structure defined by the finite probabilistic process, but also on the 'branching structure' of this process. Therefore, there is no meaning preserving translation from *pCTL** to the *monadic* logic of probability.

In the rest of this section we show that even for the class of models restricted to finite probabilistic processes, no *pCTL** formula is equivalent to the probabilistic formula $\exists t\, \mathbf{Prob}_{\geq 1} Q(t)$, where Q is a probabilistic predicate symbol (the formula $\exists t\, \mathbf{Prob}_{\geq 1} Q(t)$ expresses a natural property: there is a moment at which Q holds with probability one). More precisely, we show:

THEOREM 11
Let $\varphi = \exists t\, \mathbf{Prob}_{\geq 1} Q(t)$ where Q is a probabilistic predicate symbol. There is no *pCTL** formula ψ such that for every finite probabilistic process $\mathcal{M}$ and every state s of $\mathcal{M}$ one has $\mathcal{M}_s \models \varphi$ iff $\mathcal{M}, s \models \psi$.

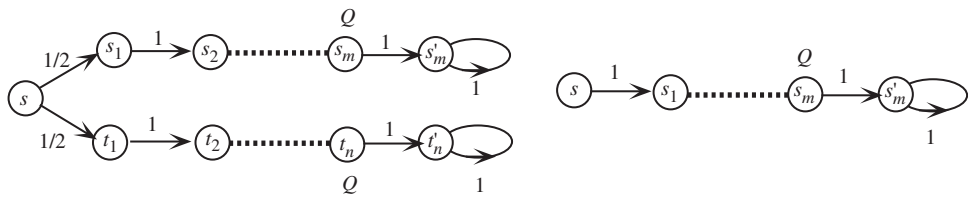

FIGURE 3. $K_{m,n}$ and K_m

Consider the finite probabilistic processes $\mathcal{K}_{m,n}$ and $\mathcal{K}_m$ for $m \geq 1$ and $n \geq 1$ as shown in Figure 3. Edges (i,j) are labelled by probabilities $P(i,j)$. Process $\mathcal{K}_m$ contains only one state (state s_m) labelled by the probabilistic predicate Q; other states have the empty labels and process $\mathcal{K}_{m,n}$ contains only two states (states s_m and t_n) labelled by the probabilistic predicate Q. Let us call Π_m the unique infinite path starting in s in $\mathcal{K}_m$.

LEMMA 9

(1) For every *pCTL** path formula g, there exists an integer $r \geq 1$ such that, for every $m \geq r$, $\mathcal{K}_m, \Pi_m \models g$ iff $\mathcal{K}_r, \Pi_r \models g$.
(2) For every *pCTL** state formula f, there exists an integer $r \geq 1$ such that for every $m, n \geq r$, $\mathcal{K}_{m,n}, s \models f$ iff $\mathcal{K}_{r,r}, s \models f$.

PROOF. The proof is by induction on the complexity of g and f.

(1) The key point is for a path formula of the form Xg. We have

$$\mathcal{K}_m, \Pi_m \models Xg \text{ iff } m > \text{ and } \mathcal{K}_{m-1}, \Pi_{m-1} \models g.$$

By induction, there exists an integer r such that for $m - 1 \geq r$,

$$\mathcal{K}_{m-1}, \Pi_{m-1} \models g \text{ iff } \mathcal{K}_r, \Pi_r \models g.$$

At last,

$$\mathcal{K}_r, \Pi_r \models g \text{ iff } \mathcal{K}_{r+1}, \Pi_{r+1} \models Xg.$$

Thus, for $m \geq r + 1$, $\mathcal{K}_m, \Pi_m \models Xg$ iff $\mathcal{K}_{r+1}, \Pi_{r+1} \models Xg$.

(2) Here the key point is for a formula f of the form $\mathbf{Prob}_{>q}(g)$. Notice that for $q \geq 1/2$,

$$\mathcal{K}_{m,n}, s \models \mathbf{Prob}_{>q}(g) \text{ iff } \mathcal{K}_m, \Pi_m \models g \text{ and } \mathcal{K}_n, \Pi_n \models g$$

for $q < 1/2$,

$$\mathcal{K}_{m,n}, s \models \mathbf{Prob}_{>q}(g) \text{ iff } \mathcal{K}_m, \Pi_m \models g \text{ or } \mathcal{K}_n, \Pi_n \models g.$$

Then we use (1). ■

Finally, we are ready to prove Theorem 11.

PROOF OF THEOREM 11
Let us suppose that such a *pCTL** formula ψ exists. From Lemma 9, there exists an integer $r \geq 1$ such that for every $m, n \geq r$, $\mathcal{K}_{m,n}, s \models \psi$ iff $\mathcal{K}_{r,r}, s \models \psi$. That contradicts the fact that $\mathcal{K}_{m,n}, s \models \varphi$ iff $m = n$. ■

8 Conclusion

Our main result is a description of a fragment of a logic of probability with decidable model checking. An important and difficult open question is whether one can prove the decidability of model checking for all values of probabilistic parameters, without exceptions. Another open question is to extend the above results to formulas with conditional probabilities. Here, we point to some difficulties which should be faced in order to extend our model-checking results.

8.1 Extension to all values of parameters

Recall that the central step in the model checking problem is based on decidability of the following problem:

Problem A
Instance: A probabilistic rational matrix M, its states s_1, s_2 and a rational r.
Task: Check whether there is n such that $(M^n)_{1,2} = r$.

In Section 4, we explained that for given M, s_1 and s_2 it is easy to decide Problem A for all but finitely many values of A. These 'bad' values are accumulating points of the sequence $\{(M^n)_{1,2}\}$. It is an open question whether Problem A is decidable.

It might be the case that there is a reduction between Problem A and the following Skolem problem [19].

Skolem Problem
Instance: An integer matrix M.
Task: Check whether there is n such that $(M^n)_{1,1} = 0$.

Decidability of the Skolem Problem is open for more than 60 years. It would be interesting to investigate the relationship between Problem A and the Skolem Problem.

8.2 Extension to formulas with conditional probabilities

Let us illustrate here some obstacles that arise in the attempt to extend the model-checking results to the formulas with conditional probabilities.

Assume that $\mathcal{M}$ is a finite state labelled Markov chain. Moreover, assume that: (i) $\mathcal{M}$ is regular, i.e., its matrix M is such that $\lim_{n\to\infty} M^n$ exists and (ii) there is exactly one state s_1 labelled by a predicate Q_1 and there is exactly one state s_2 labelled by a predicate Q_2.

Let $\varphi(t)$ be the formula $\mathbf{Prob}_{>1/2}(Q_1(t)|Q_1(t) \vee Q_2(t))$.

In order to check whether φ is satisfiable in the structure $\mathcal{M}_{s_0}$, we can do the following.

First, observe that the probability that $Q_1(t)$ (respectively, $Q_2(t)$) holds at moment n in the structure $\mathcal{M}_{s_0}$ is $(P^n)_{0,1}$ (respectively, $(P^n)_{0,2}$).

Therefore, $\mathbf{Prob}_{>1/2}(Q_1(t)|Q_1(t) \vee Q_2(t))$ holds at n in $\mathcal{M}_{s_0}$ iff $((M^n)_{0,1})/((M^n)_{0,1} + (M^n)_{0,2}) > 1/2$.

Now if $\lim_{n\to\infty}(M^n)_{0,1} + (M^n)_{0,2} > 0$, then for all but finitely many r we can check whether $\mathbf{Prob}_{>r}(Q_1(t)|Q_1(t) \vee Q_2(t))$ is satisfiable in $\mathcal{M}_{s_0}$. However, in the case when $\lim_{n\to\infty}(M^n)_{0,1} + (M^n)_{0,2} = 0$ we do not know how to verify the satisfiability in $\mathcal{M}_{s_0}$.

It is an open question whether the following conjecture holds:

CONJECTURE
Let (S, M) be a finite Markov chain. There exists a positive natural number d such that the limits

$$\lim_{m\to\infty} \frac{(M^{r+dm})_{0,1}}{(M^{r+dm})_{0,1} + (M^{r+dm})_{0,2}}$$

exist for $r = 0, 1, \ldots, d-1$.

Nevertheless, one can give a partial result following the same lines:

PROPOSITION 7
Let $\mathcal{M}$ be a finite probabilistic process, s_0 be a state of $\mathcal{M}$, and $\varphi(t), \varphi'(t)$ be two WMLO formulas with one free variable.

If the set $\{\mathbf{Prob}(\varphi'(n) \mid n \in \mathbb{N}\}$ does not admit 0 as an accumulation point (this fact is property is decidable), one can compute a finite set H of rational values not containing zero, such that for each rational $\alpha \in \mathbb{Q} \setminus H$, one can compute a WMLO formula $\psi_\alpha(t)$ such that for $n \in \mathbb{N}(\mathcal{M}, s_0)$ satisfies $\mathbf{Prob}_\alpha(\varphi(n) \mid \varphi'(n)$ iff $(\mathbb{N}, <) \models \psi(n))$.

8.3 Extension to parametric model checking

With some additional effort, one can get a similar algorithm for parametric model checking. Parameters here are the values of probabilities p in operators $\mathbf{Prob}_{>p}$. The problem is to compute for a given Finite process $\mathcal{M}$, a state s of $\mathcal{M}$ and a parameterized PMLO sentence φ with m parameters, the set of tuples $\alpha = (\alpha_1, \ldots, \alpha_m)$ for which φ_α holds in $\mathcal{M}_s$.

Let us call a m-box of $\mathbb{R}^m$ a product of m intervals of $\mathbb{R}$. The set of parameter values $\alpha = (\alpha_1, \ldots, \alpha_m)$ for which an equivalent WMLO formula can be computed can be described as a finite set of boxes. And the main point is that the WMLO formula $\psi_\alpha(t_1, \ldots, t_k)$, which is computed in Theorem 2, depends not in α but only on the box which α belongs to.

THEOREM 12
Let $\mathcal{M}$ be a finite probabilistic process, s_0 be a state of $\mathcal{M}$, and $\varphi(t_1, \ldots, t_k)$ be a parameterized formula without free predicate variables and with m parameters.

If formula φ is in the class $\mathcal{C}$, then for each rational number $\epsilon > 0$, one can compute for each parameter p_i in φ $(i = 1, \ldots, m)$ a set H_i that is union of a finite set of intervals not containing zero, with a total length less than ϵ, and a finite set of m-boxes B_j, $1 \le j \le r$ that cover $\Pi_{1\le i\le m}([0, 1] \setminus H_i)$ such that for each $j = 1, \ldots, r$, one can compute a WMLO formula $\psi_j(t_1, \ldots, t_k)$ such that for each tuple of rationals $\alpha = (\alpha_1, \ldots, \alpha_m) \in B_j$, for each $n_1, \ldots, n_k \in \mathbb{N}$ $(\mathcal{M}, s_0)$ satisfies $\varphi_\alpha(n_1, \ldots, n_k)$ iff $(\mathbb{N}, <) \models \psi_j(n_1, \ldots, n_k)$.

References

[1] M. Abadi and J. Halpern. Decidability and expressiveness for first-order logic of probability. *Information and Computation*, **112**, 1–36, 1994.

[2] A. Aziz, V. Singhal, F. Balarin, R. K. Brayton and A. L. Sangiovanni-Vincentelli. It usually works: the temporal logic of stochastic systems. In *Computer Aided Verification. Proceeding of CAV'95*, pp. 155–165. Volume 939 of *Lecture Notes in Computer Science*, Springer Verlag, 1995.
[3] J. R. Büchi. Weak second-order arithmetic and finite automata. *Zeitschrift fur Mathematische logik und Grundlagen der Mathematic*, **5**, 66–92, 1960.
[4] C. Courcoubetis and M. Yannakakis. The complexity of probabilistic verification. *Journal of the ACM*, **42**, 857–907, 1995.
[5] R. Fagin and J. Halpern. Reasoning about knowledge and probability. *Journal of the Association for Computing Machinery*, **41**, 340–367, 1994.
[6] R. Fagin, J. Y. Halpern and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, **87**, 78–128, 1990.
[7] F. R. (Feliks Ruvimovich) Gantmakher. *The Theory of Matrices*. Chelsea Pub. Co., New York, 1977.
[8] D. Gabbay, I. Hodkinson and M. Reynolds. *Temporal Logic*. Clarendon Press, Oxford, 1994.
[9] J. Halpern. An analysis of first-order logics of probability. *Artificial Intelligence*, **46**, 311–350, 1990.
[10] V. Halava. Decidable and undecidable problems in matrix theory. Technical Report 127, University of Turku, Turku Center for Computer Science, 1997.
[11] H. A. Hansson. *Time and Probability in Formal Design of Distributed Systems*. Elsevier, 1994. Series: 'Real Time Safety Critical System', vol. 1. Series Editor: H. Zedan.
[12] H. A. Hansson and B. Jonsson. A logic for reasoning about time and probability. *Formal Aspects of Computing*, **6**, 512–535, 1994.
[13] W. Hodges. *Model theory*. Cambridge University Press, 1993.
[14] H. J. Keisler. Probability quantifiers. In J. Barwise and S. Feferman, eds, *Model-Theoretic Logics*, pp. 509–556. Springer, New York, 1985.
[15] J. G. Kemeny and J. L. Snell. *Finite Markov Chains*. D Van Nostad Co., Inc., Princeton, N.J., 1960.
[16] J. G. Kemeny, J. L. Snell and A. W. Knapp. *Denumerable Markov Chains*. D Van Nostad Co., Inc., Princeton, N.J., 1966.
[17] D. Lehmann and S. Shelah. Reasoning about time and chance. *Information and Control*, **53**, 165–198, 1982.
[18] A. R. Meyer. Weak monadic second-order theory of successor is not elementary recursive. *Logic Colloquium, Proc. Symposium on Logic, Boston*, pp. 132–154, 1975.
[19] G. Norman, D. Parker, J. Rutten and M. Kwiatkowska. *Mathematical Techniques for Analyzing Con-current and Probabilistic Systems*, vol. 23. American Mathematical Society, 2004.
[20] W. Thomas. Automata on infinite objects. In J. van Leeuwen, ed., *Handbook of Theoretical Computer Science*, pp. 131–191. North-Holland, 1990.

Received 12 October 2003