

Possibilistic and probabilistic abstraction-based model checking

Michael Huth

Department of Computing, Imperial College of Science, Technology and Medicine,
180 Queen's Gate, London, SW7 2BZ, United Kingdom, huth@cis.ksu.edu

Abstract. We present a framework for the specification of abstract models whose verification results transfer to the abstracted models for a logic with unrestricted use of negation and quantification. This framework is novel in that its models have quantitative or probabilistic observables and state transitions. Properties of a quantitative temporal logic have measurable denotations in these models. For probabilistic models such denotations approximate the probabilistic semantics of full LTL. We show how predicate-based abstractions specify abstract quantitative and probabilistic models with finite state space.

1 Introduction

Probabilistic models of concurrent systems [45] are important for the quantitative design and analysis of safety-critical systems [24]. Such models are also indispensable for the analysis of quantitative behavior in a wide variety of systems, e.g. through the computation of performance measures [26]. Formal analysis of probabilistic models does not scale well. Model checking LTL formulas on concurrent labeled Markov chains is polynomial in the size of models and doubly exponential in the size of formulas [12]. These complexity bounds inflate the effects of the state-explosion problem, that the number of states of a composed model is often exponential in the number of its components. Therefore, probabilistic verification of realistic models requires the use of aggressive abstraction techniques.

Model checks $\mathcal{M} \models \phi$ can be abstracted by simplifying the model \mathcal{M} [10], the property ϕ [25], or the satisfaction relation \models . To be effective, such simplifications need to ensure that they render sound, and hopefully useful, analysis results. For qualitative systems, we present instances for all of these simplifications, prove their soundness, and discuss their utility for analyzing probabilistic systems.

These instances are realized by transferring work on three-valued model checking [33, 5, 6, 29, 22] to the realm of probabilistic verification. Three-valued models allow specifiers to state under-determinacy in non-deterministic choices: if “There are possible delays on the Bakerloo Line.” is the only available information, then it should not mean “For all other lines, there are no delays.” This additional expressiveness is also critically needed for the computation of abstract models whose verified properties carry over to the models they abstract, where

properties range over a full logic with negation and quantification. Such a range is required, for example, if one mixes abstraction-based checks with simple fairness assumptions [3, 28] or for the verification of properties that combine safety and liveness aspects. We offer this transfer also for systems whose quantities are specified in any partial order (cost, total energy, weighted sums, etc).

The resulting relational calculus for specifying and computing sound abstract models works well for abstractions based on finite, measurable partitions of the underlying state space, making it a powerful tool for practical verification tasks. However, models require that basic observables be measurable. This limits the freedom of specifying models as well as the scope of the applicability of our relational abstraction calculus from a foundational point of view. It is hoped that a more general theory will emerge from this paper that generalizes its results to abstractions that are continuous-state concurrent labeled Markov chains. Markov kernels [21], as outlined in [38, 18, 19], are a likely candidate for such a theory.

Since this paper works with a branching-time logic, we are able to give a coordinated approximation of the satisfaction relation and thresholds of probabilistic LTL formulas. Although we cannot yet comment on the practical utility of this abstraction, it has apparent connections to bounded model checking techniques [9].

Outline of paper. In Section 2 we survey existing work on abstraction of probabilistic systems. Section 3 generalizes labeled concurrent Markov chains to modal quantitative structures and develops our notions of possibilistic abstraction and refinement. A possibilistic property semantics for a quantitative mu-calculus is given in Section 4, its consistency and soundness with respect to refinement is proved and a path lemma (for CTL* formulations) is shown. In Section 5, we prove that our possibilistic property semantics is an abstraction of the usual branching-time probabilistic logic PCTL of Hansson [24] for modal probabilistic systems. A systematic way of specifying abstract models through an abstraction relation on states is presented in Section 6 and its soundness and compositionality proved. We show that a modal version of probabilistic simulations [30] is the operational equivalent of our possibilistic refinement for functional and discrete abstractions. Finally, Section 7 concludes.

2 Related work

Di Pierro and Wiklicky [41] use the Moore-Penrose pseudo-inverse of linear operators to re-cast Galois connections, which require orderings, in the setting of vector spaces; this allows for a re-formulation of soundness and optimality principles for abstract interpretations in linear spaces. Monniaux [36] systematically develops abstract interpretations of infinite-state concurrent Markov chains [45]; these analyses may use state-space partitioning.

Jonsson and Larsen [30] generalize probabilistic bisimulation [32] to a satisfaction relation between probabilistic specifications — multi-set versions of probabilistic transition systems — and probabilistic transition systems; two notions

and algorithms for refinement between probabilistic specifications are presented. D’Argenio et al. [15] define simulations between concurrent Markov chains that are based on a discrimination criterion and the co-inductive existence of distributions. Such simulations allow for the sound verification of safety properties and incremental refinement of abstractions driven by refutation evidence.

Clark et al. [8] present a program analysis of probabilistic idealized Algol that collects possibilistic information flow between high and low security variables; this (abstract) analysis is shown to be sound for the probabilistic non-interference of Sabelfeld and Sands [43]. Di Pierro et al. [40] provide a quantitative version of identity confinement for probabilistic concurrent constraint programming (without non-determinism), using a probabilistic version of the widening operator [13] for a safe abstraction of their concrete collection semantics.

In the framework of probabilistic automata, Segala and Lynch present and investigate several notions of probabilistic simulations with respect to compositionality — where these notions fare well — and the preservation of properties written in probabilistic CTL [24] — where these notions fare poorly.

Desharnais et al. [17] approximate continuous-state Markov processes by a family of finite-state labeled Markov chains; they define a notion of (probabilistic) simulation and prove its soundness with respect to a fragment of probabilistic propositional modal logic. Vardi (e.g. [46]) shows that properties of the form “with probability 1 satisfies ϕ ” can be expressed as an ergodic analysis and therefore checked through automata-theoretic means.

Morgan et al. [37] study a probabilistic version of the process algebra CSP and show that probabilistic choice distributes through all other operators; a failure/divergence semantics [27] supplies a refinement notion between such processes. MvIver [34] generalizes stationary distributions of Markov processes to models of probabilistic programs that include non-determinism (abstraction) with support for Dijkstra-style reasoning.

For a simple but practically important fragment of temporal logic, Zuck [47] replaces probabilistic assumptions with strong fairness assumptions and thereby reduces P-validity checks on parameterized probabilistic systems to validity checks over non-probabilistic programs.

Andova and Baeten [1] define a branching probabilistic bisimulation for a probabilistic process algebra without non-deterministic choice whose rooted branching variant is a congruence with respect to sequential composition and probabilistic choice; abstractions operate on internal actions.

3 Modal quantitative systems

We present modal versions of *quantitative* models for abstraction-based model checking. Labeled concurrent Markov chains [16, 45] and their modal abstractions turn out to be a special instance of such models. In a partial order (P, \leq) , we write \geq for the relational inverse $\{(r, r') \in P \times P \mid r' \leq r\}$ of \leq . The relation $<$ is obtained by removing from \leq the diagonal $\{(r, r') \in P \times P \mid r = r'\}$ of P ; as customary, its inverse is denoted by $>$.

Definition 1 (Modal quantitative Kripke structures).

1. Let \mathcal{F} be a σ -algebra [23] over a state set Σ , (P, \leq) a partial order of quantities, and $[\mathcal{F} \rightarrow P]$ the set of monotone (total) functions of type $(\mathcal{F}, \subseteq) \rightarrow (P, \leq)$; elements of $[\mathcal{F} \rightarrow P]$ are quantitative measures.
2. Given a set \mathbf{AP} of state observables, a quantitative Kripke structure \mathcal{K} with signature $(\mathbf{AP}, \mathcal{F}, P)$ is a triple (Σ, R, L) , where $L: \Sigma \rightarrow \mathcal{P}(\mathbf{AP})$ is a labeling function and $R \subseteq \Sigma \times [\mathcal{F} \rightarrow P]$ a transition relation such that for all $A \in \mathcal{F}$, $\sqsupseteq \in \{ \geq, > \}$, $r \in P$, and $p \in \mathbf{AP}$

$$\text{pre}_{\sqsupseteq r}(A) \stackrel{\text{def}}{=} \{s \in \Sigma \mid \exists (s, \mu) \in R, \mu(A) \sqsupseteq r\} \in \mathcal{F} \quad (1)$$

$$\{s \in \Sigma \mid p \in L(s)\} \in \mathcal{F};$$

3. a modal quantitative Kripke structure \mathcal{M} with signature $(\mathbf{AP}, \mathcal{F}, P)$ is a pair $(\mathcal{M}^a, \mathcal{M}^c)$ of quantitative Kripke structures $\mathcal{M}^m = (\Sigma, R^m, L^m)$, $m \in \{a, c\}$, with the same signature such that $R^a \subseteq R^c$ and $L^a(s) \subseteq L^c(s)$ for all $s \in \Sigma$.

Throughout this paper, we assume that modal quantitative Kripke structures are *finitely branching*: for all $m \in \{a, c\}$ and $s \in \Sigma$, the set $\{\mu \in [\mathcal{F} \rightarrow P] \mid (s, \mu) \in R^m\}$ is finite. Since every probability measure is also a quantitative measure [23], our models are generalizations of established systems that combine non-determinism and probabilistic transitions. Our abstractions of probability measures in Section 6 turn out to be probability measures if boolean or cartesian abstraction is used.

Example 1. Neural systems. Given a Kripke structure with finite state set Σ and state observables \mathbf{AP} , we transform it into a quantitative Kripke structure for the partial order $[0, \infty)$. Let \mathcal{F} be $\mathcal{P}(\Sigma)$. We endow each state $s \in \Sigma$ with a stimulus $k_s \in [0, \infty)$. Each vector of weights $(w_s)_{s \in \Sigma}$ with $w_s \in [0, \infty)$ then determines an element $\mu \in [\mathcal{F} \rightarrow [0, \infty)]$ given by

$$\mu(A) = \sum_{a \in A} w_a \cdot k_a. \quad (2)$$

To complete the model, we specify a labeling function L and transitions of the form (s, μ) such that all μ can be represented in the form of (2). The semantics of modal operators is then similar to the effects of information propagation in neural networks [42]. Let A be the set of all states that satisfy $p \in L(s)$. Checking whether $\text{EX}_{\sqsupseteq r} p$ holds at s_0 — as specified in Section 4 — amounts to verifying whether there is a transition $(s_0, \mu) \in R$ such that the weighted sum in (2) is $\sqsupseteq r$. In our framework of quantitative systems, the stimuli k_s are static and the monotonicity of μ demands that all weights w_s and stimuli k_s be non-negative.

Concurrent labeled Markov chains. Finite-state modal quantitative Kripke structures that satisfy $\mathcal{M}^a = \mathcal{M}^c$ and $\mathcal{F} = \mathcal{P}(\Sigma)$ and whose quantitative measures are probability measures are essentially labeled concurrent Markov chains [45] (without designated fair states).

An abstraction. Figure 1 depicts a concurrent labeled Markov chain (left) and its abstraction (right), which we re-visit in Section 6.

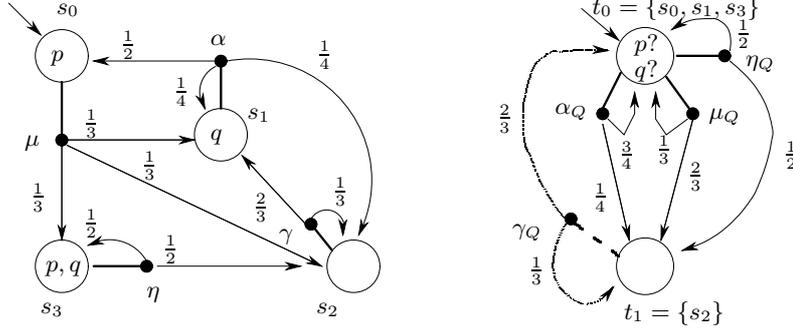


Fig. 1. Left: a graphical representation of a concurrent, labeled Markov chain. Right: predicate abstraction, along the predicate $p \vee q$, of the model on the left. The only R^a -transition is γ_Q . We write $p?$ for $p \in L^c(t_0) \setminus L^a(t_0)$ etc.

In this paper, we base the specification of abstract models on relations. For $Q \subseteq \Sigma_1 \times \Sigma_2$, $A \subseteq \Sigma_1$, and $B \subseteq \Sigma_2$, we recall the standard relational navigation $A.Q \stackrel{\text{def}}{=} \{t \in \Sigma_2 \mid \exists a \in A : (a, t) \in Q\}$ and $Q.B \stackrel{\text{def}}{=} \{s \in \Sigma_1 \mid \exists b \in B : (s, b) \in Q\}$. In measure theory, it is well known that relational navigation does not mix well with the preservation or reflection of measurable sets. Nonetheless, this paper uses relational navigation as a means for specifying abstract models, since important abstraction techniques can be carried out successfully with such a pedestrian approach. Thus, we offer a direct means of specifying boolean and cartesian abstractions for practitioners, but we encounter limitations if more general abstractions are desired. A general theory for abstraction of probabilistic systems, with Markov kernels as the prime candidates, is desirable.

Definition 2 (Measurable navigation). *Given two σ -algebras $(\Sigma_1, \mathcal{F}_1)$ and $(\Sigma_2, \mathcal{F}_2)$, a relation $Q \subseteq \Sigma_1 \times \Sigma_2$ has measurable navigation iff for all $A \in \mathcal{F}_1$ and $B \in \mathcal{F}_2$, $A.Q \in \mathcal{F}_2$ and $Q.B \in \mathcal{F}_1$.*

We emphasize that relations do not have measurable navigation in general, but we show in Section 6 that important abstraction relations do enjoy that property. For that, condition (1) is needed to ensure that all properties of our logic denote measurable sets; this is a non-condition for finite systems.

Before we present a property semantics for modal quantitative systems, we discuss their co-inductive definition of possibilistic refinement and abstraction. These notions require a lift of relations over state spaces to relations over quantitative measures. Our definitions assume a fixed partial order P and our results hold for all partial orders.

Definition 3 (Lifting relations to quantitative measures). *For every $Q \subseteq (\Sigma, \mathcal{F}) \times (\Sigma, \mathcal{F})$ with measurable navigation, we define $Q^{\text{ps}} \subseteq [\mathcal{F} \rightarrow P] \times [\mathcal{F} \rightarrow P]$ by $(\mu, \eta) \in Q^{\text{ps}}$ iff for all $A, B \in \mathcal{F}$, $\eta(A.Q) \geq \mu(A)$ and $\mu(Q.B) \geq \eta(B)$.*

Possibilistic refinements of modal quantitative Kripke structures are defined as for Kripke modal transition systems [29], except that the co-inductive constraints are put on pairs of quantitative measures (and not pairs of states) via Q^{ps} .

Definition 4 (Possibilistic refinement and abstraction). *Let \mathcal{M} be a modal quantitative Kripke structure $(\mathcal{M}^a, \mathcal{M}^c)$ with signature $(\text{AP}, \mathcal{F}, P)$.*

1. *A relation $Q \subseteq (\Sigma, \mathcal{F}) \times (\Sigma, \mathcal{F})$ with measurable navigation is a possibilistic refinement in \mathcal{M} iff $(s, t) \in Q$ implies*
 - (a) *whenever $(t, \eta) \in R^a$, there is some $(s, \mu) \in R^a$ such that $(\mu, \eta) \in Q^{\text{ps}}$;*
 - (b) *whenever $(s, \mu) \in R^c$, there is some $(t, \eta) \in R^c$ such that $(\mu, \eta) \in Q^{\text{ps}}$;*
 - (c) *$L^a(t) \subseteq L^a(s)$ and $L^c(s) \subseteq L^c(t)$.*
2. *The relational inverse Q^{-1} of a refinement Q is a possibilistic abstraction.*

Given modal quantitative Kripke structures $\mathcal{M}_i = ((\Sigma_i, R_i^a, L_i^a), (\Sigma_i, R_i^c, L_i^c))$ with $i = 1, 2$ and signatures over the same partial order (P, \leq) , we can define their sum $\mathcal{M}_1 + \mathcal{M}_2$, whose state space, state observables, and σ -algebra are the sum of the respective two structures. Thus, Definition 4 also applies *between* such models (with initial state) in the usual manner. If all measures of \mathcal{M}_1 and \mathcal{M}_2 are probabilistic, then that is also the case for their sum.

Co-inductive, monotone definitions over complete lattices have a greatest fixed point [39, 35]. Since σ -algebras are not complete lattices in general, we need to ensure that the computation of such a greatest fixed point resides within a given σ -algebra. This is guaranteed for finite-state systems.

Proposition 1 (Greatest possibilistic refinement). *For every modal quantitative Kripke structure \mathcal{M} with signature $(\text{AP}, \mathcal{F}, P)$, possibilistic refinements in \mathcal{M} are closed under the diagonal $\{(s, s) \mid s \in \Sigma\}$ of Σ , relational composition, and countable unions. In particular, for finite Σ the greatest possibilistic refinement $\prec_{\mathcal{M}}$ exists in \mathcal{M} and is a preorder on Σ .*

Proof. The diagonal of Σ is a possibilistic refinement, since the order on P is reflexive.

Possibilistic refinements Q_1 and Q_2 are closed under composition because the transitivity of \geq in P implies $(Q_1)^{\text{ps}}; (Q_2)^{\text{ps}} \subseteq (Q_1; Q_2)^{\text{ps}}$.

Possibilistic refinements Q_i are closed under countable unions, since $A \mapsto A.Q$ and $B \mapsto Q.B$ preserve all unions, so $(Q_{i_0})^{\text{ps}} \subseteq (\bigcup_{i \in I} Q_i)^{\text{ps}}$ for all i_0 in the countable set I .

For finite Σ , the union of all possibilistic refinements is finite which, by the above, is reflexive and transitive. ■

4 Possibilistic property semantics

We consider the logic \mathcal{L}_{pr} , a quantitative mu-calculus, defined by $\phi ::= \text{tt} \mid p \mid Z \mid \neg\phi \mid \phi \wedge \phi \mid \text{EX}_{\sqsupseteq, r}\phi \mid \mu Z.\phi$, where $Z \in \text{var}$ for a countable set of recursion variables var , $p \in \text{AP}$, r ranges over elements of a partial order (P, \leq) , \sqsupseteq equals \geq or $>$, and

all ϕ are formally monotone in $\mu Z.\phi$. For $\rho = (\rho^a, \rho^c)$ with $\rho^m: \text{var} \rightarrow \mathcal{F}$, $m \in \{a, c\}$, we write $s \models_\rho^a \phi$ (positive assertion check) and $s \models_\rho^c \phi$ (positive consistency check) iff $s \in \llbracket \phi \rrbracket_\rho^a$ and $s \in \llbracket \phi \rrbracket_\rho^c$, respectively.

Remark 1. Our models are *under-specified* in that they have more than one “complete” refinement, models that satisfy $\mathcal{M}^a = \mathcal{M}^c$. Positive assertion checks state that the property in question holds for all (complete) refinements. Positive consistency checks state that there is a (complete) refinement with that property.

The possibilistic property semantics $\llbracket \cdot \rrbracket^m$ is defined in Figure 2, where $\neg a \stackrel{\text{def}}{=} c$, $\neg c \stackrel{\text{def}}{=} a$, and $\text{pre}_{\sqsupseteq r}^m(A) \stackrel{\text{def}}{=} \{s \in \Sigma \mid \exists(s, \eta) \in R^m : \eta(A) \sqsupseteq r\}$ for $A \in \mathcal{F}$, is the modal quantitative version of the usual pre-image operator. This operator computes the set of states s from which there is a quantitative R^m -transition (s, η) that reaches set A with a quantity $\sqsupseteq r$. Although least fixed points are computed in $(\mathcal{P}(\Sigma), \sqsubseteq)$, condition (1) maintains that all denotations are elements of the underlying σ -algebra — as shown below. Note the special treatment of negation: to evaluate $\neg\phi$ in mode m , first evaluate ϕ in mode $\neg m$ and then negate that result [31]. Since models are finitely branching, we have $s \models^m \mu Z.\phi$ iff for

$$\begin{array}{ll} \llbracket \mathbf{tt} \rrbracket_\rho^m \stackrel{\text{def}}{=} \Sigma & \llbracket \neg\phi \rrbracket_\rho^m \stackrel{\text{def}}{=} \Sigma \setminus \llbracket \phi \rrbracket_{\rho^{\neg m}} \\ \llbracket p \rrbracket_\rho^m \stackrel{\text{def}}{=} \{s \in \Sigma \mid p \in L^m(s)\} & \llbracket \phi_1 \wedge \phi_2 \rrbracket_\rho^m \stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket_\rho^m \cap \llbracket \phi_2 \rrbracket_\rho^m \\ \llbracket Z \rrbracket_\rho^m \stackrel{\text{def}}{=} \rho^m(Z) & \llbracket \text{EX}_{\sqsupseteq r} \phi \rrbracket_\rho^m \stackrel{\text{def}}{=} \text{pre}_{\sqsupseteq r}^m(\llbracket \phi \rrbracket_\rho^m) \\ \llbracket \mu Z.\phi \rrbracket_\rho^m \stackrel{\text{def}}{=} \text{lfp } F^m; & \text{where } F^m(A) \stackrel{\text{def}}{=} \llbracket \phi \rrbracket_{\rho^m[Z \mapsto A]} \end{array}$$

Fig. 2. Semantics for modal quantitative Kripke structures in mode $m \in \{a, c\}$.

some $k \geq 0$, $s \models^m \mu_k Z.\phi$, where $\mu_k Z.\phi$ is the standard syntactic approximation of $\mu Z.\phi$ defined by $\mu_0 Z.\phi \stackrel{\text{def}}{=} \neg \mathbf{tt}$ and $\mu_{k+1} Z.\phi \stackrel{\text{def}}{=} \phi[Z \mapsto \mu_k Z.\phi]$ for all $k \geq 0$. (As customary, $\phi[Z \mapsto \mu_k Z.\phi]$ denotes the formula obtained by replacing in ϕ all free occurrences of Z with $\mu_k Z.\phi$.) Incidentally, our treatment of \mathbf{tt} , negation, conjunction, and fixed points in Figure 2 means that the set of denotations has to be a σ -algebra *even if the model is a quantitative, non-probabilistic one*.

Disjunction, implication, formulas $\text{AX}_{\sqsubseteq r} \phi$, and greatest fixed points are definable in this logic. However, this is not the case for checks of the form $s \models^m \text{AX}_{\sqsupseteq r} \phi$ which are positive if for all R^m -transitions (s, μ) , $\mu(\llbracket \phi \rrbracket^m) \sqsupseteq r$.

Our property semantics for modal quantitative Kripke structures is sound with respect to possibilistic refinement and abstraction for *all* closed formulas of \mathcal{L}_{pr} : positive assertion checks $t \models^a \phi$ remain valid for all possibilistic refinements of t ; dually, positive consistency checks $t \models^c \phi$ remain consistent for all possibilistic abstractions of t .

Theorem 1 (Soundness). *Let \mathcal{M} be a modal quantitative Kripke structure, ρ an environment, $\phi \in \mathcal{L}_{\text{pr}}$ a closed formula, and $m \in \{a, c\}$. Then $\llbracket \phi \rrbracket_\rho^m \in \mathcal{F}$.*

Moreover for any possibilistic refinement Q , $(s, t) \in Q$ entails that (1) $t \models_{\rho}^a \phi$ implies $s \models_{\rho}^a \phi$; and (2) $s \models_{\rho}^c \phi$ implies $t \models_{\rho}^c \phi$.

Proof. For measurability, the closure properties of σ -algebras take care of the clauses \mathbf{tt} , negation, conjunction, and fixed points (since models are finitely branching such fixed points are the countable union of their unfoldings). Condition (1) takes care of the clauses p and $\mathbf{EX}_{\supseteq r}$.

We show items 1 and 2 for the key clauses of $\mathbf{EX}_{\supseteq r}$ and fixed points. Let $t \models_{\rho}^a \mathbf{EX}_{\supseteq r} \phi$. Then there exists some $(t, \eta) \in R^a$ such that $\eta(\llbracket \phi \rrbracket_{\rho}^a) \supseteq r$, where $\llbracket \phi \rrbracket_{\rho}^a \in \mathcal{F}$ and item 1 holds for ϕ by induction. Since Q is a possibilistic refinement, $(s, t) \in Q$ implies that there exists some $(s, \mu) \in R^a$ such that $(\mu, \eta) \in Q^{\text{ps}}$. In particular, $Q.\llbracket \phi \rrbracket_{\rho}^a \in \mathcal{F}$. By induction, $Q.\llbracket \phi \rrbracket_{\rho}^a \subseteq \llbracket \phi \rrbracket_{\rho}^a$, so $\mu(\llbracket \phi \rrbracket_{\rho}^a) \geq \mu(Q.\llbracket \phi \rrbracket_{\rho}^a) \geq \eta(\llbracket \phi \rrbracket_{\rho}^a)$ — the first inequality follows from the monotonicity of μ , the second one follows from $(\mu, \eta) \in Q^{\text{ps}}$. But $\eta(\llbracket \phi \rrbracket_{\rho}^a) \supseteq r$ then implies $\mu(\llbracket \phi \rrbracket_{\rho}^a) \supseteq r$, since \geq is transitive and since $\geq \circ >$ and $> \circ \geq$ are contained in $>$. Thus, $(s, \mu) \in R^a$ implies $s \models_{\rho}^a \mathbf{EX}_{\supseteq r} \phi$.

Let $s \models_{\rho}^c \mathbf{EX}_{\supseteq r} \phi$. Then there exists some $(s, \mu) \in R^c$ such that $\mu(\llbracket \phi \rrbracket_{\rho}^c) \supseteq r$, where $\llbracket \phi \rrbracket_{\rho}^c \in \mathcal{F}$ and item 2 holds for ϕ by induction. Since Q is a possibilistic refinement and $(s, t) \in Q$, there exists some $(t, \eta) \in R^c$ such that $(\mu, \eta) \in Q^{\text{ps}}$. In particular, $\llbracket \phi \rrbracket_{\rho}^c.Q \in \mathcal{F}$. By induction, $\llbracket \phi \rrbracket_{\rho}^c.Q \subseteq \llbracket \phi \rrbracket_{\rho}^c$, so $\eta(\llbracket \phi \rrbracket_{\rho}^c) \geq \eta(\llbracket \phi \rrbracket_{\rho}^c.Q) \geq \mu(\llbracket \phi \rrbracket_{\rho}^c)$ — the first inequality follows from the monotonicity of η , the second one follows from $(\mu, \eta) \in Q^{\text{ps}}$. But $\mu(\llbracket \phi \rrbracket_{\rho}^c) \supseteq r$ then implies $\eta(\llbracket \phi \rrbracket_{\rho}^c) \supseteq r$, rendering $t \models_{\rho}^c \mathbf{EX}_{\supseteq r} \phi$ since $(t, \eta) \in R^c$.

By induction and the previous item, function F^a restricts to type $\mathbb{L}[\prec_{\mathcal{M}}] \rightarrow \mathbb{L}[\prec_{\mathcal{M}}]$, where $\mathbb{L}[Q] \stackrel{\text{def}}{=} \{L \in \mathcal{F} \mid \text{for all } (s, l) \in Q : l \in L \Rightarrow s \in L\}$, and so its least fixed point is an element of $\mathbb{L}[\prec_{\mathcal{M}}]$; dually, by induction, function F^c restricts to type $\mathbb{U}[\prec_{\mathcal{M}}] \rightarrow \mathbb{U}[\prec_{\mathcal{M}}]$, where $\mathbb{U}[Q] \stackrel{\text{def}}{=} \{U \in \mathcal{F} \mid \text{for all } (u, t) \in Q : u \in U \Rightarrow t \in U\}$, and so its least fixed point is an element of $\mathbb{U}[\prec_{\mathcal{M}}]$. \blacksquare

We emphasize that these results are also valid when the model \mathcal{M} is a sum $\mathcal{M}_1 + \mathcal{M}_2$, where \mathcal{M}_1 is a (more) concrete model and \mathcal{M}_2 is its possibilistic abstraction. Also note that $\prec_{\mathcal{M}}$ exists and has measurable navigation in finite-state models.

Our property semantics loses precision in two places: the interpretation of disjunction in the assertion mode a , and the interpretation of conjunction in the consistency checking mode c . For example, for $p \in L^c(s) \setminus L^a(s)$ our semantics computes $s \models_{\rho}^c p \wedge \neg p$ and $s \not\models_{\rho}^a p \vee \neg p$. The meaning of these checks, as expressed in Remark 1, reveals that positive consistency checks are *over-approximations* (not all such checks are truthful) and positive assertion checks are *under-approximations* (not all such checks discover the truth). Fortunately, the subtle treatment of negation [31] guarantees that the interplay of these approximations is sound.

Theorem 2 (Consistency). *Let \mathcal{M} be a modal quantitative Kripke structure. For all closed $\phi \in \mathcal{L}_{\text{pr}}$ and environments ρ , we have (i) $\llbracket \phi \wedge \neg \phi \rrbracket_{\rho}^a = \{\}$ and, equivalently, (ii) $\llbracket \phi \rrbracket_{\rho}^a \subseteq \llbracket \phi \rrbracket_{\rho}^c$.*

Proof. Items (i) and (ii) are equivalent. We show item 2 for the clause $\text{EX}_{\sqsupseteq r}\phi$. Let $s \in \llbracket \text{EX}_{\sqsupseteq r}\phi \rrbracket_{\rho}^a$. Then there exists some $(s, \mu) \in R^a$ such that $\mu(\llbracket \phi \rrbracket_{\rho}^a) \sqsupseteq r$. By induction, $\llbracket \phi \rrbracket_{\rho}^a \subseteq \llbracket \phi \rrbracket_{\rho}^c \in \mathcal{F}$ and so — using the monotonicity of μ — $\mu(\llbracket \phi \rrbracket_{\rho}^c) \geq \mu(\llbracket \phi \rrbracket_{\rho}^a) \sqsupseteq r$ which implies $\mu(\llbracket \phi \rrbracket_{\rho}^c) \sqsupseteq r$. But $(s, \mu) \in R^a \subseteq R^c$ renders $s \in \llbracket \text{EX}_{\sqsupseteq r}\phi \rrbracket_{\rho}^c$. ■

The loss of precision in \models^m may severely impact the quality of an analysis. Various techniques exist for obtaining more precise interpretations in *qualitative* models, although at a significant increase in complexity. We mention the focus operation of Ball et al. [4] and Bruns and Godefroid’s generalized model checking [6]; it would be of interest to investigate their quantitative analogues. As we saw above, the loss of precision in our property semantics does not compromise the validity of positive assertion checks.

For a class of quantitative measures that subsumes probability measures, one can show that possibilistic refinements lift to computation paths.

Proposition 2 (Matching computation paths). *Let \mathcal{M} be a finite-state modal quantitative Kripke structure with state set Σ and $\mathcal{F} = \mathcal{P}(\Sigma)$ such that its partial order P has a least element 0, and all its quantitative measures μ satisfy that $\mu(X) > 0$ implies $\mu(\{x\}) > 0$ for some $x \in X$. Let Q be a possibilistic refinement in \mathcal{M} with $(s_0, t_0) \in Q$. If the path $\pi = (t_0, \eta_0)(t_1, \eta_1) \dots$ is such that $(t_i, \eta_i) \in R^a$ and $\eta_i(\{t_{i+1}\}) > 0$ for all $i \geq 0$, then there exists a matching path $\kappa = (s_0, \mu_0)(s_1, \mu_1) \dots$ such that $(s_i, \mu_i) \in R^a$, $\mu_i(\{s_{i+1}\}) > 0$, $(\mu_i, \eta_i) \in Q^{\text{ps}}$, and $(s_i, t_i) \in Q$ for all $i \geq 0$. A dual property holds for R^c -paths beginning in s_0 .*

Proof. Since $(t_0, \eta_0) \in R^a$ and $(s_0, t_0) \in Q$, there is some $(s_0, \mu_0) \in R^a$ such that $(\mu_0, \eta_0) \in Q^{\text{ps}}$. The set $\{t_1\}$ is in \mathcal{F} by assumption. Therefore, $\mu_0(Q.\{t_1\}) \geq \eta_0(\{t_1\})$. But $\eta_0(\{t_1\}) > 0$ by assumption and so $\mu_0(Q.\{t_1\}) > 0$ implies that $\mu_0(\{s_1\}) > 0$ for some $s_1 \in Q.\{t_1\}$, i.e. $(s_1, t_1) \in Q$. Proceeding by induction, we construct a path κ with the desired properties. The proof for the second statement is dual. ■

Our possibilistic property semantics can be implemented with a conventional labeling algorithm such that the only changes are in the treatment of negation — leading to a-labels and c-labels on states that may be represented with two BDDs [7] — and in the computation of successor sets, based on $\text{pre}_{\sqsupseteq r}^m(A)$. In particular, in finite-state systems fixed points always converge with the size of the state space as upper bound on the number of necessary unfoldings. It would be of interest to represent this labeling algorithm symbolically, as done for the standard semantics with MTBDDs in Baier et al. [2].

We conclude this section with a discussion of how our possibilistic refinement relates to the established notion of probabilistic bisimulation [32].

Theorem 3 (Probabilistic bisimulation). *Let \mathcal{M} be a finite modal quantitative Kripke structure $((\Sigma, R^a, L^a), (\Sigma, R^c, L^c))$ with signature $(\text{AP}, \mathcal{P}(\Sigma), P)$ such that \mathcal{M}^a equals \mathcal{M}^c .*

1. For all closed $\phi \in \mathcal{L}_{\text{pr}}$ and all environments ρ : $\|\phi\|_{\rho}^{\text{a}}$ equals $\|\phi\|_{\rho}^{\text{c}}$.
2. If P equals $[0, 1]$ and every quantitative measure is probabilistic, then the probabilistic bisimulations in \mathcal{M}^{a} are exactly the possibilistic refinements in \mathcal{M} which are equivalence relations. In particular, the greatest probabilistic bisimulation of \mathcal{M}^{a} is contained in $\prec_{\mathcal{M}} \cap (\prec_{\mathcal{M}}^{-1})$.

Proof. Since $\mathcal{M}^{\text{a}} = \mathcal{M}^{\text{c}}$, $\|\cdot\|_{\rho}^{\text{a}}$ and $\|\cdot\|_{\rho}^{\text{c}}$ are identical for closed formulas.

Let Q be an equivalence relation and a possibilistic refinement with $(s, t) \in Q$. (i) Definition 4 implies $L^{\text{a}}(s) = L^{\text{a}}(t)$ (since $L^{\text{a}} = L^{\text{c}}$). (ii) Let $(t, \eta) \in R^{\text{a}}$. Then there is some $(s, \mu) \in R^{\text{a}}$ such that $(\mu, \eta) \in Q^{\text{ps}}$. But for every union of a collection of equivalence classes X of Q we have $X.Q = Q.X = X$, so $\eta(X) = \eta(X.Q) \geq \mu(X)$ and $\mu(X) = \mu(Q.X) \geq \eta(X)$. Thus, $\mu(X) = \eta(X)$ for all such X , since the order on P is anti-symmetric. (ii) Let $(s, \mu) \in R^{\text{a}} (= R^{\text{c}})$. Then we reason dually. Thus, Q is a probabilistic bisimulation in \mathcal{M}^{a} .

Conversely, let \mathcal{R} be a probabilistic bisimulation in \mathcal{M}^{a} . Given $A, B \in \mathcal{F}$, the sets $A.\mathcal{R}$ and $\mathcal{R}.B$ are in $\mathcal{F} = \mathcal{P}(\Sigma)$, are unions of a collection of equivalence classes of \mathcal{R} , and contain A and B (respectively). Let $(s, t) \in \mathcal{R}$. Then $L^{\text{m}}(s) = L^{\text{m}}(t)$ (i.e. $L^{\text{a}}(t) \subseteq L^{\text{a}}(s)$ and $L^{\text{c}}(s) \subseteq L^{\text{c}}(t)$) since \mathcal{R} is a probabilistic bisimulation. (i) If $(t, \eta) \in R^{\text{a}}$, then there is some $(s, \mu) \in R^{\text{a}}$ such that $\mu(X) = \eta(X)$ for all unions of equivalence classes X of \mathcal{R} . But then the reflexivity of \mathcal{R} renders $\eta(A.\mathcal{R}) = \mu(A.\mathcal{R}) \geq \mu(A)$ and $\mu(\mathcal{R}.B) = \eta(\mathcal{R}.B) \geq \eta(B)$, establishing $(\mu, \eta) \in \mathcal{R}^{\text{ps}}$. (ii) If $(s, \mu) \in R^{\text{c}} (= R^{\text{a}})$, we reason dually. Thus, \mathcal{R} is a possibilistic refinement and therefore contained in $\prec_{\mathcal{M}}$. Since \mathcal{R} is symmetric, it is contained in $\prec_{\mathcal{M}} \cap (\prec_{\mathcal{M}})^{-1}$. \blacksquare

5 Approximating probabilistic logics

In this section we assume that quantitative models are probabilistic: the partial order P equals $[0, 1]$ and all quantitative measures are probabilistic. This assumption enables a direct comparison of possibilistic refinement and property semantics to their probabilistic versions.

For probabilistic models, the possibilistic refinement notion seems suitable since probabilistic bisimulations are then possibilistic refinements that are equivalence classes (Theorem 3). Our possibilistic property semantics, however, is quite different in spirit from established probabilistic logics which are variants or fragments of Hansson’s logic PCTL [24]. The latter abstracts a linear semantics that assigns probabilities to sets of traces to a branching semantics through quantification over suitable adversaries. Our semantics is also branching as its models are (probabilistic) computation trees but it abstracts the adversary abstraction of the linear semantics in [24]. (For qualitative models, Cousot and Cousot [14] showed how one may systematically abstract a trace semantics into several branching-time semantics; see [44] for a corresponding abstraction of trace sets to modal transition systems.)

This abstraction is caused by a “memory-less” way of computing successor states for fixed points. Along computation paths, the threshold in $\text{EX}_{\sqsupseteq, r}$ is applied

to each state in isolation. This is akin to the use of possibility and necessity measures in artificial intelligence [20] — whence the name *possibilistic* refinement — especially if quantitative measures compute maxima: $\mu(A) = \max_{s \in A} \mu(\{a\})$. Given this memory-less treatment of probabilities, it is therefore intuitive that the thresholds for our fixed-point semantics turn into exponential thresholds for the standard probabilistic semantics (see Proposition 3).

To enable a comparison to PCTL, we restrict fixed points to those of the form $\mu Z.\psi \stackrel{\text{def}}{=} \mu Z.q \vee (p \wedge \text{EX}_{\sqsupseteq r}(Z))$. (We assume $p, q \in \text{AP}$ to simplify this discussion.) Since the underlying modal probabilistic Kripke structure \mathcal{M} is finitely-branching, we have $s \models^m \mu Z.\psi$ iff $s \models^m \mu_k Z.\psi$ for some $k > 0$. For each $m \in \{a, c\}$, we define $f^m: \Sigma \times \mathbb{N} \rightarrow \{0, 1\}$, parametric in r , through

$$\begin{aligned} f^m(s, k) &\stackrel{\text{def}}{=} 1; && \text{if } s \models^m q \\ f^m(s, k+1) &\stackrel{\text{def}}{=} 1; && \text{if } s \models^m p, s \not\models^m q \\ &&& \text{and } \exists (s, \mu) \in R^m: \mu(\{t \mid f^m(t, k) = 1\}) \sqsupseteq r \\ f^m(s, k) &\stackrel{\text{def}}{=} 0; && \text{otherwise.} \end{aligned} \tag{3}$$

Lemma 1 (Computing a possibilistic EU). *For all $0 < r \leq 1$, $m \in \{a, c\}$, and all $k \geq 0$, the function f^m is well defined and $s \models^m \mu_{k+1} Z.\psi$ iff $f^m(s, k) = 1$.*

Proof. By Theorem 1, induction on k ensures that $f^m(\cdot, \cdot)$ is well defined, since the argument of μ in the second clause of (3) is then in \mathcal{F} . For $k = 0$, we have $f^m(s, 0) = 1$ iff $s \models^m q$ iff — since $r > 0$ implies $s \not\models^m \text{EX}_{\sqsupseteq r} \neg \text{tt}$ — $s \models^m \mu_1 Z.\psi$. Assume that the statement holds for k . Then $s \models^m \mu_{k+2} Z.\psi$ iff $s \models^m q$ or $(s \models^m p$ and $s \models^m \text{EX}_{\sqsupseteq r} \mu_{k+1} Z.\psi)$ iff $s \models^m q$ or $(s \models^m p$ and — by induction — there is some $(s, \mu) \in R^m$ such that $\mu(\{t \mid f^m(t, k) = 1\}) \sqsupseteq r$) iff $s \models^m q$ or $(s \models^m p$ and $s \not\models^m q$ and $f^m(s, k+1) = 1)$ iff $f^m(s, k+1) = 1$. ■

A similar specification may be given for an AF connective, rendering a labeling algorithm for our semantics which covers full PCTL. We now compare our semantics to that of a probabilistic Until $[p \text{ EU } q]_{\sqsupseteq r}$ whose meaning may be computed via a function $g^m: \Sigma \times \mathbb{N} \rightarrow \{0, 1\}$:

$$\begin{aligned} g^m(s, k) &\stackrel{\text{def}}{=} 1; && \text{if } s \models^m q \\ g^m(s, k+1) &\stackrel{\text{def}}{=} \max_{(s, \mu) \in R^m} \left\{ \sum_{t \in \Sigma} \mu(\{t\}) \cdot g^m(t, k) \right\}; && \text{if } s \models^m p, s \not\models^m q; \\ g^m(s, k) &\stackrel{\text{def}}{=} 0; && \text{otherwise.} \end{aligned} \tag{4}$$

Note that this function is well defined only if all singletons are measurable. One may then specify that $s \models^m [p \text{ EU } q]_{\sqsupseteq r}$ holds iff $g(s, k) \sqsupseteq r$ for some $k \geq 0$. In general, our possibilistic property semantics is an abstraction of the probabilistic one in that possibilistic *positive* EU checks imply positive checks in the probabilistic interpretation, alas with an exponential penalty in the threshold.

Proposition 3 (Sound approximation). *Let all singletons in Σ be measurable. For all $m \in \{a, c\}$, $s \in \Sigma$, and $k \geq 0$, $f^m(s, k) = 1$ implies $g^m(s, k) \sqsupseteq r^{k+1}$.*

Proof. For $k = 0$, $f^m(s, 0) = 1$ iff $s \models^m q$ iff $g^m(s, 0) = 1$, which implies $g^m(s, 0) \sqsupseteq r^{0+1}$.

For $k + 1$, let $f^m(s, k + 1) = 1$. If $s \models^m q$, then $g^m(s, k + 1) = 1$ and we are done. Otherwise, $f^m(s, k + 1) = 1$ implies $s \models^m p$, $s \not\models^m q$, and the existence of some $(s, \eta) \in R^m$ such that $\sum_{f^m(t, k)=1} \eta(\{t\}) \sqsupseteq r$ since η is a probability measure. For each instance of $f^m(t, k) = 1$ we have $g^m(t, k) \sqsupseteq r^{k+1}$ by induction. Since $s \models^m p$ and $s \not\models^m q$, we therefore obtain $g^m(s, k + 1) = \max_{(s, \mu) \in R^m} \{\sum_t \mu(\{t\}) \cdot g^m(t, k)\} \geq \sum_t \eta(\{t\}) \cdot g^m(t, k) \geq \sum_{f^m(t, k)=1} \eta(\{t\}) \cdot g^m(t, k) \sqsupseteq \sum_{f^m(t, k)=1} \eta(\{t\}) \cdot r^{k+1} = r^{k+1} \cdot \sum_{f^m(t, k)=1} \eta(\{t\}) \sqsupseteq r^{k+1} \cdot r = r^{k+2}$. ■

To decide whether $s \models^m [p \text{ EU } q]_{\sqsupseteq r}$, one may therefore choose some $k \geq 0$, compute τ_k as the $k + 1$ th square root of r , and then determine $f^m(s, k)$ for parameter value τ_k ; if $f^m(s, k)$ equals 1, we know for certain that $s \models^m [p \text{ EU } q]_{\sqsupseteq r}$ holds. Thus, for each $l \geq 2$ the formula $\bigvee_{k=2}^l \mu_{k+1} Z. \psi_k$ provides a sound approximation of the probabilistic Until if interpreted in the possibilistic semantics, where all thresholds in ψ_k are τ_k . Unfortunately, the loss of precision in $r \mapsto r^k$ means that possibilistic checks may rarely give insight into true probabilistic behavior.

How does our possibilistic refinement notion fare with the preservation of properties if the Untils are interpreted via g^m ? Possibilistic refinements clearly takes care of the clause $\text{EX}_{\sqsupseteq r}$, but fails to secure the fixed-point clause for EU in general, since relational navigation is too coarse grained to reason about the sum expression in (4). Of course, this is where probabilistic simulations [30] do their work to complete satisfaction.

To define *probabilistic* refinements, we keep Definition 4 as is, except for replacing all occurrences of Q^{ps} with Q^{pr} ; the latter is the relation \sqsubseteq_R of [15] where Q plays the role of the discriminating criterion C : $(\mu, \eta) \in Q^{\text{pr}}$ iff there is some probability measure δ on $\mathcal{F} \times \mathcal{F}$ such that for all $s, t \in \Sigma$,

$$\mu(\{s\}) = \delta(\{s\} \times \Sigma), \eta(\{t\}) = \delta(\Sigma \times \{t\}), \delta(\{s\} \times \{t\}) > 0 \Rightarrow (s, t) \in Q. \quad (5)$$

Note that this definition applies to finite models with $\mathcal{F} = \mathcal{P}(\Sigma)$. We can extend the results of [15] to a full logic in re-proving Theorem 1 for the *probabilistic* semantics — which changes the possibilistic semantics of Figure 2 for the computation of Untils by using g^m instead of f^m — and *probabilistic* refinement. However, this inductive proof works only if denotations of subformulas are measurable. Thus, we encounter potential problems in properties that nest Untils. Specifically, we then owe a proof that $\{s \in \Sigma \mid \exists (s, \mu) \in R^m: \sum \mu(\{t\}) \cdot g^m(t, k) \sqsupseteq r\} \in \mathcal{F}$ for all $k \geq 0$ and $r \in [0, 1]$. With the help of condition (1), it may be possible to show the inductive step for such a claim, but we did not yet investigate that in sufficient detail.

Theorem 4 (Soundness of probabilistic abstraction). *Theorem 1 applies to finite modal probabilistic models with measurable singletons, provided that least*

fixed points are restricted to Untils whose probabilistic semantics is based on (4) and the refinement is the probabilistic one.

Proof. Let $(s, t) \in Q$. The proof only changes for the clauses $\text{EX}_{\sqsupset r}$ and Until.

Given $t \models^a \text{EX}_{\sqsupset r} \phi$, there exists some $(t, \eta) \in R^a$ such that $\eta(\|\phi\|^a) \sqsupseteq r$. Since Q is a probabilistic refinement, $(s, t) \in Q$ implies that there exists some $(s, \mu) \in R^a$ such that $(\mu, \eta) \in Q^{\text{pr}}$. Let δ be the corresponding witness. Then $\eta(\|\phi\|^a) = \sum_{t' \in \|\phi\|^a} \eta(\{t'\})$ which equals $\sum_{t' \in \|\phi\|^a} \delta(\Sigma \times \{t'\})$. Since $\delta(\{u\} \times \{v\}) > 0$ implies $(u, v) \in Q$, the latter equals $\sum_{t' \in \|\phi\|^a} \sum_{s' | (s', t') \in Q} \delta(\{s'\} \times \{t'\})$ which, by induction, is less than or equal to $\sum_{s' \in \|\phi\|^a} \sum_{t' \in \|\phi\|^a} \delta(\{s'\} \times \{t'\}) \leq \sum_{s' \in \|\phi\|^a} \delta(\{s'\} \times \Sigma)$ which equals $\sum_{s' \in \|\phi\|^a} \mu(\{s'\}) = \mu(\|\phi\|^a)$. But $\eta(\|\phi\|^a) \sqsupseteq r$ then implies $\mu(\|\phi\|^a) \sqsupseteq r$. Thus, $(s, \mu) \in R^a$ entails $s \models^a \text{EX}_{\sqsupset r} \phi$. The proof that $s \models^c \text{EX}_{\sqsupset r} \phi$ implies $t \models^c \text{EX}_{\sqsupset r} \phi$ is dual and omitted.

Given $t \models^a [\phi_1 \text{EU} \phi_2]_{\sqsupset r}$, there is some $k \geq 0$ such that $g^a(t, k) \sqsupseteq r$. Thus, it suffices to show that $g^a(s, k) \geq g^a(t, k)$ for all $(s, t) \in Q$ and $k \geq 0$. For $k = 0$, this follows by induction on ϕ_2 . For the inductive step $k + 1$, only the second clause of (4) contains a non-trivial proof obligation. Let $(t, \eta) \in R^a$ be the witness for the computation of the maximum value in that clause. Since $(s, t) \in Q$, there is some $(s, \mu) \in R^a$ such that $(\mu, \eta) \in Q^{\text{pr}}$. Let δ be the corresponding witness. We claim that the second clause of (4) applies to $g^a(s, k + 1)$ as well: by induction on ϕ_1 , we obtain $s \models^a \phi_1$ and if $s \models^a \phi_2$ is the case there is nothing to show as then $g^a(s, k + 1) = 1$. Therefore, $g^a(s, k + 1) \geq \sum_{s' \in \Sigma} \mu(\{s'\}) \cdot g^a(s', k)$ which equals $\sum_{s' \in \Sigma} \delta(\{s'\} \times \Sigma) \cdot g^a(s', k)$. The latter equals $\sum_{s' \in \Sigma} \sum_{t' | (s', t') \in Q} \delta(\{s'\} \times \{t'\}) \cdot g^a(s', k)$ which is greater or equal to $\sum_{s' \in \Sigma} \sum_{t' | (s', t') \in Q} \delta(\{s'\} \times \{t'\}) \cdot g^a(t', k) = \sum_{s' \in \Sigma} \sum_{t' \in \Sigma} \delta(\{s'\} \times \{t'\}) \cdot g^a(t', k)$ by induction on k . But the latter equals $\sum_{t' \in \Sigma} \delta(\Sigma \times \{t'\}) \cdot g^a(t', k) = g^a(t, k + 1)$. To show that $s \models^c [\phi_1 \text{EU} \phi_2]_{\sqsupset r}$ implies $t \models^c [\phi_1 \text{EU} \phi_2]_{\sqsupset r}$ it suffices to prove that $g^c(t, k) \geq g^a(s, k)$ for all $(s, t) \in Q$ and $k \geq 0$; this proof is dual to the one of the previous item. \blacksquare

Although the scope of Theorem 4 is sufficiently wide for practical abstraction-based model checking, a proper extension of this result to the full scope of models and the logic is desirable.

6 Specifying abstractions

We defined refinement and abstraction as notions *within* quantitative models. Since these models have sums (which restrict to probabilistic systems as well), such an approach did not compromise any generality. In this section, we avoid the notational overhead of castings into sum types and express abstractions between models directly. We transfer the results of Godefroid et al. [22], where a compositional calculus for specifying and computing relational abstractions of modal transition systems is developed, to modal quantitative structures.

Definition 5 (Specifying abstractions). *Let $\mathcal{M} = (\Sigma, R^a, L^a), (\Sigma, R^c, L^c)$ be a modal quantitative Kripke structure with signature $(\text{AP}, \mathcal{F}, P)$ and $Q \subseteq$*

$(\Sigma, \mathcal{F}) \times (\Sigma_Q, \mathcal{F}_Q)$ a left-total and right-total relation with measurable navigation. We define a possibilistic relational abstraction $\mathcal{M}_{Q^{\text{ps}}}$ (and a probabilistic relational abstraction $\mathcal{M}_{Q^{\text{pr}}}$ if \mathcal{M} happens to be probabilistic) of \mathcal{M} via Q . Let $\star \in \{\text{ps}, \text{pr}\}$:

- both state sets equal Σ_Q and their σ -algebra is \mathcal{F}_Q ;
- for each $t \in \Sigma_Q$, their labeling functions are given by $p \in L_{Q^\star}^a(t)$ iff for all $(s', t) \in Q$, $p \in L^a(s')$; and $p \in L_{Q^\star}^c(t)$ iff there exists some $(s', t) \in Q$ such that $p \in L^c(s')$;
- as for their transition relations, we have $(t, \eta) \in R_{Q^\star}^a$ iff for all $s \in Q.\{t\}$ there is some $(s, \mu) \in R^a$ such that $(\mu, \eta) \in Q^\star$; dually, $(t, \eta) \in R_{Q^\star}^c$ iff there is some $s \in Q.\{t\}$ and some $(s, \mu) \in R^c$ such that $(\mu, \eta) \in Q^\star$.

Since $B \mapsto Q.B$ is monotone, every $\mu \in [\mathcal{F} \rightarrow P]$ determines a $\mu_Q \in [\mathcal{F}_Q \rightarrow P]$ such that $\mu_Q(B) \stackrel{\text{def}}{=} \mu(Q.B)$ for all $B \in \mathcal{F}_Q$. We note that $\mu \mapsto \mu_Q$ does not preserve the property of being a probability measure in general, although we show below that this is the case for predicate-based abstractions. To show that the specification above renders relational abstractions, we need to gain a better understanding of the relations Q^{ps} and Q^{pr} .

Theorem 5. *Let $Q \subseteq (\Sigma, \mathcal{F}) \times (\Sigma_Q, \mathcal{F}_Q)$ be a right-total relation with measurable navigation.*

1. Q is the graph of a function $f: \Sigma \rightarrow \Sigma_Q$ iff $B = (Q.B).Q$ for all $B \subseteq \Sigma_Q$.
2. For every $\mu \in [\mathcal{F} \rightarrow P]$, $(\mu, \mu_Q) \in Q^{\text{ps}}$.
3. The relation $(\mu, \eta) \in Q^{\text{ps}}$ implies $\eta(B) \leq \mu_Q(B)$ for all $B \in \mathcal{F}_Q$.
4. Let Q be the graph of a function. Then
 - (a) $(\mu, \eta) \in Q^{\text{ps}}$ iff $\eta = \mu_Q$; and
 - (b) if μ and η are probabilistic, $\mathcal{F} = \mathcal{P}(\Sigma)$, and $\mathcal{F}_Q = \mathcal{P}(\Sigma_Q)$, then $(\mu, \eta) \in Q^{\text{pr}}$ iff $(\mu, \eta) \in Q^{\text{ps}}$.

Proof. 1. This is straightforward, noting that Q is right-total.

2. Let $A \in \mathcal{F}$. Then $\mu_Q(A.Q) = \mu(Q.(A.Q))$ by definition. Since Q is right-total, we have $A \subseteq Q.(A.Q)$ and so — using the monotonicity of μ — $\mu(Q.(A.Q)) \geq \mu(A)$. Let $B \in \mathcal{F}_Q$. Then $\mu(Q.B) = \mu_Q(B)$. Thus, $(\mu, \mu_Q) \in Q^{\text{ps}}$.

3. Let $B \in \mathcal{F}_Q$. Then $\mu_Q(B) = \mu(Q.B) \geq \eta(B)$.

4a. $B = (Q.B).Q$ implies $\eta(B) = \eta((Q.B).Q) \geq \mu(Q.B) = \mu_Q(B)$.

4b. Let $(\mu, \eta) \in Q^{\text{ps}}$, i.e. $\eta = \mu_Q$. We show that (5) is met for $\delta(\{s\} \times \{t\}) = \mu(\{s\} \cap Q.\{t\})$. Since Q is the graph of a function, $\sum_t \delta(\{s\} \times \{t\}) = \sum_t \mu(\{s\} \cap Q.\{t\}) = \mu(\{s\})$. But $\sum_s \delta(\{s\} \times \{t\}) = \sum_s \mu(\{s\} \cap Q.\{t\}) = \sum_s \{\mu(\{s\}) \mid (s, t) \in Q\} = \mu(Q.\{t\}) = \mu_Q(\{t\})$. If $\delta(\{s\} \times \{t\}) > 0$, then $\{s\} \cap Q.\{t\}$ is non-empty (as $\mu(\{s\}) = 0$), so $(s, t) \in Q$. Finally, $\Sigma \times \Sigma_Q$ has measure 1, for $\sum_s \sum_t \delta(\{s\} \times \{t\}) = \sum_s \mu(\{s\}) = 1$. Thus, $(\mu, \eta) \in Q^{\text{pr}}$.

Conversely, let $(\mu, \eta) \in Q^{\text{pr}}$. It suffices to show that $\eta = \mu_Q$. Let κ be the witness to $(\mu, \eta) \in Q^{\text{pr}}$. By assumption, for every $s \in Q$ there is a unique $t_s \in \Sigma_Q$ with $(s, t_s) \in Q$. But then $\kappa(\{s\} \times \{t\}) = 0 = \delta(\{s\} \times \{t\})$ for all $t \neq t_s$. Thus, $\delta(\{s\} \times \{t_s\}) = \sum_t \delta(\{s\} \times \{t\}) = \mu(\{s\}) = \sum_t \kappa(\{s\} \times \{t\}) = \kappa(\{s\} \times \{t_s\})$ shows $\delta = \kappa$ which implies $\eta = \mu_Q$. \blacksquare

Corollary 1 (Abstractions of finite-state probabilistic models). *Possibilistic and probabilistic abstractions coincide if the underlying relation is left-total and right-total, models are finite-state, and all measures are probabilistic.*

Left-total and right-total relations with measurable navigation specify abstractions.

Theorem 6 (Soundness of specifications). *Let $Q \subseteq (\Sigma, \mathcal{F}) \times (\Sigma_Q, \mathcal{F}_Q)$ be a left-total and right-total relation with measurable navigation.*

1. *The transformations $\mathcal{M} \mapsto \mathcal{M}_{Q^{\text{ps}}}$ and $\mathcal{M} \mapsto \mathcal{M}_{Q^{\text{pr}}}$ preserve the property of being a modal quantitative and probabilistic Kripke structure (respectively). These transformations are equal for functional abstractions of finite-state systems.*
2. *The model \mathcal{M} is a possibilistic refinement of $\mathcal{M}_{Q^{\text{ps}}}$; under the assumptions of Theorem 5.4(b), \mathcal{M} is a probabilistic refinement of $\mathcal{M}_{Q^{\text{pr}}}$.*

Proof. Let $\star \in \{\text{ps}, \text{pr}\}$. 1. For $t \in \Sigma_Q$, $L_{Q^\star}^{\text{a}}(t) \stackrel{\text{def}}{=} \bigcap_{(s',t) \in Q} L^{\text{a}}(s')$ is contained in $\bigcup_{(s',t) \in Q} L^{\text{a}}(s')$. Since $L^{\text{c}}(s') \subseteq L^{\text{a}}(s')$ for all $s' \in \Sigma$, $\bigcup_{(s',t) \in Q} L^{\text{a}}(s')$ is contained in $\bigcup_{(s',t) \in Q} L^{\text{c}}(s')$ which equals $L_{Q^\star}^{\text{c}}(t)$. Similarly, we show $R_{Q^\star}^{\text{a}} \subseteq R_{Q^\star}^{\text{c}}$ using $R^{\text{c}} \subseteq R^{\text{a}}$ and the fact that Q is left-total.

2. For $(s, t) \in Q$, let $(t, \eta) \in R_{Q^\star}^{\text{a}}$. By definition of $R_{Q^\star}^{\text{a}}$, $(s, t) \in Q$ implies the existence of some $(s, \mu) \in R^{\text{a}}$ such that $(\mu, \eta) \in Q^\star$. Let $(s, \mu) \in R^{\text{c}}$. By Theorem 5.(2 or 4(b)), $(\mu, \mu_Q) \in Q^\star$ and so $(t, \mu_Q) \in R_Q^{\text{c}}$. Since $(s, t) \in Q$, we get $L_{Q^\star}^{\text{a}}(t) = \bigcap_{(s',t) \in Q} L^{\text{a}}(s') \subseteq L^{\text{a}}(s)$ and $L^{\text{c}}(s) \subseteq \bigcup_{(s',t) \in Q} L^{\text{c}}(s')$ which equals $L_{Q^\star}^{\text{c}}(t)$. \blacksquare

If our abstractions compute only the component $\mathcal{M}_{Q^{\text{ps}}}^{\text{c}}$, then such abstractions are fully compositional in that we may first specify an abstraction via Q_1 and then specify further abstractions on the first abstraction (via some Q_2). However, the computation of $\mathcal{M}_{Q^{\text{ps}}}^{\text{a}}$ requires that we specify an abstract model through the composite $Q_1; Q_2$ — as is the case for qualitative systems [22]. Thus, we owe a proof that abstraction relations are compositional.

Proposition 4 (Compositionality of possibilistic abstractions). *The composition of left-total, right-total relations with measurable navigation is left-total, right-total, and has measurable navigation.*

6.1 Predicate abstraction

Given a finite set $\{\psi_1, \psi_2, \dots, \psi_n\}$ of closed formulas in \mathcal{L}_{pr} and a concurrent labeled Markov chain \mathcal{M} — a modal probabilistic Kripke structure \mathcal{M} with $\mathcal{M}^{\text{a}} = \mathcal{M}^{\text{c}}$ — an equivalence relation \equiv may be defined on its set of states Σ by

$$s \equiv s' \quad \text{iff} \quad \{i \mid s \models \psi_i\} = \{i \mid s' \models \psi_i\}, \quad (6)$$

where Theorem 3.1 justifies the use of the notation \models . On Σ_Q , the finite set of bit vectors of length n , we define $(s, t) \in Q$ iff for all i , $t_i = 1$ iff $s \models \psi_i$. The functional relation Q is left-total and right-total.

The relation Q is also measurable where $\mathcal{F}_Q = \mathcal{P}(\Sigma_Q)$, *regardless of the nature of the underlying σ -algebra \mathcal{F} of the model \mathcal{M}* . Given $B \subseteq \Sigma_Q$ and $t \in B$, let ϕ_t be the conjunction of all ψ_i such that $t_i = 1$ and all $\neg\psi_i$ such that $t_i = 0$; define ϕ_B as the disjunction of all such ϕ_t with $t \in B$. Then $Q.B = \|\phi_B\|_\rho \in \mathcal{F}$ by Theorem 1 and 3. Although this works for every \mathcal{F} , any choice of \mathcal{F} severely restricts the class of legitimate models \mathcal{M} through condition (1). By Theorem 5, Q^{ps} relates μ to μ_Q only.

Example 2 (Predicate abstraction). If we abstract the model in Figure 1(left) with one predicate only, $\psi_1 = p \vee q$, we obtain the model of Figure 1(right). We verify $t_0 \models^a \neg\text{EX}_{>\frac{3}{4}} \neg\text{EX}_{>\frac{3}{10}} \neg p$, i.e. $t_0 \not\models^c \text{EX}_{>\frac{3}{4}} \neg\text{EX}_{>\frac{3}{10}} \neg p$. The latter is equivalent to “for all $(t_0, \kappa) \in R_{Q^{\text{pr}}}^c$, $\kappa(\|\neg\text{EX}_{>\frac{3}{10}} \neg p\|^c) \leq \frac{3}{4}$ ”, where $\kappa \in \{\alpha_Q, \mu_Q, \eta_Q\}$. But $\|\neg\text{EX}_{>\frac{3}{10}} \neg p\|^c = \Sigma_Q \setminus \|\text{EX}_{>\frac{3}{10}} \neg p\|^a$. Now $\|\text{EX}_{>\frac{3}{10}} \neg p\|^a = \{t \mid \exists(t, \kappa) \in R_{Q^{\text{pr}}}^a : \kappa(\|\neg p\|^a) > \frac{3}{10}\}$ equals $\{t_1\}$, since (t_1, γ_Q) is the only $R_{Q^{\text{pr}}}^a$ -transition and $\gamma_Q(\{t_1\}) = \frac{1}{3} > \frac{3}{10}$. Thus, $\|\neg\text{EX}_{>\frac{3}{10}} \neg p\|^c = \{t_0\}$ from which we infer $\alpha_Q(\{t_0\}) = \frac{2}{3} \leq \frac{3}{4}$, $\mu_Q(\{t_0\}) = \frac{3}{4} \leq \frac{3}{4}$, and $\eta_Q(\{t_0\}) = \frac{1}{2} \leq \frac{3}{4}$. By Theorem 1, we now know that s_0 , s_1 , and s_3 satisfy $\neg\text{EX}_{>\frac{3}{4}} \neg\text{EX}_{>\frac{3}{10}} \neg p$. (Note that $\neg\text{EX}_{>\frac{3}{4}} \neg$ may be abbreviated as $\text{AX}_{\leq\frac{3}{4}}$.)

In the paragraph above, we proved that predicate abstraction always gives rise to an abstraction relation that has measurable navigation.

Theorem 7 (Predicate abstraction has measurable navigation). *Let \mathcal{M} be a concurrent labeled Markov chain whose σ -algebra (Σ, \mathcal{F}) satisfies condition (1). For \equiv defined as in (6), assume that its set of equivalence classes, Σ_Q , is finite and contained in \mathcal{F} . Then $Q = \{(s, t) \in \Sigma \times \Sigma_Q \mid s \in t\}$ has measurable navigation, where the σ -algebra on Σ_Q is discrete.*

The proof of this fact works as specified above, except that the disjunctive normalform has elements of \mathcal{F} as literals.

Although we presented a compositional sound formalism for the specification of relational abstractions, the computation of such abstractions may prove to be expensive. This is indeed the case for qualitative systems, where the tradeoff between size and precision has been anticipated by Cleaveland et al. in [11]. For $\star \in \{\text{ps}, \text{pr}\}$, one seeks abstraction relations $Q \subseteq \Sigma \times \Sigma_Q$ such that $\mathcal{M}_{Q^\star}^c$ is as small and $\mathcal{M}_{Q^\star}^a$ as big as possible. Since the computation of $R_{Q^\star}^a$ -transitions requires disjunctions of abstract states for the source of transitions, there are 2^{2^n} possible states for n predicates. Cartesian abstraction [4] brings this upper bound down to 3^n , alas at a likely loss of precision.

6.2 Cartesian abstraction

Continuing our discussion of Section 6.1, let $\Sigma_{Q'}$ be the set of tri-vectors over $\{0, 1, *\}$ of length n . We define $Q' \subseteq \Sigma \times \Sigma_{Q'}$ by $(s, t) \in Q'$ iff for all i , $t_i \neq *$

implies ($t_i = 1$ iff $s \models \psi_i$). The relation Q' is left-total and right-total. The relation Q' is also measurable, where $\mathcal{F}_Q = \mathcal{P}(\Sigma_Q)$. Given $B \subseteq \Sigma'_Q$ and $t \in B$, let ϕ'_t and ϕ_B be defined as in Section 6.1, where every empty conjunction ϕ'_t is understood to be \mathbf{tt} . Then $Q.B = \llbracket \phi_B \rrbracket_\rho \in \mathcal{F}$. Again, since Q' represents a function Q^{ps} relates μ to μ_Q only.

Example 3. Continuing Example 2, let Σ_Q be $\{*\}$ with four R^c -transitions, one for each transition in the concurrent, labeled Markov chain. These transitions lead back to $*$ with probability 1. All state observables p and q are in $L^c(*)$. There are no R^a -transitions and $L^a(*)$ is empty. Every finite concurrent, labeled Markov chain with such observables is a possibilistic/probabilistic refinement of that system.

Theorem 8 (Cartesian abstraction has measurable navigation). *Theorem 7 extends to the use of cartesian abstraction.*

Our results on possibilistic and probabilistic abstraction confirm existing work on sound abstraction of universal properties (e.g. reachability [15]) but extend such work to the scope of an unrestricted logic; unfortunately, the quality of abstraction-based probabilistic model checking for unrestricted properties depends crucially on the precision of the abstract model: whether we are able to compute few $R^c_{Q^*}$, and many $R^a_{Q^*}$ transitions. In any event, the presence of three-valued propositional state observables may improve the precision of reachability analyses.

7 Conclusions

We presented a quantitative notion of Kripke structures whose quantities stem from a partial order, whose properties have denotations in a σ -algebra, and whose possibilistic abstraction is sound for all verifications of properties from a quantitative logic with negation and quantification. State transitions in such models map states to quantitative measures. Modal probabilistic systems are a special instance of such models, have a probabilistic abstraction — for which we proved soundness for full probabilistic LTL — , and their possibilistic property semantics approximates the probabilistic one. Predicate-based abstractions specify abstract models in the quantitative and probabilistic case.

Acknowledgments

We wish to thank the anonymous referees for their most helpful comments.

References

1. S. Andova and J. C. M. Baeten. Abstraction in Probabilistic Process Algebras. In T. Margaria and W. Yi, editors, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'01)*, volume 2031 of *Lecture Notes in Computer Science*, pages 204–219, Genova, Italy, April 2-6 2001. Springer Verlag.

2. C. Baier, E. M. Clarke, V. Hartonas-Garmhausen, M. Kwiatkowska, and M. Ryan. Symbolic Model Checking for Probabilistic Processes. In *Proc. ICALP'97*, volume 1256 of *Lecture Notes in Computer Science*, pages 430–440, 1997.
3. C. Baier and M. Kwiatkowska. Model checking for a probabilistic branching-time logic with fairness. *Journal of Distributed Computing*, 11:125–155, 1998.
4. T. Ball, A. Podelski, and S. K. Rajamani. Boolean and Cartesian Abstraction for Model Checking C Programs. In T. Margaria and W. Yi, editors, *Proceedings of TACAS'2001*, volume 2031 of *LNCS*, pages 268–283, Genova, Italy, April 2001. Springer Verlag.
5. G. Bruns and P. Godefroid. Model Checking Partial State Spaces with 3-Valued Temporal Logics. In *Proceedings of the 11th Conference on Computer Aided Verification*, volume 1633 of *Lecture Notes in Computer Science*, pages 274–287. Springer Verlag, July 1999.
6. G. Bruns and P. Godefroid. Generalized Model Checking: Reasoning about Partial State Spaces. In *Proceedings of CONCUR'2000 (11th International Conference on Concurrency Theory)*, volume 1877 of *Lecture Notes in Computer Science*, pages 168–182. Springer Verlag, August 2000.
7. R. R. Bryant. Symbolic Boolean Manipulation with Ordered Binary-Decision Diagrams. *ACM Computing Surveys*, 24(3):293–318, September 1992.
8. D. Clark, C. Hankin, S. Hunt, and R. Nagarajan. Possibilistic Information Flow is safe for Probabilistic Non-Interference. In *Workshop on Issues in the Theory of Security (WITS '00)*, Geneva, Switzerland, 7-8 July 2000.
9. E. Clarke, A. Biere, R. Raimi, and Y. Zhu. Bounded Model Checking Using Satisfiability Solving. *Formal Methods in System Design*, 19(1), July 2001.
10. E.M. Clarke, O. Grumberg, and D.E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, 1994.
11. R. Cleaveland, P. Iyer, and D. Yankelevich. Optimality in abstractions of model checking. In *SAS'95: Proc. Second Static Analysis Symposium*, Lecture Notes in Computer Science 983, pages 51–63. Springer, 1995.
12. C. Courcoubetis and M. Yannakakis. The Complexity of Probabilistic Verification. *Journal of the Association of Computing Machinery*, 42(4):857–907, July 1995.
13. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs. In *Proc. 4th ACM Symp. on Principles of Programming Languages*, pages 238–252. ACM Press, 1977.
14. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Conference Record of the 27th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 12–25, Boston, Mass., January 2000. ACM Press, New York, NY.
15. P. R. D'Argenio, B. Jeannet, H. E. Jensen, and K. G. Larsen. Reachability Analysis of Probabilistic Systems by Successive Refinements. In L. de Alfaro and S. Gilmore, editors, *Process Algebra and Probabilistic Methods: Performance Modelling and Verification*, volume 2165 of *Lecture Notes in Computer Science*, pages 39–56, Aachen, Germany, September 12-14 2001. Springer Verlag.
16. C. Derman. *Finite-State Markovian Decision Processes*. Academic Press, New York, 1970.
17. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Approximating Labeled Markov Processes. In *15th Annual IEEE Symposium on Logic in Computer Science (LICS'00)*, Santa Barbara, California, 26-29 June 2000. IEEE Computer Society Press.
18. E.-E. Doberkat. The Converse of a Probabilistic Relation. Technical Report 113, Fachbereich Informatik, Universität Dortmund, June 2001.

19. E.-E. Doberkat. The Demonic Product of Probabilistic Relations. In *Foundations of Software Science and Computation Structures*, Lecture Notes in Computer Science, Grenoble, France, April 6-14 2002. Springer Verlag. To appear.
20. D. Dubois, J. Lang, and H. Pade. *Possibilistic logic*, volume 3 of *Handbook of Logic in Artificial Intelligence and Logic Programming*, pages 439–514. Oxford University Press, 1992.
21. M. Giry. A categorical approach to probability theory. In B. Banaschewski, editor, *Categorical Aspects of Topology and Analysis*, volume 915 of *Lecture Notes in Mathematics*, pages 68–85. Springer Verlag, 1981.
22. P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based Model Checking using Modal Transition Systems. In *Proceedings of the International Conference on Theory and Practice of Concurrency*, volume 2154 of *Lecture Notes in Computer Science*, pages 426–440. Springer Verlag, August 2001.
23. P. R. Halmos. *Measure Theory*. Graduate Texts in Mathematics 18. Springer Verlag, 1950.
24. H. Hansson. *Time and Probability in Formal Design of Distributed Systems*. PhD thesis, Department of Computer Science, Uppsala University, Uppsala, Sweden, 1991.
25. A. Harding, M. Ryan, and P.-Y. Schobbens. Approximating ATL* in ATL. In *Third International Workshop on Verification, Model Checking and Abstract Interpretation*, volume 2294 of *Lecture Notes in Computer Science*, pages 289–301, Venice, Italy, January 21-22 2002. Springer Verlag.
26. J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press, 1996.
27. C. A. R. Hoare. *Communicating Sequential Processes*. Prentice-Hall, 1985.
28. M. Huth. Model checking modal transition systems using Kripke structures. In *Third International Workshop on Verification, Model Checking and Abstract Interpretation*, volume 2294 of *Lecture Notes in Computer Science*, pages 302–316, Venice, Italy, January 21-22 2002. Springer Verlag.
29. M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In Sands D., editor, *Proceedings of the European Symposium on Programming (ESOP'2001)*, pages 155–169. Springer Verlag, April 2001.
30. B. Jonsson and K. G. Larsen. Specification and Refinement of Probabilistic Processes. In *6th Annual IEEE Symposium on Logic in Computer Science*, pages 266–277, Amsterdam, The Netherlands, 15-18 July 1991. IEEE Computer Society Press.
31. P. Kelb. Model checking and abstraction: a framework preserving both truth and failure information. Technical Report OFFIS, University of Oldenburg, Germany, 1994.
32. K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, September 1991.
33. K. G. Larsen and B. Thomsen. A Modal Process Logic. In *Third Annual Symposium on Logic in Computer Science*, pages 203–210. IEEE Computer Society Press, 1988.
34. A. McIver. A Generalization of Stationary Distributions, and Probabilistic Program Algebra. In *MFPS 2001: Seventeenth Conference on the Mathematical Foundations of Programming Semantics*, volume 45 of *Electronic Notes in Theoretical Computer Science*, Aarhus, Denmark, 23-26 May 2001. Elsevier.
35. R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

36. D. Monniaux. Abstract interpretation of programs as Markov decision processes. Technical report, Département d'Informatique, École Normale Supérieure, 45, rue d'Ulm, 75230 Paris cedex 5, France, 2001.
37. C. Morgan, A. McIver, K. Seidel, and J. W. Sanders. Refinement-oriented probability for CSP. *Formal Aspects of Computing*, 8(6):617–647, 1996.
38. Prakash Panangaden. The Category of Markov Kernels. In M. Kwiatkowska, C. Baier, M. Huth and M. Ryan, editors, *Electronic Notes in Theoretical Computer Science*, volume 22. Elsevier Science Publishers, 2000.
39. D. M. R. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, *In Proc. of the 5th GI Conference*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer Verlag, 1989.
40. A. Di Pierro, C. Hankin, and H. Wiklicky. Approximate non-interference. Submitted, February 2002.
41. A. Di Pierro and H. Wiklicky. Concurrent Constraint Programming: Towards Probabilistic Abstract Interpretation. In *Proc. of the 2nd Int'l ACM SIGPLAN conference on Principles and Practice of Declarative Programming (PPDP'00)*, pages 127–138, Montreal, Canada, September 20-23 2000. ACM Press.
42. D. E. Rumelhart, J. L. McClelland, and the PDP Research Group. *Parallel Distributed Processing*, volume 1 of *Exploitations in the Microstructure of Cognition*. The MIT Press, 1986.
43. A. Sabelfeld and D. Sands. A per model of secure information flow in sequential programs. In *Programming Languages and Systems, 8th European Symposium on Programming (ESOP'99)*, volume 1576 of *Lecture Notes in Computer Science*, pages 40–58. Springer Verlag, 1999.
44. D. A. Schmidt. From Trace Sets to Modal-Transition Systems by Stepwise Abstract Interpretation. *Electronic Notes in Theoretical Computer Science*, March 2001. Proc. Workshop on Structure Preserving Relations, Amagasaaki, Japan. To appear.
45. M. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *Proc. 26th IEEE Symp. on Foundations of Computer Science*, pages 327–338, Portland, Oregon, October 1985.
46. M. Vardi. Probabilistic Linear-Time Model Checking: an Overview of The Automata-Theoretic Approach. In J.-P. Katoen, editor, *Formal Methods for Real-Time and Probabilistic Systems, 5th Int'l AMAST Workshop (ARTS'99)*, volume 1601 of *Lecture Notes in Computer Science*, pages 265–276, Bamberg, Germany, 26-28 May 1999. Springer Verlag.
47. L. Zuck, A. Pnueli, and Y. Kesten. Automatic Verification of Probabilistic Free Choice. In A. Cortesi, editor, *Third International Workshop on Verification, Model Checking and Abstract Interpretation*, volume 2294, pages 208–224, Venice, Italy, 21-22 January 2002. Springer Verlag.