A Unifying Framework for Model Checking Labeled Kripke Structures, Modal Transition Systems, and Interval Transition Systems

Michael Huth

Department of Computing and Information Sciences, Kansas State University,
Manhattan, KS 66506-2302, huth@cis.ksu.edu,
WWW home page: http://www.cis.ksu.edu/~huth

Abstract. We build on the established work on modal transition systems and probabilistic specifications to sketch a framework in which system description, abstraction, and finite-state model checking all have a uniform presentation across various levels of qualitative and quantitative views together with mediating abstraction and concretization maps. We prove safety results for abstractions within and across such views for the entire modal mu-calculus and show that such abstractions allow for some compositional reasoning with respect to a uniform family of process algebras à la CCS.

1 Introduction and Motivation

Process algebras such as Milner's CCS [16] and modular guarded command languages such as McMillan's SMV [15] are important description languages for a wide range of computer systems. The operational meaning of such descriptions is typically captured by a triple $\mathcal{M} = (S, R, L)$, where S is a set of states, R the state-transition relation, and L contains atomic state information; the latter is usually trivial in an event-based setting. The analysis of such descriptions can be done in a variety of ways. In model checking [3, 20], the idea is to have a finite-state system $\mathcal{M}$ and a specification ϕ in some temporal logic, together with an efficient algorithm for deciding whether ϕ holds for all initial states of $\mathcal{M}$. Due to the typical exponential blow-up of the state set in the number of "parallel" components, one often requires abstraction techniques for data and even control flow paths in order to bring S down to smaller size [4]. One then needs to make certain that a positive model check of ϕ for the abstracted system $\mathcal{M}'$ means that the original system $\mathcal{M}$ satisfies the specification ϕ as well.

While this triad of system description, abstraction, and verification formalism has been well established and successful for qualitative system design and analysis, its transfer to quantitative system descriptions has, by and large, been problematic. On the conceptual side, in moving from a qualitative to a quantitative view of a system, one ordinarily has to change the description language, the notion of abstraction, and the verification engine completely; for a notable exception see J. Hillston's work in [8]. Such changes not only necessitate the knowledge

of sophisticated and computationally expensive concepts, such as measure theory [7] and probabilistic bisimulation [13, 1], but also make it hard to embed the qualitative description into such a quantitative view, or to re-interpret quantitative results as qualitative judgments. Ideally, one would like to have a *uniform* family of such triads with view-mediating maps across all three dimensions: description, abstraction, and verification.

While our paper is an initial contribution toward crafting such a family, it also proposes the development of such a model checking framework for *loosely* specifying and verifying qualitative and quantitative systems. Systems often cannot be described in complete detail and usually we would like to give an implementor more flexibility in how to realize a specified system. Note that these comments apply to qualitative systems, such as concurrency protocols, as well as to quantitative ones, like loose Markov chains, where the actual state-transition probabilities may only be known to be within some interval. Our work extends and builds upon the work on modal transition systems by K. G. Larsen and B. Thomsen [14, 12], and probabilistic specifications [10] by B. Jonsson and K. G. Larsen. Both approaches have in common that transitions $s \to^a s'$ are *loosely* specified, meaning that the system description does not determine the actual implementation fully. For modal transition systems, transitions $s \to^a s'$ are either *guaranteed* ($s \to^a_\Box s'$), or *possible* ($s \to^a_\Diamond s'$) [14]. For probabilistic specifications, we have transitions of the form $s \to^a_{\mathcal{P}} s'$, where $\mathcal{P}$ is a "set of probabilities" [10] which we will always assume to be a closed interval $[x, y]$ with $0 \leq x$ and $y \leq 1$. Conceptually, the latter models are interesting because they do not commit themselves to being "reactive", "generative", or even "probabilistic" right away. Such interpretations enter via the chosen notion of refinement, where "total" refinements, our implementations, exhibit such desired properties. In this paper, we study a modal and a probabilistic interpretation of such models. In the context of model checking loosely specified systems, "safety" now means that the information computed for a property ϕ is a consistent and valid approximation of the information that we could compute for any possible refinement, or implementation.

In the next section, we present three different views of a system along with their corresponding refinement notions. In Section 3, each such view determines a semantics of the modal mu-calculus which we prove to be sound with respect to refinement. Section 4 discussed abstractions and concretizations across system views and shows how model checking results transfer across such views. In Section 5, we hint at a process algebra framework which accommodates viewing systems at three levels and prove some compositionality results of process algebra operators with respect to refinement. Section 6 briefly covers a probabilistic view, giving rise to loose Markov chains. Finally, Section 7 provides an outlook on future work.

2 Different views of a system

To illustrate, we consider the model of an unreliable medium in Figure 1. Clearly, the fully specified qualitative system, (a), is of little use as only flawed media

(with an error state) are allowed refinements up to bisimulation. The qualitative, but loosely specified system, (b), is already faring better, since an implementation may now choose not to realize the transition from state `full` to state `error`. A possible refinement would therefore be the ideal and always reliable medium obtained from (a) by removing state `error` and all its incoming and outgoing transitions. The fully specified quantitative system, (c), prescribes even more realistic behavior by giving probabilities for correct system behavior. This Markov chain may be analyzed further, e.g. to determine its steady-state probability distribution. A *loosely specified Markov chain*, (d), however, allows more freedom in that we only specify a range for actual state-transition probabilities. This requires a generalization of existing techniques for analyzing Markov chains.

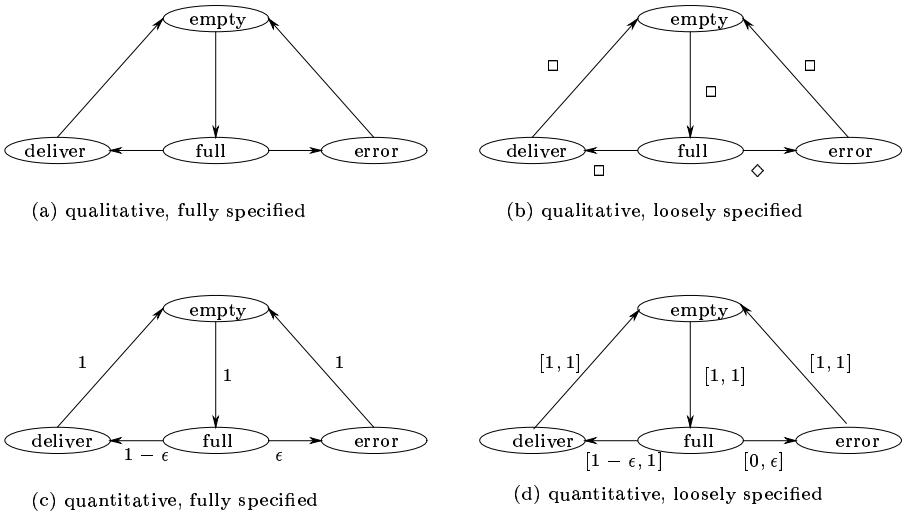

Fig. 1. Modeling an unreliable medium [10].

Three views of models. In general, we propose three views of models $\mathcal{M} = (S, R, L)$ with S a set of states, $R\colon S \times \mathtt{Act} \times S \to D$ the state-transition function, and $L\colon S \times \mathtt{AP} \to D$ the state-labeling function, where `Act` is a set of action labels, `AP` a set of atomic state predicates, and D is one of the three *domains of view*, the *type* of the model $\mathcal{M}$. We write $\mathcal{M} \triangleright D$ to indicate this relationship. If D equals `K`, the two-element lattice $\{\mathtt{ff} < \mathtt{tt}\}$, then such models are known as labeled Kripke structures (Figure 1(a); we omitted the action labels since `Act` is a singleton set); such structures are also known as *Doubly Labeled Transition Systems* ($\mathtt{L}^2\mathtt{TS}$) in the literature [6]. If D equals the three-element poset $\{\mathtt{dk}, \mathtt{ff}, \mathtt{tt}\}$, which has `dk` (`dk` for "don't know") as a least element, and all other elements are maximal; then models are essentially the modal transition systems of [14] (Figure 1(b); $\Box$ is interpreted as $\{\mathtt{tt}\}$ and $\Diamond$ as $\{\mathtt{dk}, \mathtt{tt}\}$). Finally, if D equals the interval domain

$\mathtt{I}$ [17, 21], the collection of all closed intervals $[x, y]$ with $0 \leq x \leq y \leq 1$, ordered under reverse containment: $[u, v] \leq [x, y]$ iff $u \leq x \leq y \leq v$; then models are *interval transition systems*, a special case of the probabilistic specifications in [10] (Figure 1(d)). Note that the Markov chain in Figure 1(c) can be seen as a *maximal* interval transition system as all its behavior is fully specified with respect to the information ordering on $\mathtt{I}$, by identifying any $r \in [0, 1]$ with $[r, r] \in \mathtt{I}$. It is helpful and insightful to also interpret $\Box$ and $\Diamond$ on the domains $\mathtt{K}$ and $\mathtt{I}$. On $\mathtt{K}$, both modalities are identified with the set $\{\mathtt{tt}\}$; all possible behavior is also guaranteed. On $\mathtt{I}$, we write $\Box[x, y]$ iff $x > 0$, and $\Diamond[x, y]$ iff $y > 0$: x stands for the guarantee and y for the possibility of a transition $R(s, a, s') = [x, y]$. Later on, we interpret negation on D and $\Box$ will not be the dual of $\Diamond$, unless D equals $\mathtt{K}$.

Abstractions within system views. It is straightforward to define the sum $\mathcal{M} + \mathcal{M}'$ of two systems of type D. Therefore, we may reduce the concept of "system $\mathcal{M}$ abstracts system $\mathcal{M}'$" to "state t abstracts state s in system $\mathcal{M} + \mathcal{M}'$" which, in turn, may be reduced to "state s refines state t in system $\mathcal{M} + \mathcal{M}'$". The intuitive meaning of "s refines t" is that *possible* transitions out of s are matched with possible transitions out of t, and *guaranteed* transitions out of t are matched with guaranteed transitions out of s [14]; no conditions are imposed on guaranteed transitions out of s, or possible transitions out of t. Further, a notion of refinement should be co-inductive, monotone with respect to the information ordering on D, uniform in the choice of D, and should allow for some compositional reasoning.

Definition 1. *For $\mathcal{M} = (S, R, L) \rhd D$, we define a functional $F_D \colon \mathcal{P}(S \times S) \to \mathcal{P}(S \times S)$: given $Q \subseteq S \times S$, we set $(s, t) \in F_D(Q)$ iff*

1. *For all $a \in \mathtt{Act}$, and all $s' \in S$, if $\Diamond R(s, a, s')$, then there is some $t' \in S$ such that $(s', t') \in Q$, $\Diamond R(t, a, t')$, and $R(t, a, t') \leq R(s, a, s')$ in D.*
2. *For all $a \in \mathtt{Act}$, and all $t' \in S$, if $\Box R(t, a, t')$, then there is some $s' \in S$ such that $(s', t') \in Q$, $\Box R(s, a, s')$, and $R(t, a, t') \leq R(s, a, s')$ in D.*
3. *For all $p \in \mathtt{AP}$, we have $L(t, p) \leq L(s, p)$ in D.*

Subsets $Q \subseteq S$ satisfying $Q \subseteq F_D(Q)$ are called D-refinements.

It is easily seen that these functions F_D are monotone, so they have a greatest fixed point $\sqsubseteq_D$ which is also the greatest D-refinement. One may readily show that D-refinements are closed under all unions and relational composition. For D being $\mathtt{K}$, $\mathtt{K}$-refinements are simply Milner's bisimulations [16] for all event-based models (= trivial labeling function). To illustrate, consider the model in Figure 1(d). If we annotate all transitions of Figure 1(a) with $[1, 1]$ and remove the state `error`, then the resulting system is an $\mathtt{I}$-refinement of the system in (d). Similarly, if we write $[p, p]$ for each state-transition probability p of the model in Figure 1(c), then this renders another $\mathtt{I}$-refinement of the model in (d). Our $\mathtt{M}$-refinements differ from Larsen's and Thomsen's refinement notion for modal transition systems in [14] in that they match an $R(s, a, s') = \mathtt{dk}$ with some $R(t, a, t')$ such that $R(t, a, t') \leq \mathtt{tt}$, whereas we insist on a monotone

match $R(t,a,t') = \mathtt{dk}$, since $R(t,a,t') \leq R(s,a,s')$ is enforced. This is a sharper constraint: a possible, *but not guaranteed*, transition out of the refining state s has to be matched with a possible, but not guaranteed, transition out of the refined state t. While our notion is suited for unifying it with a refinement for interval transition systems, Larsen's and Thomsen's refinement is not only sound, but also complete [12], for equivalences based on the fragment of the modal mu-calculus without fixed-points, covered in the next section.

3 Three semantics of temporal logic

We use the modal mu-calculus [11] as our logic for specifying system properties; its syntax is given by $\phi ::= \mathtt{false} \mid p \mid Z \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle\, \phi \mid [a]\, \phi \mid \mu Z.\phi$ where p ranges over $\mathtt{AP}$, Z over a set of variables, $a \in \mathtt{Act}$, and the bodies ϕ in $\mu Z.\phi$ are formally monotone. We write $\mathtt{true}$ and $\vee$ for the corresponding derived operators. Without fixed points and variables, its semantics for modal transition systems is implicitly given in [12] for a modal interpretation of Hennessey-Milner logic to obtain a characterization of their notion of refinement. There are several "natural" semantics for models of type $\mathtt{I}$; a probabilistic interpretation is sketched in Section 6. A quantitative modal semantics is developed below. We define all these semantics uniformly and only point out the salient differences. Given a model $\mathcal{M} = (S, R, L) \rhd D$, the meaning $[\![\phi]\!]^D$ is generally a function of type $\mathsf{Env}_D \to S \to D$, where Env_D is the space of all functions (environments ρ) which map variables Z to elements in D. For the remainder of this paper, we assume that all models $\mathcal{M} = (S, R, L) \rhd D$ are *image-finite*: $\{s' \in S \mid \Diamond R(s,a,s')\}$ is finite for all $s \in S$ and $a \in \mathtt{Act}$.

Semantics for $\mathtt{K}$ and $\mathtt{M}$. The interpretation of propositional logic over $\mathtt{K}$ is the usual one. For $\mathtt{M}$, we extend this interpretation by $\neg\mathtt{dk} = \mathtt{dk}$, $\mathtt{dk} \wedge \mathtt{ff} = \mathtt{ff}$, $\mathtt{dk} \wedge x = \mathtt{dk}$ if $x \neq \mathtt{ff}$, and $\vee$ is the deMorgan dual of $\wedge$ via $\neg$. Then $[\![[a]\, \phi]\!]^D \rho\, s = \bigwedge_D \{[\![\phi]\!]^\rho\, s' \mid \Diamond R(s,a,s')\}$ and $[\![\langle a \rangle\, \phi]\!]^D \rho\, s = \bigvee_D \{[\![\phi]\!]^\rho\, s' \mid \Box R(s,a,s')\}$, where $\bigwedge$ is the interpretation of the $n$ary $\wedge$ and $\bigvee$ that of $n$ary $\vee$ on $D = \mathtt{K}$ or $\mathtt{M}$. Note that this semantics is conservative with respect to refinement as the universal modality $[a]$ quantifies over all *possible* transitions, whereas the existential modality $\langle a \rangle$ only ranges over guaranteed system moves. Except for $\neg$ on $\mathtt{K}$, all operations have continuous meaning with respect to the Scott-topology on $S \to D$ (pointwise ordering). Thus, we may define the meaning of $\mu Z.\phi$ as a least fixed point (only for $\mathtt{K}$ do we require that ϕ be formally monotone). The semantics for $\mathtt{K}$ is the usual one for labeled Kripke structures, since $\Box$ and $\Diamond$ agree on $\mathtt{K}$. The semantics for $\mathtt{M}$, without fixed points, is essentially the one in [12]; note that $\neg\langle a \rangle \neg$ has a different interpretation than $[a]$ on $\mathtt{M}$. We get safety of model checks with respect to D-refinement.

Theorem 1. *Let $\mathcal{M} \rhd D$ be a model of type $\mathtt{K}$, or $\mathtt{M}$, with state set S and $s \sqsubseteq_D t$ in S. Then $[\![\phi]\!]^D \rho\, t \leq [\![\phi]\!]^D \rho\, s$ holds for all ϕ and ρ.*

Thus, model checking an abstraction will give us sound results for the model check of any of its refinements, including an actual implementation.

A modal view of $\mathtt{I}$. Interval transition systems exhibit two, almost orthogonal, dimensions of non-determinism: first, which element in $\{s' \in S \mid \Diamond R(s,a,s')\}$ will be chosen for execution; second, which r in the interval $R(s,a,s')$ may an implementation realize for the transition $s \to^a s'$? These notions overlap precisely when $R(s,a,s')$ equals $[0,y]$ with $y > 0$, for then s' may, or may not, be in the set of actual a-successors of s in the implemented system. This subtlety has to be reflected in any semantics $[\![\phi]\!]^{\mathtt{I}}$. We define a modal semantics $[\![\phi]\!]^{\mathtt{I}}\rho\, s$, which is an interval $[x,y]$, such that x is the greatest lower bound *guarantee* that $s \models_\rho \phi$ holds, whereas y is the least upper bound *possibility* thereof; note that $s \models_\rho \phi$ is a shorthand for $s \in [\![\phi]\!]^{\mathtt{K}}\rho$, where we turn a system of type $\mathtt{I}$ into one of type $\mathtt{K}$, as explained in Section 4. This intuition determines the semantics uniquely up to an interpretation of set-theoretic conjunction over $\mathtt{I}$, needed in the set qualifications for $[a]$ and $\langle a\rangle$. Our semantics therefore depends implicitly on a *t-norm* $T\colon [0,1]\times[0,1] \to [0,1]$, a Scott-continuous map (= preserving all directed suprema) which interprets conjunction and makes $([0,1],T,1)$ into a commutative monoid. The interpretation of $\neg$ is $\neg[x,y] = [1-y, 1-x]$. The meaning of $\neg$ may be justified with the prescriptive intuition given above. We illustrate such reasoning for the interpretation of $\wedge$: if $[\![\phi]\!]^{\mathtt{I}}\rho\, s = [x,y]$ and $[\![\psi]\!]^{\mathtt{I}}\rho\, s = [u,v]$, then $[x,y] \wedge [u,v]$ ought to be $[\min(x,u), \min(y,v)]$. We only justify the choice of $\min(x,u)$ as the other case is argued similarly: x is a guarantee for $s \models_\rho \phi$ and u is a guarantee for $s \models_\rho \psi$; thus, we have at least the guarantee $\min(x,u)$ in either case. Using the proof rule $\wedge$-introduction, we obtain that $\min(x,u)$ is a guarantee for $s \models_\rho \phi \wedge \psi$. If a is another such guarantee, we may use the proof rules $\wedge$-elimination twice to conclude that a is also a guarantee for $s \models_\rho \phi$ and $s \models_\rho \psi$. But then $a \leq x$ and $a \leq u$ follows as x and u are least upper bounds on the guarantees of these respective properties.

Now we define the *modal* quantitative semantics of $\langle a\rangle$ and $[a]$. In the sequel, we write $\mathrm{pr}_1\colon \mathtt{I} \to [0,1]$ for the function $[x,y] \mapsto x$ and $\mathrm{pr}_2\colon \mathtt{I} \to [0,1]$ for $[x,y] \mapsto y$. According to our primary semantic guideline, we set $[\![\langle a\rangle\,\phi]\!]^{\mathtt{I}}\rho\, s = [x,y]$, where $x = \bigvee_{[0,1]}\{T(\mathrm{pr}_1 R(s,a,s'), \mathrm{pr}_1[\![\phi]\!]^{\mathtt{I}}\rho\, s') \mid \Box R(s,a,s')\}$ and $y = \bigvee_{[0,1]}\{T(\mathrm{pr}_2 R(s,a,s'), \mathrm{pr}_2[\![\phi]\!]^{\mathtt{I}}\rho\, s') \mid \Diamond R(s,a,s')\}$. Since the $\mathrm{pr}_2 R(s,a,s')$ are all least upper bound possibilities for $s \to^a s'$, since $\mathrm{pr}_2[\![\phi]\!]^{\mathtt{I}}\rho\, s'$ is assumed to be the least upper bound possibility for $s' \models_\rho \phi$ to hold, the least upper bound for the possibility of $s \models_\rho \langle a\rangle\,\phi$ is a maximal $T(\mathrm{pr}_2 R(s,a,s'), \mathrm{pr}_2[\![\phi]\!]^{\mathtt{I}}\rho s')$, where the transition to s' is a possible one. A similar justification for x being the greatest lower bound guarantee for $s \models_\rho \langle a\rangle\,\phi$ can be given. Although the qualifications $\Box$ and $\Diamond$ are not really needed for computing the meaning of $\langle a\rangle$, they reveal a duality between $\langle a\rangle$ and $[a]$. We obtain the meaning of $[a]\,\phi$ from the one of $\langle a\rangle\,\phi$ by swapping all occurrences of $\Box$ and $\Diamond$, note that $\Box$ and $\Diamond$ are then no longer redundant, and by replacing all occurrences of $\bigvee_{[0,1]}$ with $\bigwedge_{[0,1]}$. This reflects the fact that we now have to reason about bounds for *all* possible next states. If we write $[u,v]$ for $[\![[a]\,\phi]\!]^{\mathtt{I}}\rho\, s$, then $u = \bigwedge_{[0,1]}\{T(\mathrm{pr}_1 R(s,a,s'), \mathrm{pr}_1[\![\phi]\!]^{\mathtt{I}}\rho\, s') \mid \Diamond R(s,a,s')\}$ and $v = \bigvee_{[0,1]}\{T(\mathrm{pr}_2 R(s,a,s'), \mathrm{pr}_2[\![\phi]\!]^{\mathtt{I}}\rho\, s') \mid \Box R(s,a,s')\}$. The justification of this semantics is dual to the one of $\langle a\rangle$ in the sense of "duality" explained above.

The justification for the least fixed-point semantics of $[\![\mu Z.\phi]\!]^{\mathtt{I}}\rho\, s$ is that we begin to unfold the recursive meaning with initial value $[0,1]$, the bottom of $\mathtt{I}$, at each state: initially, no guarantees, but all possibilities are given. The process of unfolding increases evidence for the guarantee of $s \models_\rho \mu Z.\phi$, whereas it decreases its possibility. If, and when this process stabilizes, we have established the best evidence we could find for $s \models_\rho \mu Z.\phi$ without knowing the particular implementation. Since $\mathtt{M}$ and $\mathtt{I}$ are not complete lattices, but are domains, we have to, and can, define the meaning of *greatest* fixed points $[\![\nu Z.\phi]\!]^D$ as $[\![\neg\mu Z.\neg\phi[\neg Z/Z]]\!]^D$, where $\phi[\neg Z/Z]$ is the result of replacing all free occurrences of Z in ϕ with $\neg Z$.

Theorem 2. *For the denotational semantics $[\![\phi]\!]^{\mathtt{I}}$, all its operations are Scott-continuous. In particular, the approximation of fixed points reaches its meaning at level ω. Moreover, if $\mathcal{M} \rhd \mathtt{I}$ has state set S with $s \sqsubseteq_{\mathtt{I}} t$ in S, then $[\![\phi]\!]^{\mathtt{I}}\rho\, t \leq [\![\phi]\!]^{\mathtt{I}}\rho\, s$ holds for all ϕ and ρ.*

This semantics is also continuous in the sense that the meaning $[\![\phi]\!]^{\mathtt{I}}$ will depend continuously on small changes made to R and L in an underlying model $\mathcal{M} = (S, R, L) \rhd \mathtt{I}$.

4 Abstractions across views.

With a semantics of temporal logic formulas for each system view at hand, we need to understand whether and how such meanings transfer if we change the view of a system under consideration. We give such an account for moving between $\mathtt{K}$ and $\mathtt{M}$, and $\mathtt{M}$ and $\mathtt{I}$, respectively.

Abstraction and safety between $\mathtt{K}$ and $\mathtt{M}$. The change of view between models of type $\mathtt{K}$ and $\mathtt{M}$ is different in quality from a move between models of type $\mathtt{M}$ and $\mathtt{I}$, for $\neg$ is *not* monotone on models of type $\mathtt{K}$. Moreover, the embedding $i\colon \mathtt{K} \to \mathtt{M}$, with $i(x) = x$ for all $x \in \mathtt{K}$, is *not* monotone as well. It induces embeddings of models $\mathcal{M} = (S, R, L) \rhd \mathtt{K}$ by setting $i\mathcal{M} = (S, i \circ R, i \circ L) \rhd \mathtt{M}$. Conversely, $\alpha_*, \alpha_*^{\mathrm{tr}}\colon \mathtt{M} \to \mathtt{K}$ are both monotone maps γ with $\gamma \circ i = \mathsf{id}_{\mathtt{K}}$ and $i \circ \gamma \geq \mathsf{id}_{\mathtt{M}}$; among those maps α_* and α_*^{tr} are uniquely defined by $\alpha_*(\mathtt{dk}) = \mathtt{ff}$ and $\alpha_*^{\mathrm{tr}}(\mathtt{dk}) = \mathtt{tt}$, respectively. We set $\alpha_*\mathcal{M}' = (S, \alpha_*^{\mathrm{tr}} \circ R', \alpha_* \circ L') \rhd \mathtt{K}$ for any $\mathcal{M}' = (S, R', L') \rhd \mathtt{M}$. The map α_* translates "truth values" pertaining to "propositional" information (model checks and labeling functions) and behaves well with respect to propositional logic: $\alpha_* \circ \neg \leq \neg \circ \alpha_*$, $\alpha_* \circ \wedge = \wedge \circ \alpha_* \times \alpha_*$, and $\alpha_* \circ \vee = \vee \circ \alpha_* \times \alpha_*$. Since α_*^{tr} gives us a conservative account of transitions, and since α_* preserves all suprema as a lower adjoint of α, which differs from i in that it sends $\mathtt{ff}$ to $\mathtt{dk}$, we may relate model checks on $\mathcal{M}' \rhd \mathtt{M}$ to those on $\alpha_*\mathcal{M} \rhd \mathtt{K}$, and, similarly, we may compare such results computed for $\mathcal{M} \rhd \mathtt{K}$ and $i\mathcal{M} \rhd \mathtt{M}$.

Theorem 3. *For all formulas ϕ of the modal mu-calculus, we have the inequality $\alpha_*[\![\phi]\!]^{\mathcal{M}' \rhd \mathtt{M}}\rho' \leq [\![\phi]\!]^{\alpha_*\mathcal{M}' \rhd \mathtt{K}}\alpha_* \circ \rho'$ and the equality $i[\![\phi]\!]^{\mathcal{M} \rhd \mathtt{K}}\rho = [\![\phi]\!]^{i\mathcal{M} \rhd \mathtt{M}} i \circ \rho$ for all models and environments of the required types.*

For $D = \mathtt{K}$ or $\mathtt{M}$, we write $s \models^{\mathcal{M}}_{\rho} \phi$, if $[\![\phi]\!]^{\mathcal{M} \triangleright D} \rho\, s = \mathtt{tt}$; and $s \not\models^{\mathcal{M}}_{\rho} \phi$, if $[\![\phi]\!]^{\mathcal{M} \triangleright D} \rho\, s = \mathtt{ff}$, where $\mathcal{M}$ is a model of type D and $\rho \in \mathsf{Env}_D$. Given any $\mathcal{M}' = (S, R', L') \triangleright \mathtt{M}$ with $s \models^{\mathcal{M}'}_{\rho} \phi$, we may use the previous theorem to infer that $\mathtt{tt} = \alpha_* [\![\phi]\!]^{\mathcal{M}' \triangleright \mathtt{M}} \rho\, s \leq [\![\phi]\!]^{\alpha_* \mathcal{M}' \triangleright \mathtt{K}} \alpha_* \circ \rho\, s$; but since $\mathtt{tt}$ is a maximal element in $\mathtt{K}$, this implies $[\![\phi]\!]^{\alpha_* \mathcal{M}' \triangleright \mathtt{K}} \alpha_* \circ \rho\, s = \mathtt{tt}$. Thus, $s \models^{\mathcal{M}'}_{\rho} \phi$ implies $s \models^{\alpha_* \mathcal{M}'}_{\alpha_* \rho} \phi$ *for all formulas of the modal mu-calculus*, where the latter is the standard notion of satisfaction for labeled Kripke structures. However, such an inference cannot be made for the negative version (at the meta-level): if $s \not\models^{\mathcal{M}'}_{\rho} \phi$, then both parts of our theorem provide no additional information in general. In this case, the inequality in this theorem is redundant as the left hand side, $\alpha_* [\![\phi]\!]^{\mathcal{M}' \triangleright \mathtt{M}} \rho'\, s$, denotes the least element of $\mathtt{K}$; the theorem's equality is of no use as well, since $i \circ \alpha_*$ is not equal to, but above, the identity $\mathsf{id}_{\mathtt{M}}$. These results are quite similar in structure to the ones obtained in [5] and it would be of interest to establish connections to the work in loc. cit.

Abstraction and safety between M and I. We embed $\mathtt{M}$ into $\mathtt{I}$ via β such that $\beta(\mathtt{dk}) = [0,1]$, $\beta(\mathtt{ff}) = [0,0]$ and $\beta(\mathtt{tt}) = [1,1]$. Note that this map is monotone and matches our semantic intuition of $[x,y]$ giving guarantees and possibilities of truth. We re-translate such truth-value intervals with the upper adjoint β^* which is uniquely determined by being monotone and satisfying $\beta^* \circ \beta = \mathsf{id}_{\mathtt{M}}$ and $\beta \circ \beta^* \leq \mathsf{id}_{\mathtt{I}}$. As for the values of transitions, we define a map $\beta^*_{\mathrm{tr}} \colon \mathtt{I} \to \mathtt{M}$ which is uniquely determined by preserving the three predicates $\Box$, $\Diamond \wedge \neg\Box$, and $\neg\Diamond$, which single out all elements of $\mathtt{M}$. Note that this map also reflects $\Box$ and $\Diamond$ from $\mathtt{M}$ back to $\mathtt{I}$. One can readily see that β^* is a homomorphism for $\neg$, $\wedge$, and $\vee$; e.g. $\beta^* \circ \neg = \neg \circ \beta^*$. As for the modalities and fixed points, we make crucial use of the fact that β^* is the upper adjoint of β. For $\mathcal{M} \triangleright \mathtt{I}$ and $\mathcal{M}' \triangleright \mathtt{M}$, we define $\beta^* \mathcal{M} = (S, \beta^*_{\mathrm{tr}} \circ R, \beta^* \circ L) \triangleright \mathtt{M}$ and $\beta \mathcal{M}' = (S, \beta \circ R', \beta \circ L') \triangleright \mathtt{I}$.

Theorem 4. *Let ϕ be any formula of the modal mu-calculus and consider models $\mathcal{M} \triangleright \mathtt{I}$ and $\mathcal{M}' \triangleright \mathtt{M}$. Then $\beta^* [\![\phi]\!]^{\mathcal{M} \triangleright \mathtt{I}} \rho \leq [\![\phi]\!]^{\beta^* \mathcal{M} \triangleright \mathtt{M}} \beta^* \circ \rho$ and $[\![\phi]\!]^{\beta \mathcal{M}' \triangleright \mathtt{I}} \rho \leq \beta [\![\phi]\!]^{\mathcal{M}' \triangleright \mathtt{M}} \beta \circ \rho$ hold for all t-norms T such that $T(a,b) = 0$ implies $a = 0$ or $b = 0$.*

The proof of this theorem reveals that the condition on the t-norm is necessary and $\mathtt{LAND}(a,b) = \max(a + b - 1, 0)$ is an example of a Scott-continuous t-norm that does not satisfy it; take a and b to be 0.5. We also require that $T(a,b) = 1$ imply $a = b = 1$, but this holds for all t-norms, since min is known to be the *greatest* t-norm in the pointwise ordering: $T(a,b) \leq \min(a,b)$ holds for all $a, b \in [0,1]$ and all t-norms T. The first inequality in the theorem above states that if a model check of type $\mathtt{I}$ results in a "truth value" $[0,0]$ or $[1,1]$, then that value is also the result of the same model check on the more concrete system of type $\mathtt{M}$. One may now combine Theorems 3 and 4 to link model-checking results between types $\mathtt{K}$ and $\mathtt{I}$.

5 Three views of description languages

We choose process algebras as system description languages which are parametric in the domain of view D, and whose structural operational semantics can be seen as an abstract interpretation, based on D, of the concrete operational semantics for $\mathtt{K}$. For sake of brevity, we only consider a fragment of Milner's CCS [16], given by the syntax $p ::= \mathsf{nil} \mid a_d.p \mid p + p \mid p||p \mid p\lceil B \mid x \mid \mathtt{fix}\, x.p$, where $d \in D$, $a \in \mathtt{Act}$, x ranges over a set of process variables, and $B \subseteq \mathtt{Act}$. Note that the only non-standard feature is the annotation of the standard prefix, $a.p$, with a domain element. We also assume the usual involution $a \mapsto \bar{a} \colon \mathtt{Act} \to \mathtt{Act}$ for communication with the self-involutive symbol $\tau \notin \mathtt{Act}$ for internal, non-observable actions. In Figure 2, the abstract interpretations $+^D$ and $\mathtt{Par}^D$ may well depend on the semantic interpretation one has in mind; e.g. whether one considers a modal or probabilistic semantics for $D = \mathtt{I}$. To wit, we define $\mathtt{Par}^D\{(d_1^a, d_2^{\bar{a}}) \mid a \in \mathtt{Act}\} = \bigvee^D\{d_1^a \wedge^D d_2^{\bar{a}} \mid a \in \mathtt{Act}\}$ for $D = \mathtt{K}$ or $\mathtt{M}$. For $D = \mathtt{I}$, we choose a modal interpretation, setting $\mathrm{pr}_2\mathtt{Par}^D\{(d_1^a, d_2^{\bar{a}}) \mid a \in \mathtt{Act}\} = 0$ if there is no $a \in \mathtt{Act}$ with $\Diamond d_1^a$ and $\Diamond d_2^{\bar{a}}$; otherwise, we define $\mathrm{pr}_2\mathtt{Par}^D\{(d_1^a, d_2^{\bar{a}}) \mid a \in \mathtt{Act}\} = \max\{\min(\mathrm{pr}_2 d_1^a, \mathrm{pr}_2 d_2^{\bar{a}}) \mid \Diamond d_1^a \text{ and } \Diamond d_2^{\bar{a}}\}$ and $\mathrm{pr}_1\mathtt{Par}^D\{(d_1^a, d_2^{\bar{a}}) \mid a \in \mathtt{Act}\} = \min\{\min(\mathrm{pr}_1 d_1^a, \mathrm{pr}_1 d_2^{\bar{a}}) \mid \Box d_1^a \text{ and } \Box d_2^{\bar{a}}\}$. Thus, this semantics computes the worst-case, respectively, best-case evidence for observing an internal τ-move. The modalities are placed as in the semantics of $[a]$ and we could have used any Scott-continuous t-norm instead of the binary min operator, as long as $\Box$ and $\Diamond$ distribute over it. The rule for recursion indicates that these interpretations have to be continuous. Note that each process term, p, determines a model of type D: if there is a judgment $\vdash R(p, a, p') = d$, then d is the value of $R(p, a, p')$; otherwise, we set it to be $[\![\mathtt{false}]\!]^D \rho\, s$. Note that $a_{\mathtt{ff}}.p$ is bisimilar to nil for D being $\mathtt{K}$.

Theorem 5. *Let $\mathtt{Par}^D$ be defined as above. For $D = \mathtt{K}$, the "abstract interpretation" in Figure 2 matches the structural operational semantics of the corresponding fragment of CCS in [16]. For $D = \mathtt{M}$, the abstract interpretation in the same figure matches the semantics of the modal process logic for the corresponding fragment in [14], where we identify $a_\Diamond.p$ and $a_\Box.p$ from [14] with $a_{\mathtt{dk}}.p$ and $a_{\mathtt{tt}}.p$, respectively.*

We are not aware of process algebras based on intervals in the literature, so we cannot compare our abstract interpretation for $D = \mathtt{I}$. Since each process term p of type D determines a model of type D, we can write $p \sqsubseteq_D q$ if p D-refines q in the system formed by the sum of p and q. We can prove that refinements are compositional for some of the process algebra operators.

Theorem 6. *For all $a \in \mathtt{Act}$, $d \in D$, and closed process algebra terms $p \sqsubseteq_D q$, $p_i \sqsubseteq_D q_i$ $(i = 1, 2)$ we have $a_d.p \sqsubseteq_D a_d.q$, $p_1||p_2 \sqsubseteq_D q_1||q_2$, and $p\lceil B \sqsubseteq_D q\lceil B$.*

This result can be extended to recursion with a machinery very similar to the one employed for $D = \mathtt{K}$ in [16].

$$\frac{}{\vdash R(a_d.p, a, p) = d}\ \text{Act} \qquad \frac{\vdash R(p_1, a, p') = d_1 \text{ and } \vdash R(p_2, a, p') = d_2}{\vdash R(p_1 + p_2, a, p') = d_1 +^D d_2}\ \text{Sum}$$

$$\frac{\vdash R(p_1, a, p_1') = d_1}{\vdash R(p_1 || p_2, a, p_1' || p_2) = d_1}\ \text{Com\_1} \qquad \frac{\vdash R(p_2, a, p_2') = d_2}{\vdash R(p_1 || p_2, a, p_1 || p_2') = d_2}\ \text{Com\_2}$$

$$\frac{\vdash R(p, a, p') = d_a \text{ and } a \in B}{\vdash R(p\lceil B, a, p'\lceil B) = d_a}\ \text{Res} \qquad \frac{\vdash R(p_1, a, p_1') = d_1^a \text{ and } \vdash R(p_2, \bar{a}, p_2') = d_2^{\bar{a}}}{\vdash R(p_1 || p_2, \tau, p_1' || p_2') = \mathtt{Par}^D\{(d_1^a, d_2^{\bar{a}}) \mid a \in \mathtt{Act}\}}\ \text{Com\_3}$$

$$\frac{\vdash R(p[\mathtt{fix}\, x.p/x], a, p') = d}{\vdash R(\mathtt{fix}\, x.p, a, p') = d}\ \text{Rec}$$

Fig. 2. Abstract interpretation of a structural operational semantics for our three process algebras

6 Loose Markov chains

Knowing the class of implementations may well allow the customization of our framework to such a class. For example, if interval transition systems are to specify labeled Markov chains, then we can restrict our attention to certain models of type $\mathtt{I}$. A labeled Markov chain (S, P, L) satisfies $\sum_{s'} P(s, a, s') = 1$ for all $a \in \mathtt{Act}$ and $s \in S$. We may approximate such a model with the same set of states by $\mathcal{M} = (S, R, L) \rhd \mathtt{I}$ such that, for all $a \in \mathtt{Act}$ and $s \in S$, we have $\sum_{s'} \mathrm{pr}_1 R(s, a, s') \leq 1$ and $\mathrm{pr}_2 R(s, a, s') \leq 1 - \sum_{s'' \neq s'} \mathrm{pr}_1 R(s, a, s'')$. The first inequality says that the lower bounds for the actual state-transition probabilities form a subprobability distribution; the sum of probabilistic guarantees must not exceed 1. The second inequality is a consistency condition, saying that the upper bound on the possible probability of $s \to^a s'$ cannot be greater than 1 minus the sum of all lower bound guarantees on probabilities of moves to any other successor state of s. We call such models *loose Markov chains*. The models in Figure 1(c) and (d) are such examples and (c) is an $\mathtt{I}$-refinement of (d). It would be of interest to define a probabilistic refinement which coincides with probabilistic bisimulation [13] for maximal models (Markov chains) and to compare such a notion with the work of [10]. As for a semantics of formulas ϕ, we change the modal semantics by re-interpreting $\wedge$, $\langle a \rangle$, and $[a]$. For $\wedge$, we may either use a safe t-norm, as done in [18, 9, 2], or develop a measure theory of measures of type $\mu \colon \Sigma(X) \to \mathtt{I}$, where the conventional measures of type $\mu \colon \Sigma(X) \to [0, 1]$ form the maximal elements of that space. As for the modalities, we identify the meaning of $\langle a \rangle$ and $[a]$ and set $\mathrm{pr}_1[\![\langle a \rangle\, \phi]\!]^{\mathtt{P}} \rho\, s = \sum_{s'} \mathrm{pr}_1 R(s, a, s') \cdot \mathrm{pr}_1[\![\phi]\!]^{\mathtt{P}} \rho\, s'$ and $\mathrm{pr}_2[\![\langle a \rangle\, \phi]\!]^{\mathtt{P}} \rho\, s = \min(1, \sum_{s'} \mathrm{pr}_2 R(s, a, s') \cdot \mathrm{pr}_2[\![\phi]\!]^{\mathtt{P}} \rho\, s')$; note that $\cdot$ is a Scott-continuous t-norm.

Theorem 7. *Let $\mathcal{M} \rhd \mathtt{I}$ be a loose Markov chain with state set S and $s \sqsubseteq_{\mathtt{I}} t$ in S. Then $[\![\phi]\!]^{\mathtt{P}} \rho\, t \leq [\![\phi]\!]^{\mathtt{P}} \rho\, s$ holds for all ϕ and ρ and all monotone interpreta-*

tions of $\wedge$; in particular, this holds when $\wedge$ is interpreted as a probabilistically conservative t-norm.

7 Outlook

The design and analysis of algorithms for deciding D-refinements needs to be done particularly for the case $D = \mathtt{I}$. It would be of interest to obtain an independent *logical characterization* of these refinements. Interval transition systems should be evaluated toward their suitability of describing systems with uncertainty, or vagueness. A guarded-command language for the description of such models may provide a foundation for the formal analysis of fuzzy interval inference systems. Connections to Bayesian networks and Dempster-Shafer theories of evidence need to be explored. The models of loose Markov chains require a customized description language; their ergodic analysis should reduce to an optimization problem. The computation of conditional probabilities, however, may require a "domain theory" for probability measures, where the latter are maximal elements in a space of "measures" of range $\mathtt{I}$. This needs to be a conservative extension in the sense that the "probability axioms" for the $\mathtt{I}$-valued measures will reduce to the familiar axioms in case that the measure is maximal. Such work may well transfer to the *generalized probabilistic logic* (GPL) designed by N. Narashima, R. Cleaveland and P. Iyer in [19]. Loose Markov chains will also benefit from a probabilistic version of $\mathtt{I}$-refinement which should coincide with a familiar probabilistic bisimulation for "maximal" models. Martin Escardo pointed out that our framework is extendible to cover infinite-state systems as well. One obtains a continuous, and computable, semantics of model checks, provided that the sets of possible ($\Diamond$) and guaranteed ($\Box$) a-successors of state s are compact for all $a \in \mathtt{Act}$ and $s \in S$, where S is a compact Hausdorff space.

Acknowledgments

A number of people have made valuable suggestions during visits, or talks, given at their institutes. Among them were Martin Escardo, Stephen Gilmore, Jane Hillston, Marta Kwiatkowska, Annabelle McIver, Carroll Morgan, and Jeff Sanders.

References

1. C. Baier. Polynomial Time Algorithms for Testing Probabilistic Bisimulation and Simulation. In *Proceedings of CAV'96*, number 1102 in Lecture Notes in Computer Science, pages 38–49. Springer Verlag, 1996.
2. C. Baier, M. Kwiatkowska, and G. Norman. Computing probability bounds for linear time formulas over concurrent probabilistic systems. *Electronic Notes in Theoretical Computer Science*, 21:19 pages, 1999.

3. E. M. Clarke and E. M. Emerson. Synthesis of synchronization skeletons for branching time temporal logic. In D. Kozen, editor, *Proc. Logic of Programs*, volume 131 of *LNCS*. Springer Verlag, 1981.
4. E. M. Clarke, O. Grumberg, and D. E. Long. Model Checking and Abstraction. In *19th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 343–354. ACM Press, 1992.
5. Dennis Dams, Rob Gerth, and Orna Grumberg. Abstract interpretation of reactive systems. *ACM Transactions on Programming Languages and Systems*, 19(2), 1997.
6. R. de Nicola and F. Vaandrager. Three Logics for Branching Bisimulation. *Journal of the Association of Computing Machinery*, 42(2):458–487, March 1995.
7. P. R. Halmos. *Measure Theory*. D. van Norstrand Company, 1950.
8. J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press. Distinguished Dissertation Series, 1996.
9. M. Huth. The Interval Domain: A Matchmaker for aCTL and aPCTL. In M. Mislove, editor, *2nd US-Brazil joint workshop on the Formal Foundations of Software Systems held at Tulane University, New Orleans, Louisiana, November 13-16, 1997*, volume 14 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 1999.
10. B. Jonsson and K. G. Larsen. Specification and Refinement of Probabilistic Processes. In *Proceedings of the International Symposium on Logic in Computer Science*, pages 266–277. IEEE Computer Society, IEEE Computer Society Press, July 1991.
11. D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.
12. K. G. Larsen. Modal Specifications. In J. Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, number 407 in Lecture Notes in Computer Science, pages 232–246. Springer Verlag, June 12–14, 1989 1989. International Workshop, Grenoble, France.
13. K. G. Larsen and A. Skou. Bisimulation through Probabilistic Testing. *Information and Computation*, 94(1):1–28, September 1991.
14. 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.
15. K. L. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.
16. R. Milner. *Communication and Concurrency*. Series in Computer Science. Prentice-Hall International, 1989.
17. R. E. Moore. *Interval Analysis*. Prentice-Hall, Englewood Cliffs, 1966.
18. C. Morgan, A. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, May 1996.
19. M. Narashima, R. Cleaveland, and P. Iyer. Probabilistic Temporal Logics via the Modal Mu-Calculus. In W. Thomas, editor, *Foundations of Software Science and Computation Structures*, volume 1578 of *Lecture Notes in Computer Science*, pages 288–305. Springer Verlag, March 1999.
20. J. P. Quielle and J. Sifakis. Specification and verification of concurrent systems in cesar. In *Proceedings of the fifth International Symposium on Programming*, 1981.
21. D. S. Scott. Lattice Theory, Data Types and Semantics. In *Formal Semantics of Programming Languages*, pages 66–106. Prentice-Hall, 1972.