The interval domain as a semantic foundation for reasoning about uncertainty or vagueness

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 re-interpret the category of relations according to *views*, pairs of dcpos $\langle P, T\rangle$ such that T embeds as a set into the set of maximal elements of P. A qualitative view $\langle \mathtt{M}, \mathbf{2}\rangle$ renders the modal transition systems of K. Larsen and B. Thomsen as a partial view, $R\colon X \times Y \to P$, of relations, $R\colon X \times Y \to \mathbf{2}$. A quantitative view represents relations as fuzzy (T is the unit interval $\mathtt{UI}$) or interval-valued (P is the interval domain $\mathtt{I}$) relations. We specify functors mediating between these categories to provide soundness of these interpretations. As for probability theory, we propose the view $\langle \mathtt{I}, \mathtt{UI}\rangle$ to embed the set of probability measures into the set of maximal elements of a space of *partial* probability measures. It is hoped that this provides a foundation for reasoning probabilistically about systems with inherent uncertainty, or vagueness, such as the probabilistic specifications of B. Jonsson and K. Larsen.

1 Motivation and outline

1.1 Motivation

The work presented here is motivated by the area of *model checking*, an automated, model-based, and property-verification approach to the formal verification of systems. Model checking, invented independently in the early eighties by E. Clarke and E.A. Emerson [5], and by J. Quielle and J. Sifakis [28], has become a quite powerful technique for modeling and reasoning about computer systems and the number of supporting tools is growing: see e.g. SMV, Verus, SPIN, cwb, FDR, The Concurrency Workbench of North Carolina, The Bandera Toolset, HyTech, and UPPAAL (the latter two verify hybrid and/or timed systems). The vital components of a model checking framework are

1. a system description language, $\mathcal{L}$, and its operational semantics which can map programs $\mathcal{P}$, written in $\mathcal{L}$, to concrete mathematical models $\mathcal{M}$ (e.g. the language SMV and its programs representing Kripke structures [22]);
2. a specification language with a precise formal semantics on models as a vehicle of expressing program behavior, originally provided in plain English, in a rigorous fashion (e.g. the branching-time logic CTL and its semantics over Kripke structures [5]);

3. feasible algorithms and implementations for deciding whether a model $\mathcal{M}$, represented by a program $\mathcal{P}$, satisfies a formal specification of behavior ϕ (e.g. symbolic model checking [3] and its implementation based on BDDs [2]);
4. a facility for informative counter-trace generation in case that $\mathcal{P}/\mathcal{M}$ does not satisfy ϕ (e.g. the debugging information provided by SMV [22]);
5. and a host of techniques for state-space reduction, combating the "state-explosion problem": equivalences (e.g. bisimulation [26, 24]), preorders (e.g. simulations [23]), abstract interpretation [8, 6], partial ordering or induction [22], to name the more prominent ones.

So far model checking has been a very successful programme for *qualitative* system design and analysis and is increasingly adopted by Research & Development departments throughout the hardware and software industry. However, its transfer to *qualitative*, or more *loosely* described systems has, by and large, been problematic. Generally speaking, viewing a system in a different mode (e.g. a probabilistic analysis) typically involves the invention of new description languages, specification logics, abstraction techniques, and verification algorithms. Having to learn several, seemingly unrelated, and monolithic model checking platforms will not persuade designers to make more use of these formal methods in their design and analysis processes. It is therefore desirable to have a model checking platform in which such changes of view impact only *minimally* on the formalisms for specifying systems and behavior; see Section 5.1 for a sketch of a possible, event-based, solution. Moreover, insights gained in one particular mode (e.g. a probabilistic one) may well be meaningful results if re-interpreted in a different mode (e.g. a qualitative one). At present, little if no work has been done which would establish links and similarities between such views *formally*.

The pair "*qualitative/quantitative*" is only one dimension along which one may vary the view of a system. Designers often would like to be more *liberal* in prescribing which actual implementations, or abstract representations thereof, *realize* a formally described system. In [20], it has been argued convincingly that equivalence notions such as bisimulations are simply too restrictive to allow for any viable degree of freedom in implementing an abstractly defined system, for implementations are confined to equivalence classes of the original system specification. As an alternative example, Timed Modal Specifications [4] is a process calculus which specifies timed labeled transition systems with **must** and **may** predicates on state transitions; ignoring "time" for sake of brevity: $s \rightarrow^a_\Box s'$ means that state s must be able to perform action a, resulting in state s'; and $s \rightarrow^a_\Diamond s'$ denotes that state s may be able to perform action a, resulting in state s'. Such a description formalism permits more freedom at the implementation level. Dually, potential model checks of such systems will have to be more *conservative* as their findings should be safe and sound for all acceptable implementations.

Another example of partially described systems are the probabilistic specifications in [19] whose state-transition function R maps triples $\langle s, a, s' \rangle$ to "sets of probabilities", or more importantly and specifically, to intervals $[x, y]$ with $0 \leq x \leq y \leq 1$. One may view these values x/y as lower/upper bounds of

actual probabilities (e.g. if the implementations are viewed as Markov decision processes [11], also known as concurrent Markov chains [31]), or these numbers could stand for lower/upper bounds of more abstract values such as *cost, confidence, vagueness, uncertainty, "hot paths",* or *evidence*; a semantic analysis of such values then has different modes as well, such as "average" or "worst/best case" behavior.

In adopting the view that finite-state models have state-transition functions R which map into a *domain of partial information*, in the form of intervals, one obtains a notion of model that makes it possible to express structures used in decision and utility theories, or fuzzy logic inference systems. Bayesian networks (see [17] for a competent introduction), while having practical impact and typically efficient design and inference algorithms, only allow for inferences of the type $P(\text{Queries} \mid \text{Evidence})$ (what is the probability that the query variables take on the specified values, given the evidence, i.e. state information?) and little formal work seems to exist that would link and compare the established state-space reduction techniques in (probabilistic) model checking to the design and inference algorithms and compactification techniques employed in Bayesian networks. As for fuzzy logic inference systems, they lack a formal semantic foundation that would make them into a proper scientific notion in the sense that one could *predict* (aspects of) such system's behaviors. The need for such predictive capabilities is particularly pressing as such inference systems are increasingly used in artifacts using engineering control systems (see e.g. [21]). A model checking framework for interval-valued, finite-state systems would provide a formally defined tool for reasoning about, and assessing, the dynamics and interaction of a set of fuzzy inference rules, rendering a design & analysis methodology for such structures.

We demonstrate below that a wide variety of different views of systems, including the ones aforementioned, have a conceptually elegant and rather uniform description if expressed in a framework for totally and partially specified systems. Furthermore, we hope that such a uniform model checking framework for partially and totally specified systems will provide a better foundation for probabilistic reasoning in the presence of *uncertainty*, based on models whose state-predicates and state-transitions have interval values; thus, we expects to provide a better account of reasoning with probabilities in the presence of uncertainty than the one provided by theories of evidence developed in the Artificial Intelligence community.

Apart from the current need for a plethora of monolithic model checking tools, another important obstacle in making model checking applicable to large-scale industrial projects is met in the "state-explosion problem": every additional state predicate (= bit) typically doubles the size of the system's state space. Hence, techniques are sought which simplify the system in a safe manner down to a manageable size. One approach is based on bisimulations [24, 26] which provide formally defined equivalence relations for replacing system components by "equivalent ones" and for approximating infinite-state systems by ones with finitely many states; however, this technique seems to perform poorly if applied

to a global system in symbolic model checking [15]. Moreover, the state-space reduction achieved by bisimulations is often insufficient for actual industrial designs and more aggressive abstraction techniques are required (see e.g. [7]). Simulations [23], for example, allow for much coarser abstractions of systems, yet, this comes at the price of being safe only for *universal* safety/liveness properties [6]. This is a serious drawback of simulations and the standard framework of abstract interpretation [8] alike, for realistic specifications of reactive system behavior frequently mix universal and existential path quantifiers in the same formal specification (e.g. "for all reachable states, there is some path leading to a reboot state"). The work in [9], although not embedded into the model-checking paradigm, adapts the conventional abstract interpretation framework to improve on this. One particular objective of this planned work, therefore, aims at providing abstraction/refinement notions which are defined *uniformly* across system views and which are safe with respect to model checks of *all* specifications, even those that mix universal and existential path quantifiers. This has already been addressed in [18].

The overall objective of this proposed line of research is to make a substantial initial contribution toward a uniform model checking framework for reasoning about *totally* specified systems (e.g. as done for SMV programs in [22]) and *partially* specified ones (e.g. the timed modal transition systems in [4]) in an integrated fashion. Conceptually, this is similar in spirit to the work done by A. Edalat and his research group at Imperial College, London, where they embed classical topological spaces into domains, making it possible to approximate points of the space (*total information*, e.g. a probability measure) with domain elements (*partial information*, e.g. a linear combination of point measures). In that project, the introduction of partial elements has led to significant contributions to numerical integration [13], the design of new image-compression algorithms based on work in dynamical systems and fractals [12], and the derivation of novel semantics and implementations of exact real arithmetic [14].

Although we propose a non-standard version of an established methodology, we hasten to point out that this *subsumes* the existing approach, as totally specified systems are just a "completed" form of partially given system. Let us discuss such an extended platform informally by means of a very simple example. Doubly Labeled Transition Systems [10] may be written as triples $\mathcal{M} = (S, R, L)$, where S is a set of states, $R\colon S \times \mathtt{Act} \times S \to \mathbf{2}$ the state-transition function ($\mathbf{2}$ is the lattice $\mathtt{ff} < \mathtt{tt}$ and $\mathtt{Act}$ is a set of action labels), and $L\colon S \times \mathtt{AP} \to \mathbf{2}$ is the state-labeling function ($\mathtt{AP}$ is a set of atomic state predicates). They generalize Kripke structures (= state-based models such as SMV programs) and labeled transition systems (= event-based models such as process algebra terms) and there are well understood ways of mapping Doubly Labeled Transition Systems down to Kripke structures and labeled transition systems [10]. We propose to change a view of such a system by changing the domain $\mathbf{2}$ to some abstract domain T of total elements.

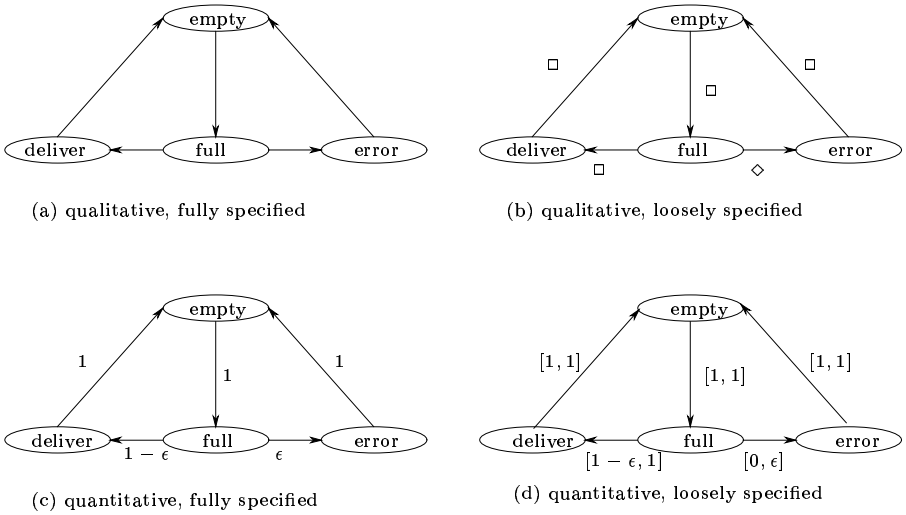
In general, if the totally specified model $\mathcal{M}$ maps into a domain T instead of $\mathbf{2}$, then a *partial* aspect of this view would require a domain P such that the

elements of T are identified with *maximal* (= total) elements in P; a notable example for the *probabilistic case* is when T is the unit interval domain $(\mathtt{UI}, \leq)$ in the usual ordering and P is the interval domain, $\mathtt{I}$, $[25, 29]$ of all interval $[x, y]$ with $0 \leq x$ and $y \leq 1$, ordered under reverse inclusion: $[x, y] \leq [u, v]$ iff $x \leq u$ and $v \leq y$. Note that the set $\mathtt{UI}$ can be identified with the set of maximal elements $\{[r, r] \mid 0 \leq r \leq 1\}$ of $\mathtt{I}$. Thus, the we model a view by a pair of domains $\langle P, T \rangle$, here given by $\langle \mathtt{I}, \mathtt{UI} \rangle$, such that T embeds into the set of maximal elements of P.

See Figure 1 for a toy example of an unreliable medium and several changes of view. The Kripke structure in (a) is obviously of little use as it allows for no qualitative or quantitative means of avoiding, or assessing, possible erroneous system behavior. The system in (b) is obtained by changing **2** to $\mathtt{M}$, the domain $\{\mathtt{dk}, \mathtt{ff}, \mathtt{tt}\}$ in which $\mathtt{dk}$ ("don't know") is the least element and all others are maximal. Thus, the unifying view is the pair $\langle \mathtt{M}, \mathbf{2} \rangle$. If one interprets $\Box$ as $\{\mathtt{tt}\}$ (necessary/guaranteed) and $\Diamond$ as $\{\mathtt{dk}, \mathtt{tt}\}$ (possible), then such systems are essentially the modal transition systems of [20]; the models of [9] are a slight variation of these as well. The intuition behind $s \rightarrow^a_\Box s'$ is that the system *guarantees* (**must** be implemented) a state transition $s \rightarrow^a s'$ in the underlying concrete model with $T = \mathbf{2}$, whereas $s \rightarrow^a_\Diamond s'$ only says that such a system move is *possible* (**may** be implemented); note that there is only one type of action in the state-based example in Figure 1, so the action labels in state transitions are omitted. With the more flexible view in (b), one is able to talk about "possible" system failure, but one needs a system as in (c), a Markov chain, to be able to *quantify* such a possibility by means of probabilistic model checking. The system in (d) also provides such quantitative descriptions, but $R(s, a, s') = [x, y]$ could now be interpreted as specifying lower (x) and upper (y) bounds of state-transition probabilities. As in the case of ordinary Markov chains, "loose Markov chains", as in (d), contain probabilistic information, but they also model the *uncertainty*, *ignorance*, or *vagueness* of such information within the same structure. This is appealing since, expect for Bayesian networks, there are no satisfactory accounts of combining probabilities and uncertainties, or ignorance, in the same framework; this is particularly true for the theories of evidence studied in Artificial Intelligence when reasoning about knowledge under uncertainty and ignorance.

1.2 Outline

In Section 2, we study the notion which is at the heart of this work: relations and their composition with respect to a given view. We define a pair of categories of relations for each view $\langle \mathtt{M}, \mathbf{2} \rangle$ and $\langle \mathtt{I}, \mathtt{UI} \rangle$. The category for **2** is just **REL**, the usual category of relations. The category for $\mathtt{UI}$ has *fuzzy relations* as morphisms, but the category for $\mathtt{I}$ recasts fuzzy relations and their composition to render a worst/best case semantics. In Section 3, we propose a notion of *partial probability measure* which generalizes ordinary probability measures in the sense that the latter turn out to be the maximal elements of a dcpo of partial probability measures. One may use such maps to compute the meaning of, say, linear temporal logic formulas for systems such as the one in Figure 1(d).



(a) qualitative, fully specified

(b) qualitative, loosely specified

(c) quantitative, fully specified

(d) quantitative, loosely specified

Fig. 1. Modeling an unreliable medium [19].

2 Categories of relations parametric in views

We refer to [1] as a general reference for domain-theorectic concepts and results; see e.g. [16] for basic notions of meausure theory, and to [27] as a basic reference to category theory. Let us recall the category **REL** of relations. Its objects are all sets $X, Y, Z, \ldots$; the morphisms $\mu \in \mathbf{REL}(X, Y)$ are all subsets of $X \times Y$; the identity morphism for X is $\mathsf{id}_X = \{(x, x') \in X \times X \mid x = x'\}$, and the composition $\mu; \nu$ of $\mu \in \mathbf{REL}(X, Y)$ and $\nu \in \mathbf{REL}(Y, Z)$ is given by $(x, z) \in \mu; \nu$ iff

$$\text{there exists } y \in Y \text{ such that } (x, y) \in \mu \text{ and } (y, z) \in \nu. \tag{1}$$

According to our agenda put forward in the introduction, we think of this category as $\mathbf{REL_2}$, for the morphisms $\mu \subseteq X \times Y$ can be written as functions $\mu\colon X \times Y \to \mathbf{2}$, where $\mathbf{2}$ is the lattice $\{\mathtt{ff} < \mathtt{tt}\}$. We will move freely between these representations throughout this paper. The dcpo $\mathbf{2}$ models a total domain T of a *qualitative view*, $\langle P, T\rangle$, since morphisms in $\mathbf{REL_2}$ specify relations totally (= completely) and in a qualitative manner. To complete the view, we require a domain $\mathtt{M}$ which adequately models relations as partial, but qualitative specifications of morphisms in $\mathbf{REL_2}$. Here we borrow from the work by K. Larsen and B. Thomsen on *modal transition systems* [20], where they consider state-transition relations whose instances may, or must be realized in an implementation. We will then develop a quantitative pair of categories of relations, based on the view $\langle \mathtt{I}, \mathtt{UI}\rangle$, point out its similarities and differences to the framework of fuzzy logic, and study ways of shifting the point of view of

relations such that the underlying categorical structure is sound with respect to such shifts.

Generally, given a view $\langle P, T\rangle$, we seek two categories $\mathbf{REL}_P$ and $\mathbf{REL}_T$, respectively, such that

1. each hom-set $\mathbf{REL}_D(X, Y)$ is a dcpo for $D = P$ or T;
2. $\mathbf{REL}_T$ embeds as a set into the set of maximal elements of $\mathbf{REL}_P$;
3. morphisms in $\mathbf{REL}_T$ model totally specified relations according to the view $\langle P, T\rangle$;
4. morphisms in $\mathbf{REL}_P$ model partially (= incompletely) specified relations according to that view and the notion of approximation in given by the ordering on the hom-sets of $\mathbf{REL}_P$;
5. the composition in these two categories is "sound" with respect to the composition in the category **REL**, provided that we have a means of saying which concrete relations are approximated by morphisms in $\mathbf{REL}_P$.

In defining the category $\mathbf{REL}_{\mathtt{M}}$, we set $\mathtt{M} = \{\mathtt{dk}, \mathtt{ff}, \mathtt{tt}\}$, where this is a dcpo with $\mathtt{dk}$ as least and all other elements as maximal elements. The semantics of $\mu\colon X \times Y \to \mathtt{M}$ is that is approximates concrete relations $R \subseteq X \times Y$ such that

$$(x, y) \in R \begin{cases} \textbf{must} \text{ be true}, & \text{if } \mu(x, y) = \mathtt{tt}; \\ \textbf{may} \text{ be true}, & \text{if } \mu(x, y) = \mathtt{dk}; \text{ and} \\ \text{cannot be true}, & \text{if } \mu(x, y) = \mathtt{ff}. \end{cases} \tag{2}$$

The pointwise ordering on the function space $\mathbf{REL}_{\mathtt{M}}(X, Y)$ precisely captures this notion of approximation in that the maximal elements above μ are exactly those concrete relations which are consistent with the partial specification μ. As in [20], we require modalities $\Box$ and $\Diamond$, for **must** and **may**, respectively, but we need to interpret them, more generally, as unary predicates over domains D. For the qualitative view $\langle \mathtt{M}, \mathbf{2}\rangle$ we set

$$\begin{array}{ll} \Box\mathbf{2} = \{\mathtt{tt}\} & \Diamond\mathbf{2} = \{\mathtt{tt}\} \\ \Box\mathtt{M} = \{\mathtt{tt}\} & \Diamond\mathbf{2} = \{\mathtt{tt}, \mathtt{dk}\}, \end{array}$$

so the modalities agree on $\mathbf{2}$, all possible elements are also guaranteed elements on $\mathbf{2}$ and $\mathtt{M}$, and $\Box$ implies $\Diamond$ on both domains. As for the view $\langle \mathtt{I}, \mathtt{UI}\rangle$, we set

$$\begin{array}{ll} \Box\mathtt{UI} = \{r \in \mathtt{UI} \mid r > 0\} & \Diamond\mathtt{UI} = \{r \in \mathtt{UI} \mid r > 0\} \\ \Box\mathtt{I} = \{[x, y] \in \mathtt{I} \mid x > 0\} & \Diamond\mathtt{I} = \{[x, y] \in \mathtt{I} \mid y > 0\}, \end{array}$$

which enjoys the same properties as mentioned for the view above. Given any view $\langle P, T\rangle$, we require that the interpretation of $\Box$ implies the one of $\Diamond$ on P and T, and that they equal on the set of maximal elements and coincide with the one of T for those maximal elements which correspond to elements of T. These constraints are met for the two views above.

2.1 The qualitative view

The category of modal relations The category $\mathbf{REL}_{\mathtt{M}}$ has as objects all sets and $\mathbf{REL}_{\mathtt{M}}(X,Y)$ equals the dcpo of all functions $\mu\colon X\times Y\to \mathtt{M}$ in the pointwise ordering. To define compositions, we need to interpret (1) over $\mathtt{M}$. For that, it suffices to give interpretation of conjunctions and disjunctions on $\mathtt{M}$. Let $\wedge^{\mathtt{M}}$ be the unique commutative extension of conjunction over $\mathbf{2}$ such that $d\wedge^{\mathtt{M}}\mathtt{ff}=\mathtt{ff}$ and $e\wedge^{\mathtt{M}}\mathtt{dk}=\mathtt{dk}$ if $e\neq\mathtt{ff}$. Extend negation from $\mathbf{2}$ such that $\neg^{\mathtt{M}}\mathtt{dk}=\mathtt{dk}$ and set $d\vee^{\mathtt{M}}e=\neg^{\mathtt{M}}(\neg^{\mathtt{M}}d\wedge^{\mathtt{M}}\neg e)$. We re-interpret (1) as

$$\mu;\nu\,(x,z)=\bigvee_{y\in Y}^{\mathtt{M}}\left(\mu(x,y)\wedge^{\mathtt{M}}\nu(y,z)\right), \tag{3}$$

where $\bigvee^{\mathtt{M}}$ is $\vee^{\mathtt{M}}$ extended to arbitrarily many arguments. Note that this expression computes $\mathtt{tt}$ iff $\Box\mu(x,y)$ and $\Box\nu(y,z)$ hold for some $y\in Y$; otherwise, it computes $\mathtt{dk}$ iff we have $\Diamond\mu(x,y')$ and $\Diamond\nu(y',z)$ for some $y'\in Y$. As identity id_X we set $\mathsf{id}_X(x,x')=\mathtt{tt}$ iff $x=x'$; otherwise, we have to define this as $\mathtt{ff}$ (setting any of this to be $\mathtt{dk}$ will not result in a two-sided identity).

Theorem 1. $\mathbf{REL}_{\mathtt{M}}$ *is a category (of modal relations) such that each hom-set is a dcpo and the maximal elements of* $\mathbf{REL}_{\mathtt{M}}(X,Y)$ *are in a one-to-one correspondence to* $\mathbf{REL}_{\mathbf{2}}(X,Y)$.

Proof. For the identities, given $\mu\in\mathbf{REL}_{\mathtt{M}}(X,Y)$ we use (3) to conlude that $\mu;\mathsf{id}_Y\,(x,y)$ equals $\mu(x,y)$; all terms $\mu(x,y')\wedge^{\mathtt{M}}\mathsf{id}_Y(y',y)$ either yield $\mu(x,y')\wedge^{\mathtt{M}}\mathtt{ff}$ or $\mu(x,y')\wedge^{\mathtt{M}}\mathtt{tt}$ (if $y=y'$), so the overall result is $\mu(x,y)$ in any event. Similarly, one shows that $\mathsf{id}_Y;\nu=\nu$ for any $\nu\in\mathbf{REL}_{\mathtt{M}}(Y,Z)$.

To prove the associativity of composition, consider $\mu\in\mathbf{REL}_{\mathtt{M}}(X,Y)$, $\nu\in\mathbf{REL}_{\mathtt{M}}(Y,Z)$, and $\eta\in\mathbf{REL}_{\mathtt{M}}(Z,W)$. Since morphisms can take on values only in $\mathtt{M}$, it suffices to show that $\mu;(\nu;\eta)\,(x,w)$ computes $\mathtt{tt}/\mathtt{ff}$ iff $(\mu;\nu);\eta\,(x,w)$ computes $\mathtt{tt}/\mathtt{ff}$.

1. If $\mu;(\nu;\eta)\,(x,w)=\mathtt{tt}$, then there exists some $y_0\in Z$ with $\mu(x,y_0)=\mathtt{tt}$ and $\nu;\eta\,(y_0,w)=\mathtt{tt}$. The latter then implies that there exists some $z_0\in Z$ with $\nu(y_0,z_0)=\mathtt{tt}$ and $\eta(z_0,w)=\mathtt{tt}$. If we read this in the reverse order, we get $\mu;\nu\,(x,z_0)=\mathtt{tt}$ and $\eta(z_0,w)=\mathtt{tt}$, so $(\mu;\nu);\eta\,(x,w)=\mathtt{tt}$ follows.
2. The converse of item 1 is argued in a symmetric manner.
3. If $(\mu;\nu);\eta\,(x,w)=\mathtt{ff}$, then $\mu;\nu\,(x,z)=\mathtt{ff}$ or $\eta(z,w)=\mathtt{ff}$ for all $z\in Z$. But this implies: for all $z\in Z$, $\eta(z,w)=\mathtt{ff}$ or (for all $y\in Y$, $\mu(x,y)=\mathtt{ff}$ or $\nu(y,z)=\mathtt{ff}$). This ensures that any way of linking (x,w) in $\mu;(\nu;\eta)\,(x,w)$ only results in $\mathtt{ff}$, so $\mu;(\nu;\eta)\,(x,w)=\mathtt{ff}$.
4. The converse of item 3 is shown in a similar way.

One may wonder about the choice of the interpretations $\wedge^{\mathtt{M}}$ and $\vee^{\mathtt{M}}$ that are instrumental in (3), but they do have universal properties. Let us call a map $T\colon \mathtt{M}\times\mathtt{M}\to\mathtt{M}$ a *t-norm over* $\mathtt{M}$ iff $(\mathtt{M},T,\mathtt{tt})$ is a commutative monoid with

$T(d,e) = \mathtt{ff}$ iff d or e equals $\mathtt{ff}$. We think of T as an interpretation of conjunction. Contrary to the situation in fuzzy logic, where the domain is $\mathtt{UI}$, such t-norms are unique.

Lemma 1. *The function $\wedge^{\mathtt{M}}$ is the unique t-norm over $\mathtt{M}$.*

Proof. Let T be any t-norm over $\mathtt{M}$. Since $\mathtt{tt}$ is an identity for T, we get $T(d,\mathtt{tt}) = d \wedge^{\mathtt{M}} \mathtt{tt}$. By the condition on $T(d,e) = \mathtt{ff}$, we get $T(d,\mathtt{ff}) = \mathtt{ff} = d \wedge^{\mathtt{M}} \mathtt{ff}$. Since T is commutative, the only remaining case is $T(\mathtt{dk},\mathtt{dk})$, but since T is monotone we get $T(\mathtt{dk},\mathtt{dk}) \leq T(\mathtt{tt},\mathtt{dk}) = \mathtt{dk}$, i.e. $T(\mathtt{dk},\mathtt{dk}) = \mathtt{dk} = \mathtt{dk} \wedge^{\mathtt{M}} \mathtt{dk}$.

Soundness of approximation With Theorem 1 in place, it remains to show that $\mathbf{REL}_{\mathtt{M}}$ is "sound" with respect to the categorical structure of $\mathbf{REL_2}$. To that end, we make use of the interpretation of the modalities on $\mathtt{M}$ to define two functors $F_\Box$ and $F_\Diamond$ from $\mathbf{REL}_{\mathtt{M}}$ to $\mathbf{REL_2}$. Intuitively, $F_\Box$ acts on morphisms by providing the *largest* concrete relation $R_{\max}$ that is consistent with respect to μ; dually, $F_\Diamond$ renders the smallest such consistent relation $R_{\min}$. Together, they specify the complete range of possible concrete relations that are approximated by μ: all relations R with $R_{\min} \subseteq R \subseteq R_{\max}$.

Definition 1. *We define $F_\Box, F_\Diamond \colon \mathbf{REL}_{\mathtt{M}} \to \mathbf{REL_2}$ on objects as $F_\Box(X) = F_\Diamond(X) = X$. For morphisms $\mu \in \mathbf{REL}_{\mathtt{M}}(X,Y)$, we set*

$$F_\Box(X) = \{(x,y) \in X \times Y \mid \Box\mu(x,y)\} \tag{4}$$
$$F_\Diamond(X) = \{(x,y) \in X \times Y \mid \Diamond\mu(x,y)\}. \tag{5}$$

The soundness of the categorical structure on $\mathbf{REL}_{\mathtt{M}}$ with respect to the one on $\mathbf{REL_2}$ now follows from the fact that $F_\Box$ and $F_\Diamond$ are monotone functors.

Proposition 1. *The functions $F_\Box$ and $F_\Diamond$ defined above are monotone functors.*

Proof. From the definition of id_X in $\mathbf{REL}_{\mathtt{M}}$ and the interpretation of the modalities on $\mathtt{M}$, it immediately follows that $F_\Box$ and $F_\Diamond$ preserve identities. Given $\mu \in \mathbf{REL}_{\mathtt{M}}(X,Y)$ and $\nu \in \mathbf{REL}_{\mathtt{M}}(Y,Z)$, the set $F_\Box(\mu;\nu)$ equals $\{(x,z) \in X \times Z \mid \Box\,(\mu;\nu\,(x,z))\}$. But

$$\begin{aligned}\Box\,(\mu;\nu\,(x,z)) &= \bigvee\nolimits^{\mathbf{2}}\{\Box\left(\mu(x,y) \wedge^{\mathtt{M}} \nu(y,z)\right) \mid y \in Y,\ \Diamond\mu(x,y), \Diamond\nu(y,z)\} \qquad (6)\\ &= \bigvee\nolimits^{\mathbf{2}}\{(\Box\mu(x,y)) \wedge^{\mathbf{2}} (\Box\nu(y,z)) \mid y \in Y,\ \Diamond\mu(x,y), \Diamond\nu(y,z)\}.\end{aligned}$$

Inspecting (1), we gather that $(x,z) \in F_\Box(\mu;\nu)$ iff $(x,z) \in F_\Box(\mu);F_\Box(\nu)$, so $F_\Box$ is a functor. Since $\Box\mathtt{M} = \{\mathtt{tt}\}$ is an upper set in $\mathtt{M}$, it follows that $F_\Box$ is monotone: $\mu \leq \mu'$ in $\mathbf{REL}_{\mathtt{M}}(X,Y)$ implies $F_\Box(\mu) \leq F_\Box(\mu')$ in $\mathbf{REL_2}(X,Y)$.

Similarly, $F_\Diamond$ is monotone as $\Diamond\mathtt{M} = \{\mathtt{tt},\mathtt{dk}\}$ is an upper set in $\mathtt{M}$. Since $\Diamond$ distributes over $\bigvee^{\mathtt{M}}$ and since $\Diamond(d \wedge^{\mathtt{M}} e)$ iff $\Diamond d$ and $\Diamond e$ hold, one readily sees that $F_\Diamond(\mu;\nu)$ equals $F_\Diamond(\mu);F_\Diamond(\nu)$.

Remark 1. Since $\bigvee^{\mathtt{M}}$ and $\wedge^{\mathtt{M}}$ agree with $\bigvee^{\mathbf{2}}$ and $\wedge^{\mathbf{2}}$ on $\{\mathtt{ff}, \mathtt{tt}\}$, the image of the function $i\colon x \mapsto x\colon \mathbf{2} \to \mathtt{M}$, we obtain a functor $G\colon \mathbf{REL_2} \to \mathbf{REL}_{\mathtt{M}}$ which leaves objects X fixed ($G(X) = X$) and send any $\mu \in \mathbf{REL_2}(X, Y)$ to $i \circ \mu \in \mathbf{REL}_{\mathtt{M}}(X, Y)$.

2.2 The quantitative view

We now present the two categories of relations based on the view $\langle \mathtt{I}, \mathtt{UI} \rangle$.

Fuzzy logic In fuzzy logic, fuzzy sets of type X, where X is an ordinary set, are functions $\mu\colon X \to \mathtt{UI}$. Similarly, fuzzy relations are functions $\mu\colon X \times Y \to \mathtt{UI}$ and compositions are either "sup-min" or "sup-T" versions of (1), where T is a t-norm (over $\mathtt{UI}$).

Definition 2. *A* linear *t*-norm *over* $\mathtt{UI}$ *is a function* $T\colon \mathtt{UI} \times \mathtt{UI} \to \mathtt{UI}$ *which preserves all least upper bounds and greatest lower bounds in each coordinate separately, satisfies* $T(a, b) = 0$ *iff* $a = 0$ *or* $b = 0$*, and makes* $(\mathtt{UI}, T, 1)$ *into a commutative monoid.*

An example of a linear t-norm is $(a, b) \mapsto \min(a, b)$. Not every t-norm from fuzzy logic is a linear t-norm. For example, the t-norm $\mathtt{LAND}(a, b) = \max(a + b - 1, 0)$ is not linear: take a and b to be 0.5, then $\mathtt{LAND}(a, b) = 0$. The categories $\mathbf{REL}_{\mathtt{UI}}$ and $\mathbf{REL}_{\mathtt{I}}$ implicitly depend on a linear t-norm, T, used in defining composition. In $\mathbf{REL}_{\mathtt{UI}}$, objects are all sets, the identity id_X maps (x, x') to 1 iff $x = x'$; otherwise, it renders 0. Given $\mu \in \mathbf{REL}_{\mathtt{UI}}(X, Y)$ and $\nu \in \mathbf{REL}_{\mathtt{I}}(Y, Z)$, we define $\mu; \nu$ as the sup-T composition of fuzzy logic:

$$\mu; \nu\,(x, z) = \bigvee^{\mathtt{UI}} \{T(\mu(x, y), \nu(y, z)) \mid y \in Y\}. \tag{7}$$

Observe that we did not require the modalities in the qualification of this set as 0 does not contribute to the least upper bound of the right hand side. This will change when we consider $\mathbf{REL}_{\mathtt{I}}$.

Theorem 2. $\mathbf{REL}_{\mathtt{UI}}$ *is a category (of fuzzy relations) such that each hom-set is a dcpo (even a complete lattice).*

Proof. This will follow directly from the corresponding result for $\mathbf{REL}_{\mathtt{I}}$, since $\mu \mapsto \mu_2\colon \mathbf{REL}_{\mathtt{I}}(X, Y) \to \mathbf{REL}_{\mathtt{UI}}(X, Y)$ will map the categorical structure of $\mathbf{REL}_{\mathtt{I}}$ onto the one in $\mathbf{REL}_{\mathtt{UI}}$.

The category of interval-valued relations If fuzzy sets are totally specified, then a partial version has to approximate the degree of belief, uncertainty, or vagueness expressed in $\mu(x, y) \in \mathtt{UI}$. This naturally leads to considering the interval domain $\mathtt{I}$ as a base domain for the corresponding category. Thus, objects in $\mathbf{REL}_{\mathtt{I}}$ are all sets, the identities id_X map (x, x') to $[1, 1]$ iff $x = x'$; otherwise, it

returns $[0,0]$. The dcpo $\mathbf{REL}_{\mathtt{I}}(X,Y)$ is given by all functions of type $\mu\colon X\times Y\to \mathtt{I}$, ordered pointwise. The choice of composition is driven by the fact that we identify $[1,1]$ with $\mathtt{tt}$ and $[0,0]$ with $\mathtt{ff}$, respectively, and that this identification should give rise to two functors from $\mathbf{REL}_{\mathtt{I}}$ to $\mathbf{REL_2}$ which factor through the functors $F_\Box$ and $F_\Diamond$ from $\mathbf{REL}_{\mathtt{M}}$ to $\mathbf{REL_2}$, respectively. For $\mu\in\mathbf{REL}_{\mathtt{I}}(X,Y)$ and $\nu\in\mathbf{REL}_{\mathtt{I}}(Y,Z)$ set $\mu;\nu\,(x,z)=[a,b]$. We interpret a/b as the minimal/maximal degree of belief in (x,z) to "be" in $\mu;\nu$; this degree could also be about some other mode such as *evidence*, *uncertainty*, etc. The interpretation of modalities on $\mathtt{I}$ is needed to define the semantics of composition with respect to the interpretation above. In the sequel, we often write μ_i for $\mathrm{pr}_i\circ\mu$, where $\mathrm{pr}_1[x,y]=x$ and $\mathrm{pr}_2[x,y]=y$ $(i=1,2)$. The value of a ought to be a minimal and conservative estimate of the degree of membership (if we think of fuzzy sets as the total elements):

$$\mathrm{pr}_1(\mu;\nu\,(x,z))=\bigwedge^{\mathtt{UI}}\{T(\mu_1(x,y),\nu_1(y,z))\mid y\in Y,\ \Box\mu(x,y),\ \Box\nu(y,z)\},\qquad(8)$$

if the set in (8) is non-empty. Otherwise, there is no guaranteed link between x and z and we decree $\mathrm{pr}_1(\mu;\nu\,(x,z))$ to be 0. Dually, we obtain a maximal and conservative degree of membership by changing $\Box$ to $\Diamond$ and $\bigwedge$ to $\bigvee$ in (8):

$$\mathrm{pr}_2((\mu;\nu)\,(x,z))=\bigvee^{\mathtt{UI}}\{T(\mu_2(x,y),\nu_2(y,z))\mid y\in Y,\ \Diamond\mu(x,y),\ \Diamond\nu(y,z)\}.\qquad(9)$$

Theorem 3. $\mathbf{REL}_{\mathtt{I}}$ *is a category (of interval-valued relations) such that each hom-set is a dcpo and the maximal elements of* $\mathbf{REL}_{\mathtt{I}}(X,Y)$ *are in a one-to-one correspondence to* $\mathbf{REL}_{\mathtt{UI}}(X,Y)$.

Proof. 1. For identities, consider $\mu\in\mathbf{REL}_{\mathtt{I}}(X,Y)$.

(a) $\mathrm{pr}_1(\mu;\mathsf{id}_Y\,(x,y))=0$ iff $\neg\Box\mu(x,y')$ or $\neg\Box\mathsf{id}_Y(y',y)$ for all $y'\in Y$ iff $\neg\Box\mu(x,y)$ (as $y'=y$ iff $\Box\mathsf{id}_Y(y',y)$) iff $\mathrm{pr}_1\mu(x,y)=0$;

(b) if $\mathrm{pr}_1\mu;\mathsf{id}_Y(x,y)>0$, then it suffices to show that $\mathrm{pr}_1(\mu;\mathsf{id}_Y(x,y))=\mu_1(x,y)$ by the previous item. Since $\mathsf{id}_Y(y,y)=[1,1]$ and $\neg\Box\mathsf{id}_Y(y',y)$ for all $y'\neq y$, we infer that $\mathrm{pr}_1\mu;\mathsf{id}_Y(x,y)=\bigvee^{\mathtt{UI}}\{T(\mu_1(x,y'),\mathrm{pr}_1(\mathsf{id}_Y(y',y)))\mid y'\in Y,\ \Box\mu(x,y),\ \Box\mathsf{id}_Y(y',y)\}$ equals $T(\mu_1(x,y),1)=\mu_1(x,y)$ as desired;

(c) finally, $\mathrm{pr}_2(\mu;\mathsf{id}_Y(x,y))$ equals

$$\bigwedge^{\mathtt{UI}}\{T(\mu_2(x,y'),\mathrm{pr}_2(\mathsf{id}_Y(y',y)))\mid y'\in Y,\ \Diamond\mu(x,y'),\ \Diamond\mathsf{id}_Y(y',y)\},$$

and since $\Diamond\mathsf{id}_Y(y',y)$ iff $y'=y$, the latter equals $T(\mu_2(x,y),1)=\mu_2(x,y)$.

Similarly, one shows $\mathsf{id}_Y;\nu=\nu$ for all $\nu\in\mathbf{REL}_{\mathtt{I}}(Y,Z)$.

2. For composition, consider $\mu\in\mathbf{REL}_{\mathtt{I}}(X,Y)$, $\nu\in\mathbf{REL}_{\mathtt{I}}(Y,Z)$, and $\eta\in\mathbf{REL}_{\mathtt{I}}(Z,W)$.

(a) We have

$$\begin{aligned}
&\mathrm{pr}_1(\mu;(\nu;\eta)\,(x,w)) = 0 \qquad (10)\\
&\text{iff}\quad \neg\Box\mu(x,y) \text{ or } \neg\Box(\nu;\eta\,(y,w)) \text{ for all } y\in Y\\
&\text{iff}\quad \text{for all } y\in Y,\ \neg\Box\mu(x,y) \text{ or (for all } z\in Z,\ \neg\Box\nu(y,z) \text{ or } \neg\Box\eta(z,w))\\
&\text{iff}\quad \text{for all } z\in Z,\ \neg\Box\eta(z,w) \text{ or (for all } y\in Y,\ \neg\Box\mu(x,y) \text{ or } \neg\Box\nu(y,z))\\
&\text{iff}\quad \mathrm{pr}_1((\mu;\nu);\eta\,(x,w)) = 0.
\end{aligned}$$

(b) Let $a = \mathrm{pr}_1(\mu;(\nu;\eta)\,(x,w)) > 0$. By the previous item, we infer that $a' = \mathrm{pr}_1((\mu;\nu);\eta\,(x,w))$ has to be greater than 0, so both expressions are defined as in (8). Thus,

$$\begin{aligned}
a &= \bigwedge\nolimits^{\mathrm{UI}}\{T(\mu_1(x,y),\mathrm{pr}_1(\nu;\eta\,(y,w))) \mid \Box\mu(x,y),\ \Box(\nu;\eta\,(y,w))\} \qquad (11)\\
&= \bigwedge_{\Box\mu(x,y),\Box(\nu;\eta\,(y,w))}^{\mathrm{UI}} T(\mu_1(x,y),\bigwedge\nolimits^{\mathrm{UI}}\{T(\nu_1(y,z),\eta_1(z,w)) \mid \Box\nu(y,z),\ \Box\eta(z,w)\})\\
&= \bigwedge_{\Box\mu(x,y),\Box(\nu;\eta\,(y,w))}^{\mathrm{UI}} \bigwedge_{\Box\nu(y,z),\ \Box\eta(z,w)\}}^{\mathrm{UI}} T(\mu_1(x,y),T(\nu_1(y,z),\eta_1(z,w)))\\
&= \bigwedge_{\Box\mu(x,y),\Box(\nu;\eta\,(y,w))}^{\mathrm{UI}} \bigwedge_{\Box\nu(y,z),\ \Box\eta(z,w)\}}^{\mathrm{UI}} T(T(\mu_1(x,y),\nu_1(y,z)),\eta_1(z,w))) \qquad (12)
\end{aligned}$$

using that T is linear, associative and that all $\Box$ terms are defined as in (8). In a completely similar fashion, without having to regroup the T-expressions, we compute

$$a' = \bigwedge_{\Box(\mu;\nu\,(x,z)),\Box\eta(z,w)}^{\mathrm{UI}} \bigwedge_{\Box\mu(x,y),\ \Box\nu(y,z)\}}^{\mathrm{UI}} T(T(\mu_1(x,y),\nu_1(y,z)),\eta_1(z,w))). \qquad (13)$$

Since all these infima are non-empty, the "quantifiers" $\Box(\mu;\nu\,(x,z))$ and $\Box(\nu;\eta\,(y,w))$ are redundant in the presence of the remaining respective quantifiers in (12) and (13).

(c) Let $b = \mathrm{pr}_2(\mu;(\nu;\eta)\,(x,w))$ and $b' = \mathrm{pr}_2((\mu;\nu);\eta)\,(x,w))$. Again, using the linearity and associativity of T, we obtain

$$\begin{aligned}
b &= \bigvee_{\Diamond\mu(x,y),\Diamond(\nu;\eta\,(y,w))}^{\mathrm{UI}} \bigvee_{\Diamond\nu(y,z),\ \Diamond\eta(z,w)\}}^{\mathrm{UI}} T(T(\mu_1(x,y),\nu_1(y,z)),\eta_1(z,w)))\\
b' &= \bigvee_{\Diamond(\mu;\nu\,(x,z)),\Diamond\eta(z,w)}^{\mathrm{UI}} \bigwedge_{\Diamond\mu(x,y),\ \Diamond\nu(y,z)\}}^{\mathrm{UI}} T(T(\mu_1(x,y),\nu_1(y,z)),\eta_1(z,w))).
\end{aligned}$$

One readily sees that these least upper bounds range over the same set, so they are equal.

The proof of Theorem 3 made crucial use of that fact the the norm T is linear. Let us stress that the identities of $\mathbf{REL}_{\mathtt{I}}$ are the ones of $\mathbf{REL}_{\mathtt{UI}}$ if we identify morphisms of $\mathbf{REL}_{\mathtt{UI}}$ with total elements in $\mathbf{REL}_{\mathtt{I}}$, but that this does not extend to the composition in these categories! Since fuzzy relations can be seen as morphisms in $\mathbf{REL}_{\mathtt{I}}$, we may compose them according to (8) and (9). This, contrary to the composition in (7), seems to be a more informative semantics as it combines the worst and best case scenario of what the real set may be like. Furthermore, the insertion of $\Box$ and $\Diamond$ in the qualifications of (8) and (9) was necessary, unlike in the case of (3).

Soundness of approximation Let D be any domain with appropriate interpretations of the modalities and let $\mathbf{REL}_D$ be a category of D-valued relations. For $\mu \in \mathbf{REL}_D(X,Y)$, we may define an interval of sets $[\Box\mu, \Diamond\mu]$ by $\Box\mu = \{(x,y) \in X \times Y \mid \Box\mu(x,y)\}$ and $\Diamond\mu = \{(x,y) \in X \times Y \mid \Diamond\mu(x,y)\}$. Cearly $\Box\mu \subseteq \Diamond\mu$. If we set $\mathtt{I}_D(X,Y)$ to be the dcpo of all those pairs $[S,T]$ with $S \subseteq T \subseteq X \times Y$ and order such pairs as in $\mathtt{I}$, then $\mu \leq \nu$ in $\mathbf{REL}_D(X,Y)$ should imply $[\Box\mu, \Diamond\mu] \leq [\Box\nu, \Diamond\nu]$. This suggests that the construction of $\mathtt{I}$ is more fundamental and should apply to domains other than $\mathtt{UI}$ as well. Returning to $\mathtt{I}$ itself, we mean to define a monotone functor $H\colon \mathbf{REL}_{\mathtt{I}} \to \mathbf{REL}_{\mathtt{M}}$; its composition with the functors $F_\Box$ and $F_\Diamond$, respectively, then gives us two monotone functors from $\mathbf{REL}_{\mathtt{I}}$ to $\mathbf{REL}_{\mathbf{2}}$.

Definition 3. *We define* $H\colon \mathbf{REL}_{\mathtt{I}} \to \mathbf{REL}_{\mathtt{M}}$ *on objects by* $H(X) = X$. *On morphisms* $\mu \in \mathbf{REL}_{\mathtt{I}}(X,Y)$, *we set* $H(\mu)\,(x,y)$ *to be* $\mathtt{tt}$ *iff* $\Box\mu(x,y)$; $\mathtt{ff}$ *iff* $\neg\Diamond\mu(x,y)$; *and* $\mathtt{dk}$ *in the remaining case* $(\Diamond\mu(x,y) \wedge \neg\Box\mu(x,y))$.

Proposition 2. *The function* $H\colon \mathbf{REL}_{\mathtt{I}} \to \mathbf{REL}_{\mathtt{M}}$ *defined above is a monotone functor.*

Proof. 1. For identities, $H(\mathsf{id}_X)\,(x,x')$ equals $\mathtt{tt}$ iff $\Box\mathsf{id}_X(x,x')$ iff $x = x'$; it equals $\mathtt{ff}$ iff $\neg\Diamond\mathsf{id}_X(x,x')$ iff $x \neq x'$; and it cannot take on the value $\mathtt{dk}$ since $\mathsf{id}_X(x,x')$ cannot satisfy "$\neg\Box \wedge \Diamond$". Thus, $H(\mathsf{id}_X)$ equals id_X in $\mathbf{REL}_{\mathtt{M}}$.

2. For composition, let $\mu \in \mathbf{REL}_{\mathtt{I}}(X,Y)$ and $\nu \in \mathbf{REL}_{\mathtt{I}}(Y,Z)$.

   (a) Let $H(\mu;\nu)\,(x,z) = \mathtt{ff}$. Then $\neg\Diamond(\mu;\nu\,(x,z))$ implies that $\mathrm{pr}_2((\mu;\nu)\,(x,z))$, which is $\bigvee^{\mathtt{UI}}\{T(\mu_2(x,y),\nu_2(y,z)) \mid y \in Y,\ \Diamond\mu(x,y),\ \Diamond\nu(y,z)\}$, equals 0. But then all the T expressions must be 0, so $\neg\Diamond\mu(x,y)$ or $\neg\Diamond\nu(y,z)$ holds for all $y \in Y$. But then $H(\mu)\,(x,y) = \mathtt{ff}$ and $H(\nu)\,(y,z) = \mathtt{ff}$ for all $y \in Y$, which implies $H(\mu);H(\nu)\,(x,z) = \mathtt{ff}$.

   (b) Let $H(\mu;\nu)\,(x,z) = \mathtt{tt}$. Then $\Box(\mu;\nu\,(x,z))$ implies that $\mathrm{pr}_1((\mu;\nu)\,(x,z))$ is greater than 0. Therefore, $\mathrm{pr}_1((\mu;\nu)\,(x,z))$ equals

$$\bigwedge^{\mathtt{UI}}\{T(\mu_1(x,y),\nu_1(y,z)) \mid y \in Y,\ \Box\mu(x,y),\ \Box\nu(y,z)\}.$$

Since this expression is greater than 0 we must have some $y_0 \in Y$ such that $\Box\mu(x, y_0)$ *and* $\Box\nu(y_0, z)$. But then $H(\mu); H(\nu)\,(x, z) = \mathtt{tt}$ since $H(\mu)\,(x, y_0) \wedge^{\mathtt{M}} H(\nu)\,(y_o, z) = \mathtt{tt}$.

(c) Finally, if $H(\mu; \nu)\,(x, z) = \mathtt{dk}$, then we infer $\neg\Box(\mu; \nu\,(x, z))$ as well as $\Diamond(\mu; \nu\,(x, z))$. The first gives us $\neg\Box\mu(x, y)$ or $\neg\Box\nu(y, z)$ for all $y \in Y$; the second implies the existence of some $y_1 \in Y$ with $\Diamond\mu(x, y_1)$ and $\Diamond\nu(y_1, z)$. The first fact ensures that no term $H(\mu)\,(x, y) \wedge^{\mathtt{M}} H(\nu)\,(y, z)$ equals $\mathtt{tt}$; the second fact implies that at least one of these terms is different from $\mathtt{ff}$. Combining this, we infer that $H(\mu); H(\nu)\,(x, w)$, the disjunction in $\mathtt{M}$ of all such terms, has to be $\mathtt{dk}$.

3. For monotonicity, let $\mu \leq \nu \in \mathbf{REL}_{\mathtt{I}}(X, Y)$. If $H(\mu)\,(x, y) = \mathtt{tt}$, then $\Box\mu(x, y)$ holds, so $\Box\nu(x, y)$ follows since $\Box\mathtt{I}$ is an upper set in $\mathtt{I}$; but then $H(\nu)\,(x, y) = \mathtt{tt}$ follows. If $H(\mu)\,(x, y) = \mathtt{ff}$, then $\neg\Diamond\mu(x, y)$ holds, so $\mu(x, y) = [0, 0]$, so $\neg\Diamond\mathtt{I} = \{[0, 0]\}$ is an upper set in $\mathtt{I}$; but then $\neg\Diamond\nu(x, y)$ renders $H(\nu)\,(x, y) = \mathtt{ff}$. If $H(\mu)\,(x, y) = \mathtt{dk}$, then $H(\mu)\,(x, y) \leq H(\nu)\,(x, y)$ is clear as $\mathtt{dk}$ is the least element of $\mathtt{M}$.

Corollary 1. *We have monotone functors*

$$\begin{aligned} H; F_{\Box} &: \mathbf{REL}_{\mathtt{I}} \to \mathbf{REL}_{\mathbf{2}} \\ H; F_{\Diamond} &: \mathbf{REL}_{\mathtt{I}} \to \mathbf{REL}_{\mathbf{2}}. \end{aligned} \tag{14}$$

Remark 2. Let $j\colon \mathtt{M} \to \mathtt{I}$ be the map which sends $\mathtt{dk}$ to $[0, 1]$, $\mathtt{ff}$ to $[0, 0]$, and $\mathtt{tt}$ to $[1, 1]$. If we define $L\colon \mathbf{REL}_{\mathtt{M}} \to \mathbf{REL}_{\mathtt{I}}$ by $L(X) = X$ and $L(\mu) = j \circ \mu$ for all sets X and Y and any $\mu \in \mathbf{REL}_{\mathtt{M}}(X, Y)$, then L is a functor, since the composition in (8) and (9) faithfully matches the one in (3) on the image of the function j.

3 Partial probability measures

We already encountered the view $\langle \mathtt{I}, \mathtt{UI} \rangle$ when we studied the categories of $\mathtt{I}$ and $\mathtt{UI}$-valued relations, respectively, in Section 2. In this section, we demonstrate that this view can be successfully extended to probability theory. For that, we develop a notion of *partial probability measure*, based on $\mathtt{I}$, which is sound for the conventional probability theory, based on $\mathtt{UI}$. We first study a set of inequalities as axioms for a partial version of probability measures. Then we turn these axioms into equalities and speculate on what justifications one could give for either one, or some other choice of axioms.

3.1 Inequational Axioms

Definition 4. *A* sigma-algebra *over a set X is a set, $\Sigma(X)$, of subsets of X which contains X, and is closed under set complementation and countable unions. We write $\Sigma(X) \to D$ for the set of functions $\mu\colon \Sigma(X) \to D$ and we define $\mu \leq \nu$ to mean $\mu(A) \leq \nu(A)$ in D, for all $A \in \Sigma(X)$.*

Remark 3. For any dcpo D and sigma-algebra $\Sigma(X)$, the pair $(\Sigma(X) \to D, \leq)$ is a dcpo.

We will focus on the cases where D equals the unit interval or the interval domain.

Definition 5. *Let* $\mathtt{I}$, *the* interval domain *[25, 30], be the partial ordering of all closed intervals* $[x, y]$ *with* $0 \leq x \leq y \leq 1$, *ordered under reverse containment:* $[u, v] \leq [x, y]$ *iff* $u \leq x$ *and* $y \leq v$. *Let* $\mathtt{UI}$, *the* unit interval, *be the partial ordering of all numbers* r *with* $0 \leq r \leq 1$, *ordered in the usual way.*

Remark 4. The partial orderings $\mathtt{UI}$ and $\mathtt{I}$ are dcpos. In $\mathtt{UI}$ and in its order dual, least upper bounds of directed sets are limits in the Euclidean topology. In $\mathtt{I}$, the least upper bound of a family $([x_i, y_i])_{i \in I}$ equals $[\bigvee^{\uparrow} x_i, \bigwedge^{\downarrow} y_i]$.

The dcpo $\Sigma(X) \to \mathtt{UI}$ contains all *probability measures*, maps which satisfy the *axioms of probability*, due to A. N. Kolmogorov:

P1. $\mu(X) = 1$,
P2. **(modular law)** $\mu(A \cup B) + \mu(A \cap B) = \mu(A) + \mu(B)$ for all $A, B \in \Sigma(X)$, and
P3. $\mu(\bigcup A_i) = \sum \mu(A_i)$ for all pairwise disjoint families of sets $(A_i)_{i \in I}$ in $\Sigma(X)$.

If μ only meets axioms P2 and P3, we call μ a *sub-probability measure.* The ordering on the ambient space $\Sigma(X) \to \mathtt{UI}$, however, is not suitable for approximating such measures.

Definition 6. *For any sigma-algebra* $\Sigma(X)$, *we denote by* $\mathtt{P}(\Sigma(X))$ *the partial ordering of all* $\mu \colon \Sigma(X) \to \mathtt{UI}$ *which satisfy axioms P1, P2, and P3, the ordering being inherited from* $\Sigma(X) \to \mathtt{UI}$.

Lemma 2. *Let* $\Sigma(X)$ *be any sigma-algebra. Then the ordering on* $\mathtt{P}(\Sigma(X))$ *is equality.*

Proof. Let $\mu \leq \nu$ in $\mathtt{P}(\Sigma(X))$ and assume that $\mu \neq \nu$. Then there has to exist some $A \in \Sigma(X)$ such that $\mu(A) < \nu(A)$. Since $X \setminus A \in \Sigma(X)$ and since μ and ν satisfy equation (17), we get $\nu(X \setminus A) = \nu(X) - \nu(A) < \nu(X) - \mu(A) = \mu(X \setminus A)$, contradicting $\mu \leq \nu$.

We would like to realize (sub)probability measures as maximal elements in a dcpo which is not an ad hoc construction, but whose elements can be seen as *partial* probability measures. This suggests to choose $\Sigma(X) \to \mathtt{I}$ as the ambient space, but it is less clear what axioms one should endorse to single out the proper notions of "partiality". Intuitively, a partial probability measure is a map of type $\mu \colon \Sigma(X) \to \mathtt{I}$ such that $\mu(A)$ is a *safe approximation* of the "probability" of A, for all (total) probability measures that refine μ. Since sigma-algebras abstract computational state, refinement is adequately modeled by the ordering in $\Sigma(X) \to \mathtt{I}$. Note that this allows us to compute such evidence in the presence of *uncertainty or vagueness*, or if the underlying computational models are,

e.g. not Markov decision processes [11], but system descriptions with inherent vagueness, or uncertainty such as the probabilistic specifications in [19].

In crafting axioms for a dcpo $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$ of partial probability measures, we need to ensure that

1. we view total elements as maximal ones in the dcpo $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$;
2. that the maximal elements in $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$ have a one-to-one correspondence to elements in $\mathtt{P}(\Sigma(X))$; and
3. that we achieve the latter by choosing axioms which, if interpreted for maximal elements, "recover" the well known axioms of probability, P1 to P3.

These requirements alone are far from determining such axioms. Essentially such conditions on $\mu\colon \Sigma(X) \to \mathtt{I}$ should demand consistency with respect to the conventional probability axioms applied to any probability measure that refines μ. We write $\mathrm{pr}_1, \mathrm{pr}_2\colon \mathtt{I} \to \mathtt{UI}$ to denote the projections $\mathrm{pr}_1[x,y] = x$ and $\mathrm{pr}_2[x,y] = y$ and we abbreviate $\mathrm{pr}_i \circ \mu$ by μ_i in the sequel $(i = 1, 2)$. So $\mu\colon \Sigma(X) \to \mathtt{I}$ may be written as a pairing $\langle \mu_1, \mu_2 \rangle$ of maps $\mu_1, \mu_2\colon \Sigma(X) \to \mathtt{UI}$ with $\mu_1 \leq \mu_2$.

As inequational consistency conditions corresponding to P1, P2, and P3, respectively, we propose:

Ie1(a). $\mu(X) \leq [1,1]$,
Ie1(b). $\mu(X) \geq [1,1]$,
Ie2(a). $\mu_1(A \cup B) + \mu_2(A \cap B) \geq \mu_1(A) + \mu_1(B)$,
Ie2(b). $\mu_2(A \cup B) + \mu_1(A \cap B) \leq \mu_2(A) + \mu_2(B)$,
Ie3(a). $\mu_1(\bigcup_{i \in I} A_i) \geq \mu_1(\bigcup_{j \in J} A_j) - \sum_{k \in J \setminus I} \mu_2(A_k)$ for all pairwise disjoint families $(A_j)_{j \in J}$ in $\Sigma(X)$, and all $I \subseteq J$,
Ie3(b). $\mu_2(\bigcup_{i \in I} A_i) \leq \mu_2(\bigcup_{j \in J} A_j) - \sum_{k \in J \setminus I} \mu_1(A_k)$ for all pairwise disjoint families $(A_j)_{j \in J}$ in $\Sigma(X)$, and all $I \subseteq J$.

Notice the duality in the pair $\langle \mu_1, \mu_2 \rangle$ and $\langle \geq, \leq \rangle$ in all axioms of type (a) and (b), respectively. Axioms Ie1(a) and Ie1(b) say that the probability of X is 1 regardless of the inherent uncertainty or vagueness of the situation. To justify, say, the inequality in Ie2(a), we may rewrite it as $\mu_1(A \cup B) \geq \mu_1(A) + \mu_1(B) - \mu_2(A \cap B)$ which should hold since the right-hand side is a conservative lower bound for the "total probability" of $A \cup B$ given the interpretation of μ_1 and μ_2 as providing lower and upper bounds of "total probabilities", respectively; so $\mu_1(A \cup B)$ cannot be strictly smaller than that. The inequality in Ie2(b) has a dual justification. Notice how the combination of these two inequalities recovers the original modular law above in case that the measure satisfies $\Delta(\mu, A) = 0$ for all $A \in \Sigma(X)$, where

$$\Delta(\mu, A) = \mu_2(A) - \mu_1(A).$$

To justify, say, Ie3(b), the right hand side is a conservative approximation of the left hand side for similar reasons as stated above, no matter what subset I

we pick. Axiom Ie3 has two special instances of interest. First, if we take the pairwise disjoint family of sets $\{A, X \setminus A\}$ and apply Ie3 to it with $I = \{A\}$, we obtain

$$\mu_1(A) \geq \mu_1(X) - \mu_2(X \setminus A) \tag{15}$$
$$\mu_2(A) \leq \mu_2(X) - \mu_1(X \setminus A). \tag{16}$$

Note that

$$\mu'(X \setminus A) = \mu'(X) - \mu'(A) \tag{17}$$

holds for all sub-probability measures μ' and that equation (17) follows from (15) and (16) if $\mu_1 = \mu_2$. In general, neither μ_1 nor μ_2 are conventional probability measures, unless μ is a maximal (= total) element in the space $\Sigma(X) \to \mathtt{I}$. Second, if $I = \{i_0\}$ for a pairwise disjoint family $(A_j)_{j \in J}$ in $\Sigma(X)$ and $i_0 \in J$, then Ie3 means

$$\mu_1(A_{i_0}) \geq \mu_1(\bigcup_{j \in J} A_j) - \sum_{i_0 \neq k \in J} \mu_2(A_k) \tag{18}$$
$$\mu_2(A_{i_0}) \leq \mu_2(\bigcup_{j \in J} A_j) - \sum_{i_0 \neq k \in J} \mu_1(A_k). \tag{19}$$

This will allow us to recover axiom P3 in case that $\mu_1 = \mu_2$.

Definition 7. *Let $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$ be the partial ordering of all maps $\mu\colon \Sigma(X) \to \mathtt{I}$ which satisfy the axioms Ie1, Ie2, and Ie3 above, the ordering being inherited from $\Sigma(X) \to \mathtt{I}$.*

We establish that $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$ is a dcpo and that $\mathtt{P}(\Sigma(X))$ has a natural embedding into the set of maximal elements of $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$.

Proposition 3. *The partial ordering $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$ is a dcpo and its least upper bounds of directed sets are the ones formed in $\Sigma(X) \to \mathtt{I}$.*

Proof. Let $(\mu^j)_{j \in J}$ be a directed set in $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$. Since $\mu\colon A \mapsto \bigvee^{\uparrow} \mu^j(A)$ is the least upper bound of that set in $\Sigma(X) \to \mathtt{I}$, it suffices to show that this map satisfies the axioms Ie1 to Ie3.

Ie1. If $\mu^j(X) = [1,1]$ for all $i \in J$, then $\mu(X) = [1,1]$ is clear.

Ie2(a). Assume that $\mu_1(A \cup B) + \mu_2(A \cap B) < \mu_1(A) + \mu_1(B)$ and note that the latter equals $\bigvee^{\uparrow}(\mu_1^j(A) + \mu_1^j(B))$ since $+$ preserves least upper bounds of directed sets. Since the left hand side is strictly smaller than $\bigvee^{\uparrow}(\mu_1^j(A) + \mu_1^j(B))$, there exists some $j_0 \in J$ such that $\mu_1(A \cup B) + \mu_2(A \cap B) < \mu_1^{j_0}(A) + \mu_1^{j_0}(B)$. But the left hand side equals $\bigvee^{\uparrow}_j \mu_1^j(A \cup B) + \bigwedge^{\downarrow}_{j'} \mu_2^{j'}(A \cap B)$ and since $+$ preserves greatest lower bounds of filtered sets we dually conclude that there

is some $j_1 \geq j_0$ in J such that $\bigvee^{\uparrow}_j \mu_1^j(A \cup B) + \mu_2^{j1}(A \cap B) < \mu_1^{j_0}(A) + \mu_1^{j_0}(B)$ which is less than, or equal, to $\mu_1^{j_1}(A) + \mu_1^{j_1}(B)$ as $j_1 \geq j_0$. But then $\mu_1^{j_1}(A \cup B) + \mu_2^{j1}(A \cap B) \leq \bigvee^{\uparrow}_j \mu_1^j(A \cup B) + \mu_2^{j1}(A \cap B) < \mu_1^{j_1}(A) + \mu_1^{j_1}(B)$ contradicts the fact that $\mu^{j_1} \in \mathsf{P}^{\mathrm{i}}(\Sigma(X))$.

Ie2(b). The reasoning for this case is dual to the one in Ie2(a).

Ie3(a). This has an argument that is dual to the one put forward for Ie3(b) below.

Ie3(b). Let $(\mu^t)_{t \in T}$ be directed in $\mathsf{P}^{\mathrm{i}}(\Sigma(X))$. For each $t \in T$, $\mu^t \in \mathsf{P}^{\mathrm{i}}(\Sigma(X))$ implies $\mu_2^t(\bigcup_{i \in I} A_i) \leq \mu_2^t(\bigcup_{j \in J} A_j) - \sum_{k \in J \setminus I} \mu_1^t(A_k)$ for all pairwise disjoint families $(A_j)_{j \in J}$ and $I \subseteq J$. Let μ be the least upper bound of $(\mu^t)_{t \in T}$. Then $\mu_2(\bigcup_{i \in I} A_i)$ equals

$$\begin{aligned}
\bigwedge^{\downarrow}_{t \in T} \mu_2^t(\bigcup_{i \in I} A_i) &\leq \bigwedge^{\downarrow}_{t \in T} \left(\mu_2^t(\bigcup_{j \in J} A_j) - \sum_{k \in J \setminus I} \mu_1^t(A_k) \right) \qquad (20) \\
&= \left(\bigwedge^{\downarrow}_{t \in T} \mu_2^t(\bigcup_{j \in J} A_j) \right) - \left(\bigvee^{\uparrow}_{t \in T} \sum_{k \in J \setminus I} \mu_1^t(A_k) \right) \\
(?) &\leq \left(\bigwedge^{\downarrow}_{t \in T} \mu_2^t(\bigcup_{j \in J} A_j) \right) - \sum_{k \in J \setminus I} \bigvee^{\uparrow}_{t \in T} \mu_1^t(A_k) \\
&= \mu_2(\bigcup_{j \in J} A_j)) - \sum_{k \in J \setminus I} \mu_1(A_k)
\end{aligned}$$

giving us Ie3(b) for μ, if only we can show that

$$\bigvee^{\uparrow}_{t \in T} \sum_{l \in L} \mu_1^t(A_l) \geq \sum_{l \in L} \bigvee^{\uparrow}_{t \in T} \mu_1^t(A_l) \qquad (21)$$

hold for all $L \subseteq J$. But this is certainly the case if L is a finite set, for $+$ preserves least upper bounds of directed sets. If L is infinite, then the infinite sum is a directed supremum of sums formed over finite subsets of L, and then we get a contradiction if we assume that the left hand side is strictly below the one on the right hand.

Proposition 4. *The map $i_X \colon \mathsf{P}(\Sigma(X)) \to \mathsf{P}^{\mathrm{i}}(\Sigma(X))$, defined by $i_X(\mu)\, A = [\mu(A), \mu(A)]$ for all $A \in \Sigma(X)$, is injective, monotone, and maps into the set of maximal elements in $\mathsf{P}^{\mathrm{i}}(\Sigma(X))$.*

Proof. One immediately verifies that $i_X(\mu)$ is an element of $\mathsf{P}^{\mathrm{i}}(\Sigma(X))$, for the axioms P1 to P3 ensure the validity of Ie1 to Ie3, noting that η_1 equals η_2 for $\eta = i_X(\mu)$. Since the ordering on maximal elements is equality, the map i_X is injective. Since the ordering on $\mathsf{P}(\Sigma(X))$ is equality, any map of this type is monotone.

Question 1. Can one characterize those sigma-algebras $\Sigma(X)$ for which *all* maximal elements of $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$ are of the form $i_X(\mu)$ for some probability measure μ?

Since $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$ is a dcpo, we know that every element $\mu \in \mathtt{P}^{\mathtt{i}}(\Sigma(X))$, seen as a partial probability measure, has at least one maximal element $\hat{\mu}$ in $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$ above it. If none of these elements are in the image of i_X, one would like to establish that μ is somehow probabilistically inconsistent; see the discussion in Section 4.

Remark 5. Let $r_i \in \mathtt{UI}$ and $\mu^i \in \mathtt{P}^{\mathtt{i}}(\Sigma(X))$ for $i = 1, 2, \ldots, n$ such that $\sum r_i = 1$. Then the function $\sum r_i \cdot \mu^i \colon \Sigma(X) \to \to \mathtt{I}$ which maps A to $[\sum r_i \cdot \mu_1^i(A), \sum r_i \cdot \mu_2^i(A)]$ and is an element of $\mathtt{P}^{\mathtt{i}}(\Sigma(X))$. Axioms Ie3, notably the inequalities (15) and (16), fail in general if one extends this construction such that r_i are proper intervals.

4 Equational axioms

The axioms presented for partial probability measures were all inequalities and seemed consistent upon first inspection. However, if computing values of μ for sets in $\Sigma(X)$ is *all we have access to*, then these inequalities have to be turned into *equalities*. For example, if $\mu_1(A \cup B) > \mu_1(A) + \mu_1(B) - \mu_2(A \cap B)$ were the case, then the computation of $\mu_1(A \cup B)$ has to involve some additional, hidden information that goes beyond what μ can provide in isolation. Therefore, it would be of great interest to render a justification of *axioms of probability with uncertainty or vagueness*, such as the ones proposed below, by successfully transferring the game-theoretic justification of the axioms of probability, provided by B. de Finetti in 1931. He showed that if some agent assigns degrees of beliefs (= elements of $\mathtt{UI}$) to a subset of $\Sigma(X)$, then these numbers violate the axioms of probability if, and only if, a betting game derived from these degrees has a winning strategy for another agent. Our modified degrees of belief would now be intervals (= elements of $\mathtt{I}$). Such a game-theoretic characterization on consistency would greatly aid in and ultimately justify the choice among a host of possible partial versions of probability measures, thereby rendering a clean mathematical foundations for the semantics of systems with uncertain probabilistic information.

Alternatively, let us call a set of axioms $\mathcal{A}$ *consistent* iff the partial ordering of all $\mu \colon \Sigma(X) \to \to \mathtt{I}$ which satisfy $\mathcal{A}$ is a dcpo whose maximal elements are isomorphic to $\mathtt{P}(\Sigma(X))$. Another satisfactory justification for our choice of axioms would be to show that E1 to E3 are somehow a minimal set of consistent sets and $\mathtt{P}^{\mathtt{e}}(\Sigma(X))$, therefore, a maximal "consistent domain".

Definition 8. *Let $\mathtt{P}^{\mathtt{e}}(\Sigma(X))$ be the partial ordering of all maps $\mu \in \Sigma(X) \to \mathtt{I}$ which satisfy the axioms E1, E2, and E3 which are obtained from the axioms Ie1 to Ie3 by changing all inequalities to equalities.*

A version for partial sub-probability measures would only consider axioms E2 and E3.

Proposition 5. *The partial ordering* $\mathtt{P}^{\mathrm{e}}(\Sigma(X))$ *is a dcpo and its least upper bounds of directed sets are the ones formed in* $\Sigma(X) \to \mathtt{I}$.

Proof. Since $\mathtt{P}^{\mathrm{e}}(\Sigma(X))$ is a subset of $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$, it suffices to show the dual inequalities of Ie1 to Ie3, which is reasoned is a similar way.

Proposition 6. *The map* $e_X \colon \mathtt{P}(\Sigma(X)) \to \mathtt{P}^{\mathrm{e}}(\Sigma(X))$, *defined by* $e_X(\mu)\,A = [\mu(A), \mu(A)]$ *for all* $A \in \Sigma(X)$, *is injective, and monotone and maps into the set of maximal elements of* $\mathtt{P}^{\mathrm{e}}(\Sigma(X))$. *Moreover, the image of* e_X *equals the set of maximal elements in* $\mathtt{P}^{\mathrm{e}}(\Sigma(X))$.

Proof. We may copy the proof for i_X and $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$ except in two places. First, e_X is a well defined map since $e_X(\mu)$ satisfies the equations E1 to E3; for P3, note that $\nu_l(\bigcup_{i\in I} A_i) = \sum_{i\in I} \nu_l(A_i)$ holds for $\nu = e_X(\mu)$ and $l = 1, 2$. Second, we also have to show that a maximal element η in $\mathtt{P}^{\mathrm{e}}(\Sigma(X))$ is in the image of e_X. To that end consider $\mu\colon \Sigma(X) \to \mathtt{UI}$ defined by $\mu(A) = (\eta_1(A) + \eta_2(A))/2$. If $\mu \in \mathtt{P}(\Sigma(X))$, then clearly $\eta \leq e_X(\mu)$ in $\Sigma(X) \to \mathtt{I}$, for $\eta_1(A) \leq \eta_2(A)$ implies $\eta_1(A) \leq (\eta_1(A) + \eta_2(A))/2 \leq \eta_2(A)$. Since η is maximal in $\mathtt{P}^{\mathrm{i}}(\Sigma(X))$, this would finish the proof. Thus, it suffices to show that $\mu \in \mathtt{P}(\Sigma(X))$:

P1. $\mu(X) = (\eta_1(X) + \eta_2(X))/2 = (1+1)/2 = 1$ by E1 applied to η;

P2. $\mu(A{\cup}B){+}\mu(A{\cap}B) = (\eta_1(A{\cup}B){+}\eta_2(A{\cup}B))/2{+}(\eta_1(A{\cap}B){+}\eta_2(A{\cap}B))/2$ and we can use axioms E2(a) and E2(b) on η to rearrange the latter expression to $\mu(A) + \mu(B)$.

P3. We proceed as for P2, but also use the fact that infinite sums over $\mathtt{UI}$ are least upper bounds of directed sets. Let $(A_j)_{j\in J}$ be a pairwise disjoint family in $\Sigma(X)$. Then we compute

$$\begin{aligned}
\mu(A_{i_0}) &= (\eta_1(A_{i_0}) + \eta_2(A_{i_0}))/2 \qquad (22)\\
&= (\eta_1(\bigcup_{j\in J} A_j) - \sum_{i_0\neq k} \eta_2(A_k))/2 + (\eta_2(\bigcup_{j\in J} A_j) - \sum_{i_0\neq k} \eta_1(A_k))/2\\
&= (\eta_1(\bigcup_{j\in J} A_j) + \eta_2(\bigcup_{j\in J} A_j))/2 - \sum_{i_0\neq k} (\eta_1(A_k) + \eta_2(A_k))/2\\
&= \mu(\bigcup_{j\in J} A_j) - \sum_{i_0\neq k} \mu(A_k)
\end{aligned}$$

yielding P3 for μ.

Partial probability measures may not enjoy properties that are known to hold for probability measures. For example, each $\mu \in \mathtt{P}(\Sigma(X))$ is monotone: $A \subseteq B$ in $\Sigma(X)$ implies $\mu(A) \leq \mu(B)$. However, for $\nu \in \mathtt{P}^{\mathrm{e}}(\Sigma(X))$ this is true iff $\nu_1 = \nu_2$ iff ν is a maximal element in that dcpo iff it "is" a probability measure.

References

1. S. Abramsky and A. Jung. Domain theory. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 3, pages 1–168. Clarendon Press, 1994.
2. R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, C-35(8), 1986.
3. J. R. Burch, E. M. Clarke, D. L. Dill K. L. McMillan, and J. Hwang. Symbolic model checking: 10^{20} states and beyond. Proceedings of the Fifth Annual Symposium on Logic in Computer Science, June 1990.
4. K. Cerans, J. Chr. Godskesen, and K. G. Larsen. Timed Modal Specification — Theory and Tools. In Costas Courcoubetis, editor, *5th International Conference, CAV'93*, pages 253–267. Springer Verlag, 1993. Elounda, Greece, June 28–July 1, 1993.
5. 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.
6. 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.
7. E.M. Clarke, O. Grumberg, H. Hiraishi, S. Jha, D.E. Long, K.L. McMillan, and L.A. Ness. Verification of the Futurebus+cache coherence protocol. In L. Claesen, editor, *Proceedings of the Eleventh International Symposium on Computer Hardware Description Languages and their Applications*. North-Holland, April 1993.
8. 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.
9. Dennis Dams, Rob Gerth, and Orna Grumberg. Abstract interpretation of reactive systems. *ACM Transactions on Programming Languages and Systems*, 19(2), 1997.
10. R. de Nicola and F. Vaandrager. Three Logics for Branching Bisimulation. *Journal of the Association of Computing Machinery*, 42(2):458–487, March 1995.
11. C. Derman. *Finite-State Markovian Decision Processes*. Academic Press, 1970. New York.
12. A. Edalat. Dynamical systems, Measures and Fractals via Domain Theory. *Information and Computation*, 120(1):32–48, 1995.
13. A. Edalat and M. H. Escardo. Integration in Real PCF. In *IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, IEEE Computer Society Press, 1996.
14. A. Edalat, P. J. Potts, and M.. Escardo. Semantics of exact arithmetic. In *Twelfth Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society Press, 1997.
15. K. Fisler and M. Y. Vardi. Bisimulation and Model Checking. In *Proceedings of the 10th IFIP WG 10.5 Advanced Research Working Conference on Correct Hardware Design and Verification Methods*, September 1999. To appear.
16. P. R. Halmos. *Measure Theory*. D. van Norstrand Company, 1950.
17. D. Heckerman. A tutorial on learning Bayesian networks. Technical Report MSR-TR-95-06, Microsoft Research, March 1995.
18. M. Huth. A Unifying Framework for Model Checking Labeled Kripke Structures, Modal Transition Systems, and Interval Transition Systems. In *19th International Conference on the Foundations of Software Technology & Theoretical Computer*

Science, Lecture Notes in Computer Science. Springer Verlag, 1999. to appear in December 1999.

19. 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.
20. 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.
21. C.T. Lin and C.S.G. Lee. Neural-network-based fuzzy logic control and decision system. *IEEE Transactions on Computers*, 40:1320–1336, 1991.
22. K. L. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.
23. R. Milner. An algebraic definition of simulation between programs. In *2nd International Joint Conference on Artificial Intelligence*, pages 481–489. British Computer Society, London, 1971.
24. R. Milner. *Communication and Concurrency*. Series in Computer Science. Prentice-Hall International, 1989.
25. R. E. Moore. *Interval Analysis*. Prentice-Hall, Englewood Cliffs, 1966.
26. D. M. Park. Concurrency on automata and infinite sequences. In P. Deussen, editor, *Conference on Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*. Springer Verlag, 1981.
27. B. Pierce. *Basic Category Theory for Computer Scientists*. Foundations of Computing Series. The MIT Press, 1991.
28. J. P. Quielle and J. Sifakis. Specification and verification of concurrent systems in cesar. In *Proceedings of the fifth International Symposium on Programming*, 1981.
29. D. S. Scott. Continuous lattices. In F. Lawvere, editor, *Toposes, Algebraic Geometry and Logic*, volume 274 of *Lecture Notes in Mathematics*, pages 97–136. Springer Verlag, 1972.
30. D. S. Scott. Lattice Theory, Data Types and Semantics. In *Formal Semantics of Programming Languages*, pages 66–106. Prentice-Hall, 1972.
31. M. Vardi. Automatic Verification of Probabilistic Concurrent Finite-State Programs. In *Proc. FOCS'85*, pages 327–338. IEEE, 1985.