Least Upper Bounds for Probability Measures and their Applications to Abstractions

Rohit Chadha [a], Mahesh Viswanathan [b], Ramesh Viswanathan [c]

[a] *University of Missouri*

[b] *University of Illinois at Urbana–Champaign*

[c] *Bell Laboratories*

Abstract

Least upper bounds play an important role in defining the semantics of programming languages, and in abstract interpretations. In this paper, we identify conditions on countable ordered measurable spaces that ensure the existence of least upper bounds for all sets of probability measures. These conditions are shown to be necessary as well — for any measurable space not satisfying these conditions, there are (finite) sets of probability measures for which no least upper bound exists. For measurable spaces meeting these conditions, the existence of least upper bounds is established constructively. Based on this least upper bound construction, we present a novel abstraction method applicable to Discrete Time Markov Chains (DTMCs), Markov Decision Processes (MDPs), and Continuous Time Markov Chains (CTMCs). The main advantage of the new abstraction techniques is that the resulting abstract models are *purely probabilistic* that may be more amenable to automated analysis than models with both nondeterministic and probabilistic transitions which arise from previously known abstraction techniques.

1 Introduction

Order structures have served a pivotal role in program semantics and analysis of probabilistic systems. Starting from the work of Saheb-Djahromi [25], and further developed by Jones [13], an ordering relation on probability measures has been used in developing a denotational semantics for probabilistic

Email addresses: chadhar@missouri.edu (Rohit Chadha), vmahesh@cs.uiuc.edu (Mahesh Viswanathan), rv@research.bell-labs.com (Ramesh Viswanathan).

programs. This ordering also plays a central role in defining the notion of simulation for probabilistic systems. In a probabilistic model, a transition specifies a probability measure on its successor states. One transition then simulates another if the probability measures they specify are related by the ordering on measures. In this manner, simulation and bisimulation relations were first defined for Deterministic Time Markov Chains (DTMC), and Markov Decision Processes (MDP) [14], and subsequently extended to Continuous Time Markov Chains (CTMC) [3]. Therefore, in all these settings, a set of transitions is abstracted by a transition if it is an upper bound for the probability measures specified by the set of transitions being abstracted.

Based on this observation that an upper bound probability measure can serve as a correct abstraction, we investigate the construction of least upper bounds for sets of probability measures and their application to abstraction. We begin by observing that in general, measures (even over simple finite spaces) do not have least upper bounds. We therefore look for a class of measurable spaces for which the existence of least upper bounds is guaranteed for arbitrary sets of measures. Since the ordering relation on measures is induced from the underlying partial order on the space over which the measures are considered, our goal is to identify conditions on the underlying partial order that are sufficient to prove the existence of least upper bounds.

For general measurable spaces, the order structure on measures is very sensitive to the specific collection of measurable subsets (σ-algebra). This makes a characterization of the necessary and sufficient conditions (for the existence of least upper bounds) for any measurable space particularly challenging. We overcome this problem by developing a new representation theorem that shows how any countable measurable space can be reduced to a countable discrete measurable space.[1] More precisely, for any countable measurable space $\mathcal{X}$ (over a set with an underlying preorder), we show how to construct a countable set $\mathsf{At}(\mathcal{X})$ and a partial order over it such that there is an *order-preserving isomorphism* between the (ordered) spaces of probability measures over $\mathcal{X}$ and the discrete probability measures over $\mathsf{At}(\mathcal{X})$. The construction of the set $\mathsf{At}(\mathcal{X})$ is based both on the measurable subsets of $\mathcal{X}$ as well as its underlying preorder. In light of the intricate sensitivity of the order structure of probability measures to the underlying order and measurable subsets, this representation theorem provides a powerful simplifying tool.

Given the representation theorem, we can, without loss of generality, restrict our attention to countable discrete measurable spaces with an underlying partial order. We define conditions on the underlying partial order that intuitively correspond to requiring the Hasse diagram of the partial order to have a "tree-

[1] A discrete measurable space is one where every subset of the universe is measurable.

like" structure. We establish these conditions to be necessary — the underlying partial order on any measurable space admitting least upper bounds is proven to satisfy the requirements of being "tree-like". For measurable spaces meeting these conditions, we present a construction of least upper bounds for arbitrary collections of probability measures.

Next, we present a new method to abstract probabilistic transition systems based on our least upper bound construction. Abstractions are constructed on the basis of an equivalence relation on the set of (concrete) states of the system being abstracted with the equivalence classes forming the (abstract) states of the abstract model (thus, the abstract model collapses all equivalent states into one). In previously constructed abstractions, each abstract state has multiple (nondeterministic) transitions corresponding to the transitions of each of the concrete states in the equivalence class. However, in our construction, the transition out of an abstract state is taken to be the *least upper bound measure* of the transitions from each of the concrete states it "abstracts." This yields a single outgoing transition resulting in an abstract model that is *purely probabilistic* which does not have any nondeterminism. These abstraction constructions are presented and proved correct for DTMCs, MDPs and CTMCs.

A few salient features of our abstract models bear highlighting. First, the fact that least upper bounds are used in the construction implies that for a particular equivalence relation on concrete states and partial order on the abstract states, the abstract model constructed is finer than (*i.e.*, can be simulated by) any purely probabilistic model that can serve as an abstraction. Thus, for verification purposes, our model is the most precise purely probabilistic abstraction on a chosen state space. Second, the set of abstract states is not completely determined by the equivalence classes of the relation on concrete states; there is freedom in the choice of states that are above the equivalence classes in the partial order. However, for any such choice that respects the "tree-like" requirement on the underlying partial order, the resulting model will be exponentially smaller than the existing proposals of [9,16]. We show that there are instances where we can get more precise results than the abstraction schemes of [9,16] while using significantly fewer states (see Example 6.9 and Section 7.2). Third, the abstract models we construct are purely probabilistic which makes model checking easier. Additionally, these abstractions can potentially be verified using statistical techniques which do not work when there is nondeterminism [30,29,27]. Finally, CTMC models with nondeterminism, called CTMDP, are known to be difficult to analyze [2]. Specifically, the measure of time-bounded reachability can only be computed approximately through an iterative process; therefore, there is only an approximate algorithm for model-checking CTMDPs against CSL. On the other hand, there is a theoretically exact solution to the corresponding model-checking problem for CTMCs by reduction to the first order theory of reals [1].

Related Work. Abstractions have been extensively studied in the context of probabilistic systems. General issues and definitions of good abstractions are presented in [14,11,12,22]. Specific proposals for families of abstract models include Markov Decision Processes [14,6,7], systems with interval ranges for transition probabilities [14,22,9,16], abstract interpretations [21], 2-player stochastic games [17], and expectation transformers [19]. Recently, theorem-prover based algorithms for constructing abstractions of probabilistic systems based on predicates have been presented [28]. All the above proposals construct models that exhibit both nondeterministic and probabilistic behavior. The abstraction method presented in this paper constructs purely probabilistic models.

The order structure on measures was first studied extensively in the context of the probabilistic powerdomain construction [25,13] for denotational semantics. This theory is based on a particular σ-algebra (the Borel field induced by Scott-open sets) and is concerned with the existence of least upper bounds only for increasing chains (directed complete partial orders); on the other hand, the work presented here considers arbitrary σ-algebras and least upper bounds of all subsets. Stronger order structures (subcategories of DCPO) have to be considered for the probabilistic powerdomain construction to satisfy the properties of a commutative monad and a significant challenge encountered in this development has been the difficulty in preserving any lattice-like structure on measures (*c.f.* [15]). While none of the order structures studied are as strong as a join semi-lattice that is characterized in this paper, an interesting point of comparison is that the finite tree-reversal posets considered in [15] for obtaining finitely separable domains is a special instance of the partial orders identified in this work. It is possible that the representation theorem and least upper bound construction presented here proves fruitful in identifying suitable semantic constructions for probabilistic domain theory though this is not the subject of this paper. Another area where the use of orders and least upper bounds plays an important role is that of abstract interpretation [5]. Partially due to the challenges of orders on measures and constructing least upper bounds, the current proposals for carrying out abstract interpretation of probabilistic programs [23,20,21] develop a framework that relies on properties of metric spaces rather than the classical theory based on Galois connections and lattices. Our results might allow one to develop a different framework for probabilistic abstract interpretation that can better leverage the well-studied classical theory [5].

A preliminary version of the results in this paper appeared as an extended abstract in [4]. The presentation here contains all the proofs, including those that were missing in the extended abstract. Furthermore, the results in [4] were limited in two ways. First, the sets over which the probability measures were being considered had to be finite. Second, the measurable space considered had to be discrete, *i.e.*, every subset of the universe had to be measurable.

In this paper, we generalize the results of [4] to be applicable to any general measurable space (with arbitrary measurable subsets) that is countable (possibly infinite). Thus, the representation theorem and the construction of least upper bounds for countably infinite spaces are new.

2 Preliminaries

We assume that the reader is familiar with basic set theory, order theory and measure theory. In this section, we present relevant notation and results that will be used throughout the paper. Additional background material is presented in Appendix A.

$\mathbb{N}, \mathbb{R}$ and $\mathbb{R}^+$ will denote the set of natural numbers, reals and positive real numbers respectively. Ordinals will be denoted by $\alpha, \beta, \gamma, \ldots$. The first infinite ordinal will be denoted by ω. For a set X, its power-set will be denoted by $\mathcal{P}(X)$.

2.1 Orders

Given a set X, a binary relation $\sqsubseteq \subseteq X \times X$ is said to be a **preorder** if $\sqsubseteq$ is reflexive and transitive. We will often write $a \sqsubseteq b$ to mean $(a, b) \in \sqsubseteq$. For the definitions below, let us fix a preorder $\mathcal{X} = (X, \sqsubseteq)$. A set $U \subseteq X$ is said to be $\sqsubseteq$**-upward closed** if for every $x \in U$ and $y \in X$ with $x \sqsubseteq y$ we have that $y \in U$; the set of $\sqsubseteq$-upward closed sets will be denoted by $\mathsf{Up}(\mathcal{X})$. A set $D \subseteq X$ is said to be $\sqsubseteq$**-downward closed** if for every $y \in D$ and $x \in X$ with $x \sqsubseteq y$ we have that $x \in D$; the collection of $\sqsubseteq$-downward closed sets will be denoted by $\mathsf{Down}(\mathcal{X})$. Observe that U is $\sqsubseteq$-upward closed iff $X \setminus U$ is $\sqsubseteq$-downward closed. We shall be particularly interested in principal downward closed sets. A set D is said to be **principal** $\sqsubseteq$**-downward closed** if there exists $a \in X$ such that $D = D_a = \{b \mid b \sqsubseteq a\}$; the collection of principal downward closed sets will be denoted by $\mathsf{Princ}(\mathcal{X})$. When clear from the context, we shall drop the qualifier $\sqsubseteq$ in $\sqsubseteq$-upward and $\sqsubseteq$-downward closed sets.

A preorder $\sqsubseteq$ is said to be a **partial order** if it is anti-symmetric also. If $\sqsubseteq$ is a partial order on X then the pair $(X, \sqsubseteq)$ is said to be a **poset.** Given a set $A \subseteq X$, x is said to be an **upper bound of** A (**lower bound**) if for every $y \in A$, we have that $y \sqsubseteq x$ ($x \sqsubseteq y$ respectively). An element z is said to be a **least upper bound of** A (**greatest lower bound of** A) if z is an upper bound (lower bound respectively) and for every upper bound (lower bound respectively) x of A, we have that $x \sqsubseteq z$ ($z \sqsubseteq x$ respectively). A poset $(X, \sqsubseteq)$ is said to be a **join semi-lattice** (**meet semi-lattice**) if every *non-empty set*

$A \subseteq X$ has a least upper bound (greatest lower bound, respectively). It turns out that in a join semi-lattice any non-empty set A which has a lower bound, also has a greatest lower bound.

Proposition 2.1 *Let $(X, \sqsubseteq)$ be a join semi-lattice. Given $A \subseteq X, A \neq \emptyset$, if A has a lower bound then A has a greatest lower bound.*

Proof. Let $B = \{b \in X \mid \forall a \in A, b \sqsubseteq a\}$. In other words B is the set of lower bounds of A. If $B \neq \emptyset$, then B has a least upper bound, say c in X. The result will follow if we can show that c is also a lower bound of A. By definition any element of A is an upper bound of B. Since c is the least upper bound of B, it follows that $c \sqsubseteq a$ for each $a \in A$. Thus c is a lower bound of A. □

Given a poset $(X, \sqsubseteq)$ and a set $X_1 \subset X$, we say that $x \in X_1$ is a **maximal element** (**minimal element**) of X_1 if for every $y \in X_1$, $x \sqsubseteq y$ ($y \sqsubseteq x$ respectively) implies that $x = y$. The set of all maximal elements of X_1 will be denoted by maximal(X_1) and the set of minimal elements of X_1 will be denoted by minimal(X_1). In general, maximal(X_1) and minimal(X_1) may be empty. However, if X_1 is finite and non-empty then maximal(X_1) and minimal(X_1) are not empty.

Finally, two posets $(X_1, \sqsubseteq_1)$ and $(X_2, \sqsubseteq_2)$ are said to be **isomorphic** if there is a bijection $g : X_1 \to X_2$ such that $x \sqsubseteq_1 y$ iff $g(x) \sqsubseteq_2 g(y)$.

2.2 Measures

Given a set X, a family of subsets of X, Σ, is said to be **σ-field** or **σ-algebra** if Σ contains the empty set and is closed under complementation and countable union. A **measurable space** is a pair (X, Σ) such that Σ is a σ-algebra. The members of Σ are called the **measurable subsets** of X. Examples of σ-fields are $\{\emptyset, X\}$ and $\mathcal{P}(X)$ (the powerset of X). The σ-field $(X, \mathcal{P}(X))$ is called a *discrete* measure space. We will sometimes abuse notation and refer to the measurable space (X, Σ) by X or by Σ, when the σ-field or set, is clear from the context. The intersection of an arbitrary collection of σ-fields on a set X is again a σ-field, and so given any $B \subseteq \mathcal{P}(X)$ there is a least σ-field containing B, which is called the σ-field **generated** by B. The σ-field generated by B shall henceforth be denoted as $\sigma(B)$.

A measurable space (X, Σ) is **countable** if X is countable. For countable measurable spaces (X, Σ), Σ is also closed under *arbitrary* (*i.e.*, not necessarily countable) unions and intersections; this is shown next.

Proposition 2.2 *Given a countable measurable space (X, Σ), let $\{A_i \in \Sigma \mid i \in I\}$ be a collection of measurable sets. Then $\bigcup_{i \in I} A_i \in \Sigma$ and $\bigcap_{i \in I} A_i \in \Sigma$.*

Proof. Since $X \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I}(X \setminus A_i)$, and measurable sets are closed under complementation, it suffices to show that Σ is closed under arbitrary union.

Now, let $B = \bigcup_{i\in I} A_i$. Given $b \in B$, fix $i_b \in I$ such that $b \in A_{i_b}$. Note that $B = \bigcup_{b\in B} A_{i_b}$. Since $B \subseteq X$, the set B is countable and therefore the collection $\{A_{i_b} \mid b \in B\}$ is countable. Since each A_{i_b} is measurable and measurable sets are closed under countable union, we get that B is measurable also. □

A **positive measure** μ on a measurable space $\mathcal{X} = (X, \Sigma)$ is a function from Σ to $[0, \infty]$ such that $\mu(\emptyset) = 0$ and μ is **countably additive**, *i.e.*, if $\{A_i \mid i \in I\}$ is a countable family of pairwise disjoint measurable sets then $\mu(\bigcup_{i\in I} A_i) = \sum_{i\in I} \mu(A_i)$. A measurable space equipped with a measure is called a **measure space**. The **total weight** of a measure μ on measurable space X is $\mu(X)$. A **probability measure** is a positive measure of total weight 1. We will denote the collection of all probability measures on $\mathcal{X}$ by $\mathcal{M}_{=1}(\mathcal{X})$.

A convenient way to define measures is by specifying their values on a subclass of the measurable subsets. The relevant result we use relates to measures on *semi-rings*. A collection of subsets $\mathcal{S}$ of X is called a **semi-ring** if it contains $\emptyset$, contains X,[2] is closed under (finite) intersection, and if $A \subseteq B$ are two sets in $\mathcal{S}$ then there are finitely many pairwise disjoint sets $C_1, C_2, \ldots C_n \in \mathcal{S}$ such that $B \setminus A = \bigcup C_i$. A **measure on a semi-ring** $\mathcal{S}$ is a function $\mu : \mathcal{S} \to [0, \infty]$ such that $\mu(\emptyset) = 0$ and μ is countably additive, *i.e.*, if $\{A_i \mid i \in I\}$ is a countable collection of pairwise disjoint sets in $\mathcal{S}$ such that $\bigcup_{i\in I} A_i \in \mathcal{S}$ then $\mu(\bigcup_{i\in I} A_i) = \sum_{i\in I} \mu(A_i)$. An important result extends measures on semi-rings to σ-field generated by them [10].

Theorem 2.3 *Let $\mathcal{S}$ be a semi-ring on a set X, and let $\mu : \mathcal{S} \to [0, \infty]$ be a measure on $\mathcal{S}$, such that the measure of any set is finite. Then there is a unique extension to a measure on $\sigma(\mathcal{S})$.*

Another result on defining measures based on functions on a subcollection that we will use is the following.

Proposition 2.4 *Let $\mathcal{A} = \{\mathsf{A}_i \mid i \in I\}$ be a countable partition of X,* i.e., *I is countable, A_is are non-empty and pairwise disjoint, and $X = \cup_{i\in I}\mathsf{A}_i$. Then any function $\mu : \mathcal{A} \to [0, \infty]$ extends to a unique measure $\hat{\mu}$ on $\sigma(\mathcal{A})$. Furthermore $\hat{\mu}$ is a probability measure iff $\sum_{i\in I} \mu(\mathsf{A}_i) = 1$.*

Proof. Let $\mathcal{B} = \{\cup_{\mathsf{A}\in\mathcal{C}}\mathsf{A} \mid \mathcal{C} \subseteq \mathcal{A}\}$. We claim that $\mathcal{B} = \sigma(\mathcal{A})$. Please note that since $\mathcal{A}$ is countable, it follows immediately that $\mathcal{B} \subseteq \sigma(\mathcal{A})$. Hence, it suffices to show that $\mathcal{B}$ is a σ-algebra. Clearly $\emptyset \in \mathcal{B}$. Now, assume that $\mathsf{C} \in \mathcal{B}$.

[2] Usually, the whole set X is not required to be in a semi-ring. If X is not in $\mathcal{S}$, then different conditions are required for guaranteeing uniqueness in Theorem 2.3.

Then there is a $\mathcal{C} \subseteq \mathcal{A}$ such that $\mathsf{C} = \cup_{\mathsf{A}\in\mathcal{C}}\mathsf{A}$. Since A_i's are disjoint and $X = \cup_{i\in I}\mathsf{A}_I$, it is easy to see that $X \setminus \mathsf{C} = \cup_{\mathsf{A}\in\mathcal{A}\setminus\mathcal{C}}\mathsf{A}$. Thus, $\mathcal{B}$ is closed under complementation. Furthermore, if $\{\mathsf{C}_j | j \in J\}$ is a collection of sets in $\mathcal{B}$, then there is a collection $\{\mathcal{C}_j \subseteq \mathcal{A} \mid j \in J\}$ such that $\mathsf{C}_j = \cup_{\mathsf{A}\in\mathcal{C}_j}\mathsf{A}$. Now clearly, $\cup_{j\in J}\mathsf{C}_j = \cup_{\mathsf{A}\in\cup_{j\in J}\mathcal{C}_j}\mathsf{A}$. As $\cup_{j\in J}\mathcal{C}_j \subseteq \mathcal{A}$, $\mathcal{B}$ is closed under countable unions also.

Now, define $\hat{\mu} : \mathcal{B} \to [0,\infty]$ as follows. Since $\mathcal{A}$ forms a partition of X, for each $\mathsf{C} \in \mathcal{B}$ there is a unique set $\mathcal{C} \subseteq \mathcal{A}$ such that $\mathsf{C} = \cup_{\mathsf{A}\in\mathcal{C}}\mathsf{A}$. Let $\hat{\mu}(\mathsf{C}) = \sum_{\mathsf{A}\in\mathcal{C}} \mu(\mathsf{A})$. It can be shown easily that $\hat{\mu}$ is a measure.

Note that if μ_1 is any other measure extending μ, then it follows from pairwise disjointness of A_i's, that $\mu_1(\mathsf{C}) = \sum_{\mathsf{A}\in\mathcal{C}} \mu(\mathsf{A}) = \hat{\mu}(C)$. Finally observe that $\hat{\mu}(X) = \hat{\mu}(\cup_{i\in I}\mathsf{A}_I) = \sum_{i\in I} \mu(\mathsf{A}_i)$. Hence, $\hat{\mu}$ is a probability measure iff $\sum_{i\in I} \mu(\mathsf{A}_i) = 1$. □

An immediate corollary is the following.

Corollary 2.5 *If X is a countable set and $\mathcal{A} = \{\{x\} \mid x \in X\}$, then any function $\mu : \mathcal{A} \to [0,\infty]$ extends to a unique measure $\hat{\mu}$ on $\mathcal{P}(X)$.*

3 Ordered measurable spaces

We now present an ordering relation on probability measures. In order to define an ordering on probability measures we need to consider measurable spaces that are equipped with an ordering relation. An **ordered measurable space** is a triple $(X, \Sigma, \sqsubseteq)$ such that (X, Σ) is a measurable space and $\sqsubseteq$ is a preorder on X. A (probability) measure on $(X, \Sigma, \sqsubseteq)$ is a (probability) measure on (X, Σ). The ordering relation on the underlying set is lifted to an ordering relation on probability measures as follows.

Definition 3.1 Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be an ordered measurable space. For any probability measures μ, ν on $\mathcal{X}$, define $\mu \preceq_{\sqsubseteq} \nu$ iff for every upward closed set $U \in \Sigma$, $\mu(U) \leq \nu(U)$.

Our definition of the ordering relation is formulated so as to be applicable to any general measurable space. It has been used previously in a number of contexts, as can be seen from the following examples.

Example 3.2 *Let X be the (finite) set of states of an MDP, and let $\sqsubseteq$ be a simulation relation. The ordering on probability measures $\preceq_{\sqsubseteq}$ is equivalent to the definition of order on measures defined using weight functions as considered in [14] to define simulations. Indeed, Definition 3.1 can be seen to be identical to the presentation of the simulation relation in [8,26] where this equivalence has been observed as well. Next, consider $\mathcal{X} = (X, \Sigma, \sqsubseteq)$, where $(X, \sqsubseteq)$ is a*

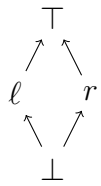

Fig. 1. Hasse Diagram of $\mathbb{T}$. Arrows directed from smaller element to larger element.

cpo, and Σ is the Borel σ-field generated by the Scott-open sets. The ordering $\preceq_{\sqsubseteq}$ is the ordering on measures used in [25] and [13] to define semantics of probabilistic programs.

The ordering relation on probability measures can be dually cast in terms of downward closed sets which is useful in the proofs of our construction.

Proposition 3.3 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be an ordered measurable space. For any probability measures μ, ν on $\mathcal{X}$, we have that $\mu \preceq_{\sqsubseteq} \nu$ iff for every downward closed set $D \in \Sigma$, $\mu(D) \geq \nu(D)$.*

Example 3.4 *For any set A, the tuple $(\mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \subseteq)$ is an ordered measure space. One special case of such a space that we will make use of in our examples is where A is $\{0, 1\}$. We will denote $\mathcal{P}(\{0, 1\})$ by T and the ordered space $(T, \mathcal{P}(T), \subseteq)$ by $\mathbb{T}$. We will denote the elements of T by $\bot = \emptyset$, $\ell = \{0\}$, $r = \{1\}$, and $\top = \{0, 1\}$. The Hasse diagram of the space is shown in Fig. 1. The upward closed sets of $\mathbb{T}$ are $\{\bot, \ell, r, \top\}, \{\ell, \top\}, \{r, \top\}$ and $\{\top\}$. Consider the probability measure λ, where ℓ has probability 1, and all the rest have probability 0. Similarly, τ is the measure where $\top$ has probability 1, and the rest 0, and in ρ, r gets probability 1, and the others 0. Now one can easily see that $\lambda \preceq_{\subseteq} \tau$ and $\rho \preceq_{\subseteq} \tau$. However $\lambda \not\preceq_{\subseteq} \rho$ and $\rho \not\preceq_{\subseteq} \lambda$.*

In general, Definition 3.1 yields a preorder that is not necessarily a partial order. However, for ordered measurable spaces generated by some collection of downward closed sets, the ordering relation is in fact a partial order. We formally define such spaces.

Definition 3.5 An ordered measurable space $(X, \Sigma, \sqsubseteq)$ is *order-respecting* if there exists $\mathcal{D} \subseteq \mathcal{P}(X)$ such that every $D \in \mathcal{D}$ is downward closed (with respect to $\sqsubseteq$) and Σ is generated by $\mathcal{D}$.

Many natural measurable spaces are order-respecting.

Example 3.6 *For any countable set X, the ordered measurable space $(X, \mathcal{P}(X), \sqsubseteq$ $)$ is order-respecting for any partial order $\sqsubseteq$ as $\mathcal{P}(X)$ is generated by $\{D_a \mid a \in X\}$. For any finite set A, the space $(\mathcal{P}(A), \mathcal{P}(\mathcal{P}(A)), \subseteq)$ is order-respecting since it is generated by all the downward closed sets of $(\mathcal{P}(A), \subseteq)$. Note that this includes the special ordered measure space $\mathbb{T}$ defined in Example 3.4. Finally, for*

any cpo $(X, \sqsubseteq)$, the Borel measurable space $(X, \mathcal{B}(X), \sqsubseteq)$ is order-respecting since every Scott-closed set is downward closed.

Observe that if $(X, \Sigma, \sqsubseteq)$ is order-respecting, then Σ is also generated by the collection of *all downward closed sets in* Σ.

Proposition 3.7 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be an ordered measurable space and let $\mathcal{D}$ be the collection of all downward closed sets in Σ,* i.e., *$\mathcal{D} = \{D \in \Sigma \mid D$ is downward closed$\}$. Then $\mathcal{X}$ is order-respecting iff Σ is generated by $\mathcal{D}$.*

Proof. ($\Rightarrow$). Assume that $\mathcal{X}$ is order-respecting. Then there is some collection $\mathcal{D}_0 \subseteq \mathcal{D}$ such that $\Sigma = \sigma(\mathcal{D}_0)$. Since $\mathcal{D}_0 \subseteq \mathcal{D}$, we get by definition, $\sigma(\mathcal{D}_0) \subseteq \sigma(\mathcal{D})$. Also, since $\sigma(\mathcal{D})$ is the smallest σ-algebra generated by $\mathcal{D}$ and $\mathcal{D} \subseteq \Sigma$, $\sigma(\mathcal{D}) \subseteq \Sigma$. Hence, $\sigma(\mathcal{D}_0) \subseteq \sigma(\mathcal{D}) \subseteq \Sigma$. But $\Sigma = \sigma(\mathcal{D}_0)$ and therefore $\sigma(\mathcal{D}) = \Sigma$. The ($\Leftarrow$) direction is immediate from definition. □

One technical property about downward closed sets and order-respecting ordered measurable spaces that is useful is that the collection of sets formed by the difference of downward closed measurable sets forms a semi-ring. We will use this often to define a probability measure on a σ-field.

Lemma 3.8 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be an ordered measurable space, and let $\mathcal{D}$ be the collection of all downward closed sets in Σ,* i.e., *$\mathcal{D} = \{D \in \Sigma \mid D$ is downward closed$\}$. Consider $\mathcal{S} = \{D_1 \setminus D_2 \mid D_1, D_2 \in \mathcal{D}$ and $D_1 \supseteq D_2\}$. Then $\mathcal{S}$ is a semi-ring. Further, if $\mathcal{X}$ is order-respecting then Σ is generated by $\mathcal{S}$.*

Proof. Observe that $\emptyset, X$ are downward closed sets, and since $\emptyset, X \in \Sigma$, $\emptyset, X \in \mathcal{D}$, and also in $\mathcal{S}$. Now if $D_1, D_2 \in \mathcal{D}$ then $D_1 \cap D_2$ and $D_1 \cup D_2$ are downward closed sets, and since Σ is closed under union and intersection, $D_1 \cup D_2$ and $D_1 \cap D_2$ are in Σ and therefore in $\mathcal{D}$.

From basic set theory we know that

$$(D_1 \setminus D_2) \cap (D_3 \setminus D_4) = (D_1 \cap D_3) \setminus ((D_1 \cap D_3) \cap (D_2 \cup D_4)).$$

Since $\mathcal{D}$ is closed under union and intersection, $(D_1 \setminus D_2) \cap (D_3 \setminus D_4) \in \mathcal{S}$. Finally,

$$\begin{aligned}&(D_1 \setminus D_2) \setminus (D_3 \setminus D_4) = \\ &(D_1 \setminus (D_2 \cup (D_3 \cap D_1))) \cup ((D_1 \cap D_4) \setminus ((D_1 \cap D_4) \cap D_2)).\end{aligned}$$

Now since $D_2 \subseteq D_1$, we have $D_2 \cup (D_3 \cap D_1) \subseteq D_1$. Further, as $D_4 \subseteq D_3$, $(D_1 \setminus (D_2 \cup (D_3 \cap D_1)))$ is disjoint from $D_1 \cap D_4$. Thus $\mathcal{S}$ is a semi-ring. Finally, we know that $\mathcal{D} \subseteq \mathcal{S} \subseteq \Sigma$, and since Σ is generated by $\mathcal{D}$ when $\mathcal{X}$ is

order-respecting (see Proposition 3.7), it follows that Σ is also generated by $\mathcal{S}$. $\square$

Using Lemma 3.8, we can also prove the main observation about the ordering on measures, namely, that it is a partial order.

Theorem 3.9 *For any ordered measurable space $\mathcal{X} = (X, \Sigma, \sqsubseteq)$, the relation $\preceq_{\sqsubseteq}$ is a preorder on $\mathcal{M}_{=1}(\mathcal{X})$. The relation $\preceq_{\sqsubseteq}$ is additionally a partial order (antisymmetric) if $\mathcal{X}$ is order-respecting.*

Proof. The proof that $\preceq_{\sqsubseteq}$ is reflexive and transitive is immediate.

If $\mu \preceq_{\sqsubseteq} \nu$ and $\nu \preceq_{\sqsubseteq} \mu$ then from Proposition 3.3 we know that $\mu(D) = \nu(D)$ on all downward closed measurable sets $D \in \Sigma$. Let $\mathcal{D}$ be the collection of all downward closed sets in Σ and $\mathcal{S} = \{D_1 \setminus D_2 \mid D_1 \supseteq D_2 \in \mathcal{D}\}$. Now since $\mu(D) = \nu(D)$ on all downward closed measurable sets, it follows that, for downward closed sets $D_1 \supseteq D_2$, $\mu(D_1 \setminus D_2) = \mu(D_1) - \mu(D_2) = \nu(D_1) - \nu(D_2) = \nu(D_1 \setminus D_2)$. Thus, $\mu(S) = \nu(S)$ for all $S \in \mathcal{S}$. Since, $\mathcal{S}$ is a semi-ring (see Lemma 3.8), we can conclude from Theorem 2.3 that $\mu(V) = \nu(V)$ for every V in the σ-field generated by $\mathcal{S}$, which is the same as Σ, when $\mathcal{X}$ is order-respecting. $\square$

4 Representation Theorem

Properties of the order on probability measures are very sensitive to the underlying order and the specific collection of sets that are measurable. We overcome this challenge by presenting a powerful simplifying technique in this section. We show that for any *countable* order-respecting measurable space $\mathcal{X} = (X, \Sigma, \sqsubseteq)$, we can construct an ordered measurable space, $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \Sigma_{\mathsf{At}(\mathcal{X})}, \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ such that

- $\mathsf{At}(\mathcal{X})$ is countable,
- $\Sigma_{\mathsf{At}(\mathcal{X})}$ is $\mathcal{P}(\mathsf{At}(\mathcal{X}))$ (and hence the underlying measure space is discrete),
- $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$ is a partial order (even if $\sqsubseteq$ is a preorder and therefore $\Lambda(\mathcal{X})$ is order-respecting), and
- the poset $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is isomorphic to the poset $(\mathcal{M}_{=1}(\Lambda(\mathcal{X})), \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}})$.

Thus, any countable order-respecting measurable space is "equivalent" to a countable, discrete measure space equipped with a partial order. We will call the space $\Lambda(\mathcal{X})$ to be the **atom space** of $\mathcal{X}$. Before defining the atom space, we present the definition of a preorder on elements of $\mathcal{X}$ that depends on both $\sqsubseteq$ and the σ-field Σ.

Definition 4.1 Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be an ordered measurable space. For any

$x, y \in \mathcal{X}$, define $x \trianglelefteq_{\mathcal{X}} y$ iff for every $\sqsubseteq$-downward closed set $D \in \Sigma$, $y \in D$ implies that $x \in D$. We will say $x \equiv_{\mathcal{X}} y$ iff for every $\sqsubseteq$-downward closed set $D \in \Sigma$, $x \in D$ iff $y \in D$.

It is easy to see that $\trianglelefteq_{\mathcal{X}}$ is a preorder on X, and is "coarser" that $\sqsubseteq$, *i.e.*, if $x \sqsubseteq y$ then $x \trianglelefteq_{\mathcal{X}} y$. The relation $\equiv_{\mathcal{X}}$ is the equivalence relation induced by the preorder $\trianglelefteq_{\mathcal{X}}$.

Example 4.2 *Let* $\mathsf{N} = \mathbb{N} \cup \{\infty\}$ *and let* $\sqsubseteq_{\mathsf{N}} \subseteq \mathsf{N} \times \mathsf{N}$ *be the preorder* $\sqsubseteq_{\mathsf{N}} = \{(a, \infty) \mid a \in \mathsf{N}\}$. *Let* Σ_{N} *be the* σ*-algebra* $\{\emptyset, \mathsf{N}, \mathbb{N}, \{\infty\}\}$. *Observe that* Σ_{N} *is generated by the* $\sqsubseteq_{\mathsf{N}}$*-downward* $\{\mathbb{N}\}$ *and therefore the space* $\mathcal{N} = (\mathsf{N}, \Sigma_{\mathsf{N}}, \sqsubseteq_{\mathsf{N}})$ *is a countable order-respecting space. The set of* $\sqsubseteq_{\mathsf{N}}$*-downward closed sets in* Σ_{N} *is* $\mathcal{D} = \{\emptyset, \mathbb{N}, \mathsf{N}\}$. *For any* $x, y \in \mathbb{N}$, $x \trianglelefteq_{\mathcal{N}} y$ *and* $x \trianglelefteq_{\mathcal{N}} \infty$. *Thus,* $x \equiv_{\mathcal{N}} y$, *for any* $x, y \in \mathbb{N}$.

When $\mathcal{X}$ is order-respecting, $\equiv_{\mathcal{X}}$ can be seen as equating any two elements that are "indistinguishable" in the σ-field Σ.

Proposition 4.3 *Let* $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ *be an order-respecting measurable space. Then,* $x \equiv_{\mathcal{X}} y$ *if and only if for every* $B \in \Sigma$, $x \in B$ *iff* $y \in B$.

Proof. ($\Leftarrow$)-direction is immediate. To prove ($\Rightarrow$) direction, let $\mathcal{D}$ be the collection of all measurable downward closed sets, *i.e.*, $\mathcal{D} = \{D \in \Sigma \mid D \text{ is downward closed}\}$. Let $\mathcal{C}$ be the collection of subsets of X that can be written as the union of the intersection of sets in $\mathcal{D}$ and their complements. It is easy to see that $\mathcal{C}$ is a σ-algebra that contains $\mathcal{D}$. As $\mathcal{X}$ is order-respecting, it follows that $\Sigma \subseteq \mathcal{C}$. Therefore, any $B \in \Sigma$ can be written as the union of the intersection of sets in $\mathcal{D}$ and their complements. Thus, if $x \in B$ then there must be $P \subseteq \mathcal{D}$ and $N \subseteq \mathcal{D}$ such that $x \in \cap_{D \in P} D \cap \cap_{D \in N} (X \setminus D)$. In other words, $x \in D$ for every $D \in P$ and $x \notin D'$ for every $D' \in N$. Since $x \equiv_{\mathcal{X}} y$, it follows that $y \in D$ for every $D \in P$ and $y \notin D'$ for every $D' \in N$ and hence $y \in B$. □

Proposition 4.3 shows that in an order-respecting space, the equivalence classes of $\equiv_{\mathcal{X}}$ consist of elements that are indistinguishable in Σ. Hence we call such sets **atoms** of $\mathcal{X}$ and they form the constituents of our atom space.

Definition 4.4 For an order-respecting space $\mathcal{X} = (X, \Sigma, \sqsubseteq)$, the atom space of $\mathcal{X}$ is $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \Sigma_{\mathsf{At}(\mathcal{X})}, \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ where

- $(\mathsf{At}(\mathcal{X}), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ is the quotient space $(X, \sqsubseteq)/\equiv_{\mathcal{X}}$, *i.e.*, $\mathsf{At}(\mathcal{X})$ is set of equivalence classes of $\equiv_{\mathcal{X}}$, and for $\mathsf{A}, \mathsf{B} \in \mathsf{At}(\mathcal{X})$, $\mathsf{A} \sqsubseteq_{\mathsf{At}(\mathcal{X})} \mathsf{B}$ iff for some $x \in \mathsf{A}$, $y \in \mathsf{B}$, $x \trianglelefteq_{\mathcal{X}} y$, and
- $\Sigma_{\mathsf{At}(\mathcal{X})} = \mathcal{P}(\mathsf{At}(\mathcal{X}))$.

Example 4.5 *Recall the order-respecting measure space* $\mathcal{N} = (\mathsf{N}, \Sigma_{\mathsf{N}}, \sqsubseteq_{\mathsf{N}})$

given in Example 4.2. The set of atoms is $\mathsf{At}(\mathcal{N}) = \{\mathbb{N}, \{\infty\}\}$. *It is easy to see that* $\sqsubseteq_{\mathsf{At}(\mathcal{N})} = \{(\mathbb{N}, \infty), (\mathbb{N}, \mathbb{N}), (\infty, \infty)\}$.

Given that $(\mathsf{At}(\mathcal{X}), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ is the quotient space $(X, \sqsubseteq)/\equiv_{\mathcal{X}}$, the following observations are immediate consequences.

(I) $\mathsf{At}(\mathcal{X})$ is a partition of X, *i.e.*, distinct elements A and B of $\mathsf{At}(\mathcal{X})$ are disjoint, and $X = \cup_{\mathsf{A} \in \mathsf{At}(\mathcal{X})} A$.
(II) If X is countable then $\mathsf{At}(\mathcal{X})$ is countable.
(III) $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$ is a partial order.

Proposition 4.6 *Let* $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ *be a countable order-respecting space and* $\mathcal{D} = \{D \in \Sigma \mid D \text{ is } \sqsubseteq\text{-downward closed}\}$. *The following properties hold of the atom space* $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \Sigma_{\mathsf{At}(\mathcal{X})}, \sqsubseteq_{\mathsf{At}(\mathcal{X})})$.

(IV) For every $D \in \mathcal{D}$, $D = \cup_{\mathsf{A} \in \mathsf{At}(\mathcal{X}),\ \mathsf{A} \subseteq D} \mathsf{A}$.
(V) Every atom is measurable, i.e., $\mathsf{At}(\mathcal{X}) \subseteq \Sigma$.
(VI) Σ *is generated by the atoms,* i.e., $\sigma(\mathsf{At}(\mathcal{X})) = \Sigma$.
(VII) Given any function $\nu : \mathsf{At}(\mathcal{X}) \to [0, \infty]$, *there is a unique measure* $\mu : \Sigma \to [0, \infty]$ *such that* $\mu(\mathsf{A}) = \nu(\mathsf{A})$ *for each* $\mathsf{A} \in \mathsf{At}(\mathcal{X})$. *Furthermore, if* $\sum_{\mathsf{A} \in \mathsf{At}(\mathcal{X})} \nu(\mathsf{A}) = 1$ *then* μ *is a probability measure.*

Proof.

(IV) Follows from the fact that for $x \equiv_{\mathcal{X}} y$ and any $D \in \mathcal{D}$, either both x, y belong to D or neither one does.
(V) From the definition of the atoms, for $\mathsf{A} \in \mathsf{At}(\mathcal{X})$,

$$\mathsf{A} = \bigcap_{D \in \mathcal{D},\ \mathsf{A} \subseteq D} D \cap \bigcap_{D \in \mathcal{D},\ \mathsf{A} \subseteq (X \setminus D)} (X \setminus D).$$

Since X is countable, measurability of A follows from Proposition 2.2 and Proposition 3.7.
(VI) From observation (V) and the fact that Σ is a σ-algebra, we have that $\sigma(\mathsf{At}(\mathcal{X})) \subseteq \Sigma$. We need to show that $\Sigma \subseteq \sigma(\mathsf{At}(\mathcal{X}))$. As Σ is order-respecting, $\Sigma = \sigma(\mathcal{D})$ (Proposition 3.7). Hence we can conclude that $\Sigma \subseteq \sigma(\mathsf{At}(\mathcal{X}))$ if we can show that $\mathcal{D} \subseteq \sigma(\mathsf{At}(\mathcal{X}))$. Consider $D \in \mathcal{D}$. By observation (IV), we have $D = \cup_{\mathsf{A} \in \mathsf{At}(\mathcal{X}), A \subseteq D} \mathsf{A}$. Since the set of atoms is countable (observation (II)), we get that $D \in \sigma(\mathsf{At}(\mathcal{X}))$.
(VII) From Proposition 2.4 and the fact that $\mathsf{At}(\mathcal{X})$ is a partition of X (observation (I)), it follows that there is a unique extension μ of the function ν over $\sigma(\mathsf{At}(\mathcal{X}))$. The result then follows from observation (VI). □

One important step in establishing the isomorphism between $\mathcal{X}$ and its atom space, is to demonstrate a bijection between $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed sets and $\sqsubseteq$-downward closed sets in Σ. We will use the following definition to establish the bijection.

Definition 4.7 Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be a countable order-respecting measurable space. Let $D \in \Sigma$ be $\sqsubseteq$-downward closed and $\mathcal{A} \in \mathcal{P}(\mathsf{At}(\mathcal{X}))$ be $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed.

- Let $\mathsf{at}(D) \subseteq \mathsf{At}(\mathcal{X})$ be the set $\{\mathsf{A} \in \mathsf{At}(\mathcal{X}) \mid \mathsf{A} \subseteq D\}$.
- Let $\mathsf{st}(\mathcal{A}) \subseteq \mathcal{X}$ be the set $\cup_{\mathsf{A} \in \mathcal{A}} \mathsf{A}$.

The function at and st define the desired bijection between downward closed sets.

Lemma 4.8 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be a countable order-respecting measurable space. Let $D \in \Sigma$ be $\sqsubseteq$-downward closed and $\mathcal{A} \in \mathcal{P}(\mathsf{At}(\mathcal{X}))$ be $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed.*

(1) The set $\mathsf{at}(D)$ is $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed.
(2) The set $\mathsf{st}(\mathcal{A})$ is in Σ and is $\sqsubseteq$-downward closed.
(3) $\mathsf{st}(\mathsf{at}(D)) = D$ and $\mathsf{at}(\mathsf{st}(\mathcal{A})) = \mathcal{A}$.

Proof.

(1) Consider $\mathsf{A}, \mathsf{B} \in \mathsf{At}(\mathcal{X})$ such that $\mathsf{A} \sqsubseteq_{\mathsf{At}(\mathcal{X})} \mathsf{B}$, and $\mathsf{B} \in \mathsf{at}(D)$. Thus, $\mathsf{B} \subseteq D$. Consider $x \in \mathsf{A}$ and $y \in \mathsf{B}$. Since $x \trianglelefteq_{\mathcal{X}} y$ and $y \in D$, it follows that $x \in D$. Hence, $\mathsf{A} \subseteq D$ or $\mathsf{A} \in \mathsf{at}(D)$.
(2) Recall that if $x \sqsubseteq y$ then $x \trianglelefteq_{\mathcal{X}} y$. Hence it follows that $\mathsf{st}(\mathcal{A})$ is $\sqsubseteq$-downward closed.
(3) From observation (IV), $D = \cup_{\mathsf{A} \in \mathsf{at}(D)} \mathsf{A}$. Thus, $D = \mathsf{st}(\mathsf{at}(D))$.
Let $D_0 = \mathsf{st}(\mathcal{A}) = \cup_{\mathsf{A} \in \mathcal{A}} \mathsf{A}$. We first show that $\mathsf{at}(D_0) \subseteq \mathcal{A}$. Consider $\mathsf{B} \in \mathsf{at}(D_0)$. By definition, this means $\mathsf{B} \subseteq D_0$. Since atoms are disjoint (part (I)) and non-empty, $\mathsf{B} \in \mathcal{A}$ follows from the fact that $D_0 = \cup_{\mathsf{A} \in \mathcal{A}} \mathsf{A}$.
To show that $\mathcal{A} \subseteq \mathsf{at}(D_0)$, consider $\mathsf{B} \in \mathcal{A}$. Since $D_0 = \cup_{\mathsf{A} \in \mathcal{A}} \mathsf{A}$, we conclude that $\mathsf{B} \subseteq D_0$, which means that $\mathsf{B} \in \mathsf{at}(D_0)$. □

We now prove the main result of this section, namely, that $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ and $(\mathcal{M}_{=1}(\Lambda(\mathcal{X})), \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}})$ are isomorphic.

Theorem 4.9 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be a countable order-respecting measurable space and let $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \mathcal{P}(\mathsf{At}(\mathcal{X})), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ be its atom space. Then the posets $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ and $(\mathcal{M}_{=1}(\Lambda(\mathcal{X})), \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}})$ are isomorphic.*

Proof. Given any $\mu \in \mathcal{M}_{=1}(\mathcal{X})$, let $\widetilde{\mu}$ be the unique measure on $\mathcal{P}(\mathsf{At}(\mathcal{X}))$ such that $\widetilde{\mu}(\{\mathsf{A}\}) = \mu(\mathsf{A})$ for each $\mathsf{A} \in \mathsf{At}(\mathcal{X})$ (see Corollary 2.5 and Observation (II)). As $X = \cup_{\mathsf{A} \in \Lambda(\mathcal{X})} \mathsf{A}$ and atoms are pairwise disjoint,

$$\mu(X) = \sum_{\mathsf{A} \in \Lambda(\mathcal{X})} \mu(\mathsf{A}) = \sum_{\mathsf{A} \in \Lambda(\mathcal{X})} \widetilde{\mu}(\{\mathsf{A}\}).$$

Since μ is a probability measure,

$$\widetilde{\mu}(\mathcal{P}(\mathsf{At}(\mathcal{X}))) = \sum_{\mathsf{A}\in\Lambda(\mathcal{X})} \widetilde{\mu}(\{\mathsf{A}\}) = \sum_{\mathsf{A}\in\Lambda(\mathcal{X})} \mu(\mathsf{A}) = 1.$$

Let $\mathcal{R} : \mathcal{M}_{=1}(\mathcal{X}) \to \mathcal{M}_{=1}(\Lambda(\mathcal{X}))$ be the function defined as $\mathcal{R}(\mu) = \widetilde{\mu}$. We will show that $\mathcal{R}$ is an isomorphism of the posets $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ and $(\mathcal{M}_{=1}(\Lambda(\mathcal{X})), \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}})$.

First note that if $\mu_1, \mu_2 \in \mathcal{M}_{=1}(\mathcal{X})$ such that $\mu_1 \neq \mu_2$ then there must be an atom A such that $\mu_1(A) \neq \mu_2(A)$ (see observation (VII) of Proposition 4.6). Thus, if $\mu_1 \neq \mu_2$ then $\mathcal{R}(\mu_1) \neq \mathcal{R}(\mu_2)$. Also, if $\rho \in \mathcal{M}_{=1}(\mathsf{At}(\mathcal{X}))$ then consider the unique measure defined μ_0 on (X, Σ) defined as $\mu_0(A) = \rho(\{A\})$ (see observation (VII) of Proposition 4.6). By definition, $\mathcal{R}(\mu_0) = \rho$. Thus, $\mathcal{R}$ is a bijection. We just need to show that $\mu_1 \preceq_{\sqsubseteq} \mu_2$ iff $\widetilde{\mu_1} \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}} \widetilde{\mu_2}$ for each $\mu_1, \mu_2 \in \mathcal{M}_{=1}(\mathcal{X})$.

Assume first that $\mu_1 \preceq_{\sqsubseteq} \mu_2$. Now, let $\mathcal{A} \in \mathcal{P}(\mathsf{At}(\mathcal{X}))$ be an arbitrary $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed set. In order to conclude that $\widetilde{\mu_1} \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}} \widetilde{\mu_2}$, we need to show that $\widetilde{\mu_2}(\mathcal{A}) \leq \widetilde{\mu_1}(\mathcal{A})$. The latter is a consequence of following observations.

(1) For $i = 1, 2$, $\widetilde{\mu_i}(\mathcal{A}) = \sum_{\mathsf{A}\in\mathcal{A}} \mu_i(\mathsf{A})$.
(2) By Lemma 4.8, the set $\mathsf{st}(\mathcal{A}) = \cup_{\mathsf{A}\in\mathcal{A}}\mathsf{A}$ is $\sqsubseteq$-downward closed and contained in Σ. Since $\mu_1 \preceq_{\sqsubseteq} \mu_2$, we have $\mu_2(\mathsf{st}(\mathcal{A})) \leq \mu_1(\mathsf{st}(\mathcal{A}))$.
(3) Furthermore, as atoms are pairwise disjoint, we also have that $\mu_i(\mathsf{st}(\mathcal{A})) = \sum_{\mathsf{A}\in\mathcal{A}} \mu_i(\mathsf{A})$ for $i = 1, 2$.

Assume now that $\widetilde{\mu_1} \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}} \widetilde{\mu_2}$. Fix a $\sqsubseteq$-downward closed set $D \in \Sigma$. In order to conclude that $\mu_1 \preceq_{\sqsubseteq} \mu_2$, we need to show that $\mu_2(D) \leq \mu_1(D)$. The latter is a consequence of the following observations

(1) Consider the set $\mathsf{at}(D) = \{\mathsf{A} \in \mathsf{At}(\mathcal{X}) \mid \mathsf{A} \subseteq D\}$. By Lemma 4.8, $D = \cup_{\mathsf{A}\in\mathsf{at}(D)}\mathsf{A}$. Since atoms are disjoint, $\mu_i(D) = \sum_{\mathsf{A}\in\mathsf{at}(D)} \mu_i(\mathsf{A})$ for $i = 1, 2$.
(2) By Lemma 4.8, the set $\mathsf{at}(D)$ is $\sqsubseteq_{\mathsf{At}(\mathcal{X})}$-downward closed. Thus, $\widetilde{\mu_2}(\mathsf{at}(D)) \leq \widetilde{\mu_1}(\mathsf{at}(D))$. Now, $\widetilde{\mu_i}(\mathsf{at}(D)) = \sum_{\mathsf{A}\in\mathsf{at}(D)} \widetilde{\mu_i}(\{\mathsf{A}\})$ for $i = 1, 2$. By definition of $\widetilde{\mu_i}$, $\widetilde{\mu_i}(\{\mathsf{A}\}) = \mu_i(\mathsf{A})$. Thus, $\widetilde{\mu_i}(\mathsf{at}(D)) = \sum_{\mathsf{A}\in\mathsf{at}(D)} \mu_i(\mathsf{A})$. □

Example 4.10 *Recall the order-respecting measure space* $\mathcal{N} = (\mathsf{N}, \Sigma_{\mathsf{N}}, \sqsubseteq_{\mathsf{N}})$ *given in Example 4.2. The set of atoms is* $\mathsf{At}(\mathcal{N}) = \{\mathbb{N}, \{\infty\}\}$ *with* $\sqsubseteq_{\mathsf{At}(\mathcal{N})} = \{(\mathbb{N}, \infty), (\mathbb{N}, \mathbb{N}), (\infty, \infty)\}$. *Suppose* μ_1 *is a probability measure on* $\mathcal{N}$ *which assigns probability* $\frac{1}{2}$ *to* $\mathbb{N}$ *and* $\frac{1}{2}$ *to* $\{\infty\}$. *Let* $\mathcal{R} : \mathcal{M}_{=1}(\mathcal{N}) \to \mathcal{M}_{=1}(\Lambda(\mathcal{N}))$ *be the map as defined in the proof of Theorem 4.9. Now* $\widetilde{\mu_1}(\infty) = \frac{1}{2}$ *and* $\widetilde{\mu_1}(\mathcal{N}) = \frac{1}{2}$. *Let measure* μ *be the measure on* $\mathcal{N}$ *which assigns probability* $\frac{1}{4}$ *to* $\mathbb{N}$ *and* $\frac{3}{4}$ *to* $\{\infty\}$. *Now* $\widetilde{\mu}(\infty) = \frac{3}{4}$ *and* $\widetilde{\mu}(\mathcal{N}) = \frac{1}{4}$. *It is easy to see that* $\mu_1 \preceq_{\sqsubseteq} \mu$ *and that* $\widetilde{\mu_1} \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{N})}} \widetilde{\mu}$.

5 Least Upper Bounds for Probability Measures

Least upper bound constructions for elements in a partial order play a crucial role in defining the semantics of languages as well as in abstract interpretation. As we shall show later in this paper, least upper bounds of probability measures can also be used to define abstract models of probabilistic systems. Unfortunately, however, probability measures over arbitrary measurable spaces do not necessarily have least upper bounds; this is demonstrated by the following example.

Example 5.1 *Consider the space $\mathbb{T}$ defined in Example 3.4. Let μ be the probability measure that assigns probability $\frac{1}{2}$ to $\bot$ and l, and 0 to everything else. Let ν be such that it assigns $\frac{1}{2}$ to $\bot$ and r, 0 to everything else. The measure τ that assigns $\frac{1}{2}$ to $\top$ and $\bot$ is an upper bound of both μ and ν. In addition, ρ that assigns $\frac{1}{2}$ to l and r, and 0 to everything else, is also an upper bound. However τ and ρ are incomparable. Moreover, any lower bound of τ and ρ must assign a probability at least $\frac{1}{2}$ to $\bot$ and probability 0 to $\top$, and so cannot be an upper bound of μ and ν. Thus, μ and ν do not have a least upper bound.*

We, therefore, identify a special class of ordered measurable spaces over which probability measures admit least upper bounds.

Definition 5.2 An order-respecting measurable space $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ *admits least upper bounds* if the poset $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice.

We will give exact conditions (necessary and sufficient) for a countable, order-respecting measurable $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ to admit least upper bounds. Observe that for any countable order-respecting measurable space $\mathcal{X}$, its atom space $\Lambda(\mathcal{X})$ is a discrete space, and since the poset $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is isomorphic to the poset $(\mathcal{M}_{=1}(\Lambda(\mathcal{X})), \preceq_{\sqsubseteq_{\mathsf{At}(\mathcal{X})}})$ (see Theorem 4.9), exact conditions on discrete spaces, in fact, identify exact conditions on non-discrete spaces. Thus, in this section, we will focus our attention on countable, discrete measure spaces $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$, where (in addition) $\sqsubseteq$ is a partial order.

For the rest of the section, fix an ordered measurable space $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$, where $(X, \sqsubseteq)$ is a countable partial order. Recall that for any element $a \in X$, D_a is used to denote the principal $\sqsubseteq$-downward closed set $\{b \in X \mid b \sqsubseteq a\}$. We begin by defining a *tree-like* partial order; intuitively, these are partial orders whose Hasse diagram resembles a tree (rooted at its greatest element).

Definition 5.3 A partial order $(X, \sqsubseteq)$ is said to be *tree-like* if and only if (i) $(X, \sqsubseteq)$ is a join semi-lattice, and (ii) for any two elements $a, b \in X$ if $D_a \cap D_b \neq \emptyset$ then either $D_a \subseteq D_b$ or $D_b \subseteq D_a$.

Remark: In [4], we had defined tree-like partial orders to be those that (i) have a largest element $\top$, and (ii) for any two elements $a, b \in X$ if $D_a \cap D_b \neq \emptyset$ then either $D_a \subseteq D_b$ or $D_b \subseteq D_a$. Observe that though in general the definition presented here is stronger than the one in [4], for finite spaces they are equivalent. Our proof showing the necessity of tree-like posets demonstrates that the stronger definition (presented here) is required when moving to infinite spaces.

We will show that $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ admits least upper bounds iff $(X, \sqsubseteq)$ is tree-like. The rest of this section is organized as follows. We start by showing necessity of tree-like partial orders for the existence of least upper bounds (Section 5.1). Next, we show how to construct least upper bounds for *finite* measure spaces with a tree-like partial order (Section 5.2). Finally, in Section 5.3, we outline the proof ideas used in extending the result to (infinite) countable spaces. The proof for the countable case is the most involved one in this paper; hence, the formal details of the construction and proof of correctness are deferred to Appendix B to improve the readability of the paper.

5.1 Necessity of tree-like partial orders

Establishing the necessity of tree-like orders for the existence of upper bounds, proceeds in two parts. First we show that if $\mathcal{M}_{=1}(\mathcal{X})$ is a join semi-lattice then $(X, \sqsubseteq)$ is a join semi-lattice (Lemma 5.4). Next (Lemma 5.5), we show that this also implies that condition (ii) in the tree-like definition holds. For this second part, Example 5.1 is generalized to establish it. Recall that we are considering a countable space $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$.

Lemma 5.4 *If $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice, then $(X, \sqsubseteq)$ is a join semi-lattice.*

Proof. Assume that $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice. Let $S \subseteq X$ be any non-empty set. For each $a \in S$, let $\delta_a \in \mathcal{M}_{=1}(\mathcal{X})$ be the unique measure such that $\delta_a(\{a\}) = 1$ and $\delta_a(\{b\}) = 0$ for all $b \in X, b \neq a$. Let

$$\Gamma_S = \{\delta_a \mid a \in S\}.$$

Γ_S is non-empty (as S is non-empty). Hence the least upper bound of Γ_S exists. Let the least upper bound of Γ_S be μ_0. Let $S_0 \subseteq X$ be the set $\{b \in X \mid \mu_0(\{b\}) > 0\}$. Since μ_0 is a probability measure, S_0 is non-empty.

Fix $a_0 \in S_0$ and let $D_{a_0} = \{b \in X \mid b \sqsubseteq a_0\}$.

By definition $\mu_0(a_0) > 0$ and hence $\mu_0(D_{a_0}) > 0$. Now pick $a \in S$. Since μ_0 is the least upper bound of Γ_S, $\delta_a \preceq_{\sqsubseteq} \mu_0$. By Proposition 3.3, this implies that

$\delta_a(D_{a_0}) \geq \mu_0(D_{a_0}) > 0$. Now, $\delta_a(D_{a_0}) > 0$ iff $a \in D_{a_0}$. Thus, $a \in D_{a_0}$ and hence $a \sqsubseteq a_0$. Since a is an arbitrary element of S, we get that a_0 is an upper bound of S.

We claim that a_0 is the least upper bound of S (and hence S_0 consists of exactly one element). We proceed by contradiction. If a_0 is not the least upper bound of S, then there is an $a_1 \in X$ such that a_1 is an upper bound of S and $a_0 \not\sqsubseteq a_1$. Now, let μ_1 be the unique measure such that:

$$\mu_1(\{b\}) = \begin{cases} 0 & \text{if } b = a_0; \\ \mu_0(\{b\}) + \mu_0(\{a_0\}) & \text{if } b = a_1; \\ \mu_0(\{b\}) & \text{otherwise.} \end{cases}$$

We first show that μ_1 is an upper bound of Γ_S. Fix an arbitrary $\delta_a \in \Gamma_S$ and an arbitrary $\sqsubseteq$-upward closed set $U \subseteq X$. As μ_0 is an upper bound of Γ_S, we have that $\delta_a(U) \leq \mu_0(U)$. We also have, by definition, $\delta_a(U) > 0$ iff $a \in U$. Note that if $a \in U$, then as both a_0 and a_1 are upper bounds of S, $\mu_1(U) = \mu_0(U)$. Hence $\delta_a(U) \leq \mu_1(U)$ and therefore $\delta_a \preceq_{\sqsubseteq} \mu_1$ for each $\delta_a \in \Gamma_S$.

Now consider the $\sqsubseteq$-downward closed set $D_{a_1} = \{b \in X \mid b \sqsubseteq a_1\}$. Now, as $a_0 \not\sqsubseteq a_1$, we get that $a_0 \notin D_{a_1}$. This implies that $\mu_1(D_{a_1}) > \mu_0(D_{a_1})$. Thus, $\mu_0 \not\preceq_{\sqsubseteq} \mu_1$. But μ_0 is the least upper bound of Γ_S. A contradiction! $\square$

Example 5.1 can be generalized to show the following result.

Lemma 5.5 *If $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice, then for any two elements $a, b \in X$ if $D_a \cap D_b \neq \emptyset$ then either $D_a \subseteq D_b$ or $D_b \subseteq D_a$.*

Proof. Assume that $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice. We proceed by contradiction. Fix $a, b \in X$ such that $D_a \cap D_b \neq \emptyset$, $a \not\sqsubseteq b$ and $b \not\sqsubseteq a$. Fix $c \in D_a \cap D_b$. As $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice, Lemma 5.4 says that there is a $d \in X$ such that $a \sqsubseteq d$ and $b \sqsubseteq d$. Fix d. Clearly a, b, c and d are distinct elements.

Let $\mu_l, \mu_r \in \mathcal{M}_{=1}(\mathcal{X})$ be the probability measures such that $\mu_l(\{a\}) = \mu_l(\{c\}) = \frac{1}{2}$ and $\mu_r(\{b\}) = \mu_r(\{c\}) = \frac{1}{2}$. Let $\rho, \tau \in \mathcal{M}_{=1}(\mathcal{X})$ be such that $\rho(\{a\}) = \rho(\{b\}) = \frac{1}{2}$ and $\tau(\{c\}) = \tau(\{d\}) = \frac{1}{2}$. It is easy to check that $\mu_l, \mu_r \preceq_{\sqsubseteq} \tau$ and $\mu_l, \mu_r \preceq_{\sqsubseteq} \rho$.

Since $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice, there exists $\mu \in \mathcal{M}_{=1}(\mathcal{X})$ such that $\mu_l, \mu_r \preceq_{\sqsubseteq} \mu$ and $\mu \preceq_{\sqsubseteq} \tau, \rho$.

Note that for any $\sqsubseteq$-upward closed set U and $\nu \in \{\tau, \rho\}$, we have $\mu_l(U) \leq \mu(U) \leq \nu(U)$ (as $\mu_l \preceq_{\sqsubseteq} \mu \preceq_{\sqsubseteq} \nu$.) Let U_a be the $\sqsubseteq$-upward closed set

$\{e \in X \mid a \sqsubseteq e\}$. We have $\mu_l(U_a) = \rho(U_a) = \frac{1}{2}$. Thus, $\mu(U_a) = \frac{1}{2}$. Now consider the upward closed set $(U_a \setminus \{a\})$. The set $U_a \setminus \{a\}$ consists of all elements e such $e \neq a$ and $a \sqsubseteq e$. Thus, $d \in U_a \setminus \{a\}$ but $a, b, c \notin U_a \setminus \{a\}$. Therefore, $\mu_l(U_a \setminus \{a\}) = \rho(U_a \setminus \{a\}) = 0$. Hence $\mu(U_a \setminus \{a\}) = 0$. Therefore, $\mu(\{a\}) = \frac{1}{2}$. Similarly, $\mu(\{b\}) = \frac{1}{2}$. Hence, $\mu(U_a \cup U_b) = 1$. As $\mu \preceq_{\sqsubseteq} \tau$ also, $\tau(U_a \cup U_b) \geq 1$. But $\tau(U_a \cup U_b) = \frac{1}{2}$. A contradiction. □

The main result of this section now follows.

Theorem 5.6 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measure space such that $\sqsubseteq$ is a partial order. If $\mathcal{M}_{=1}(\mathcal{X})$ is a join semi-lattice, then $(X, \sqsubseteq)$ is a tree-like partial order.*

Proof. Follows from Lemmas 5.4 and 5.5. □

5.2 Upper bounds in Finite Tree-like Posets

In the previous section (Section 5.1), we showed that the existence of least upper bounds of probability measures implies that the underlying order on the universe is tree-like. We will now show that tree-like partial orders are in fact sufficient. The proof of this fact is very complicated, when we consider infinite spaces. In this section we, therefore, show how least upper bounds of probability measures can be constructed when the space is *finite*. This proof is simple, and highlights many of the intuitions behind the construction of least upper bounds in the more general case. The general case of countable spaces is considered in Section 5.3.

Theorem 5.7 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be an ordered measurable space such that X is finite, and $(X, \sqsubseteq)$ is tree-like. For any $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$, there is a probability measure $\nabla_{\sqsubseteq}(\Gamma)$ such that $\nabla_{\sqsubseteq}(\Gamma)$ is the least upper bound of Γ.*

Proof. Recall that for a set $S \subseteq X$, its set of maximal elements is denoted by maximal(S). Since X is finite, for any $\sqsubseteq$-downward closed set D, we have that $D = \cup_{a \in \text{maximal}(D)} D_a$. From condition (ii) of Definition 5.3, if a, b are two distinct maximal elements of a downward closed set D then $D_a \cap D_b = \emptyset$ and the sets comprising the union are pairwise disjoint. For any measure μ, we therefore have that $\mu(D) = \sum_{a \in \text{maximal}(D)} \mu(D_a)$ for any downward closed set D.

Define the function ν on downward closed subsets of X as follows. For a principal downward closed set of the form D_a, where $a \in X$, take

$$\nu(D_a) = \inf_{\mu \in \Gamma} \mu(D_a),$$

and for any downward closed set D take

$$\nu(D) = \sum_{a \in \text{maximal}(D)} \nu(D_a).$$

We will define the least upper bound measure $\nabla_{\sqsubseteq}(\Gamma)$ by specifying its value pointwise on each element of X. Observe that for any $a \in X$, the set $D_a \setminus \{a\}$ is also downward closed. We therefore define $\nabla_{\sqsubseteq}(\Gamma)(\{a\}) = \nu(D_a) - \nu(D_a \setminus \{a\})$, for any $a \in X$.

To complete the proof we need to show that $\nabla_{\sqsubseteq}(\Gamma)$ is the desired least upper bound of Γ. This requires us to establish that $\nabla_{\sqsubseteq}(\Gamma)$ is a probability measure. In other words, (a) $\nabla_{\sqsubseteq}(\Gamma)$ is well-defined, *i.e.*, $\nabla_{\sqsubseteq}(\Gamma)(\{a\}) \geq 0$ for every $a \in X$, and (b) $\nabla_{\sqsubseteq}(\Gamma)(X) = 1$. Finally, we need to show that (c) $\nabla_{\sqsubseteq}(\Gamma)$ is the least upper bound of Γ. We will establish each of these in order.

Observe that for all downward closed sets D, $\nu(D) \leq \inf_{\mu \in \Gamma} \mu(D)$. Furthermore, for each a and each $\mu \in \Gamma$, we have that $\mu(D_a) \geq \mu(D_a \setminus \{a\})$ implying that $\nu(D_a) \geq \inf_{\mu \in \Gamma} \mu(D_a \setminus \{a\}) \geq \nu(D_a)$. We therefore have that $\nabla_{\sqsubseteq}(\Gamma)(\{a\}) \geq 0$. Thus, $\nabla_{\sqsubseteq}(\Gamma)$ is well defined.

To complete the proof that $\nabla_{\sqsubseteq}(\Gamma)$ is a probability measure, we first establish that for any downward closed set D, $\nabla_{\sqsubseteq}(\Gamma)(D) = \nu(D)$. Notice that since $(X, \sqsubseteq)$ is tree-like and (therefore) for any measure μ, $\mu(D) = \sum_{a \in \text{maximal}(D)} \mu(D_a)$, we just need establish this for downward sets of the form D_a. This is done by induction on the number of descendants in Hasse diagram of $(X, \sqsubseteq)$. For $a \in \text{minimal}(X)$, $D_a \setminus \{a\} = \emptyset$, and so by definition, $\nabla_{\sqsubseteq}(\Gamma)(D_a) = \nu(D_a)$. For the inductive step, we have

$$\nabla_{\sqsubseteq}(\Gamma)(D_a) = \nabla_{\sqsubseteq}(\Gamma)(\{a\}) + \sum_{b \in \text{maximal}(D_a \setminus \{a\})} \nabla_{\sqsubseteq}(\Gamma)(D_b)$$

Now using the definition of $\nabla_{\sqsubseteq}(\Gamma)$ and the inductive hypothesis on the sets D_b, where $b \in \text{maximal}(D_a \setminus \{a\})$, we get that $\nabla_{\sqsubseteq}(\Gamma)(D_a) = \nu(D_a)$. Finally, observe that since $(X, \sqsubseteq)$ is tree-like (and hence a join semi-lattice), there is a largest element $\top \in X$. Using all our observations thus far, we get,

$$\nabla_{\sqsubseteq}(\Gamma)(X) = \nabla_{\sqsubseteq}(\Gamma)(D_\top) = \nu(D_\top) = \inf_{\mu \in \Gamma} \mu(D_\top) = 1$$

This completes the proof that $\nabla_{\sqsubseteq}(\Gamma)$ is a probability measure on $\mathcal{X}$.

For any downward closed set D, we have that $\nabla_{\sqsubseteq}(\Gamma)(D) = \nu(D)$ and $\nu(D) \leq \inf_{\mu \in \Gamma} \mu(D)$ which allows us to conclude that $\nabla_{\sqsubseteq}(\Gamma)$ is an upper bound of Γ. Now consider any measure τ that is an upper bound of Γ. Then, $\tau(D) \leq \mu(D)$ for any measure $\mu \in \Gamma$ and all downward closed sets D. In particular, for any element $a \in X$, $\tau(D_a) \leq \inf_{\mu \in \Gamma} \mu(D_a) = \nu(D_a) = \nabla_{\sqsubseteq}(\Gamma)(D_a)$. Thus, for any downward closed set D, we have that $\tau(D) = \sum_{a \in \text{maximal}(D)} \tau(D_a) \leq$

$\sum_{a \in \text{maximal}(D)} \nabla_{\sqsubseteq}(\Gamma)(D_a) = \nabla_{\sqsubseteq}(\Gamma)(D)$. Hence, $\nabla_{\sqsubseteq}(\Gamma) \preceq_{\sqsubseteq} \tau$, which concludes the proof. □

5.3 Upper bounds in Countable Tree-like Posets

Before extending the upper bound construction to countable spaces, let us recall the main ideas from the construction of finite spaces (Section 5.2). Let $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ be a non-empty set.

(1) Recall that $\mathsf{Princ}(\mathcal{X})$ is the set of all principal downward closed sets of X. Consider the map $\nu(\Gamma) : \mathsf{Princ}(\mathcal{X}) \to [0,1]$ as $\nu(\Gamma)(D_a) = \inf_{\mu \in \Gamma} \mu(D_a)$.
(2) Next, construct the upper bound $\nabla_{\sqsubseteq}(\Gamma) : \mathcal{P}(\mathcal{X}) \to [0,1]$ by defining it on single element sets and then extend it to $\mathcal{P}(\mathcal{X})$. For single element sets, $\nabla_{\sqsubseteq}(\Gamma)$ is defined as $\nabla_{\sqsubseteq}(\Gamma)(\{a\}) = \nu(D_a) - \sum_{b \in \text{maximal}(D_a \setminus \{a\})} \nu(D_b)$. Observe that here we have utilized the fact that X is finite which guarantees the existence of maximal elements of $D_a \setminus \{a\}$.
(3) Finally, we establish that $\nabla_{\sqsubseteq}(\Gamma)$ is a probability measure (i.e. $\nabla_{\sqsubseteq}(\Gamma)(X) = 1$) and is indeed the least upper bound of Γ. For this it suffices to show that for each $a \in X$, $\nabla_{\sqsubseteq}(\Gamma)(D_a) = \nu(\Gamma)(D_a) = \inf_{\mu \in \Gamma} \mu(D_a)$. The latter fact is shown by an easy induction; we first show it on the "leaf nodes" of the Hasse diagram of $(X, \sqsubseteq)$ and then proceed "upwards" in the partial order. Observe that this step also utilizes the fact that X is finite since it assumes existence of the "leaf" nodes.

Since steps 2 and 3 in the above construction depend on the fact that X is finite, the countable case has to be treated differently. The construction for the countable case will also extend the domain of $\nu(\Gamma)$ from $\mathsf{Princ}(\mathcal{X})$ to $\mathcal{P}(\mathcal{X})$; this will ensure that the extension enjoys the desired properties. Recall that a common technique employed to construct a measure by extension is to extend a measure on a semi-ring $\mathcal{C}$ to $\sigma(\mathcal{C})$ (see Theorem 2.3). In order to apply the theorem for our purposes, we thus have to first construct a semi-ring $\mathcal{C}$ such $\mathsf{Princ}(\mathcal{X}) \subseteq \mathcal{C}$ (note that $\mathsf{Princ}(\mathcal{X})$ is not a semi-ring), extend $\nu(\Gamma)$ to $\mathcal{C}$ and prove that the extension is a measure on the semi-ring $\mathcal{C}$. Since $\sigma(\mathsf{Princ}(\mathcal{X})) = \mathcal{P}(\mathcal{X})$ for countable X, we have thus extended $\nu(\Gamma)$ to a measure on $\mathcal{P}(\mathcal{X})$ and the extension will enjoy the desired properties. This plan is carried out as follows.

- We construct $\mathcal{C}$ as follows. First, we define $\mathsf{FinGen}(\mathcal{X})$ to be collection of subsets of X which can be written as a union of finite number of elements of $\mathsf{Princ}(\mathcal{X})$. The collection $\mathcal{C}$ is taken to be

$$\{D_a \setminus D \mid a \in X, D \subseteq D_a, \text{ and } D \in \mathsf{FinGen}(\mathcal{X})\}.$$

  The elements of $\mathcal{C}$ are called *finite difference sets* and $\mathcal{C}$ is shown to be

semi-ring in Appendix B.2.

- For any finite difference set A such that $A \neq \emptyset$, the tree-like structure of $(X, \sqsubseteq)$ implies that there is some unique $a \in X$, unique $k \geq 0$ and unique elements $a_1, a_2, \ldots a_k$ such that $\forall i, j.((i \neq j) \Rightarrow (D_{a_i} \cap D_{a_j} = \emptyset))$, $\forall i. a_i \sqsubseteq a$, $a_i \neq a$ and $A = D_a \setminus (\cup_{0 \leq i \leq k} D_{a_i})$. We say $\mathsf{Pos}(A) = \{a\}$ and $\mathsf{Neg}(A) = \{a_1, \ldots, a_k\}$. We extend $\nu(\Gamma)$ to $\mathcal{C}$ by defining $\nabla_{\sqsubseteq}(\Gamma)(A) = \nu(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}(A)} \nu(\Gamma)(D_b)$. This is carried out in Appendix B.3.

Next, we have to show that $\nabla_{\sqsubseteq}(\Gamma) : \mathcal{C} \to [0, 1]$ is a measure on the semi-ring. The most difficult part of the proof is to show that $\nabla_{\sqsubseteq}(\Gamma) : \mathcal{C} \to [0, 1]$ is countably additive. This is equivalent to showing that for each $a \in X$ and a countable collection of pairwise disjoint sets $\{A_i \mid i \in I\} \subseteq \mathcal{C}$ such that $A_i \neq \emptyset$ and $D_a = \cup_{i \in I} A_i$, it is the case that $\nabla_{\sqsubseteq}(\Gamma)(D_a) = \sum_{i \in I} \nabla_{\sqsubseteq}(\Gamma)(A_i)$. The proof of this part proceeds as follows. Let $\mathsf{Pos} = \cup_{i \in I} \mathsf{Pos}(A_i)$ and let $\mathsf{Neg} = \cup_{i \in I} \mathsf{Neg}(A_i)$.

(1) Since $a \in D_a$, there must be a $i_0 \in I$ such that $\mathsf{Pos}(A_{i_0}) = \{a\}$. Let $\mathsf{Pos}_0 = \{a\}$, $\mathsf{Neg}_0 = \mathsf{Neg}(A_{i_0})$, $F_0 = \{A_{i_0}\}$. Note that

$$\sum_{A \in F_0} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}_0} \nu(\Gamma)(D_b).$$

Let $D_0 = D_a$.

(2) From the tree-like structure of $(X, \sqsubseteq)$ and the fact $\mathsf{Neg}_0 \subseteq D_a$, we can show that for each $b \in \mathsf{Neg}_0$, there is a unique $i_b \in I$ such that $\mathsf{Pos}(A_{i_b}) = \{b\}$. Now, let $\mathsf{Pos}_1 = \mathsf{Neg}_0$, $\mathsf{Neg}_1 = \cup_{b \in \mathsf{Neg}_0} \mathsf{Neg}(A_{i_b})$ and $F_1 = \{A_{i_b} \mid b \in \mathsf{Neg}_0\}$. Let $D_1 = \cup_{b \in \mathsf{Pos}_1} D_b$. Note that $F_1 \cap F_0 = \emptyset$ and

$$\sum_{A \in F_0 \cup F_1} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}_0} \nu(\Gamma)(D_b) + \sum_{b \in \mathsf{Neg}_0} \nu(\Gamma)(D_b) - \sum_{b \in \mathsf{Neg}_1} \nu(\Gamma)(D_b)$$

We get that

$$\sum_{A \in F_0 \cup F_1} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}_1} \nu(\Gamma)(D_b)$$

and

$$\sum_{A \in F_0} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}_0} \nu(\Gamma)(D_b) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \nu(\Gamma)(D_1).$$

Note that $\mathsf{Pos}_1 \cap \mathsf{Pos}_0 = \emptyset$, and $D_1 \subseteq D_0$.

(3) Now we proceed as above, and for each $j \in \mathbb{N}$, construct sets Pos_j, Neg_j, D_j, and F_j such that for each $j \in \mathbb{N}$,

$$\sum_{A \in \cup_{1 \leq l \leq j} F_l} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \sum_{b \in \mathsf{Neg}_j} \nu(\Gamma)(D_b) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \nu(\Gamma)(D_{j+1}).$$

We also have $\mathsf{Pos}_{j+1} \subseteq \mathsf{Pos} \setminus (\cup_{0 \leq l \leq j} \mathsf{Pos}_l)$ and $D_{j+1} \subseteq D_j$.

(4) Now, if the set I is finite, we will get that there exists some j_0 such that $\mathsf{Neg}_{j_0} = \emptyset$, $D_{j_0+1} = \emptyset$ and $\cup_{1 \leq l \leq j_0} F_l = \{A_i \mid i \in I\}$ and we will get our countable additivity. However, if I is infinite then this process will go on. It is possible that even the collection $\cup_{1 \leq l \in \mathbb{N}} F_l \subsetneq \{A_i \mid i \in I\}$ and in that case we will obtain a decreasing sequence of sets $\{D_j \mid j \in \mathbb{N}\}$ such that

$$\sum_{A \in \cup_{l \in \mathbb{N}} F_l} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \lim_{j \to \infty} \nu(\Gamma)(D_j).$$

Furthermore, the set $\cap_{j \in \mathbb{N}} D_j$ is not empty if $\cup_{1 \leq l \in \mathbb{N}} F_l \subsetneq \{A_i \mid i \in I\}$.

(5) However, the sets $D_j s$ and $\cap_{j \in \mathbb{N}} D_j$ are of a special form. They are *canonically generated*. A set D is canonically generated if there is a (possibly infinite) set $S \subseteq X$ called the *generating set of* D such that $\forall b, c \in S.(b \neq c) \rightarrow ((D_b \cap D_c) = \emptyset)$ and $D = \cup_{b \in S} D_b$. The canonically generated sets form a Ψ-family (i.e., limit of decreasing sequences of canonically generated sets is also a canonically generated set; see Appendix B.1). Furthermore the natural extension of ν to canonically generated sets defined as $\nu(D) = \sum_{b \in S} \nu(D_b)$ preserves ω-limits (i.e., for any decreasing sequence C_j of canonically generated sets $\nu(\Gamma)(\cap_{j \in \mathbb{N}} C_j) = \lim_{j \to \infty} \nu(\Gamma)(C_j)$; see Appendix B.3). Thus, we get that

$$\sum_{A \in \cup_{l \in \mathbb{N}} F_l} \nabla_{\sqsubseteq}(\Gamma)(A) = \nabla_{\sqsubseteq}(\Gamma)(D_a) - \nu(\Gamma)(D_\omega)$$

where $D_\omega = \cap_{j \in \mathbb{N}} D_j$.

(6) We can show that if S_ω is the generating set of D_ω, then $S_\omega \subseteq \mathsf{Pos} \setminus \cup_{j \in \mathbb{N}} \mathsf{Pos}_j$. Furthermore for each $b \in \mathsf{Pos} \setminus \cup_{j \in \mathbb{N}} \mathsf{Pos}_j$, there is a $c \in S_\omega$ such that $b \sqsubseteq c$. So, now we take that $\mathsf{Pos}_\omega = S_\omega$, $I_\omega = \{i \in I \mid \mathsf{Pos}(A_i) \in S_\omega\}$, $\mathsf{Neg}_\omega = \{\mathsf{Neg}(A_i) \mid i \in I_\omega\}$, and $F_\omega = \{A_i \mid i \in I_\omega\}$.

(7) Now, we can construct the sequences for $\omega + 1$, $\omega + 2$, ... as in Step 2. When we approach a limit ordinal we construct the sequence as in steps 5 and 6. There must be a countable ordinal γ such that that $\mathsf{Pos}_\gamma = \emptyset$ (since X is countable) and we will get the desired result at γ.

This plan is carried out in detail in Appendix B and we have the following main result of the paper.

Theorem 5.8 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be a countable order-respecting measurable space and let $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \mathcal{P}(\mathsf{At}(\mathcal{X})), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ be its atom space. Then $\mathcal{X}$ admits least upper bounds iff $(\mathsf{At}(\mathcal{X}), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ is a tree-like partial order.*

6 Abstracting DTMCs and MDPs

In this section we outline how our upper bound construction can be used to abstract MDPs and DTMCs using DTMCs. We begin by recalling the definitions

of these models along with the notion of simulation and logic preservation in Section 6.1, before presenting our proposal in Section 6.2.

6.1 Preliminaries

We recall 3-valued PCTL [9] and its discrete time models. In 3-valued logic, a formula can evaluate to either *true* ($\top$), *false* ($\bot$), or *indefinite* (?); let $\mathbb{B}_3 = \{\bot, ?, \top\}$. The formulas of PCTL are built up over a finite set of atomic propositions AP and are inductively defined as follows.

$$\varphi ::= \text{true} \mid a \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathcal{P}_{\bowtie p}(X\varphi) \mid \mathcal{P}_{\bowtie p}(\varphi \,\mathcal{U}\, \varphi)$$

where $a \in \text{AP}$, $\bowtie \in \{<, \leq, >, \geq\}$, and $p \in [0, 1]$.

These formulas are interpreted over *Markov Decision Processes*, formally defined as follows. Let Q be a finite set of states and let $\mathcal{Q} = (Q, \mathcal{P}(Q))$ be the corresponding discrete measure space. A Markov Decision Process (MDP) $\mathcal{M}$ is a tuple $(Q, \rightarrow, L)$, where $\rightarrow \subseteq Q \times \mathcal{M}_{=1}(\mathcal{Q})$ (non-empty and finite), and $L : (Q \times \text{AP}) \rightarrow \mathbb{B}_3$ is a labeling function that assigns a value in $\mathbb{B}_3$ to each atomic proposition in each state. We will say $q \rightarrow \mu$ to mean $(q, \mu) \in \rightarrow$. A *Discrete Time Markov Chain* (DTMC) is an MDP with the restriction that for each state q there is exactly one probability measure μ such that $q \rightarrow \mu$. The 3-valued semantics of PCTL associates a truth value in $\mathbb{B}_3$ for each formula φ in a state q of the MDP; we denote this by $[\![q, \varphi]\!]_{\mathcal{M}}$. The formal semantics is similar to the semantics for AMCs given explicitly in [9], and can be found Appendix C. The proof of the following theorem, which is similar to a theorem for AMCs proved in [9] can also be found in Appendix C.

Theorem 6.1 *Given an MDP $\mathcal{M}$, and a PCTL formula φ, the value of $[\![q, \varphi]\!]_{\mathcal{M}}$ for each state q, can be computed in time polynomial in $|\mathcal{M}|$ and linear in $|\varphi|$, where $|\mathcal{M}|$ and $|\varphi|$ denote the sizes of $\mathcal{M}$ and φ, respectively.*

Simulation for MDPs, originally presented in [14] and adapted to the 3-valued semantics in [9], is defined as follows. A preorder $\sqsubseteq \subseteq Q \times Q$ is said to be a *simulation* iff whenever $q_1 \sqsubseteq q_2$ the following conditions hold.

- If $L(q_2, a) = \top$ or $\bot$ then $L(q_1, a) = L(q_2, a)$ for every proposition $a \in \text{AP}$,
- If $q_1 \rightarrow \mu_1$ then there exists μ_2 such that $q_2 \rightarrow \mu_2$ and $\mu_1 \preceq_{\sqsubseteq} \mu_2$, where μ_1 and μ_2 are viewed as probability measures over the ordered measurable space $(Q, \mathcal{P}(Q), \sqsubseteq)$.

We say $q_1 \preceq q_2$ iff there is a simulation $\sqsubseteq$ such that $q_1 \sqsubseteq q_2$.

Remark: The ordering on probability measures used in simulation definition

presented in [14,9] is defined using *weight functions*. However, the definition presented here is equivalent, as has been also observed in [8,26].

A state q_1 in an MDP $\mathcal{A}$ is simulated by a state q_2 in MDP $\mathcal{B}$ iff there is a simulation $\sqsubseteq$ on the direct sum of the two MDPs such that $(q_1, 0) \sqsubseteq (q_2, 1)$. Recall that the direct sum of $\mathcal{A}$ and $\mathcal{B}$ is defined as follows.

Definition 6.2 Given MDPs $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$ and $\mathcal{B} = (Q_{\mathcal{B}}, \rightarrow_{\mathcal{B}}, L_{\mathcal{B}})$, the direct sum of $\mathcal{A}$ and $\mathcal{B}$ denoted as $\mathcal{A} \uplus \mathcal{B}$ is the MDP $\mathcal{M} = \mathcal{A} \uplus \mathcal{B} = (Q_{\mathcal{M}}, \rightarrow, L_{\mathcal{M}})$ where $Q_{\mathcal{M}}, \rightarrow$ and $L_{\mathcal{M}}$ are defined as follows.

- $Q_{\mathcal{M}} = Q_{\mathcal{A}} \times \{0\} \cup Q_{\mathcal{B}} \times \{1\}$.
- $\rightarrow = \rightarrow_0 \cup \rightarrow_1$ where $\rightarrow_0, \rightarrow_1$ are defined as follows.

(1) For each $q \in Q_{\mathcal{A}}$ and $q \rightarrow_{\mathcal{A}} \mu$ we say that $(q, 0) \rightarrow_0 \mu \times \{0\}$ where $\mu \times \{0\}((q_1, 0)) = \mu(q_1)$ and $\mu \times \{0\}((q_1, 1)) = 0$.
(2) For each $q \in Q_{\mathcal{B}}$ and $q \rightarrow_{\mathcal{B}} \nu$ we say that $(q, 1) \rightarrow_1 \nu \times \{1\}$ where $\nu \times \{1\}((q_1, 0)) = 0$ and $\nu \times \{1\}((q_1, 1)) = \nu(q_1)$.

- $L_{\mathcal{M}}(q \times \{0\}) = L_{\mathcal{A}}(q)$ and $L_{\mathcal{M}}(q \times \{1\}) = L_{\mathcal{B}}(q)$.

Finally, there is a close correspondence between simulation and the satisfaction of PCTL formulas according to the 3-valued interpretation. The following result which is an adaptation of a similar result in [9] which establishes this correspondence; the proof of this result for MDPs can be found in Appendix C (Theorem C.4).

Theorem 6.3 (Fecher-Leucker-Wolf [9]) *Consider q, q' states of MDP $\mathcal{M}$ such that $q \preceq q'$. For any formula φ, if $[\![q', \varphi]\!]_{\mathcal{M}} \neq ?$ then $[\![q, \varphi]\!]_{\mathcal{M}} = [\![q', \varphi]\!]_{\mathcal{M}}$.*

6.2 Abstraction by DTMCs

Abstraction, followed by progressive refinement, is one way to construct a small model that either proves the correctness of the system or demonstrates its failure to do so. Typically, the abstract model is defined with the help of an equivalence relation on the states of the system. Informally, the construction proceeds as follows. For an MDP/DTMC $\mathcal{M} = (Q, \rightarrow, L)$ and equivalence relation $\equiv$ on Q, the abstraction is the MDP $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$, where $Q_{\mathcal{A}} = \{[q]_{\equiv} \mid q \in Q\}$ is the set of equivalence classes of Q under $\equiv$, and $[q]_{\equiv}$ has a transition corresponding to each $q' \rightarrow \mu$ for $q' \in [q]_{\equiv}$.

However, as argued by Fecher-Leucker-Wolf [9], model checking $\mathcal{A}$ directly may not be feasible because it has large number of transitions and therefore a large size. It maybe beneficial to construct a further abstraction of $\mathcal{A}$ and analyze the further abstraction. In what follows, we have an MDP, which maybe obtained as outlined above, that we would like to (further) abstract;

for the rest of this section let us fix this MDP to be $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$. We will first present the Fecher-Leucker-Wolf proposal, then ours, and compare the approaches, discussing their relative merits.

Fecher et al. suggest that a set of transitions be approximated by *intervals* that bound the probability of transitioning from one state to the next, according to any of the non-deterministic choices present in $\mathcal{A}$. The resulting abstract model, which they call an *Abstract Markov Chain* (AMC) is formally defined as follows.

Definition 6.4 The Abstract Markov Chain (AMC) associated with $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$ is formally the tuple $\mathcal{M} = (Q_{\mathcal{M}}, \rightarrow_{\ell}, \rightarrow_{u}, L_{\mathcal{M}})$, where $Q_{\mathcal{M}} = Q_{\mathcal{A}}$ is the set of states, and $L_{\mathcal{M}} = L_{\mathcal{A}}$ is the labeling function on states. The lower bound transition $\rightarrow_{\ell}$ and upper bound transition $\rightarrow_{u}$ are both functions of type $Q_{\mathcal{M}} \rightarrow (Q_{\mathcal{M}} \rightarrow [0,1])$, and are defined as follows:

$$q \rightarrow_{\ell} \mu \text{ iff } \forall q' \in Q_{\mathcal{M}}.\ \mu(q') = \min_{q \rightarrow_{\mathcal{A}} \nu} \nu(\{q'\})$$
$$q \rightarrow_{u} \mu \text{ iff } \forall q' \in Q_{\mathcal{M}}.\ \mu(q') = \max_{q \rightarrow_{\mathcal{A}} \nu} \nu(\{q'\})$$

Semantically, the AMC $\mathcal{M}$ is interpreted as an MDP having from each state q any transition $q \rightarrow \nu$, where ν is a probability measure that respects the bounds defined by $\rightarrow_{\ell}$ and $\rightarrow_{u}$. More precisely, if $q \rightarrow_{\ell} \mu_{\ell}$ and $q \rightarrow_{u} \mu_{u}$ then $\mu_{\ell} \leq \nu \leq \mu_{u}$, where $\leq$ is to be interpreted as pointwise ordering on functions.

Fecher et al. demonstrate that the AMC $\mathcal{M}$ (defined above) does indeed simulate $\mathcal{A}$, and using Theorem 6.3 the model checking results of $\mathcal{M}$ can be reflected to $\mathcal{A}$. The main advantage of $\mathcal{M}$ over $\mathcal{A}$ is that $\mathcal{M}$ can be model checked in time that is a polynomial in $2^{|Q_{\mathcal{M}}|} = 2^{|Q_{\mathcal{A}}|}$; model checking $\mathcal{A}$ may take time more than polynomial in $2^{|Q_{\mathcal{A}}|}$, depending on the number of transitions out of each state q.

We suggest using the upper bound construction, presented in Section 5.2, to construct *purely probabilistic* abstract models that do not have any non-determinism. Let $(X, \sqsubseteq)$ be a tree-like partial order. Recall that the set of minimal elements of X, denoted by minimal(X), is given by minimal$(X) = \{x \in X \mid \forall y \in X.\ y \sqsubseteq x \ \Rightarrow\ x = y\}$.

Definition 6.5 Consider the MDP $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$. Let $(Q, \sqsubseteq)$ be a tree-like partial order, such that minimal$(Q) = Q_{\mathcal{A}}$. Let $\mathcal{Q} = (Q, \mathcal{P}(Q), \sqsubseteq)$ be the ordered measurable space over Q. Define the DTMC $\mathcal{D} = (Q_{\mathcal{D}}, \rightarrow_{\mathcal{D}}, L_{\mathcal{D}})$, where

- $Q_{\mathcal{D}} = Q$,
- For $q \in Q_{\mathcal{D}}$, let $\Gamma_q = \{\mu \mid \exists q' \in Q_{\mathcal{A}}.\ q' \sqsubseteq q \text{ and } q' \rightarrow_{\mathcal{A}} \mu\}$. Now, $q \rightarrow_{\mathcal{D}} \nabla_{\sqsubseteq}(\Gamma_q)$, and

- For $q \in Q_{\mathcal{D}}$ and $a \in \text{AP}$, if for every $q_1, q_2 \in Q_{\mathcal{A}}$ with $q_1 \sqsubseteq q$ and $q_2 \sqsubseteq q$, we have $L(q_1, a) = L(q_2, a)$ then $L(q, a) = L(q_1, a)$. Otherwise $L(q, a) =?$

Lemma 6.6 *The DTMC $\mathcal{D}$ simulates the MDP $\mathcal{A}$, where $\mathcal{A}$ and $\mathcal{D}$ are as given in Definition 6.5.*

Proof. In order to show that $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$ is simulated by $\mathcal{D} = (Q_{\mathcal{D}}, \rightarrow_{\mathcal{D}}, L_{\mathcal{D}})$ we construct a simulation on the direct sum $\mathcal{M} = \mathcal{A} \uplus \mathcal{D} = (Q_{\mathcal{M}}, \rightarrow, L_{\mathcal{M}})$. Consider the relation $R_{\sqsubseteq}$ over the $Q_{\mathcal{M}} = Q_{\mathcal{A}} \times \{0\} \cup Q_{\mathcal{D}} \times \{1\}$, defined as $R_{\sqsubseteq} = \{((q,0),(q,0)) \mid q \in Q_{\mathcal{A}}\} \cup \{((q',1),(q'',1)) \mid q', q'' \in Q_{\mathcal{D}}, q' \sqsubseteq q''\} \cup \{((q,0),(q',1)) \mid q \in Q_{\mathcal{A}}, q' \in Q_{\mathcal{D}}, q \sqsubseteq q'\}$.

We claim that the relation $R_{\sqsubseteq}$ is a simulation relation. It can be checked easily that $R_{\sqsubseteq}$ is reflexive and transitive. It can also be checked that for any $s_1 R_{\sqsubseteq} s_2$, if $L_{\mathcal{M}}(s_2)(a) \neq ?$ then $L_{\mathcal{M}}(s_1)(a) = L_{\mathcal{M}}(s_2)(a)$ for each proposition a. We need to check that for any $s_1, s_2 \in Q_{\mathcal{A}} \times \{0\} \cup Q_{\mathcal{D}} \times \{1\}$, such that $s_1 R_{\sqsubseteq} s_2$, $s_1 \rightarrow \nu$ and $s_2 \rightarrow \nu'$, we have that $\nu \preceq_{R_{\sqsubseteq}} \nu'$. We shall show this statement for the case where $s_1 = (q,0)$ $s_2 = (q',1)$, $\nu = \mu \times \{0\}$ and $\nu' = \nabla_{\sqsubseteq}(\Gamma_{q'}) \times \{1\}$ for some $q \in Q_{\mathcal{A}}, q' \in Q_{\mathcal{D}}, q \rightarrow \nu, q' \rightarrow \nu'$. The case where $s_1 = (q,0)$ and $s_2 = (q,0)$ is trivial. The other case can be dealt with similarly.

We have, by definition, $q \sqsubseteq q'$, $q \rightarrow_{\mathcal{A}} \mu$ and $\Gamma_{q'} = \{\rho \mid \exists q'' \in Q_{\mathcal{A}}.\ q'' \sqsubseteq q' \text{ and } q'' \rightarrow_{\mathcal{A}} \rho\}$. In particular $\mu \in \Gamma_{q'}$.

It suffices to show that for any non-empty $R_{\sqsubseteq}$-downward closed set D we have $(\mu \times \{0\})(D) \geq (\nabla_{\sqsubseteq} \Gamma_{q'} \times \{1\})(D)$. Now, any non-empty downward closed set D of $R_{\sqsubseteq}$ is of the form $Q_1 \times \{0\} \cup Q_2 \times \{1\}$ such that $Q_1 \subseteq Q_{\mathcal{A}}$, Q_2 is $\sqsubseteq$-downward closed and $Q_2 \cap Q_{\mathcal{A}} \subseteq Q_1$. By definition, $(\mu \times \{0\})(D) = \mu(Q_1)$. Also, by definition $(\nabla_{\sqsubseteq}(\Gamma_{q'}) \times \{1\})(D) = \nabla_{\sqsubseteq}(\Gamma_{q'})(Q_2)$. Since Q_2 is $\sqsubseteq$-downward closed, $\mu \in \Gamma_{q'}$ and $\nabla_{\sqsubseteq}$ a least upper-bound operator, we have $\nabla_{\sqsubseteq}(\Gamma_{q'})(Q_2) \leq \mu(Q_2)$. But $\mu(Q_2) = \mu(Q_2 \cap Q_{\mathcal{A}}) \leq \mu(Q_1)$. The result follows. □

The minimality of our upper bound construction actually allows to conclude that $\mathcal{D}$ is as good as any DTMC abstraction can be on a given state space. This is stated precisely in the next lemma.

Lemma 6.7 *Let $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$ be an MDP and $(Q_{\mathcal{D}}, \sqsubseteq)$ be a tree-like partial order, such that* $\text{minimal}(Q_{\mathcal{D}}) = Q_{\mathcal{A}}$. *Consider the DTMC $\mathcal{D} = (Q_{\mathcal{D}}, \rightarrow_{\mathcal{D}}, L_{\mathcal{D}})$, as given in Definition 6.5. If $\mathcal{D}' = (Q_{\mathcal{D}}, \rightarrow_{\mathcal{D}'}, L_{\mathcal{D}'})$ is a DTMC such that the relation $R_{\sqsubseteq}$ defined in the proof of Lemma 6.6 is a simulation of $\mathcal{A}$ by $\mathcal{D}'$ then $\mathcal{D}'$ simulates $\mathcal{D}$ also.*

Proof. Given $q \in Q_{\mathcal{D}}$, let μ_q and μ'_q be the unique probability measures such that $q \rightarrow_{\mathcal{D}} \mu_q$ and $q \rightarrow_{\mathcal{D}'} \mu'_q$. We have by definition $\mu_q = \nabla_{\sqsubseteq}(\Gamma_q) = \{\nu \mid \exists q' \in Q_{\mathcal{A}}.\ q' \sqsubseteq q \text{ and } q' \rightarrow_{\mathcal{A}} \nu\}$.

Claim 1: For each $q, q' \in Q_{\mathcal{D}}$ such that $q \sqsubseteq q'$, $\mu_q \preceq_{\sqsubseteq} \mu'_{q'}$.

Proof of the claim: We first show that $\nabla_{\sqsubseteq}(\Gamma_{q'}) \preceq_{\sqsubseteq} \mu'_{q'}$. Pick $q_1 \in Q_{\mathcal{A}}$ and μ such that $q_1 \sqsubseteq q'$ and $q_1 \rightarrow_{Q_{\mathcal{A}}} \mu$. It suffices to show that $\mu \preceq_{\sqsubseteq} \mu'_{q'}$. Let $D \subseteq Q_{\mathcal{D}}$ be an arbitrary $\sqsubseteq$-downward closed set. Fix D. Please note that $\bar{D} = ((D \cap Q_{\mathcal{A}}) \times \{0\}) \cup (D \times \{1\})$ is a $R_{\sqsubseteq}$-downward closed set. Since $R_{\sqsubseteq}$ is simulation, we get that $\mu'_{q'}(D) \leq \mu(D \cap Q_{\mathcal{A}})$. But $\mu(D \cap Q_{\mathcal{A}}) = \mu(D)$ and hence $\mu \preceq_{\sqsubseteq} \mu'_{q'}$.

Therefore, $\nabla_{\sqsubseteq}(\Gamma_{q'}) \preceq_{\sqsubseteq} \mu'_{q'}$. We also have, by construction, that $\Gamma_q \subseteq \Gamma_{q'}$ for $q \sqsubseteq q'$. Hence, any upper bound of $\Gamma_{q'}$ is also an upper bound of Γ_q. Hence $\nabla_{\sqsubseteq}(\Gamma_q) \preceq_{\sqsubseteq} \nabla_{\sqsubseteq}(\Gamma_{q'})$. Thus, we get $\mu_q = \nabla_{\sqsubseteq}(\Gamma_q) \preceq_{\sqsubseteq} \mu'_{q'}$. $\Box$(**End proof of the claim.**)

Now, consider the relation $R \subseteq Q_{\mathcal{D}} \times \{0\} \cup Q_{\mathcal{D}} \times \{1\}$ defined as $R = \{((q_1, i), (q_2, j)) \mid q_1, q_2 \in Q_{\mathcal{D}}, i, j \in \{0, 1\}, i \leq j \text{ and } q_1 \sqsubseteq q_2\}$. We claim that R is a simulation relation on the DTMC $\mathcal{M}' = \mathcal{D} \uplus \mathcal{D}' = (Q_{\mathcal{M}'}, \rightarrow_{\mathcal{M}'}, L_{\mathcal{M}'})$, the direct sum of DTMC's $\mathcal{D}$ and $\mathcal{D}'$. Please note that R is a partial order. That R is a simulation follows from the following two observations.

Claim 2: For all $(q_1, i)\ R\ (q_2, j)$,

(1) If $L_{\mathcal{M}'}(q_2, j) \neq ?$ then $L_{\mathcal{M}'}(q_1, i) = L_{\mathcal{M}'}(q_2, j)$.
(2) If $(q_1, i) \rightarrow_{\mathcal{M}'} \mu_1$ and $(q_2, j) \rightarrow_{\mathcal{M}'} \mu_2$ then $\mu_1 \preceq_R \mu_2$.

Proof of the claim:

(1) Note that if $i = j = 0$ then the result follows from definition of $Q_{\mathcal{D}}$. If $j = 1$ then the result can be shown from the fact that $R_{\sqsubseteq}$ is simulation of $\mathcal{A}$ by $\mathcal{D}'$.
(2) Consider first the case $i = 0$ and $j = 1$. Then μ_1 is μ_{q_1} and μ_2 is μ'_{q_2}. By the claim 1, $\mu_{q_1} \preceq_{\sqsubseteq} \mu'_{q_2}$.

    Note that any R-downward closed set $\tilde{D}$ is of the form $D_1 \times \{0\} \cup D_2 \times \{1\}$ where D_1, D_2 are $\sqsubseteq$-downward closed and $D_2 \subseteq D_1$. We can conclude $\mu_1 \preceq_R \mu_2$ if we can show that $\mu_2(\tilde{D}) \leq \mu_1(\tilde{D})$. This follows from the following observations.
    (a) By definition, $\mu_1(\tilde{D}) = \mu_{q_1}(D_1)$ and $\mu_2(\tilde{D}) = \mu'_{q_2}(D_2)$.
    (b) Since $\mu_{q_1} \preceq_{\sqsubseteq} \mu'_{q_2}$, $\mu'_{q_2}(D_2) \leq \mu_{q_1}(D_2)$.
    (c) As $D_2 \subseteq D_1$, $\mu_{q_1}(D_2) \leq \mu_{q_1}(D_1)$ and hence $\mu'_{q_2}(D_2) \leq \mu_{q_1}(D_1)$.
    The claim for the case $i = j = 0$ follows from definition of $Q_{\mathcal{D}}$ and the the claim for $i = j = 1$ follows from the fact that $R_{\sqsubseteq}$ is a simulation of $\mathcal{A}$ by $\mathcal{D}'$. $\Box$

Observe that any tree-like partial order $(Q, \sqsubseteq)$ such that minimal$(Q) = Q_{\mathcal{A}}$ is of size at most $O(|Q_{\mathcal{A}}|)$; thus, in the worst case the time to model check $\mathcal{D}$ is exponentially smaller than the time to model check $\mathcal{M}$. Further, we have freedom to pick the partial order $(Q, \sqsubseteq)$. The following proposition says that adding more elements to the partial order on the abstract states does indeed result in a refinement.

Lemma 6.8 *Let $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\mathcal{A}}, L_{\mathcal{A}})$ be an MDP and $(Q_1, \sqsubseteq_1)$ and $(Q_2, \sqsubseteq_2)$ be tree-like partial orders such that $Q_1 \subseteq Q_2$, $\sqsubseteq_2 \cap (Q_1 \times Q_1) = \sqsubseteq_1$, and $Q_{\mathcal{A}} = \text{minimal}(Q_1) = \text{minimal}(Q_2)$. Let $\mathcal{D}_1$ be a DTMC over $(Q_1, \sqsubseteq_1)$ and $\mathcal{D}_2$ a DTMC over $(Q_2, \sqsubseteq_2)$ as in Definition 6.5. Then, $\mathcal{D}_1$ simulates $\mathcal{D}_2$.*

Proof. Given $q' \in Q_1$, let $D^1_{q'} \subseteq Q_1$ be the principal $\sqsubseteq_1$-downward closed set $\{q_1 \in Q_1 \mid q_1 \sqsubseteq_1 q'\}$ and $\pi(D^1_{q'}) \subseteq Q_2$ be the principal $\sqsubseteq_2$-downward closed set $\{q_2 \in Q_2 \mid q_2 \sqsubseteq_2 q'\}$. Since $(Q_1, \sqsubseteq_1)$ is tree-like, any $\sqsubseteq_1$-downward closed set D^1 can be written as a disjoint union $\cup_{q' \in \text{maximal}(D^1)} D^1_{q'}$ of principal $\sqsubseteq_1$-downward closed sets. Given $D^1 = \cup_{q' \in \text{maximal}(D^1)} D^1_{q'}$, let $\pi(D^1) = \cup_{q' \in \text{maximal}(D^1)} \pi(D^1_{q'})$. Clearly, $\pi(D^1)$ is a $\sqsubseteq_2$-downward closed set and $\pi(D^1_{q_a} \cap \pi(D^1_{q_b}) = \emptyset$ for $q_a, q_b \in \text{maximal}(D^1), q_a \neq q_b$.

Claim: Let $q_2 \in Q_2$ and $q_1 \in Q_1$ be such that $q_2 \sqsubseteq_2 q_1$ and let μ_2, μ_1 be such that $q_2 \rightarrow_{\mathcal{D}_2} \mu_2$ and $q_1 \rightarrow_{\mathcal{D}_1} \mu_1$. For any $\sqsubseteq_1$-downward closed set $D^1 \subseteq Q_1$, $\mu_1(D^1) \leq \mu_2(\pi(D^1))$.

Proof the claim: Note that $q_1 \in Q_2$. Let μ'_1 be such that $q_1 \rightarrow_{\mathcal{D}_2} \mu'_1$. Note that the construction of $\mathcal{D}_2$ ensures that $\mu_2 \preceq_{\sqsubseteq_2} \mu'_1$ and hence $\mu'_1(\pi(D^1)) \leq \mu_2(\pi(D^1))$. The result will follow once we show that $\mu'_1(\pi(D^1)) = \mu_1(D^1)$.

Since $D^1 = \cup_{q' \in \text{maximal}(D^1)} D^1_{q'}$, $\pi(D^1)$ is the disjoint union $\cup_{q' \in \text{maximal}(D^1)} \pi(D^1_{q'})$. Hence the desired result will follow if we can show that for each $\sqsubseteq_1$-principal downward closed set $D^1_{q'}$, $\mu'_1(\pi(D^1_{q'})) = \mu_1(D^1_{q'})$. Fix $q' \in Q_1$.

We proceed as follows. Let $\Gamma_{q_1} = \{\mu \mid \exists q_{\mathcal{A}} \in Q_{\mathcal{A}}.\ q_{\mathcal{A}} \sqsubseteq_1 q_1 \text{ and } q_{\mathcal{A}} \rightarrow_{\mathcal{A}} \mu\}$. By definition, $\mu_1(D^1_{q'}) = \inf_{\mu \in \Gamma_{q'}}(\mu(D^1_{q'}))$. Note that $\mu(D^1_{q'}) = \mu(D^1_{q'} \cap Q_{\mathcal{A}})$ for each $\mu \in \Gamma_{q_1}$. Hence, $\mu_1(D^1_{q'}) = \inf_{\mu \in \Gamma_q}(\mu(D^1_{q'} \cap Q_{\mathcal{A}}))$.

Let $\Gamma'_{q_1} = \{\mu \mid \exists q_{\mathcal{A}} \in Q_{\mathcal{A}}.\ q_{\mathcal{A}} \sqsubseteq_2 q_1 \text{ and } q_{\mathcal{A}} \rightarrow_{\mathcal{A}} \mu\}$. Now, as above $\mu'_1(\pi(D^1_{q'})) = \inf_{\mu \in \Gamma'_q}(\mu(\pi(D^1_{q'}) \cap Q_{\mathcal{A}}))$. The result now follows by observing that $\Gamma'_{q_1} = \Gamma_{q_1}$ and $D^1_{q'} \cap Q_{\mathcal{A}} = \pi(D^1_{q'}) \cap Q_{\mathcal{A}}$. $\square$(**End proof the claim**.)

We now proceed with the main Lemma. Consider the relation R on the DTMC $\mathcal{M} = \mathcal{D}_2 \uplus \mathcal{D}_1 = (Q_{\mathcal{M}}, \rightarrow_{\mathcal{M}}, L_{\mathcal{M}})$ defined as $R = \{((q,0),(q',0)) \mid q, q' \in Q_2, q \sqsubseteq_2 q'\} \cup \{((q,1),(q',1)) \mid q, q' \in Q_1, q \sqsubseteq_1 q'\} \cup \{((q,0),(q',1)) \mid q \in$

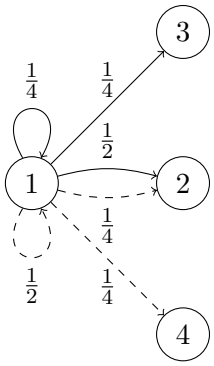

Fig. 2. Example MDP $\mathcal{A}$

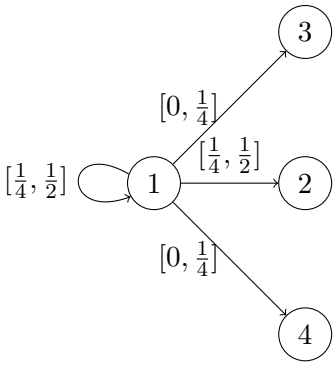

Fig. 3. AMC $\mathcal{M}$ corresponding to MDP $\mathcal{A}$

$Q_2, q' \in Q_1, q \sqsubseteq_2 q'\}$.

We claim that R is a simulation of $\mathcal{D}_2$ by $\mathcal{D}_1$. Please note that R is a partial order. It can be shown easily from the definition that if $(q,i)\ R\ (q',j)$ then $L_{\mathcal{M}}(q',j) \neq ?$ implies that $L_{\mathcal{M}}(q',j) = L_{\mathcal{M}}(q,i)$.

We need to show that if $(q,i)\ R\ (q',j)$, $(q,i) \to \mu$ and $(q',j) \to \mu'$ then $\mu \preceq_R \mu'$. We consider the case when $i = 0$ and $j = 1$. The other cases are straightforward consequences of the proof of Lemma 6.6.

We need to show that for any R-downward closed set D, $\mu'(D) \leq \mu(D)$. Fix D. Now if $(q,0)\ R\ (q',1)$ then $q \sqsubseteq_2 q'$ by definition. Also, if $(q,0) \to \mu$ and $(q',1) \to \mu'$ then by definition $\mu = \mu_2 \times \{0\}$ and $\mu' = \mu_1 \times \{1\}$, where μ_2 and μ_1 are such that $q \to_{\mathcal{D}_2} \mu_2$ and $q' \to_{\mathcal{D}_1} \mu_1$. Now, note since D is R-downward closed set, $D = D^2 \times \{0\} \cup D^1 \times \{1\}$ where

- D^2 is $\sqsubseteq_2$-downward closed,
- D^1 is $\sqsubseteq_1$-downward closed, and
- $\pi(D^1) \subseteq D^2$.

By definition $\mu(D) = \mu_2(D^2) \geq \mu_2(\pi(D^1))$ and $\mu'(D) = \mu_1(D^1)$. The result now follows from the above claim. □

Thus, one could potentially identify the appropriate tree-like partial order to be used for the abstract DTMC through a process of abstraction-refinement.

Finally, we can demonstrate that even though the DTMC $\mathcal{D}$ is exponentially more succinct (w.r.t. model-checking) than the AMC $\mathcal{M}$, there are examples where model checking $\mathcal{D}$ can give a more precise answer than $\mathcal{M}$.

Example 6.9 *Consider an MDP $\mathcal{A}$ shown in Fig. 2 where state 1 has two transitions one shown as solid edges and the other as dashed edges; transitions out of other states are not shown since they will not play a role. Suppose the atomic proposition a is $\top$ in $\{1,2\}$ and $\bot$ in $\{3,4\}$, and the proposition b is $\top$*

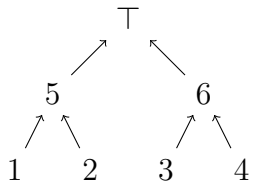

Fig. 4. Hasse diagram of partial order

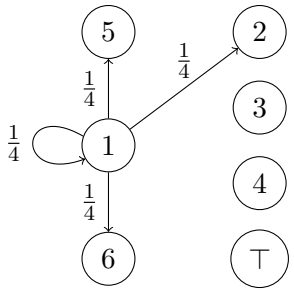

Fig. 5. Transition out of 1 in DTMC $\mathcal{D}$

in $\{1,3\}$ *and* $\bot$ *in* $\{2,4\}$. *The formula* $\varphi = \mathcal{P}_{\leq \frac{3}{4}}(Xa)$ *evaluates to* $\top$ *in state* 1.

The AMC $\mathcal{M}$ *as defined in Definition 6.4, is shown in Fig. 3. Now, because the distribution* ν, *given by* $\nu(\{1\}) = \frac{1}{2}$, $\nu(\{2\}) = \frac{1}{2}$, $\nu(\{3\}) = 0$, *and* $\nu(\{4\}) = 0$ *satisfies the bound constraints out of* 1 *but violates the property* φ, φ *evaluates to* ? *in state* 1 *of* $\mathcal{M}$.

Now consider the tree-like partial order shown in Fig. 4; arrows in the figure point from the smaller element to the larger one. If we construct the DTMC $\mathcal{D}$ *over this partial order as in Definition 6.5, the transition out of state* 1 *will be as shown in Fig. 5. Observe also that proposition* a *is* $\top$ *in* $\{1,2,5\}$, $\bot$ *in* $\{3,4,6\}$ *and* ? *in state* $\top$*; and proposition* b *is* $\top$ *in* $\{1,3\}$, $\bot$ *in* $\{2,4\}$ *and* ? *in* $\{5,6,\top\}$. *Now* φ *evaluates to* $\top$ *in state* 1, *because the measure of paths out of* 1 *that satisfy* $X\neg a$ *is* $\frac{1}{4}$. *Thus, by Theorem 6.3,* $\mathcal{M}$ *is not simulated by* $\mathcal{D}$. *It is useful to observe that the upper bound managed to capture the constraint that the probability of transitioning to either* 3 *or* 4 *from* 1 *is at least* $\frac{1}{4}$. *Constraints of this kind that relate to the probability of transitioning to a set of states, cannot be captured by the interval constraints of an AMC, but can be captured by upper bounds on appropriate partial orders.*

7 Detailed Examples

We discuss two examples, illustrating how the choice of the partial orders can effect the verification of 3-valued PCTL formulas. In order to carry out the computations we used the probabilistic model checker PRISM [18].

7.1 Random walk

Consider the upper-right quadrant of the integer plane, $\mathbb{P} = \{(i,j) \mid i,j \in \mathbb{N}\}$. Consider a random walk on $\mathbb{P}$. The random walker always moves to one of its

neighbors. At each position, the walker chooses to walk horizontally with probability $\frac{1}{2}$ and vertically with probability $\frac{1}{2}$. Once the walker chooses whether to walk horizontally or vertically, it has at most two possible choices. If there are two choices then it tosses another fair coin, otherwise it takes the only remaining choice. The random walk can be modeled as a DTMC with $\mathbb{P}$ as the set of states. The resulting DTMC is depicted in Figure 6.

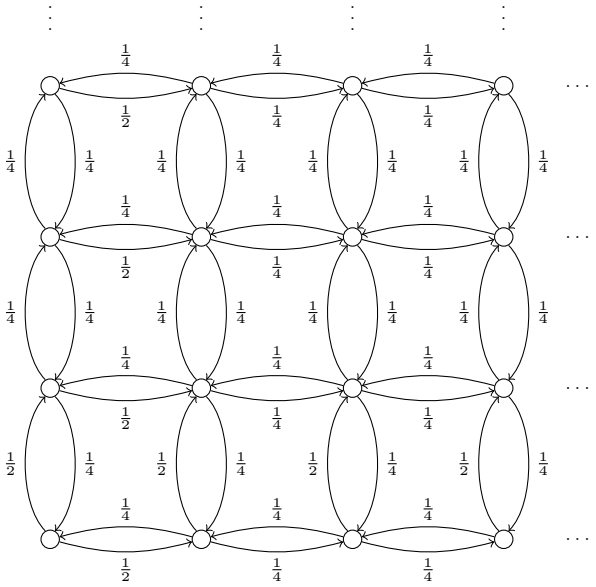

Fig. 6. Infinite state Markov chain with states (i, j); the bottom left corner is state $(0, 0)$. Transitions are determined by two fair coin tosses: first one decides whether to move in the x or the y direction, and the second one decides which direction (left/right or up/down) to move in.

Suppose that the random walker starts at position $(\lceil \frac{3k}{2} \rceil, 0)$ where k is some natural number ≥ 3, and we want to compute the probability that the walker reaches a position in the set $\{(i, 3) \mid i \in \mathbb{N}\}$ without first visiting the set $\{(0, j) \mid j \in \mathbb{N}\} \cup \{(3k + 1, j) \mid j \in \mathbb{N}\}$. Let u be the set $\{(i, j) \mid i \geq 0, j \geq 3\}$. Let ℓ and r be the sets $\{(0, j) \mid 0 \leq j \leq 2\}$ and $\{(i, j) \mid 0 \leq j \leq 2, i \geq 3k + 1\}$ respectively. Let a denote the proposition that is true in every state in u and false otherwise. Let b be the proposition that is true in every state in $\ell \cup r$ and false otherwise. We need to compute the measure of paths satisfying $\neg b \,\mathcal{U}\, a$.

While computing the exact measure of such paths might be daunting (especially if k is large), we can construct MDPs as described in Section 6.2 in order to obtain bounds on the measure. We discuss one such abstraction which aids us in obtaining a lower bound.

The abstract MDP $\mathcal{M}$ we construct consists of 12 abstract states $\ell, r, u, x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2$, and z_3. The states u, ℓ and r correspond to the sets u, ℓ, r as above. The states x_1, x_2, x_3 are obtained by dividing the set $\{(i, 0) \mid 1 \leq i \leq 3k\}$ into 3 equal parts; x_n is the set $\{(i, 0) \mid k(n - 1) + 1 \leq i \leq kn\}$. The states

y_1, y_2, y_3 are obtained by dividing the set $\{(i,1) \mid 1 \le i \le 3k\}$ andz_1, z_2, z_3 are obtained by dividing the set $\{(i,2) \mid 1 \le i \le 3k\}$ in a similar fashion.

The proposition a is true in state u and false in every other state of $\mathcal{M}$. The proposition b is true in states ℓ and r, and is false in every other state of $\mathcal{M}$. We do not describe the transitions explicitly here; instead we have given the PRISM code of $\mathcal{M}$ in Appendix D. The state x_2 is the initial state.

We computed the minimum measure of paths in the MDP satisfying $\neg b \,\mathcal{U}\, a$ using PRISM, which turns out to be 0.259 rounded to 3 decimal places. Hence the PCTL formula $\mathcal{P}_{\ge \frac{1}{4}}(\neg b \,\mathcal{U}\, a)$ evaluates to true in state x_2.

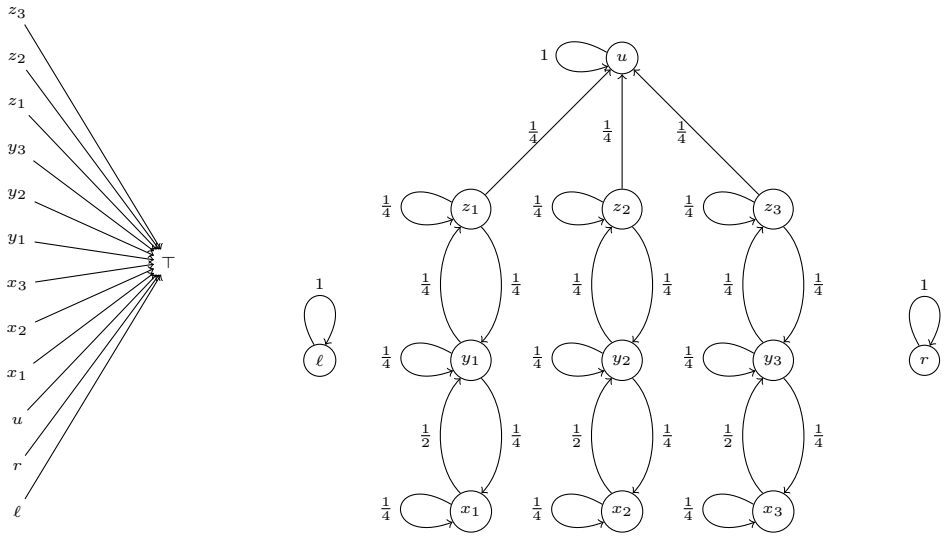

Fig. 7. Finite state DTMC abstraction of Figure 6. Abstract states are: $\ell = \{(0,j) \,|\, 0 \le j \le 2\}$, $r = \{(i,j) \,|\, i \ge 3k+1,\ 0 \le j \le 2\}$, $u = \{(i,j) \,|\, i \ge 0,\ j \ge 3\}$, $x_n = \{(i,0) \mid k(n-1)+1 \le i \le kn\}$, $y_n = \{(i,1) \mid k(n-1)+1 \le i \le kn\}$, $z_n = \{(i,2) \mid k(n-1)+1 \le i \le kn\}$. The Hasse diagram of the tree-like order is shown on the left; directed edge $a \to b$ indicates $a \le b$. The transition diagram (on the right) is constructed for the property, and so ℓ, r, u are absorbing states. $\top$, not shown in the picture is also an absorbing state, and all "missing" probability (of $\frac{1}{4}$) from x_n, y_n, and z_n go to $\top$.

Now, suppose we want to use our upper bound construction. A trivial way to build a tree-like order is to just add a state $\top$ to $\mathcal{M}$ which dominates all other states (see Figure 7). The propositions a and b are both ? in the state $\top$. The resulting DTMC is depicted in Figure 7. (Note that for computing the measure of the path formula $\neg b \,\mathcal{U}\, a$, we can take u, ℓ and r to be absorbing). Now, the measure of paths in which the formula $\neg b \,\mathcal{U}\, a$ evaluates to true for this DTMC is 0.111 rounded to 3 decimal places. The path formula $\neg b \,\mathcal{U}\, a$ almost surely evaluates to true or ?. Hence, the PCTL formula $\mathcal{P}_{\ge \frac{1}{4}}(\neg b \,\mathcal{U}\, a)$ evaluates to ? in state x_2.

Can we do better by refining this partial order? If we examine the DTMC

constructed then we observe that there is a transition from z_2 to $\top$ with probability $\frac{1}{4}$. The propositions a and b are ? in state $\top$. Furthermore, the state $\top$ is an absorbing state. Hence, the path formula $\neg b\,\mathcal{U}\,a$ evaluates to ? with probability 1 from this state. In the MDP $\mathcal{M}$, on the other hand, z_2 transits to only states from where the formula $\neg b\,\mathcal{U}\,a$ evaluates to true with non-zero probability. This causes a loss of precision (the same situation holds for x_2 and y_2). The transition to $\top$ from z_2 occurs because we have an "uncertainty" of transitioning to z_1, z_2, z_3 from z_2. This suggests introduction of a new state $z_\top$ which dominates z_1, z_2, z_3 and is dominated by $\top$. The advantage of introducing $z_\top$ is that the proposition b is false here (and hence more "defined"). Similarly, we can introduce $y_\top$ and $x_\top$. The resulting DTMC is depicted in Figure 8. Now, the measure of paths in which the formula $\neg b\,\mathcal{U}\,a$ evaluates to true for this DTMC is 0.259 rounded to 3 decimal places. Hence, the PCTL formula $\mathcal{P}_{\geq\frac{1}{4}}(\neg b\,\mathcal{U}\,a)$ evaluates to true in state x_2.

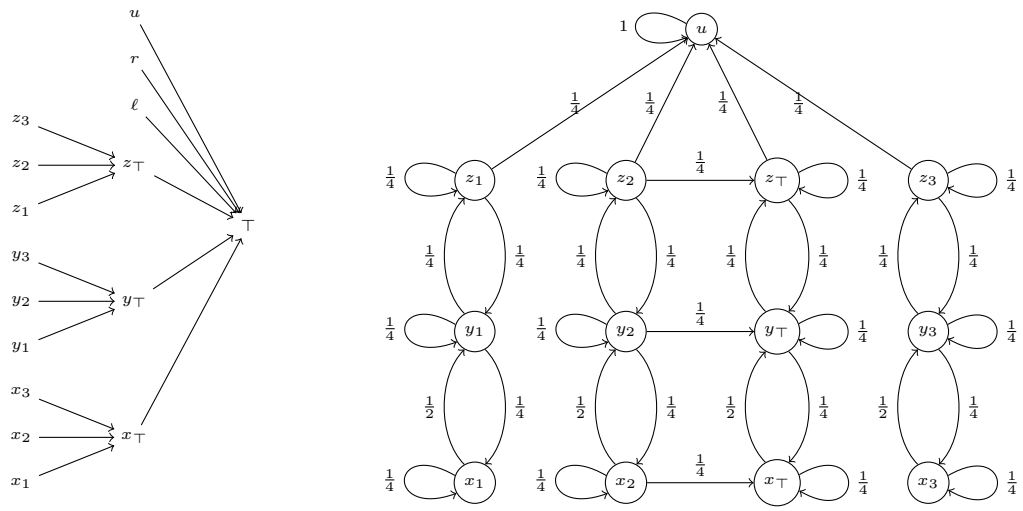

Fig. 8. DTMC after refining the tree-like order in Figure 7. The refined Hasse diagram is shown on the left. Once again, the transition diagram (on the right) is constructed for the property. The states ℓ, r, and $\top$ are absorbing and are not shown. All "missing" probability (of $\frac{1}{4}$) from $x_1, x_3, x_\top, y_1, y_3, y_\top, z_1, z_3$, and $z_\top$ go to $\top$.

For the MDP $\mathcal{M}$, when we construct the AMC as in Definition 6.4, we get that the minimum probability that the path formula $\neg b\,\mathcal{U}\,a$ evaluates to true with probability is 0.259 rounded to 3 decimal places. Hence, for this example, MDPs, DTMCs and AMCs all give the same answer.

7.2 Random walk with a phase transition

Now, consider the random walk on $\mathbb{P}$ which is similar to the one described in Section 7.1 except that there is a "phase transition" at some $k \geq 3$: for each

position (i, j) with $i > k$, the probability of moving left is $\frac{1}{8}$ (instead of $\frac{1}{4}$) and the remaining $\frac{1}{8}$ is divided evenly between going up and down (see Figure 9). Let a denote the proposition that is true in the state $(i, j) \in \mathbb{P}$ iff $j \geq 3$ and false otherwise. Let b be the proposition that is true in the state $(i, j) \in \mathbb{P}$ iff $i = 0, 0 \leq j \leq 2$ or $i \geq 2k + 1, 0 \leq j \leq 2$ and false otherwise. Assuming that the random walker starts at some position $(i, 0)$ with $1 \leq i \leq 2k$, we want to compute a lower bound on the measure of all paths satisfying $\neg b \, \mathcal{U} \, a$.

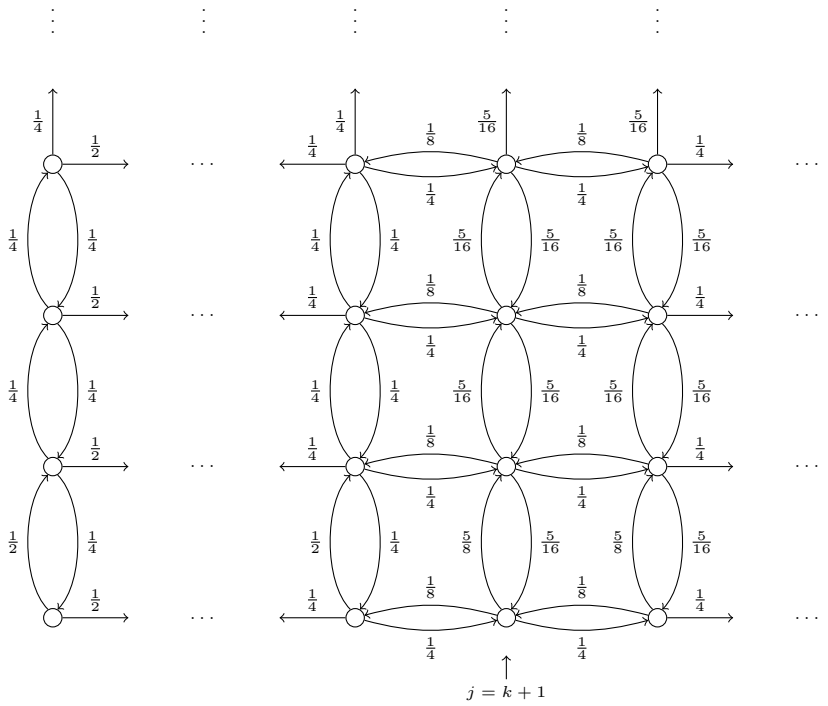

Fig. 9. Infinite state Markov chain similar to Figure 6 with a phase transition. All states (i, j) with $i \leq k$ behave like in Figure 6. States (i, j) with $i > k$ move left with probability $\frac{1}{8}$, and the remaining $\frac{1}{8}$ probability is divided evenly between going up and down.

In order to compute this, we construct an MDP abstraction $\mathcal{M}$ with 6 states, ℓ, r, u, x, y, z where $\ell = \{(0, j) \mid 0 \leq j \leq 2\}, r = \{(i, j) \mid i \geq 2k + 1, 0 \leq j \leq 2\}$, $u = \{(i, j) \mid i \geq 0, j \geq 3\}, x = \{(i, 0) \mid 1 \leq i \leq 2k\}, y = \{(i, 1) \mid 1 \leq i \leq 2k\}$ and $z = \{(i, 2) \mid 1 \leq i \leq 2k\}$. The PRISM code for the MDP is given in Appendix D.

The minimum measure of paths in MDP starting in x and satisfying $\neg b \, \mathcal{U} \, a$ gives a lower bound on the measure of paths satisfying $\neg b \, \mathcal{U} \, a$ in the actual random walk. PRISM tells us that this measure is 0.111 rounded to 3 decimal places.

Instead of MDP model checking, we can construct an AMC as in Definition 6.4. The resulting AMC is depicted in Figure 10. The minimum measure of all

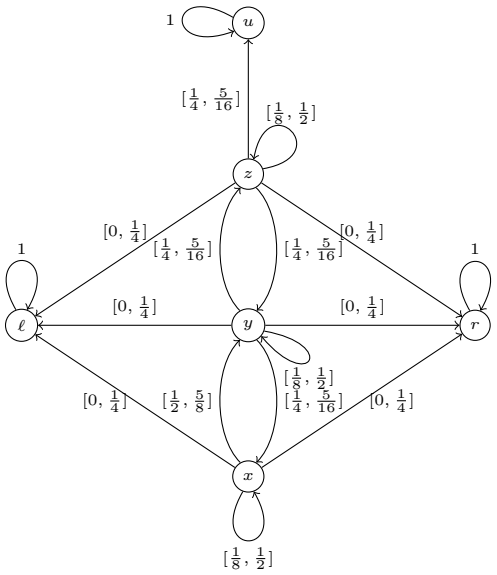

Fig. 10. AMC abstraction of Figure 9. Abstract states are: $\ell = \{(0, j) \mid 0 \leq j \leq 2\}$, $r = \{(i, j) | i \geq 2k{+}1,\ 0 \leq j \leq 2\}$, $u = \{(i, j) | i \geq 0,\ j \geq 3\}$, $x = \{(i, 0) | 1 \leq i \leq 2k\}$, $y = \{(i, 1) \mid 1 \leq i \leq 2k\}$, $z = \{(i, 2) \mid 1 \leq i \leq 2k\}$. The transition diagram of the AMC is constructed for the property, and so ℓ, r, u are absorbing states.

paths where $\neg b\ \mathcal{U}\ a$ evaluates to true in this case is 0.0618, rounded to 3 decimal places. The concrete DTMC that achieves this minimum probability has the following transitions: from each of x, y, z there is a probability $\frac{1}{4}$ of transitioning to ℓ and a probability $\frac{1}{8}$ of transitioning to r. All other transition probabilities are the minimum ones allowed by the respective intervals.

Hence, there is a gap between the results of model checking the MDP and model checking AMC. Can we do better with upper bound construction? If we start with the trivial tree-like order (see Figure 11) with one element $\top$ dominating all other states, we get the lower bound of 0.0618. This is the same answer given by AMC model checking. So, now we consider the question of refining this order.

If we examine the state z in the MDP, we realize that there is an "uncertainty" in transitioning to u, ℓ, r, z, y which appears in the form of transition to $\top$, where propositions a and b evaluate to ?. The uncertainty in transitioning to ℓ or r is not a problem for lower bound (for the most pessimistic case, we must assume that b becomes false as early as possible). The uncertainty in transitioning between u, z and y, however, causes a loss of precision. We can start accounting for this loss by further refining the partial order.

The first refinement that we consider accounts for uncertainty in transitioning between z and u. This is achieved by introducing an element u_z which dominates u and z. Note that the proposition b is false in u_z and the proposition a is ?. Using this partial order, we obtain, a minimum probability of 0.0665

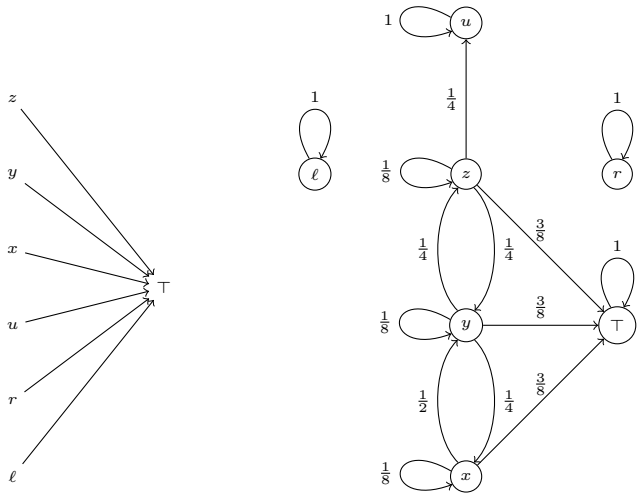

Fig. 11. DTMC constructed using the same abstract states as Figure 10. The Hasse diagram of the tree-like order is shown on the left. The transition diagram (on the right) is constructed for the property, and so ℓ, r, u are absorbing states.

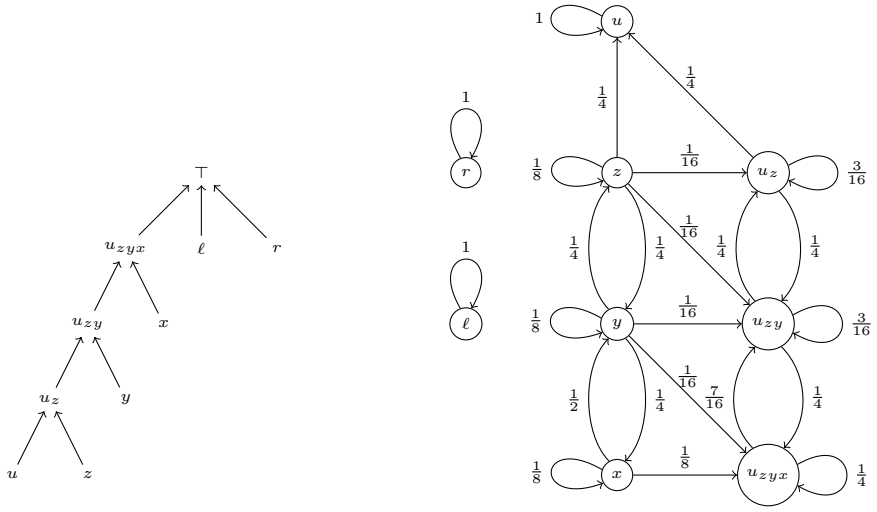

Fig. 12. DTMC after refining the tree-like order in Figure 11. The refined Hasse diagram is shown on the left. Once again, the transition diagram (on the right) is constructed for the property. The state $\top$ is not shown. It is absorbing, and all "missing" probability from states go to $\top$; thus, from x, y, z there is a transition with probability $\frac{1}{4}$ to $\top$, and from u_z, u_{zy}, u_{zyx} there is a transition with probability $\frac{5}{16}$ to $\top$.

rounded to 3 decimal places. This already improves the minimum probability obtained from AMC model checking. There is room for improvement, because we have not accounted for uncertainty in going to y. Thus, we add a state u_{zy} which dominates y and u_z. Finally, we can also add a state u_{zyx} which dominates x and u_{zy} (see Figure 12) which accounts for uncertainty in transitions

from x and y. The resulting DTMC on this partial order is depicted in Figure 12. For this DTMC, the minimum probability of satisfying $\neg b\,\mathcal{U}\,a$ turns out to be 0.0935 rounded to 3 decimal places. This significantly improves the lower bound from AMCs. In particular, the PCTL formula $\mathcal{P}_{\geq 0.090}(\neg b\ \mathcal{U}\ a)$ evaluates to true in this DTMC and ? in AMCs.

8 Abstracting CTMCs

We now outline how our upper bound construction gives us a way to abstract CTMC by other CTMCs. We begin with recalling the definitions of CTMCs, simulation and logical preservation, before presenting our abstraction scheme.

8.1 Preliminaries

The formulas of CSL are built up over a finite set of atomic propositions AP and are inductively defined as follows.

$$\varphi ::= \text{true} \mid a \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathcal{P}_{\bowtie p}(\varphi\,\mathcal{U}^t\,\varphi)$$

where $a \in \text{AP}$, $\bowtie \in \{<, \leq, >, \geq\}$, $p \in [0,1]$, and $t \in \mathbb{R}^+ \cup \{\infty\}$.

The 3-valued semantics of CSL is defined over *Continuous Time Markov Chains* (CTMC), where in each state every atomic proposition gets a truth value in $\mathbb{B}_3$. Formally, let Q be a finite set of states and let $\mathcal{Q} = (Q, \mathcal{P}(Q))$ be a measure space. A (uniform) CTMC [3] $\mathcal{M}$ is a tuple $(Q, \to, L, E)$, where $\to\colon Q \to \mathcal{M}_{=1}(\mathcal{Q})$, $L : (Q \times \text{AP}) \to \mathbb{B}_3$ is a labeling function that assigns a value in $\mathbb{B}_3$ to each atomic proposition in each state, and $E \in \mathbb{R}^+$ is the *exit rate* from any state. We will say $q \to \mu$ to mean $(q, \mu) \in \to$. The formal semantics of the CTMC is standard can be found in textbooks such as [24].

CSL's 3-valued semantics associates a truth value in $\mathbb{B}_3$ for each formula φ in a state q of the CTMC; we denote this by $[\![q, \varphi]\!]_{\mathcal{M}}$. The formal semantics can be found in [16]. The model checking algorithm presented in [1] for the 2-valued semantics, can be adapted to the 3-valued case.

Simulation for uniform CTMCs, originally presented in [3], has been adapted to the 3-valued setting in [16] and is defined in exactly the same way as simulation in a DTMC; since the exit rate is uniform, it does not play a role.

[3] We only look at uniform CTMCs here; in general, any CTMC can be transformed to a uniform one that is weakly bisimilar to the original CTMC. The size of CTMCs in terms of states and transitions remain the same; the numbers may change.

As before, we say q_1 is simulated by q_2, denoted as $q_1 \preceq q_2$, iff there is a simulation $\sqsubseteq$ such that $q_1 \sqsubseteq q_2$. Once again, there is a close correspondence between simulation and the satisfaction of CSL formulas according to the 3-valued interpretation.

Theorem 8.1 (Katoen-Klink-Leucker-Wolf [16]) *Consider any states q, q' of CTMC $\mathcal{M}$ such that $q \preceq q'$. For any formula φ, if $[\![q', \varphi]\!]_{\mathcal{M}} \neq ?$ then $[\![q, \varphi]\!]_{\mathcal{M}} = [\![q', \varphi]\!]_{\mathcal{M}}$.*

8.2 Abstracting based on Upper Bounds

Abstraction can, once again, be accomplished by collapsing concrete states into a single abstract state on the basis of an equivalence relation on concrete states. The transition rates out of a single state can either be approximated by intervals giving upper and lower bounds, as suggested in [16], or by upper bound measures as we propose. Here we first present the proposal of Abstract CTMCs, where transition rates are approximated by intervals, before presenting our proposal. We conclude with a comparison of the two approaches.

Definition 8.2 Consider a CTMC $\mathcal{M} = (Q_{\mathcal{M}}, \rightarrow_{\mathcal{M}}, L_{\mathcal{M}}, E_{\mathcal{M}})$ with an equivalence relation $\equiv$ on $Q_{\mathcal{M}}$. An *Abstract CTMC* (ACTMC) [16] that abstracts $\mathcal{M}$ is a tuple $\mathcal{A} = (Q_{\mathcal{A}}, \rightarrow_{\ell}, \rightarrow_{u}, L_{\mathcal{A}}, E_{\mathcal{A}})$, where

- $Q_{\mathcal{A}} = \{[q] \mid q \in Q_{\mathcal{M}}\}$ is the set of equivalence classes of $\equiv$,
- $E_{\mathcal{A}} = E_{\mathcal{M}}$,
- If for all $q_1, q_2 \in [q]$, $L_{\mathcal{M}}(q_1, a) = L_{\mathcal{M}}(q_2, a)$ then $L_{\mathcal{A}}([q], a) = L_{\mathcal{M}}(q, a)$. Otherwise, $L_{\mathcal{A}}([q], a) = ?$,
- $\rightarrow_{\ell}$: $Q_{\mathcal{A}} \rightarrow (Q_{\mathcal{A}} \rightarrow [0, 1])$ where

$$[q] \rightarrow_{\ell} \mu \text{ iff } \forall [q_1] \in Q_{\mathcal{A}}\ \mu([q_1]) = \min_{q' \in [q]\ \wedge\ q' \rightarrow_{\mathcal{A}} \nu} \nu([q_1])$$

- Similarly, $\rightarrow_{u}$: $Q_{\mathcal{A}} \rightarrow (Q_{\mathcal{A}} \rightarrow [0, 1])$ where

$$[q] \rightarrow_{u} \mu \text{ iff } \forall [q_1] \in Q_{\mathcal{A}}\ \mu([q_1]) = \max_{q' \in [q]\ \wedge\ q' \rightarrow_{\mathcal{A}} \nu} \nu([q_1]).$$

Semantically, at a state $[q]$, the ACTMC can make a transition according to any transition rates that satisfy the lower and upper bounds defined by $\rightarrow_{\ell}$ and $\rightarrow_{u}$, respectively.

Katoen et al. demonstrate that the ACTMC $\mathcal{A}$ (defined above) does indeed simulate $\mathcal{M}$, and using Theorem 8.1 the model checking results of $\mathcal{A}$ can be reflected to $\mathcal{M}$. The measure of paths reaching a set of states within a time bound t can be approximated using ideas from [2], and this can be used to

answer model checking question for the ACTMC (actually, the path measures can only be calculated upto an error).

Like in Section 6.2, we will now show how the upper bound construction can be used to construct (standard) CTMC models that abstract the concrete system. Before presenting this construction, it is useful to define how to lift a measure on a set with an equivalence relation $\equiv$, to a measure on the equivalence classes of $\equiv$.

Definition 8.3 Given a measure μ on $(Q, \mathcal{P}(Q))$ and equivalence $\equiv$ on Q, the lifting of μ (denoted by $[\mu]$) to the set of equivalence classes of Q is defined as $[\mu](\{[q]\}) = \mu(\{q' \mid q' \equiv q\})$.

Definition 8.4 Let $\mathcal{M} = (Q_{\mathcal{M}}, \rightarrow_{\mathcal{M}}, L_{\mathcal{M}}, E_{\mathcal{M}})$ be a CTMC with an equivalence relation $\equiv$ on $Q_{\mathcal{M}}$. Let $(Q, \sqsubseteq)$ be a tree-like partial order, such that $\text{minimal}(Q) = \{[q] \mid q \in Q_{\mathcal{M}}\}$. Let $\mathcal{Q} = (Q, \mathcal{P}(Q), \sqsubseteq)$ be the ordered measurable space over Q. Define the CTMC $\mathcal{C} = (Q_{\mathcal{C}}, \rightarrow_{\mathcal{C}}, L_{\mathcal{C}}, E_{\mathcal{C}})$, where

- $Q_{\mathcal{C}} = Q$,
- $E_{\mathcal{C}} = E_{\mathcal{M}}$,
- For $q \in Q_{\mathcal{C}}$, let $\Gamma_q = \{[\mu] \mid \exists q' \in Q_{\mathcal{A}}.\ [q'] \sqsubseteq q \text{ and } q' \rightarrow_{\mathcal{A}} \mu\}$. Now, $q \rightarrow_{\mathcal{C}} \nabla_{\sqsubseteq}\Gamma_q$, and
- If for all $q_1, q_2 \in Q_{\mathcal{M}}$ such that $[q_1] \sqsubseteq q$ and $[q_2] \sqsubseteq q$, $L_{\mathcal{M}}(q_1, a) = L_{\mathcal{M}}(q_2, a)$ then $L_{\mathcal{C}}(q, a) = L_{\mathcal{M}}(q_1, a)$. Otherwise, $L_{\mathcal{C}}(q, a) = ?$.

Once again, from the properties of least upper bounds, and definition of simulation, we can state and prove results analogous to Propositions 6.6 and 6.7. That is, the CTMC $\mathcal{C}$ does indeed abstract $\mathcal{M}$ and it is the best possible on a given state space; the formal statements and proofs are skipped.

Comparison with Abstract CTMCs. All the points made when comparing the DTMC abstraction with the AMC abstraction scheme, also apply here. That is, $\mathcal{C}$ is exponentially more succinct (w.r.t. model-checking) than ACTMC $\mathcal{A}$. Moreover, we can choose the tree-like partial order used in the construction of $\mathcal{C}$ through a process of abstraction refinement. And finally, Example 6.9 can be modified to demonstrate that there are situations where the CTMC $\mathcal{C}$ gives a more precise result than the ACTMC $\mathcal{A}$. However, in the context of CTMCs there is one further advantage. ACTMCs can only be model checked approximately, while CTMCs can be model checked exactly. While it is not clear how significant this might be in practice, from a theoretical point of view, it is definitely appealing.

9 Conclusions

Our main technical contribution is the construction of least upper bounds for probability measures on measure spaces equipped with a partial order. We have developed an exact characterization of the underlying orderings for which the induced ordering on probability measures admits the existence of least upper bounds, and provided a natural construction for defining them. We showed how these upper bound constructions can be used to abstract DTMCs, MDPs, and CTMCs by models that are purely probabilistic. In some situations, our abstract models yield more precise model checking results than previous proposals for abstraction. Finally, we believe that the absence of nondeterminism in the abstract models we construct might make their model-checking more practical.

In terms of future work, it would be important to evaluate how these abstraction techniques perform in practice. In particular, the technique of identifying the right tree-like state space for the abstract models using abstraction-refinement needs to be examined further.

References

[1] A. Aziz, K. Sanwal, V. Singhal, and R. Brayton. Model checking continuous-time Markov chains. *ACM Transactions on Computational Logic*, 1:162–170, 2000.

[2] C. Baier, B. Haverkort, H. Hermanns, and J.-P. Katoen. Efficient computation of time-bounded reachability probabilities in uniform continuous-time Markov decision processes. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 61–76, 2004.

[3] C. Baier, H. Hermanns, J.-P. Katoen, and V. Wolf. Comparative branching-time semantics for Markov chains. *Information and Computation*, 200:149–214, 2005.

[4] R. Chadha, M. Viswanathan, and R. Viswanathan. Least upper bounds for probability measures and their applications to abstractions. In *Proceedings of the International Conference on Concurrency Theory*, pages 264–278. Springer, 2008.

[5] P. Cousot and R. Cousot. Abstract Interpretation: A unified lattice model for static analysis of programs. In *Proceedings of the ACM Symposium on the Principles of Programming Languages*, pages 238–252, 1977.

[6] P. R. D'Argenio, B. Jeannet, H. E. Jensen, and K. G. Larsen. Reachability analysis of probabilistic systems by successive refinements. In *Proceedings of PROBMIV*, pages 39–56, 2001.

[7] P. R. D'Argenio, B. Jeannet, H. E. Jensen, and K. G. Larsen. Reduction and refinement strategies for probabilistic analysis. In *Proceeding of PROBMIV*, pages 57–76, 2002.

[8] J. Desharnais. *Labelled Markov Processes*. PhD thesis, McGill University, 1999.

[9] H. Fecher, M. Leucker, and V. Wolf. Don't know in probabilistic systems. In *Proceedings of SPIN*, pages 71–88, 2006.

[10] G.B. Folland. *Real Analysis: Modern Techniques and Their Applications*. Wiley-Interscience, 1984.

[11] M. Huth. An abstraction framework for mixed non-deterministic and probabilistic systems. In *Validation of Stochastic Systems: A Guide to Current Research*, pages 419–444. 2004.

[12] M. Huth. On finite-state approximants for probabilistic computation tree logic. *Theoretical Computer Science*, 346:113–134, 2005.

[13] C. Jones. *Probabilistic Non-determinism*. PhD thesis, University of Edinburgh, 1990.

[14] B. Jonsson and K. G. Larsen. Specification and refinement of probabilistic processes. In *Proceedings of the IEEE Symposium on Logic in Computer Science*, pages 266–277, 1991.

[15] Achim Jung and Regina Tix. The troublesome probabilistic powerdomain. In *Proceedings of Workshop on Computation and Approximation*, volume 13, pages 70 – 91, 1998.

[16] J.-P. Katoen, D. Klink, M. Leucker, and V. Wolf. Three-valued abstraction for continuous-time Markov chains. In *Proceedings of the International Conference on Computer-Aided Verifiction*, pages 311–324, 2007.

[17] M. Kwiatkowska, G. Norman, and D. Parker. Game-based abstraction for Markov decision processes. In *Proceedings of the International Conference on Quantitative Evaluation of Systems*, pages 157–166, 2006.

[18] M. Kwiatkowska, G. Norman, and D. Parker. PRISM 4.0: Verification of probabilistic real-time systems. In G. Gopalakrishnan and S. Qadeer, editors, *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)*, volume 6806 of *LNCS*, pages 585–591. Springer, 2011.

[19] A. McIver and C. Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer, 2004.

[20] D. Monniaux. Abstract Interpretation of Probabilistic Semantics. In *Proceedings of the International Static Analysis Symposium*, pages 322–339, 2000.

[21] D. Monniaux. Abstract interpretation of programs as Markov decision processes. *Science of Computer Programming*, 58:179–205, 2005.

[22] G. Norman. Analyzing randomized distributed algorithms. In *Validation of Stochastic Systems: A Guide to Current Research*, pages 384–418. 2004.

[23] A. Di Pierro and H. Wiklicky. Concurrent Constraint Programming: Towards Probabilistic Abstract Interpretation. In *Proceedings of the International ACM SIGPLAN Conference on Declarative Programming*, pages 127–138, 2000.

[24] J. J .M. M. Rutten, M. Kwiatkowska, G. Norman, and D. Parker. *Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems*. AMS, 2004.

[25] N. Saheb-Djahromi. Probabilistic LCF. In *Proceedings of the International Conference on the Mathematical Foundations of Computer Science*, pages 442–451, 1978.

[26] R. Segala. Probability and nondeterminism in operational models of concurrency. In *Proceedings of the International Conference on Concurrency Theory*, pages 64–78, 2006.

[27] K. Sen, M. Viswanathan, and G. Agha. Model checking Markov chains in the presence of uncertainties. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 394–410, 2006.

[28] B. Wachter, L. Zhang, and H. Hermanns. Probabilistic model checking modulo theories. In *Proceedings of the International Conference on Quantitative Evaluation of Systems*, pages 129–140, 2007.

[29] H.L.S. Younes, M. Kwiatkowska, G. Norman, and D. Parker. Numerical vs. statistical probabilistic model checking: An empirical study. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 46–60, 2004.

[30] H.L.S Younes and R.G. Simmons. Probabilistic verification of discrete event systems using acceptance sampling. In *Proceedings of the International Conference on Computer-Aided Verifiction*, pages 223–235, 2002.

A Additional Background Material

A.1 Sequences, limits and sums

Recall that a **sequence** [10] of elements of X is a function $f : \mathbb{N} \to X$. We will abuse notation and often denote a sequence f as an indexed collection $\{(f(j))_j \mid j \in \mathbb{N}\}$. (Note here the indexing will ensure that $(f(j))_j$ and $(f(j'))_{j'}$ are different for $j \neq j'$ even if $f(j) = f(j')$). Sometimes, we will be sloppy and not write the brackets around $f(j)$ in $(f(j))_j$. We generalize the notion to sequences to arbitrary ordinals as follows. Given an ordinal $\alpha > 0$, we say that an **α-sequence** of elements from X is a function from the set $\{\beta \mid \beta \text{ is a ordinal and } \beta < \alpha\}$ into the set X. We will abuse notation and often denote an α-sequence f as an indexed-collection $\{(f(\beta))_\beta \mid \beta < \alpha\}$. Note that with this definition, the traditionally defined sequences are ω-sequences where ω is the first infinite ordinal. For ω-sequences, we will often drop the qualifier ω.

An α-sequence $\{r_\beta \mid \beta < \alpha\}$ of real numbers is said to **increasing (decreasing)** if for all $\beta_1 < \beta_2$, $r_{\beta_1} \leq r_{\beta_2}$, ($r_{\beta_2} \leq r_{\beta_1}$, respectively). An α-sequence $\{r_\beta \mid \beta < \alpha\}$ of real numbers is said to **converge** to a real number r, denoted $r = \lim_{\beta \to \alpha} r_\beta$ if for each $\epsilon > 0$, there is a $\gamma < \alpha$ such that for all $\gamma \leq \beta < \alpha$, $|r_\beta - r| < \epsilon$. Note that if α is the successor ordinal $\gamma + 1$, then $\lim_{\beta \to \alpha} r_\beta$ exists and is equal to r_γ. For the case when α is ω, this coincides with the standard definition of limits. In that case we will write $r = \lim_{j \to \infty} r_j$. The following follows immediately from the properties of real numbers.

Proposition A.1 *If $\{r_\beta \mid \beta < \alpha\}$ is an increasing (decreasing respectively) sequence of real numbers such that $\{r_\beta \mid \beta < \alpha\}$ has an upper bound (lower bound respectively) then $\lim_{\beta \to \alpha} r_\alpha$ exists and is equal to $\sup(\{r_\beta \mid \beta < \alpha\})$ ($\inf(\{r_\beta \mid \beta < \alpha\})$ respectively).*

Given a set X, an α-sequence $\{A_\beta \mid \beta < \alpha\}$ of subsets of X is said to be **increasing (decreasing respectively)** if for all $\beta_1 < \beta_2$, $A_{\beta_1} \subseteq A_{\beta_2}$, ($A_{\beta_2} \subseteq A_{\beta_1}$, respectively). An increasing α-sequence $\{A_\beta \mid \beta < \alpha\}$ of subsets of X is said to **converge** to A, denoted $A = \lim_{\beta \to \alpha} A_\beta$ if $A = \cup_{\beta < \alpha} A_\alpha$. A decreasing sequence $\{A_\beta \mid \beta < \alpha\}$ of subsets of X converges to $A = \cap_{\beta < \alpha} A_\alpha$. Note that if α is the successor ordinal $\gamma + 1$, then $\lim_{\beta \to \alpha} A_\beta = A_\gamma$. For the case when α is ω, we will write $A = \lim_{j \to \infty} A_j$. The following proposition will be useful.

Proposition A.2 *If X is countable, then for any increasing (or decreasing) α-sequence $\{A_\beta \mid \beta < \alpha\}$ of subsets of X, there is a function $f : \mathbb{N} \to$*

$\{\beta \mid \beta < \alpha\}$ *such that* $j \leq k \Rightarrow f(j) \leq f(k)$ *and*

$$\lim_{\beta \to \alpha} A_\beta = \lim_{j \to \infty} A_{f(j)}.$$

Proof. If each A_β is $\emptyset$, the result is obvious. First assume that $\{A_\beta \mid \beta < \alpha\}$ is an increasing sequence and let $A = \cup_{\beta<\alpha} A_\beta$. Since X is countable, A is also countable. Let $a_0, a_1, a_2, \ldots$ be an enumeration of elements of A (with possible repetition). We construct f by induction. Let $f(0)$ be some β_0 such that $a_0 \in A_{\beta_0}$. Now assume that $f(j)$ has been defined for all $j \leq k$. Let f_{k+1} be β_{k+1} such that $\beta_{k+1} \geq f(k)$ and $a_{k+1} \in A_{\beta_{k+1}}$ (such a β can always be chosen as A_β is an increasing sequence). Clearly, f is the desired function.

If $\{A_\beta \mid \beta < \alpha\}$ is a decreasing sequence, then the sequence $\{A_0 \setminus A_\beta \mid \beta < \alpha\}$ is an increasing sequence. Then by the previous part, there is a function $f : \mathbb{N} \to \{\beta \mid \beta < \alpha\}$ such that $j < k \Rightarrow f(j) \leq f(k)$ and $\cup_{\beta<\alpha}(A_0 \setminus A_\beta) = \cup_{j\in\mathbb{N}}(A_0 \setminus A_{f(j)})$. Now, $\cap_{\beta<\alpha}(A_\beta) = A_0 \setminus (\cup_{\beta<\alpha}(A_0 \setminus A_\beta)) = A_0 \setminus (\cup_{j\in\mathbb{N}}(A_0 \setminus A_{f(j)})) = \cap_{j\in\mathbb{N}} A_{f(j)}$. The result follows. □

Now, given an indexed set $A = \{r_i \mid i \in I\}$ of positive real numbers, we say that A is **integrable** if the collection $\{\sum_{j\in J} r_j \mid j \in J, J \text{ is finite and } J \subseteq I\}$ has an upper bound in $\mathbb{R}^+$. If A is integrable we define $\sum_{r\in A} r = \sum_{i\in I} r_i = \sup\{\sum_{j\in J} r_j \mid j \in J, J \text{ is finite and } J \subseteq I\}$. This definition generalizes the standard definition of the sum of series $\sum_{j\in\mathbb{N}} r_j$. The following facts about sequences and real numbers follow from definition.

Proposition A.3 *Let* $\{r_\alpha \mid \alpha < \gamma\}$ *and* $\{s_\alpha \mid \alpha < \gamma\}$ *be two sequences of positive reals numbers.*

(1) If $r_\alpha < s_\alpha$ *for each* α, $\lim_{\alpha\to\gamma} r_\alpha = r$ *and* $\lim_{\alpha\to\gamma} s_\alpha = s$, *then* $r \leq s$.
(2) If $\lim_{\alpha\to\gamma} r_\alpha = r$ *and* $\lim_{\alpha\to\gamma} s_\alpha = s$ *then* $\lim_{\alpha\to\gamma}(r_\alpha + s_\alpha) = r + s$ $\lim_{\alpha\to\gamma}(r_\alpha - s_\alpha) = r - s$.
(3) If $s \leq r_\alpha < s_\alpha$ *for each* α *and* $\lim_{\alpha\to\gamma} s_\alpha = s$, *then* $\lim_{\alpha\to\gamma} r_\alpha = s$.
(4) If $\{r_\alpha \mid \alpha < \gamma\} \subseteq \mathbb{R}^+$ *is integrable then* $\{r_\alpha \mid \alpha < \beta\} \subseteq \mathbb{R}^+$ *is integrable for each* $\beta < \gamma$ *and* $\sum_{\alpha<\gamma} r_\alpha = \lim_{\beta\to\gamma}(\sum_{\alpha<\beta} r_\alpha)$.
(5) If $A = \{r_i \mid i \in I\} \subseteq \mathbb{R}^+$ *and* $B = \{s_i \mid i \in I\} \subseteq \mathbb{R}^+$ *are integrable and* $s_i \geq r_i$ *for each* i *then the set* $C = \{s_i - r_i \mid \in I\}$ *is integrable and* $\sum_{c\in C} c = (\sum_{b\in B} b) - (\sum_{a\in A} a)$.

Finally, recall that a doubly-indexed sequence of positive reals is a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{R}^+$. A doubly indexed sequence f will be denoted as the indexed collection $\{(f(i,j))_{i,j} \mid i, j \in \mathbb{N}\}$.

We conclude this section be recalling some useful results from the theory of integration, and proving a useful result. The reader is referred to [10] for details of this theory, but we recall some useful results from this theory here. First note that for any set X, the measurable space $\mathcal{X} = (X, \mathcal{P}(X))$ can

be equipped with a measure μ_{count}, called the **counting measure**, defined as follows. $\mu_{\mathsf{count}}(A)$ is the cardinality of the set A if A is finite, otherwise $\mu_{\mathsf{count}}(A)$ is ∞. A function $f : X \to \mathbb{R}^+$ is said to be μ_{count}**-integrable** if the indexed collection $\{(f(x))_x \mid x \in X\}$ is integrable and we write $\int f = \sum_{x \in X} f(x)$. A sequence $\{f_i \mid i \in \mathbb{N}\}$ of functions $f_i : X \to \mathbb{R}^+$ is said to converge to $f : X \to \mathbb{R}^+$ if $\lim_{i\to\infty} f_i(x) = f(x)$ for each $x \in X$. A well-known theorem on integrable functions is the Lebesgue dominated convergence theorem.

Theorem A.4 *Let (X, Σ) be a measurable space and $\mu : \Sigma \to \mathbb{R}^+ \cup \{\infty\}$ be a measure. Let $\{f_i \mid n \in \mathbb{N}\}$, $\{g_i \mid n \in \mathbb{N}\}$ be sequences of μ-measurable functions from X into the set of positive reals such that*

- *g_i is μ-integrable for each $i \in \mathbb{N}$,*
- *$f_i \leq g_i$ for each $i \in \mathbb{N}$,*
- *there is an μ-integrable function g such that $\lim_{i\to\infty} g_i = g$,*
- *$\lim_{i\to\infty} \int g_i = \int g$, and*
- *there is a function f such that $\lim_{i\to\infty} f_i = f$.*

Then f_i is μ-integrable for each i, f is μ-integrable and $\lim_{i\to\infty} \int f_i = \int f$.

We conclude this section by proving the following useful result.

Theorem A.5 *Let $\{r_{i,j} \mid i, j \in \mathbb{N}\} \subseteq \mathbb{R}^+$ and $\{s_{i,j} \mid i, j \in \mathbb{N}\} \subseteq \mathbb{R}^+$ be two doubly indexed sequences such that the following hold.*

- *$r_{i,j} \leq s_{i,j}$ for all $i, j \in \mathbb{N}$.*
- *For each j, $\lim_{i\to\infty} r_{i,j}$ and $\lim_{i\to\infty} s_{i,j}$ exist. Let $\lim_{i\to\infty} r_{i,j} = r_j$ and $\lim_{i\to\infty} s_{i,j} = s_j$*
- *For each i, the indexed set $\{s_{i,j} \mid j \in \mathbb{N}\}$ is integrable. The indexed set $\{s_j \mid j \in \mathbb{N}\}$ is integrable and $\lim_{i\to\infty} \sum_{j\in\mathbb{N}} s_{i,j} = \sum_{j\in\mathbb{N}} s_j$.*

Then for each i, the indexed set $\{r_{i,j} \mid j \in \mathbb{N}\}$ is integrable. The indexed set $\{r_j \mid j \in \mathbb{N}\}$ is also integrable and $\lim_{i\to\infty} \sum_{j\in\mathbb{N}} r_{i,j} = \sum_{j\in\mathbb{N}} r_j$.

Proof. The result follows from Theorem A.4 by taking X to be the set of natural numbers, Σ to be $\mathcal{P}(\mathbb{N})$, μ to be the counting measure, and f_i, g_j, f and g to be the functions defined as follows. [4] For each $j \in \mathbb{N}$, $f_i(j) = r_{i,j}, g_i(j) = s_{i,j}, f(j) = r_j$ and $g(j) = s_j$. □

[4] We have not defined measurable functions, but the definition ensures that if the Σ is the discrete measure space, then any function into the positive reals is measurable.

In mathematics, one often considers families of sets which are closed under certain operations. For us, collection of sets which are closed under limit operation will be important (actually we will only consider decreasing sequences for the limit operation).

Definition A.6 Given a set X, a collection of subsets $\mathcal{A} = \{A_i \mid i \in J, A_i \subseteq X\}$ is said to be **Ψ-family** if for any ordinal $\alpha > 0$ and any decreasing α-sequence $\{B_\beta \mid \beta < \alpha\}$ such that $B_\beta \in \mathcal{A}$ the set $\lim_{\beta\to\alpha} B_\beta \in \mathcal{A}$.

Note that for any collection of sets $\mathcal{A}$, set containment is a partial order.

Definition A.7 Given a set X and a Ψ-family $\mathcal{A} \subseteq \mathcal{P}(X)$, a function $f : \mathcal{A} \to \mathbb{R}$ is said to be *monotonic* if for $A, B \in \mathcal{A}$, $A \subseteq B \Rightarrow f(A) \leq f(B)$.

Now, for a Ψ-family $\mathcal{A}$, a monotonic function $f : \mathcal{A} \to \mathbb{R}$, a decreasing α-sequence $\{B_\beta \mid \beta < \alpha\}$, the sequence $\{f(B_\beta) \mid \beta < \alpha\}$ is decreasing and bounded below by $f(\lim_{\beta\to\alpha} B_\beta)$. Hence $\lim_{\beta\to\alpha} f(B_\beta)$ exists and is greater than or equal to $f(\lim_{\beta\to\alpha} B_\beta)$.

Definition A.8 Given a set X and a Ψ-family $\mathcal{A} \subseteq \mathcal{P}(X)$, a monotonic function $f : \mathcal{A} \to \mathbb{R}$ is said to be $\omega-$**continuous** if for any decreasing sequence $\{B_j \mid j \in \mathbb{N}\}$ of elements of $\mathcal{A}$, $\lim_{j\to\infty} f(B_j) = f(\lim_{j\to\infty} B_j)$. The function f is said to **continuous** if for any ordinal α and decreasing α-sequence $\{B_\beta \mid \beta < \alpha\}$ of elements of $\mathcal{A}$, $\lim_{\beta\to\alpha} f(B_\beta) = f(\lim_{\beta\to\alpha} B_\beta)$.

It turns out that for countable X and any Ψ-family $\mathcal{A} \subseteq \mathcal{P}(\mathcal{X})$, a monotonic function f is continuous iff f is ω-continuous.

Proposition A.9 *Let X be a countable set. Then for a Ψ-family $\mathcal{A} \subseteq \mathcal{P}(X)$ and monotonic $f : \mathcal{A} \to \mathbb{R}$, f is continuous iff f is ω-continuous.*

Proof. Clearly if f is continuous then f is ω-continuous.

Assume now that f is ω-continuous. Given an ordinal α and decreasing α-sequence $\{B_\beta \mid \beta < \alpha\}$ of elements of $\mathcal{A}$, fix a function $g : \mathbb{N} \to \{\beta \mid \beta < \alpha\}$ such that

- $j \leq k \Rightarrow g(j) \leq g(k)$ and
- $\lim_{\beta\to\alpha} B_\beta = \lim_{j\to\infty} B_{g(j)}$.

Such a function g exists thanks to Proposition A.2. Now, $\{B_{g(j)} \mid j \in \mathbb{N}\}$ is a decreasing sequence of sets in $\mathcal{A}$. Since f is ω-continuous we have $\inf_{j\in\mathbb{N}} f(B_{g(j)})$ $= f(\lim_{j\to\infty} B_{g(j)}) = f(\lim_{\beta\to\alpha} B_\beta)$. Now note that the collection $\{B_{g(j)} \mid j \in \mathbb{N}\}$ is a sub-collection of $\{B_\beta \mid \beta < \alpha\}$. Hence $\inf_{\beta<\alpha} f(B_\beta) \leq \inf_{j\in\mathbb{N}} f(B_{g(j)}) \leq$

$f(\lim_{\beta\to\alpha} B_\beta)$.

Note that since f is monotonic, for each $\beta < \alpha$, we also have $f(B_\beta) \geq f(\lim_{\beta\to\alpha} B_\beta)$. Hence $\inf_{\beta<\alpha} f(B_\beta) \geq f(\lim_{\beta\to\alpha} B_\beta)$. The result now follows. □

B Detailed Proof of Upper Bound Construction for the countable case

In this section, we the details of the proof steps sketched out in Section 5.3 to show that for a countable space $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ with $(X, \sqsubseteq)$ is a tree-like poset, the space $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice. For this section, the reader might find the additional background material presented in Appendix A, useful.

This section is organized as follows. We start by defining two $\Psi-$families on tree-like partial orders (Section B.1). Recall that given a set X, a Ψ-family is a collection of subsets of X which are closed under the limit operation on decreasing sequences of sets. Next, we show that collection of finite difference sets forms a semi-ring, in Section B.2. Finally, the construction of the upper bound along with its proof of correctness is presented in Section B.3.

B.1 Two Ψ-families

Recall that $\mathsf{Princ}(\mathcal{X})$ is the set of all principal downward closed sets of X. For tree-like partial orders $\mathcal{P} = \emptyset \cup \mathsf{Princ}(\mathcal{X})$ is a Ψ-family.

Proposition B.1 *Let $\mathcal{X} = (X, \sqsubseteq)$ be a tree-like partial order. Then $\mathcal{P} = \emptyset \cup \mathsf{Princ}(\mathcal{X})$ is a Ψ-family.*

Proof. Let $\{D_\alpha \mid \alpha < \gamma\}$ be a γ-sequence of decreasing sets in $\mathcal{P}$. If $D_\alpha = \emptyset$ for any α then $\lim_{\alpha\to\gamma} D_{a_\alpha} = \emptyset \in \mathcal{P}$.

Hence the interesting case is when for each $\alpha < \gamma$, $D_\alpha = D_{a_\alpha}$ for some $a_\alpha \in X$. Note that if $\lim_{\alpha\to\gamma} D_{a_\alpha} = \bigcap_{\alpha<\gamma} D_{a_\alpha} \neq \emptyset$, then the set $\{a_\alpha \mid \alpha < \gamma\}$ has a lower-bound and hence a greatest lower bound $c \in X$ (see Proposition 2.1). It is easy to see that $\lim_{\alpha\to\gamma} D_{a_\alpha} = \bigcap_{\alpha<\gamma} D_{a_\alpha} = D_c \in \mathcal{P}$. □

Another Ψ-family is the collection of downward closed sets that can be written as a disjoint union of principal downward closed sets.

Definition B.2 Given a poset $(X, \sqsubseteq)$, we say that a $\sqsubseteq$-downward closed set D is *canonically generated* if there is a set $S \subseteq X$ such that $D = \cup_{a\in S} D_a$ and $D_a \cap$

$D_b = \emptyset$ for each $a, b \in S, a \neq b$. The set S is said to be a *canonical generating set* of D. We denote the set of all canonically generated $\sqsubseteq$-downward closed sets by $\mathsf{CanGen}(\mathcal{X})$.

Please note that $\emptyset$ is a canonically generated set with the $\emptyset$ as the generating set. The following proposition states that canonical generating sets are unique.

Proposition B.3 *Given a poset $(X, \sqsubseteq)$, a set $D \in \mathsf{CanGen}(\mathcal{X})$. If S is a canonical generating set of D then $S = \text{maximal}(D)$. Hence if S_1 and S_2 are canonical generating sets of D then $S_1 = S_2$.*

Proof. Since S is a canonical generating set of D, we have $D = \cup_{a \in S} D_a$. Furthermore $(D_a \cap D_b \neq \emptyset) \Rightarrow (a = b)$.

Fix $a \in S$. If there is a $b \in D$ such that $a \sqsubseteq b$, then there must be a $b' \in S$ such that $b \sqsubseteq b'$. Thus, we have $a \sqsubseteq b \sqsubseteq b'$. Now, $a \in D_a \cap D_{b'}$. Thus $a = b'$ and hence $a = b$. Therefore $S \subseteq \text{maximal}(D)$.

Fix $b \in \text{maximal}(D)$. There is an $a \in S$ such that $b \sqsubseteq a$. But b is maximal. Hence $b = a$. Thus $\text{maximal}(D) \subseteq S$ also. □

For tree-like partial orders, the set of canonically generated sub-sets is a Ψ-family.

Proposition B.4 *Let $(X, \sqsubseteq)$ be a tree-like partial order. Then $\mathsf{CanGen}(\mathcal{X})$ is a Ψ-family.*

Proof. Let $\{D_\alpha \mid \alpha < \gamma\}$ be a γ-sequence of decreasing sets in $\mathsf{CanGen}(\mathcal{X})$. If $\cap_{\alpha<\gamma} D_\alpha = \emptyset$ then $\lim_{\alpha \to \gamma} D_{a_\alpha} = \emptyset \in \mathsf{CanGen}(\mathcal{X})$.

Assume that $\cap_{\alpha<\gamma} D_\alpha \neq \emptyset$ and for each $\alpha < \gamma$, let S_α be the generating set of D_α.

Claim: Let $a, b \in \cap_{\alpha<\gamma} D_\alpha \neq \emptyset$.

(1) For each $\alpha < \gamma$ there is a unique $a_\alpha \in S_\alpha$ such that $a \in D_{a_\alpha}$.
(2) $a_{\alpha_2} \sqsubseteq a_{\alpha_1}$ for each $\alpha_1 \leq \alpha_2 < \gamma$.
(3) There exists a unique $a_\gamma \in \cap_{\alpha<\gamma} D_\alpha$ such that $a \sqsubseteq a_\gamma$ and $D_{a_\gamma} = \cap_{\alpha<\gamma} D_{a_\alpha}$.
(4) If $a_\gamma \neq b_\gamma$ then $D_{a_\gamma} \cap D_{b_\gamma} = \emptyset$.

Proof of the claim:

(1) Follows immediately from the fact that $a \in D_\alpha$ and S_α is a generating set of D_α.
(2) Since $D_{\alpha_2} \subseteq D_{\alpha_1}$, $a_{\alpha_2} \in D_{\alpha_1}$. Hence there exists a $d \in S_{\alpha_1}$ such that $a_{\alpha_2} \sqsubseteq d$. Now, note that $a \sqsubseteq a_{\alpha_2}$ and thus $a \sqsubseteq d$. By the first part a_{α_1} is the unique element c of S_{α_1} such that $a \sqsubseteq c$. Hence $d = a_{\alpha_1}$ and the

result follows.

(3) By the previous part $\{D_{a_\alpha} \mid \alpha < \gamma\}$ is a decreasing sequence which contains a. The result now follows from the fact that $\emptyset \cup \mathsf{Princ}(\mathcal{X})$ is a Ψ-family (see Proposition B.1). The uniqueness is a consequence of the fact that if $\cap_{\alpha<\gamma} D_{a_\alpha} = D_b = D_{b'}$ then $b \sqsubseteq b'$ and $b' \sqsubseteq b$.

(4) Assume that $D_{a_\gamma} \cap D_{b_\gamma} \neq \emptyset$. Fix $c \in D_{a_\gamma} \cap D_{b_\gamma}$. We have $c \in D_{a_\gamma} \Rightarrow c \in D_{a_\alpha}$ for each $\alpha < \gamma$. Similarly $c \in D_{b_\alpha}$ for each $\alpha < \gamma$. By first part $a_\alpha = b_\alpha$ for all $\alpha < \gamma$. Thus $D_{a_\gamma} = D_{b_\gamma}$ and hence $a_\gamma = b_\gamma$. (**End Proof of the claim.**)

The result now follows by observing that the set $\cap_{\alpha<\gamma} D_\alpha$ is generated by $\{a_\gamma \mid a \in \cap_{\alpha<\gamma} D_\alpha\}$. □

Please note that neither the principal downward closed nor canonically generated sets form a semi-ring. The difference of two principal downward closed sets (canonically generated sets) cannot be written as a finite union of pairwise disjoint principal downward closed sets (canonically generated sets respectively).

B.2 The semi-ring of finite difference sets

In this section, we show that the collection of finite difference sets forms a semi-ring. This observation will then be used in constructing the least upper bound of probability measures.

Definition B.5 Given a poset $(X, \sqsubseteq)$, we say that a $\sqsubseteq$-downward closed set D is *finitely generated* if there is a finite set $S \subseteq X$ such that $D = \cup_{a \in S} D_a$. S is said to be a *generating set* of D. We denote the set of all finitely generated $\sqsubseteq$-downward closed sets by $\mathsf{FinGen}(\mathcal{X})$.

Note that $\emptyset \in \mathsf{FinGen}(\mathcal{X})$ ($\emptyset$ is generated by $\emptyset$). $\mathsf{FinGen}(\mathcal{X})$ is closed under finite unions and finite intersections.

Proposition B.6 *If $(X, \sqsubseteq)$ is a tree-like partial order and $D_1, D_2 \in \mathsf{FinGen}(\mathcal{X})$, then $D_1 \cup D_2 \in \mathsf{FinGen}(\mathcal{X})$ and $D_1 \cap D_2 \in \mathsf{FinGen}(\mathcal{X})$.*

Proof. Let S_1 and S_2 be the generating sets of D_1 and D_2 respectively. Then $D_1 \cup D_2$ is generated by $S_1 \cup S_2$.

Note that $D_1 \cap D_2 = \cup_{a \in S_1, b \in S_2} D_a \cap D_b$. Since $(X, \sqsubseteq)$ is tree-like, for each $a \in S_1$ and each $b \in S_2$, if $D_a \cap D_b \neq \emptyset$ then either $a \sqsubseteq b$ or $b \sqsubseteq a$. Therefore $D_1 \cap D_2 = \cup_{a \in S_1, b \in S_2, D_a \cap D_b \neq \emptyset} D_{\min\{a,b\}}$ and is finitely generated. □

For tree-like partial orders, each finitely generated downward closed set is canonically generated and has a unique finite canonical generating set.

Proposition B.7 *If $\mathcal{X} = (X, \sqsubseteq)$ is tree-like and D is finitely generated then $D \in \mathsf{CanGen}(\mathcal{X})$ and D has a unique finite canonical generating set.*

Proof. Let S be a generating set of D. By definition $D = \cup_{a \in S} D_a$. By taking $S_0 = \text{maximal}(S)$, we can easily see that $D = \cup_{a \in S_0} D_a$ also. Now, note that if $a, b \in S_0$ and $a \neq b$ then we have that $a \not\sqsubseteq b$ and $b \not\sqsubseteq a$ (as S_0 consists of maximal elements of S). Since D is tree-like, we get $D_a \cap D_b = \emptyset$. The uniqueness is a direct consequence of Proposition B.3. □

Note that the collection of finitely generated sets themselves do not form a semi-ring (difference of two finitely generated sets may not be expressible as a union of finitely generated sets). This leads to the following definition.

Definition B.8 Given a poset $\mathcal{X} = (X, \sqsubseteq)$, a set $S \subseteq X$ is said to be a *finite difference set* if there is an $a \in X$ and a finitely generated $\sqsubseteq$-downward closed $D \subseteq D_a$ such that $S = D_a \setminus D$. The set of all difference sets of $(X, \sqsubseteq)$ shall be denoted by $\mathsf{FinDiff}(\mathcal{X})$.

Please note $\mathsf{FinDiff}(\mathcal{X}) \subseteq \mathcal{B} = \{D_1 \setminus D_2 \mid D_1, D_2 \in \mathsf{Down}(\mathcal{X}), D_2 \subseteq D_1\}$. We have already seen that $\mathcal{B}$ is a semi-ring. It turns out $\mathsf{FinDiff}(\mathcal{X})$ is also a semi-ring.

Lemma B.9 *For any tree-like poset $\mathcal{X} = (X, \sqsubseteq)$, $\mathsf{FinDiff}(\mathcal{X})$ is a semi-ring. If X is countable then $\sigma(\mathsf{FinDiff}(\mathcal{X})) = \mathcal{P}(X)$.*

Proof. Note that $\emptyset = D_a \setminus D_a$ for all $a \in X$. Also, note that since $\mathcal{X}$ is a join-semi-lattice, X contains a largest element $\top$. Hence $X = D_\top \setminus \emptyset$. Thus, $\emptyset, X \in \mathsf{FinDiff}(\mathcal{X})$. Let $a_1, a_2 \in X$ and D_1 and D_2 be finitely generated $\sqsubseteq$-downward closed sets such that $D_1 \subseteq D_{a_1}$ and $D_2 \subseteq D_{a_2}$.

From basic set theory we know that

$$(D_{a_1} \setminus D_1) \cap (D_{a_2} \setminus D_2) = (D_{a_1} \cap D_{a_2}) \setminus ((D_{a_1} \cap D_{a_2}) \cap (D_1 \cup D_2)).$$

Since $\mathcal{X}$ is tree-like, we have that $D_{a_1} \cap D_{a_2}$ is $\emptyset$ or D_{a_1} or D_{a_2}. Since finitely generated sets are closed under union and intersection (see Proposition B.6), we get that $(D_{a_1} \setminus D_1) \cap (D_{a_2} \setminus D_2) \in \mathsf{FinDiff}(\mathcal{X})$.

From basic set theory we also know that

$$\begin{aligned}(D_{a_1} \setminus D_1) \setminus (D_{a_2} \setminus D_2) = \\ (D_{a_1} \setminus (D_1 \cup (D_{a_2} \cap D_{a_1}))) \cup \\ ((D_{a_1} \cap D_2) \setminus ((D_{a_1} \cap D_2) \cap D_1)).\end{aligned}$$

Now, let $A_1 = (D_{a_1} \setminus (D_1 \cup (D_{a_2} \cap D_{a_1})))$ and $A_2 = ((D_{a_1} \cap D_2) \setminus ((D_{a_1} \cap D_2) \cap (D_1 \cap D_2)))$. Observe first that A_1 and A_2 are disjoint (since $(D_{a_1} \cap D_2) \subseteq (D_{a_1} \cap D_{a_2})$). Also note that since finitely generated sets are closed under union and intersection $A_1 \in \mathsf{FinDiff}(\mathcal{X})$.

Now, $A_2 = (D_{a_1} \cap D_2) \setminus A_3$ where $A_3 \subseteq (D_{a_1} \cap D_2)$ is finitely generated. If $(D_{a_1} \cap D_2) = \emptyset$ then $A_2 \in \mathsf{FinDiff}(\mathcal{X})$. Otherwise, thanks to Proposition B.7, there exists $k \geq 1$ and $b_1, b_2, \ldots, b_k$ such that $D_{b_i} \cap D_{b_j} = \emptyset$ for each $i \neq j, 1 \leq i, j \leq k$ and $D_{a_1} \cap D_2 = \cup_{1 \leq i \leq k} D_{b_i}$. Basic set theory says that since $D'_{b_i}s$ are pairwise disjoint and $A_3 \subseteq \cup_{1 \leq i \leq k} D_{b_i}$

$$(D_{a_1} \cap D_2) \setminus A_3 = \cup_{1 \leq i \leq k} (D_{b_i} \setminus (D_{b_i} \cap A_3)).$$

Note that $(D_{b_i} \setminus (D_{b_i} \cap A_3)) \cap (D_{b_j} \setminus (D_{b_j} \cap A_3)) = \emptyset$ for each $i \neq j, 1 \leq i, j \leq k$. Hence, we can conclude that $\mathsf{FinDiff}(\mathcal{X})$ is a semi-ring.

If X is countable, then $\mathcal{P}(X)$ is generated by $\{D_a \mid a \in X\}$ (see Example 3.6). Now, $\{D_a \mid a \in X\} \subseteq \mathsf{FinDiff}(\mathcal{X}) \subseteq \mathcal{P}(X)$ and hence $\mathcal{P}(X) \subseteq \sigma(\mathsf{FinDiff}(\mathcal{X})) \subseteq \mathcal{P}(X)$. □

B.3 Least upper bound construction

The strategy for defining least upper bounds of sets of probability measures will be to first define a measure on the semi-ring of finite difference sets and then extend it to the power-set using Theorem 2.3. The measure on the semi-ring of finite difference sets is defined by first defining it on finitely generated sets.

Definition B.10 Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given a *non-empty set* $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$, let $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinGen}(\mathcal{X}) \to \mathbb{R}^+$ be defined as follows. For any $D \in \mathsf{FinGen}(\mathcal{X})$ with S as the finite canonical generating set,

$$\nabla_{\sqsubseteq}(\Gamma)(D) = \sum_{a \in S} \inf_{\mu \in \Gamma} \mu(D_a).$$

Please note that thanks to Proposition B.7, $\nabla_{\sqsubseteq}(\Gamma)$ is well-defined. We show next that $\nabla_{\sqsubseteq}(\Gamma)$ is monotonic and takes values in the interval $[0, 1]$.

Proposition B.11 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$is a tree-like partial order. Let $\top$ be the largest element of $(X, \sqsubseteq)$. Let $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ be such that $\Gamma \neq \emptyset$. Then,*

(1) $\nabla_{\sqsubseteq}(\Gamma)(\emptyset) = 0$ and $\nabla_{\sqsubseteq}(\Gamma)(D_\top) = 1$.

(2) If $D_1, D_2 \in \mathsf{FinGen}(\mathcal{X})$*, then* $D_2 \subseteq D_1$ *implies* $\nabla_{\sqsubseteq}(\Gamma)(D_2) \leq \nabla_{\sqsubseteq}(\Gamma)(D_1)$.
(3) $\forall D \in \mathsf{FinGen}(\mathcal{X}), 0 \leq \nabla_{\sqsubseteq}(\Gamma)(D) \leq 1$.

Proof. Note that the third part of the Proposition follows immediately from the first two. Also note that for each $\mu \in \Gamma$, we have $\mu(\emptyset) = 0$ and $\mu(D_\top) = \mu(X) = 1$. Hence, $\nabla_{\sqsubseteq}(\Gamma)(\emptyset) = 0$ and $\nabla_{\sqsubseteq}(\Gamma)(D_\top) = 1$.

Now, let $D_1, D_2 \in \mathsf{FinGen}(\mathcal{X})$ be such that $D_2 \subseteq D_1$. Let S_1, S_2 be the canonical generating sets of D_1 and D_2. As $D_2 \subseteq D_1$ and S_1 a canonical generating set, for each $b \in S_2$ there is a unique $a \in S_1$ such that $b \sqsubseteq a$. Given $a \in S_1$, let $S_{2,a} = \{b \in S_2 \mid b \sqsubseteq a\}$. We have that $\nabla_{\sqsubseteq}(\Gamma)(D_2) = \sum_{a \in S_1} \sum_{b \in S_{2,a}} \inf_{\mu \in \Gamma} \mu(D_b)$. Hence the result will follow if we can show that $\sum_{b \in S_{2,a}} \inf_{\mu \in \Gamma} \mu(D_b) \leq \inf_{\mu \in \Gamma} \mu(D_a)$.

Fix $a \in S_1$. Note that we have $\cup_{b \in S_{2,a}} D_b \subseteq D_a$. Hence, $\mu_1(\cup_{b \in S_{2,a}} D_b) \leq \mu_1(D_a)$ for each $\mu_1 \in \Gamma$. Now, $D_{b_1} \cap D_{b_2} = \emptyset$ for $b_1, b_2 \in S_{2,a}, b_1 \neq b_2$. Therefore, for each $\mu_1 \in \Gamma$, $\mu_1(\cup_{b \in S_{2,a}} D_b) = \sum_{b \in S_{2,a}} \mu_1(D_b) \geq \sum_{b \in S_{2,a}} \inf_{\mu \in \Gamma} \mu(D_b)$. Hence, for each $\mu_1 \in \Gamma, \sum_{b \in S_{2,a}} \inf_{\mu \in \Gamma} \mu(D_b) \leq \mu_1(D_a)$. The result follows. □

We are almost ready to extend the least upper bound construction to finite difference sets. We first show that any non-empty difference set has a unique representation in terms of set difference of two finitely generated sets.

Proposition B.12 *Let* $S \in \mathsf{FinDiff}(\mathcal{X})$ *be such that* $S \neq \emptyset$*. If* $S = D_{a_1} \setminus D_1$ *and* $S = D_{a_2} \setminus D_2$ *for some* $a_1, a_2 \in X$ *and* $D_1, D_2 \in \mathsf{Down}(\mathcal{X})$ *such that* $D_1 \subseteq D_{a_1}$ *and* $D_2 \subseteq D_{a_2}$ *then* $a_1 = a_2$ *and* $D_1 = D_2$*.*

Proof. Since $S \neq \emptyset$ and $S = D_{a_1} \setminus D_1$, it follows that $a_1 \notin D_1$. Therefore $a_1 \in S = D_{a_2} \setminus D_2$ which implies $a_1 \sqsubseteq a_2$. Similarly, $a_2 \sqsubseteq a_1$ and thus $a_1 = a_2$. Now $D_1 = D_{a_1} \setminus S = D_{a_2} \setminus S = D_2$. □

We extend the least upper bound construction to finite difference sets.

Definition B.13 Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given a *non-empty set* $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$, the function $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinGen}(\mathcal{X}) \to [0,1]$ is extended to $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinDiff}(\mathcal{X}) \to [0,1]$ as follows.

$$\nabla_{\sqsubseteq}(\Gamma)(A) = \begin{cases} 0 & \text{if } A = \emptyset; \\ \nabla_{\sqsubseteq}(\Gamma)(D_a) - \nabla_{\sqsubseteq}(\Gamma)(D) & \text{if } A = D_a \setminus D \text{ for} \\ & D \subsetneq D_a, D \in \mathsf{FinGen}(\mathcal{X}). \end{cases}$$

Note that thanks to Proposition B.11 and Proposition B.12, $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinDiff}(\mathcal{X}) \to [0,1]$ is well-defined.

We have to show that the $\nabla_{\sqsubseteq}(\Gamma)$ so defined is indeed a measure on the semiring of finite difference sets. We start by showing that $\nabla_{\sqsubseteq}(\Gamma)$ preserves limits for the Ψ-family $\mathcal{P} = \emptyset \cup \mathsf{Princ}(\mathcal{X})$. Note that the class $\mathcal{P}$ is a subset of finitely generated downward closed sets and that the function $\nabla_{\sqsubseteq}(\Gamma)$ is monotonic on $\mathcal{P}$ (see Proposition B.11). We will make use of the following well-known result on the continuity of measures.

Proposition B.14 *Let $\mathcal{X} = (X, \Sigma)$ be a measurable space and $\mu \in \mathcal{M}_{=1}(\mathcal{X})$. Let $\{A_j \mid j \in \mathbb{N}\}$ be a increasing or decreasing sequence of measurable subsets. Then $\lim_{j\to\infty} \mu(A_j) = \mu(\lim_{j\to\infty} A_j)$.*

Lemma B.15 *Let be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Let $\mathcal{P} = \emptyset \cup \mathsf{Princ}(\mathcal{X})$ and $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ be such that $\Gamma \neq \emptyset$. Then the monotonic function $\nabla_{\sqsubseteq}(\Gamma) : \mathcal{P} \to [0, 1]$ preserves limits.*

Proof. Note that thanks to Proposition A.9, we only need to show that $\nabla_{\sqsubseteq}(\Gamma)$ preserves ω-limits. Let $\{D_j \mid j \in \mathbb{N}\}$ be a ω-sequence of decreasing sets in $\mathcal{P}$. We need to show that $\nabla_{\sqsubseteq}(\Gamma)(\lim_{j\to\infty} D_j) = \lim_{j\to\infty} \nabla_{\sqsubseteq}(\Gamma)(D_j)$.

If $D_j = \emptyset$ for any j then $D_k = \emptyset$ for each $k \geq j$ and $\lim_{j\to\infty} D_{a_j} = \emptyset$. The result holds for this case.

Hence, the interesting case is when for each j, $D_j = D_{a_j}$ for some $a_j \in X$. Let $D_\omega = \lim_{j\to\infty} D_{a_j}$. We need to show that $\nabla_{\sqsubseteq}(\Gamma)(D_\omega) = \lim_{j\to\infty} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j})$. Note that since $\nabla_{\sqsubseteq}(\Gamma)$ is monotonic (see Proposition B.11), we have $\nabla_{\sqsubseteq}(\Gamma)(D_\omega) \leq \inf_{j\in\infty} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j})$. We just need to show the reverse inequality.

Assume first that $D_\omega = \emptyset$. We have $\nabla_{\sqsubseteq}(\Gamma)(D_\omega) = 0$. Fix $\mu \in \Gamma$. By Proposition B.14, $\lim_{j\to\infty} \mu(D_{a_j}) = \mu(D_\omega) = 0$ for each $\mu \in \Gamma$. Now $0 \leq \nabla_{\sqsubseteq}(\Gamma)(D_{a_j}) \leq \mu(D_{a_j})$ for each j and $\mu \in \Gamma$. Thus, $\lim_{j\to\infty} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j}) = 0 = \nabla_{\sqsubseteq}(\Gamma)(D_\omega)$.

Assume that $D_\omega = D_c$ for some $c \in X$. By definition, given $\epsilon > 0$, there is a $\mu \in \Gamma$ such that $\mu(D_\omega) < \nabla_{\sqsubseteq}(\Gamma)(D_\omega) + \frac{\epsilon}{2}$. Fix one such μ. By Proposition B.14, $\lim_{j\to\infty} \mu(D_{a_j}) = \mu(D_\omega)$. Hence there exists j_0 such that $\forall j.\ j \geq j_0$, $\mu(D_{a_j}) < \mu(D_\omega) + \frac{\epsilon}{2}$. Hence, $\forall j.\ j_0 \leq j$, $\nabla_{\sqsubseteq}(\Gamma)(D_{a_j}) \leq \mu(D_{a_j}) < \mu(D_\omega) + \frac{\epsilon}{2} < \nabla_{\sqsubseteq}(\Gamma)(D_\omega) + \epsilon$. Thus, $\lim_{j\to\infty} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j}) < \nabla_{\sqsubseteq}(\Gamma)(D_\omega) + \epsilon$. Since ϵ is arbitrary, the result follows. □

We shall now show that the function $\nabla_{\sqsubseteq}(\Gamma)$ also preserves limits for the Ψ-family of canonically generated sets (see Proposition B.4). Please note that $\nabla_{\sqsubseteq}(\Gamma)$ has not been defined on canonically generated sets, and hence we first extend $\nabla_{\sqsubseteq}(\Gamma)$ in the obvious way. Observe first that if D is canonically generated by S, then for any *finite* collection $S_1 \subseteq S$, $0 \leq \sum_{a\in S_1} \nabla_{\sqsubseteq}(\Gamma)(D_a) \leq 1$ (see Proposition B.11). Furthermore, D has a unique canonical generating set. Hence, we can extend $\nabla_{\sqsubseteq}(\Gamma)$ to $\nu(\Gamma)$ as follows.

Definition B.16 Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ such that $\Gamma \neq \emptyset$, define $\nu(\Gamma) : \mathsf{CanGen}(\mathcal{X}) \to [0,1]$ as follows. Given $D \in \mathsf{CanGen}(\mathcal{X})$ with S as the generating of D, let $\nu(\Gamma)(D) = \sum_{a \in S} \nabla_{\sqsubseteq}(\Gamma)(D_a)$.

We now show that ν is monotonic.

Proposition B.17 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ such that $\Gamma \neq \emptyset$. Then the function $\nu(\Gamma) : \mathsf{CanGen}(\mathcal{X}) \to [0,1]$ is monotonic. Furthermore, for any $\mu \in \Gamma$ and $D \in \mathsf{CanGen}(\mathcal{X})$, $\nu(\Gamma)(D) \leq \mu(D)$.*

Proof. First observe that for any $\mu \in \Gamma$ and $D \in \mathsf{CanGen}(\mathcal{X})$ with S as the generating set; $\mu(D) = \sum_{a \in S} \mu(D_a) \geq \sum_{a \in S} \nabla_{\sqsubseteq}(\Gamma)(D_a) = \nu(\Gamma)(D)$.

Now, we show that $\nu(\Gamma)$ is monotonic. Let $D, D' \in \mathsf{CanGen}(\mathcal{X})$ be such that $D \subseteq D'$. Let S, S' be the canonical generating sets of D and D'. If $S = \emptyset$ then the result is obvious. Now fix $a_0, a_1, \ldots a_k \in S$ such that $a_j \neq a_{j'}$ for $j \neq j'$. The result will follow if we can show that $\sum_{0 \leq j \leq k} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j}) \leq \nu(\Gamma)(D')$.

Note that for each $0 \leq j \leq k$, there exist $b_j \in D'$ such that $a_j \sqsubseteq b_j$. Let $S_0 = \{a_j \mid 0 \leq j \leq k\}$ and $S_0' = \{b_j \mid 0 \leq j \leq k\}$. Please note that $D_{a_j} \cap D_{a_{j'}} = \emptyset$ for $j \neq j'$. We also have that $S_0 \subseteq S$ and $S_0' \subseteq S'$.

Now consider the finitely generated sets $D_0 = \cup_{a \in S_0} D_a$ and $D_0' = \cup_{a \in S_0'} D_a$. D_0 is canonically generated by S_0 while D_0' is canonically generated by S_0'. Note that $D_0 \subseteq D_0'$ and hence $\nabla_{\sqsubseteq}(\Gamma)(D_0) \leq \nabla_{\sqsubseteq}(\Gamma)(D_0')$ (see Proposition B.11). Now, $\nabla_{\sqsubseteq}(\Gamma)(D_0) = \sum_{a \in S_0} \nabla_{\sqsubseteq}(\Gamma)(D_a) = \sum_{0 \leq j \leq k} \nabla_{\sqsubseteq}(\Gamma)(D_{a_j})$. The result follows by observing that $\nabla_{\sqsubseteq}(\Gamma)(D_0') = \sum_{a \in S_0'} \nabla_{\sqsubseteq}(\Gamma)(D_a) \leq \sum_{a \in S'} \nabla_{\sqsubseteq}(\Gamma)(D_a) \leq \nu(\Gamma)(D')$. □

We are ready to show that $\nu(\Gamma)$ preserves limits.

Lemma B.18 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measurable space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X})$ such that $\Gamma \neq \emptyset$. Then the function $\nu(\Gamma) : \mathsf{CanGen}(\mathcal{X}) \to [0,1]$ preserves limits.*

Proof. Thanks to Proposition A.9, we just need to show that $\nu(\Gamma)$ preserves ω-limits. Let $\{D_j \mid j \in \mathbb{N}\}$ be a decreasing sequence of canonically generated sets. Let $D_\infty = \cap_{j \in \mathbb{N}} D_j$. For each j, let S_j be the generating set of D_j and let S_∞ be the generating set of D_∞. Now for each j, let $\widehat{S}_j = \{a \in S_j \mid \exists b \in D_\infty . b \sqsubseteq a\}$ and $\widetilde{S}_j = S_j \setminus \widehat{S}_j$. Let $\widehat{D_j} = \cup_{a \in \widehat{S}_j} D_a$ and $\widetilde{D_j} = \cup_{a \in \widetilde{S}_j} D_a$. We have the following.

(1) $\widehat{D_j}, \widetilde{D_j} \in \mathsf{CanGen}(\mathcal{X})$, $D_j = \widehat{D_j} \cup \widetilde{D_j}$, $\widehat{D_j} \cap \widetilde{D_j} = \emptyset$.

(2) $\{\widehat{D}_j \mid j \in \mathbb{N}\}$ is a decreasing sequence and $D_\infty = \cap_{j\in\mathbb{N}}\widehat{D}_j$.
(3) $\nu(\Gamma)(D_j) = \nu(\Gamma)(\widehat{D}_j) + \nu(\Gamma)(\widetilde{D}_j)$.

We need to show that $\lim_{j\to\infty}\nu(\Gamma)(D_j) = \nu(\Gamma)(D_\infty)$. The result now follows from the following claim.

Claim 1 *We have*

(1) $\lim_{j\to\infty}\nu(\Gamma)(\widetilde{D}_j) = 0$ *and*
(2) $\lim_{j\to\infty}\nu(\Gamma)(\widehat{D}_j) = \nu(\Gamma)(D_\infty)$.

Proof of the claim.

(1) Fix $\mu \in \Gamma$. Note that we have $0 \leq \nu(\Gamma)(\widetilde{D}_j) \leq \mu(\widetilde{D}_j)$. Hence, the result will follow if we can show that $\lim_{j\to\infty}\mu(\widetilde{D}_j) = 0$. Now, note that we have for each j, $\mu(D_j) = \mu(\widetilde{D}_j) + \mu(\widehat{D}_j)$. As $\{D_j \mid j \in \mathbb{N}\}$ is a decreasing sequence and $D_\infty = \cap_{j\in\mathbb{N}}D_j$, we get by Proposition B.14, $\lim_{j\to\infty}\mu(D_j) = \mu(D_\infty)$. Similarly, $\lim_{j\to\infty}\mu(\widehat{D}_j) = \mu(D_\infty)$. Hence, $\lim_{j\to\infty}\mu(\widetilde{D}_j)$ exists and is equal to $\lim_{j\to\infty}(\mu(D_j) - \mu(\widehat{D}_j)) = 0$.
(2) As in the proof of Proposition B.4, for each $a \in S_\infty$ there a unique a_j such that $a_j \in \widehat{S}_j$ and $a \in D_{a_j}$. We have $\{D_{a_j} \mid j \in \mathbb{N}\}$ is a decreasing sequence and $\cap_{j\in\mathbb{N}}D_{a_j} = D_a$. Since $\nabla_\sqsubseteq(\Gamma)$ preserves limits (see Lemma B.15) $\lim_{j\to\infty}\nabla_\sqsubseteq(\Gamma)(D_{a_j}) = \nabla_\sqsubseteq(\Gamma)(D_a)$. Also note that for $b \in S_\infty, a \neq b$, there is a j_0 st $a_j \neq b_j$ for all $j \geq j_0$.

We will prove the result for the case S_∞ is countably infinite (the finite case can be dealt with similarly). Now let $a^0, a^1, a^2, \ldots$ be an enumeration of elements of S_∞. For each $k \in \mathbb{N}$, let $\{a^k_j \mid j \in \mathbb{N}\}$ be the sequence of elements such that $a^k_j \in \widehat{S}_j$ and $a^k \in D_{a^k_j}$ for each $j \in \mathbb{N}$. Now we construct a doubly-indexed sequence $\{D_{j,k} \mid j \in \mathbb{N}, k \in \mathbb{N}\}$ by induction on k as follows. For $k = 0$, $D_{j,0} = D_{a^0_j}$. Now assume that the sequence has been constructed for all $k \leq l$. For $k = l+1$, let j_0 be the smallest index m such $a^{l+1}_m \notin \{a^n_m \mid 1 \leq n \leq l\}$. For each $j < j_0$, let $D_{j,l+1} = \emptyset$ and for each $j \geq j_0$, $D_{j,l+1} = D_{a^{l+1}_j}$.

Fix $\mu \in \Gamma$. For each j, k let $r_{j,k} = \nabla_\sqsubseteq(\Gamma)(D_{j,k})$ and $s_{j,k} = \mu(D_{j,k})$. We have the following.

- $\widehat{D}_j = \cup_{k\in\mathbb{N}}D_{j,k}$.
- $r_{j,k} \leq s_{j,k}$.
- $\nu(\Gamma)(\widehat{D}_j) = \sum_{k\in\mathbb{N}} r_{j,k}$ and $\mu(\widehat{D}_j) = \sum_{k\in\mathbb{N}} s_{j,k}$.
- We can conclude $\mu(D_\infty) = \sum_{k\in\mathbb{N}}\lim_{j\to\infty} s_{j,k} = \lim_{j\to\infty}\sum_{k\in\mathbb{N}} s_{j,k}$ as follows.
  (a) $\lim_{j\to\infty} s_{j,k} = \mu(D_{a^k})$ as $\lim_{j\to\infty}\mu(D_{a^k_j}) = \mu(D_{a^k})$ (Proposition B.14).
  (b) $\mu(D_\infty) = \sum_{k\in\mathbb{N}}\mu(D_{a^k})$ as D_∞ is the disjoint union $\cup_{k\in\mathbb{N}}D_{a^k}$.
  (c) By definition $\lim_{j\to\infty}\sum_{k\in\mathbb{N}} s_{j,k} = \lim_{j\to\infty}\mu(\widehat{D}_j)$.

(d) By Proposition B.14, $\lim_{j\to\infty} \mu(\widehat{D_j}) = \mu(D_\infty)$.

- We have that $\lim_{j\to\infty} r_{j,k} = \nabla_{\sqsubseteq}(\Gamma)(D_{a^k})$ (as $\lim_{j\to\infty} D_{a_j^k} = D_{a^k}$).
- By Theorem A.5, $\lim_{j\to\infty} \sum_{k\in\mathbb{N}} r_{j,k}$ and $\sum_{k\in\mathbb{N}} \lim_{j\to\infty} r_{j,k}$ exist and are equal. The result follows by observing that $\sum_{k\in\mathbb{N}} r_{j,k}$ is $\nu(\Gamma)(\widehat{D_j})$ and $\sum_{k\in\mathbb{N}} \lim_{j\to\infty} r_{j,k} = \sum_{k\in\mathbb{N}} \nabla_{\sqsubseteq}(\Gamma)(D_{a^k}) = \nu(\Gamma)(D_\infty)$. . □

We are almost ready to show that $\nabla_{\sqsubseteq}(\Gamma)$ is a measure on the semi-ring of finite difference sets. We introduce some notation and propositions which will make our proof easier.

Notation: Let $A \in \mathsf{FinDiff}(\mathcal{X})$ be such that $A \neq \emptyset$ and let $a \in X$ and $D \in \mathsf{FinGen}(\mathcal{X})$ be such that $A = D_a \setminus D$. We say $\mathsf{Pos}(A) = \{a\}$ and $\mathsf{Neg}(A) = \text{maximal}(D)$. If $\mathcal{C} = \{A_i \mid i \in I\}$ is an indexed collection of sets of sets in $\mathsf{FinDiff}(\mathcal{X})$, we say that $\mathsf{Pos}(\mathcal{C}) = \cup_{i\in I}\mathsf{Pos}(A_i)$ and $\mathsf{Neg}(\mathcal{C}) = \cup_{i\in I}\mathsf{Neg}(A_i)$.

Definition B.19 Let $\mathcal{X} = (X, \mathcal{P}(\mathcal{X}), \sqsubseteq)$ be a countable ordered measure space such that $(X, \sqsubseteq)$ is a tree-like partial order. Given $A \in \mathsf{FinDiff}(\mathcal{X})$, we say a countable indexed collection $\mathcal{C} = \{A_i \mid i \in I\} \subseteq \mathsf{FinDiff}(\mathcal{X})$ *canonically covers* A if $A_i \neq \emptyset$ for each i, $A_i \cap A_j = \emptyset$ for each $i, j \in I, i \neq j$, and $\cup_{i\in I} A_i = A$.

The following result says that for countable additivity we just need to consider some special cases.

Proposition B.20 *Let $\mathcal{X} = (X, \mathcal{P}(\mathcal{X}), \sqsubseteq)$ be a countable ordered measure space such that $(X, \sqsubseteq)$ is a tree-like partial order. Then, given $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X}), \Gamma \neq \emptyset$, the function $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinDiff}(\mathcal{X}) \to [0, 1]$ is countably additive iff for each $a \in X$ and each countable collection $\mathcal{C} = \{A_i \mid i \in I\}$ of finite difference sets such that $\mathcal{C}$ canonically covers D_a, $\nabla_{\sqsubseteq}(\Gamma)(D_a) = \sum_{i\in I} \nabla_{\sqsubseteq}(\Gamma)(A_i)$.*

Proof. ($\Leftarrow$). For simplicity sake, we shall write μ for the $\nabla_{\sqsubseteq}(\Gamma)$. We need to show that for any finite difference set A and countable indexed collection of disjoint finite difference sets $\{A_i \mid \in I\}$ such that $A = \cup_{i\in I} A_i$, $\mu(D_a \setminus D) = \sum_{i\in I} \mu(A_i)$. Please note that as $\mu(\emptyset) = 0$, we can assume without loss of generality each $A_i \neq \emptyset$. Let $A = D_a \setminus D$ for some $a \in X, D \in \mathsf{FinGen}(\mathcal{X})$ and $D \subsetneq D_a$. If D is canonically generated by $a_0, a_1, \ldots, a_k$ then $D_a = (\cup_{0\leq j\leq k} D_{a_j}) \cup (\cup_{i\in I} A_i)$. Furthermore $D_{a_j} \cap A_i = \emptyset$ for each $0 \leq j \leq k$ and $i \in I$. Thus, the collection $\{D_{a_j} \mid 0 \leq j \leq k\} \cup \{A_i \mid i \in I\}$ canonically covers D_a. Hence, $\mu(D_a) = \sum_{0\leq j\leq k} D_{a_j} + \sum_{i\in I} \mu(A_i)$ which implies that $\mu(D_a) = \mu(D) + \sum_{i\in I} \mu(A_i)$. Thus $\mu(D_a \setminus D) = \sum_{i\in I} \mu(A_i)$.

The ($\Rightarrow$)-direction is obvious. □

The following result will also be useful.

Proposition B.21 *Let $\mathcal{X} = (X, \mathcal{P}(\mathcal{X}), \sqsubseteq)$ be a countable ordered measure*

space such that $(X, \sqsubseteq)$ is a tree-like partial order. Let $a \in X$ and $\mathcal{C} = \{A_i \mid \in I\}$ be a countable indexed collection of finite difference sets such that $\mathcal{C}$ canonically covers D_a. Then the following hold.

(1) For each b in $\mathsf{Neg}(\mathcal{C})$, there is exactly one i such that $b \in \mathsf{Neg}(A_i)$.
(2) $\mathsf{Neg}(\mathcal{C}) \subseteq \mathsf{Pos}(\mathcal{C})$.

Proof. For each $i \in I$, let $\mathsf{Pos}(A_i) = \{a\}_i$ Clearly as each A_i is non-empty, $a_i \in A_i$. Hence $a_i \in D_{a_i}$ for each $i \in I$. Furthermore, let D_i be the finitely generated set $D_{a_i} \setminus A_i$. Recall that $\mathsf{Neg}(A_i) = \text{maximal}(D_i)$.

(1) Fix $b \in \mathsf{Neg}(\mathcal{C})$. Let j and k be such that $j \neq k$, $b \in \mathsf{Neg}(A_j)$ and $b \in \mathsf{Neg}(A_k)$. We have $b \sqsubseteq a_j$ and $b \sqsubseteq a_k$. Since $(X, \sqsubseteq)$ is tree-like, either $a_j \sqsubseteq a_k$ or $a_k \sqsubseteq a_j$. Assume, without loss of generality, that $a_j \sqsubseteq a_k$. We have $a_j \in A_j$. Since $\mathcal{C}$ is a canonical collection, we must have $a_j \notin A_k$. But $A_k = D_{a_k} \setminus D_k$. Hence $a_j \in D_k$. Note that b is a maximal element of D_k and that $b \sqsubseteq a_j$. Hence $b = a_j$. This implies that $A_j = \emptyset$. A contradiction.
(2) Fix $b \in \mathsf{Neg}(\mathcal{C})$. Let $j \in I$ be such that $b \in \mathsf{Neg}(A_j)$. We have $b \sqsubseteq a_j$ and hence $b \sqsubseteq a$ also. Therefore there exists some k such that $b \in A_k$. Clearly $j \neq k$. Thus, we have $b \sqsubseteq a_k$ also and hence either $a_j \sqsubseteq a_k$ or $a_k \sqsubseteq a_j$. Assume first that if $a_j \sqsubseteq a_k$. In this case, we must have $a_j \notin A_k$ and hence $a_j \in D_k$. This implies that $b \in D_k$ and hence $b \notin A_k$. A contradiction. Hence $a_k \sqsubseteq a_j$. Again, we must have $a_k \notin A_j$ and hence $a_k \in D_j$. But $b \sqsubseteq a_k$ and b is a maximal element of D_j. Hence $b = a_k \in \mathsf{Pos}(\mathcal{C})$. □

We are ready to show that $\nabla_{\sqsubseteq}(\Gamma)$ is a measure on the semi-ring $\mathsf{FinDiff}(\mathcal{X})$.

Theorem B.22 *Let $\mathcal{X} = (X, \mathcal{P}(\mathcal{X}), \sqsubseteq)$ be a countable ordered measure space such that $(X, \sqsubseteq)$ is a tree-like partial order. Then, given $\Gamma \subseteq \mathcal{M}_{=1}(\mathcal{X}), \Gamma \neq \emptyset$, the function $\nabla_{\sqsubseteq}(\Gamma) : \mathsf{FinDiff}(\mathcal{X}) \to [0, 1]$ is a measure on the semi-ring $\mathsf{FinDiff}(\mathcal{X})$.*

Proof. We just need to show that $\nabla_{\sqsubseteq}(\Gamma)$ is countably additive. Recall for $D \in \mathsf{CanGen}(\mathcal{X})$ generated by $\mathcal{X}$, $\nu(\Gamma) = \sum_{a \in S} \nabla_{\sqsubseteq}(\Gamma)(D_a)$. For simplicity sake, for the rest of the proof we shall write μ for $\nabla_{\sqsubseteq}(\Gamma)$ and ν for $\nu(\Gamma)$.

Let $a \in X$ and $\mathcal{C} = \{A_i \mid \in I\}$ be a countable indexed collection of finite difference sets such that $\mathcal{C}$ canonically covers D_a. Let each $A_i = D_{a_i} \setminus D_i$ where $D_i \in \mathsf{FinGen}(\mathcal{X})$ and $D_i \subsetneq D_{a_i}$. Let $S_i = \mathsf{Neg}(A_i) = \text{maximal}(D_i)$. We can easily show from the fact $a \in D_a$, $a \in \mathsf{Pos}(\mathcal{C})$ also. For the rest of the proof we shall write Pos for $\mathsf{Pos}(\mathcal{C})$ and Neg for $\mathsf{Neg}(\mathcal{C})$.

Now, let ω_1 be the first uncountable ordinal. We shall construct, by transfinite induction, sequences $\{\mathsf{Pos}_\delta \mid \delta < \omega_1\}, \{\mathsf{Neg}_\delta \mid \delta < \omega_1\}, \{H_\delta \mid \delta < \omega_1\}$ and $\{F_\delta \mid \delta < \omega_1\}$ such that the following hold.

(1) $\mathsf{Pos}_0 = \{a\}$. $\mathsf{Pos}_\delta \subseteq \mathsf{Pos} \setminus (\cup_{\beta<\delta}\mathsf{Pos}_\beta)$ and for each $b, c \in \mathsf{Pos}_\delta$, $(b \neq c) \Rightarrow (D_b \cap D_c = \emptyset)$.
(2) Let $I_\delta = \{i \in I \mid a_i \in \mathsf{Pos}_\delta\}$. Then $\mathsf{Neg}_\delta = \cup_{i\in I_\delta} S_i$. For each $i, j \in I_\delta, i \neq j$, $(b \in S_i$ and $c \in S_j) \Rightarrow (D_b \cap D_c = \emptyset)$. Thus for $b, c \in \mathsf{Neg}_\delta$ $(b \neq c) \Rightarrow (D_b \cap D_c = \emptyset)$. Furthermore, $\mathsf{Neg}_\delta \subseteq \mathsf{Pos} \setminus (\cup_{\beta\leq\delta}\mathsf{Pos}_\beta)$.
(3) $H_\delta = \cup_{b\in\mathsf{Pos}_\delta} D_b$. Thus H_δ is canonically generated by Pos_δ. $H_{\delta_1} \subseteq H_{\delta_2}$ for each $\delta_1 \leq \delta_2$.
(4) $F_\delta = \{(D_{a_i} \setminus D_i) \mid a_i \in \mathsf{Pos}_\delta\}$ and thus $F_\delta \subseteq \mathcal{C}$. Note the first condition ensures that each $A_i \in \mathcal{C}$ occurs in at most one F_δ.
(5) $H_\delta = D_a \setminus (\cup_{\beta<\delta}(\cup_{A\in F_\beta} A))$.
(6) $\sum_{A\in(\cup_{\beta<\delta}F_\beta)} \mu(A) = \mu(D_a) - \nu(H_\delta)$.

Before we show how to construct the sequences, we first show how once the sequences are constructed, the main result will follow. Note that by first condition, we have $\mathsf{Pos}_{\delta_1} \cap \mathsf{Pos}_{\delta_2} = \emptyset$ for $\delta_1 \neq \delta_2$. Now, as X is countable and ω_1 is the first uncountable ordinal, there must exists some $\delta_0 < \omega_1$ such that $\mathsf{Pos}_{\delta_0} = \emptyset$. In that case $H_{\delta_0} = \emptyset$ (condition 3) and hence $D_a = (\cup_{\beta<\delta_0}(\cup_{A\in F_\beta} A))$ (condition 5). From this, it can be easily shown that $\mathcal{C} = \cup_{\beta<\delta_0} F_\beta$. Hence $\sum_{A\in\mathcal{C}} \mu(A) = \sum_{A\in(\cup_{\beta<\delta_0}F_\beta)} \mu(A) = \mu(D_a) - \nu(H_{\delta_0}) = \mu(D_a)$ as required.

Now we show how to construct the sequences by transfinite induction. The construction proceeds as follows.

Base Case: δ is 0. Let $\mathsf{Pos}_0 = \{a\}$. Let $i_0 \in I$ be such that $a_{i_0} = a$. Then let $\mathsf{Neg}_0 = S_{i_0}$, $H_0 = D_a$ and $F_0 = \{D_a \setminus D_{i_0}\}$. Clearly, the above conditions hold for $\mathsf{Pos}_0, \mathsf{Neg}_0, D_0$ and F_0.

Induction Step. There are two cases.

Case 1. δ is the successor ordinal $\gamma + 1$. Let $\mathsf{Pos}_{\gamma+1} = \mathsf{Neg}_\gamma$. Let $I_{\gamma+1} = \{i \in I \mid a_i \in \mathsf{Pos}_{\gamma+1}\}$ and $\mathsf{Neg}_{\gamma+1} = \cup_{i\in I_{\gamma+1}} S_i$. Let $H_{\gamma+1} = \cup_{b\in\mathsf{Pos}_{\gamma+1}} D_b$ and $F_{\gamma+1} = \{(D_{a_i} \setminus D_i) \mid a_i \in \mathsf{Pos}_{\gamma+1}\}$.

Note that the first condition holds by induction hypothesis (follows directly by condition satisfied by Neg_γ). The third and fourth conditions also follow by construction.

Also, note that we have $D_a \setminus H_{\gamma+1} = (D_a \setminus H_\gamma) \cup (H_\gamma \setminus H_{\gamma+1})$. By induction hypothesis, $(D_a \setminus H_\gamma) = \cup_{\beta<\gamma}(\cup_{A\in F_\beta} A)$. Note, again that by construction and induction hypothesis, $H_\gamma \setminus H_{\gamma+1} = \cup_{b\in\mathsf{Pos}_\gamma} D_b \setminus \cup_{c\in\mathsf{Neg}_\gamma} D_c = \cup_{A\in F_\gamma} A$. Hence $H_{\gamma+1} = D_a \setminus (\cup_{\beta<\gamma+1}(\cup_{GAinF_\beta} A))$. Hence the fifth condition is also satisfied.

Now, we have $\mu(D_a) - \nu(H_{\gamma+1}) = \mu(D_a) - \nu(H_\gamma) + \nu(H_\gamma) - \nu(H_{\gamma+1})$. By induction, $\mu(D_a) - \nu(H_\gamma) = \sum_{A\in(\cup_{\beta<\gamma}F_\beta)} \mu(A)$. Now, $F_\gamma = \{(D_{a_i} \setminus D_i) \mid a_i \in \mathsf{Pos}_\gamma\}$ and $\mu(D_{a_i} \setminus D_i) = \mu(D_{a_i}) - \sum_{b\in S_i} \mu(D_b)$. Thus, $\sum_{A\in F_\gamma} \mu(A) = \sum_{b\in\mathsf{Pos}_\gamma} \mu(D_b) - \sum_{i\in I_\gamma} \sum_{b\in S_i} \mu(D_b)$. But the former sum is $\nu(H_\gamma)$, while the latter sum is

$\nu(H_{\gamma+1})$. Hence the sixth condition is also satisfied.

We have to show that the second condition is satisfied. Let $i, j \in I_{\gamma+1}$ be such that $i \neq j$. Now, we have by construction $D_{a_i} \cap D_{a_j} = \emptyset$. Thus, if $b \in S_i$ and $c \in S_j$, we have $D_b \subseteq D_{a_i}$ and $D_c \subseteq D_{a_j}$ and hence $D_b \cap D_c = \emptyset$. Also clearly if $b, c \in S_i$ for $i \in I_{\gamma+1}$then from the fact that $(X, \sqsubseteq)$ is tree-like and b, c are maximal elements of D_i, we get $D_b \cap D_c = \emptyset$.

Now, observe by construction $\mathsf{Neg}_{\gamma+1} \subseteq \mathsf{Neg} \subseteq \mathsf{Pos}$ (see Proposition B.21). We need to show that $\mathsf{Neg}_{\gamma+1} \cap (\cup_{\beta \leq \gamma+1} \mathsf{Pos}_\beta) = \emptyset$. Note by construction $\mathsf{Neg}_{\gamma+1} \subseteq H_{\gamma+1} = D_a \setminus (\cup_{\beta<\gamma+1}(\cup_{A \in F_\beta} A))$. Now, it is easily seen that $\mathsf{Pos}_\beta \subseteq \cup_{A \in F_\beta} A$ for each β. Hence $\mathsf{Neg}_{\gamma+1} \cap \cup_{\beta \leq \gamma} \mathsf{Pos}_\beta = \emptyset$. We just need to show that $\mathsf{Neg}_{\gamma+1} \cap \mathsf{Pos}_{\gamma+1} = \emptyset$. Pick $b \in \mathsf{Neg}_{\gamma+1}$. There there is a $i \in I_{\gamma+1}$ such that $b \in S_i$. Now, note that $b \sqsubseteq a_i$, but $a_i \neq b$ (otherwise $A_i = \emptyset$). Now if $b \in \mathsf{Pos}_{\gamma+1}$ then we will get that $b \in D_{a_i} \cap D_b$ which contradicts the first condition.

Case 2. δ is the limit ordinal γ. Observe first that by induction hypothesis, $\{H_\beta \mid \beta < \gamma\}$ is a decreasing sequence of canonically generated sets. Hence the set $\widetilde{H} = \cap_{\beta<\gamma} H_\beta$ is canonically generated (see Proposition B.4). Let $\widetilde{S}$ be the generating set of $\widetilde{H}$.

We first claim that $\widetilde{S} \subseteq \mathsf{Pos} \setminus (\cup_{\beta<\gamma} \mathsf{Pos}_\beta)$. Observe that, by induction, we have $H_\beta = D_a \setminus (\cup_{\beta'<\beta}(\cup_{A \in F_{\beta'}} A))$ for all $\beta < \gamma$. Hence

$$\begin{aligned} \widetilde{H} = \cap_{\beta<\gamma} H_\beta &= \cap_{\beta<\gamma}(D_a \setminus (\cup_{\beta'<\beta}(\cup_{A \in F_{\beta'}} A))) \\ &= D_a \setminus (\cup_{\beta<\gamma}(\cup_{A \in F_\beta} A)). \end{aligned}$$

It is easy to show by induction hypothesis that $\mathsf{Pos}_\beta \subseteq \cup_{A \in F_\beta} A$ for all $\beta < \gamma$. Hence $\widetilde{S} \cap (\cup_{\beta<\gamma} \mathsf{Pos}_\beta) = \emptyset$. Now, let $\mathcal{C}'$ be the collection $\mathcal{C} \setminus \cup_{\beta<\gamma} F_\beta$. Since $\mathcal{C}$ canonically covers D_a we have that

$$\widetilde{H} = D_a \setminus (\cup_{\beta<\gamma}(\cup_{A \in F_\beta} A)) = \cup_{A \in \mathcal{C}'} A.$$

Clearly all maximal elements of $\widetilde{H} = \cup_{A \in \mathcal{C}'} A$ are contained in the set $\mathsf{Pos}(\mathcal{C}') \subseteq \mathsf{Pos}$. But $\widetilde{S}$ is the set of the maximal elements of $\widetilde{H}$. Hence $\widetilde{S} \subseteq \mathsf{Pos}$. Since $\widetilde{S} \cap (\cup_{\beta<\gamma} \mathsf{Pos}_\beta) = \emptyset$, we get $\widetilde{S} \subseteq \mathsf{Pos} \setminus (\cup_{\beta<\gamma} \mathsf{Pos}_\beta)$.

Now, let $\mathsf{Pos}_\gamma = \widetilde{S}$ and $H_\gamma = \widetilde{H}$. Let $I_\gamma = \{i \in I \mid a_i \in \mathsf{Pos}_\gamma\}$ and $\mathsf{Neg}_\gamma = \cup_{i \in I_\gamma} S_i$. Let $F_\gamma = \{(D_{a_i} \setminus D_i) \mid a_i \in \mathsf{Pos}_\gamma\}$. The first, third and fourth conditions required are satisfied by construction. By construction, we have that $H_\gamma = \widetilde{H} = D_a \setminus (\cup_{\beta<\gamma}(\cup_{A \in F_\beta} A))$ also.

Now note that we have

$$\begin{aligned}\sum_{A\in(\cup_{\beta'<\gamma}F_{\beta'})}\mu(A) &= \lim_{\beta\to\gamma}\sum_{A\in(\cup_{\beta'<\beta}F_{\beta})}\mu(A)\\ &= \lim_{\beta\to\gamma}(\mu(D_a)-\nu(H_\beta))\\ &\qquad\qquad\text{(by induction hypothesis)}\\ &= \mu(D_a)-\nu(H_\gamma)\text{(see Lemma B.18).}\end{aligned}$$

Hence the sixth condition is also satisfied. We can show also that the second condition is satisfied by an argument similar to the argument used for the case when δ is a successor ordinal. □

Thus, we can show that least upper bounds of probability measures exist for tree-like partial orders.

Lemma B.23 *Let $\mathcal{X} = (X, \mathcal{P}(X), \sqsubseteq)$ be a countable ordered measure space such that $(X, \sqsubseteq)$ is a tree-like partial order. Then $(\mathcal{M}_{=1}(\mathcal{X}), \preceq_{\sqsubseteq})$ is a join semi-lattice.*

Proof. Thanks to Theorem 2.3, Lemma B.9 and Theorem B.22, given $\Gamma \in \mathcal{M}_{=1}(\mathcal{X}), \Gamma \neq \emptyset$, there is a unique measure $\mu : \mathcal{P}(X) \to [0,1]$ such that $\mu(A) = \nabla_{\sqsubseteq}(\Gamma)(A)$ for each $A \in \mathsf{FinDiff}(\mathcal{X})$.

We claim μ is the least upper bound of Γ. We need to show that for any $\nu \in \Gamma$ and $\nu' \in \mathcal{M}_{=1}(\mathcal{X})$ such that ν' is an $\preceq_{\sqsubseteq}$-upper-bound of Γ, $\nu \preceq_{\sqsubseteq} \mu \preceq_{\sqsubseteq} \nu'$. It suffices to show that for each $\sqsubseteq$-downward closed D, $\nu(D) \geq \mu(D) \geq \nu'(D)$. (Please note that $\nu(D) \geq \nu'(D)$ follows from the fact that ν' is an upper-bound of Γ).

Note that if $D = D_a$ for some $a \in X$ then we have by definition of $\nabla_{\sqsubseteq}(\Gamma)$, $\nu(D_a) \geq \mu(D_a) \geq \nu'(D_a)$. If D is finitely generated by the canonical generating set S, then we have $\lambda(D) = \sum_{a\in S}\lambda(D_a)$ for each $\lambda \in \{\nu, \mu, \nu'\}$. Hence $\nu(D) \geq \mu(D) \geq \nu'(D)$ for each finitely generated D.

Now if D is an arbitrary $\sqsubseteq$-downward closed set (not necessarily finitely generated), then fix an enumeration $a_0, a_1, \ldots$ of elements of D. Let $D_i = \cup_{0\leq i} D_{a_i}$. Clearly $\{D_i \mid i \in \mathbb{N}\}$ is an increasing sequence of finitely generated downward closed sets and $\lim_{i\to\infty} D_i = D$. Hence, by Proposition B.14, $\lim_{i\to\infty}\lambda(D_i) = \lambda(D)$ for each $\lambda \in \{\nu, \mu, \nu'\}$. Now, as D_i is finitely generated, we have $\nu(D_i) \geq \mu(D_i) \geq \nu'(D_i)$ and hence $\nu(D) \geq \mu(D) \geq \nu'(D)$ also. □

Combining Theorem 4.9, Theorem 5.6 and Lemma B.23, we get the main result of the paper.

Theorem 5.8 *Let $\mathcal{X} = (X, \Sigma, \sqsubseteq)$ be a countable order-respecting measurable space and let $\Lambda(\mathcal{X}) = (\mathsf{At}(\mathcal{X}), \mathcal{P}(\mathsf{At}(\mathcal{X})), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ be its atom space. Then $\mathcal{X}$*

admits least upper bounds iff $(\mathsf{At}(\mathcal{X}), \sqsubseteq_{\mathsf{At}(\mathcal{X})})$ *is a tree-like partial order.*

C Three-valued PCTL for MDPs

We show how to extend the the 3-valued PCTL defined for Abstract Markov Chains [9] to MDPs. For the semantics, we assume a total partial order $\leq$ on $\mathbb{B}_3 = \{\bot, ?, \top\}$ defined as $\bot < ? < \top$. The semantics also assumes two operations $\bar{\cdot} : \mathbb{B}_3 \to \mathbb{B}_3$ and $\cdot \sqcap \cdot : \mathbb{B}_3 \times \mathbb{B}_3 \to \mathbb{B}_3$ defined as follows–

- $\overline{?} = ?; \overline{\top} = \bot$ and $\overline{\bot} = \top$.
- $c \sqcap d = \min(c, d)$.

For an MDP $\mathcal{M} = (Q, \to, L)$ [5], the set of ω-sequences of Q (denoted Q^ω) shall henceforth be called the set of *paths*. Given a finite word $\eta \in Q^+$, let $\mathcal{C}(\eta) = \{\pi \in Q^\omega \mid \eta \text{ is a prefix of } \pi\}$. Let Σ be the measure space generated by the set $\{\mathcal{C}(\eta) \mid \eta \in Q^+\}$. We also assume that the reader is familiar with the concept of schedulers. A scheduler resolves non-determinism. Formally, a scheduler is a function $\mathcal{S} : Q^+ \to \mathcal{M}_{=1}(Q)$ such that for any $\eta = q_0, q_2, \ldots q_n$, $(q_n, \mathcal{S}\eta) \in \to$. In presence of a scheduler $\mathcal{S}$, a MDP becomes a (countable) DTMC and generates a probability measure $\Pr^{\mathcal{S}}_{\mathcal{M}}$ on Σ. We omit the details of this construction and the reader is referred to [24] for a complete construction.

We are ready to define the semantics of the 3-valued PCTL for MDPs. Given a state $q \in Q$ and a formula φ, the function $[\![q, \varphi]\!]_{\mathcal{M}}$ is defined in Figure C.1. Please note that the semantics assumes the following auxiliary functions–

- $[\![\pi, \psi]\!]_{\mathcal{M}}$ is a function which given a path $\pi \in Q^\omega$ and a path formula [6] ψ returns an element in $\mathbb{B}_3$. This function is also defined in Figure C.1.
- $\Pr^l_{\mathcal{M}}(q, \psi, c)$ which given $q \in Q$, a path formula ψ and $c \in \mathbb{B}_3$ is defined as– $\Pr^l_{\mathcal{M}}(q, \psi, c) = \inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(\{\pi \mid \pi(0) = q \text{ and } [\![\pi, \psi]\!]_{\mathcal{M}} = c\})$.

We need to show that if $q \preceq q'$ then for any formula φ, $[\![q', \varphi]\!]_{\mathcal{M}} \neq ?$ implies that $[\![q, \varphi]\!]_{\mathcal{M}} = [\![q', \varphi]\!]_{\mathcal{M}}$. We recall some relevant notation and results proved in [6].

Notation: Sometimes it will be useful to consider MDPs which are not labeled by propositions. A pair $\mathcal{M} = (Q, \to)$ is be said to be a *unlabeled* MDP if Q is a finite set of states and $\to \subseteq Q \times \mathcal{M}_{=1}((Q, \mathcal{P}(Q)))$. As expected, we can extend the definition of simulation to unlabeled MDPs. For any $q_0 \in Q$ and set $Q_1 \subseteq Q$, let $Reach(q_0, Q_1) = \{\pi \in Q^\omega \mid \pi(0) = q_0 \text{ and } \exists j \in \mathbb{N}.\ \pi(j) \in Q_1\}$.

[5] We only consider the case where Q is finite.
[6] A path formula is either $X\varphi$ or $\varphi \,\mathcal{U}\, \phi$ where φ and ϕ are PCTL formulas.

$$
\begin{array}{lcl}
[\![q, \text{true}]\!]_{\mathcal{M}} & = & \top \\
[\![q, a]\!]_{\mathcal{M}} & = & L(q,a) \\
[\![q, \neg\varphi]\!]_{\mathcal{M}} & = & \overline{[\![q,\varphi]\!]_{\mathcal{M}}} \\
[\![q, \varphi \wedge \phi]\!]_{\mathcal{M}} & = & [\![q,\varphi]\!]_{\mathcal{M}} \sqcap [\![q,\phi]\!]_{\mathcal{M}} \\
[\![q, \mathcal{P}_{\leq p}(\psi)]\!]_{\mathcal{M}} & = & \begin{cases} \top \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\bot) \geq 1-p \\ \bot \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\top) > p \\ ? \text{ otherwise} \end{cases} \\
[\![q, \mathcal{P}_{<p}(\psi)]\!]_{\mathcal{M}} & = & \begin{cases} \top \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\bot) > 1-p \\ \bot \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\top) \geq p \\ ? \text{ otherwise} \end{cases} \\
[\![q, \mathcal{P}_{\geq p}(\psi)]\!]_{\mathcal{M}} & = & \begin{cases} \top \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\top) \geq p \\ \bot \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\bot) > 1-p \\ ? \text{ otherwise} \end{cases} \\
[\![q, \mathcal{P}_{>p}(\psi)]\!]_{\mathcal{M}} & = & \begin{cases} \top \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\top) > p \\ \bot \text{ if } \Pr^l_{\mathcal{M}}(q,\psi,\bot) \geq 1-p \\ ? \text{ otherwise} \end{cases} \\
[\![\pi, X\varphi]\!]_{\mathcal{M}} & = & [\![\pi(1),\varphi]\!]_{\mathcal{M}} \\
[\![\pi, \varphi\, \mathcal{U}\, \phi]\!]_{\mathcal{M}} & = & \begin{cases} \top \text{ if } \exists i.([\![\pi(i),\phi]\!]_{\mathcal{M}} = \top \text{ and } \forall 0 \leq j < i [\![\pi(j),\varphi]\!]_{\mathcal{M}} = \top) \\ \bot \text{ if } \forall i.([\![\pi(i),\phi]\!]_{\mathcal{M}} \neq \bot \Longrightarrow \exists 0 \leq j < i [\![\pi(j),\varphi]\!]_{\mathcal{M}} = \bot) \\ ? \text{ otherwise} \end{cases}
\end{array}
$$

Table C.1
Semantics for three-valued PCTL

The following result is proved in [6].

Theorem C.1 *Given an unlabeled MDP $\mathcal{M} = (Q, \rightarrow)$ and a simulation relation $\sqsubseteq \subseteq Q \times Q$ on $\mathcal{M}$, let $q, q' \in Q$ be such that $q \sqsubseteq q'$.*

(1) For any $\sqsubseteq$-upward closed set U, $\sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(Reach(q,U)) \leq \sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(Reach(q',U))$.

(2) For any $\sqsubseteq$-downward closed set D, $\inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(Reach(q,D)) \geq \inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(Reach(q',D))$.

From this we can deduce the following.

Lemma C.2 *Given propositions a and b labeling an MDP $\mathcal{M} = (Q, \rightarrow, L)$*

and state $q_0 \in Q$, let $A(q_0) = \{\pi \in Q^\omega \mid \pi(0) = q_0$ and $[\![\pi, b\,\mathcal{U}\,a]\!]_{\mathcal{M}} = \top\}$. Then given a simulation relation $\sqsubseteq \subseteq Q \times Q$, states q, q' such that $q \sqsubseteq q'$,

$$\inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(A(q)) \geq \inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(A(q')).$$

Proof. Let $Q_1 = \{q_1 \in Q \mid L(q_1, b) \neq \top$ and $L(q_1, a) \neq \top\}$ and let $Q_2 = Q \setminus Q_1$. Clearly Q_1 is a $\sqsubseteq$-upward closed set and Q_2 a downward closed set. Without loss of generality, we can assume that $q' \in Q_2$ (otherwise the result follows trivially). Thus $q \in Q_2$ also.

Pick a new state $q_\top \notin Q$. Let $Q_\top = Q_2 \cup \{q_\top\}$. Furthermore for any $\mu \in \mathcal{M}_{=1}((Q, \mathcal{P}(Q)))$, let $\mu_\top \in \mathcal{M}_{=1}((Q_\top, \mathcal{P}(Q_\top)))$ be defined as follows–

$$\mu_\top(q_2) = \begin{cases} \mu(q_2) \text{ if } q_2 \in Q_2 \\ \mu(Q_1) \text{ if } q_2 = q_\top. \end{cases}$$

Finally, let $\delta_{q_\top}$ be the unique probability measure such that $\delta_{q_\top}(q_\top) = 1$.

Consider the unlabeled MDP $\mathcal{M}_\top = (Q_\top, \to_\top)$ where

$$\to_\top = (q_\top, \delta_{q_\top}) \cup \{(q_2, \mu_2) \mid q_2 \in Q_2 \text{ and } \exists \mu.\ \mu_2 = \mu_\top \text{ and } q_2 \to \mu\}.$$

Let $D \subseteq Q_2 = \{q_2 \mid L(q_2, a) = \top\}$. It is easy to see that for any $q_2 \in Q_2$,

$$\inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(A(q_2)) = \inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}_\top}(\mathit{Reach}(q_2, D)).$$

Now consider the relation $\sqsubseteq_\top = (\sqsubseteq \cap (Q_2 \times Q_2)) \cup (Q_\top \times \{q_\top\})$. It is easy to see that $\sqsubseteq_\top$ is a simulation relation on $\mathcal{M}_\top$ and D is a $\sqsubseteq_\top$-downward closed set. Therefore the desired result follows from Theorem C.1. □

We also have the following.

Lemma C.3 *Given propositions a and b labeling an MDP $\mathcal{M} = (Q, \to, L)$, and state q_0, let $B(q_0) = \{\pi \in Q^\omega \mid \pi(0) = q_0$ and $[\![\pi, b\,\mathcal{U}\,a]\!]_{\mathcal{M}} = \bot\}$. Then given a simulation relation $\sqsubseteq \subseteq Q \times Q$, states q, q' such that $q \sqsubseteq q'$,*

$$\inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(B(q)) \geq \inf_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(B(q')).$$

Proof. Please note that as $B(q_0) = Q^\omega \setminus C(q_0)$ where

$$C(q_0) = \{\pi \in Q^\omega \mid \pi(0) = q_0 \text{ and } [\![\pi, b\,\mathcal{U}\,a]\!]_{\mathcal{M}} \in \{\top, ?\}\},$$

it suffices to show that

$$\sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(C(q)) \leq \sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr{}^{\mathcal{S}}_{\mathcal{M}}(C(q')).$$

Let $Q_1 = \{q_1 \in Q \mid L(q_1, b) \neq \bot \text{ or } L(q_1, a) \neq \bot\}$ and let $Q_2 = Q \setminus Q_1$. Clearly Q_1 is a $\sqsubseteq$-upward closed set and Q_2 a downward closed set. Without loss of generality, we can assume that $q \in Q_1$ (otherwise the result follows trivially). Thus $q' \in Q_1$ also.

Pick a new state $q_\bot \notin Q$. Let $Q_\bot = Q_1 \cup \{q_\bot\}$. Furthermore for any $\mu \in \mathcal{M}_{=1}((Q, \mathcal{P}(Q)))$, let $\mu_\bot \in \mathcal{M}_{=1}((Q_\bot, \mathcal{P}(Q)))$ be defined as follows–

$$\mu_\bot(q_1) = \begin{cases} \mu(q_1) \text{ if } q_1 \in Q_1 \\ \mu(Q_2) \text{ if } q_1 = q_\bot. \end{cases}$$

Finally, let $\delta_{q_\bot}$ be the unique probability measure such that $\delta_{q_\bot}(q_\bot) = 1$.

Consider the unlabeled MDP $\mathcal{M}_\bot = (Q_\bot, \to_\bot)$ where

$$\to_\bot = (q_\bot, \delta_{q_\bot}) \cup \{(q_1, \mu_1) \mid q_1 \in Q_1 \text{ and } \exists \mu.\ \mu_1 = \mu_\bot \text{ and } q_1 \to \mu\}.$$

Let $U \subseteq Q_1 = \{q_1 \mid L(q_1, a) \neq \bot\}$. It is easy to see that for any $q_1 \in Q_1$,

$$\sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}}(C(q_1)) = \sup_{\{\mathcal{S} \text{ is a scheduler}\}} \Pr^{\mathcal{S}}_{\mathcal{M}_\bot}(Reach(q_1, U)).$$

Now consider the relation $\sqsubseteq_\bot = (\sqsubseteq \cap (Q_1 \times Q_1)) \cup (\{q_\bot\} \times Q_\bot)$. It is easy to see that $\sqsubseteq_\bot$ is a simulation relation on $\mathcal{M}_\bot$ and U is a $\sqsubseteq_\bot$-upward closed set. Therefore the desired result follows again from Theorem C.1. □

We have the main theorem of this Section.

Theorem C.4 *Consider q, q' states of MDP $\mathcal{M} = (Q, \to, L)$ such that $q \preceq q'$. For any formula φ, if $[\![q', \varphi]\!]_{\mathcal{M}} \neq ?$ then $[\![q, \varphi]\!]_{\mathcal{M}} = [\![q', \varphi]\!]_{\mathcal{M}}$.*

Proof. The proof proceeds by induction on the structure of φ. We consider just the case when φ is $\mathcal{P}_{\leq p}(\varphi_1 \,\mathcal{U}\, \varphi_2)$.

Pick two new propositions a_{φ_1} and a_{φ_2}. Let $\mathcal{M}_{\mathsf{new}}$ be a MDP which is same as $\mathcal{M}$ except that $L(q_0, a_{\varphi_i}) = [\![q_0, \varphi_i]\!]_{\mathcal{M}}$ for each $q_0 \in Q$ and $i \in \{1, 2\}$. It is easy to see that $[\![q_0, \varphi]\!]_{\mathcal{M}} = [\![q_0, \mathcal{P}_{\leq p}(a_{\varphi_1} \,\mathcal{U}\, a_{\varphi_2})]\!]_{\mathcal{M}_{\mathsf{new}}}$. Let $\varphi_{\mathsf{new}} = \mathcal{P}_{\leq p}(a_{\varphi_1} \,\mathcal{U}\, a_{\varphi_2})$.

Observe by induction hypothesis, if $q_0 \sqsubseteq q'_o$ then $L(q'_0, a_{\varphi_i}) \neq ?$ implies $L(q'_0, a_{\varphi_i}) = L(q_0, a_{\varphi_i})$ for each $i \in \{1, 2\}$. Hence $\sqsubseteq$ is a simulation on $\mathcal{M}_{\mathsf{new}}$ also.

Now, if $[\![q', \varphi]\!]_{\mathcal{M}} \neq ?$ then $[\![q', \varphi_{\mathsf{new}}]\!]_{\mathcal{M}_{\mathsf{new}}} = \top$ or $\bot$. If $[\![q', \varphi_{\mathsf{new}}]\!] = \top$ then we have $\mathcal{P}^l_{\mathcal{M}_{\mathsf{new}}}(q', a_{\varphi_1} \,\mathcal{U}\, a_{\varphi_2}, \bot) > 1 - p$. This implies that $\mathcal{P}^l_{\mathcal{M}_{\mathsf{new}}}(q, a_{\varphi_1} \,\mathcal{U}\, a_{\varphi_2}, \bot) > 1 - p$ also (see Lemma C.3). Hence $[\![q, \varphi]\!]_{\mathcal{M}} = [\![q, \varphi_{\mathsf{new}}]\!] = \top$. Similarly, we can show that if $[\![q', \varphi_{\mathsf{new}}]\!]_{\mathcal{M}_{\mathsf{new}}} = \bot$ then $[\![q, \varphi]\!]_{\mathcal{M}} = \bot$. □

D PRISM code for MDPs in Section 7

MDP for the random walk. We present below the PRISM code for the random walk in Section 7.1. For $1 \leq n \leq 3$, the MDP state x_n is modeled by the state $row = 0, column = n$, y_n is modeled by the state $row = 1, column = n$, and z_n by the state $row = 2, column = n$. The state $row = 3$ models the MDP state u. The states $column = 0$ and $column = 4$ model the MDP states ℓ and r respectively. Note that for the property under consideration, we can consider the states $row = 3$, $column = 0$ and $column = 4$ absorbing.

```
mdp


module threeband

    row : [0..3] init 0;
    column:  [0..4] init 2;



    //row=0, column =1
    [] row =0 & column=1 -> 0.25:(column'=0) +0.25:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=1 -> 0.5:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=1 -> 0.25:(row'=row) + 0.25:(column'=2) + 0.5:(row'=1);

    //row=0, column =2
    [] row =0 & column=2 -> 0.25:(column'=1) +0.25:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=2 -> 0.5:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=2 -> 0.25:(row'=row) + 0.25:(column'=3) + 0.5:(row'=1);

    //row=0, column= 3
    [] row =0 & column=3 -> 0.25:(column'=2) +0.25:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=3 -> 0.5:(row'=row) + 0.5:(row'=1);
    [] row =0 & column=3 -> 0.25:(row'=row) + 0.25:(column'=4) + 0.5:(row'=1);


    //row=1, column =1
    [] row =1 & column=1 -> 0.25:(column'=0) +0.25:(row'=row) +
                                              0.25:(row'=0)+ 0.25:(row'=2);
    [] row =1 & column=1 -> 0.5:(row'=row) + 0.25:(row'=0)+ 0.25:(row'=2);
    [] row =1 & column=1 -> 0.25:(row'=row) + 0.25:(column'=2) +
                                              0.25:(row'=0)+ 0.25:(row'=2);

    //row=1, column =2
```

```
[] row =1 & column=2 -> 0.25:(column'=1) +0.25:(row'=row) +
                                          0.25:(row'=0)+ 0.25:(row'=2);
[] row =1 & column=2 -> 0.5:(row'=row) + 0.25:(row'=0)+ 0.25:(row'=2);
[] row =1 & column=2 -> 0.25:(row'=row) + 0.25:(column'=3) +
                                         0.25:(row'=0)+ 0.25:(row'=2);

//row=1, column= 3
[] row =1 & column=3 -> 0.25:(column'=2) +0.25:(row'=row) +
                                          0.25:(row'=0)+ 0.25:(row'=2);
[] row =1 & column=3 -> 0.5:(row'=row) + 0.25:(row'=0)+ 0.25:(row'=2);
[] row =1 & column=3 -> 0.25:(row'=row) + 0.25:(column'=4) +
                                          0.25:(row'=0)+ 0.25:(row'=2);


//row=2, column =1
[] row =2 & column=1 -> 0.25:(column'=0) +0.25:(row'=row) +
                                          0.25:(row'=3)+ 0.25:(row'=1);
[] row =2 & column=1 -> 0.5:(row'=row) + 0.25:(row'=3)+ 0.25:(row'=1);
[] row =2 & column=1 -> 0.25:(row'=row) + 0.25:(column'=2) +
                                         0.25:(row'=3)+ 0.25:(row'=1);

//row=2, column =2
[] row =2 & column=2 -> 0.25:(column'=1) +0.25:(row'=row) +
                                         0.25:(row'=3)+ 0.25:(row'=1);
[] row =2 & column=2 -> 0.5:(row'=row) + 0.25:(row'=3)+ 0.25:(row'=1);
[] row =2 & column=2 -> 0.25:(row'=row) + 0.25:(column'=3) +
                                          0.25:(row'=3)+ 0.25:(row'=1);

//row=2, column= 3
[] row =2 & column=3 -> 0.25:(column'=2) +0.25:(row'=row) +
                                          0.25:(row'=3)+ 0.25:(row'=2);
[] row =2 & column=3 -> 0.5:(row'=row) + 0.25:(row'=3)+ 0.25:(row'=1);
[] row =2 & column=3 -> 0.25:(row'=row) + 0.25:(column'=4) +
                                          0.25:(row'=3)+ 0.25:(row'=1);


endmodule
```

MDP for the random walk with phase transition. We present below the PRISM code for the random walk in Section 7.2. The MDP state x is modeled by the state $row = 0, column = 1$, y by the state $row = 1, column = 1$, and z by the state $row = 2, column = 1$. The state $row = 3$ models the MDP state u. The states $column = 0$ and $column = 2$ model the MDP states ℓ and r respectively. Note that for the property under consideration, we can

consider the states $row = 3$, $column = 0$ and $column = 2$ absorbing.

```
mdp


module oneband

    row : [0..3] init 0;
    column:  [0..2] init 1;



    //row=0
    [] row =0 & column=1 -> 1/4:(column'=0) +1/4:(row'=row) + 1/2:(row'=1);
    [] row =0 & column=1 -> 1/2:(row'=row) + 1/2:(row'=1);
    [] row =0 & column=1 -> 3/8:(row'=row) + 5/8:(row'=1);
    [] row =0 & column=1 -> 1/8:(row'=row) + 1/4:(column'=2) + 5/8:(row'=1);



    //row=1
    [] row =1 & column=1 -> 1/4:(column'=0) +1/4:(row'=row) +
                                              1/4:(row'=0)+ 1/4:(row'=2);
    [] row =1 & column=1 -> 1/2:(row'=row) + 1/4:(row'=0)+ 1/4:(row'=2);
    [] row =1 & column=1 -> 3/8:(row'=row) + 5/16:(row'=0)+ 5/16:(row'=2);
    [] row =1 & column=1 -> 1/8:(row'=row) + 1/4:(column'=2)+ 5/16:(row'=0)+
                                              5/16:(row'=2);



    //row=2
    [] row =2 & column=1 -> 1/4:(column'=0) +1/4:(row'=row) +
                                              1/4:(row'=1)+ 1/4:(row'=3);
    [] row =2 & column=1 -> 1/2:(row'=row) + 1/4:(row'=1)+ 1/4:(row'=3);
    [] row =2 & column=1 -> 3/8:(row'=row) + 5/16:(row'=1)+
                                              5/16:(row'=3);
    [] row =2 & column=1 -> 1/8:(row'=row) + 1/4:(column'=2)+
                                              5/16:(row'=0)+ 5/16:(row'=3);



endmodule
```