

On the Relationship between Bisimulation and Trace Equivalence in an Approximate Probabilistic Context (Extended Version)

Gaoang Bian^{1,2} and Alessandro Abate²

¹ Google Inc, United States

² Dept. of Computer Science, University of Oxford, UK

Abstract. This work introduces a notion of approximate probabilistic trace equivalence for labelled Markov chains, and relates this new concept to the known notion of approximate probabilistic bisimulation. In particular this work shows that the latter notion induces a tight upper bound on the approximation between finite-horizon traces, as expressed by a total variation distance. As such, this work extends corresponding results for exact notions and analogous results for non-probabilistic models. This bound can be employed to relate the closeness in satisfaction probabilities over bounded linear-time properties, and allows for probabilistic model checking of concrete models via abstractions. The contribution focuses on both finite-state and uncountable-state labelled Markov chains, and claims two main applications: firstly, it allows an upper bound on the trace distance to be decided for finite state systems; secondly, it can be used to synthesise discrete approximations to continuous-state models with arbitrary precision.

1 Introduction

Often in formal verification one is interested in approximations of concrete models. Models are often built from experimental data that are themselves approximate, and taking approximations can reduce the size and complexity of the state space. Markov models in particular can be defined either syntactically as a transition structure (with states and matrices), or semantically as a random process whose trajectory satisfy the Markov property. Each representation gives rise to its own notions of approximation [1]: “the transition matrices have similar numbers and/or structure” vs “the trajectories have similar probability distributions”, respectively. While the syntactic representation is used for computations and model checking with concrete numbers, often one is interested in results in terms of the semantics, e.g. “what is the probability of reaching a failure state within 100 steps”. This gives practical value to studying how approximations in terms of transition matrices translate into approximations in terms of traces of the random process.

In this paper we build on the notion of ε -approximate probabilistic bisimulation, introduced in [12] as a natural extension to exact probabilistic bisimulation [11]. There, the notion of ε -approximate probabilistic bisimulation (or just

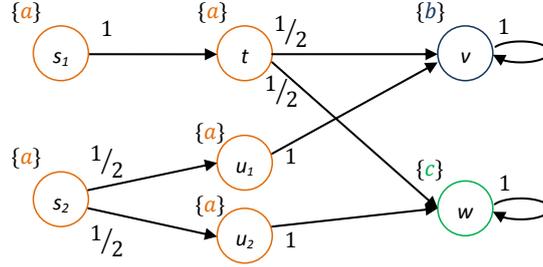


Fig. 1. Branching vs Linear Time Behaviour. In the Labelled Markov Chain below (cf. Section 2 for the LMC model), the states s_1, s_2 both emit traces $\langle\{a\}, \{a\}, \{b\}\rangle$ and $\langle\{a\}, \{a\}, \{c\}\rangle$ with probability 0.5 each, and hence s_1, s_2 have the same linear time behaviour. However, s_1, s_2 have different branching behaviour, since exclusively s_1 satisfies the PCTL formula $P_{=1} [X P_{=0.5} [X b]]$. Conversely, only s_2 satisfies $P_{=0.5} [X P_{=1} [X b]]$.

ε -bisimulation) is defined in terms of the transition structure, and given ε the maximal ε -bisimulation relation can be computed for finite state systems with n states in $\mathcal{O}(n^7)$ time [12].

It is on the other hand of interest to explore what ε -bisimulation means in terms of trajectories. While ε -bisimulation does have characterizations (on countable state spaces) in terms of logics and games [11], this logic is branching in nature, and does not directly relate to the trajectory of the model as it leaks information about the state space (similarly to the difference between CTL and LTL), as illustrated in Figure 1.

In this paper, we investigate what ε -approximate probabilistic bisimulation means in terms of trajectories. We will prove that for Labelled Markov Chains (over potentially uncountable state spaces), ε -bisimulation between two states places the tight upper bound of $1 - (1 - \varepsilon)^k$ (which is $\leq k\varepsilon$) on the total variation [17] between the distributions of length $k+1$ traces starting from those states, for all $k \in \mathbb{N}$. We will formulate these bounds by introducing the notion of $f(k)$ -trace equivalence. As such, we extend the well known result that bisimulation implies trace equivalence in non-probabilistic systems to the context of approximate and probabilistic models (the exact probabilistic case having been considered in [6]).

One direct repercussion of our result is that it provides a method to efficiently bound the total variation of length k traces from two finite-state LMCs (or two states in an LMC), since the aforementioned result in [12] can be used to decide or to compute ε -bisimulation between two states in polynomial time. We will also apply our results to the quantitative verification of continuous-state Markov models [2, 3, 15], improving on the current class of properties approximated and the corresponding approximation errors.

Related Work. Literature on approximations of (finite-state) Markov models can be distinguished into two main branches: one focusing on one-step similarity,

the other dealing with trace distances. One-step similarity can be studied via the notion of probabilistic bisimulation, introduced in the context of finite-state models by [19], and related to lumpability in [22]. [12] discusses a notion of approximate bisimulation, related to quasi-lumpability conditions in [5, 21]. From the perspective of process algebra, [16] studies operators on probabilistic transition systems that preserve the approximate bisimulation distance. The work in [12, 20] is seminal in introducing notions of (exact) probabilistic simulation, much extended in subsequent literature.

On the other hand, there are a few papers studying the total variation distance over traces. [8] presents an algorithm for approximating the total variation of infinite traces of labelled Markov systems and prove the problem of deciding whether it exceeds a given threshold to be NP-hard. [7] shows that the undiscounted bisimilarity pseudometric is a (non-tight) upper bound on the total variation of infinite traces (like ε -bisimulation, the bisimilarity pseudometric is defined on the syntax of the model and there are efficient algorithms for computing it [7, 9, 23]). The contribution in this paper, focusing on finite traces rather than infinite traces, is that the total variation of finite traces is much less conservative, and moreover allows manipulating models under specific error bounds on length k traces, as we will show in Section 5.

[13] studies notions based on the total variation of finite and infinite traces: employing a different notion of ε -bisimulation than ours, it proves error bounds on trace distances, which however depend on additional properties of the structure of the transition kernel (as shown in Section 7 the error bound on reachability probabilities could go to 1 in two steps, for any $\varepsilon > 0$). Finite abstractions of continuous-state Markov models can be synthesised by notions that are variations of the ε -bisimulation in this work [1, 3, 15]. Tangential to our work, [10] shows that the total variation of finite traces can be statically estimated via repeated observations. [25] investigates ways of compressing Hidden Markov Models by searching for a smaller model that minimises the total variation of length- k traces of the two models.

Structure of this article. In Section 2, we introduce the reference model (labelled Markov chains – LMC – over general state spaces) and provide a definition of ε -bisimulation for LMCs. In Section 3, we introduce the notion of approximate probabilistic trace equivalence (and the derived notion of probabilistic trace distance), and discuss how it relates to bounded linear time properties, and to the notion of distinguishability. In Section 4, we present the main result: we will derive a tight upper bound on the probabilistic trace distance between ε -bisimilar states. In Section 5, we show how these results can be used to approximately model check continuous state systems, and Section 6 discusses a case study. In Section 7, we discuss an alternative notion of approximate probabilistic bisimulation that appears in literature and show that it cannot be used to effectively bound probabilistic trace distance. The Appendix contains the lengthier proofs of some the statements in this work and details on the implementation of the Case Study.

2 Preliminaries

2.1 Labelled Markov Chains

We will work with discrete-time Labelled Markov Chains (LMCs) over general state spaces. Known definitions of countable- or finite-state LMCs represent special instances of the general models we introduce next.

Definition 1 (LMC syntax). *A Labelled Markov Chain (LMC) is a structure $\mathcal{M} = (S, \Sigma, \tau, L)$ where:*

- S is a (potentially uncountable) set of states.
- $\Sigma \subseteq \mathcal{P}(S)$ is a Σ -algebra over S representing the set of measurable subsets of S .
- $\tau : S \times \Sigma \rightarrow [0, 1]$ is a transition kernel. That is, for all $s \in S$, $\tau(s, \cdot)$ is a probability measure on the measure space (S, Σ) , and for all $A \in \Sigma$ we require $\tau(\cdot, A)$ to be Σ -measurable.
- $L : S \rightarrow \mathcal{O}$ labels each state $s \in S$ with a subset of atomic propositions from AP, where $\mathcal{O} = 2^{\text{AP}}$. L is required to be Σ -measurable, and we will assume AP to be finite.

$L(s)$ captures all the observable information at state $s \in S$: this drives our notion relating pairs of states, and we characterise properties over the codomain of this function.

Definition 2 (LMC semantics). *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC. Given an initial distribution p_0 over S , the state of \mathcal{M} at time k is a random variable $\mathcal{M}_k^{p_0}$ over S , such that*

$$\begin{aligned} \mathbb{P}[\mathcal{M}_0^{p_0} \in A_0] &= p_0(A_0), \\ \mathbb{P}[\mathcal{M}_0^{p_0} \in A_0, \dots, \mathcal{M}_k^{p_0} \in A_k] &= \int_{y_0 \in A_0} p_0(dy_0) \\ &\quad \cdot \int_{y_1 \in A_1} \tau(y_0, dy_1) \cdots \int_{y_{k-1} \in A_{k-1}} \tau(y_{k-2}, dy_{k-1}) \cdot \tau(y_{k-1}, A_k), \end{aligned}$$

for all $k \in \mathbb{N} \setminus \{0\}$, $A_k \in \Sigma$, where of course $\tau(y_{k-1}, A_k) = \int_{y_k \in A_k} \tau(y_{k-1}, dy_k)$.

Models in related work. A body of related literature works with labelled MDPs, which are more general models allowing a non-deterministic choice $u \in \mathcal{U}$ (for some finite \mathcal{U}) of the transition kernel τ_u at each step. This choice is made by a “policy” that probabilistically selects u based on past observations of the process. Whilst we will ignore non-determinism and work with LMCs for simplicity, our results can be adapted to labelled MDPs by quantifying over all policies, or over all choices u for properties like ε -bisimulation, in order to remove the non-determinism. The seminal work on bisimulation and ε -bisimulation dealt with models known as LMPs [11]. LMPs allow for non-determinism (like labelled MDPs) but their states are unlabelled and at each step they have a probability of halting. For the study of bisimulation in this work, LMPs can be considered as a simplification of labelled MDPs to the case $\mathcal{O} = \{\emptyset, \{\text{halted}\}\}$.

2.2 Exact and Approximate Probabilistic Bisimulations

The notion of approximate probabilistic bisimulation (in this work just ε -bisimulation) is a structural notion of closeness, based on the stronger notion of exact probabilistic bisimulation [11]. We discuss both next. Considering a binary relation R over set X , we say that a subset $\tilde{S} \subseteq X$ is R -closed if \tilde{S} contains its own image under R . That is, if $R(\tilde{S}) := \{y \in X \mid x \in \tilde{S}, xRy\} \subseteq \tilde{S}$.

Definition 3 (Exact probabilistic bisimulation). *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC. An equivalence relation $R \subseteq S \times S$ over the state space is an exact probabilistic bisimulation relation if*

$$\forall (s_1, s_2) \in R, \quad \text{we have that } L(s_1) = L(s_2),$$

$$\forall (s_1, s_2) \in R, \forall \tilde{T} \in \Sigma \text{ s.t. } \tilde{T} \text{ is } R\text{-closed}, \quad \text{we have that } \tau(s_1, \tilde{T}) = \tau(s_2, \tilde{T}).$$

A pair of states $s_1, s_2 \in S$ are said to be (exactly probabilistically) bisimilar if there exists an exact probabilistic bisimulation relation R such that $s_1 R s_2$.

Note that since R is an equivalence relation, R -closed sets are exactly the unions of whole equivalence classes.

Next, we adapt the notion of ε -bisimulation (as discussed in [12] for LMPs over countable state spaces) to LMCs over general spaces.

Definition 4 (ε -bisimulation). *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC. For $\varepsilon \in [0, 1]$, a symmetric binary relation $R_\varepsilon \subseteq S \times S$ over the state space is an ε -approximate probabilistic bisimulation relation (or just ε -bisimulation relation) if*

$$\forall T \in \Sigma, \quad \text{we have } R_\varepsilon(T) \in \Sigma, \tag{1}$$

$$\forall (s_1, s_2) \in R_\varepsilon, \quad \text{we have } L(s_1) = L(s_2), \tag{2}$$

$$\forall (s_1, s_2) \in R_\varepsilon, \forall T \in \Sigma, \quad \text{we have } \tau(s_2, R_\varepsilon(T)) \geq \tau(s_1, T) - \varepsilon. \tag{3}$$

Two states $s_1, s_2 \in S$ are said to be ε -bisimilar if there exists an ε -bisimulation relation R_ε such that $s_1 R_\varepsilon s_2$.

The condition raised in (3) could be understood intuitively as “for any move that s_1 can take (say, into set T), s_2 can match it with higher likelihood over the corresponding set $R_\varepsilon(T)$, up to ε tolerance.” Notice that (1) is not a necessary requirement for countable state models, but for uncountable state models it is needed to ensure that $R_\varepsilon(T)$ is measurable and $\tau(s_2, R_\varepsilon(T))$ is defined in (3).

[12] showed that in countable state spaces, 0-approximate probabilistic bisimulation corresponds to exact probabilistic bisimulation. On uncountable state spaces, not every exact probabilistic bisimulation relation is a 0-bisimulation relation because of the additional measurability requirement, but we still have that 0-bisimulation implies exact probabilistic bisimulation.

Theorem 1. *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC, and let $s_1, s_2 \in S$. If s_1, s_2 are 0-bisimilar, then they are (exactly, probabilistically) bisimilar.*

Although above s_1, s_2 are required to belong to the state space of a given LMC, the notions of exact- and ε -bisimulation can be extended to hold over pairs of LMCs by combining their state spaces, as follows.

Definition 5 (ε -bisimulation of pairs of LMCs). *Consider two LMCs $\mathcal{M}_1 = (S_1, \Sigma_1, \tau_1, L_1)$ and $\mathcal{M}_2 = (S_2, \Sigma_2, \tau_2, L_2)$. Without loss of generality, assume that their state spaces S_1, S_2 are disjoint. The direct sum $\mathcal{M}_1 \oplus \mathcal{M}_2$ of \mathcal{M}_1 and \mathcal{M}_2 is the LMC formed by combining the state spaces of \mathcal{M}_1 and \mathcal{M}_2 . Formally, $\mathcal{M}_1 \oplus \mathcal{M}_2 = (S_1 \uplus S_2, \sigma(\Sigma_1 \times \Sigma_2), \tau_1 \oplus \tau_2, L_1 \uplus L_2)$, where:*

- $S_1 \uplus S_2$ is the union of S_1 and S_2 where we have assumed wlog (by relabelling if necessary) that S_1, S_2 are disjoint;
- $\sigma(\Sigma_1 \times \Sigma_2)$ is the smallest σ -algebra containing $\Sigma_1 \times \Sigma_2$;
- $\tau_1 \oplus \tau_2(s, T) := \begin{cases} \tau_1(s, T \cap S_1) & \text{if } s \in S_1 \\ \tau_2(s, T \cap S_2) & \text{if } s \in S_2 \end{cases}$ for $s \in S_1 \uplus S_2, T \in \sigma(\Sigma_1 \times \Sigma_2)$;
- $L_1 \uplus L_2(s) := \begin{cases} L_1(s) & \text{if } s \in S_1 \\ L_2(s) & \text{if } s \in S_2 \end{cases}$ for $s \in S_1 \uplus S_2$.

Let $s_1 \in S_1, s_2 \in S_2$. We say that s_1, s_2 are ε -bisimilar iff s_1, s_2 are ε -bisimilar as states in the direct sum LMC $\mathcal{M}_1 \oplus \mathcal{M}_2$.

Other Notions of ε -Bisimulation in Literature. There is an alternative, more direct, extension of exact probabilistic bisimulation in literature [1, 3, 13], which simply requires $|\tau(s_1, \tilde{T}) - \tau(s_2, \tilde{T})| \leq \varepsilon$ instead of the conditions in Def. 4. However, this requirement alone is too weak to guarantee properties that we later discuss (cf. Section 7).

3 Approximate Probabilistic Trace Equivalence for LMCs

In this section we introduce the concept of approximate probabilistic trace equivalence (or just $f(k)$ -trace equivalence) to represent closeness of observable linear time behaviour. Based on the likelihood over traces of a given LMC, this notion depends on its operational semantics (cf. Definition 2), rather than on the structure of its transition kernel (as in the case of approximate bisimulation). The notion can alternatively be thought of inducing a distance among traces, as elaborated below.

Definition 6 (Trace likelihood). *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be an LMC, $s_0 \in S$, and $k \in \mathbb{N}$. Let TRACE denote a set of traces (each of length $k + 1$), taking values in time over 2^{AP} , so that $\text{TRACE} \subseteq \mathcal{O}^{k+1}$. Denote with $P_k(s_0, \text{TRACE})$ the probability that the LMC \mathcal{M} , given an initial state s_0 , generates any of the runs $\langle \alpha_0, \dots, \alpha_k \rangle \in \text{TRACE}$, namely*

$$P_k(s_0, \text{TRACE}) = \sum_{\substack{\langle \alpha_0, \dots, \alpha_k \rangle \\ \in \text{TRACE}}} \mathbb{P}[\mathcal{M}_0^{s_0} \in L^{-1}(\{\alpha_0\}), \dots, \mathcal{M}_k^{s_0} \in L^{-1}(\{\alpha_k\})],$$

where $\mathcal{M}_t^{s_0}$ is the state of \mathcal{M} at step t , with a degenerate initial distribution p_0 that is concentrated on point s_0 (cf. Definition 2).

As intuitive, we consider traces of length $k + 1$ (rather than of length k) because a length $k + 1$ trace is produced by one initial state and precisely k transitions. Notice that the set of sequences of states generating TRACE is measurable, being defined via a measurable map L over a finite set of traces.

Definition 7 (Total variation [14]). Let (Z, \mathcal{G}) be a measure space where \mathcal{G} is a σ -algebra over Z , and let μ_1, μ_2 be probability measures over (Z, \mathcal{G}) . The total variation between μ_1, μ_2 is $d_{\text{TV}}(\mu_1, \mu_2) := \sup_{A \in \mathcal{G}} |\mu_1(A) - \mu_2(A)|$.

Definition 8 ($f(k)$ -trace equivalence). Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC. For a non-decreasing function $f : \mathbb{N} \rightarrow [0, 1]$, we say that states $s_1, s_2 \in S$ are $f(k)$ -approximate probabilistic trace equivalent if for all $k \in \mathbb{N}$,

$$d_{\text{TV}}(P_k(s_1, \cdot), P_k(s_2, \cdot)) \leq f(k),$$

or alternatively if over $\text{TRACE} \subseteq \mathcal{O}^{k+1}$,

$$|P_k(s_1, \text{TRACE}) - P_k(s_2, \text{TRACE})| \leq f(k).$$

The condition on monotonicity follows from the requirement on the total variation distance, which is defined over a product output space and necessarily accumulates over time. The notion of $f(k)$ -trace equivalence can be used to relate states from two different LMCs, much in the same way as ε -bisimulation.

One can introduce the notion of *probabilistic trace distance* between pairs of states s_1, s_2 as

$$\min\{f(k) \geq 0 \mid s_1 \text{ is } f(k)\text{-trace equivalent to } s_2\} = d_{\text{TV}}(P_k(s_1, \cdot), P_k(s_2, \cdot)).$$

Notice that the RHS is clearly a pseudometric. We discuss the development of tight bounds on the probabilistic trace distance in Section 4.

3.1 Interpretation and Application of ε -Trace Equivalence

The notion of ε -trace equivalence subsumes closeness of finite-time traces, and can be interpreted in two different ways. Firstly, ε -trace equivalence leads to closeness of satisfaction probabilities over bounded-horizon linear time properties, e.g. bounded LTL formulae, as follows.

Theorem 2. Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be an LMC, and let $s_1, s_2 \in S$ be ε -trace equivalent. Let ψ be any bounded LTL property over a k -step time horizon, defined within the LTL fragment $\phi = \top \mid a \mid \phi \wedge \phi \mid \neg\phi \mid \phi \text{U}^{\leq t} \phi$ for $t \leq k$. Then,

$$\left| \mathbb{P}[s_1 \models \psi] - \mathbb{P}[s_2 \models \psi] \right| \leq f(k),$$

where $P[s \models \psi]$ is the probability that starting from state s , the LMC satisfies property ψ .

Proof. Formula ψ is satisfied by a specific set of length $k + 1$ traces. \square

Alternatively, via its connection to the notion of total variation, ε -trace distance leads to the notion of distinguishability of the underlying LMC, namely the ability (of an agent external to the model) to distinguish a model by observing its traces.

Theorem 3. Let s_1, s_2 be two states of an LMC. Suppose one of them is selected by a secret fair coin toss. An external agent guesses which one has been selected by observing a trace of length $k + 1$ emitted from the unknown state. Then, an optimal agent guesses correctly with probability

$$\frac{1}{2} + \frac{1}{2}f(k),$$

with $f(k) = d_{\text{TV}}(P_k(s_1, \cdot), P_k(s_2, \cdot))$ being the probabilistic trace distance.

4 ε -Probabilistic Bisimulation induces Approximate Probabilistic Trace Equivalence

In this section we present the main result: we show that ε -bisimulation induces a tight upper bound on the probabilistic trace distance, quantifiable as $(1 - (1 - \varepsilon)^k)$. This translates to a guarantee on all the properties implied by ε -trace equivalence, such as closeness of satisfaction probabilities for bounded linear time properties. In addition, since for finite state LMPs the maximal ε -bisimulation relation can be computed in $\mathcal{O}(|S|^7)$ time [12], this result allows to establish an upper bound on the probabilistic trace distance with the same time complexity.

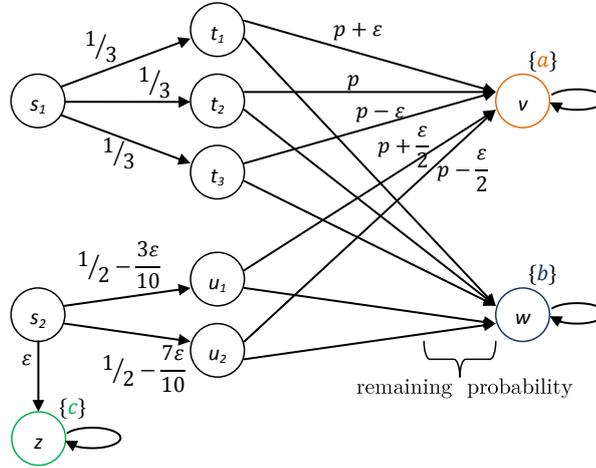


Fig. 2. LMC for the proof of Theorem 4.

Theorem 4 (ε -bisimulation implies $(1 - (1 - \varepsilon)^k)$ -trace equivalence). *Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC. If $s_1, s_2 \in S$ are ε -bisimilar, then s_1, s_2 are $(1 - (1 - \varepsilon)^k)$ -trace equivalent.*

Proof (Sketch). The full proof, developed for LMCs over uncountable state spaces, can be found in Appendix C. Here we offer a sketch of proof, employing the finite-state LMP in Figure 2 as an illustrating example (where for simplicity we have omitted the labels for internal states, which can as well be labelled with $\emptyset \in \mathcal{O}$).

The maximal (i.e. coarsest) ε -bisimulation relation R_ε is obtained by pairs of states within the sets

$$\{t_1, t_2, u_1\}, \{t_2, t_3, u_2\}, \{s_1, s_2\}, \{v\}, \{w\}, \{z\}.$$

We would like to prove that these ε -bisimilar states are also ε -trace equivalent. In the full proof, we will show this by induction on the length of the trace, for all ε -bisimilar states at the same time. In this sketch proof, we aim to illustrate the induction step by showing how to bound

$$|P_3(s_1, \diamond^{\leq 3} a) - P_3(s_2, \diamond^{\leq 3} a)|,$$

where $\diamond^{\leq k} a$ is the set of traces of length $k + 1$, which reach a state labelled with a (which in this case is just state v). The idea is to match each of the outgoing transitions from s_1 to an outgoing transition from s_2 and to an ε -bisimilar state. Specifically, we explicitly write

$$\begin{aligned} P_3(s_1, \diamond^{\leq 3} a) &= \frac{1}{3}P_2(t_1, \diamond^{\leq 2} a) + \frac{1}{6}P_2(t_2, \diamond^{\leq 2} a) \\ &+ \frac{1}{6}P_2(t_2, \diamond^{\leq 2} a) + \frac{1}{3}P_2(t_3, \diamond^{\leq 2} a), \end{aligned} \quad (4)$$

and respectively

$$\begin{aligned} P_3(s_2, \diamond^{\leq 3} a) &= \left(\frac{1}{3} - \frac{3\varepsilon}{10}\right) \cdot P_2(u_1, \diamond^{\leq 2} a) + \frac{1}{6}P_2(u_1, \diamond^{\leq 2} a) \\ &+ \frac{1}{6}P_2(u_2, \diamond^{\leq 2} a) + \left(\frac{1}{3} - \frac{7\varepsilon}{10}\right) \cdot P_2(u_2, \diamond^{\leq 2} a). \end{aligned} \quad (5)$$

We then match-off the terms in the expansions for $P_3(s_1, \diamond^{\leq 3} a)$ and $P_3(s_2, \diamond^{\leq 3} a)$, one term at a time. We use the induction hypothesis to argue that the probabilities in the matched terms are $(1 - (1 - \varepsilon)^k)$ -close to each other (here $k = 1$), since they concern ε -bisimilar states. That is,

$$\begin{aligned} |P_2(t_1, \diamond^{\leq 2} a) - P_2(u_1, \diamond^{\leq 2} a)| &\leq 1 - (1 - \varepsilon)^k \\ |P_2(t_2, \diamond^{\leq 2} a) - P_2(u_1, \diamond^{\leq 2} a)| &\leq 1 - (1 - \varepsilon)^k \\ \dots \end{aligned}$$

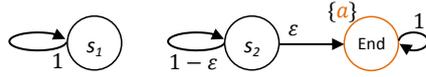
where again $k = 1$. The total amount of difference between the matching coefficients is no more than ε . It can be shown (Lemma 1 in Appendix C) that these conditions guarantee the required bound on $|P_3(s_1, \diamond^{\leq 3} a) - P_3(s_2, \diamond^{\leq 3} a)|$.

The main difficulty is choosing a suitable decomposition of $P_3(s_1, \diamond^{\leq 3}a)$ and $P_3(s_2, \diamond^{\leq 3}a)$. This is non-trivial since in (4), the $1/3$ probability of transitioning into t_2 had to be broken up into two terms with $1/6$ probability each. However, we can tackle this issue using an extension of Hall's Matching Theorem [4] (cf. Appendix C). It is then relatively straight forward to adapt this proof to LMCs on uncountable state spaces by converging on integrals with simple functions. \square

We now show that the expression for the induced bound on probabilistic trace distance proved in Theorem 4, namely $(1 - (1 - \varepsilon)^k)$, is tight, in the sense that for any k and ε , the bound can be attained by some pair of ε -bisimilar states in some LMC. In other words, it is not possible to provide bounds on the induced approximation level for traces, that are smaller than the expression discussed above and that are valid in general.

Theorem 5. *For any $\varepsilon \geq 0$, there exists a LMC $\mathcal{M} = (S, \Sigma, \tau, L)$ and states $s_1, s_2 \in S$ such that s_1, s_2 are ε -bisimilar, and for all $k \in \mathbb{N}$ there exists a set TRACE of length $k + 1$ traces s.t. $|P_k(s_1, \text{TRACE}) - P_k(s_2, \text{TRACE})| = 1 - (1 - \varepsilon)^k$.*

Proof. Select $\varepsilon \geq 0$ and consider the following LMC:



Here s_1, s_2 are ε -bisimilar, and for all $k \in \mathbb{N}$, $P_k(s_1, \diamond^{\leq k}a) = 0$, whereas $P_k(s_2, \diamond^{\leq k}a) = \sum_{i=1}^k (1 - \varepsilon)^{i-1} \varepsilon = 1 - (1 - \varepsilon)^k$. \square

The result in Theorem 4 can be viewed as an extension of the known fact that bisimulation implies trace equivalence in non-probabilistic transition systems. Similar to the deterministic case, the converse of Theorem 4 does not hold.

Theorem 6. $(1 - (1 - \varepsilon)^k)$ -trace equivalence does not imply ε -bisimulation.

Proof. In Figure 1, states s_1, s_2 are not ε -bisimilar for any $\varepsilon < 1/2$, yet their probabilistic trace distance is equal to 0. \square

This example shows that ε -bisimulation cannot be used to effectively estimate the probabilistic trace distance between individual states. In particular, while the $(1 - (1 - \varepsilon)^k)$ -bound on probabilistic trace distance discussed above is tight as a uniform bound, it is not tight for individual pairs of states.

5 Application to Model Checking of Continuous-State LMCs

Suppose we are given an LMC $\mathcal{M}^c = (S^c, \Sigma^c, \tau^c, L^c)$, which we shall refer to as the “concrete” model, possibly over a continuous state space. We are interested

in calculating its probability of satisfying a given LTL formula, starting from certain initial states. One approach is to construct a finite-state LMC $\mathcal{M}^A = (S^A, \Sigma^A, \tau^A, L^A)$ (the “abstract model”) that can be related to \mathcal{M}^C (in a way to be made precise shortly). Probabilistic model checking can then be run over \mathcal{M}^A using standard tools for finite-state models such as PRISM [18], and since \mathcal{M}^A is related to \mathcal{M}^C , this leads to approximate outcomes that are valid for \mathcal{M}^C . The above approach has been studied in several papers [2, 3, 15], and the method for constructing \mathcal{M}^A from \mathcal{M}^C is to raise smoothness assumptions on the kernel τ^C of \mathcal{M}^C , and to partition the state space S^C , thus obtaining S^A and τ^A (the sigma algebra and labels being directly inherited).

In this section we will demonstrate the application of our results. We will employ ε -bisimulation to relate \mathcal{M}^A and \mathcal{M}^C , and use our results to bound their trace distance. This method produces tighter error bounds, for a broader class of properties, than are currently established in literature. The first step is to establish simpler conditions that guarantee ε -bisimulation between \mathcal{M}^C and \mathcal{M}^A .

Theorem 7. *Let $\varepsilon \in [0, 1]$, and suppose there exists a finite measurable partition $\mathcal{Q}_\varepsilon = \{P_1, \dots, P_N\}$ of S^C such that for all $P \in \mathcal{Q}_\varepsilon$, $s_1, s_2 \in P$, we have that $L^C(s_1) = L^C(s_2)$ and³*

$$\max_{J \subseteq \{1, \dots, N\}} \left| \tau^C \left(s_1, \bigcup_{j \in J} P_j \right) - \tau^C \left(s_2, \bigcup_{j \in J} P_j \right) \right| \leq \varepsilon.$$

Assume wlog $P_i \neq \emptyset$, and for each $i \in \{1, \dots, N\}$ choose a representative point $s_i^C \in P_i$. Consider the abstract model to be $\mathcal{M}^A = (S^A, \Sigma^A, \tau^A, L^A)$ formed by merging each P_i into s_i^C . Formally,

- $S^A = \{s_1^A, \dots, s_N^A\}$.
- $\Sigma^A = \mathcal{P}(S^A)$.
- τ^A is such that $\tau^A(s_i^A, \{s_j^A\}) = \tau^C(s_i^C, P_j)$.
- $L^A(s_i^A) = L^C(s_i^C)$.

Then, for all $i \in \{1, \dots, N\}$, $s^C \in P_i$, we have that s^C is ε -bisimilar to s_i^A , and hence $1 - (1 - \varepsilon)^k$ -trace equivalent.

In practical terms the partition \mathcal{Q}_ε can be straightforwardly constructed in many cases. As shown in Theorem 8, the approach in [2, 3, 24] generates a partition of S^C satisfying the conditions of Theorem 7. Thus, ε -bisimulation can be seen as the underlying reason for the closeness of probabilities of events.

Theorem 8. *Consider an LMC $\mathcal{M}^C = (S^C, \Sigma^C, \tau^C, L^C)$ where S^C is a Borel subset of \mathbb{R}^d . Suppose that $\tau^C(s, T)$ is of the form $\int_{t \in T} f(s, t) dt$, so that for each state $s \in S^C$, $f(s, \cdot) : S^C \rightarrow \mathbb{R}_0^+$ is the probability density of the next state.*

³ The left hand side is just $d_{TV}(\mu_1, \mu_2)$ where for $i = 1, 2$, for $A \subseteq \mathcal{Q}_\varepsilon$, $\mu_i(A) := \tau^C(s_i, \bigcup A)$

Suppose further that $f(\cdot, t)$ is uniformly K -Lipschitz continuous for all $t \in S^C$. That is, for some $K \in \mathbb{R}$, for all $s_1, s_2, t \in S^C$,

$$|f(s_1, t) - f(s_2, t)| \leq K \cdot \|s_1 - s_2\|.$$

For $A \in \Sigma^C$ (so $A \subseteq \mathbb{R}^d$), let $\lambda(A)$ be the volume of A and $\delta(A) := \sup_{x_1, x_2 \in A} \{\|x_1 - x_2\|\}$ be the diameter of A . For any $\varepsilon \in [0, 1]$, finite $\lambda(S^C)$, suppose partition $\mathcal{Q} = \{P_1, \dots, P_N\}$ of S^C is such that

$$\max_{j \in \{1, \dots, N\}} \delta(P_j) \leq \frac{2\varepsilon}{K\lambda(S^C)}.$$

Then, we have that \mathcal{Q} satisfies the conditions of Theorem 7 and can be used to construct the abstract model \mathcal{M}^A .

There are a number of adaptations that could be made to this result. [15] improves a related approach by varying the size of each partition in response to the local Lipschitz constant, rather than enforcing a globally uniform K . Similarly to this paper, [3] also discusses the relation of approximate probabilistic bisimulation to the problem of generating the abstract model, but a strictly weaker definition of approximate probabilistic bisimulation is employed (cf. Section 7). Finally, note that using algorithms in [12], we can compute ε -bisimulation relations on \mathcal{M}^A : this allows \mathcal{M}^A to be further compressed (at the cost of an additional ε_2 approximation), by merging the states that are ε_2 -bisimilar to each other.

6 Case Study

Concrete Model. Consider the concrete model $\mathcal{M}^C = (S^C, \Sigma^C, \tau^C, L^C)$, describing the weather forecast for a resort. Here $S^C = \{0, 1\} \times [0, 1]$, $\Sigma^C = \mathcal{B}(S^C)$, and the state at time t is (R_t, H_t) , where

- $R_t \in \{0, 1\}$ is a random variable representing whether it rains on day t ,
- $H_t \in [0, 1]$ is a random variable representing the humidity after day t .

Raining on day t causes it to become more likely to rain on day $t + 1$, but it also tends to reduce the humidity, which causes it to become gradually less likely to rain in the future. The meteorological variations are encompassed by τ^C , which is such that the model evolves according to

$$\begin{aligned} \mathbb{P}(R_{t+1} \mid R_0, \dots, R_t, H_0, \dots, H_t) &= \mathbb{P}(R_{t+1} \mid R_t, H_t) \\ &\sim \begin{cases} \text{B}(\frac{1}{4} + \frac{3}{4}H_t) & \text{if } R_t = 1 \\ \text{B}(\frac{3}{4}H_t) & \text{if } R_t = 0 \end{cases}, \\ \mathbb{P}(H_{t+1} \mid R_0, \dots, R_t, H_0, \dots, H_t, R_{t+1}) &= \mathbb{P}(H_{t+1} \mid H_t, R_{t+1}) \\ &\sim \begin{cases} \text{U}[0, \frac{1+H_t}{2}] & \text{if } R_{t+1} = 1 \\ \text{U}[\frac{H_t}{2}, 1] & \text{if } R_{t+1} = 0 \end{cases}, \end{aligned}$$

where $B(p)$ is the Bernoulli distribution with probability p of producing 1, and $U[a, b)$ is the uniform distribution over the real interval $[a, b)$. Finally, the states of the model are labelled according to whether it rains on that day, namely

$$L^C((r, h)) = \begin{cases} \{\text{RAIN}\} & \text{if } r = 1 \\ \emptyset & \text{if } r = 0. \end{cases}$$

Given \mathcal{M}^C we are interested in computing the likelihood of events expressing meteorological predictions, given knowledge of present weather conditions.

Synthesis of the Abstract Model. Notice that \mathcal{M}^C does not directly satisfy the smoothness assumptions of Theorem 8, in view of the discrete/continuous structure of its state space and the discontinuous probability density resulting from the uniform distribution. Nonetheless, we can still construct \mathcal{M}^A by taking a sensible partition of S^C and proving that it satisfies the conditions of Theorem 7. Let $\mathcal{Q}_\varepsilon := \{P_{r,h} \mid r \in \{0, 1\}, h \in \{0, \dots, N-1\}\}$, where $P_{r,h} = \{r\} \times [h/N, (h+1)/N)$.

Theorem 9. *For any $\varepsilon \in [0, 1]$, by taking $N \geq 2/\varepsilon$, we have that \mathcal{Q}_ε satisfies the conditions of Theorem 7.*

Therefore, we may construct the abstract model using Theorem 7. We choose the abstract state $(r^A, h^A) \in S^A := \{0, 1\} \times \{0, \dots, N-1\}$ to correspond to the partition $P_{r^A, h^A} \in \mathcal{Q}_\varepsilon$, and within each partition we select the concrete state with the lowest H_t -coordinate to be the representative state. This produces the abstract model $\mathcal{M}^A = (S^A, \Sigma^A, \tau^A, L^A)$, where $\Sigma^A = \mathcal{P}(S^A)$, $L^A((r, h)) = L^C((r, h))$, and

$$\tau^A((h_0, r_0), \{(h_1, r_1)\}) = \begin{cases} p_{R_1|R_0}(h_0) \cdot p_{H_1|R_1}(h_0, h_1) & \text{if } r_0 = 1, r_1 = 1 \\ (1 - p_{R_1|R_0}(h_0)) \cdot p_{H_1|\neg R_1}(h_0, h_1) & \text{if } r_0 = 1, r_1 = 0 \\ p_{R_1|\neg R_0}(h_0) \cdot p_{H_1|R_1}(h_0, h_1) & \text{if } r_0 = 0, r_1 = 1 \\ (1 - p_{R_1|\neg R_0}(h_0)) \cdot p_{H_1|\neg R_1}(h_0, h_1) & \text{if } r_0 = 0, r_1 = 0, \end{cases}$$

where

$$\begin{aligned} - p_{R_1|R_0}(h_0) &= \frac{1}{4} + \frac{3}{4} \frac{h_0}{N}, \text{ and } p_{R_1|\neg R_0}(h_0) = \frac{3}{4} \frac{h_0}{N}, \\ - p_{H|\neg R}(h_0, h_1) &= \frac{2}{2N-h_0} \cdot \max(\min(h_1 + 1 - h_0/2, 1), 0), \\ - p_{H|R}(h_0, h_1) &= \frac{2}{N+h_0} \cdot \max(\min(\frac{N+h_0}{2} - h_1, 1), 0). \end{aligned}$$

Computation of Approximate Satisfaction Probabilities. Suppose that at the end of day 0, we have $R_0 = 0, H_0 = 0.5$, and a travel agent wants to know the risk of there being 2 consecutive days of rain over the next three days.

This probability can be computed algorithmically according to \mathcal{M}^A , and for $N = 1000$, this is 0.365437 (see Appendix G). Since point $(0, 500) \in S^A$ is 0.001-bisimilar with $(0, 0.5) \in S^C$, this means that according \mathcal{M}^C with initial state $(0, 0.5) \in S^C$, the probability of there being two consecutive days of rain over

the next three days is 0.365437 ± 0.003 .

Analytical Validation of the Result. In this setup it is possible to evaluate the exact result for \mathcal{M}^C analytically:

$$\mathbb{P}[R_1 = 1, R_2 = 1] = \mathbb{P}[R_1 = 1] \int_0^1 f_{H_1|R_1=1}(h_1) \cdot \mathbb{P}[R_2 = 1 | H_1 = h_1, R_1 = 1] dh_1,$$

which amounts to 0.199219, and similarly $\mathbb{P}[R_1 = 0, R_2 = 1, R_3 = 1] = 0.166626$. This yields

$$\begin{aligned} \mathbb{P}[\text{Two consecutive rainy days over next 3 days}] = \\ \mathbb{P}[R_1 = 1, R_2 = 1] + \mathbb{P}[R_1 = 0, R_2 = 1, R_3 = 1] = 0.365845, \end{aligned}$$

which is within the error bounds guaranteed by ε -trace equivalence, as expected.

7 Other Notions of ε -Bisimulation

The following condition appears in literature [1, 3, 13] as the definition of approximate probabilistic bisimulation. For simplicity, let us restrict our attention to finite state spaces.

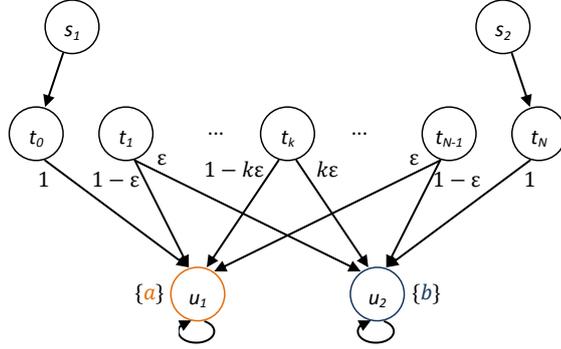
Definition 9 (Alternative notion of approximate probabilistic bisimulation, adapted from [3]). Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC, where S is finite and $\Sigma = \mathcal{P}(S)$. For $\varepsilon \in [0, 1]$, a binary relation R_ε on S satisfies Definition 9 if:

$$\begin{aligned} \forall (s_1, s_2) \in R_\varepsilon, \quad \text{we have } L(s_1) = L(s_2), \\ \forall (s_1, s_2) \in R_\varepsilon, \quad \forall \tilde{T} \subseteq S \text{ s.t. } \tilde{T} \text{ is } R_\varepsilon\text{-closed,} \quad \text{we have } \left| \tau(s_1, \tilde{T}) - \tau(s_2, \tilde{T}) \right| \leq \varepsilon. \end{aligned}$$

This is different from our notion of approximate probabilistic bisimulation because \tilde{T} ranges over R_ε -closed sets rather than all (measurable) sets. This definition is closer to exact probabilistic bisimulation (cf. Definition 3), but it is too weak to effectively bound probabilistic trace distance.

Theorem 10. For any $\varepsilon > 0$, there exists an LMC $\mathcal{M} = (S, \Sigma, \tau, L)$, a binary relation R_ε on S , and a pair of states $(s_1, s_2) \in R_\varepsilon$, such that R_ε satisfies the conditions in Definition 9, but the 2-step reachability probabilities from s_1, s_2 differ by 1 for some destination states.

Proof. For $\varepsilon > 0$, let $N \in \mathbb{Z}^+$, $1/N \leq \varepsilon$. Consider the following LMC. Let $R_\varepsilon := \{(s_1, s_2)\} \cup \{(t_k, t_{k+1}) \mid k \in \{0, \dots, N-1\}\}$.



The only R_ε -closed sets are $\{s_1, s_2\}$, $\{t_0, \dots, t_N\}$, $\{u_1\}$, $\{u_2\}$ and unions of these sets, and so R_ε satisfies Definition 9.

We have $s_1 R_\varepsilon s_2$, and yet $P_2(s_1, \diamond^{\leq 2} a) = 1$ but $P_2(s_2, \diamond^{\leq 2} a) = 0$, where $\diamond^{\leq 2} a$ is the set of length 3 traces that reach a state labelled with a .

As shown in [13] however, there is still some relationship between the probabilities of specific traces, which hinges on additional details of the structure of the transition kernel.

8 Conclusions and Extensions

In this paper we have developed a theory of $f(k)$ -trace equivalence. We derived the minimum $f(k)$ such that ε -bisimulation implies $f(k)$ -trace equivalence, thus extending the well known result for the exact non-probabilistic case. By linking error bounds on the total variation of length k traces to a notion of approximation based on the underlying transition kernel, we provided a means of computing upper bounds for the total variation and of synthesising abstract models with arbitrarily small total variation to a given concrete model.

It is of interest to extend our results to allow the states of the LMC to be labelled with bounded real-valued rewards, and then to limit the difference in expected reward between approximately bisimilar states.

Acknowledgments

The authors would like to thank Marta Kwiatkowska for discussions on an earlier version of this draft.

References

1. Abate, A.: Approximation metrics based on probabilistic bisimulations for general state-space Markov processes: a survey. *Electronic Notes in Theoretical Computer Science* 297, 3–25 (2013)

2. Abate, A., Katoen, J.P., Lygeros, J., Prandini, M.: Approximate model checking of stochastic hybrid systems. *European Journal of Control* 16(6), 624–641 (2010)
3. Abate, A., Kwiatkowska, M., Norman, G., Parker, D.: Probabilistic model checking of labelled Markov processes via finite approximate bisimulations. In: *Horizons of the Mind. A Tribute to Prakash Panangaden*, pp. 40–58. Springer (2014)
4. Bollobás, B., Varopoulos, N.: Representation of systems of measurable sets. *Mathematical Proceedings of the Cambridge Philosophical Society* 78(02), 323–325 (1975)
5. Buchholz, P.: Exact and ordinary lumpability in finite Markov chains. *Journal of applied probability* pp. 59–75 (1994)
6. Castro, P.S., Panangaden, P., Precup, D.: Notions of state equivalence under partial observability. In: *IJCAI* (2009)
7. Chen, D., van Breugel, F., Worrell, J.: On the complexity of computing probabilistic bisimilarity. In: *Foundations of Software Science and Computational Structures*, pp. 437–451. Springer (2012)
8. Chen, T., Kiefer, S.: On the total variation distance of labelled Markov chains. In: *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. p. 33. ACM (2014)
9. Comanici, G., Panangaden, P., Precup, D.: On-the-fly algorithms for bisimulation metrics. In: *Quantitative Evaluation of Systems (QEST), 2012 Ninth International Conference on*. pp. 94–103. IEEE (2012)
10. Daca, P., Henzinger, T.A., Kretínský, J., Petrov, T.: Linear distances between markov chains. In: *27th International Conference on Concurrency Theory, CONCUR 2016, August 23-26, 2016, Québec City, Canada*. pp. 20:1–20:15 (2016)
11. Desharnais, J., Edalat, A., Panangaden, P.: Bisimulation for labelled Markov processes. *Information and Computation* 179(2), 163–193 (2002)
12. Desharnais, J., Laviolette, F., Tracol, M.: Approximate analysis of probabilistic processes: Logic, simulation and games. In: *Quantitative Evaluation of Systems, 2008. QEST'08. Fifth International Conference on*. pp. 264–273. IEEE (2008)
13. D’Innocenzo, A., Abate, A., Katoen, J.P.: Robust PCTL model checking. In: *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*. pp. 275–286. ACM (2012)
14. Durrett, R.: *Probability: Theory and Examples - Third Edition*. Duxbury Press (2004)
15. Esmaeil Zadeh Soudjani, S., Abate, A.: Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes. *SIAM Journal on Applied Dynamical Systems* 12(2), 921–956 (2013)
16. Gebler, D., Tini, S.: Compositionality of approximate bisimulation for probabilistic systems. In: *EXPRESS/SOS 2013*. pp. 32–46 (2013)
17. Gibbs, A.L., Su, F.E.: On choosing and bounding probability metrics. *International statistical review* 70(3), 419–435 (2002)
18. Kwiatkowska, M., Norman, G., Parker, D.: PRISM 4.0: Verification of probabilistic real-time systems. In: *Computer aided verification*. pp. 585–591. Springer (2011)
19. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. In: *Conference Record of the 16th ACM Symposium on Principles of Programming Languages (POPL)*. pp. 344–352 (1989)
20. Segala, R., Lynch, N.: Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing* (1995)
21. Spears, W.M.: A compression algorithm for probability transition matrices. *SIAM journal on matrix analysis and applications* 20(1), 60–77 (1998)

22. Sproston, J., Donatelli, S.: Backward bisimulation in Markov chain model checking. *Software Engineering, IEEE Transactions on* 32(8), 531–546 (2006)
23. Tang, Q., van Breugel, F.: Computing probabilistic bisimilarity distances via policy iteration. In: *27th International Conference on Concurrency Theory, CONCUR 2016, August 23-26, 2016, Québec City, Canada*. pp. 22:1–22:15 (2016)
24. Tkachev, I., Abate, A.: Formula-free finite abstractions for linear temporal verification of stochastic hybrid systems. In: *Proceedings of the 16th international conference on Hybrid systems: computation and control*. pp. 283–292. ACM (2013)
25. Wu, H., Noé, F.: Probability distance based compression of hidden Markov models. *Multiscale Modeling & Simulation* 8(5), 1838–1861 (2010)

A Proof of Theorem 1

Proof. Suppose s_1, s_2 are 0-bisimilar. Let R_ε be a 0-bisimulation relation s.t. $s_1 R_\varepsilon s_2$, and assume wlog that R_ε is reflexive (by enlarging it if necessary).

Let R^∞ be the transitive closure of R_ε , so that R^∞ is an equivalence relation. Since $s_1 R^\infty s_2$, we only need to show that R^∞ is an exact probabilistic bisimulation relation. The other conditions being easy to check, we will only prove $\tau(s_1, \tilde{T}) = \tau(s_2, \tilde{T})$ for all $(s_1, s_2) \in R^\infty$ for all R^∞ -closed $\tilde{T} \in \Sigma$.

Let $(s_1, s_2) \in R^\infty$, and let $\tilde{T} \in \Sigma$ be R^∞ -closed. Then, $s_1 R_\varepsilon y_1 R_\varepsilon \cdots R_\varepsilon y_N R_\varepsilon s_2$ for some $y_1, \dots, y_N \in S$. We have $\tau(s_1, \tilde{T}) \leq \tau(y_1, R_\varepsilon(\tilde{T}))$ since R_ε is a 0-bisimulation relation, and we have $\tau(y_1, R_\varepsilon(\tilde{T})) = \tau(y_1, \tilde{T})$ since $R_\varepsilon(\tilde{T}) = \tilde{T}$. We therefore have $\tau(s_1, \tilde{T}) = \tau(y_1, \tilde{T})$ since R_ε is symmetric. Similarly, we have $\tau(y_1, \tilde{T}) = \tau(y_2, \tilde{T}) = \cdots = \tau(y_N, \tilde{T}) = \tau(s_2, \tilde{T})$. \square

B Proof of Theorem 3

Proof. Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be an LMC and $s_1, s_2 \in S$. Let \mathcal{M} start at the initial state s_C where C is a uniform random variable taking values in $\{1, 2\}$. Conditional on $C = c$, the length $k + 1$ trace emitted from \mathcal{M} is a random variable X taking values in \mathcal{O}^{k+1} with distribution $P_k(s_c, \cdot)$.

After observing outcome $X = x$, an optimal agent guesses C to be 1 if $\mathbb{P}[C = 1|X = x] > \mathbb{P}[C = 2|X = x]$, and C to be 2 if $\mathbb{P}[C = 2|X = x] > \mathbb{P}[C = 1|X = x]$, in order to maximize the probability of being correct. So,

$$\begin{aligned}
& \mathbb{P}[\text{CORRECT}|X = x] \\
&= \max\{\mathbb{P}[C = 1|X = x], \mathbb{P}[C = 2|X = x]\} \\
&= \frac{1}{2} \left(\mathbb{P}[C = 1|X = x] + \mathbb{P}[C = 2|X = x] + |\mathbb{P}[C = 1|X = x] - \mathbb{P}[C = 2|X = x]| \right) \\
&= \frac{1}{2} + \frac{1}{2} \left| \mathbb{P}[C = 1|X = x] - \mathbb{P}[C = 2|X = x] \right| \\
&= \frac{1}{2} + \frac{|\mathbb{P}[X = x|C = 1] - \mathbb{P}[X = x|C = 2]|}{4\mathbb{P}[X = x]} \\
&\quad \text{since } \mathbb{P}[C = 1|X = x] = \mathbb{P}[X = x|C = 1] \frac{\mathbb{P}[C = 1]}{\mathbb{P}[X = x]} = \frac{\mathbb{P}[X = x|C = 1]}{2\mathbb{P}[X = x]} \\
&\quad \text{and similarly for } \mathbb{P}[C = 2|X = x].
\end{aligned}$$

We obtain

$$\begin{aligned}
& \mathbb{P}[\text{CORRECT}] \\
&= \sum_{x \in \mathcal{O}^{k+1}} \mathbb{P}[\text{CORRECT} | X = x] \mathbb{P}[X = x] \\
&= \frac{1}{2} + \frac{1}{4} \sum_{x \in \mathcal{O}^{k+1}} \left| \mathbb{P}[X = x | C = 1] - \mathbb{P}[X = x | C = 2] \right| \\
&= \frac{1}{2} + \frac{1}{2} \max_{\text{TRACE} \subseteq \mathcal{O}^{k+1}} \left| \mathbb{P}[X \in \text{TRACE} | C = 1] - \mathbb{P}[X \in \text{TRACE} | C = 2] \right| \\
&= \frac{1}{2} + \frac{1}{2} d_{\text{TV}}(P_k(s_1, \cdot), P_k(s_2, \cdot)).
\end{aligned}$$

□

C Proof of Theorem 4

We say that (Z, \mathcal{F}, μ) is a measure space if Z is a set, $\mathcal{F} \subseteq \mathcal{P}(Z)$ is a σ -algebra over Z and $\mu : \mathcal{F} \rightarrow \mathbb{R}_0^+$ is a measure function. We say that $S \in \mathcal{F}$ is an atom if $\mu(S) > 0$, and if for any measurable subset $T \subseteq S$, we have either $\mu(T) = \mu(S)$ or $\mu(T) = 0$. For instance, for any measurable singleton point $\{x\} \in \mathcal{F}$, if $\mu(\{x\}) > 0$ then $\{x\}$ is an atom. We borrow the following fact.

Theorem 11 ([4]). *Let (Z, \mathcal{F}, μ) be an atomless measure space. Let A be an index set, $(X_\alpha)_{\alpha \in A}$ be a family of measurable sets in \mathcal{F} of finite measure, and $(\lambda_\alpha)_{\alpha \in A}$ be a family of non-negative real numbers. The following holds: There exists a family of measurable sets $(Y_\alpha)_{\alpha \in A}$ in \mathcal{F} such that $\forall \alpha \in A$ we have $Y_\alpha \subseteq X_\alpha$, $\mu(Y_\alpha) = \lambda_\alpha$, and $\forall \alpha, \alpha' \in A$ with $\alpha \neq \alpha'$ we have $\mu(Y_\alpha \cap Y_{\alpha'}) = 0$*

\iff

For every finite subset $B \subseteq A$, $\mu(\bigcup_{\alpha \in B} X_\alpha) \geq \sum_{\alpha \in B} \lambda_\alpha$.

We will also use the following lemma, where $u_i \cdot x_i$ corresponds to the terms in Equation (4) in the sketch proof (e.g. $u_1 = 1/3$, $x_1 = P_2(t_1, \diamond^{\leq 2}a)$), and similarly $v_i \cdot y_i$ corresponds to the terms in Equation (5).

Lemma 1. *Let $\varepsilon, \delta \geq 0$. Let $u_i, v_i, x_i, y_i \in [0, 1]$ for $i \in \{1, 2, \dots, M\}$. Suppose that*

$$|x_i - y_i| \leq \delta \quad \forall i \in \{1, \dots, M\}, \quad (6)$$

$$\sum_{i=1}^M u_i \leq 1, \quad (7)$$

$$\sum_{i|u_i > v_i} (u_i - v_i) \leq \varepsilon. \quad (8)$$

Then $\sum_{i=1}^M x_i u_i - \sum_{i=1}^M y_i v_i \leq \varepsilon + \delta - \varepsilon \delta$.

Proof. Let $y'_i := \max\{0, x_i - \delta\}$, so that $y_i \geq y'_i$ by (6) and by $y_i \in [0, 1]$. Then,

$$\sum_{i=1}^M x_i u_i - \sum_{i=1}^M y_i v_i \leq \sum_{i=1}^M x_i u_i - \sum_{i=1}^M y'_i v_i = \sum_{i=1}^M u_i (x_i - y'_i) + \sum_{i=1}^M y'_i (u_i - v_i).$$

Now,

$$\begin{aligned} \sum_{i=1}^M u_i (x_i - y'_i) &= \sum_{i=1}^M u_i \min\{x_i, \delta\} \leq \delta \sum_{i=1}^M u_i \\ &\leq \delta \quad \text{by (7)}. \end{aligned}$$

We conclude that

$$\begin{aligned} \sum_{i=1}^M y'_i (u_i - v_i) &\leq \sum_{i|u_i > v_i \text{ and } y'_i \neq 0} y'_i (u_i - v_i) \\ &\leq (1 - \delta) \sum_{i|u_i > v_i \text{ and } y'_i > 0} (u_i - v_i) \\ &\quad \text{since for } i \text{ s.t. } y'_i \neq 0, \text{ we have } y'_i = x_i - \delta \leq 1 - \delta \\ &\leq (1 - \delta) \varepsilon \quad \text{by (8)}. \end{aligned}$$

□

Main Proof. We are now ready for the proof of the main theorem. Let $\mathcal{M} = (S, \Sigma, \tau, L)$ be a LMC, let $\varepsilon \in [0, 1]$, let R_ε be an ε -bisimulation relation on \mathcal{M} . We prove by induction on $k \in \mathbb{N}$ that for any $(s_1, s_2) \in R_\varepsilon$, we have that

$$d_{\text{TV}}(P_k(s_1, \cdot), P_k(s_2, \cdot)) \leq 1 - (1 - \varepsilon)^k.$$

For the base case $k = 0$, since $s_1 R_\varepsilon s_2$, we have $L(s_1) = L(s_2)$. Let $\alpha_0 := L(s_1) = L(s_2)$, then

$$P_0(s_1, \text{TRACE}) = P_0(s_2, \text{TRACE}) = \begin{cases} 1 & \text{if } \langle \alpha_0 \rangle \in \text{TRACE} \\ 0 & \text{otherwise} \end{cases}$$

For the induction step, we assume (as the induction hypothesis) that for a fixed $k - 1 \in \mathbb{N}$, for any $(s_1, s_2) \in R_\varepsilon$,

$$d_{\text{TV}}(P_{k-1}(s_1, \cdot), P_{k-1}(s_2, \cdot)) \leq \delta,$$

where $\delta := 1 - (1 - \varepsilon)^{k-1}$. We will prove the result for k by showing for any fixed $\text{TRACE} \subseteq \mathcal{O}^{k+1}$,

$$P_k(s_2, \text{TRACE}) \geq P_k(s_1, \text{TRACE}) - \left(1 - (1 - \varepsilon)^k\right).$$

Since R_ε is symmetric, we can reverse the roles of s_1 and s_2 to get the required result.

Let $\alpha := L(s_1)$. Let $\text{TRACE}_{\langle \alpha \rangle} := \{ \langle \alpha_1, \dots, \alpha_k \rangle \mid \langle \alpha, \alpha_1, \dots, \alpha_k \rangle \in \text{TRACE} \}$ be the set of traces from TRACE after seeing an initial α . By conditioning on the first step, we have (from Definition 1 and Definition 6):

$$P_k(s_1, \text{TRACE}) = \int_{y \in \mathcal{S}} P_{k-1}(y, \text{TRACE}_{\langle \alpha \rangle}) \tau(s_1, dy).$$

Let $T(y) := P_{k-1}(y, \text{TRACE}_{\langle \alpha \rangle})$. From the construction of the integral, this becomes

$$P_k(s_1, \text{TRACE}) = \sup \left\{ \sum_{r=1}^K c_r \tau(s_1, G_r) \mid \sum_{r=1}^K c_r \mathbb{1}_{G_r}(t) \leq T(t) \text{ and } G_r \in \Sigma \text{ are disjoint} \right\},$$

where $\mathbb{1}_G$ is the indicator function. Now let

$$\phi_1(t) = \sum_{i=1}^M a_i \mathbb{1}_{D_i}(t) \leq T(t)$$

be any such function on \mathcal{S} . Assume wlog that ϕ_1 is a simple function in canonical form, that is, $a_i \in [0, 1]$, $D_i \in \Sigma$, $D_i \neq \emptyset$ and D_i form a partition of \mathcal{S} . In the rest of the proof, we construct a second simple function

$$\phi_2(t) = \sum_{j=1}^N b_j \mathbb{1}_{E_j}(t) \leq T(t)$$

(where $b_j \in [0, 1]$, $E_j \in \Sigma$, E_j are disjoint) such that

$$\sum_{j=1}^N b_j \tau(s_2, E_j) \geq \left(\sum_{i=1}^M a_i \tau(s_1, D_i) \right) - \left(1 - (1 - \varepsilon)^k \right)$$

in order to show $P_k(s_2, \text{TRACE}) \geq P_k(s_1, \text{TRACE}) - \left(1 - (1 - \varepsilon)^k \right)$.

Take $\{E_1, \dots, E_N\}$ to be the (measurable) partition of \mathcal{S} generated by the equivalence relation induced by belonging to exactly the same $R_\varepsilon(D_i)$, so that $N \leq 2^M$. That is, $\forall x, y \in \mathcal{S}$, x and y are in the same E_j iff we have: $\forall i, x \in R_\varepsilon(D_i) \iff y \in R_\varepsilon(D_i)$.

We now use Theorem 11 to find appropriate b_j . Denote by $\mathcal{B}(I)$ the Borel σ -algebra on I for any interval $I \in \mathbb{R}$. Denote by l the Borel measure on \mathbb{R} . Let $*$ be some fresh element not in \mathcal{S} (which we will use as padding to represent the ε error), and let $\mathcal{Y} := \{*\} \times [0, \varepsilon]$. With reference to Theorem 11, take:

- $Z := (\mathcal{S} \times [0, 1]) \uplus \mathcal{Y}$
- \mathcal{F} to be the smallest σ -algebra on Z containing $(\Sigma \times \mathcal{B}([0, 1])) \uplus (\{*\} \times \mathcal{B}([0, \varepsilon]))$
- μ to be the unique measure on \mathcal{F} satisfying:

- for $S \times I \in \Sigma \times \mathcal{B}([0, 1])$, $\mu(S \times I) = \tau(s_2, S) \times l(I)$
 for $\{*\} \times I \in \{*\} \times \mathcal{B}([0, \varepsilon])$, $\mu(\{*\} \times I) = l(I)$
 – $A := \{1, \dots, M\}$
 – $X_i := (R_\varepsilon(D_i) \times [0, 1]) \uplus \mathcal{Y}$
 – $\lambda_i := \tau(s_1, D_i)$.

Now, Z is atomless since real intervals with the Borel measure are atomless. X_i have finite measure, since $\mu(Z) = 1 + \varepsilon$. Since $s_1 R_\varepsilon s_2$, we have $\tau(s_2, R_\varepsilon(S)) + \varepsilon \geq \tau(s_1, S) \forall S \in \Sigma$. Therefore, we have that for any (finite) $B \subseteq A$,

$$\begin{aligned} \mu(\cup_{i \in B} X_i) &= \mu(\cup_{i \in B} R_\varepsilon(D_i) \times [0, 1]) + \mu(\{*\} \times [0, \varepsilon]) \\ &= \tau(s_2, \cup_{i \in B} R_\varepsilon(D_i)) + \varepsilon \\ &= \tau(s_2, R_\varepsilon(\cup_{i \in B} D_i)) + \varepsilon \\ &\geq \tau(s_1, \cup_{i \in B} D_i) \\ &= \sum_{i \in B} \lambda_i. \end{aligned}$$

Therefore by Theorem 11, there exist $Y_i \in \mathcal{F}$ s.t.

$$\begin{aligned} Y_i &\subseteq X_i \\ \mu(Y_i) &= \tau(s_1, D_i) \\ \mu(Y_i \cap Y_{i'}) &= 0 \quad \forall i \neq i'. \end{aligned}$$

Let $E'_j := E_j \times [0, 1]$ so that $\mu(E'_j) = \tau(s_2, E_j)$. Take

$$b_j := \begin{cases} \sum_{i=1}^M \frac{\mu(Y_i \cap E'_j)}{\mu(E'_j)} (a_i - \delta)^+ & \text{if } \mu(E'_j) > 0 \\ 0 & \text{otherwise} \end{cases}$$

where $(a_i - \delta)^+ := \max\{0, a_i - \delta\}$. The b_j here serve the same purpose as the coefficients in Equations (4) and (5) in the sketch proof of this theorem in Section 4.

We now show $\phi_2(t) \leq T(t)$. Fix any $j \in \{1, \dots, N\}$ s.t. $\mu(E'_j) > 0$, and fix any $t \in E_j$. Let i be such that $Y_i \cap E'_j \neq \emptyset$. $Y_i \subseteq X_i$, so $R_\varepsilon(D_i) \cap E_j \neq \emptyset$, so $E_j \subseteq R_\varepsilon(D_i)$ by construction of E_j , so $t \in R_\varepsilon(D_i)$. There exists $x \in D_i$ such that $x R_\varepsilon t$. We have $a_i = \phi_1(x) \leq T(x)$, and so by the induction hypothesis we have

$$T(t) \geq T(x) - \delta \geq a_i - \delta.$$

This holds for every i such that $Y_i \cap E'_j \neq \emptyset$, and $\sum_{i | Y_i \cap E'_j \neq \emptyset} \frac{\mu(Y_i \cap E'_j)}{\mu(E'_j)} \leq 1$, so we get

$$T(t) \geq \sum_{i | Y_i \cap E'_j \neq \emptyset} \frac{\mu(Y_i \cap E'_j)}{\mu(E'_j)} (a_i - \delta)^+ = b_j = \phi_2(t)$$

This holds for any $t \in E_j$ where $\mu(E_j) > 0$. We also have $T(t) \geq 0 = \phi_2(t)$ for $t \in E_j$ where $\mu(E_j) = 0$. Hence for any $t \in \mathcal{S}$, we have $T(t) \geq \phi_2(t)$.

We now show that

$$\sum_{i=1}^M a_i \tau(s_1, D_i) - \sum_{j=1}^N b_j \tau(s_2, E_j) \leq 1 - (1 - \varepsilon)^k$$

Noting that E'_j form a partition of $\mathcal{S} \times [0, 1]$, we have

$$\begin{aligned} \sum_{j=1}^N b_j \tau(s_2, E_j) &= \sum_{j|\mu(E_j) > 0} \tau(s_2, E_j) \sum_{i=1}^M \frac{\mu(Y_i \cap E'_j)}{\mu(E'_j)} (a_i - \delta)^+ \\ &= \sum_{j=1}^N \sum_{i=1}^M \mu(Y_i \cap E'_j) (a_i - \delta)^+ \\ &= \sum_{i=1}^M (a_i - \delta)^+ \sum_{j=1}^N \mu(Y_i \cap E'_j) \\ &= \sum_{i=1}^M (a_i - \delta)^+ \mu \left(\bigcup_{j=1}^N (Y_i \cap E'_j) \right) \\ &= \sum_{i=1}^M (a_i - \delta)^+ \mu(Y_i \setminus \mathcal{Y}). \end{aligned}$$

We obtain

$$\sum_{i=1}^M a_i \tau(s_1, D_i) - \sum_{j=1}^N b_j \tau(s_2, E_j) = \sum_{i=1}^M a_i \tau(s_1, D_i) - \sum_{i=1}^M (a_i - \delta)^+ \mu(Y_i \setminus \mathcal{Y}).$$

We now apply Lemma 1 to the RHS of this equation. We check the conditions of Lemma 1 (in fact, by taking $y_i := (a_i - \delta)^+$, we get $y'_i = y_i$ in the proof of Lemma 1):

$$\begin{aligned} a_i - (a_i - \delta)^+ &\leq \delta \\ \sum_{i=1}^M \tau(s_1, D_i) &\leq 1 \\ \sum_{i|\mu(Y_i \setminus \mathcal{Y}) < \tau(s_1, D_i)} (\tau(s_1, D_i) - \mu(Y_i \setminus \mathcal{Y})) &\leq \varepsilon, \end{aligned}$$

where the last condition holds because $\forall i \neq i' \mu(Y_i \cap Y_{i'}) = 0$, and so we have for any $J \subseteq \{1, \dots, M\}$,

$$\begin{aligned} \sum_{i \in J} \mu(Y_i \setminus \mathcal{Y}) &= \mu\left(\bigcup_{i \in J} (Y_i \setminus \mathcal{Y})\right) \\ &= \mu\left(\bigcup_{i \in J} Y_i\right) - \mu\left(\mathcal{Y} \cap \bigcup_{i \in J} Y_i\right) \\ &\geq \mu\left(\bigcup_{i \in J} Y_i\right) - \varepsilon \\ &= \sum_{i \in J} \tau(s_1, D_i) - \varepsilon. \end{aligned}$$

So, by Lemma 1,

$$\begin{aligned} \sum_{i=1}^M a_i \tau(s_1, D_i) - \sum_{j=1}^N b_j \tau(s_2, E_j) &\leq \varepsilon + \delta - \varepsilon \delta \\ &= 1 - (1 - \varepsilon)^k. \end{aligned}$$

In conclusion, ϕ_2 has all of the required properties.

D Proof of Theorem 7

Proof. Wlog, assume S^C and S^A are disjoint. We will prove that s^C, s^A are ε -bisimilar as states in the direct sum LMC $\mathcal{M}^C \oplus \mathcal{M}^A = (S^C \uplus S^A, \Sigma^\oplus, \tau^\oplus, L^\oplus)$, as per Definition 5.

Let

$$R_\varepsilon := \left\{ (s_k^A, s_k^A), (s_k^A, s^C), (s^C, s_k^A), (s^C, s^{C'}) \mid k \in \{1, \dots, N\}, s^C, s^{C'} \in P_k \right\}$$

be a binary relation over $S^C \uplus S^A$. Here, we have taken R_ε to be the largest ε -bisimulation relation over $\mathcal{M}^C \oplus \mathcal{M}^A$; other choices of R_ε also work. Since the other conditions are clearly satisfied, to prove that R_ε is an ε -bisimulation relation we will only check

$$\tau^\oplus(s_1, R_\varepsilon(T)) \geq \tau^\oplus(s_1, R_\varepsilon(T)) - \varepsilon$$

for all $s_1, s_2 \in S^C \uplus S^A, T \in \Sigma^\oplus$.

Decompose T as $T = V \uplus \{s_i^A \mid i \in I\}$, where $V = T \cap S^C, \{s_i^A \mid i \in I\} = T \cap S^A, I \subseteq \{1, \dots, N\}$, and let $J := \{j \in \{1, \dots, N\} \mid T \cap P_j \neq \emptyset\}$, so that

$$R_\varepsilon(T) = \{s_i^A \mid i \in I \cup J\} \uplus \bigcup_{j \in I \cup J} P_j.$$

Let $(s_1, s_2) \in R_\varepsilon$. For $(s_1, s_2) = (s_k^A, s_k^A)$ where $k \in \{1, \dots, N\}$,

$$\begin{aligned} \tau^\oplus(s_1, R_\varepsilon(T)) &= \tau^A(s_1, R_\varepsilon(T) \cap S^A) \\ &\geq \tau^A(s_1, \{s_i^A \mid i \in I\}) \\ &= \tau^A(s_2, \{s_i^A \mid i \in I\}) \quad (\text{since } s_1 = s_2) \\ &= \tau^A(s_2, T \cap S^A) \\ &= \tau^\oplus(s_2, T). \end{aligned}$$

For $(s_1, s_2) = (s^C, s^{C'})$ where $s^C, s^{C'} \in P_k$,

$$\begin{aligned} \tau^\oplus(s_1, R_\varepsilon(T)) &= \tau^C(s_1, R_\varepsilon(T) \cap S^C) \\ &\geq \tau^C(s_1, \cup_{j \in J} P_j) \\ &\geq \tau^C(s_2, \cup_{j \in J} P_j) - \varepsilon \\ &\quad (\text{by assumption, since } s_1, s_2 \text{ are in the same partition } P_k) \\ &\geq \tau^C(s_2, T \cap S^C) - \varepsilon \\ &= \tau^\oplus(s_2, T) - \varepsilon. \end{aligned}$$

For $(s_1, s_2) = (s_k^A, s^C)$ where $k \in \{1, \dots, N\}$, $s^C \in P_k$,

$$\begin{aligned} \tau^\oplus(s_1, R_\varepsilon(T)) &\geq \tau^A(s_1, \{s_j^A \mid j \in J\}) \\ &= \tau^C(s_k^C, \cup_{j \in J} P_j) \quad (\text{by def of } \tau^A) \\ &\geq \tau^C(s_2, \cup_{j \in J} P_j) - \varepsilon \\ &\quad (\text{by assumption, since } s^C, s_2 \text{ are in the same partition } P_k) \\ &\geq \tau^\oplus(s_2, T) - \varepsilon. \end{aligned}$$

For $(s_1, s_2) = (s^C, s_k^A)$ where $k \in \{1, \dots, N\}$, $s^C \in P_k$, similarly we have

$$\begin{aligned} \tau^\oplus(s_1, R_\varepsilon(T)) &\geq \tau^C(s_1, \cup_{i \in I} P_i) \\ &\geq \tau^C(s_k^C, \cup_{i \in I} P_i) - \varepsilon \\ &= \tau^A(s_2, \{s_i^A \mid i \in I\}) - \varepsilon \\ &= \tau^\oplus(s_2, T). \end{aligned}$$

□

E Proof of Theorem 8

Proof.

$$|\tau^{\mathcal{C}}(s_1, T) - \tau^{\mathcal{C}}(s_2, T)| \leq K \cdot \|s_1 - s_2\| \cdot \lambda(T) \leq K \cdot \delta(T) \cdot \lambda(T),$$

and so

$$\begin{aligned} & \max_{J \subseteq \{1, \dots, N\}} \left| \tau^{\mathcal{C}} \left(s_1, \bigcup_{j \in J} P_j \right) - \tau^{\mathcal{C}} \left(s_2, \bigcup_{j \in J} P_j \right) \right| \\ &= \frac{1}{2} \sum_{j=1}^N |\tau^{\mathcal{C}}(s_1, P_j) - \tau^{\mathcal{C}}(s_2, P_j)| \\ &\leq \frac{1}{2} K \cdot \max_{j \in \{1, \dots, N\}} \delta(P_j) \cdot \lambda(S^{\mathcal{C}}) \\ &\leq \varepsilon. \end{aligned}$$

□

F Proof of Theorem 9

Proof. For any $r \in \{0, 1\}$, $h \in \{0, \dots, N-1\}$ and $s_1, s_2 \in P_{r,h}$, assume wlog $s_1 = (r, x_1)$, $s_2 = (r, x_2)$ and $x_1 \leq x_2$. Then, $\tau^{\mathcal{C}}(s_1, \cdot)$, $\tau^{\mathcal{C}}(s_2, \cdot)$ differ only on $V \subseteq S^{\mathcal{C}}$, where

$$V = \begin{cases} \{0, 1\} \times \left[\frac{1+x_1}{2}, \frac{1+x_2}{2} \right) & \text{if } r = 1 \\ \{0, 1\} \times \left[\frac{x_1}{2}, \frac{x_2}{2} \right) & \text{if } r = 0. \end{cases}$$

Therefore, we have for all $T \in \Sigma^{\mathcal{C}}$,

$$\begin{aligned} & |\tau^{\mathcal{C}}(s_1, T) - \tau^{\mathcal{C}}(s_2, T)| \\ &\leq \sup_{s \in S^{\mathcal{C}}} \tau^{\mathcal{C}}(s, V) \\ &\leq \sup_{p_{\text{rain}} \in [0,1]} \left| p_{\text{rain}}(x_2 - x_1) + (1 - p_{\text{rain}})(x_2 - x_1) \right| \\ &= 1/N. \end{aligned}$$

□

G Case study - model checking abstract model \mathcal{M}^A with PRISM

\mathcal{M}^A from Section 6 is model checked algorithmically by setting up the PRISM [18] model in Figure 3.

Fig. 3. PRISM model for \mathcal{M}^A with $N = 1000$. The length of this textual specification grows linearly with N , and it was generated with the help of a script.

```
// PRISM specification for the Abstract Model.

dtmc
formula N = 1000;
formula pToRain = r = 1 ? 1/4 + 3/4 * h/N : 3/4 * h/N;
module weatherAbstractModel

// State space
r : [0..1];
h : [0.. (N-1)];

[] true ->
  (pToRain * 2/(N + h) * max(min((N+h)/2 - 000, 1), 0))
  : (r'=1) & (h'=0)
+ (pToRain * 2/(N + h) * max(min((N+h)/2 - 001, 1), 0))
  : (r'=1) & (h'=1)
<<< ... TRIMMED (same pattern for 997 lines) ... >>>
+ (pToRain * 2/(N + h) * max(min((N+h)/2 - 999, 1), 0))
  : (r'=1) & (h'=999)
+ ((1-pToRain) * 2/(2*N-h) * max(min(000 + 1 - h/2, 1), 0))
  : (r'=0) & (h'=0)
+ ((1-pToRain) * 2/(2*N-h) * max(min(001 + 1 - h/2, 1), 0))
  : (r'=0) & (h'=1)
<<< ... TRIMMED (same pattern for 997 lines) ... >>>
+ ((1-pToRain) * 2/(2*N-h) * max(min(999 + 1 - h/2, 1), 0))
  : (r'=0) & (h'=999);

endmodule
```

The probability of there being 2 consecutive days of rain over the next three days is computed by expressing the PRISM property

```
filter(state, P=? [
  ( (X (r=1)) & (X X (r=1)) )
  | ( (X X (r=1)) & (X X X (r=1)) )
], r=0&h=500)
```

On a 2.5 GHZ processor using PRISM 4.3, it took 24 sec to parse and build the model, and 1 sec to compute this particular probability.