Approximating a Behavioural Pseudometric without Discount for Probabilistic Systems

Franck van Breugel[1], Babita Sharma[1], and James Worrell[2] *

[1] York University
4700 Keele Street, Toronto, M3J 1P3, Canada
[2] Oxford University Computing Laboratory
Parks Road, Oxford, OX1 3QD, England

Abstract. Desharnais, Gupta, Jagadeesan and Panangaden introduced a family of behavioural pseudometrics for probabilistic transition systems. These pseudometrics are a quantitative analogue of probabilistic bisimilarity. Distance zero captures probabilistic bisimilarity. Each pseudometric has a discount factor, a real number in the interval $(0, 1]$. The smaller the discount factor, the more the future is discounted. If the discount factor is one, then the future is not discounted at all. Desharnais et al. showed that the behavioural distances can be calculated up to any desired degree of accuracy if the discount factor is smaller than one. In this paper, we show that the distances can also be approximated if the future is not discounted. A key ingredient of our algorithm is Tarski's decision procedure for the first order theory over real closed fields. By exploiting the Kantorovich-Rubinstein duality theorem we can restrict to the existential fragment for which more efficient decision procedures exist.

1 Introduction

For systems that contain quantitative information, like, for example, probabilities, time and costs, several *behavioural pseudometrics* (and closely related notions) have been introduced (see, for example, [4, 6, 8, 12, 13, 16–19, 26, 31]). In this paper, we focus on *probabilistic transition systems*, which are a variant of Markov chains. Desharnais, Gupta, Jagadeesan and Panangaden [16] introduced a family of behavioural pseudometrics for these systems. These pseudometrics assign a distance, a real number in the interval $[0, 1]$, to each pair of states of the probabilistic transition system. The distance captures the behavioural similarity of the states. The smaller the distance, the more alike the states behave. The distance is zero if and only if the states are *probabilistic bisimilar*, a behavioural equivalence introduced by Larsen and Skou [24].

The pseudometrics of Desharnais et al. are defined via real-valued interpretations of Larsen and Skou's probabilistic modal logic. Formulae assume truth values in the interval $[0, 1]$. Conjunction and disjunction are interpreted using

* The first and second author were supported by NSERC.

the lattice structure of the unit interval. The modality $\langle a \rangle$ is interpreted arithmetically by integration. The behavioural distance between states s_1 and s_2 is then defined as the supremum over all formulae φ of the difference in the truth value of φ in s_1 and in s_2.[3]

The definition of the behavioural pseudometrics of Desharnais et al. is parametrized by a *discount factor* δ, a real number in the interval $(0, 1]$. The smaller the discount factor, the more (behavioural differences in) the future are discounted. In the case that δ equals one, the future is not discounted. All differences in behaviour, whether in the near or far future, contribute alike to the distance. For systems that (in principle) run forever, we may be interested in all these differences and, hence, in the pseudometric that does not discount the future.

In [14], Desharnais et al. presented an *algorithm* to *approximate* the behavioural distances for δ smaller than one. The first and third author [5] presented also an approximation algorithm for δ smaller than one.

There is a fundamental difference between pseudometrics that discount the future and the one that does not. This is, for example, reflected by the fact that all pseudometrics that discount the future give rise to the same topology, whereas the pseudometric that does not discount the future gives rise to a different topology (see, for example, [16, page 350]). As a consequence, it may not be surprising that neither approximation algorithm mentioned in the previous paragraph can be modified in an obvious way to handle the case that δ equals one.

The main contribution of this paper is an algorithm that approximates behavioural distances in case the discount factor δ equals one. Starting from the *logical* definition of the pseudometric by Desharnais et al., we first give a characterisation of the pseudometric as the greatest (post-)fixed point of a functional on a complete lattice $[0, 1]^S$, where S is the set of states of the probabilistic transition system in question. This functional is closely related to the Kantorovich metric [22] on probability measures. Next, we dualize this characterization exploiting the Kantorovich-Rubinstein duality theorem [23]. Subsequently, we show, exploiting the dual characterization, that a pseudometric being a post-fixed point can be expressed in the existential fragment of the first order theory over real closed fields. Based on the fact that this first order theory is decidable, a result due to Tarski [29], we show how to approximate the behavioural distances. Finally, we discuss an implementation of our algorithm in Mathematica.

Exploiting the techniques put forward in this paper, we have also developed an algorithm to approximate the behavioural pseudometric that is presented in [3]. Due to lack of space, we cannot present this algorithm here. That other algorithm and also the proofs of the results in this paper can be found in [28].

[3] More generally, de Alfaro [11] and McIver and Morgan [25] have given real-valued interpretations to the modal mu-calculus following this pattern. Moreover, de Alfaro has shown that the behavioural pseudometrics induced by mu-calculus formulae agree with those of [16].

2 Systems and pseudometrics

Some basic notions that will play a role in the rest of this paper are presented below. First we introduce the systems of interest: probabilistic transition systems.

Definition 1. *A probabilistic transition system is a tuple $\langle S, \pi \rangle$ consisting of*

- *a finite set S of states and*
- *a function $\pi : S \times S \to [0,1] \cap \mathbb{Q}$ satisfying $\sum_{s' \in S} \pi(s, s') \in \{0, 1\}$.*

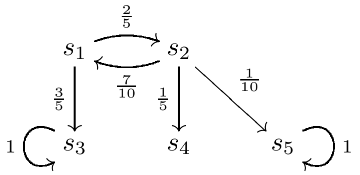
We write $s \to$ if $\sum_{s' \in S} \pi(s, s') = 1$ and $s \not\to$ if $\sum_{s' \in S} \pi(s, s') = 0$.

For states s and s', $\pi(s, s')$ is the probability of making a transition to state s' given that the system is in state s. Each state s either has no outgoing transitions ($s \not\to$) or a transition is taken with probability 1 ($s \to$). To simplify the presentation, we do not consider the case that a state s may refuse to make a transition with some probability, that is, $\sum_{s' \in S} \pi(s, s') \in (0, 1)$. However, all our results can easily be generalized to handle that case as well (see [28]). We also do not consider transitions that are labelled with actions. All our results can also easily be modified to handle labelled transitions (see [28]). In the labelled case, the definition of probabilistic transition system is a mild generalisation of the notion of Markov chain.

In the rest of this paper, we will use the following probabilistic transition system as our running example.

Example 1. We consider a probabilistic transition system with five states: s_1, s_2, s_3, s_4 and s_5. The following table contains the transition probabilities and, hence, captures π. The probabilistic transition system be depicted as the following graph.

	s_1	s_2	s_3	s_4	s_5
s_1	0	$\frac{2}{5}$	$\frac{3}{5}$	0	0
s_2	$\frac{7}{10}$	0	0	$\frac{1}{5}$	$\frac{1}{10}$
s_3	0	0	1	0	0
s_4	0	0	0	0	0
s_5	0	0	0	0	1



We consider states of a probabilistic transition system behaviourally equivalent if they are probabilistic bisimilar [24].

Definition 2. *Let $\langle S, \pi \rangle$ be a probabilistic transition system. An equivalence relation $\mathcal{R}$ on the set of states S is a probabilistic bisimulation if $s_1 \mathcal{R} s_2$ implies $\sum_{s \in E} \pi(s_1, s) = \sum_{s \in E} \pi(s_2, s)$ for all $\mathcal{R}$-equivalence classes E. States s_1 and s_2 are probabilistic bisimilar, denoted $s_1 \sim s_2$, if $s_1 \mathcal{R} s_2$ for some probabilistic bisimulation $\mathcal{R}$.*

Note that probabilistic bisimilar states s_1 and s_2 have the same probability of transitioning to an equivalence class E of probabilistic bisimilar states.

Example 2. Consider the probabilistic transition system of Example 1. The smallest equivalence relation containing (s_3, s_5) is a probabilistic bisimulation. Hence, the states s_3 and s_5 are probabilistic bisimilar.

The behavioural pseudometrics that we study in this paper yield pseudometric spaces on the state space of probabilistic transition systems.

Definition 3. *A 1-bounded pseudometric space is a pair (X, d_X) consisting of a set X and a distance function $d_X : X \times X \to [0, 1]$ satisfying*

1. *for all $x \in X$, $d_X(x, x) = 0$,*
2. *for all x, $y \in X$, $d_X(x, y) = d_X(y, x)$, and*
3. *for all x, y, $z \in X$, $d_X(x, z) \leq d_X(x, y) + d_X(y, z)$.*

Instead of (X, d_X) we often write X and we denote the distance function of a metric space X by d_X.

A (1-bounded) pseudometric space differs from a (1-bounded) metric space in that different points may have distance zero in the former and not in the latter. Since different states of a system may behave the same, such states will have distance zero in our behavioural pseudometrics.

In the characterization of a behavioural pseudometric in Section 4 nonexpansive functions play a key role.

Definition 4. *Let X be a 1-bounded pseudometric space. A function $f : X \to [0, 1]$ is nonexpansive if for all x_1, $x_2 \in X$,*

$$|f(x_1) - f(x_2)| \leq d_X(x_1, x_2).$$

The set of nonexpansive functions from X to $[0, 1]$ is denoted by $X \mathrel{\relbar\joinrel\succcurlyeq} [0, 1]$.

3 Behavioural pseudometrics

Desharnais, Gupta, Jagadeesan and Panangaden [16] introduced a family of behavioural pseudometrics for probabilistic transitions systems. Below, we will briefly review the key ingredients of their definition.

To define their behavioural pseudometrics, Desharnais et al. defined a real-valued semantics of a variant of Larsen and Skou's probabilistic modal logic [24]. We describe this variant, adapted to the case of unlabelled transition systems, in Definition 5.

Definition 5. *The logic $\mathcal{L}$ is defined by*

$$\varphi ::= \text{true} \mid \Diamond\varphi \mid \varphi \land \varphi \mid \neg\varphi \mid \varphi \ominus q$$

where $q \in [0, 1] \cap \mathbb{Q}$.

The main difference between the above logic and the one of Larsen and Skou is that we have $\Diamond\varphi$ and $\varphi \ominus q$ whereas they combine the operators $\Diamond$ and $\ominus q$ into one. Since they consider labelled transitions, they use the notation $\langle a \rangle_q$ for this combined operator.

Desharnais et al. provided a family of real-valued interpretations of the logic. That is, given a probabilistic transition system and a discount factor δ, the interpretation gives a quantitative measure of the validity of a formula φ of the logic in a state s of the system. The interpretation $[\![\varphi]\!]_\delta(s)$ is a real number in the interval $[0,1]$. It measures the validity of the formula φ in the state s. This real number can roughly be thought of as the probability that φ is true in s.

Definition 6. *Given a probabilistic transition system $\langle S, \pi \rangle$ and a discount factor $\delta \in (0,1]$, for each $\varphi \in \mathcal{L}$, the function $[\![\varphi]\!]_\delta : S \to [0,1]$ is defined by*

$$\begin{aligned}
[\![\mathrm{true}]\!]_\delta(s) &= 1\\
[\![\Diamond\varphi]\!]_\delta(s) &= \delta \textstyle\sum_{s' \in S} \pi(s,s')[\![\varphi]\!]_\delta(s')\\
[\![\varphi \wedge \psi]\!]_\delta(s) &= \min\{[\![\varphi]\!]_\delta(s), [\![\psi]\!]_\delta(s)\}\\
[\![\neg\varphi]\!]_\delta(s) &= 1 - [\![\varphi]\!]_\delta(s)\\
[\![\varphi \ominus q]\!]_\delta(s) &= \max\{[\![\varphi]\!]_\delta(s) - q, 0\}
\end{aligned}$$

Example 3. Consider the probabilistic transition system of Example 1. For this system, $[\![\Diamond\mathrm{true}]\!]_\delta(s_3) = \delta$ and $[\![\Diamond\mathrm{true}]\!]_\delta(s_4) = 0$.

Given a discount factor $\delta \in (0,1]$, the behavioural pseudometric d_δ assigns a distance, a real number in the interval $[0,1]$, to every pair of states of a probabilistic transition system. The distance is defined in terms of the logical formulae and their interpretation. Roughly speaking, the distance is captured by the logical formula that distinguishes the states the most.

Definition 7. *Given a probabilistic transition system $\langle S, \pi \rangle$ and a discount factor $\delta \in (0,1]$, the distance function $d_\delta : S \times S \to [0,1]$ is defined by*

$$d_\delta(s_1, s_2) = \sup_{\varphi \in \mathcal{L}} [\![\varphi]\!]_\delta(s_1) - [\![\varphi]\!]_\delta(s_2).$$

Example 4. Consider the probabilistic transition system of Example 1. For example, the states s_3 and s_4 are δ apart. This distance is witnessed by the formula $\Diamond$true. The distances[4] are collected in the following table. Since a distance function is symmetric and the distance from a state to itself is zero, we do not give all the entries.

	s_1	s_2	s_3	s_4
s_2	$\frac{25\delta^2-2\delta^4}{125-25\delta-35\delta^2+7\delta^3}$			
s_3	$\frac{2\delta^3}{25-7\delta^2}$	$\frac{5\delta^2}{25-7\delta^2}$		
s_4	δ	δ	δ	
s_5	$\frac{2\delta^3}{25-7\delta^2}$	$\frac{5\delta^2}{25-7\delta^2}$	0	δ

[4] These distances were obtained "by hand" and checked for numerous different discount factors using the algorithm described in [5].

Proposition 1 ([16, Theorem 5.2]). *d_δ is a 1-bounded pseudometric space.*

Each behavioural pseudometric d_δ is a quantitative analogue of probabilistic bisimilarity. This behavioural equivalence is exactly captured by those states that have distance zero.

Proposition 2 ([16, Theorem 4.10]). *Given a probabilistic transition system $\langle S, \pi\rangle$ and a discount factor $\delta \in (0, 1]$, for all s_1, $s_2 \in S$,*

$$d_\delta(s_1, s_2) = 0 \textit{ if and only if } s_1 \sim s_2.$$

In [14], Desharnais et al. present a decision procedure for the behavioural pseudometric d_δ when δ is smaller than one. Let us briefly sketch their algorithm. They define the depth of a logical formula as follows.

$$\begin{aligned}
\mathrm{depth}(\mathrm{true}) &= 0 \\
\mathrm{depth}(\Diamond\varphi) &= \mathrm{depth}(\varphi) + 1 \\
\mathrm{depth}(\varphi \wedge \psi) &= \max\{\mathrm{depth}(\varphi), \mathrm{depth}(\psi)\} \\
\mathrm{depth}(\neg\varphi) &= \mathrm{depth}(\varphi) \\
\mathrm{depth}(\varphi \ominus q) &= \mathrm{depth}(\varphi)
\end{aligned}$$

One can easily verify that $[\![\varphi]\!]_\delta(s_1) - [\![\varphi]\!]_\delta(s_2) \leq \delta^{\mathrm{depth}(\varphi)}$ for each $\varphi \in \mathcal{L}$. This suggests that one can compute d_δ to any desired degree of accuracy by restricting attention to formulae φ of a fixed modal depth. Clearly, there exist infinitely many formulae of each fixed modal depth. Nevertheless Desharnais et al. show how to construct a finite subset $\mathcal{F}_n$ of the logical formulae of at most depth n such that

$$d_\delta(s_1, s_2) - \sup_{\varphi \in \mathcal{F}_n} [\![\varphi]\!]_\delta(s_1) - [\![\varphi]\!]_\delta(s_2) \leq \delta^n.$$

In this way, $d_\delta(s_1, s_2)$ can be approximated up to arbitrary accuracy *provided δ* is smaller than one.

4 A fixed point characterization and its dual

For the rest of this paper, we focus on the behavioural pseudometric that does not discount the future. That is, we concentrate on the pseudometric d_1. Below, we present an alternative characterization of this pseudometric. In particular, we characterize d_1 as the greatest (post-)fixed point of a function from a complete lattice to itself. This characterization can be viewed as a quantitative analogue of the greatest fixed point characterization of bisimilarity [27].

We also dualize the definition of Δ exploiting the Kantorovich-Rubinstein duality theorem [23]. As we will see in Section 5, this dual characterization will allow us to define Δ as the solution to a minimization problem rather than a maximization problem, as above. In turn this will allow us to capture the fact that a pseudometric is a post-fixed point of Δ in the existential fragment of the first order theory over real closed fields.

For the rest of this paper, we fix a probabilistic transition system $\langle S, \pi\rangle$. We endow the set of pseudometrics on S with the following order.

Definition 8. *The relation $\sqsubseteq$ on 1-bounded pseudometrics on S is defined by*

$$d_1 \sqsubseteq d_2 \text{ if } d_1(s_1, s_2) \geq d_2(s_1, s_2) \text{ for all } s_1,\ s_2 \in S.$$

Note the reverse direction of $\sqsubseteq$ and $\geq$ in the above definition. We decided to make this reversal so that d_1 is a greatest fixed point, in analogy with the characterization of bisimilarity, rather than a least fixed point. This choice has no impact on any results in this paper.

Proposition 3 ([15, Lemma 3.2]). *The set of 1-bounded pseudometrics on S endowed with the order $\sqsubseteq$ forms a complete lattice.*

Next, we introduce a function from this complete lattice to itself of which the behavioural pseudometric d_1 is the greatest fixed point.

Definition 9. *Let d be a 1-bounded pseudometric on S. The distance function $\Delta(d) : S \times S \to [0, 1]$ is defined by*

$$\Delta(d)(s_1, s_2) = \max \left\{ \sum_{s \in S} f(s)(\pi(s_1, s) - \pi(s_2, s)) \;\middle|\; f \in (S, d) \mathrel{\rightarrow\!\!\!\!\!\succsim} [0, 1] \right\}$$

if $s_1 \to$ and $s_2 \to$, and $\Delta(d)(s_1, s_2) = \begin{cases} 0 \text{ if } s_1 \not\to \text{ and } s_2 \not\to \\ 1 \text{ otherwise.} \end{cases}$

Proposition 4. *$\Delta(d)$ is a 1-bounded pseudometric on S.*

To conclude that Δ has a greatest fixed point, it suffices to show that Δ is order-preserving.

Proposition 5. *Δ is order-preserving.*

According to Tarski's fixed point theorem [30, Theorem 1], the fixed points of an order-preserving function on a complete lattice form a complete lattice and, hence, the function has a greatest fixed point. We denote the greatest fixed point of Δ by $\text{gfp}(\Delta)$. This greatest fixed point of Δ is also the greatest post-fixed point of Δ (see, for example, [10, Theorem 4.11][5]).

Theorem 1. $d_1 = \text{gfp}(\Delta)$.

The greatest fixed point of an order-preserving function on a complete lattice can be obtained by iteration (see, for example, [10, Exercise 4.13]).

Definition 10. *For each ordinal α, the 1-bounded pseudometric d^α on S is defined by*

$$\begin{aligned} d^0 &= \top \\ d^{\alpha+1} &= \Delta(d^\alpha) \\ d^\beta &= \bigsqcap_{\alpha \in \beta} d^\alpha \text{ if } \beta \text{ is a limit ordinal} \end{aligned}$$

[5] d is a *post-fixed point* of Δ if $d \sqsubseteq \Delta(d)$. In [10, page 94], such a d is called a prefixpoint.

For $\varDelta$, we need to iterate (at most) ω times before reaching the greatest fixed point. For the system of Example 1 we need ω iterations.

Proposition 6. $\mathrm{gfp}(\varDelta) = d^{\omega}$.

Let us recall (a minor variation of) the Kantorovich-Rubinstein duality theorem. Let X be a 1-bounded compact pseudometric space. Let μ_1 and μ_2 be Borel probability measures on X. We denote the set of Borel probability measures on the product space with marginals μ_1 and μ_2, that is, the Borel probability measures μ on X^2 such that for all Borel subsets B of X,

$$\mu(B \times X) = \mu_1(B) \text{ and } \mu(X \times B) = \mu_2(B),$$

by $\mu_1 \otimes \mu_2$. The Kantorovich-Rubinstein duality theorem tells us

$$\max\left\{ \int_X f d\mu_1 - \int_X f d\mu_2 \,\middle|\, f \in X \rightarrow\!\!\!\!\!\!\approx [0,1] \right\} = \min\left\{ \int_{X^2} d_X d\mu \,\middle|\, \mu \in \mu_1 \otimes \mu_2 \right\}.$$

The following proposition, which is a consequence of the Kantorovich-Rubinstein duality theorem, defines $\varDelta(d)$ as a minimum as opposed to the maximum in Definition 9.

Proposition 7. *Let d be a 1-bounded pseudometric on S. Let s_1, $s_2 \in S$ such that $s_1 \to$ and $s_2 \to$. Then*

$$\varDelta(d)(s_1, s_2) = \min\left\{ \sum_{(s_i,s_j)\in S^2} d(s_i, s_j)\mu(s_i, s_j) \,\middle|\, \mu \in \pi(s_1, \cdot) \otimes \pi(s_2, \cdot) \right\}$$

where $\mu \in \pi(s_1, \cdot) \otimes \pi(s_2, \cdot)$ if

$$\forall s_j \in S \sum_{s_i \in S} \mu(s_i, s_j) = \pi(s_1, s_j) \wedge \forall s_i \in S \sum_{s_j \in S} \mu(s_i, s_j) = \pi(s_2, s_i).$$

5 The algorithm

Before we present our algorithm, we first show that the fact that a pseudometric is a post-fixed point of $\varDelta$ can be expressed in (the existential fragment of) the first order theory over real closed fields. This will allow us to exploit Tarski's decision procedure to approximate the behavioural pseudometric.

For the rest of this paper, we assume that the probabilistic transition system $\langle S, \pi \rangle$ has N states s_1, s_2, $\ldots$, s_N. Instead of $\pi(s_i, s_j)$ we will write π_{ij}. We represent a 1-bounded pseudometric on the set S of states of the probabilistic transition system, as (the values of) a collection of real valued variables d_{ij}.

The fact that d is a 1-bounded pseudometric can now be captured as follows.

Definition 11. *The predicate* pseudo(d) *is defined by*

$$\begin{aligned}\mathrm{pseudo}(d) \equiv & \bigwedge_{1 \leq i,j \leq N} d_{ij} \geq 0 \wedge d_{ij} \leq 1 \wedge \\ & \bigwedge_{1 \leq i \leq N} d_{ii} = 0 \wedge \bigwedge_{1 \leq i,j \leq N} d_{ij} = d_{ji} \wedge \bigwedge_{1 \leq h,i,j \leq N} d_{hj} \leq d_{hi} + d_{ij}\end{aligned}$$

Furthermore, the fact that d is a post-fixed point of Δ can be captured as follows.

Definition 12. *The predicate* post-fixed(d) *is defined by*

$$\begin{aligned}&\text{post-fixed}(d)\\ &\equiv \bigwedge_{1 \leq i_0,j_0 \leq N} \text{post-fixed}_1(d, i_0, j_0) \vee \text{post-fixed}_2(d, i_0, j_0) \vee \text{post-fixed}_3(d, i_0, j_0)\end{aligned}$$

where

$$\begin{aligned}\text{post-fixed}_1(d, i_0, j_0) \equiv & \sum_{1 \leq i \leq N} \pi_{i_0 i} > 0 \wedge \sum_{1 \leq j \leq N} \pi_{j_0 j} > 0 \wedge \\ & \exists (\mu_{ij})_{1 \leq i,j \leq N} \bigwedge_{1 \leq i,j \leq N} \mu_{ij} \geq 0 \wedge \mu_{ij} \leq 1 \\ & \qquad \bigwedge_{1 \leq j \leq N} \sum_{1 \leq i \leq N} \mu_{ij} = \pi_{i_0 j} \wedge \\ & \qquad \bigwedge_{1 \leq i \leq N} \sum_{1 \leq j \leq N} \mu_{ij} = \pi_{j_0 i} \wedge \\ & \qquad \sum_{1 \leq i,j \leq N} d_{ij} \mu_{ij} \leq d_{i_0 j_0} \\ \text{post-fixed}_2(d, i_0, j_0) \equiv & \sum_{1 \leq i \leq N} \pi_{i_0 i} = 0 \wedge \sum_{1 \leq j \leq N} \pi_{j_0 j} = 0 \wedge 0 \leq d_{i_0 j_0} \\ \text{post-fixed}_3(d, i_0, j_0) \equiv & \left(\left(\sum_{1 \leq i \leq N} \pi_{i_0 i} > 0 \wedge \sum_{1 \leq j \leq N} \pi_{j_0 j} = 0 \right) \vee \right. \\ & \left. \left(\sum_{1 \leq i \leq N} \pi_{i_0 i} = 0 \wedge \sum_{1 \leq j \leq N} \pi_{j_0 j} > 0 \right) \right) \wedge \\ & 1 \leq d_{i_0 j_0}\end{aligned}$$

Now we are ready to present our algorithm. Consider the states s_{i_0} and s_{j_0}. We restrict our attention to the case that $s_{i_0} \rightarrow$ and $s_{j_0} \rightarrow$. In the other cases the computation of the distance is trivial.

In our algorithm, we use the algorithm `tarski` that takes as input a sentence of the first order theory of real closed fields and decides the truth or falsity of the given sentence. The fact that there exists such an algorithm was first proved by Tarski [29].

Let ϵ be the desired accuracy. That is, we want to find an interval $[\ell_0, u_0] \subseteq [0, 1]$ such that $u_0 - \ell_0 \leq \epsilon$ and $d_1(s_{i_0}, s_{j_0}) \in [\ell_0, u_0]$. The algorithm approximate takes as input an interval $[\ell, u] \subseteq [0, 1]$ such that $d_1(s_{i_0}, s_{j_0}) \in [\ell, u]$ and returns the desired result. As a consequence, approximate(0, 1) returns an approximation of $d_1(s_{i_0}, s_{j_0})$ with accuracy ϵ.

```
approximate($\ell$, $u$):
   if $u - \ell \leq \epsilon$
      return $[\ell, u]$
   else
      $m = \frac{\ell+u}{2}$
      if tarski($\exists d\, \text{pseudo}(d) \wedge \text{post-fixed}(d) \wedge d_{i_0 j_0} \leq m$)
         return approximate($\ell$, $m$)
      else
         return approximate($m$, $u$)
```

Note that the argument of tarski is a sentence that is part of the existential fragment of the first order theory over real closed fields. For this fragment there are more efficient decision procedures than for the general theory (see, for example, [2]).

Let us sketch a correctness proof of our algorithm. Assume that $d_1(s_{i_0}, s_{j_0}) \in [\ell, u]$. We distinguish the following three cases.

- If $u - \ell \leq \epsilon$, then the algorithm obviously returns the desired result.
- Assume that $u - \ell > \epsilon$ and suppose that tarski returns true. Then there exists a 1-bounded pseudometric d that is a post-fixed point of Δ and $d(s_{i_0}, s_{j_0}) \leq m$. Since d_1 is the greatest post-fixed point of Δ, we have that $d \sqsubseteq d_1$. Hence, $d_1(s_{i_0}, s_{j_0}) \leq d(s_{i_0}, s_{j_0}) \leq m$. Therefore, $d_1(s_{i_0}, s_{j_0}) \in [\ell, m]$.
- Assume that $u - \ell > \epsilon$ and suppose that tarski returns false. Then $d(s_{i_0}, s_{j_0}) > m$ for every 1-bounded pseudometric d that is a post-fixed point of Δ. Since d_1 is a post-fixed point of Δ, we have that $d_1(s_{i_0}, s_{j_0}) > m$. Therefore, $d_1(s_{i_0}, s_{j_0}) \in [m, u]$.

Obviously, the algorithm terminates.

6 An implementation in Mathematica

A decision procedure for the first order theory of real closed fields based on quantifier elimination was first given by Tarski [29]. A number of algorithms have been developed thereafter for the theory (see, for example, [2, 9, 21]). Collin's algorithm is implemented in the tool Mathematica and can be used for solving our formulae. However, it works for very small examples and therefore it is essential to simplify the formula and reduce its size to make it solvable. To simplify the formula, we first compute some of the distances using the following results.

Proposition 8.

- *If* $s_1 \not\rightarrow$ *and* $s_2 \not\rightarrow$ *then* $d_1(s_1, s_2) = 0$.
- *If* $s_1 \not\rightarrow$ *and* $s_2 \rightarrow$, *or* $s_1 \rightarrow$ *and* $s_2 \not\rightarrow$ *then* $d_1(s_1, s_2) = 1$.

Example 5. Consider the probabilistic transition system of Example 1. State s_4 has distance one to all other states.

Next, we present a simple characterization of the distance between a state that never terminates (that is, the probability of reaching a state with no outgoing transitions is zero) and another state.

Given a state s and $n \in \omega + 1$, $\tau_n(s)$ is the probability of terminating in less than n transitions when started in s.

Definition 13. *For each* $n \in \omega + 1$*, the function* $\tau_n : S \to [0, 1]$ *is defined by*

$$\begin{aligned}
\tau_0(s) &= 0 \\
\tau_{n+1}(s) &= \begin{cases} 1 & \textit{if } s \not\rightarrow \\ \sum_{s' \in S} \pi(s, s')\tau_n(s') & \textit{otherwise} \end{cases} \\
\tau_\omega(s) &= \sup_{n \in \omega} \tau_n(s)
\end{aligned}$$

Example 6. Consider the probabilistic transition system of Example 1. Then we have that $\tau_\omega(s_1) = \frac{1}{9}$, $\tau_\omega(s_2) = \frac{5}{18}$, $\tau_\omega(s_3) = 0$, $\tau_\omega(s_4) = 1$ and $\tau_\omega(s_5) = 0$.

Obviously, for a state s without outgoing transitions, we have that $\tau_\omega(s) = 1$. For a state s that cannot reach any state without outgoing transitions, we have that $\tau_\omega(s) = 0$. For the remaining states, we can compute the probability of termination using standard techniques as described in, for example, [20, Section 11.2].

Proposition 9. *If* $\tau_\omega(s_2) = 0$ *then* $d_1(s_1, s_2) = \tau_\omega(s_1)$.

Example 7. Consider the probabilistic transition system of Example 1. From Proposition 9 we can conclude that $d_1(s_1, s_3) = \frac{1}{9}$, $d_1(s_2, s_3) = \frac{5}{18}$, $d_1(s_4, s_3) = 1$ and $d_1(s_5, s_3) = 0$.

Given a probabilistic bisimulation $\mathcal{R}$, we can quotient the probabilistic transition system $\langle S, \pi \rangle$ as follows.

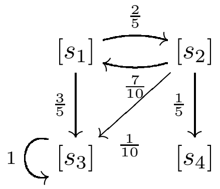
Definition 14. *Let* $\mathcal{R}$ *be a probabilistic bisimulation. The probabilistic transition system* $\langle S_\mathcal{R}, \pi_\mathcal{R} \rangle$ *consists of*

- *the set* $S_\mathcal{R} = \{\, [s] \mid s \in S \,\}$ *of* $\mathcal{R}$*-equivalence classes and*
- *the function* $\pi_\mathcal{R} : S_\mathcal{R} \times S_\mathcal{R} \to [0, 1]$ *defined by*

$$\pi_\mathcal{R}([s], [s']) = \sum_{s'' \mathcal{R} s'} \pi(s, s'').$$

Note that the function $\pi_\mathcal{R}$ is well-defined since $\mathcal{R}$ is a probabilistic bisimulation. We will apply the above quotient construction for probabilistic bisimilarity (which can be computed in polynomial time [1]).

Example 8. Consider the probabilistic transition system of Example 1. The smallest equivalence relation containing $\{\langle s_3, s_5\rangle\}$ is a probabilistic bisimulation. The resulting quotient can be depicted as



By quotienting, the number of states that need to be considered and, hence, the number of variables in the formula may be reduced. However, we still have to check that the quotiented system gives rise to the same distances. Next we relate the behavioural pseudometric d_1 of the original system $\langle S, \pi\rangle$ with the behavioural pseudometric $d_{\mathcal{R}}$ of the quotiented system $\langle S_{\mathcal{R}}, \pi_{\mathcal{R}}\rangle$.

Proposition 10. *For all s_1, $s_2 \in S$, $d_{\mathcal{R}}([s_1], [s_2]) = d_1(s_1, s_2)$.*

To simplify the formula even further, we exploit the following three observations.

- Since d is a pseudometric, $d_1(s_i, s_i) = 0$ and $d_1(s_i, s_j) = d_1(s_j, s_i)$. Therefore, in $\text{pseudo}(d) \wedge \text{post-fixed}(d)$ we can replace all d_{ii}'s with zero and all d_{ij}'s where $i > j$ with d_{ji}'s. As a consequence, we only need to consider d_{ij}'s with $i < j$. This reduces the number of variables in the formula considerably.
- Let C be the set of pairs of states for which the distances have already been computed. Then
$$\exists d\, \text{pseudo}(d) \wedge \text{post-fixed}(d) \wedge d_{i_0 j_0} \leq m$$
is equivalent to
$$\exists d\, \text{pseudo}(d) \wedge \text{post-fixed}(d) \wedge d_{i_0 j_0} \leq m \wedge \bigwedge_{(i,j) \in C} d_{ij} = d_1(s_i, s_j)$$
since d_1 is the greatest post-fixed point. As a consequence, we can replace all d_{ij}'s where $(i, j) \in C$ with their already computed distances $d_1(s_i, s_j)$. Again, the number of variables may be reduced.
- If $\pi_{i_0 j} = 0$, we can infer that $\mu_{ij} = 0$ for all $1 \leq i \leq N$. As a consequence, we can replace the occurrences of all those μ_{ij}'s with 0. Symmetrically, if $\pi_{j_0 i} = 0$ we can simplify the formula similarly. Also this simplification may reduce the number of variables.

We have implemented these simplifications in the form of a Java program that takes as input the probability matrix π and that produces as output the simplified formula in a format that can be fed to Mathematica.[6]

[6] The code and documentation is available at the URL `www.cse.yorku.ca/~franck/research/pm2m`.

Example 9. Consider the probabilistic transition system of Example 1. The simplified formula for this system is given below.

```
1  Reduce[
2    Exists[d12,
3      (0 <= d12 <= 1) && (0.11112 <= d12 + 0.27778) && (d12 <= 0.38889) &&
4      Exists[{u12,u13,u32,u42,u43,u33},
5        (0 <= u12 <= 1) && (0 <= u13 <= 1) && (0 <= u32 <= 1) &&
6        (0 <= u42 <= 1) && (0 <= u43 <= 1) &&
7        (u12 + u32 + u42 == 0.4) && (u13 + u43 + u33 == 0.6) &&
8        (u12 + u13 == 0.7) && (u32 + u33 == 0.1) && (u42 + u43 == 0.2) &&
9        (d12 * u12 + 0.11112 * u13 + 0.27778 * u32 + u42 + u43 <= d12)] &&
10     Exists[{u21,u23,u24,u31,u33, u34},
11       (0 <= u21 <= 1) && (0 <= u23 <= 1) && (0 <= u24 <= 1) &&
12       (0 <= u31 <= 1) && (0 <= u34 <= 1) &&
13       (u21 + u31 == 0.7) && (u23 + u33 == 0.1) && (u24 + u34 == 0.2) &&
14       (u21 + u23 + u24 == 0.4) && (u31 + u33 + u34 == 0.6) &&
15       (d12 * u21 + 0.27778 * u23 + u24 + 0.11112 * u31 + u34 <= d12)] &&
16     (0 <= d12 <= 0.5)]]
```

Line 3 correspond to pseudo(d), line 4–9 correspond to post-fixed$_1(d, 1, 2)$ and line 10–15 correspond to post-fixed$_1(d, 2, 1)$. The formula was reduced to true by Mathematica in 8.2 seconds on a 3GHz machine with 1GB RAM. When feeding Mathematica the formula that has not been simplified, it runs out of memory after some time.

We also attempted to solve this example with a solver called QEPCAD B [7] but the performance of Mathematica on this example was better.

7 Conclusion

This paper combines a number of ingredients, known already for a long time, including the Kantorovich-Rubinstein duality theorem of the fifties, Tarski's fixed point theorem of the fourties and Tarski's decision procedure for the first order theory of real closed fields of the thirties. We show that the behavioural pseudometric d_1, which does not discounts the future, can be approximated up to an arbitrary accuracy. While the combination of the above results into a decision procedure for the pseudometric is not technically difficult, we do solve a problem that has been open since 1999. Most of the results in Section 3 and 4 are (variations on) known results. As far as we know, the results in Section 5 and 6 are new. The techniques exploited in this paper have also been used to approximate other behavioural pseudometrics that do not discount the future like, for example, the one presented in [3]. Furthermore, our algorithm can easily be adjusted to the discounted case. As future work, we plan to apply our techniques to obtain approximation algorithms for other behavioural pseudometrics like, for example, the one presented in [13]. Since the satisfiability problem for the existential fragment of the first order theory of the real closed fields is PSPACE [2], it is not surprising that our algorithm can only handle small examples as we have shown in Section 6. As a consequence, the quest for practical algorithms to approximate d_1 is still open. Since the closure ordinal of Δ is ω, as proved in Proposition 6, an iterative algorithm might be feasible.

Acknowledgements The authors would like to thank Christel Baier for providing some pointers to the literature and Jeff Edmonds, Parke Godfrey and the referees for their constructive feedback.[7]

References

1. C. Baier, B. Engelen, and M. Majster-Cederbaum. Deciding bisimilarity and similarity for probabilistic processes. *Journal of Computer and System Sciences*, 60(1):187–231, 2000.
2. S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43(6):1002–1045, 1996.
3. F. van Breugel. A behavioural pseudometric for metric labelled transition systems. In *Proceedings of the 16th International Conference on Concurrency Theory*, volume 3653 of *Lecture Notes in Computer Science*, pages 141–155. Springer-Verlag, 2005.
4. F. van Breugel and J. Worrell. A behavioural pseudometric for probabilistic transition systems. *Theoretical Computer Science*, 331(1):115–142, 2005.
5. F. van Breugel and J. Worrell. An algorithm for approximating behavioural pseudometrics for probabilistic transition systems. *Theoretical Computer Science*, 360(1/3):373–385, 2006.
6. M. Broucke. Regularity of solutions and homotopic equivalence for hybrid systems. In *Proceedings of the 37th IEEE Conference on Decision and Control*, volume 4, pages 4283–4288. IEEE, 1998.
7. C.W. Brown. An overview of QEPCAD B: a tool for real quantifier elimination and formula simplification. *Journal of Japan Society for Symbolic and Algebraic Computation*, 10(1):13–22, 2003.
8. P. Caspi and A. Benveniste. Toward an approximation theory for computerised control. In *Proceedings of the 2nd International Conference on Embedded Software*, volume 2491 of *Lecture Notes in Computer Science*, pages 294–304. Springer-Verlag, 2002.
9. G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Proceedings of the 2nd GI Conference on Automata Theory and Formal Languages*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183. Springer-Verlag, 1975.
10. B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*, Cambridge University Press, 1990.
11. L. de Alfaro. Quantitative verification and control via the mu-calculus. In *Proceedings of the 14th International Conference on Concurrency Theory*, volume 2761 of *Lecture Notes in Computer Science*, pages 102–126. Springer-Verlag, 2003.
12. L. de Alfaro, T.A. Henzinger, and R. Majumdar. Discounting the future in systems theory. In *Proceedings of 30th International Colloquium on Automata, Languages and Programming*, volume 2719 of *Lecture Notes in Computer Science*, pages 1022–1037. Springer-Verlag, 2003.

[7] Due to lack of space, some suggestions could unfortunately not be implemented.

13. Y. Deng, T. Chothia, C. Palamidessi, and J. Pang. Metrics for action-labelled quantitative transition systems. In *Proceedings of 3rd Workshop on Quantitative Aspects of Programming Languages*, volume 153(2) of *Electronic Notes in Theoretical Computer Science*, pages 79–96. Elsevier, 2005.
14. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Metrics for labeled Markov systems. In *Proceedings of 10th International Conference on Concurrency Theory*, volume 1664 of *Lecture Notes in Computer Science*, pages 258–273. Springer-Verlag, 1999.
15. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. The metric analogue of weak bisimulation for probabilistic processes. In *Proceedings of 17th Annual IEEE Symposium on Logic in Computer Science*, pages 413–422. IEEE, 2002.
16. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Metrics for labelled Markov processes. *Theoretical Computer Science*, 318(3):323–354, 2004.
17. A. Di Pierro, C. Hankin, and H. Wiklicky. Quantitative relations and approximate process equivalences. In *Proceedings of the 14th International Conference on Concurrency Theory*, volume 2761 of *Lecture Notes in Computer Science*, pages 508–522. Springer-Verlag, 2003.
18. A. Giacalone, C.-C. Jou, and S.A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of the IFIP WG 2.2/2.3 Working Conference on Programming Concepts and Methods*, pages 443–458. North-Holland, 1990.
19. A. Girard and G.J. Pappas. Approximate bisimulations for nonlinear dynamical systems. In *Proceedings of the 44th IEEE Conference on Decision and Control and the European Control Conference*, pages 684–689. IEEE, 2005.
20. C.M. Grinstead and J.L. Snell. *Introduction to Probability*, AMS, 1997.
21. L. Hörmander. *The Analysis of Linear Partial Differential Operators II: Differential Operators with Constant Coefficients*, Springer-Verlag, 2005.
22. L. Kantorovich. On the transfer of masses (in Russian). *Doklady Akademii Nauk*, 37(2):227–229, 1942. Translated in *Management Science*, 5:1–4, 1959.
23. L.V. Kantorovich and G.Sh. Rubinstein. On the space of completely additive functions. *Vestnik Leningradskogo Universiteta*, 3(2):52–59, 1958. In Russian.
24. K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991.
25. A.K. McIver and C.C. Morgan. Results of the quantitative μ-calculus qMμ. *ACM Transactions on Computational Logic*. To appear.
26. J.C Mitchell, A. Ramanathan, A. Scedrov, and V. Teague. A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols. *Theoretical Computer Science*, 353(1/3):118–164, 2006.
27. D. Park. Concurrency and automata on infinite sequences. In *Proceedings of 5th GI-Conference on Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer-Verlag, 1981.
28. B. Sharma. An algorithm to quantify behavioural similarity between probabilistic systems. Master's thesis, York University, Toronto, 2006.
29. A. Tarski. *A decision method for elementary algebra and geometry*, University of California Press, 1951.
30. A. Tarski. A lattice-theoretic fixed point theorem and its applications. *Pacific Journal of Mathematics*, 5(2):285–309, 1955.
31. M. Ying. Bisimulation indexes and their applications. *Theoretical Computer Science*, 275(1/2):1–68, 2002.