ARTICLE IN PRESS YINCO:4328

Information and Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Probabilistic bisimilarity as testing equivalence

Yuxin Deng [a,*], Yuan Feng [b]

[a] Shanghai Key Laboratory of Trustworthy Computing, MOE International Joint Lab of Trustworthy Software, and International Research Center of Trustworthy Software, East China Normal University, China
[b] University of Technology Sydney, Australia

ARTICLE INFO

Article history:
Received 26 October 2016
Received in revised form 23 September 2017
Available online xxxx

Keywords:
Probabilistic processes
Bisimilarity
Testing equivalence
Modal logic

ABSTRACT

Larsen and Skou initiated the study of probabilistic bisimilarity and its characterisation in terms of tests. Later on, van Breugel et al. showed that, for labelled Markov processes with continuous state spaces, probabilistic bisimilarity nicely coincides with a simple notion of testing equivalence. Their proof employs advanced machinery from topology. In the discrete case of finite-state reactive probabilistic processes, we prove that coincidence result with an elementary and more accessible proof.

1. Introduction

Bisimulation [17,18] is a central concept in concurrency theory. Bisimilarity, the largest bisimulation, admits beautiful characterisations in terms of fixed points, modal logics, coalgebras, games, algorithms, pseudometrics, etc. Its generalisation in the probabilistic setting is initiated by Larsen and Skou in [16] and has subsequently been widely investigated in probabilistic concurrency theory. Various characterisations of probabilistic bisimilarity by probabilistic extensions of Hennessy–Milner logic [11] have appeared in the literature [16,8,9,19,4,12,10,7,3]. Most characterisations employ some modalities indexed with numbers. A typical modal formula, dated back to [16], is $\langle a\rangle_p\phi$, where p is a probability value. A state s satisfies this formula if the probability that s can make an a-labelled transition to the set of states satisfying ϕ exceeds p. For reactive probabilistic processes [16,22] with a minimal probability assumption, it is also shown in [16] that probabilistic bisimilarity can be characterised by a very simple testing framework. Two remarkable features of this framework are the *absence* of any modality indexed with numbers and the arithmetic interpretation of conjunction as multiplication. To prove the testing characterisation result, a notion of observation is introduced, every test is associated with a set of observations, and a testing equivalence is defined for states as the equality of probabilities on these observations. Furthermore, the coincidence proof of probabilistic bisimilarity with the testing equivalence crucially relies on the modal characterisation of probabilistic bisimilarity by a variant of Hennessy–Milner logic. In [21] van Breugel et al. avoid observations and directly define a testing equivalence for states as the equality of probabilities on tests. They generalise the testing characterisation of [16] to labelled Markov processes, i.e. reactive probabilistic processes [16,22] with continuous state spaces, and surprisingly, without going through any modal logic. Usually, the simpler the logical or testing characterisation, the more difficult the completeness proof, since constructing distinguishing formulae or tests for non-bisimilar states with fewer modalities is more challenging. Van Breugel et al. prove such an elegant result by using advanced machinery

* Corresponding author.
E-mail addresses: yxdeng@sei.ecnu.edu.cn (Y. Deng), Yuan.Feng@uts.edu.au (Y. Feng).

https://doi.org/10.1016/j.ic.2017.09.014
0890-5401/

such as the Lawson topology on probabilistic powerdomains [13] and Banach algebras. However, if we confine ourselves to discrete rather than continuous state spaces, as in e.g. [16], it is still unclear how to give a more direct and much simpler proof of the coincidence result given in [21], though intuitively it should be possible. The current work aims to provide a clear answer to this question. We consider finite-state reactive probabilistic processes and give an elementary proof of the coincidence of bisimilarity with the aforementioned testing equivalence while avoiding all the advanced machinery used in [21]. Our arguments only involve simple probability theory, ranks of matrices, and induction. It is worth mentioning that our proof is also constructive.

In the current work we focus on reactive probabilistic processes. Testing equivalences for other models have received a lot of attention. For example, Kwiatkowska and Norman [15] have generalised the testing framework of [16] to probabilistic systems with external and internal choice. Cleaveland et al. [1] have generalised the testing theory of [2] to generative probabilistic processes. Jonsson and Wang [14] have generalised [2] to nondeterministic probabilistic processes, which is further developed in [20,6,5,3]. For the moment, we are not clear if our proof idea can be used in a setting with both probabilities and nondeterminism, which is left as an open problem.

2. Preliminaries

Let S be a finite set. A *(discrete) probability distribution* over set S is a function $\Delta : S \to [0,1]$ with $\sum_{s\in S}\Delta(s) = 1$. Its *support*, written $\lceil\Delta\rceil$, is the set $\{s \in S \mid \Delta(s) > 0\}$. Let $\mathcal{D}(S)$ denote the set of all distributions over S. We write $\overline{s}$ for the point distribution, satisfying $\overline{s}(t) = 1$ if $t = s$, and 0 otherwise. If $p_i \geq 0$ and Δ_i is a distribution for each i in some finite index set I, then $\sum_{i\in I} p_i \cdot \Delta_i$ is given by

$$(\sum_{i\in I} p_i \cdot \Delta_i)(s) \quad = \quad \sum_{i\in I} p_i \cdot \Delta_i(s)$$

If $\sum_{i\in I} p_i = 1$ then this is easily seen to be a distribution in $\mathcal{D}(S)$.

Definition 1. A *reactive probabilistic labelled transition system* (rpLTS) is a triple $(S, A, \to)$, where S is a set of states, A is a set of actions, and the transition relation $\to$ is a partial function from $S \times A$ to $\mathcal{D}(S)$.

We write $s \xrightarrow{a} \Delta$ for $\to(s,a) = \Delta$. In the current work, we focus on rpLTSs with finitely many states. Let us fix a rpLTS $(S, A, \to)$ for the rest of this note, with S and A being finite sets.

In the probabilistic setting, formal systems are usually modelled as distributions over states. To compare two systems involves the comparison of two distributions. So we need a way of lifting relations on states to relations on distributions. A few approaches have appeared in the literature. The following one is taken from [5],

Definition 2. Given two sets S, T and a binary relation $\mathcal{R} \subseteq S \times T$, the lifted relation $\mathcal{R}^\dagger \subseteq \mathcal{D}(S) \times \mathcal{D}(T)$ is the smallest relation that satisfies:

(i) $s\,\mathcal{R}\,t$ implies $\overline{s}\,\mathcal{R}^\dagger\,\overline{t}$;
(ii) $\Delta_i\,\mathcal{R}^\dagger\,\Theta_i$ for all $i \in I$ implies $(\sum_{i\in I} p_i \cdot \Delta_i)\,\mathcal{R}^\dagger\,(\sum_{i\in I} p_i \cdot \Theta_i)$, where I is a finite index set and $\sum_{i\in I} p_i = 1$.

There are alternative presentations of Definition 2; see [3, Chapter 3] for more detailed discussion. The following property is very useful.

Proposition 1. *Let Δ and Θ be distributions over S and $\mathcal{R}$ be an equivalence relation. Then $\Delta\,\mathcal{R}^\dagger\,\Theta$ if and only if $\Delta(C) = \Theta(C)$ for all equivalence classes $C \in S/\mathcal{R}$, where $\Delta(C)$ stands for the accumulation probability $\sum_{s\in C}\Delta(s)$.*

Bisimulation is a central notion in concurrency theory. Larsen and Skou [16] generalised it to the probabilistic setting and defined probabilistic bisimulation for rpLTSs.

Definition 3. A binary relation $\mathcal{R} \subseteq S \times S$ is a *probabilistic simulation* if $s\,\mathcal{R}\,t$ and $s \xrightarrow{a} \Delta$ implies the existence of some transition $t \xrightarrow{a} \Theta$ with $\Delta\,\mathcal{R}^\dagger\,\Theta$.

If both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are probabilistic simulations, then $\mathcal{R}$ is a *probabilistic bisimulation*. The largest probabilistic bisimulation is called *probabilistic bisimilarity*, denoted by $\sim$.

Note that $\sim$ is an equivalence relation on S.

Various characterisations of probabilistic bisimilarity by probabilistic versions of Hennessy–Milner logic [11] have appeared in the literature. For example, Desharnais et al. [8] use a logic with the grammar

$$\phi ::= \top \mid \phi \wedge \phi \mid \langle a\rangle_q \phi$$