Generic Forward and Backward Simulations II: Probabilistic Simulation

Ichiro Hasuo

1 RIMS, Kyoto University, Japan
2 PRESTO Research Promotion Program, Japan Science and Technology Agency

Abstract. Jonsson and Larsen’s notion of probabilistic simulation is studied from a coalgebraic perspective. The notion is compared with two generic coalgebraic definitions of simulation: Hughes and Jacobs’ one, and the one introduced previously by the author. We show that the first almost coincides with the second, and that the second is a special case of the last. We investigate implications of this characterization; notably the Jonsson-Larsen simulation is shown to be sound, i.e. its existence implies trace inclusion.

1 Introduction

Use of probabilistic algorithms in distributed and concurrent applications is common practice. Consequently, modeling and verification techniques for probabilistic systems have been extensively developed. One fundamental branch therein is about probabilistic (bi)simulation: it gives an answer when a probabilistic system is “equivalent” to another, or when one “refines” another.

In this paper we focus on simulation notions for purely probabilistic systems. For such systems it is standard to define a notion of simulation using weight functions. The idea is first devised by Jonsson and Larsen [12]; it has inspired a large body of work including [1]. Our aim in this paper is to shed fresh, mathematical light on the idea, from the viewpoint of coalgebra.

Coalgebra is a mathematical/categorical presentation of state-based systems. Its initial success was brought about by a generic, coalgebraic characterization of bisimulation that applies to a variety of systems, including probabilistic ones (see e.g. [11, 17, 19]). The theory has since been extended to include various aspects of concurrency theory—such as SOS and modal logic (see e.g. [13]). Simulation, as “one-sided bisimulation,” is one of such aspects.

Two approaches have been presented towards a coalgebraic theory of simulation: Hughes and Jacobs’ [10] and the current author’s [5]. Both approaches are generic, applicable to non-deterministic systems like LTS as well as probabilistic ones. In this paper we restrict them to a purely probabilistic setting and conduct a comparative study. The comparison is among the Jonsson-Larsen simulation, the Hughes-Jacobs simulation, and the one in the author’s previous work [5] which we call the Kleisli simulation.

Among the three, the notion of Kleisli simulation is the most distinguishable: it is given not as a relation but as a function $X \to DY$, where $X$ and $Y$ are the state spaces.

1 Unlike e.g. Segala’s probabilistic automata [18], they do not feature non-determinism.

© Springer-Verlag Berlin Heidelberg 2010
of the involved systems. Therefore it is not suitable as a candidate of a refinement relation, the original motivation for the Jonsson-Larsen one. The Kleisli simulation rather follows the spirit of Lynch and Vaandrager [16]: it is a powerful tool for showing trace inclusion. While a direct proof of trace inclusion involves transitions within arbitrary many steps, finding a simulation is a stepwise matter. Indeed the notion of Kleisli simulation is precisely a coalgebraic generalization of the one in [16]; the former comes with the forward and backward variations just like the latter. The theory in [5] has been successfully applied to verification of probabilistic anonymity in [9].

Our findings are as follows. The standard Jonsson-Larsen simulation, defined in §3 concretely for a specific kind of probabilistic systems (we describe them in §2), is identified with a slightly restricted variant of the Hughes-Jacobs simulation (§4). This allows us to remove the unnecessary restriction that was hidden in the original concrete definition (§4.4), as well as provides a guideline in transferring the definition to other kinds of probabilistic systems (§4.5). On another link in the triangle, we identify the Hughes-Jacobs simulation as a special case of the Kleisli simulation (§5). From the generic soundness theorem [5]—existence of a Kleisli simulation implies (finite) trace inclusion—we thus conclude soundness of the Hughes-Jacobs notion, hence of the Jonsson-Larsen one.

Our expedition will be in a leisurely pace. In particular, no categorical or coalgebraic prerequisites are assumed; they are introduced on our way, on a call-by-need basis. Due to space limitation, most proofs are deferred to an extended version [7]. It has also a series of example systems for further comparison of different simulation notions.

Notations. A square in a diagram which is not filled means that it commutes, that is, the equality symbol = is implicit in it.

A probability (sub)distribution γ over a set X is often denoted like a table: \[ x \mapsto \gamma(x) \mid x \in X \]. When an entry \( x \in X \) is missing in the table, the probability 0 is assigned. Hence for example, when \( x_0 \in X \) is a fixed element, \[ x_0 \mapsto 1 \] means the distribution γ such that \( \gamma(x_0) = 1 \) and \( \gamma(x) = 0 \) for \( x \neq x_0 \).

2 Probabilistic System

We will be mainly interested in two kinds of purely probabilistic systems—GPAs and DTMCs—which we now define formally.

Definition 2.1 (Generative probabilistic automaton, GPA). Let \( \mathcal{A} \) be a fixed nonempty alphabet; we refer to its element as an action. A generative probabilistic automaton (GPA) over \( \mathcal{A} \) is a triple \( \mathcal{X} = (X, x_0, c) \) where

- \( X \) is a nonempty set of states;
- \( x_0 \in X \) is a chosen state which is called the initial one; and
- \( c : X \rightarrow D(\{\checkmark\} + \mathcal{A} \times X) \) is a transition function. Here \( \{\checkmark\} \) is a singleton; + denotes the disjoint union; and \( D \) is the subdistribution operation such that for a set \( Y \)

\[
DY = \{\gamma : Y \rightarrow [0, 1] \mid \sum_{y \in Y} \gamma(y) \leq 1\}.
\] (1)

Such \( d \in DY \) is called a sub-distribution since its values add up to not more than 1, instead of precisely 1.