Sound and Complete Axiomatization of Trace Semantics for Probabilistic Systems

Alexandra Silva[1,2]

Centrum Wiskunde & Informatica, The Netherlands

Ana Sokolova[3,4]

Department of Computer Sciences, University of Salzburg, Austria

Abstract

We present the first sound and complete axiomatization of trace semantics for probabilistic transition systems. Our approach is coalgebraic, which opens the door to axiomatize other types of systems. In order to prove soundness and completeness, we employ determinization and show that coalgebraic traces can be recovered via determinization, a result interesting in itself. The approach is also applicable to labelled transition systems, for which we can recover the known axiomatization of trace semantics (work of Rabinovich).

1 Introduction

Quite some amount of work in formal methods, in particular on process algebra and process calculi, concentrates on representing processes by expressions (terms in some process algebraic language) and providing axiomatizations of behavior semantics, in most cases branching-time semantics.

Coalgebras arose as a mathematical model of state-based systems in the last couple of decades. The strength of coalgebraic modeling lies in the fact that many important notions are parametrized by the type of the system, formally given by a functor. On the one hand, the coalgebraic framework is

[1] Email: ams@cwi.nl

[2] Visiting researcher at Cornell University

[3] Email: anas@cs.uni-salzburg.at

[4] Research supported by the Austrian Science Fund (FWF) grant V00125

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

unifying, allowing for a uniform study of different systems and making precise the connection between them. On the other hand, it can serve as a guideline for the development of basic notions for new models of computation.

In [SBBR10b], Bonchi, Bonsangue, Rutten and the first author made use of the coalgebraic view on systems to devise a framework where languages of specification and axiomatizations can be uniformly derived for a large class of systems, including quantitative systems, such as weighted and probabilistic automata. The axiomatizations considered were proved, in a uniform way, to be sound and complete with respect to bisimilarity.

Bisimilarity may sometimes be considered a too strong equivalence between states of a system [NV09]. For applications where the branching in the system is irrelevant, linear-time semantics like trace semantics might be more appropriate. Consider for example the following two probabilistic transition systems

$$\bullet \xrightarrow{a,\frac{1}{2}} \bullet \xrightarrow{b,\frac{1}{3}} \bullet \xrightarrow{1} * \qquad\qquad \bullet \xrightarrow{a,\frac{1}{3}} \bullet \xrightarrow{b,\frac{1}{2}} \bullet \xrightarrow{1} *$$

where the labels a and b are action labels, and the labels $\frac{1}{2}$, $\frac{1}{3}$ are quantities that represent probabilistic branching (the probability of getting from one state to another with a given label). These two systems are not bisimilar, but they are trace equivalent since for (finite) trace equivalence only the total probability to reach termination with a word of labels matters (for both systems this probability is $\frac{1}{6}$ by the unique possible word ab).

In [HJS07], Hasuo, Jacobs and the second author provided a notion of (finite) trace semantics for a large class of coalgebras and showed that their abstract notion coincides with existing notions in the literature, such as the ones for labeled transition systems or (generative) probabilistic automata. The theory works for TF-coalgebras in **Sets** with T a suitable monad modeling branching and F a suitable functor modeling linear behavior (involving the existence of a distributive law $\lambda{:}FT \Rightarrow TF$ that distributes branching over linear behavior). Coalgebraic trace semantics shows that linear-time semantics fits into the paradigm of final coalgebra semantics (in the Kleisli category of the monad T), and can thus benefit from the associated machinery, for instance in showing compositionality/congruence of bisimilarity and trace equivalence for various coalgebras [HJS07]. This paper shows another benefit of the generic trace theory, allowing for new sound and complete axiomatizations of trace semantics for probabilistic transition systems in a coalgebraic view.

The paper combines the work on generic axiomatizations [SBBR10b] bringing process algebra to coalgebra and coalgebraic trace semantics [HJS07] and provides a sound and complete axiomatization of trace semantics for probabilistic transition systems. Probabilistic transition systems are coalgebras of type $\mathcal{D}_\omega(1 + A \times id)$, where $\mathcal{D}_\omega$ is the subdistribution monad. The work presented here can be seen as a step towards the goal to derive a framework where axiomatizations for trace semantics can be uniformly derived for a larger class of systems. However, it is difficult to describe a class of monads for which the conditions of the generic trace theory are met. The generic trace theory works for the powerset monad which allows us to use the same approach and provide sound and complete axiomatization of (finite) trace semantics for labeled transition systems (LTS), in which case we can recover the results of Rabinovich.

We build on the framework of [SBBR10b] in the sense that we keep the same specification language but add new axioms. This is natural and also in accordance to the strategy used by Rabinovich, who presented a sound and complete axiomatization of trace semantics for LTS [Rab93] by adding one axiom to the sound and complete axiomatization of bisimilarity proposed by Milner for the same language [Mil84]. In our case two additional axioms suffice: the one takes care of multiplying weights along paths (corresponding to the monad multiplication), and the other one involves distributivity (corresponding to the distributive law). It should be noted however that the step from qualitative, that is LTS, to general quantitative systems is not at all trivial. The main difficulty is caused by the following: while every finite LTS can be changed to a finite trace-equivalent LTS that is deterministic (in any state there is at most one a-labelled transition), this is not the case for probabilities/general weights. For a finite system (hence corresponding to an expression), there may be no finite deterministic system that is trace equivalent to it. Hence, the difficulty is in finding a "normal form" expression for all expressions that represent trace equivalent systems, since expressions correspond to finite systems only. Coalgebraic proofs of soundness and completeness [Jac06,BRS09,SBBR10b] involve a finality argument that avoids reasoning about normal forms. This is our way out as well: We use the (infinite) determinization of a probabilistic transition system but avoid reasoning about normal forms by using a (more involved) finality argument.

Organization of the paper Section 2 and Section 3 are the introductory part of the paper introducing basics of coalgebras and coalgebraic trace semantics, and probabilistic transition systems and their trace semantics in concrete terms, respectively. In Section 4 we present the syntax of expressions for quantitative transition systems, followed by the axiomatization in Section 5 where the main results (soundness and completeness) are presented and proven. We wrap-up with concluding remarks in Section 6. The proofs are available in [SS11].

2 Preliminaries

In this section, we introduce the basic definitions on coalgebras and (coalgebraic) trace semantics.

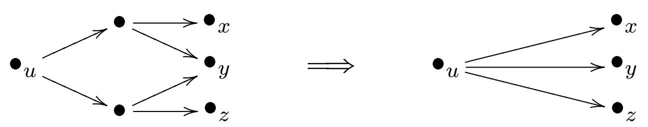
Coalgebras and algebras. Let F be an endofunctor on **Sets**, the category of sets and functions. An F-coalgebra is a pair $(X, \alpha\colon X \to F(X))$ where X is the carrier set, the set of states, and α is the coalgebra transition map. An F-algebra is a pair $(X, \mathfrak{a}\colon F(X) \to X)$. For brevity, we often identify a (co)algebra with its (co)algebra map. Given two F-coalgebras $\alpha\colon X \to F(X)$ and $\beta\colon Y \to F(Y)$, a coalgebra homomorphism from α to β is a map $h\colon X \to Y$ such that $\beta \circ h = F(h) \circ \alpha$. Given two F-algebras $\mathfrak{a}\colon F(X) \to X$ and $\mathfrak{b}\colon F(Y) \to Y$, an algebra homomorphism from $\mathfrak{a}$ to $\mathfrak{b}$ is a map $h\colon X \to Y$ such that $\mathfrak{b} \circ D(h) = h \circ \mathfrak{a}$. F-(co)algebras together with their coalgebra homomorphisms form a category.

A final F-(co)algebra is a final object in the category of F-(co)algebras: From any F-(co)algebra α there is a unique homomorphism beh_α to the final one. If a final coalgebra exists, it induces a final coalgebra semantics which identifies two states if and only if they are mapped to the same element of the final coalgebra via the unique homomorphism. In **Sets**, for weak pullback preserving functors, the final coalgebra semantics coincides with bisimilarity, i.e., for states x and y in a coalgebra $\alpha\colon X \to F(X)$, $x \sim y \Leftrightarrow \mathrm{beh}_\alpha(x) = \mathrm{beh}_\alpha(y)$.

Trace semantics. In this paper we are further interested in (finite) trace semantics, which also happens to be a final coalgebra semantics, only in a different category. Coalgebraic (finite) trace semantics has been developed for coalgebras of the form $X \to TF(X)$ where T is a suitable monad and F a suitable functor, see [HJS07]. Essential for coalgebraic trace semantics is the Kleisli category of a monad. A monad (T, η, μ), which we will frequently denote by T, on **Sets** consists of an endofunctor T on **Sets** and two natural transformations, the unit $\eta\colon id \Rightarrow T$ and the multiplication $\mu\colon TT \Rightarrow T$, that is, functions $\eta_X{:}X \to T(X)$ and $\mu_X\colon TT(X) \to T(X)$ for each set X satisfying a naturality condition. The unit and multiplication satisfy the compatibility conditions $\mu_X \circ \eta_{TX} = \mu_X \circ T\eta_X = id \quad$ and $\mu_X \circ T\mu_X = \mu_X \circ \mu_{TX}$.

The monad structures provide a perfect way of modelling "branching". Intuitively, the unit η embeds a non-branching behavior as a trivial branching (with a single branch) whereas the multiplication μ "flattens" two successive branchings into one branching, abstracting away internal branchings.

An example of a monad is the powerset monad $\mathcal{P}$ with unit given by singleton, and multiplication given by union. Here, the "flattening"-of-a-"branching" metaphore is obvious, as pictured below.



A monad T on **Sets** allows for a definition of a Kleisli category $\mathcal{K}\ell(T)$ whose objects are sets, and a morphism $f\colon X \mathrel{\multimap\!\!\!\!\!\to} Y$ is a function $f\colon X \to TY$. The identity morphism on X is η_X, and composition of morphisms is defined as

$$f \bullet g = \mu \circ Tf \circ g = \left(X \xrightarrow{g} TY \xrightarrow{Tf} TTZ \xrightarrow{\mu} TZ \right).$$

There is a canonical lifting functor $J\colon \mathbf{Sets} \to \mathcal{K}\ell(T)$ which is the identity on objects, and maps a function $f\colon X \to Y$ to the function $J(f) = \eta \circ f\colon X \to TY$.

The coalgebraic trace result of [HJS07] applies to TF-coalgebras in **Sets** if T and F satisfy a number requirements:

- There exists a distributive law $\lambda\colon FT \Rightarrow TF$. As a consequence, F lifts to a functor $\overline{F}$ on $\mathcal{K}\ell(T)$, with $\overline{F}(X) = F(X)$ and for a Kleisli arrow $f\colon X \mathrel{\multimap\!\!\!\!\!\to} Y$, i.e., a map $f\colon X \to TY$, $\overline{F}(f) = \lambda \circ F(f)$. Hence TF-coalgebras in **Sets** are $\overline{F}$-coalgebras in $\mathcal{K}\ell(T)$.
- The Kleisli category $\mathcal{K}\ell(T)$ is suitably order-enriched, with order $\sqsubseteq$ on Kleisli homsets, bottom element $\perp$ and suprema of directed subsets.
- The lifting $\overline{F}\colon \mathcal{K}\ell(T) \to \mathcal{K}\ell(T)$ is locally monotone.

The requirements are explained in detail in [HJS07]. The main result of the generic trace theory [HJS07] is:

> If T and F satisfy the requirements of the generic trace theory and there exists an initial F-algebra $\iota\colon F(I) \xrightarrow{\cong} I$ in **Sets**, then the lifted coalgebra $J(\iota^{-1}) = \eta \circ \iota^{-1}\colon I \to TF(I)$ is final $\overline{F}$-coalgebra in $\mathcal{K}\ell(T)$.

This enables defining trace semantics for TF-coalgebras in **Sets** as the final coalgebra semantics for $\overline{F}$-coalgebras in $\mathcal{K}\ell(T)$. More precisely, for a coalgebra $\alpha\colon X \to TFX$ in **Sets**, i.e., $\alpha\colon X \mathrel{\multimap\!\!\!\!\!\to} \overline{F}Y$ in $\mathcal{K}\ell(T)$, we denote by tr_α the final coalgebra map in $\mathcal{K}\ell(T)$, called the trace map. The trace of a state $x \in X$ is given by the image $\mathrm{tr}_\alpha(x)$. Trace equivalence is defined by $x \sim_{\mathrm{tr}} y \Leftrightarrow \mathrm{tr}_\alpha(x) = \mathrm{tr}_\alpha(y)$.

The requirements of the generic trace theory hold for the powerset monad $\mathcal{P}$, the subdistribution monad $\mathcal{D}$, and the lift monad $1 + id$, together with the inductively defined class of all "shapely functors" [HJS07].

Slightly abusing the notation for sake of simplicity, throughout the paper we will denote the lifted functor $\overline{F}$ by F as well.

3 Probabilistic transition systems and their traces

In this paper, we consider generative probabilistic transition systems [vGSS95] with explicit termination. They are modeled as TF coalgebras of the subdistribution monad $\mathcal{D}_\omega$ and the linear-behavior functor $F = 1 + A \times id$ where A is a set of labels and $1 = \{*\}$ is a singleton set, used to model termination.

The monad $\mathcal{D}_\omega$ assigns to a set X the set

$$\mathcal{D}_\omega(X) = \{\varphi \in [0,1]^X \mid \varphi \text{ has finite support and } \sum_{x \in \mathrm{supp}(\varphi)} \varphi(x) \leqslant 1\}$$

and to a function $f\colon X \to Y$, the function $\mathcal{D}_\omega(f)\colon \mathcal{D}_\omega(X) \to \mathcal{D}_\omega(Y)$:

$$\mathcal{D}_\omega(f)(\varphi) = \lambda y. \sum_{x \in f^{-1}(\{y\})} \varphi(x).$$

The unit of $\mathcal{D}_\omega$ is given by $\eta_X(x) = (x \mapsto 1)$ and the multiplication by

$$\mu(\Phi)(x) = \sum_{\varphi \in \mathcal{D}_\omega(X)} \Phi(\varphi) \cdot \varphi(x), \qquad \Phi \in \mathcal{D}_\omega\mathcal{D}_\omega(X)$$

Hence, our probabilistic transition systems are $\mathcal{D}_\omega(1 + A \times \mathit{id})$-coalgebras on **Sets**. The finite support requirement ensures finite branching and is necessary for representing probabilistic transition systems by finite expressions. The functor $1 + A \times \mathit{id}$ provides linear behavior, in which a state can either successfully terminate or make a labelled transition to another state. The monad $\mathcal{D}_\omega$ provides probabilistic branching.

Given a probabilistic transition system $\alpha\colon\ X \to \mathcal{D}_\omega(1 + A \times X)$ we write

$$x \xrightarrow{p} * \quad \text{if} \quad \alpha(x)(*) = p,$$

i.e., x successfully terminates with probability p, and

$$x \xrightarrow{a,p} y \quad \text{if} \quad \alpha(x)(a, y) = p,$$

i.e., if x can make an a-labelled step to y with weight p. Here, and throughout the paper, without any risk of confusion, we are omitting the coproduct injections when representing elements of $1 + A \times X$.

The monad $\mathcal{D}_\omega$ is not suitable for describing traces. The reason (intuitively) is that a trace of a state is a distribution over words. Even if the system is defined with finitely-supported distributions only, the trace will in general not have finite support. For example, consider the finite probabilistic transition system

$$\begin{tikzcd} x \arrow[loop above, "a{,}\frac{1}{2}"] \arrow[r, "\frac{1}{2}"] & * \end{tikzcd}.$$

The trace of state x is the distribution that assigns probability $\frac{1}{2^{n+1}}$ to the word a^n for all $n \in \mathbb{N}$ and hence has infinite support. In terms of the generic trace theory requirements, $\mathcal{D}_\omega$ fails to satisfy the requirement of existence of suprema of directed subsets.

However, the requirements of the general trace theory do hold for the monad $\mathcal{D}$ which is defined as $\mathcal{D}_\omega$ by dropping the finite support condition. We will apply the generic trace results by using the natural injection $i\colon \mathcal{D}_\omega(X) \to \mathcal{D}(X)$. The conditions for applicability of the generic trace results hold for the functor $F = 1 + A \times id$.

In particular, we need to include explicit termination since the initial algebra of the functor $A \times id$ is trivial. As a result, we can only deal with (finite) terminating traces. In case of LTS, this is no restriction: one can add the possibility to explicitly terminate to each state of an LTS, and so the finite terminating traces of this transformed LTS are all finite traces of the original one. With probabilities, this is not the case: if in a state the probability to terminate is zero and the sum of the probabilities to make a step is one, then there is no place for adding termination. Nevertheless, (finite) terminating traces are of sufficient interest and have been studied under the name completed-trace semantics in process theory.

For completeness, we mention the distributive law $\lambda\colon 1 + A \times \mathcal{D} \Rightarrow \mathcal{D}(1 + A \times id)$ that enables the lifting of F to $\mathcal{K}\ell(\mathcal{D})$. It is is defined by $\lambda_X(*) = \eta(*)$ and $\lambda_X(a, \xi) = \lambda(a, x).\xi(x)$ for $\xi \in \mathcal{D}(X)$.

It seems possible, but requires significant additional work, to extend the results presented here to an inductively defined class of so-called shapely functors (cf. [HJS07]).

The final $1 + A \times id$-coalgebra in $\mathcal{K}\ell(\mathcal{D})$ is $\eta \circ \iota\colon A^* \longrightarrow \mathcal{D}(1 + A \times A^*)$ with $\iota\colon A^* \xrightarrow{\cong} 1 + A \times A^*$ being the (inverse of the) initial algebra isomorphism, given by $\iota(\varepsilon) = *$ and $\iota(aw) = (a, w)$.

The trace map, for a coalgebra $X \xrightarrow{\alpha} \mathcal{D}_\omega(1 + A \times X)$, is defined by applying the generic trace theory to the coalgebra $X \xrightarrow{\alpha} \mathcal{D}_\omega(1 + A \times X) \xrightarrow{i} \mathcal{D}(1 + A \times X)$, as we depict on the right, and can be instantiated to the concrete definition:

$$
\begin{aligned}
\mathrm{tr}(x)(\varepsilon) &= p, \quad \text{if } x \xrightarrow{p} * \\
\mathrm{tr}(x)(aw) &= \textstyle\sum_{x \xrightarrow{a,p} y} p \cdot \mathrm{tr}(y)(w).
\end{aligned}
\qquad
\begin{tikzcd}
X \arrow[r, "tr"] \arrow[d, "i \circ \alpha"'] & A^* \arrow[d, "\eta \circ \iota"] \\
1 + A \times X \arrow[r] & 1 + A \times A^*
\end{tikzcd}
$$

In the diagram above the black dot on the arrows indicates Kleisli arrows and therefore the composition is Kleisli composition.

The coalgebraic trace definition provides a natural (terminating, finite) trace distribution of a state in a probabilistic transition system. We note that this trace distribution is different than the (possibly infinite) trace distribution (without explicit termination) [Seg95] which is a probability measure over a σ-algebra generated by so-called cones. We are not aware of a possibility to deal with such trace semantics coalgebraically.

We note that, as expected, (coalgebraic) bisimilarity implies (coalgebraic) trace equivalence, i.e., $x \sim y \Rightarrow x \sim_{\mathrm{tr}} y$.

4 Syntax

In this section, we introduce the syntax of the specification language for which we will introduce a sound and complete axiomatization of trace semantics. The language is an instance of the framework introduced in [SBBR10b], where uniform sound and complete calculi for bisimilarity were introduced. We illustrate the definitions of this section with examples that we shall use in the subsequent sections and which capture key differences between bisimilarity and trace.

Definition 4.1 [Expressions for probabilistic transition systems] Given a set of input actions A and a set of fixed-point variables X, the set Exp of expressions for quantitative transition systems is given by the closed expressions contained in the following BNF, for $a \in A$ and $x \in X$:

$$\begin{aligned}
\mathsf{E} &::= \bigoplus_{i \in I} p_i \cdot \mathsf{F}_i \mid \mu x.\mathsf{E}^g \mid x && (p_i \in [0,1], \sum_{i \in I} p_i \leqslant 1)\\
\mathsf{E}^g &::= \bigoplus_{i \in I} p_i \cdot \mathsf{F}_i \mid \mu x.\mathsf{E}^g && (p_i \in [0,1], \sum_{i \in I} p_i \leqslant 1)\\
\mathsf{F}_i &::= * \mid a \cdot \mathsf{E}
\end{aligned}$$

The operator μ in the expression $\mu x.\mathsf{E}^g$ functions as a binder for all the occurrences of the variable x in E^g. Note that the only difference between E^g and E is the occurrence of x (E^g is an expression where x occurs *guarded*, that is only inside an expression of the shape $p \cdot a \cdot -$). An expression E is *closed* if all variables $x \in X$ occurring in E are bound.

Intuitively, an expression $\bigoplus_{i \in I} p_i \cdot \mathsf{F}_i$ behaves as the expression F_i with probability p_i, and μ-expressions are used to represent loops: a μ-expression behaves the same as its unfolding. We make this precise by providing the set of expressions with a coalgebraic structure.

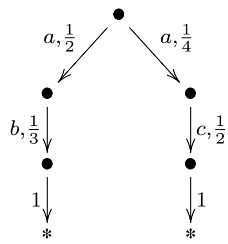
We define $c \colon \mathsf{Exp} \to \mathcal{D}_\omega(1 + A \times \mathsf{Exp})$ by induction on the number of nested fixed-points as follows:

$$\begin{aligned}
c(\bigoplus_{i \in I} p_i \cdot \mathsf{F}_i)(*) &= \sum_{i\colon \mathsf{F}_i = *} p_i\\
c(\bigoplus_{i \in I} p_i \cdot \mathsf{F}_i)(a, \mathsf{E}) &= \sum_{i\colon \mathsf{F}_i = a \cdot \mathsf{E}} p_i\\
c(\mu x.\mathsf{E}^g) &= c(\mathsf{E}^g[\mu x.\mathsf{E}^g / x])
\end{aligned}$$

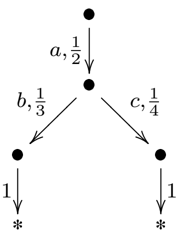
Having a coalgebra structure on the set of expressions has two advantages: it provides immediately a natural semantics, using the unique homomorphism into the final coalgebra (which can be thought of as the universe of behaviors), and it enables to define when a state s of a probabilistic transition system and an expression E are bisimilar, $s \sim \mathsf{E}$, or trace equivalent, $s \sim_{\mathsf{tr}} \mathsf{E}$.

Example 4.2 [Some specifications and corresponding systems] To give an intuition for the type of systems each expression specifies we present below a few examples of expressions and equivalent systems (more precisely, the top state of each system is bisimilar to the expression).

(1)

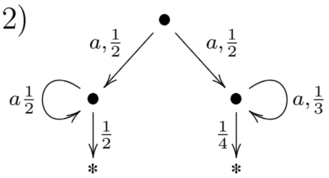


$\frac{1}{2} \cdot a \cdot \frac{1}{3} \cdot b \cdot 1 \cdot * \oplus \frac{1}{4} \cdot a \cdot \frac{1}{2} \cdot c \cdot 1 \cdot *$

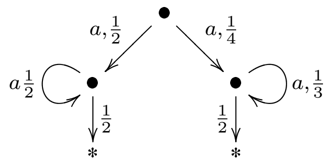


$\frac{1}{2} \cdot a \cdot \left(\frac{1}{3} \cdot b \cdot 1 \cdot * \oplus \frac{1}{4} \cdot c \cdot 1 \cdot *\right)$

(2)



$$\frac{1}{2} \cdot a \cdot \mu x. \left(\frac{1}{2} \cdot a \cdot x \oplus \frac{1}{2} \cdot *\right)$$
$$\oplus \frac{1}{2} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right)$$



$$\frac{1}{2} \cdot a \cdot \mu x. \left(\frac{1}{2} \cdot a \cdot x \oplus \frac{1}{2} \cdot *\right)$$
$$\oplus \frac{1}{4} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{2} \cdot *\right)$$

The systems on the right and on the left in each row are trace equivalent. However, they are not bisimilar and, therefore, each pair of expressions in each row would not be provably equivalent using the axiomatization of [SBBR10b]. We will show later how to syntactically prove the trace equivalence of the expressions, making use of the axiomatization we will introduce for trace semantics.

Theorem 4.3 (Kleene's theorem for trace) *For every expression* $\mathsf{E} \in \mathsf{Exp}$ *there exists a (finite) probabilistic transition system* (S, α) *and* $s \in S$ *such that* $\mathsf{E} \sim_{\mathsf{tr}} s$*. Conversely, for every locally finite probabilistic transition system* (S, α) *and* $s \in S$ *there exists an expression* $\mathsf{E} \in \mathsf{Exp}$ *such that* $s \sim_{\mathsf{tr}} \mathsf{E}$.

Proof. Direct consequence from the similar theorem for bisimilarity [SBBR10b, Theorem 4.9] and the fact that bisimilarity implies trace equivalence. $\square$

In the formulation of Kleene's theorem we use *locally finite* probabilistic systems. These are probabilistic systems in which from each state only finitely many states are reachable (coalgebraically, this means that the subcoalgebra generated by each state is finite).

5 Sound and complete axiomatization for trace

In this section, we present an equational system to reason about probabilistic expressions. We will prove it sound and complete with respect to trace semantics.

For sake of simplicity, in what follows we first introduce a nulary operation $\underline{\varnothing}$ (denoting the empty $\bigoplus$-sum) and two partial operations on expressions: a binary sum $\mathsf{E} \oplus \mathsf{E}'$, and a unary scalar product $p\mathsf{E}$ for a non-negative real number p, and write the axioms with help of these auxiliary operations. They are defined as follows:

The binary sum $\mathsf{E} \oplus \mathsf{E}'$ is defined if and only if $\mathsf{E} = \bigoplus_{i\in I} p_i \cdot \mathsf{F}_i$, $\mathsf{E}' = \bigoplus_{j\in J} q_j \cdot \mathsf{F}'_j$, and $\sum_{i\in I} p_i + \sum_{j\in J} q_j \leqslant 1$, in which case it equals (as expected) the expression $\bigoplus_{k\in I+J} r_k \cdot \mathsf{F}''_k$ with $r_k = p_i, \mathsf{F}''_k = \mathsf{F}_i$ for $k = i \in I$ and $r_k = q_j, \mathsf{F}''_k = \mathsf{F}'_j$ for $k = j \in J$. Clearly, we then have $\bigoplus_{i\in I} p_i \cdot \mathsf{F}_i = (p_1 \cdot \mathsf{F}_1 \oplus (p_2 \cdot \mathsf{F}_2 \oplus (\cdots))$

Given a non-negative real number p, the scalar product $p\mathsf{E}$ is defined if and only if $\mathsf{E} = \bigoplus_{i\in I} p_i \cdot \mathsf{F}_i$, $\sum_{i\in I} pp_i \leqslant 1$, in which case it equals $\bigoplus_{i\in I} pp_i \cdot \mathsf{F}_i$.

In what follows, we present an axiom system for probabilistic expressions using the binary sum, the zero expression, and the scalar product. An axiom $\mathsf{E}_1 \equiv \mathsf{E}_2$ is to be understood as: if *both* E_1 and E_2 are well-defined expressions, then they are equivalent with respect to $\equiv$.

Let the relation $\equiv \subseteq \mathsf{Exp} \times \mathsf{Exp}$, written infix-style, be the least equivalence relation satisfying the axioms (and implication rules) from Figure 1. From the axioms, only the last two are related to traces. The subset of the axioms in Figure 1 excluding the last two is sound and complete w.r.t. bisimilarity, as it was shown in [SBBR10b].

Example 5.1 We now show some examples of the derivation of trace equivalence of two expressions. The expressions we consider in this example already appeared in Example 4.2 (1) and (2), together with equivalent transition systems. We start by showing that the expressions from Example 4.2 (1) are $\equiv$-equivalent, i.e.,

$$\left(\frac{1}{2}\cdot a\cdot\frac{1}{3}\cdot b\cdot 1\cdot *\right)\oplus\left(\frac{1}{4}\cdot a\cdot\frac{1}{2}\cdot c\cdot 1\cdot *\right)\equiv\frac{1}{2}\cdot a\cdot\left(\frac{1}{3}\cdot b\cdot 1\cdot *\oplus\frac{1}{4}\cdot c\cdot 1\cdot *\right).$$

First, we observe that $\frac{1}{4}\cdot a\cdot\frac{1}{2}\cdot c\cdot 1\cdot * \stackrel{(M)}{\equiv} \frac{1}{2}\cdot a\cdot\frac{1}{4}\cdot c\cdot 1\cdot *$. Then,

$$\begin{aligned}\left(\frac{1}{2}\cdot a\cdot\frac{1}{3}\cdot b\cdot 1\cdot *\right)\oplus\left(\frac{1}{4}\cdot a\cdot\frac{1}{2}\cdot c\cdot 1\cdot *\right) &\stackrel{(Cong)}{\equiv} \left(\frac{1}{2}\cdot a\cdot\frac{1}{3}\cdot b\cdot 1\cdot *\right)\oplus\left(\frac{1}{2}\cdot a\cdot\frac{1}{4}\cdot c\cdot 1\cdot *\right)\\ &\stackrel{(D)}{\equiv} \frac{1}{2}\cdot a\cdot\left(\frac{1}{3}\cdot b\cdot 1\cdot *\oplus\frac{1}{4}\cdot c\cdot 1\cdot *\right).\end{aligned}$$

$$
\begin{array}{llll}
\mathsf{E}_1 \oplus (\mathsf{E}_2 \oplus \mathsf{E}_3) & \equiv & (\mathsf{E}_1 \oplus \mathsf{E}_2) \oplus \mathsf{E}_3 & (A) \\
\mathsf{E}_1 \oplus \mathsf{E}_2 & \equiv & \mathsf{E}_2 \oplus \mathsf{E}_1 & (C) \\
\mathsf{E} \oplus \underline{\emptyset} & \equiv & \mathsf{E} & (E) \\
\mu x.\mathsf{E} & \equiv & \mathsf{E}[\mu x.\mathsf{E}/x] & (FP) \\
\gamma[\mathsf{E}/x] \equiv \mathsf{E} & \Rightarrow & \mu x.\gamma \equiv \mathsf{E} & (UFP) \\
\mu x.\mathsf{E} & \equiv & \mu y.\mathsf{E}[y/x] \;\text{ if } y \text{ is not free in } \mathsf{E} & (\alpha - equiv) \\
\mathsf{E}_1 \equiv \mathsf{E}_2 & \Rightarrow & \mathsf{E}[\mathsf{E}_1/x] \equiv \mathsf{E}[\mathsf{E}_2/x] & (Cong) \\
0 \cdot \mathsf{E} & \equiv & \underline{\emptyset} & (Z) \\
p \cdot \mathsf{E} \oplus p' \cdot \mathsf{E} & \equiv & (p + p') \cdot \mathsf{E} & (S) \\
 & & & \\
p \cdot a \cdot \mathsf{E} & \equiv & (pq) \cdot a \cdot \frac{1}{q}\mathsf{E} & (M) \\
p \cdot a \cdot \mathsf{E}_1 \oplus p \cdot a \cdot \mathsf{E}_2 & \equiv & p \cdot a \cdot (\mathsf{E}_1 \oplus \mathsf{E}_2) & (D)
\end{array}
$$

Fig. 1. Axioms for trace semantics

A more interesting example is provided by the expressions from Example 4.2 (2). The proof of equivalence of these expressions requires the use of the (UFP) rule. We first start by observing that the left side of the sum in each expression is the same. Thus, using $(Cong)$, it suffices to prove that

$$\frac{1}{2} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right) \equiv \frac{1}{4} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{2} \cdot *\right)$$

In what follows let E stand for the expression $\mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{2} \cdot *\right)$

$$
\begin{array}{ll}
\ \frac{1}{2} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right) \equiv \frac{1}{4} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{2} \cdot *\right) & \\
\Leftrightarrow \frac{1}{2} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right) \equiv \frac{1}{4} \cdot a \cdot \left(\frac{1}{3} \cdot a \cdot \mathsf{E} \oplus \frac{1}{2} \cdot *\right) & (Cong) \text{ and } (FP) \\
\Leftrightarrow \frac{1}{2} \cdot a \cdot \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right) \equiv \frac{1}{2} \cdot a \cdot \left(\frac{1}{6} \cdot a \cdot \mathsf{E} \oplus \frac{1}{4} \cdot *\right) & (M) \\
\Leftrightarrow \mu y. \left(\frac{1}{3} \cdot a \cdot y \oplus \frac{1}{4} \cdot *\right) \equiv \frac{1}{6} \cdot a \cdot \mathsf{E} \oplus \frac{1}{4} \cdot * & (Cong)
\end{array}
$$

	Soundness		Completeness
	$\mathsf{E}_1 \equiv \mathsf{E}_2$		$\mathsf{E}_1 \sim_{\mathsf{tr}} \mathsf{E}_2$
$\Leftrightarrow$	$[\mathsf{E}_1] = [\mathsf{E}_2]$	$\Leftrightarrow$	$\mathrm{tr}(\mathsf{E}_1) = tr(\mathsf{E}_2)$
$\overset{(*)}{\Rightarrow}$	$out_{\equiv}([\mathsf{E}_1]) = out_{\equiv}([\mathsf{E}_2])$	$\overset{(\triangle)}{\Leftrightarrow}$	$out_{\equiv}([\mathsf{E}_1]) = out_{\equiv}([\mathsf{E}_2])$
$\overset{(\triangle)}{\Leftrightarrow}$	$tr(\mathsf{E}_1) = tr(\mathsf{E}_2)$	$\overset{(\heartsuit)}{\Rightarrow}$	$[\mathsf{E}_1] = [\mathsf{E}_2]$
$\Leftrightarrow$	$\mathsf{E}_1 \sim_{\mathsf{tr}} \mathsf{E}_2$	$\Leftrightarrow$	$\mathsf{E}_1 \equiv \mathsf{E}_2$

Fig. 2. Soundness and completeness. $(*)$: existence of $out_{\equiv}$, $(\triangle)$: $out_{\equiv} \circ [-] = tr$, $(\heartsuit)$: $out_{\equiv}$ is injective.

$$\begin{aligned}
&\Leftarrow \tfrac{1}{3} \cdot a \cdot \left(\tfrac{1}{6} \cdot a \cdot \mathsf{E} \oplus \tfrac{1}{4} \cdot *\right) \oplus \tfrac{1}{4} \cdot * \equiv \tfrac{1}{6} \cdot a \cdot \mathsf{E} \oplus \tfrac{1}{4} \cdot * && (\mathit{UFP})\\
&\Leftrightarrow \tfrac{1}{3} \cdot a \cdot \left(\tfrac{1}{6} \cdot a \cdot \mathsf{E} \oplus \tfrac{1}{4} \cdot *\right) \equiv \tfrac{1}{6} \cdot a \cdot \mathsf{E} && (\mathit{Cong})\\
&\Leftrightarrow \tfrac{1}{6} \cdot a \cdot \left(\tfrac{1}{3} \cdot a \cdot \mathsf{E} \oplus \tfrac{1}{2} \cdot *\right) \equiv \tfrac{1}{6} \cdot a \cdot \mathsf{E} && (M)\\
&\Leftrightarrow \mathsf{E} \equiv \mathsf{E} && (\mathit{Cong}) \text{ and } (\mathit{FP})
\end{aligned}$$

In the next sections, we will show that the axiomatization, obtained from the sound and complete axiomatization for bisimilarity by adding two new axioms, is sound and complete with respect to trace semantics. This is the main technical result of the paper and, despite the simplicity of the axioms, proving that they are enough to achieve completeness is not a trivial task. Before we provide the technical details of the proof, let us present the intuitive idea behind it.

5.1 *Soundness and completeness: An overview*

We want to show that the axiomatization above is sound and complete with respect to trace semantics. That is,

$$\mathsf{E}_1 \sim_{\mathsf{tr}} \mathsf{E}_2 \Leftrightarrow \mathsf{E}_1 \equiv \mathsf{E}_2$$

Our strategy is to show that the trace map tr is equal to a composition of two maps $out_{\equiv} \circ [-]$, where $out_{\equiv}$ is an injective map, which we will define below, and $[-]$ is the canonical map mapping each expression to its $\equiv$-class. Having this, soundness and completeness follow easily, as shown in Figure 2.

We proceed as follows: in Section 5.2 we discuss determinization of probabilistic transition systems, define $out_{\equiv}$ and show that $out_{\equiv} \circ [-]$ is a Kleisli homomorphism from $(\mathsf{Exp}, i \circ c)$ to the final $(A^*, \eta \circ \iota)$, which by finality yields $out_{\equiv} \circ [-] = tr$ and soundness follows; in Section 5.3, we show that $out_{\equiv}$ is an injective map, which will have as consequence completeness.

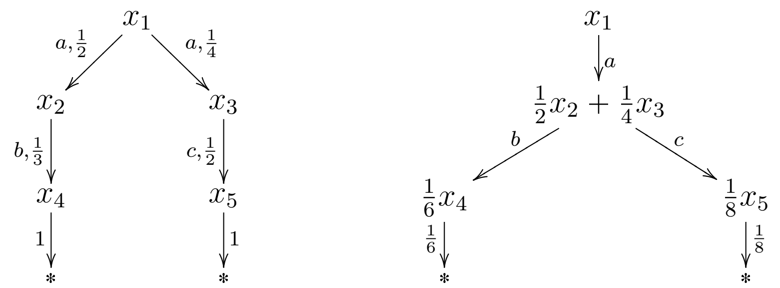
5.2 A way out: Determinization of probabilistic transition systems

The determinization of a probabilistic transition system

$$\alpha \colon X \to \mathcal{D}_\omega(1 + A \times X)$$

is a "deterministic" system of type $G = [0,1] \times id^A$ and state space $\mathcal{D}_\omega(X)$. The idea is that in the determinization, states are uncertain, i.e., we only know that with a given probability the system is in one of the original states.

We start by an example of such determinization: the automaton on the right is part of the determinization of the one on the left. In general, the determinization yields an infinite automaton. In this example, we show the accessible part when starting from the state $\eta(x_1)$, the Dirac distribution of x_1, and we denote the distributions by formal sums.



The actual definition of the determinization is as follows. Given a probabilistic transition system $\alpha \colon X \to \mathcal{D}_\omega(1 + A \times X)$ its determinization is the system $\overline{\alpha} \colon \mathcal{D}_\omega(X) \to [0,1] \times (\mathcal{D}_\omega(X))^A$ defined by

$$\overline{\alpha}(\xi) = \langle \sum_{x \in X} \xi(x) \cdot \alpha(x)(*), \lambda a.\lambda x'. \sum_{x \in X} \xi(x) \cdot \alpha(x)(a, x') \rangle$$

for a distribution $\xi \in \mathcal{D}_\omega(X)$.

A state y in a coalgebra $\beta \colon Y \to [0,1] \times Y^A$ of type G, with $\beta(y) = \langle p, f \rangle$, either terminates with probability p or given a label a it transits to a unique next state $f(a)$. Moreover, for any such deterministic coalgebra $\beta \colon Y \to [0,1] \times Y^A$ of type G, there is a canonical map $out_\beta \colon Y \to [0,1]^{A^*}$ given by

$$out_\beta(y)(\varepsilon) = p, \qquad out_\beta(y)(aw) = out_\beta(f(a))(w).$$

In the example above, $out(\eta(x_1))(ab) = \frac{1}{6}$ and $out(\frac{1}{2}x_2 + \frac{1}{4}x_3)(c) = \frac{1}{8}$.

The map out_β is actually the unique homomorphism from β into the final G-coalgebra. The final G-coalgebra is $([0,1]^{A^*}, \langle \varepsilon?, (-)_a \rangle)$ where for a map $\xi \colon A^* \to [0,1]$, we have $\varepsilon?(\xi) = \xi(\varepsilon)$ and $(\xi)_a = \lambda a.\lambda w.\xi(aw)$. Hence, the following diagram commutes.

$$\begin{tikzcd} Y \arrow[r, dashed, "out_\beta"] \arrow[d, "\beta"'] & {[0,1]^{A^*}} \arrow[d, "\langle \varepsilon?, (-)_a \rangle"] \\ {[0,1] \times Y^A} \arrow[r, dashed, "id \times out_\beta^A"] & {[0,1] \times ([0,1]^{A^*})^A} \end{tikzcd}$$

The concrete definition of a determinization can be structured in the following way. We observe that there is an injective natural transformation $\delta\colon \mathcal{D}_\omega(1 + A \times X) \to [0,1] \times \mathcal{D}_\omega(X)^A$, given by $\delta(\xi) = \langle \xi(*), \lambda a.\lambda x.\xi(a,x) \rangle$. The determinization map satisfies $\overline{\alpha} = \delta \circ \mu \circ \mathcal{D}_\omega \alpha$ and makes the following diagram commute

$$\begin{tikzcd} X \arrow[r, "\eta_X"] \arrow[d, "\alpha"'] & \mathcal{D}_\omega(X) \arrow[ddl, "\overline{\alpha}"] \\ \mathcal{D}_\omega(1 + A \times X) \arrow[d, "\delta"'] & \\ {[0,1] \times \mathcal{D}_\omega(X)^A.} & \end{tikzcd}$$

To summarize, the situation is shown in the following diagram:

$$\begin{tikzcd} X \arrow[r, "\eta_X"] \arrow[d, "\alpha"'] & \mathcal{D}_\omega(X) \arrow[r, dashed, "out"] \arrow[ddl, "\overline{\alpha}"] & {[0,1]^{A^*}} \arrow[dd, "\langle \varepsilon?, (-)_a \rangle"] \\ \mathcal{D}_\omega(1 + A \times X) \arrow[d, "\delta"'] & & \\ {[0,1] \times \mathcal{D}_\omega(X)^A} \arrow[rr, dashed, "id \times out^A"] & & {[0,1] \times ([0,1]^{A^*})^A} \end{tikzcd}$$

More generally, this fits into the generalized powerset construction [SBBR10a]. The generalized powerset construction can be applied to a coalgebra of type HT, for T a monad and H a functor with a T-algebra lifting ($HT(X)$ has a T-algebra structure h), or equivalently, for H such that there is a distributive law $\pi\colon TH \to HT$. Given a coalgebra $\gamma\colon X \to HTX$, where H and T satisfy the above conditions, the coalgebra $\gamma^\sharp\colon TX \to HTX$ obtained by applying the generalized powerset construction to γ is defined as $\gamma^\sharp = h \circ T\gamma = H\mu \circ \pi \circ T\gamma$. It can be thought of as a determinization of γ in the sense that any side effects modeled by the monad T will now be buried in the state space of the new coalgebra. Taking T to be the powerset monad and $H = 2 \times (-)^A$, the functor defining the type of deterministic automata, one obtains the usual powerset construction, which allows to define a deterministic automaton language-equivalent to a given non-deterministic automaton. The construction is applicable to $T = \mathcal{D}_\omega$ and $H = G$, since $G\mathcal{D}_\omega(X)$ has a $\mathcal{D}_\omega$-algebra structure, leading $(\delta \circ \alpha)^\sharp = \overline{\alpha}$.

Remark 5.2 There seems to be a relationship between the functor G and the functor F, that may shed light on how to extend the current work to other functors in place of F, e.g. shapely functors. Given a functor H that is inductively built from the identity functor, constant functors, finite products and coproducts (or even if infinite coproducts in which case H can be any shapely functor), we can define a corresponding functor G_H as follows: $G_{id} = id$, $G_A = \mathcal{D}_\omega(A)$, $G_{H_1+H_2} = G_{H_1} \times G_{H_2}$ and $G_{H_1 \times H_2} = (G_{H_2})^{H_1}$. Note that in our particular example $F = 1 + A \times -$ and $G_F = G = [0,1] \times (-)^A$, where $[0,1] = \mathcal{D}_\omega(1)$. Such a functor G_H may be useful to determinize $\mathcal{D}_\omega H$-coalgebras, and a corresponding natural transformation $\delta_H \colon \mathcal{D}_\omega H \Rightarrow G_H \mathcal{D}_\omega$ could also be inductively defined. The details of this generalization remain future work. In addition, the definition of expressions should change accordingly (the F-type expressions) and the trace semantics needs to be instantiated to such functors H in order to gain understanding of the situation.

We now need to formally connect the semantics given by *out* and the trace semantics given by tr. The first observation is the following.

Lemma 5.3 *Starting from a coalgebra $X \xrightarrow{\alpha} \mathcal{D}_\omega(1 + A \times X)$, the image of the map out, as depicted in the commuting diagram below, is in $\mathcal{D}(A^*)$.*

$$\begin{tikzcd}
X \arrow[r, "\eta_X"] \arrow[d, "\alpha"'] & \mathcal{D}_\omega(X) \arrow[r, dashed, "out"] \arrow[ddl, "\overline{\alpha}"] & \mathcal{D}(A^*) \arrow[r, tail] \arrow[d, "\mathcal{D}\iota"] & {[0,1]^{A^*}} \arrow[dd, "\langle \varepsilon?, (-)_a \rangle"] \\
\mathcal{D}_\omega(1 + A \times X) \arrow[d, "\delta"'] & & \mathcal{D}(1 + A \times A^*) \arrow[d, "\delta"'] & \\
{[0,1] \times \mathcal{D}_\omega(X)^A} \arrow[rr, dashed, "id \times out^A"] & & {[0,1] \times (\mathcal{D}(A^*))^A} \arrow[r, tail] & {[0,1] \times ([0,1]^{A^*})^A}
\end{tikzcd}$$

Remark 5.4 A consequence of our further results, which we can also show independently, is that $out \circ \eta = tr$, which is also expected from the definition of *out* and the determinization. This is in itself a very interesting result since it shows that coalgebraic traces can be recovered via determinization. However, for the axiomatization we need another map $out_{\equiv}$ and its connection to coalgebraic traces.

Our goal in the remainder of this section is to define $out_{\equiv}$ and show that $out_{\equiv} \circ [-]$ is a Kleisli homomorphism from $(\mathsf{Exp}, i \circ c)$ to the final F-coalgebra in $\mathcal{K}\ell(\mathcal{D})$, $(A^*, \eta \circ \iota)$.

Let us start with summarizing in a diagram some of the maps we are dealing with:

$$\begin{tikzcd}
\mathsf{Exp} \arrow[r, "{[-]_\sim}"] \arrow[d, "c"'] \arrow[rr, bend left, two heads, "{[-]}"] & \mathsf{Exp}/_\sim \arrow[r, two heads, "{[-]_\equiv}"] \arrow[d, "c_0"'] & \mathsf{Exp}/_\equiv \\
\mathcal{D}_\omega(1 + A \times \mathsf{Exp}) \arrow[r, "\mathcal{D}_\omega(1 + A \times [-]_\sim)"] & \mathcal{D}_\omega(1 + A \times \mathsf{Exp}/_\sim) &
\end{tikzcd}$$

Here, $[-]_\sim$ denotes the surjective equivalence map which quotients only using the axioms for bisimilarity (all axioms except (M) and (D)), and $[-]_\equiv$ quotients with the axioms (M) and (D). The commutativity of the square above was proved in [SBBR10b], and had as consequence the soundness of the axioms w.r.t. bisimilarity. We know, however, that we cannot fill the diagram on the right side in the same way, that is, $\mathsf{Exp}/_\equiv$ will never have a coalgebra structure making $[-]_\equiv$ a coalgebra homomorphism. Hence, we will take a different approach, inspired by [Mil10,BMS11].

From now on *positive convex structures* [Dob06,Dob08] play an important role in our work. They are the Eilenberg-Moore algebras of the monad $\mathcal{D}_\omega$ [Dob08]. In concrete terms, a positive convex structure is an algebra with a finite convex sum operation $\boxplus_{i\in I} p_i x_i$ for $p_i \in [0,1]$ and $\sum_{i\in I} p_i \leqslant 1$, satisfying the axioms:

$$
\begin{array}{ll}
(i) & \boxplus_{i\in I} p_{i,k} x_i = x_k \qquad \text{if } p_{i,k} = 1 \text{ for } i = k \text{ and } p_{i,k} = 0 \text{ otherwise} \\
(ii) & \boxplus_{i\in I} p_i \left(\boxplus_{j\in J} q_{i,j} x_{i,j} \right) = \boxplus_{j\in J} \left(\sum_{i\in I} p_i q_{i,j} \right) x_j .
\end{array}
$$

Given a positive convex structure $\boxplus$ on a set X, it provides a $\mathcal{D}_\omega$-algebra $\mathfrak{a}{:}\mathcal{D}_\omega(X) \to X$ by $\mathfrak{a}(\xi) = \boxplus_{x\in \mathsf{supp}(\xi)} \xi(x) x$. Our first observation is that $\mathsf{Exp}/_\sim$ carries a positive convex structure.

Proposition 5.5 **($\mathsf{Exp}/_\sim$ is a PCA)** *The set $\mathsf{Exp}/_\sim$ has a positive convex algebra structure, that is, for every $[E_1]_\sim, \cdots, [E_n]_\sim \in \mathsf{Exp}/_\sim$ and $p_1, \ldots, p_n \in [0,1]$ satisfying $\sum_{i=1}^n p_i \leqslant 1$, the operation given by*

$$
\boxplus_i p_i [E_i]_\sim = [\bigoplus_i p_i E_i]_\sim
$$

is a positive convex structure, where the scalar product on Exp is defined by

$$
p\left(\bigoplus_{i\in I} p_i \cdot E_i \right) = \bigoplus_{i\in I} (p p_i) \cdot E_i, \qquad p(\mu x.E) = p(E[\mu x.E/x]).
$$

Proposition 5.5 has the interesting consequence that, since $\mathcal{D}_\omega$ preserves surjections (like any functor on **Sets**) and $[-]_\equiv$ is surjective, also $\mathsf{Exp}/_\equiv$ is a positive convex algebra, with $[-]_\equiv$ an algebra homomorphism. Let $\mathbf{a}_\sim$ denote the algebra map $\mathbf{a}_\sim\colon \mathcal{D}_\omega(\mathsf{Exp}/_\sim) \to \mathsf{Exp}/_\sim$ given by the positive convex structure. We denote by $\mathbf{a}_\equiv$ a chosen induced algebra map on $\mathsf{Exp}/_\equiv$ making $[-]_\equiv$ an algebra homomorphism.

We can then expand the above diagram in the following way, where the coalgebra structure d exists because of Lemma 5.6 below:

$$\begin{tikzcd}
\mathsf{Exp} \arrow[r, "{[-]_\sim}"] \arrow[d, "c"'] \arrow[rr, bend left, "{[-]}"] & \mathsf{Exp}/_\sim \arrow[r, two heads, "{[-]_\equiv}"] \arrow[d, "c_0"'] & \mathsf{Exp}/_\equiv \arrow[ddd, "d"] \\
\mathcal{D}_\omega(1 + A \times \mathsf{Exp}) \arrow[r, "\mathcal{D}_\omega(1+A\times{[-]_\sim})"] & \mathcal{D}_\omega(1 + A \times \mathsf{Exp}/_\sim) \arrow[d, "\delta"'] & \\
& {[0,1]} \times \mathcal{D}_\omega(\mathsf{Exp}/_\sim)^A \arrow[d, "id\times \mathbf{a}_\sim^A"'] & \\
& {[0,1]} \times \mathsf{Exp}/_\sim^A \arrow[r, "id\times{[-]_\equiv}^A"] & {[0,1]} \times \mathsf{Exp}/_\equiv^A
\end{tikzcd}$$

Lemma 5.6 *Let $E_1, E_2 \in \mathsf{Exp}$ such that $E_1 \equiv E_2$. Then*

$$G[-]_\equiv \circ G\mathbf{a}_\sim \circ \delta \circ c_0([E_1]_\sim) = G[-]_\equiv \circ G\mathbf{a}_\sim \circ \delta \circ c_0 \circ ([E_2]_\sim).$$

Lemma 5.7 *The unique homomorphism $out_\equiv$ into the final G-coalgebra from the G-coalgebra $(\mathsf{Exp}/_\equiv, d)$ makes the following diagram commute.*

$$\begin{tikzcd}
\mathsf{Exp}/_\equiv \arrow[r, dashed, "out_\equiv"] \arrow[dd, "d"'] & \mathcal{D}(A^*) \arrow[r, tail] \arrow[d, "\mathcal{D}\iota"] & {[0,1]}^{A^*} \arrow[dd, "{\langle \varepsilon?, (-)_a \rangle}"] \\
& \mathcal{D}(1 + A \times A^*) \arrow[d, "\delta"'] & \\
{[0,1]} \times \mathsf{Exp}/_\equiv^A \arrow[r, dashed] & {[0,1]} \times (\mathcal{D}(A^*))^A \arrow[r, tail] & {[0,1]} \times ([0,1]^{A^*})^A
\end{tikzcd}$$

The following lemma implies that $out_\equiv \circ [-] = tr$, by finality.

Lemma 5.8 *The map $out_\equiv \circ [-]$ is a Kleisli homomorphism from $(\mathsf{Exp}, i \circ c)$ to $(A^*, \eta \circ \iota)$.*

This yields the soundness of the axiomatization, see Figure 2.

Theorem 5.9 (Soundness) *For all $E_1, E_2 \in \mathsf{Exp}$, $E_1 \equiv E_2 \Rightarrow E_1 \sim_{\mathsf{tr}} E_2$.*

5.3 Completeness

To prove completeness, as announced in Figure 2, it remains to prove that $out_\equiv$ is an injective map. Borrowing inspiration from [Jac06], we proceed as follows. We first factorize the map $out_\equiv$ into a surjective map followed by an injective one:

$$out_\equiv = \mathsf{Exp}/_\equiv \overset{e}{\twoheadrightarrow} I \overset{m}{\rightarrowtail} D(A^*)$$

Then, we show that $(\mathsf{Exp}/_\equiv, \mathbf{a}_\equiv, d)$ is final in a particular category of bialgebras: these are triples $(X, \mathfrak{a}, \alpha)$ with $\mathfrak{a}\colon \mathcal{D}_\omega(X) \to X$ a $\mathcal{D}_\omega$-algebra and $\alpha\colon X \to G(X)$ a locally finite G-coalgebra, and morphisms that are both coalgebra and algebra homomorphisms between the corresponding structures.

Note that factorizations in **Sets** carry on to categories of coalgebras. This equips the image I from the factorization in **Sets** with a coalgebra structure, such that e is a coalgebra homomorphism. Furthermore, since $\mathcal{D}_\omega$ (like any functor on **Sets**) preserves surjections, there is a $\mathcal{D}_\omega$-algebra on I making e an algebra homomorphism as well. Thus I is also a bialgebra in the same category, and it is also final. So the map e is an isomorphism and, therefore, $out_\equiv$ is injective.

Lemma 5.10 *The map* $out_\equiv \colon \mathsf{Exp}/_\equiv \to \mathcal{D}_\omega A^*$ *is injective.*

This is the last ingredient we needed for completeness.

Theorem 5.11 (Completeness) *For all* $E_1, E_2 \in \mathsf{Exp}$, $E_1 \sim_{\mathsf{tr}} E_2 \Rightarrow E_1 \equiv E_2$.

6 Conclusions

In this paper, we presented the first sound and complete axiomatization of (finite, terminating) trace semantics for generative probabilistic transition systems (with explicit termination).

Inspired by the work of Rabinovich, who axiomatized trace semantics for LTS, we took as basis a calculus sound and complete w.r.t. bisimilarity and we extended it with two extra axioms. Our approach is coalgebraic. This means that constructions and results are phrased in quite general terms which might be helpful to pinpoint which conditions on the functor type of the system are crucial and which generalizations are possible.

The fact that a sound and complete calculus w.r.t. bisimilarity can be extended to a sound and complete calculus w.r.t. coalgebraic language equivalence has recently been studied by Bonsangue, Milius and the first author [BMS11]. The class of systems they consider is however different from the one considered in this paper (formally, they consider coalgebras for FT, with F a functor and T a monad, such that F preserves T-algebras). In the determinization step, we relate to the powerset construction [SBBR10a] which also served as basis for the proofs in [BMS11]. However, we had to deal with the extra difficulty of showing that the semantics of the determinized automaton is actually a subdistribution over words (that is, an element of $\mathcal{D}(A^*)$) and not just any arbitrary function $[0,1]^{A^*}$. This fact is quite instructive and we believe that it will serve as basis to clarify the connection between the coalgebraic trace semantics of [HJS07] and the coalgebraic language equivalence of [BMS11] and describe a framework in which both semantics can be considered.

Acknowledgments.

The authors are indebted for valuable suggestions and pointers to the literature from Marcello Bonsangue and Stefan Milius.

References

[Bar] Falk Bartels. On generalized coinduction and probabilistic specification formats. Ph.D. thesis, Vrije Universiteit Amsterdam (2004)

[BMS11] Marcello Bonsangue, Stefan Milius, and Alexandra Silva. Sound and complete axiomatizations of coalgebraic language equivalence. preprint, 2011.

[BRS09] Marcello M. Bonsangue, Jan J. M. M. Rutten, and Alexandra Silva. An algebra for Kripke polynomial coalgebras. In *Proc. LICS*, pages 49–58. IEEE Computer Society, 2009.

[Dob06] Ernst-Erich Doberkat. Eilenberg-Moore algebras for stochastic relations. *Inf. Comput.*, 204(12):1756–1781, 2006.

[Dob08] Ernst-Erich Doberkat. Erratum and addendum: Eilenberg-Moore algebras for stochastic relations. *Inf. Comput.*, 206(12):1476–1484, 2008.

[HJS07] Ichiro Hasuo, Bart Jacobs, and Ana Sokolova. Generic trace semantics via coinduction. *Logical Methods in Computer Science*, 3(4), 2007.

[Jac06] Bart Jacobs. A bialgebraic review of deterministic automata, regular expressions and languages. In K. Futatsugi et al., editors, *Essays Dedicated to Joseph A. Goguen*, volume 4060 of *Lecture Notes in Computer Science*, pages 375–404. Springer, 2006.

[Joh] Peter Johnstone. Adjoint lifting theorems for categories of algebras. Bull. London Math. Soc. 7, 294–297 (1975)

[Mil84] Robin Milner. A complete inference system for a class of regular behaviours. *J. Comput. Syst. Sci.*, 28(3):439–466, 1984.

[Mil10] Stefan Milius. A sound and complete calculus for finite stream afteruits. In *Proc. LICS*, pages 421–430. IEEE Computer Society, 2010.

[NV09] Sumit Nain and Moshe Y. Vardi. Trace semantics is fully abstract. In *Proc. LICS*, pages 59–68. IEEE Computer Society, 2009.

[Rab93] Alexander Moshe Rabinovich. A complete axiomatisation for trace congruence of finite state behaviors. In S. Brookes et al., editors, *Proc. MFPS*, volume 802 of *Lecture Notes in Computer Science*, pages 530–543. Springer, 1993.

[Seg95] Roberto Segala. A compositional trace-based semantics for probabilistic automata. In *Proc. CONCUR*, volume 9622 of *Lecture Notes in Computer Science*, pages 234–248. Springer, 1995.

[SBBR10a] Alexandra Silva, Filippo Bonchi, Marcello Bonsangue, and Jan Rutten. Generalizing the powerset construction, coalgebraically. In K. Lodaya and M. Mahajan, editors, *Proc. FSTTCS 2010*, volume 8 of *LIPIcs*, pages 272–283, 2010.

[SBBR10b] Alexandra Silva, Filippo Bonchi, Marcello M. Bonsangue, and Jan J. M. M. Rutten. Quantitative Kleene coalgebras. *Information and Computation*, 2010.

[SS11] Alexandra Silva and Ana Sokolova. Sound and complete axiomatization of trace semantics for probabilistic systems. Technical report SEN-1108, CWI, 2011.

[vGSS95] Rob J. van Glabbeek, Scott A. Smolka, and Bernhard Steffen. Reactive, generative and stratified models of probabilistic processes. *Inf. Comput.*, 121(1):59–80, 1995.

A Proofs

Recall that $G = [0,1] \times -^A$ and $F = 1 + A \times -$.

Proof. [Proof of Lemma 5.3] We want to show that, starting from a coalgebra $X \xrightarrow{\alpha} \mathcal{D}_\omega(1 + A \times X)$, the image of the map *out*, as depicted in the commuting diagram below, is in $\mathcal{D}(A^*)$.

$$
\begin{tikzcd}
X \arrow[r, "\eta_X"] \arrow[d, "\alpha"'] & \mathcal{D}_\omega(X) \arrow[r, dashed, "out"] \arrow[ddl, "(\delta\circ\alpha)^\sharp"] & \mathcal{D}(A^*) \arrow[r, tail] \arrow[d, "\mathcal{D}\iota"] & {[0,1]^{A^*}} \arrow[dd, "\langle \varepsilon?, (-)_a \rangle"] \\
\mathcal{D}_\omega(1 + A \times X) \arrow[d, "\delta"'] & & \mathcal{D}(1 + A \times A^*) \arrow[d, "\delta"'] & \\
{[0,1] \times \mathcal{D}_\omega(X)^A} \arrow[rr, dashed, "id \times out^A"] & & {[0,1] \times (\mathcal{D}(A^*))^A} \arrow[r, tail] & {[0,1] \times ([0,1]^{A^*})^A}
\end{tikzcd}
$$

It is direct to check that the diagram on the right commutes. This, after we show that $out(\xi) \in \mathcal{D}(A^*)$ for any $\xi \in \mathcal{D}_\omega(X)$, provides also commutativity of the inner part, i.e., *out* is the unique homomorphism into $(\mathcal{D}(A^*), \delta \circ \mathcal{D}\iota)$.

Let $\xi \in \mathcal{D}_\omega(X)$. We now check that indeed $out(\xi) \in \mathcal{D}(A^*)$. We need to show that

$$\sum_{w \in A^*} out(\xi)(w) \leqslant 1.$$

Consider $W_i = \{w \in A^* \mid |w| = i\}$, for $i \in \mathbb{N}$. Each W_i is finite, since the label set A is finite. We have

$$\sum_{w \in A^*} out(\xi)(w) = \sum_{i \in \mathbb{N}} \left(\sum_{w \in W_i} out(\xi)(w) \right),$$

and the series converges if the sequence of partial sums converges, in this case if the limit

$$\lim_{n \to \infty} \left(\sum_{\substack{w \in W_i \\ i \leqslant n}} out(\xi)(w) \right) = \lim_{n \to \infty} \left(\sum_{w : |w| \leqslant n} out(\xi)(w) \right)$$

exists. Our sequence of partial sums is monotonically non-decreasing, i.e.,

$$\sum_{w : |w| \leqslant n} out(\xi)(w) \leqslant \sum_{w : |w| \leqslant n+1} out(\xi)(w).$$

If we show that it is also bounded from above by 1, then we are done since then the limit exists and it is smaller than or equal to 1. Therefore, we next show that for any $n \in \mathbb{N}$, $\sum_{w:|w| \leqslant n} out(\xi)(w) \leqslant 1$ which will complete the proof.

Recall that

$$\begin{aligned} out(\xi)(\varepsilon) &= \sum_{x \in X} \xi(x) \cdot \alpha(x)(*) \\ out(\xi)(aw) &= out(\lambda x. \sum_{x' \in X} \xi(x') \cdot \alpha(x')(a,x))(w). \end{aligned}$$

So, we have

$$\begin{aligned} &\sum_{w:|w|\leqslant n} out(\xi)(w) = \\ &\quad = \sum_{x_0 \in X} \xi(x_0) \cdot \alpha(x_0)(*) + \sum_{\substack{a_1 \in A \\ x_0, x_1 \in X}} \xi(x_0) \cdot \alpha(x_0)(a_1, x_1) \cdot \alpha(x_1)(*) \\ &\qquad + \cdots + \sum_{\substack{a_1,\ldots,a_n \in A \\ x_0,x_1,\ldots,x_n \in X}} \xi(x_0) \cdot \alpha(x_0)(a_1,x_1) \cdots \alpha(x_{n-1})(a_n, x_n) \cdot \alpha(x_n)(*) \\ &\quad = \sum_{x_0 \in X} \xi(x_0) \cdot \Big[\alpha(x_0)(*) + \sum_{\substack{a_1 \in A \\ x_1 \in X}} \alpha(x_0)(a_1,x_1) \cdot \alpha(x_1)(*) \\ &\qquad + \cdots + \sum_{\substack{a_1,\ldots,a_n \in A \\ x_1 \ldots x_n \in X}} \alpha(x_0)(a_1,x_1) \cdots \alpha(x_{n-1})(a_n,x_n) \cdot \alpha(x_n)(*) \Big] \\ &\quad = \sum_{x_0 \in X} \xi(x_0) \cdot S_0(x_0) \end{aligned}$$

where, for $0 \leqslant k \leqslant n-1$,

$$S_k(x_k) = \alpha(x_k)(*) + \sum_{a_{k+1} \in A, x_{k+1} \in X} \alpha(x_k)(a_{k+1}, x_{k+1}) \cdot S_{k+1}(x_{k+1})$$

and

$$S_n(x_n) = \alpha(x_n)(*).$$

Note that $S_n(x_n) \leqslant 1$ and $S_{k+1}(x_{k+1}) \leqslant 1 \implies S_k(x_k) \leqslant 1$, for $0 \leqslant k \leqslant n-1$. Hence, we have that all $S_k(x_k) \leqslant 1$ for $0 \leqslant k \leqslant n$, showing finally that

$$\begin{aligned} \sum_{w:|w|\leqslant n} out(\xi)(w) &= \sum_{x_0 \in X} \xi(x_0) \cdot S_0(x_0) \\ &\leqslant \sum_{x_0 \in X} \xi(x_0) \\ &\leqslant 1. \end{aligned}$$

□

Proof. [Proof of Proposition 5.5]

We need to check that conditions (i) and (ii) hold for the PCA structure on $\mathsf{Exp}/_\sim$. For (i), given that $p_{i,k} = 1$ for $i = k$ and $p_{i,k} = 0$ otherwise, we have

$$\boxplus_i p_{i,k}[\mathsf{E}_i]_\sim = \left[\bigoplus_i p_{i,k}\mathsf{E}_i\right]_\sim \stackrel{(*)}{=} [1\mathsf{E}_i]_\sim = [\mathsf{E}_i]_\sim$$

where the equality marked by $(*)$ holds using the axioms $(Cong)$, (Z), and (E), and the last equality is easily provable from the definition of a scalar product.

For (ii), let $[\mathsf{E}_j]_\sim \in \mathsf{Exp}/_\sim$, $p_i, q_{i,j} \in [0,1]$ for $i \in I$ and $j \in J$ (both index sets finite) such that $\sum_i p_i \leqslant 1$ and $\sum_j q_{i,j} \leqslant 1$ for all $i \in I$. First, we note that any expression is bisimilar to a $\bigoplus$-expression. In particular, there is a finite index set K, such that for every $j \in J$ there are $r_{j,k} \in [0,1]$ for $k \in K$ with $E_j \sim \bigoplus_k r_{j,k}\mathsf{F}_{j,k}$ for some expressions $F_{j,k}$. That is, $[\mathsf{E}_j]_\sim = [\bigoplus_k r_{j,k}\mathsf{F}_{j,k}]_\sim$.

Then we have

$$\begin{aligned}
\boxplus_i p_i\left(\boxplus_j q_{i,j}[\mathsf{E}_j]_\sim\right) &= \boxplus_i p_i\left[\bigoplus_j q_{i,j}\mathsf{E}_j\right]_\sim \\
&= \left[\bigoplus_i p_i\left(\bigoplus_j q_{i,j}\mathsf{E}_j\right)\right]_\sim \\
&= \left[\bigoplus_{i,j}(p_i q_{i,j})\mathsf{E}_j\right]_\sim \\
&= \left[\bigoplus_{i,j,k}(p_i q_{i,j})r_{j,k}\cdot\mathsf{F}_{j,k}\right]_\sim \\
&\stackrel{(S)}{=} \left[\bigoplus_{j,k}\left(\sum_i(p_i q_{i,j})r_{j,k}\right)\cdot\mathsf{F}_{j,k}\right]_\sim \\
&= \left[\bigoplus_{j,k}\left(\sum_i p_i q_{i,j}\right)r_{j,k}\cdot\mathsf{F}_{j,k}\right]_\sim \\
&= \left[\bigoplus_{j}\left(\sum_i p_i q_{i,j}\right)\mathsf{E}_j\right]_\sim \\
&= \boxplus_j\left(\sum_i p_i q_{i,j}\right)[\mathsf{E}_j]_\sim
\end{aligned}$$

which completes the proof. □

Proof. [Proof of Lemma 5.6] By induction on the length of derivations for $\equiv$. We actually prove that $G\mathbf{a}_\sim \circ \delta \circ c_0([\mathsf{E}_1]_\sim) = G\mathbf{a}_\sim \circ \delta \circ c_0([\mathsf{E}_2]_\sim)$.

For all the axioms but the last two the result follows directly from the result for bisimilarity (for a formal proof see [BMS11]). Hence, we just need to show the proof for (M) and (D). Using that $c_0 \circ [-]_\sim = \mathcal{D}_\omega(1 + A \times [-]_\sim) \circ c$, we calculate for the axiom (M):

$$G\mathbf{a}_\sim \circ \delta \circ c_0([p \cdot a \cdot \mathsf{E}]_\sim) = \langle 0, f_a \rangle$$

where $f_a(a) = [p\mathsf{E}]_\sim$ and $f_a(b) = [\underline{\varnothing}]_\sim$ for $b \neq a$. Also,

$$G\mathbf{a}_\sim \circ \delta \circ c_0([(pq) \cdot a \cdot \tfrac{1}{q}\mathsf{E}]_\sim) = \langle 0, f'_a \rangle$$

where $f'_a(a) = [(pq)\frac{1}{q}\mathsf{E}]_\sim$ and $f_a(b) = [\underline{\varnothing}]_\sim$ for $b \neq a$. The equality now follows using the property $(pq)\frac{1}{q}\mathsf{E} = p\mathsf{E}$ of the scalar product. Further, for the axiom (D), we have:

$$G\mathbf{a}_\sim \circ \delta \circ c_0([p \cdot a \cdot \mathsf{E}_1 \oplus p \cdot a \cdot \mathsf{E}_2]_\sim) = \langle 0, g_a \rangle$$

where $g_a(a) = [p\mathsf{E}_1 \oplus p\mathsf{E}_2]_\sim$ and $g_a(b) = [\underline{\varnothing}]_\sim$ for $b \neq a$. We note that in the derivation, we distinguish two cases: $\mathsf{E}_1 \sim \mathsf{E}_2$ and $\mathsf{E}_1 \not\sim \mathsf{E}_2$, which using the axiom (S) still lead to the same result. Also,

$$G\mathbf{a}_\sim \circ \delta \circ c_0([p \cdot a \cdot (\mathsf{E}_1 \oplus \mathsf{E}_2)]_\sim) = \langle 0, g'_a \rangle$$

with $g'_a(a) = [p(\mathsf{E}_1 \oplus \mathsf{E}_2)]_\sim$ and $g'_a(b) = [\underline{\varnothing}]_\sim$ for $b \neq a$. The equality now follows by definition of the scalar product, since $p\mathsf{E}_1 \oplus p\mathsf{E}_2 = p(\mathsf{E}_1 \oplus \mathsf{E}_2)$. In this last equality, if one of the sides is defined, the other one is defined as well.
$\square$

Proof. [Proof of Lemma 5.7] We need to show that the image of $out_\equiv$ lives in $\mathcal{D}(A^*)$. We proceed as follows. First, put $out_\sim = out_\equiv \circ [-]_\equiv$. Note that it is the unique homomorphism from $(\mathsf{Exp}/_\sim, G\mathbf{a}_\sim \circ \delta \circ c_0)$ to the final G-coalgebra, hence the name is deserved. Then, since $[-]_\equiv$ is surjective, it is enough to prove that the image of $out_\sim$ lives in $\mathcal{D}(A^*)$.

For this we first prove that $out_\sim \circ \mathbf{a}_\sim$ is a coalgebra homomorphism from the determinization $\big(\mathcal{D}_\omega \mathsf{Exp}/_\sim, (\delta \circ c_0)^\#\big)$ to the final G-coalgebra. This will show that $out_\sim \circ \mathbf{a}_\sim = out$ where the map out on the right side is the unique homomorphism from the determinization to the final. Furthermore, using that $(\mathsf{Exp}_\sim, \mathbf{a}_\sim)$ is an Eilenberg-Moore algebra for the monad $\mathcal{D}_\omega$, this implies that $out_\sim = out_\sim \circ \mathbf{a}_\sim \circ \eta = out \circ \eta$ and since the image of out lives in $\mathcal{D}(A^*)$, by Lemma 5.3, this completes the proof.

So, we check that $out_\sim \circ \mathbf{a}_\sim$ is indeed a coalgebra homomorphism. Since $out_\sim$ is a coalgebra homomorphism from $(\mathsf{Exp}/_\sim, G\mathbf{a}_\sim \circ \delta \circ c_0)$ it suffices to prove that $G\mathbf{a}_\sim \circ \delta \circ c_0 \circ \mathbf{a}_\sim = G\mathbf{a}_\sim \circ (\delta \circ c_0)^\#$, as in the diagram below.

$$\begin{tikzcd}
\mathcal{D}_\omega \mathsf{Exp}/_\sim \arrow[r, "\mathbf{a}_\sim"] \arrow[d, "(\delta\circ c_0)^\#"'] & \mathsf{Exp}/_\sim \arrow[r, "out_\sim"] \arrow[d, "G\mathbf{a}_\sim\circ\delta\circ c_0"] & {[0,1]^{A^*}} \arrow[d, "\cong"] \\
G(\mathcal{D}_\omega \mathsf{Exp}/_\sim) \arrow[r, "G\mathbf{a}_\sim"] & G(\mathsf{Exp}/_\sim) \arrow[r, "Gout_\sim"] & G([0,1]^{A^*})
\end{tikzcd}$$

Recall that $(\delta \circ c_0)^\# = \delta \circ \mu \circ \mathcal{D}_\omega c_0$. We need

$$G\mathbf{a}_\sim \circ \delta \circ c_0 \circ \mathbf{a}_\sim = G\mathbf{a}_\sim \circ \delta \circ \mu \circ \mathcal{D}_\omega c_0$$

which holds since $c_0 \circ \mathbf{a}_\sim = \mu \circ \mathcal{D}_\omega c_0$, as can readily be checked using the definitions. □

Proof. [Proof of Lemma 5.8] Just like in the previous proof of Lemma 5.7, we start by noticing that $out_\sim = out_\equiv \circ [-]_\equiv$ satisfies $out_\equiv \circ [-] = out_\sim \circ [-]_\sim$.

Therefore, it suffices to prove that $out_\sim \circ [-]_\sim$ is a Kleisli homomorphism from $(\mathsf{Exp}, i \circ c)$ to $(\mathcal{D}(A^*), \eta \circ \iota)$, the final $\overline{F}$-coalgebra in the Kleisli category of the subdistribution monad $\mathcal{D}$, i.e. the following diagram commutes.

$$\begin{tikzcd}
\mathsf{Exp} \arrow[r, "out_\sim\circ[-]_\sim"] \arrow[d, "i\circ c"'] & A^* \arrow[d, "\eta\circ\iota"] \\
1 + A \times \mathsf{Exp} \arrow[r, "\overline{id+id\times(out_\sim\circ[-]_\sim)}"] & 1 + A \times A^*
\end{tikzcd}$$

We first represent the above diagram in **Sets**.

$$\begin{tikzcd}
\mathsf{Exp} \arrow[r, "{[-]_\sim}"] \arrow[d, "i\circ c"'] & \mathsf{Exp}/_\sim \arrow[r, "out_\sim"] \arrow[d, "i\circ c_0"'] & \mathcal{D}(A^*) \arrow[d, "\mathcal{D}(\eta\circ\iota)"] \arrow[dd, bend left, "\mathcal{D}\iota"] \\
\mathcal{D}F(\mathsf{Exp}) \arrow[r, "{\mathcal{D}[-]_\sim}"] \arrow[d, "\mathcal{D}F(out_\sim\circ[-]_\sim)"'] & \mathcal{D}F(\mathsf{Exp}/_\sim) \arrow[dl, "\mathcal{D}F(out_\sim)"] & \mathcal{D}\mathcal{D}F(A^*) \arrow[d, "\mu"] \\
\mathcal{D}F\mathcal{D}(A^*) \arrow[r, "\mathcal{D}\lambda"] & \mathcal{D}\mathcal{D}F(A^*) \arrow[r, "\mu"] & \mathcal{D}F(A^*)
\end{tikzcd}$$

The first observation is that, since $\delta \colon \mathcal{D}F(X) \to G\mathcal{D}(X)$ is injective, we can actually prove that:

$$
\begin{aligned}
&\delta \circ \mu \circ \mathcal{D}\lambda \circ \mathcal{D}F(out_\sim \circ [-]_\sim) \circ i \circ c \\
&\quad = \ \delta \circ \mu \circ \mathcal{D}\lambda \circ \mathcal{D}F(out_\sim) \circ i \circ c_0 \circ [-]_\sim \\
&\quad \overset{(a)}{=} \ G\mu \circ \delta \circ \mathcal{D}F(out_\sim) \circ i \circ c_0 \circ [-]_\sim \\
&\quad \overset{(nat.\delta)}{=} \ G\mu \circ G\mathcal{D}(out_\sim) \circ \delta \circ i \circ c_0 \circ [-]_\sim \\
&\quad \overset{(b)}{=} \ G\mu \circ G\mathcal{D}(out_\sim) \circ Gi \circ \delta \circ c_0 \circ [-]_\sim \\
&\quad = \ G(\mu \circ out_\sim \circ i) \circ \delta \circ c_0 \circ [-]_\sim \\
&\quad \overset{(c)}{=} \ G(out_\sim \circ \mathbf{a}_\sim) \circ \delta \circ c_0 \circ [-]_\sim \\
&\quad = \ G(out_\sim) \circ G\mathbf{a}_\sim \circ \delta \circ c_0 \circ [-]_\sim \\
&\quad \overset{(d)}{=} \ \delta \circ \mathcal{D}\iota \circ out_\sim \circ [-]_\sim
\end{aligned}
$$

which implies the commutativity of the above diagram. In the above calculation, the equality marked by (a) holds since δ, μ and the distributive law $\lambda{:}F\mathcal{D}(X) \to \mathcal{D}F(X)$ satisfy $\delta \circ \mu \circ \mathcal{D}\lambda = G\mu \circ \delta$. Recall from [HJS07] that the distributive law is given by $\lambda(*) = \eta(*)$ and $\lambda(a,\varphi) = \lambda\langle a,x\rangle.\varphi(x)$. Further on, the equality marked by (b) is a consequence of $\delta \circ i = Gi \circ \delta$. The equality marked by (c) is a consequence of $\mu \circ \mathcal{D}out_\sim \circ i = out_\sim \circ \mathbf{a}_\sim$ which holds since $out_\sim$ is an algebra homomorphism between $\mathcal{D}_\omega(\mathsf{Exp}_\sim)$ and $\mathcal{D}(A^*)$ (this is a consequence of [Bar, Theorem 3.2.3], our Lemma 5.3 and the fact that $i \circ \mathcal{D}_\omega(out_\sim) = \mathcal{D}(out_\sim) \circ i$). Finally, the equality marked by (d) is a consequence of the previous proof, of Lemma 5.7, and the statement of Lemma 5.3.

□

Before we prove Lemma 5.10 we need two more lemmas.

Lemma A.1 *There exists an algebra map $d^{-1}\colon [0,1] \times \mathsf{Exp}/^A_\equiv \to \mathsf{Exp}/_\equiv$ such that $d^{-1} \circ d = id$.*

Proof.

We define $d^{-1}\colon [0,1] \times \mathsf{Exp}/^A_\equiv \to \mathsf{Exp}/_\equiv$ as follows

$$
d^{-1}(\langle p, f\rangle) = \left[p \cdot \star \oplus \bigoplus_{a \in A} p_a \cdot a \cdot \mathsf{E}_a \right], \qquad f(a) = [p_a \mathsf{E}_a] \text{ and } \sum_{a \in A} p_a \leqslant 1 - p
$$

Note that d^{-1} is only defined for those f which allow the rewriting above. For instance, if $f(a) = 1 \cdot \star$ and $p = 0.5$ then d^{-1} would not be defined. However, $d^{-1}(d([E]))$ will always be defined, and moreover, equal to $[\mathsf{E}]$, as we prove next, by induction of the number of nested fixed points.

$$
\begin{array}{rcll}
d^{-1}(d([\mu x.\mathsf{E}])) & = & d^{-1}(d(([\mathsf{E}[\mu x.\mathsf{E}/x]])) & \\
 & \stackrel{\text{(IH)}}{=} & [\mathsf{E}[\mu x.\mathsf{E}/x]] = \mu x.\mathsf{E} & \\
d^{-1}(d([\bigoplus_{i\in I} p_i \cdot \mathsf{E}_i])) & = & d^{-1}(\sum_{i\in I} p_i \overline{d}(\mathsf{E}_i)) & (d \text{ is an algebra map}) \\
 & = & \boxplus_{i\in I} p_i d^{-1}(\overline{d}(\mathsf{E}_i)) & (d^{-1} \text{ is an algebra map}) \\
 & = & \boxplus_{i\in I} p_i [1 \cdot \mathsf{E}_i] & (d^{-1}(\overline{d}(E_i)) = [1 \cdot \mathsf{E}_i]) \\
 & = & \left[\bigoplus_{i\in I} p_i \cdot \mathsf{E}_i\right] &
\end{array}
$$

In the calculations above, $\overline{d}(\mathsf{E}_i)$ is given by

$$
\overline{d}(\star) = \langle 1, \lambda a.[\underline{\varnothing}]\rangle \qquad\qquad \overline{d}(a \cdot \mathsf{E}) = \left\langle 0, \lambda a'. \begin{cases} [\mathsf{E}] & a' = a \\ [\underline{\varnothing}] & \mathit{otherwise} \end{cases} \right\rangle
$$

Also note that $d^{-1}(\overline{d}(E_i)) = [1 \cdot \mathsf{E}_i]$ can easily be checked:

$$
\begin{aligned}
d^{-1}(\overline{d}(\star)) &= \left[1 \cdot \star \oplus \bigoplus_{a\in A} 0.a.\underline{\varnothing}\right] = [1.\star] \\
d^{-1}(\overline{d}(a \cdot \mathsf{E})) &= \left[0 \cdot \star \oplus 1 \cdot a \cdot \mathsf{E} \oplus \bigoplus_{a'\in A\setminus\{a\}} 0.a'.\underline{\varnothing}\right] = [1 \cdot a \cdot \mathsf{E}]
\end{aligned}
$$

using the (Z) and (E) axioms.

The last thing we need to prove is that d^{-1} is indeed an algebra map:

$$
d^{-1}\left(\boxplus_{i\in I} \alpha_i \langle o_i, f_i\rangle\right) = \boxplus_{i\in I} \alpha_i d^{-1}(\alpha_i \langle o_i, f_i\rangle)
$$

That is,

$$
\left[\left(\sum_{i\in I} \alpha_i o_i\right) \cdot \star \oplus \bigoplus_{a\in A} p_a \cdot a \cdot \mathsf{E}_a\right] = \boxplus_{i\in I} \alpha_i \left[o_i \cdot \star \oplus \bigoplus_{a\in A} p_a^i \cdot a \cdot \mathsf{E}_a^i\right]
$$

where $p_a[\mathsf{E}_a] = \boxplus_{i\in I} \alpha_i f_i(a)$ and $p_a^i[\mathsf{E}_a^i] = f_i(a)$. Observe that

$$\begin{aligned}\boxplus_{i\in I}\alpha_i\left(\bigoplus_{a\in A}p_a^i\cdot a\cdot \mathsf{E}_a^i\right) &= \bigoplus_{i\in I}\alpha_i\left(\bigoplus_{a\in A}p_a^i\cdot a\cdot \mathsf{E}_a^i\right)\\ &\overset{(M)}{\equiv} \bigoplus_{i\in I}\alpha_i\tfrac{p_a^i}{\beta_a}\left(\bigoplus_{a\in A}\beta_a\cdot a\cdot \mathsf{E}_a^i\right), \qquad \beta_a = min\ p_a^i\\ &\overset{(D)}{\equiv} \bigoplus_{a\in A}\beta_a\cdot a\cdot\bigoplus_{i\in I}\alpha_i\tfrac{p_a^i}{\beta_a}\mathsf{E}_a^i\end{aligned}$$

Hence, we have that

$$\boxplus_{i\in I}\alpha_i\left[o_i\cdot\star\oplus\bigoplus_{a\in A}p_a^i\cdot a\cdot\mathsf{E}_a^i\right] = \left[\left(\sum_{i\in I}\alpha_i o_i\right)\cdot\star\oplus\bigoplus_{a\in A}\beta_a\cdot a\cdot\alpha_i\frac{p_a^i}{\beta_a}\mathsf{E}_a^i\right]$$

Now, using the fact that

$$\beta_a\left[\bigoplus_{i\in I}\alpha_i\frac{p_a^i}{\beta_a}\mathsf{E}_a^i\right] = \left[\bigoplus_{i\in I}\alpha_i p_a^i\mathsf{E}_a^i\right] = \boxplus_{i\in I}\alpha_i(p_a^i[\mathsf{E}_a^i]) = \boxplus_{i\in I}\alpha_i f_i(a) = p_a[\mathsf{E}_a]$$

we can conclude that

$$\left[(\sum_{i\in I}\alpha_i o_i)\cdot\star\oplus\bigoplus_{a\in A}\beta_a\cdot a\cdot\alpha_i\frac{p_a^i}{\beta_a}\mathsf{E}_a^i\right] = \left[(\sum_{i\in I}\alpha_i o_i)\cdot\star\oplus\bigoplus_{a\in A}p_a\cdot a\cdot\mathsf{E}_a\right]$$

where $p_a[\mathsf{E}_a] = \boxplus_{i\in I}\alpha_i f_i(a)$. $\square$

In what follows, we will use the well-known fact that to have a lifting of a functor G to $\mathbf{Sets}^T$, the Eilenberg-Moore category for a monad T, is the same as to have a distributive law π of the functor G over the monad T [Joh], that is, a natural transformation $\pi\colon TG \to GT$ which satisfies the laws $\pi\circ\eta = F\eta$ and $\pi\circ\mu = F\mu\circ\pi\circ T\pi$. The functor $G = [0,1]\times(-)^A$ that we consider has a canonical lifting to $\mathbf{Sets}^{\mathcal{D}_\omega}$. In the rest of this section, we will be working in the category of *locally-finite bialgebras* for the (canonical) distributive law $\pi\colon \mathcal{D}_\omega G(S)\to G\mathcal{D}_\omega(S)$. The objects in this category are π-bialgebras $(S,\mathfrak{a},\alpha)$ such that for every $s\in S$, the subcoalgebra $\langle s\rangle$ is finite. Homomorphisms are the usual bialgebra homomorphisms.

Lemma A.2 *For every locally finite π-bialgebra $(S,\mathfrak{a},\alpha)$, there exists a* *unique bialgebra homomorphism* h *into* $\mathsf{Exp}/_{\equiv}$ *that is*

$$\begin{tikzcd} \mathcal{D}_\omega(S) \arrow[r, "\mathcal{D}_\omega h"] \arrow[d, "\mathfrak{a}"'] & \mathcal{D}_\omega(\mathsf{Exp}/_{\equiv}) \arrow[d, "\mathbf{a}_{\equiv}"] \\ S \arrow[r, dashed, "h"] \arrow[d, "\alpha"'] & \mathsf{Exp}/_{\equiv} \arrow[d, "d"] \\ GS \arrow[r, "Gh"'] & G\mathsf{Exp}/_{\equiv} \end{tikzcd}$$

Proof. To see that $(\mathsf{Exp}/_{\equiv}, \mathbf{a}_{\equiv}, d)$ is a locally finite bialgebra we use that the coalgebra $(\mathsf{Exp}/_{\sim}, c_0)$ is locally finite (shown in [SBBR10b]) and, hence, also $(\mathsf{Exp}/_{\sim}, G\mathbf{a}_{\sim} \circ \delta \circ c_0)$ is locally finite. Since $\mathsf{Exp}/_{\equiv}$ is a quotient coalgebra of $\mathsf{Exp}/_{\sim}$, we see that $\mathsf{Exp}/_{\equiv}$ is locally finite.

Let $m\colon (S, \mathfrak{a}, \alpha) \to (\mathsf{Exp}/_{\equiv}, \mathbf{a}_{\equiv}, d)$ by any bialgebra homomorphism and let $s \in S$. Since $\langle s \rangle = \{ s_1, \ldots, s_n \}$ is finite we prove that the $m(s_i)$ are uniquely determined.

In order to prove this, we will first define closed expressions $\langle\!\langle s_i \rangle\!\rangle$ and then show that these are provably equivalent to $m(s_i)$.

The expressions $\langle\!\langle x_i \rangle\!\rangle$ are defined by an n-step process. Let

$$\alpha(s_i) = \langle o_i, f_i \rangle, \qquad o_i \in [0,1], \quad f_i{:}A \to S, \quad i = 1, \ldots, n. \tag{A.1}$$

Our expressions will involve n variables $x_1, \ldots, x_n$. For every $i = 1, \ldots, n$ let

$$A_i^0 = \mu x_i. \left(o_i \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_i(a) = s_j}} (\xi(x_j) \cdot a \cdot x_j) \right), \text{ for some } \xi \ s.t.\ \mathfrak{a}(\xi) = x_i$$

Now define for $k = 0, \ldots, n-1$

$$A_i^{k+1} = \begin{cases} A_i^k\{A_{k+1}^k/x_{k+1}\} \text{ if } i = k+1 \\ \\ \qquad A_i^k \qquad\quad \text{if } i = k+1, \end{cases}$$

where $\{A/x\}$ denotes syntactic replacement (i. e., substitution without renaming of bound variables). It is easy to see that the set of free variables of A_i^k is $\{x_{k+1}, \ldots x_n\} \backslash \{ x_i \}$, and moreover, every occurrence of those variables is free.

We also see that for every i,

$$\begin{aligned} A_i^n &= A_i^0\{A_1^0/x_1\}\{A_2^1/x_2\} \cdots \{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\} \cdots \{A_n^{n-1}/x_n\} \\ &= A_i^{i-1}\{A_{i+1}^i/x_{i+1}\} \cdots \{A_n^{n-1}/x_n\}. \end{aligned}$$

Observe that A_i^n is a closed term. Moreover, the variable x_i from A_i^0 is never syntactically replaced and it is bound by the outermost μx_i. All other occurrences of x_i in A_i^n are not bound by this μ-operator (but by μ-operators further inside the term). We define

$$\langle\!\langle s_i \rangle\!\rangle = A_i^n.$$

First, we show that $h = [-] \circ \langle\!\langle - \rangle\!\rangle$ is an algebra homomorphism, that is

$$[\langle\!\langle s_k \rangle\!\rangle] = p_1[\langle\!\langle s_1 \rangle\!\rangle] + \cdots + p_n[\langle\!\langle s_n \rangle\!\rangle], \qquad s_k = p_1 s_1 + \ldots + p_n s_n$$

This follows easily if one observes that for any k

$$\begin{aligned} o_k &= p_1 o_1 + \ldots + p_n o_n \\ f_k(a) &= p_1 f_1(a) + \ldots + p_n f_n(a) \end{aligned}$$

which implies that

$$\begin{aligned} & o_k \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_k(a)=s_j}} (\xi(x_j)\cdot a \cdot x_j), \qquad \text{for some } \xi \text{ } s.t. \text{ } \mathfrak{a}(\xi) = s_k \\ &= (p_1 o_1 + \ldots + p_n o_n)\cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_i(a)=s_j^i}} (\xi(x_j)\cdot a \cdot (p_1 x_j^1 \oplus p_1 x_j^2 \cdots \oplus p_n x_j^n)) \\ &= p_1(o_1 \cdot \star) \oplus \bigoplus_{\substack{a\in A \\ f_1(a)=s_j}} (p_j \cdot a \cdot (p_1 x_j)) \oplus \cdots \oplus \bigoplus_{\substack{a\in A \\ f_n(a)=s_j}} (p_j \cdot a \cdot (p_n x_j)) \\ &= p_1 \left(o_1 \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_1(a)=s_j}} (p_j \cdot a \cdot x_j) \right) \oplus \cdots \oplus p_n \left(o_n \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_n(a)=s_j}} (p_j \cdot a \cdot x_j) \right) \end{aligned}$$

In the one but last step, we used the fact that

$$\mathfrak{a}(\xi) = s_k \iff \mathfrak{a}(\xi) = p_1 s_1 + \ldots + p_n s_n \iff \xi(s_j) = p_j$$

So now we have $A_k^0 = p_1 A_1^0 \oplus \cdots p_n A_n^0$, which is sufficient to conclude that

$$[\langle\!\langle s_k \rangle\!\rangle] = p_1[\langle\!\langle s_1 \rangle\!\rangle] + \cdots + p_n[\langle\!\langle s_n \rangle\!\rangle], \qquad s_k = p_1 s_1 + \ldots + p_n s_n$$

We also have that h is a coalgebra homomorphism between (S, α) and $(\mathsf{Exp}/_{\equiv}, d)$ (this is a consequence of h being a coalgebra homomorphism between $(X, \overline{\alpha})$, for $\overline{\alpha}$ the unique morphism such that $\alpha = Ga \circ \delta \circ \overline{\alpha}$, and $(\mathsf{Exp}/_{\sim}, c_0)$ and $\mathsf{Exp}/_{\equiv}$ being a quotient of Exp).

It remains to prove uniqueness. From now on we shall abuse notation and we will denote equivalence classes $[\mathsf{E}]$ of expressions in $\mathsf{Exp}/_{\equiv}$ simply by expressions E representing them. It is our goal to prove that $m(s_i) \equiv \langle\!\langle s_i \rangle\!\rangle$. Let us write m_i for (some representative of) $m(s_i)$, for short. Using the fact that m is a coalgebra homomorphism, Lemma A.1 and equation A.1 and we see that

$$\begin{aligned} m_i &= d^{-1} \circ Gm \circ \alpha(s_i) \\ &= d^{-1} \circ Gm(\langle o_i, f_i \rangle) \\ &= d^{-1}(\langle o_i, m \circ f_i \rangle) \\ &= o_i \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_i(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} m_j, \qquad \textstyle\sum_{a \in A} p_a \leqslant 1 - o_i \end{aligned} \tag{A.2}$$

For the proof of $m_i \equiv \langle\!\langle s_i \rangle\!\rangle$, we show the case $n = 3$ in detail; the general case is completely analogous and is left to the reader.

We start by proving that $m_1 \equiv A_1^0[m_2/x_2][m_3/x_3]$ by an application of the uniqueness rule. From equation (A.2) we get

$$\begin{aligned} m_1 &\equiv o_1 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_1(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} m_j \\ &= ((o_1 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_i(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j)[m_2/x_2][m_3/x_3])[m_1/x_1] \\ & \qquad\qquad \Downarrow (UFP) \\ m_1 &\equiv \mu x_1.(o_1 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_i(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j)[m_2/x_2][m_3/x_3] \\ &\equiv A_0^1[m_2/x_2][m_3/x_3] \end{aligned}$$

Next, we prove that $m_2 \equiv A_2^1[m_3/x_3]$. Notice that

$$A_1^0[m_2/x_2][m_3/x_3] = A_1^0[m_3/x_3][m_2/x_2]$$

since m_2 and m_3 are closed. Then, applying equation (A.2), we have

$$\begin{aligned} m_2 &\equiv o_2 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_2(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} m_j \\ &\equiv o_2 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_2(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j \, [A_1^0[m_2/x_2][m_3/x_3]/x_1] \, [m_2/x_2][m_3/x_3] \\ &= \left(o_2 \cdot \star \oplus \bigoplus_{\substack{a \in A \\ f_2(a) = s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j [A_1^0/x_1][m_3/x_3] \right) [m_2/x_2], \end{aligned}$$

and so we can apply the uniqueness rule to obtain the desired equation.

Now, we are able to prove that

$$m_1 \equiv A_1^0\{A_2^1/x_2\}[m_3/x_3].$$

First, note that we have $A_1^0\{A_2^1/x_2\} = A_1^0[A_2^1/x_2]$ since x_1 (which is bound in A_1^0) is not free in A_2^1. We obtain

$$\begin{aligned} A_1^0[A_2^1/x_2][m_3/x_3] &\equiv A_1^0[m_3/x_3][A_2^1[m_3/x_3]/x_2] \\ &\equiv A_1^0[m_3/x_3][m_2/x_2] \\ &\equiv m_1. \end{aligned}$$

Finally, we show that $m_3 \equiv A_3^2$ by another application of the uniqueness rule; we have

$$\begin{aligned} m_3 &\equiv o_3 \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_3(a)=s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j \\ &\equiv o_3 \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_3(a)=s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j[A_1^0\{A_2^1/x_2\}[m_3/x_3]/x_1][A_2^1[m_3/x_3]/x_2][m_3/x_3] \\ &\equiv o_3 \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_3(a)=s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j[A_1^0\{A_2^1/x_2\}/x_1][A_2^1/x_2][m_3/x_3] \\ &= \left(o_3 \cdot \star \oplus \bigoplus_{\substack{a\in A \\ f_3(a)=s_j}} p_a \cdot a \cdot \tfrac{1}{p_a} x_j[A_1^0\{A_2^1/x_2\}/x_1][A_2^1/x_2] \right)[m_3/x_3]. \end{aligned}$$

So we have proved

$$m_3 \equiv A_3^2 = A_3^3 = \langle\!\langle s_3 \rangle\!\rangle.$$

This implies that

$$m_2 \equiv A_2^1[m_3/x_3] \equiv A_2^1[A_3^2/x_3] = A_2^1\{A_3^2/x_3\} = A_2^3 = \langle\!\langle s_2 \rangle\!\rangle,$$

where the third step holds since the bound variables x_1 and x_2 of A_2^1 are also bound in A_3^2. Similarly, we have

$$\begin{aligned} m_1 &\equiv A_1^0\{A_2^1/x_2\}[m_3/x_3] \\ &\equiv A_1^0\{A_2^1/x_2\}[A_3^2/x_3] \\ &= A_1^0\{A_2^1/x_2\}\{A_3^2/x_3\} = A_1^3 = \langle\!\langle s_1 \rangle\!\rangle. \end{aligned}$$

□

Corollary A.3 *The bialgebra* $(\mathsf{Exp}/_{\equiv}, \mathbf{a}_{\equiv}, d)$ *is final among the locally finite bialgebras for the monad* $\mathcal{D}_\omega$ *and functor* $G = [0,1] \times -$.

We are now ready to prove that $out_{\equiv}$, the unique coalgebra homomorphism from $(\mathsf{Exp}/_{\equiv}, d)$ into the final coalgebra, is injective.

Proof. [Proof of Lemma 5.10] First we note that the final G-coalgebra $[0,1]^{A^*}$ has a $\mathcal{D}_\omega$ structure and that $out_{\equiv}$ is a bialgebra homomorphism [Bar, Theorem 3.2.3]. We then factorize the map $out_{\equiv}$ into an epimorphism followed by a monomorphism:

$$\begin{tikzcd}
\mathcal{D}_\omega(\mathsf{Exp}/_{\equiv}) \arrow[r, two heads, "\mathcal{D}_\omega e"] \arrow[d] & \mathcal{D}_\omega(I) \arrow[r, "\mathcal{D}_\omega m"] \arrow[d] & \mathcal{D}_\omega([0,1]^{A^*}) \arrow[d] \\
\mathsf{Exp}/_{\equiv} \arrow[r, two heads, "e"] \arrow[d] & I \arrow[r, tail, "m"] \arrow[d] & {[0,1]^{A^*}} \arrow[d] \\
G\mathsf{Exp}/_{\equiv} \arrow[r] & GI \arrow[r] & G[0,1]^{A^*}
\end{tikzcd}$$

Note that factorizations in **Sets** carry on to categories of coalgebras. This equips the image I from the factorization in **Sets** with a coalgebra structure, such that e is a coalgebra homomorphism. Furthermore, since $\mathcal{D}_\omega$ (like any functor on **Sets**) preserves surjections, there is a $\mathcal{D}_\omega$-algebra on I making e an algebra homomorphism as well. Thus I is also a bialgebra in the same category, and it is also final. Since, by Corollary A.3 we have that $\mathsf{Exp}/_{\equiv}$ is final, we can conclude that the map e is an isomorphism and, therefore, $out_{\equiv}$ is injective. $\square$

B Axioms

For completeness sake, we present to this end the general axioms (in terms of $\bigoplus$ instead of binary plus). The relation $\equiv \subseteq \mathsf{Exp} \times \mathsf{Exp}$, written infix-style, is the least equivalence relation satisfying the following axioms (and rules):

$$\begin{array}{lll}
\bigoplus_{i\in I} p_i \cdot \mathsf{F}_i \equiv \bigoplus_{i\in I} p_{\sigma(i)} \cdot \mathsf{F}_{\sigma(i)}, & \text{for } \sigma{:}I \to I \text{ a permutation} & (\mathit{Perm}) \\
\mu x.\mathsf{E} \equiv \mathsf{E}[\mu x.\mathsf{E}/x] & & (\mathit{FP}) \\
\gamma[\mathsf{E}/x] \equiv \mathsf{E} \Rightarrow \mu x.\gamma \equiv \mathsf{E} & & (\mathit{UFP}) \\
\mu x.\mathsf{E} \equiv \mu y.\mathsf{E}[y/x] & \text{if } y \text{ is not free in } \mathsf{E} & (\alpha - \mathit{equiv}) \\
\mathsf{E}_1 \equiv \mathsf{E}_2 \Rightarrow \mathsf{E}[\mathsf{E}_1/x] \equiv \mathsf{E}[\mathsf{E}_2/x] & & (\mathit{Cong})
\end{array}$$

$$\bigoplus_{i\in I} p_i \cdot \mathsf{F}_i \equiv \bigoplus_{j\in J} q_j \cdot \mathsf{F}'_j, \quad \begin{array}{l} \text{for } J \subseteq I, \\ p_i = 0 \text{ for all } i \in I\backslash J, \\ \text{and for } j \in J,\, q_j = p_j, \mathsf{F}'_j = \mathsf{F}_j \end{array} \tag{Z}$$

$$\bigoplus_{i\in I} p_i \cdot \mathsf{F}_i \equiv \bigoplus_{j\in J} q_j \cdot \mathsf{F}'_j, \quad \begin{array}{l} \text{for } J \subset I, \text{ and } j_1 \in J \text{ is such that} \\ \text{for all } i \in I\backslash J,\, \mathsf{F}_i = \mathsf{F}_{j_1}, \\ \text{for } j \neq j_1,\, q_j = p_j, \mathsf{F}'_j = F_j \\ \text{and } q_{j_1} = \sum_{i\in I\backslash J \cup \{j_1\}} p_i,\, F'_{j_1} = F_{j_1} \end{array} \tag{S}$$

$$\bigoplus_{i\in I} p_i \cdot a_i \cdot \mathsf{E}_i \equiv \bigoplus_{j\in J} q_j \cdot b_j \cdot \mathsf{E}'_j, \quad \begin{array}{l} \text{for } J = I, \text{ and } j_1 \in J \text{ is such that} \\ \text{for } j \neq j_1,\, q_j = p_j, b_j = a_j, \mathsf{E}'_j = \mathsf{E}_j \\ q_{j_1} = p \in [0,1], b_{j_1} = a_{j_1}, \text{ and} \\ \mathsf{E}'_{j_1} = \frac{p_{j_1}}{p}\mathsf{E}_{j_1} \text{ such that} \\ \sum_{j\in J} q_j \leqslant 1 \text{ and } \frac{p_{j_1}}{p}\mathsf{E}_{j_1} \text{ is defined} \end{array} \tag{M}$$

$$\bigoplus_{i\in I} p_i \cdot \mathsf{F}_i \equiv \bigoplus_{j\in J} q_j \cdot \mathsf{F}'_j, \quad \begin{array}{l} \text{for } J \subset I, \text{ and } j_1 \in J \text{ such that} \\ \text{for } j \neq j_1,\, q_j = p_j, \mathsf{F}'_j = \mathsf{F}_j \\ \text{for all } i \in I\backslash J \cup \{j_1\},\, F_i = a \cdot \bigoplus_{k\in K} p_{i,k} \cdot F_{i,k} \\ \text{with } \sum_{i\in I\backslash J\cup\{j_1\}} \sum_{k\in K} p_{i,k} \leqslant 1 \\ \text{and } q_{j_1} = p_{j_1}, F_{j_1} = a \cdot \bigoplus_{\substack{i\in I\backslash J\cup\{j_1\} \\ k\in K}} p_{i,k} \cdot F_{i,k} \end{array} \tag{D}$$