Reasoning about Probabilistic Programs using Coalgebra

Codrin Iftode

Radboud University

January 20, 2026

Goal

Goal: reason about **probabilistic imperative programs**

Goal

Goal: reason about **probabilistic imperative programs**

Main paper, by Różowski and Silva, 2023 [1]: reason about **simple** probabilistic programs, **generically**

Goal

Goal: reason about **probabilistic imperative programs**

Main paper, by Różowski and Silva, 2023 [1]: reason about **simple** probabilistic programs, **generically**

Second paper, by Rutten, 2000 [2]: 'generically'

Context

A *language* is a function $A^* \to \mathbb{B}$.

ϵ	a	aa	aaa	...
false	**true**	**true**	**true**	...

Context

A *language* is a function $A^* \to \mathbb{B}$.

ϵ	a	aa	aaa	...
false	**true**	**true**	**true**	...

A language is *regular* if recognised by either:

Regular Expression (RE): $a \,;\, (a^*)$

Context

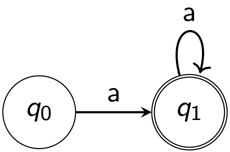
A *language* is a function $A^* \to \mathbb{B}$.

ϵ	a	aa	aaa	...
false	**true**	**true**	**true**	...

A language is *regular* if recognised by either:

Regular Expression (RE): $a\,;(a^*)$

Deterministic Finite Automaton (DFA):



Context

A *language* is a function $A^* \to \mathbb{B}$.

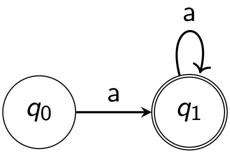
ϵ	a	aa	aaa	...
false	**true**	**true**	**true**	...

A language is *regular* if recognised by either:

Regular Expression (RE): $a\,;(a^*)$

$\updownarrow$ Kleene's Theorem

Deterministic Finite Automaton (DFA):



Context (2)

Is $a \,;\, a^*$ the same as $a^* \,;\, a$?
We want a reasoning system, i.e. an equivalence relation $\equiv$ with:

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

See e.g. Salomaa [3].

Probablistic Languages

A *probabilistic language* is a function $A^* \to [0,1]$.

ϵ	a	aa	aaa	$\ldots$
0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\ldots$

Probablistic Languages

A *probabilistic language* is a function $A^* \to [0, 1]$.

ϵ	a	aa	aaa	$\dots$
0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\dots$

'Probabilistic' Regular Expression (PRE)?

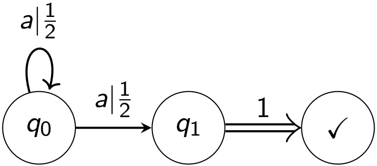
Probablistic Languages

A *probabilistic language* is a function $A^* \to [0,1]$.

ϵ	a	aa	aaa	...
0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	...

'Probabilistic' Regular Expression (PRE)?

Generative Probabilistic Transition System (GPTS):



Probablistic Languages

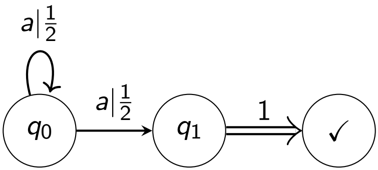
A *probabilistic language* is a function $A^* \to [0,1]$.

ϵ	a	aa	aaa	...
0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	...

'Probabilistic' Regular Expression (PRE)?

$\updownarrow$ Probabilistic Kleene's Theorem?

Generative Probabilistic Transition System (GPTS):



Probablistic Languages

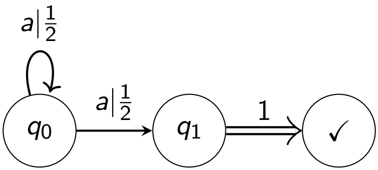
A *probabilistic language* is a function $A^* \to [0, 1]$.

ϵ	a	aa	aaa	...
0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	...

Probabilistic Regular Expression (PRE)

$\updownarrow$ Probabilistic Kleene's Theorem

Generative Probabilistic Transition System (GPTS):



Soundness and Completeness

Do we have a reasoning system?

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

Soundness and Completeness

We have a reasoning system!

$$e \equiv f \quad \xrightarrow{\text{soundness}} \quad [\![e]\!] = [\![f]\!]$$

$$e \equiv f \quad \xleftarrow[\text{completeness}]{} \quad [\![e]\!] = [\![f]\!]$$

Structure

1. Coalgebra
2. Probabilistic Regular Expressions
3. Language equivalence
4. Soundness
5. Completeness

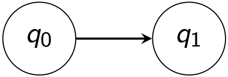
Coalgebras

An *F-coalgebra* is a function $S \xrightarrow{\beta} F(S)$.

Intuition: S is a set of states, β encodes transitions.

Coalgebras

Determinstic:

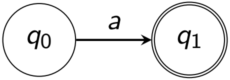


$S \xrightarrow{\beta} S$

$\beta(q_0) = q_1$

Coalgebras

DFA:

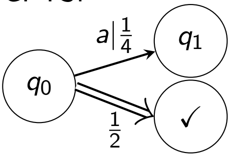


$S \xrightarrow{\beta} \mathbb{B} \times (A \Rightarrow S)$

$\beta(q_0) = (\textbf{false}, a \mapsto q_1)$
$\beta(q_1) = (\textbf{true}, \_ \mapsto q_1)$

Coalgebras

GPTS:

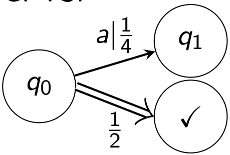


$S \xrightarrow{\beta} ((1 + A \times S) \Rightarrow [0,1])$

$\beta(q_0)(a, q_1) = \frac{1}{4}$
$\beta(q_0)(\checkmark) = \frac{1}{2}$

Coalgebras

GPTS:



$S \xrightarrow{\beta} \mathcal{D}(1 + A \times S)$

$\beta(q_0)(a, q_1) = \frac{1}{4}$
$\beta(q_0)(\checkmark) = \frac{1}{2}$

where $\mathcal{D}X$ is the set of maps $f : X \to [0,1]$ with $\sum_{x \in X} f(x) \leq 1$.

Coalgebra Homomorphism

A coalgebra *homomorphism* from $\beta : S \to FS$ to $\gamma : R \to FR$ is a map $f : S \to R$ such that the square commutes:

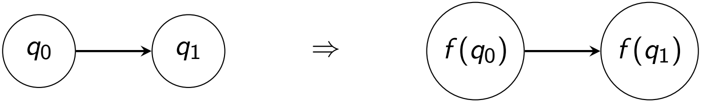
$$\begin{array}{ccc} S & \xrightarrow{f} & R \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ FS & \xrightarrow[Ff]{} & FR \end{array}$$

Coalgebra Homomorphism

A coalgebra *homomorphism* from $\beta : S \to FS$ to $\gamma : R \to FR$ is a map $f : S \to R$ such that the square commutes:

$$\begin{array}{ccc} S & \xrightarrow{f} & R \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ FS & \xrightarrow[Ff]{} & FR \end{array}$$

Intuition: f preserves 'transition structure'.



Probabilistic Regular Expressions (PRE)

For an alphabet A, and $p \in [0,1]$, define

$$e, f \in \text{Exp} ::= 0 \mid 1 \mid a \in A \mid e \oplus_p f \mid e \,;\, f \mid e^{[p]}$$

$$a \oplus_{\frac{1}{3}} b$$

$$a \,;\, a^{[\frac{1}{2}]}$$

Progress

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

Operational Semantics of PREs

Defining $[\![-]\!] : \mathsf{Exp} \to (A^* \Rightarrow [0, 1])$ directly is hard.

Operational Semantics of PREs

Defining $[\![-]\!] : \mathsf{Exp} \to (A^* \Rightarrow [0,1])$ directly is hard.

First define operational semantics $\partial : \mathsf{Exp} \to \mathcal{D}(1 + A \times \mathsf{Exp})$.

Operational Semantics of PREs

Defining $[\![-]\!] : \mathsf{Exp} \to (A^* \Rightarrow [0,1])$ directly is hard.

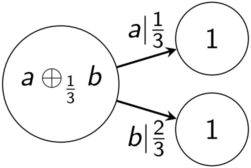
First define operational semantics $\partial : \mathsf{Exp} \to \mathcal{D}(1 + A \times \mathsf{Exp})$.

$$a \oplus_{\frac{1}{3}} b$$

Operational Semantics of PREs

Defining $[\![-]\!] : \mathsf{Exp} \to (A^* \Rightarrow [0,1])$ directly is hard.

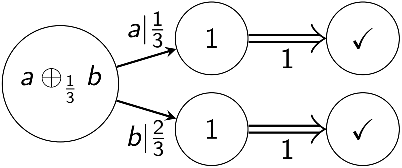
First define operational semantics $\partial : \mathsf{Exp} \to \mathcal{D}(1 + A \times \mathsf{Exp})$.



Operational Semantics of PREs

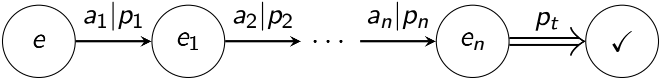
Defining $[\![-]\!] : \mathsf{Exp} \to (A^* \Rightarrow [0,1])$ directly is hard.

First define operational semantics $\partial : \mathsf{Exp} \to \mathcal{D}(1 + A \times \mathsf{Exp})$.



Operational gives Denotational

Recall: $[\![e]\!]$ assigns a probability to each word $a_1 a_2 \dots a_n$.



Semantics via Final Coalgebra

A coalgebra $\omega : \Omega \to F\Omega$ is *final* if for any coalgebra $\beta : S \to FS$ there is a unique homomorphism $\dagger\beta : S \to \Omega$.

$$\begin{array}{ccc} S & \overset{\dagger\beta}{\dashrightarrow} & \Omega \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\omega} \\ FS & \xrightarrow[F(\dagger\beta)]{} & F\Omega \end{array}$$

Semantics via Final Coalgebra

$$\begin{array}{ccc} S & \overset{\dagger\beta}{\dashrightarrow} & \Omega \\ {\scriptstyle\beta}\big\downarrow & & \\ FS & & \end{array}$$

Semantics via Final Coalgebra

$$
\begin{array}{ccc}
S & \xrightarrow{[\![-]\!]} & A^* \Rightarrow \mathbb{B} \\
{\scriptstyle \beta}\downarrow & & \\
\mathbb{B} \times (A \Rightarrow S) & &
\end{array}
$$

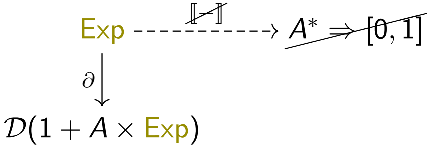
Semantics via Final Coalgebra

$$\begin{array}{ccc} \mathsf{Exp} & \overset{[\![-]\!]?}{\dashrightarrow} & A^* \Rightarrow [0,1] \\ \partial \downarrow & & \\ \mathcal{D}(1 + A \times \mathsf{Exp}) & & \end{array}$$

Semantics via Final Coalgebra

$$
\begin{array}{ccc}
\mathsf{Exp} & \overset{[\![-]\!]}{\dashrightarrow} & A^* \Rightarrow [0,1] \\
\Big\downarrow \partial & & \\
\mathcal{D}(1 + A \times \mathsf{Exp}) & &
\end{array}
$$

Semantics via Final Coalgebra



$A^* \Rightarrow [0,1]$ is **not** the final coalgebra for functor $\mathcal{D}(1 + A \times (-))$.

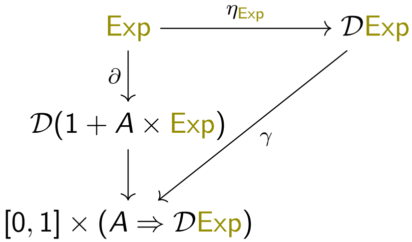
Reason: GPTS is nondeterministic.

Solution: determinisation [4].

Determinisation

$$\begin{array}{c} \mathsf{Exp} \\ \downarrow{\scriptstyle \partial} \\ \mathcal{D}(1 + A \times \mathsf{Exp}) \\ \downarrow \\ [0,1] \times (A \Rightarrow \mathcal{D}\mathsf{Exp}) \end{array}$$

Determinisation



Determinisation

$$\begin{array}{ccccc} \mathsf{Exp} & \xrightarrow{\eta_{\mathsf{Exp}}} & \mathcal{D}\mathsf{Exp} & \overset{\dagger\gamma}{\dashrightarrow} & A^* \Rightarrow [0,1] \\ \partial\downarrow & \swarrow\gamma & & & \\ \mathcal{D}(1 + A \times \mathsf{Exp}) & & & & \\ \downarrow & & & & \\ [0,1] \times (A \Rightarrow \mathcal{D}\mathsf{Exp}) & & & & \end{array}$$

Determinisation

$$\mathsf{Exp} \xrightarrow{\eta_{\mathsf{Exp}}} \mathcal{D}\mathsf{Exp} \xrightarrow{\dagger\gamma} A^* \Rightarrow [0,1]$$

$$\mathsf{Exp} \xrightarrow{[\![-]\!]} A^* \Rightarrow [0,1]$$

See [5] for a proof.

Progress

$$e \equiv f \quad \xrightarrow{\text{soundness}} \quad [\![e]\!] = [\![f]\!]$$

$$e \equiv f \quad \xleftarrow[\text{completeness}]{} \quad [\![e]\!] = [\![f]\!]$$

Language Equivalence

Probabilistic Choice

$e \equiv e \oplus_p e$

$e \oplus_p f \equiv f \oplus_{1-p} e$

$\dots$

Sequencing

$1; e \equiv e$

$e; (f; g) \equiv (e; f); g$

$\dots$

Distributivity

$(e \oplus_p f); g \equiv (e; g) \oplus_p (f; g)$

Loops

$e; e^{[p]} \oplus_p 1 \equiv e^{[p]}$

$\dots$

Fixpoint rule

$$\frac{g \equiv e; g \oplus_p f \quad E(e) = 0}{g \equiv e^{[p]}; f}$$

$\dots$

Soundness and Completeness

$$e \equiv f \quad \xrightarrow{\text{soundness}} \quad [\![e]\!] = [\![f]\!]$$

$$e \equiv f \quad \xleftarrow[\text{completeness}]{} \quad [\![e]\!] = [\![f]\!]$$

Soundness and Completeness

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

Suppose we could write $[\![-]\!]$ as the composition:

$$\mathrm{Exp} \xrightarrow{[-]} \mathrm{Exp}/\equiv \xrightarrow{\dagger d} A^* \Rightarrow [0,1]$$

Soundness and Completeness

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

Suppose we could write $[\![-]\!]$ as the composition:

$$\text{Exp} \xrightarrow{[-]} \text{Exp}/\equiv \xrightarrow{\dagger d} A^* \Rightarrow [0,1]$$

Then, soundness:

$$\begin{aligned} &e \equiv f \\ \Rightarrow\ &[e] = [f] \\ \Rightarrow\ &\dagger d([e]) = \dagger d([f]) \\ \Rightarrow\ &[\![e]\!] = [\![f]\!] \end{aligned}$$

Soundness and Completeness

$$e \equiv f \quad \overset{\text{soundness}}{\Longrightarrow} \quad [\![e]\!] = [\![f]\!]$$

$$e \equiv f \quad \underset{\text{completeness}}{\Longleftarrow} \quad [\![e]\!] = [\![f]\!]$$

Suppose we could write $[\![-]\!]$ as the composition:

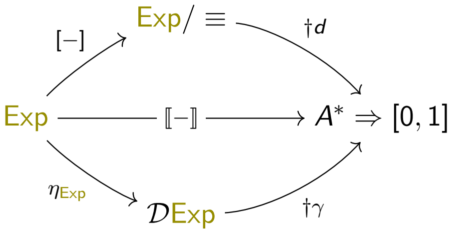
$$\mathrm{Exp} \xrightarrow{[-]} \mathrm{Exp}/\equiv \xrightarrow{\dagger d} A^* \Rightarrow [0,1]$$

Also completeness, if $\dagger d$ is **injective**:

$$\begin{aligned} & e \equiv f \\ \Leftarrow\ & [e] = [f] \\ \Leftarrow\ & \dagger d([e]) = \dagger d([f]) \\ \Leftarrow\ & [\![e]\!] = [\![f]\!] \end{aligned}$$

Soundness

For soundness, remains to show two maps are equal:



Soundness Idea

We know $\dagger\gamma$ is the **unique** homomorphism $\mathcal{D}\mathsf{Exp} \to (A^* \Rightarrow [0,1])$.
So if we build a coalgebra homomorphism:

$$\mathcal{D}\mathsf{Exp} \longrightarrow \ldots \longrightarrow A^* \Rightarrow [0,1]$$

it must be equal to $\dagger\gamma$.

Soundness Idea

We build such a coalgebra homomorphism:

$$\mathcal{D}\mathsf{Exp} \xrightarrow{\mathcal{D}[-]_{\equiv_0}} \mathcal{D}\mathsf{Exp}/{\equiv_0} \xrightarrow{\alpha_0} \mathsf{Exp}/{\equiv_0} \xrightarrow{[-]_{\equiv}} \mathsf{Exp}/{\equiv} \xrightarrow{\dagger d} A^* \Rightarrow [0,1]$$

$\equiv_0$ is the same as $\equiv$, but without two axioms.

Can we quotient coalgebras?

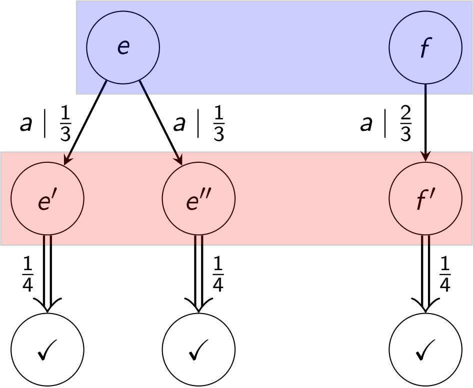
Does the quotient $\mathsf{Exp}/\equiv_0$ have a coalgebra structure?

Can we quotient coalgebras?

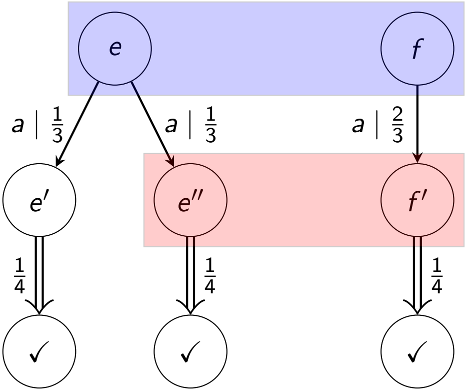
Does the quotient $\mathsf{Exp}/{\equiv_0}$ have a coalgebra structure?

Yes, since $\equiv_0$ is a **bisimulation** equivalence (Lemma 6.1 [1]).

GPTS Bisimulation Equivalence Example



GPTS Bisimulation Equivalence Anti-Example



Quotienting with a Bisimulation Equivalence

Proposition 5.8 [2]: The quotient of a coalgebra with a bisimulation equivalence is a coalgebra.

$$\begin{array}{ccc} S & \xrightarrow{[-]_R} & S/R \\ {\scriptstyle \beta_S}\downarrow & & \\ FS & & \end{array}$$

Quotienting with a Bisimulation Equivalence

Proposition 5.8 [2]: The quotient of a coalgebra with a bisimulation equivalence is a coalgebra.

$$
\begin{array}{ccc}
S & \xrightarrow{[-]_R} & S/R \\
{\scriptstyle \beta_S}\downarrow & & \downarrow{\scriptstyle \beta} \\
FS & \xrightarrow[F[-]_R]{} & F(S/R)
\end{array}
$$

Quotienting with a Bisimulation Equivalence

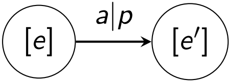
Proposition 5.8 [2]: The quotient of a coalgebra with a bisimulation equivalence is a coalgebra.

$$\begin{array}{ccc} \mathsf{Exp} & \xrightarrow{[-]_{\equiv_0}} & \mathsf{Exp}/{\equiv_0} \\ {\scriptstyle \partial}\downarrow & & \downarrow{\scriptstyle \beta} \\ \mathcal{D}(1 + A \times \mathsf{Exp}) & \xrightarrow[F[-]_{\equiv_0}]{} & \mathcal{D}(1 + A \times \mathsf{Exp}/{\equiv_0}) \end{array}$$

Quotienting with a Bisimulation Equivalence

Proposition 5.8 [2]: The quotient of a coalgebra with a bisimulation equivalence is a coalgebra.

$$\begin{array}{ccc}
\mathsf{Exp} & \xrightarrow{[-]_{\equiv_0}} & \mathsf{Exp}/{\equiv_0} \\
\Big\downarrow \partial & & \Big\downarrow \beta \\
\mathcal{D}(1 + A \times \mathsf{Exp}) & \xrightarrow[F[-]_{\equiv_0}]{} & \mathcal{D}(1 + A \times \mathsf{Exp}/{\equiv_0})
\end{array}$$

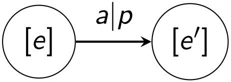


iff $p = \sum_{e \xrightarrow{a|q} f \equiv_0 e'} q$

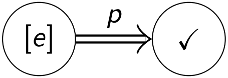
Quotienting with a Bisimulation Equivalence

Proposition 5.8 [2]: The quotient of a coalgebra with a bisimulation equivalence is a coalgebra.

$$\begin{array}{ccc} \mathsf{Exp} & \xrightarrow{[-]_{\equiv_0}} & \mathsf{Exp}/\equiv_0 \\ \downarrow \partial & & \downarrow \beta \\ \mathcal{D}(1 + A \times \mathsf{Exp}) & \xrightarrow[F[-]_{\equiv_0}]{} & \mathcal{D}(1 + A \times \mathsf{Exp}/\equiv_0) \end{array}$$



iff $p = \sum_{e \xrightarrow{a|q} f \equiv_0 e'} q$



iff $e \stackrel{p}{\Longrightarrow} \checkmark$

Completeness

We want $\dagger d : \text{Exp}/{\equiv} \to (A^* \Rightarrow [0,1])$ to be injective:

$$
\begin{aligned}
& e \equiv f \\
\Leftarrow\ & [e] = [f] \\
\Leftarrow\ & \dagger d([e]) = \dagger d([f]) \\
\Leftarrow\ & [\![e]\!] = [\![f]\!]
\end{aligned}
$$

Completeness Overview

$\mathsf{Exp}/\!\equiv$ also has algebra structure $\mathcal{D}\mathsf{Exp}/\!\equiv \xrightarrow{\alpha} \mathsf{Exp}/\!\equiv$.

Completeness Overview

Exp$/\equiv$ also has algebra structure $\mathcal{D}$Exp$/\equiv \xrightarrow{\alpha}$ Exp$/\equiv$.

We can lift functor $[0,1] \times (A \Rightarrow -)$ to $\mathcal{D}$-algebras, and restrict it to a functor $\hat{G}$ whose coalgebras, when determinised, correspond to GPTS.

Completeness Overview

$\mathsf{Exp}/{\equiv}$ also has algebra structure $\mathcal{D}\mathsf{Exp}/{\equiv} \xrightarrow{\alpha} \mathsf{Exp}/{\equiv}$.

We can lift functor $[0,1] \times (A \Rightarrow -)$ to $\mathcal{D}$-algebras, and restrict it to a functor $\hat{G}$ whose coalgebras, when determinised, correspond to GPTS.

$\mathsf{Exp}/{\equiv}$ is the **rational fixpoint** of $\hat{G}$; here, a subcoalgebra of its final coalgebra $\Omega_{\hat{G}}$:

$$\mathsf{Exp}/{\equiv} \hookrightarrow \Omega_{\hat{G}} \hookrightarrow (A^* \Rightarrow [0,1])$$

$$=$$

$$\mathsf{Exp}/{\equiv} \xrightarrow{\dagger d} (A^* \Rightarrow [0,1])$$

Conclusion

$$e \equiv f \quad \underset{\text{completeness}}{\overset{\text{soundness}}{\rightleftarrows}} \quad [\![e]\!] = [\![f]\!]$$

We have PREs, and a sound and complete system for reasoning about equivalence.

References

[1] Różowski, W. and Silva, A. (2024). A completeness theorem for probabilistic regular expressions. In *Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '24, New York, NY, USA. Association for Computing Machinery.

[2] Rutten, J. (2000). Universal coalgebra: a theory of systems. *Theoretical Computer Science*, 249(1):3–80. Modern Algebra.

[3] Salomaa, A. (1966). Two complete axiom systems for the algebra of regular events. *J. ACM*, 13(1):158–169.

[4] Silva, A., Bonchi, F., Bonsangue, M. M., and Rutten, J. J. M. M. (2010). Generalizing the powerset construction, coalgebraically. In Lodaya, K. and Mahajan, M., editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 272–283, Dagstuhl, Germany. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[5] Silva, A. and Sokolova, A. (2011). Sound and complete axiomatization of trace semantics for probabilistic systems. *Electronic Notes in Theoretical Computer Science*, 276:291–311. Twenty-seventh Conference on the Mathematical Foundations of Programming Semantics (MFPS XXVII).