General Framework for Probabilistic Characteristic Formulae

Joshua Sack[1], Lijun Zhang[2]

Philadelphia Jan 22, 2012

[1]California State University Long Beach
[2]Danish Technical University

Verifying Correctness of Reactive Systems

Equivalence/Preorder Checking

$$Impl \equiv Spec$$

- $\equiv$ is a 'behavioral' equivalence/preorder,
- *Spec* is expressed in the same language as *Impl*—typically in terms of (a language for describing) automata
- *Spec* provides the (full) specification of the intended behavior

Model Checking

$$Impl \models Property$$

- $\models$ is the satisfaction relation
- *Property* is a (partial) specification of the intended behavior, often expressed in a modal or temporal logic

Verifying Correctness of Reactive Systems

Equivalence/Preorder Checking

$$Impl \equiv Spec$$

- $\equiv$ is a 'behavioral' equivalence/preorder,
- *Spec* is expressed in the same language as *Impl*—typically in terms of (a language for describing) automata
- *Spec* provides the (full) specification of the intended behavior

Model Checking

$$Impl \models Property$$

- $\models$ is the satisfaction relation
- *Property* is a (partial) specification of the intended behavior, often expressed in a modal or temporal logic

Characteristic Formulae: A Bridge Between the Worlds

Characteristic Formulae

A characteristic formula for *Spec* modulo $\equiv$ is a formula $F(Spec)$ such that, for each *Impl*,

$$Impl \equiv Spec \text{ iff } Impl \models F(Spec) \ .$$

The Role of Characteristic Formulae

- Using characteristic-formula constructions one can effectively reduce implementation verification to model checking.

Characteristic Formulae: A Bridge Between the Worlds

Characteristic Formulae

A characteristic formula for *Spec* modulo $\equiv$ is a formula $F(Spec)$ such that, for each *Impl*,

$$Impl \equiv Spec \text{ iff } Impl \models F(Spec) \ .$$

The Role of Characteristic Formulae

- Using characteristic-formula constructions one can effectively reduce implementation verification to model checking.

Other uses of characteristic formulae

Expressivity

Being able to characterize certain properties of relations, such as equivalence classes, in the language is a measure of expressivity.

Completeness and decidability

Some modal completeness and decidability theorems can be proved by constructing a finite satisfying model whose elements are canonical formulae.

Other uses of characteristic formulae

Expressivity

Being able to characterize certain properties of relations, such as equivalence classes, in the language is a measure of expressivity.

Completeness and decidability

Some modal completeness and decidability theorems can be proved by constructing a finite satisfying model whose elements are canonical formulae.

Recent related work

- Characterising Probabilistic Processes Logically. (Deng and Glabeek, LNCS, 2010)

  Characteristic formulae for behavioral relations over probabilistic automata. Each proof has its own technique

- Characteristic formulae for fixed-point semantics: a general approach. (Aceto et al, to appear in MSCS)

  A general approach to non-probabilistic characteristic formulae. A single method for creating and proving characteristic formulae for a wide variety of behavioral relations that are defined as fixed points of suitable monotone functions.

Our Question and The Main Message

Our Motivating Question and Aim

Can the unified treatment of results in Aceto et al be adapted to a probabilistic setting?

The Message in a Bottle

Yes! We do so by bringing together

- fixed-point characterizations of probabilistic behavioral relations
  - a key difference between the probabilistic characterizations and non-probabilistic characterizations is the involvement of relation liftings,
- a two-sorted fixed-point probability logic (for probabilistic forward simulation, a one-sorted logic), and
- the main theorem in Aceto *et al* (for probabilistic forward simulation, a generalized version).

Our Question and The Main Message

Our Motivating Question and Aim

Can the unified treatment of results in Aceto et al be adapted to a probabilistic setting?

The Message in a Bottle

Yes! We do so by bringing together

- fixed-point characterizations of probabilistic behavioral relations
  - a key difference between the probabilistic characterizations and non-probabilistic characterizations is the involvement of relation liftings,
- a two-sorted fixed-point probability logic (for probabilistic forward simulation, a one-sorted logic), and
- the main theorem in Aceto *et al* (for probabilistic forward simulation, a generalized version).

Probabilistic Automata

Definition

A probability distribution over a set S is a function $\mu : S \to \mathbb{R}^{\geq 0}$, such that

- $\{s \mid \mu(s) \neq 0\}$ is countable, and
- $\sum_{s \in S} \mu(s) = 1$.

Let $Dist(S)$ be the set of all probability distributions over S.

Definition

A (non-deterministic) probabilistic automaton is a triple $\mathcal{M} = (S, Act, Steps)$, where

- S is a countable set of *states*,
- Act is a countable set of *actions*, and
- $Steps \subseteq S \times Act \times Dist(S)$ is the *transition relation*.

Probabilistic Automata

Definition

A probability distribution over a set S is a function $\mu : S \to \mathbb{R}^{\geq 0}$, such that

- $\{s \mid \mu(s) \neq 0\}$ is countable, and
- $\sum_{s \in S} \mu(s) = 1$.

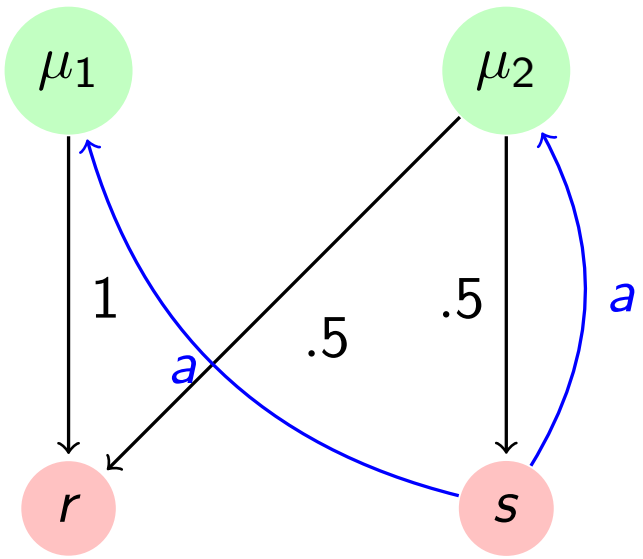
Let $Dist(S)$ be the set of all probability distributions over S.

Definition

A (non-deterministic) probabilistic automaton is a triple $\mathcal{M} = (S, Act, Steps)$, where

- S is a countable set of *states*,
- Act is a countable set of *actions*, and
- $Steps \subseteq S \times Act \times Dist(S)$ is the *transition relation*.

Example



- $S = \{r, s\}$
- $Act = \{a\}$
- *Steps* does not transition from r to any distribution, but has two transitions from s: to μ_1 and μ_2.

Relation Lifting

As our transitions are between states S and distributions $Dist(S)$, we need to *lift* binary relations from *states* to *distributions*.

Definition

Given a relation $R \subseteq X \times Y$, we define its lifting $\hat{R} \subseteq Dist(X) \times Dist(Y)$ by

$$\mu \hat{R} \nu \Leftrightarrow \forall A \subseteq Supp(\mu).\ \mu(A) \leq \nu(R(A)).$$

Other (equivalent) characterizations of liftings involve *weight functions* as are used in *Deng and van Glabeek*.

Bisimilarity given by an endofunction

Strong bisimilarity $\sim_{bisim}$ is the greatest fixed-point of the monotonic endofunction $\mathcal{F}_{bisim}(R)$ on $\mathcal{P}(S \times S)$, where for $R \subseteq S \times S$,

$$(s, t) \in \mathcal{F}_{bisim}(R)$$

iff for every $a \in Act$, both of the following hold:

1. if $s \xrightarrow{a} \mu$, then there exists some $\nu \in Dist(S)$ such that $t \xrightarrow{a} \nu$ and $(\mu, \nu) \in \hat{R}$
2. if $t \xrightarrow{a} \nu$, then there exists some $\mu \in Dist(S)$ such that $s \xrightarrow{a} \mu$ and $(\mu, \nu) \in \hat{R}$

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

Two-sorted probability logic with variables

State formulas:

$$\varphi ::= \top \mid \bot \mid X_i \mid \bigwedge_{k \in K} \varphi_k \mid \bigvee_{k \in K} \varphi_k \mid \langle a \rangle \psi \mid [a]\psi,$$

where K is a cardinal, $i \in I$ is an index set, and $a \in Act$.
Distribution formulas:

$$\psi ::= \top \mid \bot \mid \bigwedge_{k \in K} \psi_k \mid \bigvee_{k \in K} \psi_k \mid L_p(\varphi),$$

where p is some rational number.

Sample well-formed formula: $\langle a \rangle (L_p X_i \wedge L_q [a] \bot)$

Two-sorted probability logic with variables

State formulas:

$$\varphi ::= \top \mid \bot \mid X_i \mid \bigwedge_{k \in K} \varphi_k \mid \bigvee_{k \in K} \varphi_k \mid \langle a \rangle \psi \mid [a]\psi,$$

where K is a cardinal, $i \in I$ is an index set, and $a \in Act$.
Distribution formulas:

$$\psi ::= \top \mid \bot \mid \bigwedge_{k \in K} \psi_k \mid \bigvee_{k \in K} \psi_k \mid L_p(\varphi),$$

where p is some rational number.

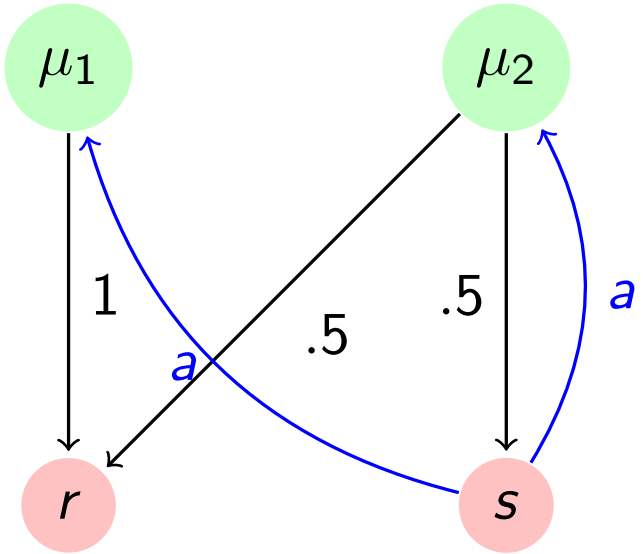
Sample well-formed formula: $\langle a \rangle (L_p X_i \wedge L_q [a] \bot)$

Basic Semantics

a variable interpretation is a function $\sigma : I \to \mathcal{P}(S)$. Select components of the semantics are given by:

$\sigma, s \models X_z$	iff $s \in \sigma(z)$
$\sigma, s \models \langle T \rangle \psi$	iff $\sigma, \mu \models \psi$ for some μ such that $sT\mu$
$\sigma, s \models [T]\psi$	iff $\sigma, \mu \models \psi$ for all μ such that $sT\mu$
$\sigma, \mu \models \mathsf{L}_p \varphi$	iff $\mu(\{s \mid \sigma, s \models \varphi\}) \geq p$

Examples of the semantics



Let $X_r \mapsto \{r\}$, $\sigma : X_s \mapsto \{s\}$.

- $\sigma, r \models [a]\bot$, but $\sigma, s \not\models [a]\bot$,
- $\sigma, s \models \langle a \rangle \mathsf{L}_{.5} X_s$, but $\sigma, s \not\models [a]\mathsf{L}_{.5} X_s$,
- $\sigma, s \models [a]\mathsf{L}_{.5} X_r$.

Involving Recursion

An endodeclaration is a function $E : I \to \mathcal{L}(I)$. An endodeclaration induces an endofunction $[\![E]\!] : \mathcal{P}(S)^I \to \mathcal{P}(S)^I$, such that

$$([\![E]\!]\sigma)(i) = \{s \mid (\sigma, s) \models E(i)\} \stackrel{\text{def}}{=} [\![E(i)]\!]\sigma$$

Key observation:

$[\![E]\!]$ is a monotone endofunction on the complete lattice of variable interpretations, and hence has a greatest and least fixed point.

Involving Recursion

An endodeclaration is a function $E : I \to \mathcal{L}(I)$. An endodeclaration induces an endofunction $[\![E]\!] : \mathcal{P}(S)^I \to \mathcal{P}(S)^I$, such that

$$([\![E]\!]\sigma)(i) = \{s \mid (\sigma, s) \models E(i)\} \stackrel{\text{def}}{=} [\![E(i)]\!]\sigma$$

Key observation:

$[\![E]\!]$ is a monotone endofunction on the complete lattice of variable interpretations, and hence has a greatest and least fixed point.

The Aceto et al theorem

Let $\Phi : \mathcal{P}(S \times S) \to \mathcal{P}(S)^S$ mapping

$\Phi : R \mapsto \sigma_R$, where $\sigma_R : s \mapsto \{t \mid sRt\}$.

Definition

An endodeclaration E expresses an endofunction $\mathcal{F}$ if for all R

$$\Phi(R), t \models E(s) \Leftrightarrow (s, t) \in \mathcal{F}(R),$$

Definition

An endodeclaration E characterizes a behavioral relation $\mathrm{gfp}\,\mathcal{F}$ if

$$\mathrm{gfp}[\![E]\!], t \models E(s) \Leftrightarrow (s, t) \in \mathrm{gfp}\,\mathcal{F}.$$

Theorem (Aceto et al)

If E expresses $\mathcal{F}$, then E characterizes $\mathrm{gfp}\,\mathcal{F}$.

The Aceto et al theorem

Let $\Phi : \mathcal{P}(S \times S) \to \mathcal{P}(S)^S$ mapping

$\Phi : R \mapsto \sigma_R$, where $\sigma_R : s \mapsto \{t \mid sRt\}$.

Definition

An endodeclaration E expresses an endofunction $\mathcal{F}$ if for all R

$$\Phi(R), t \models E(s) \Leftrightarrow (s, t) \in \mathcal{F}(R),$$

Definition

An endodeclaration E characterizes a behavioral relation $\mathrm{gfp}\,\mathcal{F}$ if

$$\mathrm{gfp}[\![E]\!], t \models E(s) \Leftrightarrow (s, t) \in \mathrm{gfp}\,\mathcal{F}.$$

Theorem (Aceto et al)

If E expresses $\mathcal{F}$, then E characterizes $\mathrm{gfp}\,\mathcal{F}$.

The Aceto et al theorem

Let $\Phi : \mathcal{P}(S \times S) \to \mathcal{P}(S)^S$ mapping

$\Phi : R \mapsto \sigma_R$, where $\sigma_R : s \mapsto \{t \mid sRt\}$.

Definition

An endodeclaration E expresses an endofunction $\mathcal{F}$ if for all R

$$\Phi(R), t \models E(s) \Leftrightarrow (s, t) \in \mathcal{F}(R),$$

Definition

An endodeclaration E characterizes a behavioral relation $\mathrm{gfp}\,\mathcal{F}$ if

$$\mathrm{gfp}[\![E]\!], t \models E(s) \Leftrightarrow (s, t) \in \mathrm{gfp}\,\mathcal{F}.$$

Theorem (Aceto et al)

If E expresses $\mathcal{F}$, then E characterizes $\mathrm{gfp}\,\mathcal{F}$.

The Aceto et al theorem

Let $\Phi : \mathcal{P}(S \times S) \to \mathcal{P}(S)^S$ mapping

$\Phi : R \mapsto \sigma_R$, where $\sigma_R : s \mapsto \{t \mid sRt\}$.

Definition

An endodeclaration E expresses an endofunction $\mathcal{F}$ if for all R

$$\Phi(R), t \models E(s) \Leftrightarrow (s, t) \in \mathcal{F}(R),$$

Definition

An endodeclaration E characterizes a behavioral relation $\mathrm{gfp}\,\mathcal{F}$ if

$$\mathrm{gfp}[\![E]\!], t \models E(s) \Leftrightarrow (s, t) \in \mathrm{gfp}\,\mathcal{F}.$$

Theorem (Aceto et al)

If E expresses $\mathcal{F}$, then E characterizes $\mathrm{gfp}\,\mathcal{F}$.

Reasoning behind the Aceto et al theorem

E expressing $\mathcal{F}$ guarantees that the following commutes:

$$\begin{tikzcd}
\mathcal{P}(S \times S) \arrow[r, "\mathcal{F}"] \arrow[d, "\Phi"'] & \mathcal{P}(S \times S) \arrow[d, "\Phi"] \\
\mathcal{P}(S)^S \arrow[r, "{[\![E]\!]}"'] & \mathcal{P}(S)^S
\end{tikzcd}$$

- Φ is an isomorphism.
- such isomorphisms map $\mathrm{gfp}\,\mathcal{F}$ to $\mathrm{gfp}[\![E]\!]$.

Then using $\mathrm{gfp}\,\mathcal{F}$ for R in expresses, we have

$$\Phi(\mathrm{gfp}\,\mathcal{F}), t \models E(s) \Leftrightarrow (s,t) \in \mathcal{F}(\mathrm{gfp}\,\mathcal{F})$$
$$\mathrm{gfp}[\![E]\!], t \models E(s) \Leftrightarrow (s,t) \in \mathrm{gfp}\,\mathcal{F}.$$

which means E characterizes $\mathrm{gfp}\,\mathcal{F}$.

bisimilarity characterized by an endodeclaration

We will see that the endodeclaration

$$E_{bisim} : s \mapsto \left(\bigwedge_{a \in Act} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)} \Big(\bigvee_{z \in A} X_z \Big) \right)$$
$$\wedge \left(\bigwedge_{a \in Act} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)} \Big(\bigvee_{z \in A} X_z \Big) \right)$$

expresses $\mathcal{F}_{bisim}$ and hence characterizes bisimilarity gfp $\mathcal{F}_{bisim}$.

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$
$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$
$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$
$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\, s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\Big(\bigvee_{z \in A} X_z\Big) \right)$$

Expressing bisimulation

By directly checking, one can see that E_{bisim} expresses $\mathcal{F}_{bisim}$.

$$\begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, "a"'] & t \arrow[d, dashed, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, dotted, no head, "\mathcal{F}_{bisim}(R)"] \arrow[d, dashed, "a"'] & t \arrow[d, "a"] \\ \mu \arrow[r, dashed, no head, "\hat{R}"'] & \nu \end{tikzcd}$$

$$E_{bisim}(p) = \left(\bigwedge_{a \in \mathbf{A}} \bigwedge_{\mu.\ s \xrightarrow{a} \mu} \langle a \rangle \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\left(\bigvee_{z \in A} X_z \right) \right)$$

$$\wedge \left(\bigwedge_{a \in \mathbf{A}} [a] \bigvee_{\mu.\ s \xrightarrow{a} \mu} \bigwedge_{A \subseteq Supp(\mu)} \mathsf{L}_{\mu(A)}\left(\bigvee_{z \in A} X_z \right) \right)$$

Applications

Modifications of the language allow us to apply this setting to

- probabilistic bisimulation (using "combined transition" and infinitary formulae)
- weak bisimulation (using "weak transitions")

But there there is a setting that requires further generalization:

- probabilistic forward simulation (which relate states to distributions)

Applications

Modifications of the language allow us to apply this setting to

- probabilistic bisimulation (using "combined transition" and infinitary formulae)
- weak bisimulation (using "weak transitions")

But there there is a setting that requires further generalization:

- probabilistic forward simulation (which relate states to distributions)

Applications

Modifications of the language allow us to apply this setting to

- probabilistic bisimulation (using "combined transition" and infinitary formulae)
- weak bisimulation (using "weak transitions")

But there there is a setting that requires further generalization:

- probabilistic forward simulation (which relate states to distributions)

Weak transitions and lifted distributions

Probabilistic forward simulations make use of weak transitions:

Let $Act_\tau = Act \cup \{\tau\}$, where τ is a silent transition.

A weak transition $\mu \overset{a}{\Rightarrow} \nu$ is a transition that makes an a-transition preceded or followed by arbitrarily many τ transitions.

(These transitions are derived from the original probabilistic automata using certain type of relation lifting.)

Definition (lifted distribution)

Given a distribution $\mu \in Dist(S)$, we define $\breve{\mu} \in Dist(Dist(S))$ by

$$\breve{\mu}(\nu) = \begin{cases} \mu(s) & \nu = \delta_s \\ 0 & \text{otherwise} \end{cases} .$$

Weak transitions and lifted distributions

Probabilistic forward simulations make use of weak transitions:

Let $Act_\tau = Act \cup \{\tau\}$, where τ is a silent transition.

A weak transition $\mu \overset{a}{\Rightarrow} \nu$ is a transition that makes an a-transition preceded or followed by arbitrarily many τ transitions.

(These transitions are derived from the original probabilistic automata using certain type of relation lifting.)

Definition (lifted distribution)

Given a distribution $\mu \in Dist(S)$, we define $\breve{\mu} \in Dist(Dist(S))$ by

$$\breve{\mu}(\nu) = \begin{cases} \mu(s) & \nu = \delta_s \\ 0 & \text{otherwise} \end{cases} .$$

Probabilistic forward simulation

Probabilistic forward similarity is the greatest fixed point of $F_{\underset{\approx}{\prec}^f}$ mapping

$$R \mapsto \{(s,\mu) \in S \times Dist(S) \mid \forall a \in Act_\tau.\ \forall s \xrightarrow{a} \nu.\ \exists \mu'.\mu \overset{\hat{a}}{\Rightarrow} \mu' : \nu \hat{R} \breve{\mu}'\}$$

$$\begin{tikzcd}
s \arrow[r, dotted, no head, "\mathcal{F}_{\underset{\approx}{\prec}^f}(R)"] \arrow[d, "a"'] & \mu \arrow[d, equal] \arrow[d, Rightarrow, "a"] \\
\nu \arrow[r, dashed, no head, "\hat{R}"'] & \breve{\mu}', \mu'
\end{tikzcd}$$

Modified theory

A new definition of *expresses* guarantees the following commutes:

$$\begin{tikzcd}
\mathcal{P}(S \times P) \arrow[r, "F_{\underset{\approx}{\prec} f}"] \arrow[d, "\Phi"'] & \mathcal{P}(S \times P) \arrow[d, "\Phi"] \\
\mathcal{P}(P)^S \arrow[r, "g"'] & \mathcal{P}(P)^S
\end{tikzcd}$$

Let $P = Dist(S)$. We

- changed $\mathcal{P}(S \times S)$ to $\mathcal{P}(S \times P)$
- changed $\mathcal{P}(S)^S$ to $\mathcal{P}(P)^S$.
- define $\Phi(R)$ by $\Phi(R)(s) = \{\mu \mid (s, \mu) \in R\}$.

But what is g? It will have to be defined over distributions.

Modified theory

A new definition of *expresses* guarantees the following commutes:

$$\begin{tikzcd}
\mathcal{P}(S \times P) \arrow[r, "F_{\underset{\approx}{\prec} f}"] \arrow[d, "\Phi"'] & \mathcal{P}(S \times P) \arrow[d, "\Phi"] \\
\mathcal{P}(P)^S \arrow[r, "g"'] & \mathcal{P}(P)^S
\end{tikzcd}$$

Let $P = Dist(S)$. We

- changed $\mathcal{P}(S \times S)$ to $\mathcal{P}(S \times P)$
- changed $\mathcal{P}(S)^S$ to $\mathcal{P}(P)^S$.
- define $\Phi(R)$ by $\Phi(R)(s) = \{\mu \mid (s, \mu) \in R\}$.

But what is g? It will have to be defined over distributions.

New language

Define formulas (all) interpreted over distributions, by

$$\varphi ::= X_z \mid \top \mid \bot \mid \bigwedge_{k \in K} \varphi_k \mid \bigvee_{k \in K} \varphi_k \mid \langle \overset{a}{\Rightarrow} \rangle \varphi \mid [\overset{a}{\Rightarrow}] \varphi \mid \mathsf{L}_p \varphi$$

where

$z \in S$

$a \in Act_\tau$

Define a variable interpretation $\sigma : S \to \mathcal{P}(P)$, where $P = Dist(S)$.

$\sigma, \mu \models X_z$	iff $\mu \in \sigma(z)$
$\sigma, \mu \models \langle \overset{a}{\Rightarrow} \rangle \psi$	iff $\sigma, \nu \models \psi$ for some ν where $\mu \overset{a}{\Rightarrow} \nu$
$\sigma, \mu \models [\overset{a}{\Rightarrow}] \psi$	iff $\sigma, \nu \models \psi$ for all ν where $\mu \overset{a}{\Rightarrow} \nu$
$\sigma, \mu \models \mathsf{L}_p \varphi$	iff $\breve{\mu}(\{\nu \mid \sigma, \nu \models \varphi\}) \geq p$

Characteristic formula

Then the endofunction

$$E_{\underset{\approx}{\prec}f} : s \mapsto \bigwedge_{a \in Act_\tau} \bigwedge_{\nu : s \xrightarrow{a} \nu} \langle \overset{a}{\Rightarrow} \rangle \bigwedge_{A \subseteq Supp(\nu)} \mathsf{L}_{\nu(A)} \bigvee_{z \in A} X_z .$$

expresses $F_{\underset{\approx}{\prec}f}$.

The Aceto et al theorem can be adapted to this setting, and hence, $E_{\underset{\approx}{\prec}f}$ characterizes probabilistic forward similarity gfp $F_{\underset{\approx}{\prec}f}$.

Summary

- One technique can characterize many probabilistic behavioral relations:
  - find a monotone endodeclaration that *expresses* the endofunction whose greatest fixed point is the behavioral relation.
  - That endodeclaration will *characterize* the behavioral relation.
- This technique, which was drawn from Aceto et al, might be useful in constructing characteristic formulae for behavioral relations on other types of structures, such as continuous-time Markov chains.

Thank you!