Verifying Probabilistic Programs Using a Hoare like Logic

Tim Quatmann

Seminar on Probabilistic Programs WS 2014/15

RWTH Aachen, Lehrstuhl für Informatik 2
Supervisor: Nils Jansen

February 03, 2015

Motivation

- Aim: Verify claims regarding the variables of a program

Motivation

- Aim: Verify claims regarding the variables of a program
- For non-probabilistic programs:

Hoare Logic (1969)

- Formulate *Hoare triples* of the form

$$\{\,\text{precondition}\,\}\ \texttt{program}\ \{\,\text{postcondition}\,\}$$

  where the conditions are first order predicate formulae
- Check whether a Hoare triple holds, i.e.:
  - For every variable assignment satisfying the precondition
  - ...the resulting assignment after executing the `program`
  - ...satisfies the postcondition
- The *derivation system* H can be used for this purpose

Motivation

The derivation system H:

$$\{\,p\,\}\ \mathsf{skip}\ \{\,p\,\} \qquad \text{(Skip)}$$

$$\frac{\{\,p \wedge c\,\}\ \mathsf{s}\ \{\,q\,\} \quad \{\,p \wedge \neg c\,\}\ \mathsf{s}'\ \{\,q\,\}}{\{\,p\,\}\ \mathsf{if}\ c\ \mathsf{then}\ \mathsf{s}\ \mathsf{else}\ \mathsf{s}'\ \mathsf{fi}\ \{\,q\,\}} \qquad \text{(If)}$$

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\} \qquad \text{(Assign)}$$

$$\frac{\{\,p \wedge c\,\}\ \mathsf{s}\ \{\,p\,\}}{\{\,p\,\}\ \mathsf{while}\ c\ \mathsf{do}\ \mathsf{s}\ \mathsf{od}\ \{\,p \wedge \neg c\,\}} \qquad \text{(While)}$$

$$\frac{\{\,p\,\}\ \mathsf{s}\ \{\,p'\,\} \quad \{\,p'\,\}\ \mathsf{s}'\ \{\,q\,\}}{\{\,p\,\}\ \mathsf{s};\mathsf{s}'\ \{\,q\,\}} \qquad \text{(Seq)}$$

$$\frac{p' \Rightarrow p \quad \{\,p\,\}\ \mathsf{s}\ \{\,q\,\} \quad q \Rightarrow q'}{\{\,p'\,\}\ \mathsf{s}\ \{\,q'\,\}} \qquad \text{(Cons)}$$

Motivation

$\langle x \bmod y = 0 \wedge (y = 2 \vee y = 3) \rangle$
if $(y = 2)$ then

$x := 3 \cdot x$

else

$x := 2 \cdot x$

fi
$\langle x \bmod 6 = 0 \rangle$

Motivation

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \rangle$

if $(y = 2)$ then

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y = 2 \rangle$

$x := 3 \cdot x$

$\langle x \bmod 6 = 0 \rangle$

else

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y \neq 2 \rangle$

$x := 2 \cdot x$

$\langle x \bmod 6 = 0 \rangle$

fi

$\langle x \bmod 6 = 0 \rangle$

Motivation

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \rangle$

if $(y = 2)$ then

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y = 2 \rangle$

$\langle 3 \cdot x \bmod 6 = 0 \rangle$

$x := 3 \cdot x$

$\langle x \bmod 6 = 0 \rangle$

else

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y \neq 2 \rangle$

$x := 2 \cdot x$

$\langle x \bmod 6 = 0 \rangle$

fi

$\langle x \bmod 6 = 0 \rangle$

Motivation

$\langle x \bmod y = 0 \land (y = 2 \lor y = 3) \rangle$

if $(y = 2)$ then

$\quad \langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y = 2 \rangle$

$\quad \langle 3 \cdot x \bmod 6 = 0 \rangle$

$\quad x := 3 \cdot x$

$\quad \langle x \bmod 6 = 0 \rangle$

else

$\quad \langle x \bmod y = 0 \land (y = 2 \lor y = 3) \land y \neq 2 \rangle$

$\quad \langle 2 \cdot x \bmod 6 = 0 \rangle$

$\quad x := 2 \cdot x$

$\quad \langle x \bmod 6 = 0 \rangle$

fi

$\langle x \bmod 6 = 0 \rangle$

Motivation

Is this feasible for *probabilistic programs*?

Motivation

Is this feasible for *probabilistic programs*?

- The value of variables depends on probabilistic choices
- Preconditions and postconditions are only satisfied with a certain probability
- Hence, it is not clear whether a Hoare triple holds

Motivation

Is this feasible for *probabilistic programs*?

- The value of variables depends on probabilistic choices
- Preconditions and postconditions are only satisfied with a certain probability
- Hence, it is not clear whether a Hoare triple holds

We need to extend the occuring notions!

Motivation

Is this feasible for *probabilistic programs*?

- The value of variables depends on probabilistic choices
- Preconditions and postconditions are only satisfied with a certain probability
- Hence, it is not clear whether a Hoare triple holds

We need to extend the occuring notions!

- This is the topic of this talk
- Based on the paper of *den Hartog* (1999):

  Verifying Probabilistic Programs using a Hoare like Logic

Overview

The Language $\mathcal{L}_{\text{pw}}$

- The language of *probabilistic programs* ($\mathcal{L}_{\text{pw}}$) is given by:

$$\mathtt{s} ::= \mathtt{skip} \mid x := e \mid \mathtt{s}; \mathtt{s} \mid \mathtt{s} \oplus_r \mathtt{s} \mid \mathtt{if}\ c\ \mathtt{then}\ \mathtt{s}\ \mathtt{else}\ \mathtt{s}\ \mathtt{fi} \mid \mathtt{while}\ c\ \mathtt{do}\ \mathtt{s}\ \mathtt{od}$$

- $\mathtt{s} \oplus_r \mathtt{s}'$ can be seen as a (biased) coin flip
  - $\mathtt{s}$ is executed with probability r
  - $\mathtt{s}'$ is executed with probability $1 - r$
- Semantics will be discussed later

Example: Probabilistic Program

Consider the Program $\mathbf{s} \in \mathcal{L}_{\mathrm{pw}}$:

$$
\begin{aligned}
&(x := 0 \oplus_{0.3} x := 1);\\
&\textsf{if } (x = 0) \textsf{ then}\\
&\quad y := 1\\
&\textsf{else}\\
&\quad y := 0\\
&\textsf{fi}
\end{aligned}
$$

Probabilistic States

- The value of variables depends on probabilistic choices
- The value of two variables might depend on each other

Probabilistic States

- The value of variables depends on probabilistic choices
- The value of two variables might depend on each other

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

After execution we obtain:

- $x = 0$ with probability 0.3
- $y = 0$ with probability 0.7

Probabilistic States

- The value of variables depends on probabilistic choices
- The value of two variables might depend on each other

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

After execution we obtain:

- $x = 0$ with probability 0.3
- $y = 0$ with probability 0.7
- But:
  $x = y = 0$ with probability 0

Probabilistic States

- The value of variables depends on probabilistic choices
- The value of two variables might depend on each other

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

After execution we obtain:

- $x = 0$ with probability 0.3
- $y = 0$ with probability 0.7
- But:
  $x = y = 0$ with probability 0

We need a notion to capture this information!

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

After execution the variable assignment is either σ_1 or σ_2, where

$$\sigma_1(x) = 1 \quad \sigma_1(y) = 0 \text{ and}$$
$$\sigma_2(x) = 0 \quad \sigma_2(y) = 1$$

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables

Example

Consider the program:

$(x := 0 \oplus_{0.3} x := 1);$
if $(x = 0)$ then
  $y := 1$
else
  $y := 0$
fi

After execution the variable assignment is either σ_1 or σ_2, where

$$\sigma_1(x) = 1 \quad \sigma_1(y) = 0 \text{ and}$$
$$\sigma_2(x) = 0 \quad \sigma_2(y) = 1$$

Yielding the probabilistic state θ with

$$\theta(\sigma_1) = 0.7 \quad \theta(\sigma_2) = 0.3$$

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables
- A variable assignment (= *deterministic state*) can be seen as a mapping $\sigma\colon \mathrm{Var} \to \mathrm{Val}$
- The set of all deterministic states is denoted by $\mathcal{S}$

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables
- A variable assignment (= *deterministic state*) can be seen as a mapping $\sigma\colon \mathrm{Var} \to \mathrm{Val}$
- The set of all deterministic states is denoted by $\mathcal{S}$
- A probabilistic state is a mapping $\theta\colon \mathcal{S} \to [0,1]$ such that $\sum_{\sigma\in\mathcal{S}} \theta(\sigma) \leq 1$

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables
- A variable assignment (= *deterministic state*) can be seen as a mapping $\sigma\colon \mathrm{Var} \to \mathrm{Val}$
- The set of all deterministic states is denoted by $\mathcal{S}$
- A probabilistic state is a mapping $\theta\colon \mathcal{S} \to [0,1]$ such that $\sum_{\sigma\in\mathcal{S}} \theta(\sigma) \leq 1$

Example

Let: $\theta(\sigma_1) = 0.7 \quad \theta(\sigma_2) = 0.3$

$\sigma_1(x) = 1 \quad \sigma_1(y) = 0$

$\sigma_2(x) = 0 \quad \sigma_2(y) = 1$

Probabilistic States

- A *probabilistic state* assigns a probability ratio to every possible assignment of all variables
- A variable assignment (= *deterministic state*) can be seen as a mapping $\sigma\colon \mathrm{Var} \to \mathrm{Val}$
- The set of all deterministic states is denoted by $\mathcal{S}$
- A probabilistic state is a mapping $\theta\colon \mathcal{S} \to [0,1]$ such that $\sum_{\sigma\in\mathcal{S}} \theta(\sigma) \leq 1$

Example

Let: $\theta(\sigma_1) = 0.7 \quad \theta(\sigma_2) = 0.3$

$\sigma_1(x) = 1 \quad \sigma_1(y) = 0$

$\sigma_2(x) = 0 \quad \sigma_2(y) = 1$

θ can also be depicted by:

$\theta(\sigma_i)$	0.7	0.3
$\sigma_i(x)$	1	0
$\sigma_i(y)$	0	1

Operations on Probabilistic States

To define the *semantics* of $\mathcal{L}_{\mathrm{pw}}$ as well as *probabilistic predicates*, we need to define the following operations on probabilistic states:

Operations on Probabilistic States

To define the *semantics* of $\mathcal{L}_{\text{pw}}$ as well as *probabilistic predicates*, we need to define the following operations on probabilistic states:

Scaling

$$(r \cdot \theta)(\sigma) = r \cdot \theta(\sigma)$$

Merging

$$(\theta + \theta')(\sigma) = \theta(\sigma) + \theta'(\sigma)$$

Restricting

$$c?\theta(\sigma) = \begin{cases} \theta(\sigma) & \text{if } c \text{ is } \mathit{true} \text{ with respect to } \sigma \\ 0 & \text{otherwise} \end{cases}$$

Example: Scaling and Merging

- Consider the probabilistic states θ and θ':

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

$\theta'(\sigma_i)$	0.2	0.2
$\sigma_i(x)$	1	1
$\sigma_i(y)$	1	0

Example: Scaling and Merging

- Consider the probabilistic states θ and θ':

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

$\theta'(\sigma_i)$	0.2	0.2
$\sigma_i(x)$	1	1
$\sigma_i(y)$	1	0

- The *scaled* state $0.5 \cdot \theta'$ is given by:

$(0.5 \cdot \theta')(\sigma_i)$	0.1	0.1
$\sigma_i(x)$	1	1
$\sigma_i(y)$	1	0

Example: Scaling and Merging

- Consider the probabilistic states θ and θ':

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

$\theta'(\sigma_i)$	0.2	0.2
$\sigma_i(x)$	1	1
$\sigma_i(y)$	1	0

- The *scaled* state $0.5 \cdot \theta'$ is given by:

$(0.5 \cdot \theta')(\sigma_i)$	0.1	0.1
$\sigma_i(x)$	1	1
$\sigma_i(y)$	1	0

- The *merged* state $\theta + \theta'$ is given by:

$(\theta + \theta')(\sigma_i)$	0.2	0.5	0.2	0.1
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

Example: Restricting

- Consider the probabilistic state θ:

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

  and the condition $c := (x = 1)$

Example: Restricting

- Consider the probabilistic state θ:

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

  and the condition $c := (x = 1)$

- The *restricted* states $c?\theta$ and $\neg c?\theta$ are given by:

$c?\theta(\sigma_i)$	0.3
$\sigma_i(x)$	1
$\sigma_i(y)$	0

$\neg c?\theta(\sigma_i)$	0.2	0.1
$\sigma_i(x)$	0	0
$\sigma_i(y)$	1	0

Example: Restricting

- Consider the probabilistic state θ:

$\theta(\sigma_i)$	0.3	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

  and the condition $c := (x = 1)$

- The *restricted* states $c?\theta$ and $\neg c?\theta$ are given by:

$c?\theta(\sigma_i)$	0.3
$\sigma_i(x)$	1
$\sigma_i(y)$	0

$\neg c?\theta(\sigma_i)$	0.2	0.1
$\sigma_i(x)$	0	0
$\sigma_i(y)$	1	0

- It holds that $c?\theta + \neg c?\theta = \theta$

Semantics for $\mathcal{L}_{\text{pw}}$

- The semantics for $\mathcal{L}_{\text{pw}}$ is given by a mapping

$$\mathcal{D}\colon \mathcal{L}_{\text{pw}} \to (\Pi \to \Pi)$$

  where Π is the set of all probabilistic states
- $\mathcal{D}(\mathtt{s})(\theta) \in \Pi$ is obtained when starting in θ and executing $\mathtt{s}$

Semantics for $\mathcal{L}_{\text{pw}}$

- The semantics for $\mathcal{L}_{\text{pw}}$ is given by a mapping

$$\mathcal{D}\colon \mathcal{L}_{\text{pw}} \to (\Pi \to \Pi)$$

  where Π is the set of all probabilistic states
- $\mathcal{D}(\mathtt{s})(\theta) \in \Pi$ is obtained when starting in θ and executing $\mathtt{s}$

$$\begin{aligned}
\mathcal{D}(\mathtt{skip})(\theta) &= \theta \\
\mathcal{D}(\mathtt{s}; \mathtt{s}')(\theta) &= \mathcal{D}(\mathtt{s}')(\mathcal{D}(\mathtt{s})(\theta)) \\
\mathcal{D}(\mathtt{s} \oplus_r \mathtt{s}')(\theta) &= \Big(r \cdot \mathcal{D}(\mathtt{s})(\theta)\Big) + \Big((1-r) \cdot \mathcal{D}(\mathtt{s}')(\theta)\Big) \\
&\vdots
\end{aligned}$$

Probabilistic Predicates

- We need to express conditions on probabilistic states
- Evaluation to either $true$ or $false$ is desired
- Deterministic predicates as used for non-probabilistic programs are not feasible

Probabilistic Predicates

- We need to express conditions on probabilistic states
- Evaluation to either $true$ or $false$ is desired
- Deterministic predicates as used for non-probabilistic programs are not feasible

Example

$\theta(\sigma_i)$	0.7	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

- $\theta \models x = 0 \wedge y \leq 1$?

Probabilistic Predicates

- We need to express conditions on probabilistic states
- Evaluation to either $true$ or $false$ is desired
- Deterministic predicates as used for non-probabilistic programs are not feasible

Example

$\theta(\sigma_i)$	0.7	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

- $\theta \models x = 0 \wedge y \leq 1$
  ...only holds with probability 0.3

Probabilistic Predicates

- We need to express conditions on probabilistic states
- Evaluation to either $true$ or $false$ is desired
- Deterministic predicates as used for non-probabilistic programs are not feasible

Example

$\theta(\sigma_i)$	0.7	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

- $\theta \models x = 0 \wedge y \leq 1$
  ...only holds with probability 0.3

Solution: Probabilistic predicates

- Consider the probability that a deterministic predicate holds

Probabilistic Predicates

- We need to express conditions on probabilistic states
- Evaluation to either $true$ or $false$ is desired
- Deterministic predicates as used for non-probabilistic programs are not feasible

Example

$\theta(\sigma_i)$	0.7	0.2	0.1
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	0	1	0

- $\theta \models x = 0 \wedge y \leq 1$
  ...only holds with probability 0.3
- $\theta \models \mathbb{P}(x = 0 \wedge y \leq 1) = 0.3$

Solution: Probabilistic predicates

- Consider the probability that a deterministic predicate holds

Probabilistic Predicates

- $\mathbb{P}(dp) \prec r$ is a probabilistic predicate for $\prec \in \{<, \leq, =, \geq, >\}$

$$\theta \models \mathbb{P}(dp) \prec r \iff \sum_{\sigma \models dp} \theta(\sigma) \prec r$$

Probabilistic Predicates

- $\mathbb{P}(dp) \prec r$ is a probabilistic predicate for $\prec \in \{<, \leq, =, \geq, >\}$

$$\theta \models \mathbb{P}(dp) \prec r \iff \sum_{\sigma \models dp} \theta(\sigma) \prec r$$

More probabilistic predicates:

- $\neg p$, $p \wedge q$, $\exists i : p$, ... (common logical operators)
- $p[x/e]$ (replace $x \in \mathrm{Var}$ with $e \in \mathrm{Exp}$)
- $r \cdot p$, $p + q$, $c?p$ (describe scaled, merged, restricted versions of states satisfying p, q)

Scaled States

$\theta \models r \cdot p$ if θ is a scaled state $r \cdot \theta'$ for some state θ' that satisfies p

Scaled States

$\theta \models r \cdot p$ if θ is a scaled state $r \cdot \theta'$ for some state θ' that satisfies p

Example

- Consider the state θ:

$\theta(\sigma_i)$	0.2	0.1	0.2
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	1	1	0

  and the predicate $p := \Big(\mathbb{P}(x = 0){=}0.6\Big) \wedge \Big(\mathbb{P}(y = 1){=}0.6\Big)$

- $\theta \models 0.5 \cdot p$?

Scaled States

$\theta \models r \cdot p$ if θ is a scaled state $r \cdot \theta'$ for some state θ' that satisfies p

Example

- Consider the state θ:

$\theta(\sigma_i)$	0.2	0.1	0.2
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	1	1	0

$\theta'(\sigma_i)$	0.4	0.2	0.4
$\sigma_i(x)$	1	0	0
$\sigma_i(y)$	1	1	0

  and the predicate $p := \Big(\mathbb{P}(x = 0){=}0.6\Big) \wedge \Big(\mathbb{P}(y = 1){=}0.6\Big)$

- $\theta \models 0.5 \cdot p$ since $\theta = 0.5 \cdot \theta'$ and $\theta' \models p$

Merged States

$\theta \models p + q$ if θ is a merged state $\theta_1 + \theta_2$ for some states θ_1, θ_2 with $\theta_1 \models p$ and $\theta_2 \models q$

Merged States

$\theta \models p + q$ if θ is a merged state $\theta_1 + \theta_2$ for some states θ_1, θ_2 with $\theta_1 \models p$ and $\theta_2 \models q$

Example

- Consider the state θ and the predicates p and q:

$\theta(\sigma_i)$	0.2	0.3	0.1	0.4
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

$p := \mathbb{P}(x = 0 \wedge y = 1) = 0.1$
$q := \mathbb{P}(x = 0) = 0.2$

- $\theta \models p + q$?

Merged States

$\theta \models p + q$ if θ is a merged state $\theta_1 + \theta_2$ for some states θ_1, θ_2 with $\theta_1 \models p$ and $\theta_2 \models q$

Example

- Consider the state θ and the predicates p and q:

$\theta(\sigma_i)$	0.2	0.3	0.1	0.4
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

$p := \mathbb{P}(x = 0 \wedge y = 1) = 0.1$
$q := \mathbb{P}(x = 0) = 0.2$

- $\theta \models p + q$ since $\theta = \theta_1 + \theta_2$, $\theta_1 \models p$ and $\theta_2 \models q$ with

$\theta_1(\sigma_i)$	0.2	0.3	0.1	0.2
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

$\theta_2(\sigma_i)$	0.2
$\sigma_i(x)$	0
$\sigma_i(y)$	0

Restricted States

$\theta \models c?p$ if θ is a restricted state $c?\theta'$ for some state θ' that satisfies p

Restricted States

$\theta \models c?p$ if θ is a restricted state $c?\theta'$ for some state θ' that satisfies p

Example

- Consider the states θ and θ':

$\theta(\sigma_i)$	0.2	0.1
$\sigma_i(x)$	1	0
$\sigma_i(y)$	1	1

$\theta'(\sigma_i)$	0.2	0.3	0.1	0.4
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

- For $c := (y = 1)$ it holds that $\theta = c?\theta'$

Restricted States

$\theta \models c?p$ if θ is a restricted state $c?\theta'$ for some state θ' that satisfies p

Example

- Consider the states θ and θ':

$\theta(\sigma_i)$	0.2	0.1
$\sigma_i(x)$	1	0
$\sigma_i(y)$	1	1

$\theta'(\sigma_i)$	0.2	0.3	0.1	0.4
$\sigma_i(x)$	1	1	0	0
$\sigma_i(y)$	1	0	1	0

- For $c := (y = 1)$ it holds that $\theta = c?\theta'$

$\Longrightarrow$ $\theta \models c?p$ for all predicates p that are satisfied by θ'

$\Longrightarrow$ $\theta \models \mathbb{P}(\neg c){=}0$

$\Longrightarrow$ $\theta \models \Big(\mathbb{P}(\mathit{true}){=}r\Big) \leftrightarrow \Big(\mathbb{P}(c){=}r\Big)$

Shorthand Notations

- $[dp] \coloneqq \mathbb{P}(dp){=}1$
- $p \oplus_r q \coloneqq \Big(r \cdot p\Big) + \Big((1-r) \cdot q\Big)$

Shorthand Notations

- $[dp] \coloneqq \mathbb{P}(dp){=}1$
- $p \oplus_r q \coloneqq \Big(r \cdot p\Big) + \Big((1-r) \cdot q\Big)$

Example

- Consider the state θ and the predicate p:

$\theta(\sigma_i)$	0.3	0.7
$\sigma_i(y)$	1	0

$$p = [y = 1] \vee [y = 0]$$

- $\theta \not\models p$

Shorthand Notations

- $[dp] \coloneqq \mathbb{P}(dp){=}1$
- $p \oplus_r q \coloneqq \Big(r \cdot p\Big) + \Big((1-r) \cdot q\Big)$

Example

- Consider the state θ and the predicate p:

$\theta(\sigma_i)$	0.3	0.7
$\sigma_i(y)$	1	0

$$p = [y = 1] \vee [y = 0]$$

- $\theta \not\models p$
- $\theta \models p \oplus_{0.3} p$ since $\theta = \theta_1 + \theta_2$

$\theta_1(\sigma_i)$	0.3
$\sigma_i(y)$	1

$\theta_2(\sigma_i)$	0.7
$\sigma_i(y)$	0

Shorthand Notations

- $[dp] \coloneqq \mathbb{P}(dp){=}1$
- $p \oplus_r q \coloneqq \Big(r \cdot p\Big) + \Big((1-r) \cdot q\Big)$

Example

- Consider the state θ and the predicate p:

$\theta(\sigma_i)$	0.3	0.7
$\sigma_i(y)$	1	0

$$p = [y = 1] \vee [y = 0]$$

- $\theta \not\models p$
- $\theta \models p \oplus_{0.3} p$ since $\theta = \theta_1 + \theta_2 = 0.3 \cdot \theta'_1 + 0.7 \cdot \theta'_2$ where

$\theta_1(\sigma_i)$	0.3
$\sigma_i(y)$	1

$\theta_2(\sigma_i)$	0.7
$\sigma_i(y)$	0

$\theta'_1(\sigma_i)$	1
$\sigma_i(y)$	1

$\theta'_2(\sigma_i)$	1
$\sigma_i(y)$	0

Note that: $\theta'_1, \theta'_2 \models p$

Hoare Triples for Probabilistic Programs

- Almost similar to the non-probabilistic case

Hoare Triples for Probabilistic Programs

- Almost similar to the non-probabilistic case
- A *Hoare triple* is of the form $\{\, p \,\}\ \mathtt{s}\ \{\, q \,\}$
  - p and q are probabilistic predicates called precondition and postcondition
  - $\mathtt{s}$ is a probabilistic program
- $\{\, p \,\}\ \mathtt{s}\ \{\, q \,\}$ is said to *hold* if:
  - For all probabilistic states satisfying the precondition p
  - ... the resulting state after executing the program $\mathtt{s}$
  - ... satisfies the postcondition q
- In this case we write $\models \{\, p \,\}\ \mathtt{s}\ \{\, q \,\}$

Example: Hoare triples

Consider the Program s:

$$(x := 0 \oplus_{0.3} x := 1);$$
if $(x = 0)$ then
$$y := 1$$
else
$$y := 0$$
fi

Example: Hoare triples

Consider the Program s:

$$
\begin{array}{l}
(x := 0 \oplus_{0.3} x := 1); \\
\textsf{if } (x = 0) \textsf{ then} \\
\quad y := 1 \\
\textsf{else} \\
\quad y := 0 \\
\textsf{fi}
\end{array}
$$

- $\not\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(x = 0 \wedge y = 0) > 0 \,\}$

Example: Hoare triples

Consider the Program s:

$$
\begin{array}{l}
(x := 0 \oplus_{0.3} x := 1); \\
\textsf{if } (x = 0) \textsf{ then} \\
\quad y := 1 \\
\textsf{else} \\
\quad y := 0 \\
\textsf{fi}
\end{array}
$$

- $\not\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(x = 0 \wedge y = 0) {>} 0 \,\}$
- $\not\models \{\, \mathbb{P}(true) {\geq} 0 \,\}\ \mathtt{s}\ \{\, \mathbb{P}(y = 0) {=} 0.7 \,\}$

Example: Hoare triples

Consider the Program s:

$$
\begin{array}{l}
(x := 0 \oplus_{0.3} x := 1); \\
\textsf{if } (x = 0) \textsf{ then} \\
\quad y := 1 \\
\textsf{else} \\
\quad y := 0 \\
\textsf{fi}
\end{array}
$$

- $\not\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(x = 0 \wedge y = 0) {>} 0 \,\}$
- $\not\models \{\, \mathbb{P}(true) {\geq} 0 \,\}\ \mathtt{s}\ \{\, \mathbb{P}(y = 0) {=} 0.7 \,\}$
- $\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(y = 0) {=} 0.7 \,\}$

The Derivation System pH

- The derivation system H needs to be adjusted to work for probabilistic programs:
  - Handling of probabilistic choices: $\mathtt{s} \oplus_r \mathtt{s}'$
  - Handling of probabilistic states where a Boolean condition $c \in \mathrm{BC}$ evaluates to true (or false) with probability < 1

- This yields the new derivation system pH

The Derivation System pH

$$\{\,p\,\}\ \mathtt{skip}\ \{\,p\,\} \qquad \text{(Skip)}$$

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\} \qquad \text{(Assign)}$$

$$\frac{\{\,p\,\}\ \mathtt{s}\ \{\,p'\,\} \quad \{\,p'\,\}\ \mathtt{s}'\ \{\,q\,\}}{\{\,p\,\}\ \mathtt{s};\mathtt{s}'\ \{\,q\,\}} \qquad \text{(Seq)}$$

$$\frac{p' \Rightarrow p \quad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \quad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}} \qquad \text{(Cons)}$$

$$\frac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \quad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}} \qquad \text{(Prob)}$$

$$\frac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \quad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s}\ \{\,q \oplus_r q'\,\}} \qquad \text{(Or)}$$

$$\frac{\{\,p[j]\,\}\ \mathtt{s}\ \{\,q\,\} \quad j \notin p, q}{\{\,\exists i\colon p[i]\,\}\ \mathtt{s}\ \{\,q\,\}} \qquad \text{(Exists)}$$

$$\frac{\{\,p\,\}\ \mathtt{s}\ \{\,q[j]\,\} \quad j \notin p, q}{\{\,p\,\}\ \mathtt{s}\ \{\,\forall i\colon q[i]\,\}} \qquad \text{(Forall)}$$

$$\frac{\{\,c?p\,\}\ \mathtt{s}\ \{\,q\,\} \quad \{\,\neg c?p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{if}\ c\ \mathtt{then}\ \mathtt{s}\ \mathtt{else}\ \mathtt{s}'\ \mathtt{fi}\ \{\,q + q'\,\}} \qquad \text{(If)}$$

$$\frac{p\ \text{invariant for}\ \langle c, \mathtt{s}\rangle}{\{\,p\,\}\ \mathtt{while}\ c\ \mathtt{do}\ \mathtt{s}\ \mathtt{od}\ \{\,p \wedge \mathbb{P}(c){=}0\,\}} \qquad \text{(While)}$$

The Derivation System pH

pH is correct:

- Only valid Hoare triples can be derived from pH
- This can be shown by induction on the depth of a proof tree
- Consider the last used rule and conclude that the obtained Hoare triple holds

The Derivation System pH

pH is correct:

- Only valid Hoare triples can be derived from pH
- This can be shown by induction on the depth of a proof tree
- Consider the last used rule and conclude that the obtained Hoare triple holds

Is pH complete?

- Can we derive every valid Hoare triple from pH?
- This question is still open

Example: Proof

Consider again the Program s:

$$
\begin{array}{l}
(x := 0 \oplus_{0.3} x := 1); \\
\text{if } (x = 0) \text{ then} \\
\quad y := 1 \\
\text{else} \\
\quad y := 0 \\
\text{fi}
\end{array}
$$

We want to show that

$$\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(y = 0) = 0.7 \,\}$$

Example: Proof

Consider again the Program $\mathtt{s}$:

$$
\begin{array}{l}
(x := 0 \oplus_{0.3} x := 1); \\
\mathsf{if}\ (x = 0)\ \mathsf{then} \\
\quad y := 1 \\
\mathsf{else} \\
\quad y := 0 \\
\mathsf{fi}
\end{array}
$$

We want to show that

$$\models \{\, [true] \,\}\ \mathtt{s}\ \{\, \mathbb{P}(y = 0){=}0.7 \,\}$$

Auxiliary statement:

$$\models \{\, [true] \,\}\ x := 0 \oplus_{0.3} x := 1\ \{\, \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big) \,\}$$

Example: Proof

$$\frac{}{\{\,[\mathit{true}]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,\big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)\,\}}$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ \text{(Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ \text{(Cons)}$$

$$\frac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ \text{(Prob)}$$

Example: Proof

$$\frac{\{\,[\mathit{true}]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x \neq 0]\,\}}{\{\,[\mathit{true}]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x \neq 0){=}0.7)\,\}}\ (\text{Cons})$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ (\text{Assign})$$

$$\frac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ (\text{Cons}) \qquad \frac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ (\text{Prob})$$

Example: Proof

Show that

$$[x = 0] \oplus_{0.3} [x \neq 0] \text{ implies } \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)$$

Proof:

$$\begin{aligned} & \theta \models [x = 0] \oplus_{0.3} [x \neq 0] \\ \Longrightarrow\ & \theta \models 0.3 \cdot [x = 0] + 0.7 \cdot [x \neq 0] \end{aligned}$$

Example: Proof

Show that

$$[x = 0] \oplus_{0.3} [x \neq 0] \text{ implies } \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)$$

Proof:

$$\begin{aligned} & \theta \models [x = 0] \oplus_{0.3} [x \neq 0] \\ \Longrightarrow\ & \theta \models 0.3 \cdot [x = 0] + 0.7 \cdot [x \neq 0] \\ \Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models 0.3 \cdot \big([x = 0]\big) \\ & \qquad\qquad\qquad\qquad\quad \theta_2 \models 0.7 \cdot \big([x \neq 0]\big) \end{aligned}$$

Example: Proof

Show that

$$[x = 0] \oplus_{0.3} [x \neq 0] \text{ implies } \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)$$

Proof:

$$\begin{aligned} & \theta \models [x = 0] \oplus_{0.3} [x \neq 0] \\ \Longrightarrow\ & \theta \models 0.3 \cdot [x = 0] + 0.7 \cdot [x \neq 0] \\ \Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models 0.3 \cdot \big([x = 0] \wedge \mathbb{P}(x \neq 0){=}0\big) \\ & \qquad\qquad\qquad\qquad\quad \theta_2 \models 0.7 \cdot \big([x \neq 0] \wedge \mathbb{P}(x = 0){=}0\big) \end{aligned}$$

Example: Proof

Show that

$$[x = 0] \oplus_{0.3} [x \neq 0] \text{ implies } \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)$$

Proof:

$$\begin{aligned}
& \theta \models [x = 0] \oplus_{0.3} [x \neq 0] \\
\Longrightarrow\ & \theta \models 0.3 \cdot [x = 0] + 0.7 \cdot [x \neq 0] \\
\Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models 0.3 \cdot \big([x = 0] \wedge \mathbb{P}(x \neq 0){=}0\big) \\
& \qquad\qquad\qquad\qquad\quad \theta_2 \models 0.7 \cdot \big([x \neq 0] \wedge \mathbb{P}(x = 0){=}0\big) \\
\Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0\big) \\
& \qquad\qquad\qquad\qquad\quad \theta_2 \models \big(\mathbb{P}(x \neq 0){=}0.7\big) \wedge \big(\mathbb{P}(x = 0){=}0\big)
\end{aligned}$$

Example: Proof

Show that

$$[x = 0] \oplus_{0.3} [x \neq 0] \text{ implies } \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)$$

Proof:

$$\begin{aligned}
& \theta \models [x = 0] \oplus_{0.3} [x \neq 0] \\
\Longrightarrow\ & \theta \models 0.3 \cdot [x = 0] + 0.7 \cdot [x \neq 0] \\
\Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models 0.3 \cdot \big([x = 0] \wedge \mathbb{P}(x \neq 0){=}0\big) \\
& \qquad\qquad\qquad\qquad\quad \theta_2 \models 0.7 \cdot \big([x \neq 0] \wedge \mathbb{P}(x = 0){=}0\big) \\
\Longrightarrow\ & \theta = \theta_1 + \theta_2 \text{ with } \theta_1 \models \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0\big) \\
& \qquad\qquad\qquad\qquad\quad \theta_2 \models \big(\mathbb{P}(x \neq 0){=}0.7\big) \wedge \big(\mathbb{P}(x = 0){=}0\big) \\
\Longrightarrow\ & \theta \models \big(\mathbb{P}(x = 0){=}0.3\big) \wedge \big(\mathbb{P}(x \neq 0){=}0.7\big)
\end{aligned}$$

Example: Proof

$$\frac{\{\,[\mathit{true}]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x \neq 0]\,\}}{\{\,[\mathit{true}]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x \neq 0){=}0.7)\,\}}\ (\text{Cons})$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ (\text{Assign})$$

$$\frac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ (\text{Cons}) \qquad \frac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ (\text{Prob})$$

Example: Proof

$$\dfrac{\dfrac{\dfrac{}{\{\,[true]\,\}\ x := 0\ \{\,[x=0]\,\}} \qquad \dfrac{}{\{\,[true]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x\neq 0]\,\}}\ (\text{Prob})}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x\neq 0){=}0.7)\,\}}\ (\text{Cons})$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ (\text{Assign})$$

$$\dfrac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ (\text{Cons})$$

$$\dfrac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ (\text{Prob})$$

Example: Proof

$$\dfrac{\dfrac{\dfrac{\{\,[0=0]\,\}\ x:=0\ \{\,[x=0]\,\}}{\{\,[true]\,\}\ x:=0\ \{\,[x=0]\,\}}\ \text{(Cons)} \qquad \dfrac{}{\{\,[true]\,\}\ x:=1\ \{\,[x\neq 0]\,\}}}{\{\,[true]\,\}\ x:=0\ \oplus_{0.3}\ x:=1\ \{\,[x=0]\ \oplus_{0.3}\ [x\neq 0]\,\}}\ \text{(Prob)}}{\{\,[true]\,\}\ x:=0\ \oplus_{0.3}\ x:=1\ \{\,(\mathbb{P}(x=0){=}0.3)\ \wedge\ (\mathbb{P}(x\neq 0){=}0.7)\,\}}\ \text{(Cons)}$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x:=e\ \{\,p\,\}\ \text{(Assign)}$$

$$\dfrac{p'\Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q\Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ \text{(Cons)} \qquad \dfrac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s}\ \oplus_r\ \mathtt{s}'\ \{\,q\ \oplus_r\ q'\,\}}\ \text{(Prob)}$$

Example: Proof

$$\dfrac{\dfrac{\dfrac{}{\{\,[0=0]\,\}\ x := 0\ \{\,[x=0]\,\}}\ \text{(Assign)}}{\{\,[true]\,\}\ x := 0\ \{\,[x=0]\,\}}\ \text{(Cons)} \qquad \dfrac{}{\{\,[true]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x\neq 0]\,\}}\ \text{(Prob)}$$

$$\dfrac{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x\neq 0]\,\}}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x\neq 0){=}0.7)\,\}}\ \text{(Cons)}$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ \text{(Assign)}$$

$$\dfrac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ \text{(Cons)}$$

$$\dfrac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ \text{(Prob)}$$

Example: Proof

$$\dfrac{\dfrac{\dfrac{}{\{\,[0=0]\,\}\ x := 0\ \{\,[x=0]\,\}}\ \text{(Assign)}}{\{\,[true]\,\}\ x := 0\ \{\,[x=0]\,\}}\ \text{(Cons)} \qquad \dfrac{\{\,[1\neq 0]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}{\{\,[true]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}\ \text{(Cons)}}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x\neq 0]\,\}}\ \text{(Prob)}$$
$$\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x\neq 0){=}0.7)\,\}\ \text{(Cons)}$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ \text{(Assign)}$$

$$\dfrac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ \text{(Cons)} \qquad \dfrac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ \text{(Prob)}$$

Example: Proof

$$\dfrac{\dfrac{\dfrac{}{\{\,[0=0]\,\}\ x := 0\ \{\,[x=0]\,\}}\ (\text{Assign})}{\{\,[true]\,\}\ x := 0\ \{\,[x=0]\,\}}\ (\text{Cons}) \qquad \dfrac{\dfrac{\dfrac{}{\{\,[1\neq 0]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}\ (\text{Assign})}{\{\,[true]\,\}\ x := 1\ \{\,[x\neq 0]\,\}}\ (\text{Cons})}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,[x=0] \oplus_{0.3} [x\neq 0]\,\}}\ (\text{Prob})}{\{\,[true]\,\}\ x := 0 \oplus_{0.3} x := 1\ \{\,(\mathbb{P}(x=0){=}0.3) \wedge (\mathbb{P}(x\neq 0){=}0.7)\,\}}\ (\text{Cons})$$

Recall the derivation rules:

$$\{\,p[x/e]\,\}\ x := e\ \{\,p\,\}\ (\text{Assign})$$

$$\dfrac{p' \Rightarrow p \qquad \{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad q \Rightarrow q'}{\{\,p'\,\}\ \mathtt{s}\ \{\,q'\,\}}\ (\text{Cons}) \qquad \dfrac{\{\,p\,\}\ \mathtt{s}\ \{\,q\,\} \qquad \{\,p\,\}\ \mathtt{s}'\ \{\,q'\,\}}{\{\,p\,\}\ \mathtt{s} \oplus_r \mathtt{s}'\ \{\,q \oplus_r q'\,\}}\ (\text{Prob})$$

Example: Proof

$(x := 0 \oplus_{0.3} x := 1);$

if $(x = 0)$ then

$y := 1$

else

$y := 0$

fi

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \}\ \text{(Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)} \qquad \frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$

if $(x = 0)$ then

$y := 1$

else

$y := 0$

fi

$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \}\ \text{(Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)} \qquad \frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$

if $(x = 0)$ then

$y := 1$

else

$y := 0$

fi

$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \}\ \text{(Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)} \qquad \frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then

$y := 1$

else

$y := 0$

fi

$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \} \text{ (Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}} \text{ (Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}} \text{ (If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
$\quad \langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$

$\quad y := 1$

else
$\quad \langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$

$\quad y := 0$

fi

$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$\{ p[x/e] \}\ x := e\ \{ p \}$ (Assign)

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
  $\langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(1 = 0) = 0 \rangle$
  $y := 1$
else
  $\langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $y := 0$
fi
$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \} \text{ (Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}} \text{ (Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}} \text{ (If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
  $\langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(1 = 0) = 0 \rangle$
  $y := 1$
  $\langle \mathbb{P}(y = 0) = 0 \rangle$
else
  $\langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $y := 0$
fi
$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$\{ p[x/e] \}\ x := e\ \{ p \}$ (Assign)

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
  $\langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(1 = 0) = 0 \rangle$
  $y := 1$
  $\langle \mathbb{P}(y = 0) = 0 \rangle$
else
  $\langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(0 = 0) = 0.7 \rangle$
  $y := 0$
fi
$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \} \text{ (Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}} \text{ (Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}} \text{ (If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
  $\langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(1 = 0) = 0 \rangle$
  $y := 1$
  $\langle \mathbb{P}(y = 0) = 0 \rangle$
else
  $\langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(0 = 0) = 0.7 \rangle$
  $y := 0$
  $\langle \mathbb{P}(y = 0) = 0.7 \rangle$
fi

$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$\{ p[x/e] \}\ x := e\ \{ p \}$ (Assign)

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}}\ \text{(Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi}\ \{ q + q' \}}\ \text{(If)}$$

Example: Proof

$\langle [true] \rangle$
$(x := 0 \oplus_{0.3} x := 1);$
$\langle (\mathbb{P}(x = 0) = 0.3) \wedge (\mathbb{P}(x \neq 0) = 0.7) \rangle$
$\langle \mathbb{P}(x \neq 0) = 0.7 \rangle$
if $(x = 0)$ then
  $\langle (x = 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(1 = 0) = 0 \rangle$
  $y := 1$
  $\langle \mathbb{P}(y = 0) = 0 \rangle$
else
  $\langle (x \neq 0)?(\mathbb{P}(x \neq 0) = 0.7) \rangle$
  $\langle \mathbb{P}(0 = 0) = 0.7 \rangle$
  $y := 0$
  $\langle \mathbb{P}(y = 0) = 0.7 \rangle$
fi
$\langle (\mathbb{P}(y = 0) = 0) + (\mathbb{P}(y = 0) = 0.7) \rangle$
$\langle \mathbb{P}(y = 0) = 0.7 \rangle$

Recall the derivation rules:

$$\{ p[x/e] \}\ x := e\ \{ p \} \text{ (Assign)}$$

$$\frac{p' \Rightarrow p \qquad \{ p \}\ \mathtt{s}\ \{ q \} \qquad q \Rightarrow q'}{\{ p' \}\ \mathtt{s}\ \{ q' \}} \text{ (Cons)}$$

$$\frac{\{ c?p \}\ \mathtt{s}\ \{ q \} \qquad \{ \neg c?p \}\ \mathtt{s}'\ \{ q' \}}{\{ p \}\ \text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi } \{ q + q' \}} \text{ (If)}$$

While Loops

Recall: $$\frac{p \text{ invariant for } \langle c, \mathtt{s} \rangle}{\{\, p \,\} \text{ while } c \text{ do } \mathtt{s} \text{ od } \{\, p \wedge \mathbb{P}(c){=}0 \,\}} \text{ (While)}$$

When is a predicate p invariant for $\langle c, \mathtt{s} \rangle$?

While Loops

$$\text{Recall:} \quad \frac{p \text{ invariant for } \langle c, \mathtt{s} \rangle}{\{\, p \,\} \text{ while } c \text{ do } \mathtt{s} \text{ od } \{\, p \wedge \mathbb{P}(c){=}0 \,\}} \text{ (While)}$$

When is a predicate p invariant for $\langle c, \mathtt{s} \rangle$?

- If while c do s od always terminates (independent of probabilistic choices), it suffices to show

$$\models \{\, p \,\} \text{ if } c \text{ then } \mathtt{s} \text{ else skip fi } \{\, p \,\}$$

While Loops

$$\text{Recall:} \quad \frac{p \text{ invariant for } \langle c, \mathtt{s} \rangle}{\{\, p \,\} \text{ while } c \text{ do } \mathtt{s} \text{ od } \{\, p \wedge \mathbb{P}(c){=}0 \,\}} \text{ (While)}$$

When is a predicate p invariant for $\langle c, \mathtt{s} \rangle$?

- If while c do s od always terminates (independent of probabilistic choices), it suffices to show

$$\models \{\, p \,\} \text{ if } c \text{ then } \mathtt{s} \text{ else skip fi } \{\, p \,\}$$

- Otherwise, it is additionally required that p is *$\langle c, \mathtt{s} \rangle$-closed* (Definition not trivial and therefore omitted in this talk)

Conclusion

- The idea of *Hoare triples* can be applied to probabilistic programs by using *probabilistic states* and *probabilistic predicates*
- Proving correctness of Hoare triples can be challenging
- A new *derivation system* pH can be used for this purpose

Conclusion

- The idea of *Hoare triples* can be applied to probabilistic programs by using *probabilistic states* and *probabilistic predicates*
- Proving correctness of Hoare triples can be challenging
- A new *derivation system* pH can be used for this purpose

- The approach uses already existing ideas
- Increasing the potential for other approaches and tools to be adapted to work on probabilistic programs

Conclusion

- The idea of *Hoare triples* can be applied to probabilistic programs by using *probabilistic states* and *probabilistic predicates*
- Proving correctness of Hoare triples can be challenging
- A new *derivation system* pH can be used for this purpose

- The approach uses already existing ideas
- Increasing the potential for other approaches and tools to be adapted to work on probabilistic programs

Thank you for your attention!

Semantics for $\mathcal{L}_{\mathrm{pw}}$

- The semantics for $\mathcal{L}_{\mathrm{pw}}$ is given by a mapping

$$\mathcal{D}\colon \mathcal{L}_{\mathrm{pw}} \to (\Pi \to \Pi)$$

  where Π is the set of all probabilistic states
- $\mathcal{D}(\mathtt{s})(\theta) \in \Pi$ is obtained when starting in θ and executing $\mathtt{s}$

$$\mathcal{D}(\mathtt{skip})(\theta) = \theta$$

$$\mathcal{D}(x := e)(\theta) = \theta[x/\mathrm{eval}(e)]$$

$$\mathcal{D}(\mathtt{s}; \mathtt{s}')(\theta) = \mathcal{D}(\mathtt{s}')(\mathcal{D}(\mathtt{s})(\theta))$$

$$\mathcal{D}(\mathtt{s} \oplus_r \mathtt{s}')(\theta) = \Big(r \cdot \mathcal{D}(\mathtt{s})(\theta)\Big) + \Big((1-r) \cdot \mathcal{D}(\mathtt{s}')(\theta)\Big)$$

$$\mathcal{D}(\text{if } c \text{ then } \mathtt{s} \text{ else } \mathtt{s}' \text{ fi})(\theta) = \Big(\mathcal{D}(\mathtt{s})(c?\theta)\Big) + \Big(\mathcal{D}(\mathtt{s}')(\neg c?\theta)\Big)$$

$$\mathcal{D}(\text{while } c \text{ do } \mathtt{s} \text{ od})(\theta) = \text{the least fixed point of } \Psi_{\langle c,\mathtt{s}\rangle}$$

$$\Psi_{\langle c,\mathtt{s}\rangle}(\psi)(\theta) = \psi\Big(\mathcal{D}(\mathtt{s})(c?\theta)\Big) + \neg c?\theta$$

$\langle c, \mathrm{s} \rangle$-closeness: Intuition

- Consider sequences of states $(\theta_n)_{n \in \mathbb{N}}$ where
  - θ_n corresponds to the state reached after n iterations of while c do s od
  - $\theta_n \models p$ for the considered predicate p

$\langle c, \mathrm{s} \rangle$-closeness: Intuition

- Consider sequences of states $(\theta_n)_{n \in \mathbb{N}}$ where
  - θ_n corresponds to the state reached after n iterations of while c do s od
  - $\theta_n \models p$ for the considered predicate p

Example

- Consider: while $\underbrace{(x = 0)}_{=:c}$ do $\underbrace{x := 1 \oplus_{0.5} \text{skip}}_{=:\mathrm{s}}$ od
- One of the sequences might be:

$\theta_n(\sigma_i)$	0.5^n	$1 - 0.5^n$
$\sigma_i(x)$	0	1

$\langle c, \mathrm{s} \rangle$-closeness: Intuition

- Consider sequences of states $(\theta_n)_{n \in \mathbb{N}}$ where
  - θ_n corresponds to the state reached after n iterations of while c do s od
  - $\theta_n \models p$ for the considered predicate p
- The limit of the sequence $(\neg c ? \theta_n)_{n \in \mathbb{N}}$ also has to satisfy p

Example

- Consider: while $\underbrace{(x = 0)}_{=:c}$ do $\underbrace{x := 1 \oplus_{0.5} \text{skip}}_{=:\mathrm{s}}$ od
- One of the sequences might be:

$\theta_n(\sigma_i)$	0.5^n	$1 - 0.5^n$
$\sigma_i(x)$	0	1

$\langle c, \mathtt{s} \rangle$-closeness: Intuition

- Consider sequences of states $(\theta_n)_{n \in \mathbb{N}}$ where
  - θ_n corresponds to the state reached after n iterations of while c do $\mathtt{s}$ od
  - $\theta_n \models p$ for the considered predicate p
- The limit of the sequence $(\neg c ? \theta_n)_{n \in \mathbb{N}}$ also has to satisfy p

Example

- Consider: while $\underbrace{(x = 0)}_{=:c}$ do $\underbrace{x := 1 \oplus_{0.5} \text{skip}}_{=:\mathtt{s}}$ od
- One of the sequences might be:

$\theta_n(\sigma_i)$	0.5^n	$1 - 0.5^n$
$\sigma_i(x)$	0	1

- The limit of

$\neg c ? \theta_n(\sigma_i)$	$1 - 0.5^n$
$\sigma_i(x)$	1

is

$\theta(\sigma_i)$	1
$\sigma_i(x)$	1

$\langle c, \mathrm{s} \rangle$-closeness: Definition

Consider a program while c do s od and a probabilistic predicate p

- A *$\langle c, \mathrm{s} \rangle$-sequence* within p is a sequence of probabilistic states $(\theta_n)_{n \in \mathbb{N}}$ such that
  - $\theta_n \models p$ for all $n \in \mathbb{N}$
  - $(\neg c ? \theta_n)_{n \in \mathbb{N}}$ is an ascending chain
  - the probability for $\neg c$ in the state θ_n is at least the n-step termination ratio, i.e.,

$$\sum_{\sigma \models \neg c} \theta_n(\sigma) \geq r^n_{\langle c, \mathrm{s} \rangle}.$$

where $r^n_{\langle c, \mathrm{s} \rangle}$ is the minimum probability that, starting from a state satisfying p, the loop terminates within n steps

$\langle c, \mathrm{s} \rangle$-closeness: Definition

Consider a program while c do s od and a probabilistic predicate p

- A *$\langle c, \mathrm{s} \rangle$-sequence* within p is a sequence of probabilistic states $(\theta_n)_{n \in \mathbb{N}}$ such that
  - $\theta_n \models p$ for all $n \in \mathbb{N}$
  - $(\neg c ? \theta_n)_{n \in \mathbb{N}}$ is an ascending chain
  - the probability for $\neg c$ in the state θ_n is at least the n-step termination ratio, i.e.,

$$\sum_{\sigma \models \neg c} \theta_n(\sigma) \geq r^n_{\langle c, \mathrm{s} \rangle}.$$

    where $r^n_{\langle c, \mathrm{s} \rangle}$ is the minimum probability that, starting from a state satisfying p, the loop terminates within n steps
- The predicate p is *$\langle c, \mathrm{s} \rangle$-closed* if for all $\langle c, \mathrm{s} \rangle$-sequences $(\theta_n)_{n \in \mathbb{N}}$ within p the least upper bound of the chain $(\neg c ? \theta_n)_{n \in \mathbb{N}}$ satisfies p.