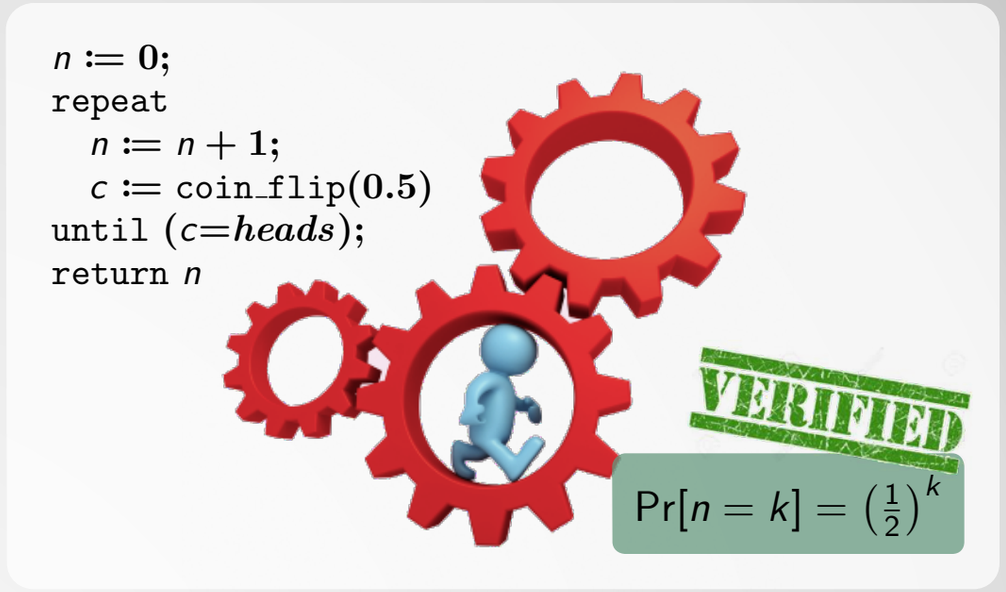
Seminar on

"Verification of Probabilistic Programs"



Lecture 4:

Probabilisitic Hoare Logic

Federico Olmedo

Software Modeling and Verification Group
RWTH AACHEN UNIVERSITY

Agenda

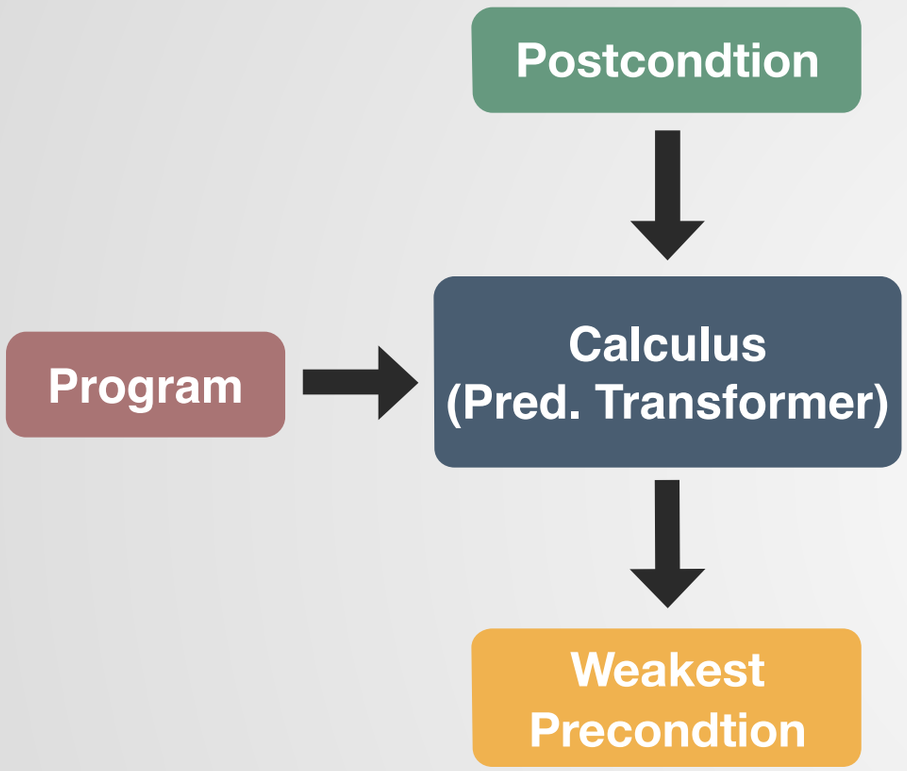
- Recap on Hoare logic
- Extension of Hoare logic to probabilistic programs
- Comparison between expectation transformers and probabilistic Hoare logic
- Summary

Agenda

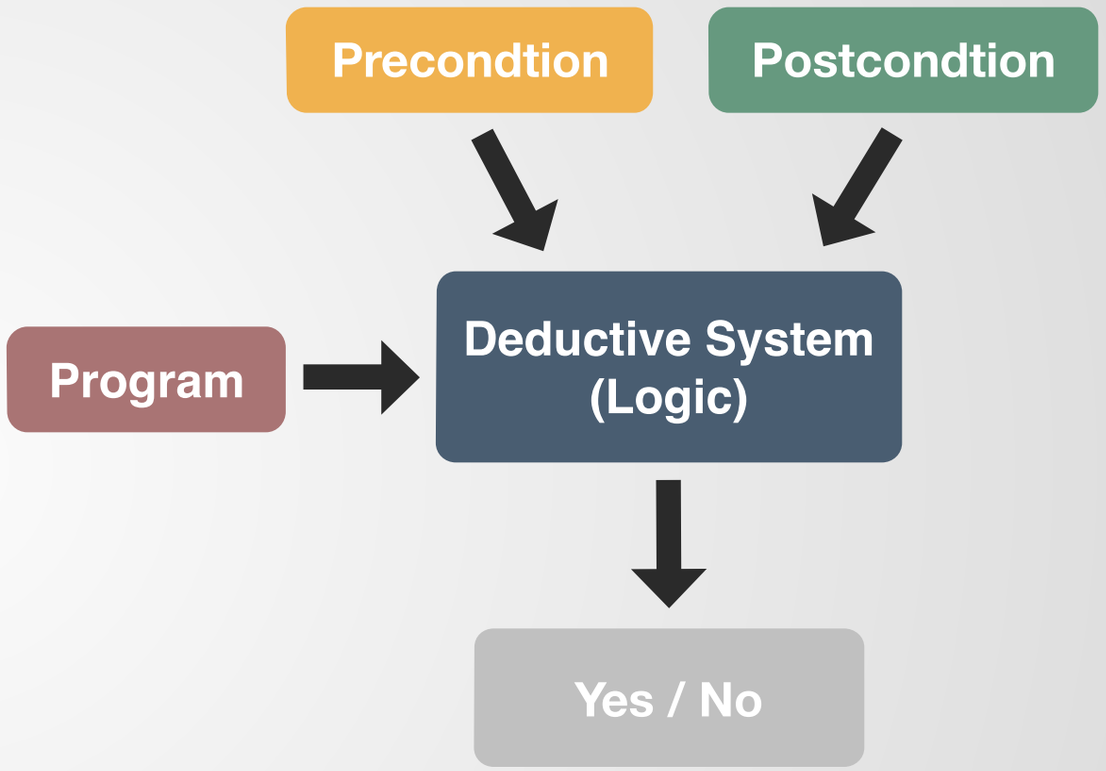
- Recap on Hoare logic
- Extension of Hoare logic to probabilistic programs
- Comparison between expectation transformers and probabilistic Hoare logic
- Summary

Verification Tool Comparison

Weakest Precondition Calculus



Hoare Logics



Hoare Logic — Judgments

Hoare Triple (HT)

$$\{P\}\ c\ \{Q\}$$

- Precondition
- Program
- Postcondition

P and *Q* are predicate over program states, ie $P, Q \subseteq \mathcal{P}(\mathcal{S})$

Interpretation of Hoare Triples

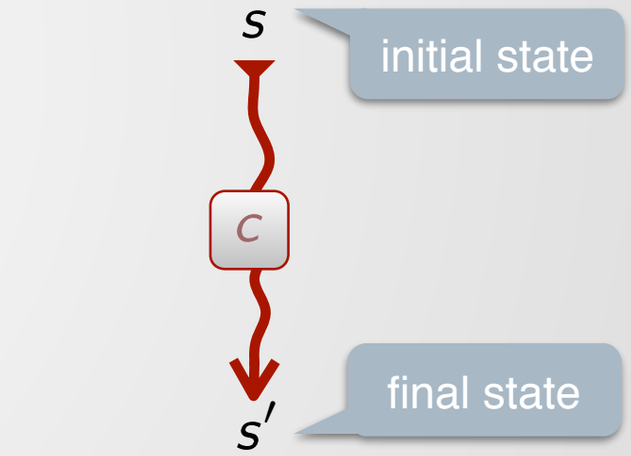
Validity of Hoare Triple {P} c {Q}

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall s \in \mathcal{S} \bullet\ s \models P \implies [\![c]\!](s) \models Q$$

Final state from executing *c* in state *s*

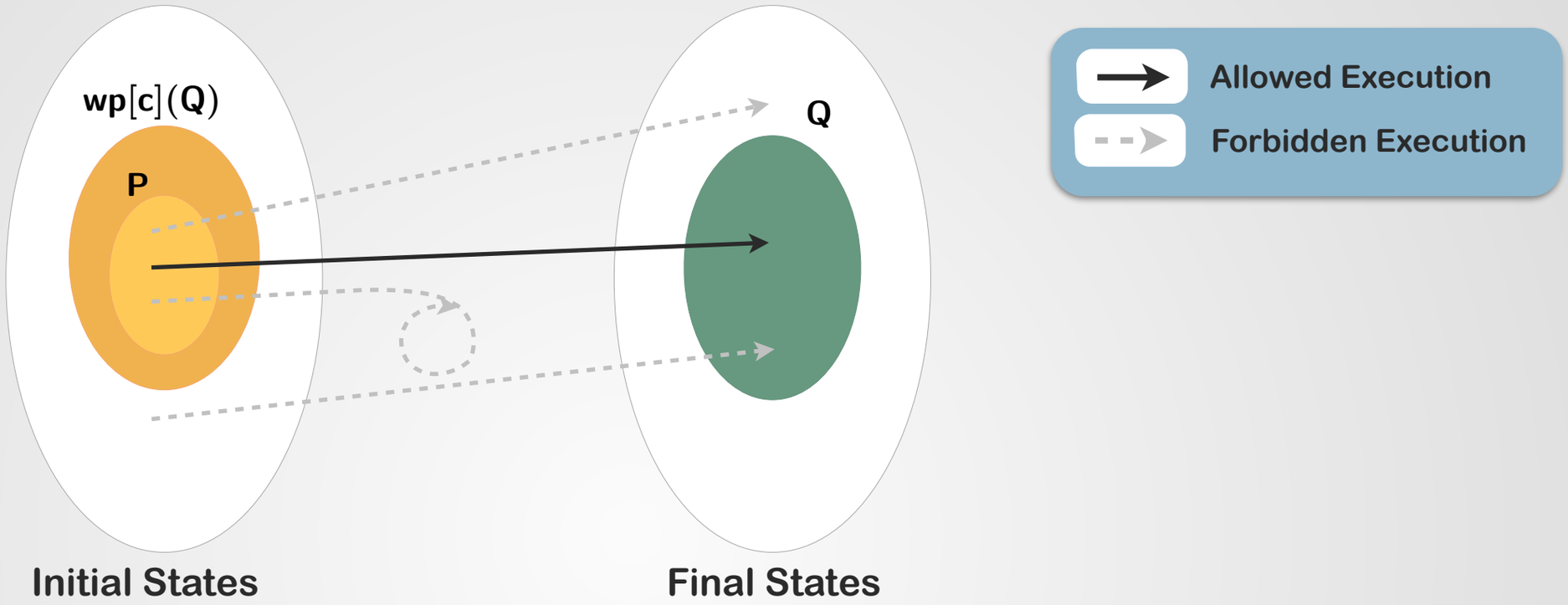


$$s \models P \implies s' \models Q$$

Examples

- $\models \{x \geq 0\}\ x := x{+}2\ \{x \geq 0\}$
- $\models \{a{=}{-}1\}\ a := a{+}1;\ b := b{-}1\ \{a \cdot b{=}0\}$
- $\not\models \{a{=}0\}\ a := a{+}1;\ b := b{-}1\ \{a \cdot b{=}0\}$

Hoare Logic — Connection to Predicate Transformers



$$\models \{P\}\ c\ \{Q\} \qquad \text{iff} \qquad P \implies \text{wp}[c](Q)$$

Hoare Logic — Deductive System

The GCL language

$\mathcal{C}$	$:=$	$\texttt{skip}$	nop
	$\mid$	$\texttt{abort}$	abortion
	$\mid$	$x := E$	assignment
	$\mid$	$\texttt{if}\ G\ \texttt{then}\ \mathcal{C}\ \texttt{else}\ \mathcal{C}$	conditional
	$\mid$	$\texttt{while}\ G\ \texttt{do}\ \mathcal{C}$	while loop
	$\mid$	$\mathcal{C};\ \mathcal{C}$	sequence

Proof System H

$$\frac{}{\vdash \{P\}\ \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort}\ \{Q\}}\ [\text{abort}] \qquad \frac{}{\vdash \{Q[x/E]\}\ x := E\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{P \wedge G\}\ c_1\ \{Q\} \quad \vdash \{P \wedge \neg G\}\ c_2\ \{Q\}}{\vdash \{P\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{Q\}}\ [\text{if}] \qquad \frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\ c\ \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\ c\ \{Q\}}\ [\text{cons}]$$

$$\frac{\vdash \{P\}\ c_1\ \{Q'\} \quad \vdash \{Q'\}\ c_2\ \{Q\}}{\vdash \{P\}\ c_1; c_2\ \{Q\}}\ [\text{seq}] \qquad \frac{\vdash \{I \wedge G \wedge v{=}k\}\ c\ \{I \wedge v{<}k\} \quad \models (I \wedge G \Longrightarrow v{\geq}0)}{\vdash \{I\}\ \texttt{while}\ (G)\ \texttt{do}\ c\ \{I \wedge \neg G\}}\ [\text{while}]$$

Hoare Logic — Deductive System

Soundness and Relative Completeness of the Deductive System

The proof system **H** generates valid Hoare triples, ie for GCL program c

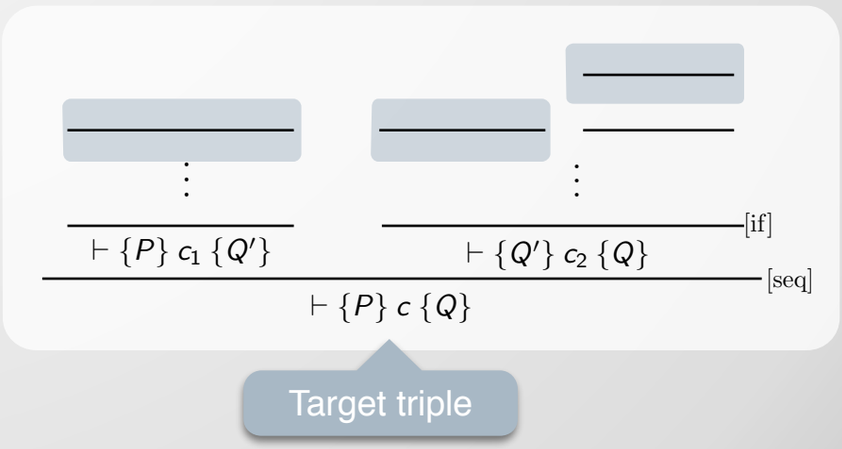
$$\vdash \{P\}\, c\, \{Q\} \implies \models \{P\}\, c\, \{Q\} \qquad \textbf{(soundness)}$$

Moreover, if we have access to an oracle that decides the side conditions of the form $\models (P \implies Q)$, there exists always a derivation in **H** for valid Hoare triples, i.e.

$$\models \{P\}\, c\, \{Q\} \implies \vdash \{P\}\, c\, \{Q\} \qquad \textbf{(relative completeness)}$$

We can prove the validity of a triple $\{P\}\, c\, \{Q\}$ by exhibiting a **derivation tree** in H, where:

- The root is $\vdash \{P\}\, c\, \{Q\}$
- Leaves are axioms ([assg], [abort] or [skip])
- Side conditions of the form $\models (P \implies Q)$ must be discharged ([cons],[while])



Hoare Logic — Example

We want to prove the validity of the following Hoare triple:

$$\{y{=}2 \lor y{=}3\}\ \texttt{if}\ (y{=}2)\ \texttt{then}\ \{x \coloneqq 3{\cdot}y\}\ \texttt{else}\ \{x \coloneqq 2{\cdot}y\}\ \ \{x \bmod 6{=}0\}$$

$$\frac{}{\vdash \{Q[x/E]\}\, x \coloneqq E\, \{Q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{P \land G\}\, c_1\, \{Q\} \quad \vdash \{P \land \neg G\}\, c_2\, \{Q\}}{\vdash \{P\}\, \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\, \{Q\}}\ [\text{if}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\, c\, \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\, c\, \{Q\}}\ [\text{cons}]$$

Hoare Logic — Example

We want to prove the validity of the following Hoare triple:

$$\{y{=}2 \lor y{=}3\}\ \texttt{if}\ (y{=}2)\ \texttt{then}\ \{x \coloneqq 3{\cdot}y\}\ \texttt{else}\ \{x \coloneqq 2{\cdot}y\}\ \{x \bmod 6{=}0\}$$

$\langle y{=}2 \lor y{=}3 \rangle$

$\texttt{if}\ (y{=}2)\ \texttt{then}$

$x \coloneqq 3{\cdot}y$

$\texttt{else}$

$x \coloneqq 2{\cdot}y$

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

$$\frac{}{\vdash \{Q[x/E]\}\, x \coloneqq E\, \{Q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{P \land G\}\, c_1\, \{Q\} \quad \vdash \{P \land \neg G\}\, c_2\, \{Q\}}{\vdash \{P\}\, \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\, \{Q\}}\ [\text{if}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\, c\, \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\, c\, \{Q\}}\ [\text{cons}]$$

Hoare Logic — Example

We want to prove the validity of the following Hoare triple:

$$\{y{=}2 \lor y{=}3\}\ \texttt{if}\ (y{=}2)\ \texttt{then}\ \{x := 3{\cdot}y\}\ \texttt{else}\ \{x := 2{\cdot}y\}\ \{x \bmod 6{=}0\}$$

$\langle y{=}2 \lor y{=}3 \rangle$

$\texttt{if}\ (y{=}2)\ \texttt{then}$

$\quad \langle (y{=}2 \lor y{=}3) \land y{=}2 \rangle$

$\quad x := 3{\cdot}y$

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

$\quad\quad\quad \texttt{else}$

$\quad \langle (y{=}2 \lor y{=}3) \land y{\neq}2 \rangle$

$\quad x := 2{\cdot}y$

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

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

$$\frac{}{\vdash \{Q[x/E]\}\ x := E\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{P \land G\}\ c_1\ \{Q\} \quad \vdash \{P \land \neg G\}\ c_2\ \{Q\}}{\vdash \{P\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{Q\}}\ [\text{if}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\ c\ \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\ c\ \{Q\}}\ [\text{cons}]$$

Hoare Logic — Example

We want to prove the validity of the following Hoare triple:

$$\{y{=}2 \lor y{=}3\}\ \texttt{if}\ (y{=}2)\ \texttt{then}\ \{x := 3{\cdot}y\}\ \texttt{else}\ \{x := 2{\cdot}y\}\ \{x \bmod 6{=}0\}$$

$\langle y{=}2 \lor y{=}3 \rangle$

$\texttt{if}\ (y{=}2)\ \texttt{then}$

$\quad \langle (y{=}2 \lor y{=}3) \land y{=}2 \rangle$

$\quad \langle 3{\cdot}y \bmod 6{=}0 \rangle$

$\quad x := 3{\cdot}y$

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

$\qquad \texttt{else}$

$\quad \langle (y{=}2 \lor y{=}3) \land y{\neq}2 \rangle$

$\quad \langle 2{\cdot}y \bmod 6{=}0 \rangle$

$\quad x := 2{\cdot}y$

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

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

$$\frac{}{\vdash \{Q[x/E]\}\ x := E\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{P \land G\}\ c_1\ \{Q\} \quad \vdash \{P \land \neg G\}\ c_2\ \{Q\}}{\vdash \{P\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{Q\}}\ [\text{if}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\ c\ \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\ c\ \{Q\}}\ [\text{cons}]$$

Agenda

- Recap on Hoare logic
- Extension of Hoare logic to probabilistic programs
- Comparison between expectation transformers and probabilistic Hoare logic
- Summary

Roadmap

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall s \in \mathcal{S} \quad \bullet \quad s \models P \implies [\![c]\!](s) \models Q$$

Roadmap

- View probabilistic programs as distribution transformers

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall \mu \in \mathcal{D}(\mathcal{S}) \bullet \ \mu \models P \implies [\![c]\!](\mu) \models Q$$

Roadmap

- View probabilistic programs as distribution transformers

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

- Consider probabilistic predicates as program assertions

$$\mathsf{PP} \subseteq \mathcal{D}(S) \to \{\mathsf{true}, \mathsf{false}\}$$

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall \mu \in \mathcal{D}(\mathcal{S}) \bullet \quad \mu \models P \implies [\![c]\!](\mu) \models Q$$

Roadmap

- View probabilistic programs as distribution transformers

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

- Consider probabilistic predicates as program assertions

$$\mathsf{PP} \subseteq \mathcal{D}(S) \to \{\mathsf{true}, \mathsf{false}\}$$

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall \mu \in \mathcal{D}(\mathcal{S}) \bullet \ \mu \models P \implies [\![c]\!](\mu) \models Q$$

- Adapt the proof system

Roadmap

- View probabilistic programs as distribution transformers

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

- Consider probabilistic predicates as program assertions

$$\mathrm{PP} \subseteq \mathcal{D}(S) \to \{\mathsf{true}, \mathsf{false}\}$$

$$\models \{P\}\ c\ \{Q\}$$

iff

$$\forall \mu \in \mathcal{D}(\mathcal{S}) \bullet \ \mu \models P \implies [\![c]\!](\mu) \models Q$$

- Adapt the proof system

Probabilistic States — Definition

Deterministic State → Variable valuation

$$\mathcal{S} \triangleq \mathsf{PVar} \to \mathsf{Val}$$

Probabilistic State → Sub-probability distribution over deterministic states

$$\mathcal{D}(\mathcal{S}) \triangleq \left\{\mu \colon \mathcal{S} \to [0,1] \mid \textstyle\sum_{s \in \mathcal{S}} \mu(s) \leq 1\right\}$$

missing probability $1 - w(\mu)$

Total mass of μ

→ partial information or non-termination

Notation for probabilistic states

$$\mu \;=\; 0.1 \cdot \langle x{=}1 \rangle + 0.5 \cdot \langle x{=}2 \rangle$$

Probabilistic States — Operations

- Scaling $(k \cdot \mu)(s) \;=\; k \cdot \mu(s)$ $(k \in [0,1],\ \mu \in \mathcal{D}(\mathcal{S}))$
- Merge $(\mu_1 + \mu_2)(s) \;=\; \mu_1(s) + \mu_2(s)$ $(\mu_1, \mu_2 \in \mathcal{D}(\mathcal{S}))$
- Convex combination $\mu_1 \oplus_r \mu_2 \;=\; r \cdot \mu_1 + (1-r) \cdot \mu_2$ $(r \in [0,1],\ \mu_1, \mu_2 \in \mathcal{D}(\mathcal{S}))$
- Generalized convex combination $\mu \blacktriangleright f \;=\; \sum_{a \in A} \mu(a) \cdot f(a)$ $(\mu \in \mathcal{D}(A),\ f\colon A \to \mathcal{D}(\mathcal{S}))$
- Restriction $(G?\mu)(s) \;=\; \mu(s) \lhd [\![G]\!](s) \rhd 0$ $(G \in \mathrm{BC}\langle \mathrm{PVar} \rangle,\ \mu \in \mathcal{D}(\mathcal{S}))$

Derived properties: $\mu = \mu \oplus_r \mu$ and $\mu = G?\mu + (\neg G)?\mu$

Probabilistic States — Operations

$$\mu_1 = 0.1\cdot\langle x{=}1\rangle + 0.5\cdot\langle x{=}2\rangle$$
$$\mu_2 = 0.2\cdot\langle x{=}1\rangle + 0.1\cdot\langle x{=}3\rangle$$

- Scaling

$$(k\cdot\mu)(s) = k\cdot\mu(s) \qquad (k\in[0,1],\ \mu\in\mathcal{D}(\mathcal{S}))$$

$$0.5\cdot\mu_1 = 0.05\cdot\langle x{=}1\rangle + 0.25\cdot\langle x{=}2\rangle$$

- Merge

$$(\mu_1+\mu_2)(s) = \mu_1(s)+\mu_2(s) \qquad (\mu_1,\mu_2\in\mathcal{D}(\mathcal{S}))$$

$$\mu_1+\mu_2 = 0.3\cdot\langle x{=}1\rangle + 0.5\cdot\langle x{=}2\rangle + 0.1\cdot\langle x{=}3\rangle$$

- Convex combination

$$\mu_1 \oplus_r \mu_2 = r\cdot\mu_1 + (1{-}r)\cdot\mu_2 \qquad (r\in[0,1],\ \mu_1,\mu_2\in\mathcal{D}(\mathcal{S}))$$

$$\mu_1 \oplus_{0.5} \mu_2 = 0.15\cdot\langle x{=}1\rangle + 0.25\cdot\langle x{=}2\rangle + 0.05\cdot\langle x{=}3\rangle$$

- Generalized convex combination

$$\mu \blacktriangleright f = \sum_{a\in A} \mu(a)\cdot f(a) \qquad (\mu\in\mathcal{D}(A),\ f\colon A\to\mathcal{D}(\mathcal{S}))$$

- Restriction

$$(G?\mu)(s) = \mu(s)\lhd[\![G]\!](s)\rhd 0 \qquad (G\in \mathrm{BC}\langle\mathrm{PVar}\rangle,\ \mu\in\mathcal{D}(\mathcal{S}))$$

$$odd(x)?\mu_1 = 0.1\cdot\langle x{=}1\rangle$$

Derived properties: $\mu = \mu\oplus_r\mu$ and $\mu = G?\mu + (\neg G)?\mu$

Programs as Probabilistic State Transformers

Goal: given pGCL program c, define semantic function

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

$$[\![c]\!] : \mathcal{S} \to \mathcal{D}(\mathcal{S})$$

$$\begin{aligned}
[\![\texttt{skip}]\!] &= \lambda s \bullet \eta_s \\
[\![\texttt{abort}]\!] &= \lambda s \bullet \mathbf{0} \\
[\![x := E]\!] &= \lambda s \bullet \eta_{s'} \quad \text{where } s' = s[E/x] \\
[\![\texttt{if } G \texttt{ then } c_1 \texttt{ else } c_2]\!] &= \lambda s \bullet [\![c_1]\!](s) \lhd [\![G]\!](s) \rhd [\![c_2]\!](s) \\
[\![\{c_1\}\ [p]\ \{c_2\}]\!] &= \lambda s \bullet p \cdot [\![c_1]\!](s) + (1-p) \cdot [\![c_2]\!](s) \\
[\![c_1; c_2]\!] &= \lambda s \bullet [\![c_1]\!](s) \blacktriangleright [\![c_2]\!] \\
[\![\texttt{while } G \texttt{ do } c]\!] &= \mathit{lfp}(F) \quad \text{where } F(f) = \lambda s \bullet ([\![c]\!](s) \blacktriangleright f) \lhd [\![G]\!](s) \rhd \eta_s
\end{aligned}$$

We define

$$\begin{aligned}
&[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S}) \\
&[\![c]\!](\mu) \;=\; \mu \blacktriangleright [\![c]\!]
\end{aligned}$$

Roadmap

- Consider probabilistic predicates as program assertions

$$\mathsf{PP} \subseteq \mathcal{D}(S) \to \{\mathsf{true}, \mathsf{false}\}$$

Probabilistic Predicates — Informal Introduction

Intuition

Pre-/post-conditions

$\prec \in \{=, \leq, \ldots\}$

$$\text{probabilistic predicate} \quad = \quad \cdots \quad \mathbb{P}\left(\begin{smallmatrix}\text{deterministic}\\ \text{predicate}\end{smallmatrix}\right) \prec r \quad \cdots$$

Example: $q \;=\; \mathbb{P}(x{\geq}1){=}\frac{1}{4}$

Interpretation: $\mu \models q \quad \text{iff} \quad \sum_{s \models x \geq 1} \mu(s) = \frac{1}{4}$

Examples of Hoare triples

c: $\{x := 0\}\ [0.3]\ \{x := 1\};$
`if` $(x{=}0)$ `then` $\{y := 1\}$ `else` $\{y := 0\}$

- $\models \{\mathbb{P}(\text{true}){=}1\}\ c\ \{\mathbb{P}(x{=}0 \wedge y{=}1){=}0.3\}$
- $\models \{\mathbb{P}(\text{true}){=}r \wedge 0{\leq}r{\leq}1\}\ c\ \{\mathbb{P}(x{=}0 \wedge y{=}1){=}0.3r\}$
- $\not\models \{\mathbb{P}(\text{true}){=}1\}\ c\ \{\mathbb{P}(x{=}0 \wedge y{=}0){>}0\}$
- $\models \{\mathbb{P}(\text{true}){=}1\}\ c\ \{\mathbb{P}(x{=}0){>}0 \wedge \mathbb{P}(y{=}0){>}0\}$

Probabilistic Predicates as Program Assertions

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$

  Variable x is geometrically distributed

- $\{\mathbb{P}(x=1 \lor x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$

  c is almost sure terminating from any initial probabilistic state that "satisfies" $x=1 \lor x=2$

- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

  c preserve the mass of the initial probabilistic state

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \vee x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \wedge pp \mid pp \vee pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

$\mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^x$ → $\exists j \bullet\ \mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \wedge\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \lor x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \land pp \mid pp \lor pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

~~$\mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^x$~~ → $\exists j \bullet\ \mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \land\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\text{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \lor x=2)=1\}\ c\ \{\mathbb{P}(\text{true})=1\}$
- $\{\mathbb{P}(\text{true})=r\}\ c\ \{\mathbb{P}(\text{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \text{true} \mid \text{false} \\
& \mid & e = e \mid e \leq e \mid \dots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \dots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \text{Expr}\langle \text{PVar} \cup \text{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \text{LVar},\ \delta \in \mathbb{R}$
$e \in \text{Expr}\langle \text{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \dots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \dots
\end{array}
$$

$c \in \text{BC}\langle \text{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \land pp \mid pp \lor pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\dots)$ expressions

$\mathbb{P}(c=\text{true}) = \left(\frac{1}{2}\right)^x$ → $\exists j \bullet\ \mathbb{P}(c=\text{true}) = \left(\frac{1}{2}\right)^j \ \land\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \lor x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet dp \mid \exists i \bullet dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \land pp \mid pp \lor pp \\
& \mid & \forall i \bullet pp \mid \exists i \bullet pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

$\mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^x$ → $\exists j \bullet \mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \land\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \lor x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \land pp \mid pp \lor pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

~~$\mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^x$~~ → $\exists j \bullet\ \mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \land\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \vee x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \wedge pp \mid pp \vee pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp
\end{array}
$$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

$\mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^x$ → $\exists j \bullet\ \mathbb{P}(c=\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \wedge\ \mathbb{P}(x=j) = 1$

Probabilistic Predicates — Syntax

- $\{\mathbb{P}(\mathsf{true})=1\}\ c\ \{\forall n \bullet\ n \geq 0 \implies \mathbb{P}(x=n) = (1/2)^n\}$
- $\{\mathbb{P}(x=1 \vee x=2)=1\}\ c\ \{\mathbb{P}(\mathsf{true})=1\}$
- $\{\mathbb{P}(\mathsf{true})=r\}\ c\ \{\mathbb{P}(\mathsf{true})=r\}$

Deterministic Predicates

$$
\begin{array}{rcl}
dp & ::= & \mathsf{true} \mid \mathsf{false} \\
& \mid & e = e \mid e \leq e \mid \ldots \\
& \mid & \neg dp \mid dp \Rightarrow dp \mid \ldots \\
& \mid & \forall i \bullet\ dp \mid \exists i \bullet\ dp
\end{array}
$$

$e \in \mathsf{Expr}\langle \mathsf{PVar} \cup \mathsf{LVar} \rangle$

Real Expressions

$$
\begin{array}{rcl}
e_r & ::= & \mathbb{P}(dp) \mid r \mid \delta \\
& \mid & e_r + e_r \mid e_r * e_r \\
& \mid & e_r^e
\end{array}
$$

$r \in \mathsf{LVar},\ \delta \in \mathbb{R}$
$e \in \mathsf{Expr}\langle \mathsf{LVar} \rangle$

Real-based Conditions

$$
\begin{array}{rcl}
c_r & ::= & c \\
& \mid & e_r = e_r \mid e_r \leq e_r \mid \ldots \\
& \mid & \neg c_r \mid c_r \Rightarrow c_r \mid \ldots
\end{array}
$$

$c \in \mathsf{BC}\langle \mathsf{LVar} \rangle$

Probabilistic Predicates

$$
\begin{array}{rcl}
pp & ::= & c_r \\
& \mid & pp \wedge pp \mid pp \vee pp \\
& \mid & \forall i \bullet\ pp \mid \exists i \bullet\ pp \\
& \mid & k \cdot pp \\
& \mid & pp + pp \\
& \mid & pp \oplus_k pp \\
& \mid & G?pp
\end{array}
$$

$k \in [0,1],\ G \in \mathsf{BC}\langle \mathsf{PVar} \rangle$

WARNING Program variables allowed only within $\mathbb{P}(\ldots)$ expressions

~~$\mathbb{P}(c{=}\mathsf{true}) = \left(\frac{1}{2}\right)^x$~~ → $\exists j \bullet\ \mathbb{P}(c{=}\mathsf{true}) = \left(\frac{1}{2}\right)^j \ \wedge\ \mathbb{P}(x{=}j) = 1$

Probabilistic Predicates — Semantics

The satisfiability relation of a probabilistic state wrt a probabilistic predicate is parametrized by an interpretation that assigns values to logical variables.

$$\mu \models^{\mathcal{I}} p_1 \wedge p_2 \quad \text{iff} \quad \mu \models^{\mathcal{I}} p_1,\ \mu \models^{\mathcal{I}} p_2$$

$$\mu \models^{\mathcal{I}} \forall i \bullet p \quad \text{iff} \quad \mu \models^{\mathcal{I}[i \mapsto v]} p[i/v] \text{ for all } v$$

$$\mu \models^{\mathcal{I}} k \cdot p \quad \text{iff} \quad \exists \mu' \bullet k \cdot \mu' = \mu,\ \mu' \models^{\mathcal{I}} p$$

$$\mu \models^{\mathcal{I}} p_1 + p_2 \quad \text{iff} \quad \exists \mu_1, \mu_2 \bullet \mu_1 + \mu_2 = \mu,\ \mu_1 \models^{\mathcal{I}} p_1,\ \mu_2 \models^{\mathcal{I}} p_2$$

$$\mu \models^{\mathcal{I}} p_1 \oplus_k p_2 \quad \text{iff} \quad \exists \mu_1, \mu_2 \bullet k \cdot \mu_1 + (1-k) \cdot \mu_2 = \mu,\ \mu_1 \models^{\mathcal{I}} p_1,\ \mu_2 \models^{\mathcal{I}} p_2$$

$$\mu \models^{\mathcal{I}} G?p \quad \text{iff} \quad \exists \mu' \bullet G?\mu' = \mu,\ \mu' \models^{\mathcal{I}} p$$

Probabilistic Predicates

$$\begin{aligned} pp \ ::= \ & c_r \\ \mid \ & p \wedge p \mid p \vee p \\ \mid \ & \forall i \bullet pp \mid \exists i \bullet pp \\ \mid \ & k \cdot pp \\ \mid \ & pp + pp \\ \mid \ & pp \oplus_k pp \\ \mid \ & G?pp \end{aligned}$$

$k \in [0,1]$, $G \in \mathsf{BC}\langle \mathsf{PVar} \rangle$

Probabilistic Predicates — Semantics

If p_1 and p_2 are probabilistic predicates, we define

$$\models (p_1 \implies p_2) \quad \triangleq \quad \mu \models^{\mathcal{I}} p_1 \implies \mu \models^{\mathcal{I}} p_2 \ \text{ for all } \mathcal{I} \text{ and } \mu$$

Intricacy

$$p \oplus_k p \implies p$$

If we let

$$p \ = \ \mathbb{P}(x{=}1){=}1 \vee \mathbb{P}(x{=}2){=}1$$

we have

$$\tfrac{1}{2}\cdot\langle x{=}1\rangle + \tfrac{1}{2}\cdot\langle x{=}2\rangle \models p \oplus_{1/2} p$$
$$\tfrac{1}{2}\cdot\langle x{=}1\rangle + \tfrac{1}{2}\cdot\langle x{=}2\rangle \not\models p$$

Probabilistic Hoare Triples

Validity of Hoare Triples (probabilistic case)

Let c be a pGCL program and P, Q probabilistic predicates. Then

$$\models \{P\}\, c\, \{Q\} \qquad \text{iff} \qquad \mu \models^{\mathcal{I}} P \implies [\![c]\!](\mu) \models^{\mathcal{I}} Q \quad \text{forall } \mu, \mathcal{I}$$

Roadmap

- View probabilistic programs as distribution transformes

$$[\![c]\!] : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S})$$

- Consider probabilistic predicates as program assertions

$$\mathsf{PP} \subseteq \mathcal{D}(S) \to \{\mathsf{true}, \mathsf{false}\}$$

- Adapt the proof system

Proof System pH

$$\frac{}{\vdash \{p\}\ \texttt{skip}\ \{p\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort}\ \{q\}}\ [\text{abort}] \qquad \frac{}{\vdash \{q[x/E]\}\ x \coloneqq E\ \{q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{p\}\ c_1\ \{q'\} \quad \vdash \{q'\}\ c_2\ \{q\}}{\vdash \{p\}\ c_1; c_2\ \{q\}}\ [\text{seq}] \qquad \frac{\models (p \Longrightarrow p') \quad \vdash \{p'\}\ c\ \{q'\} \quad \models (q' \Longrightarrow q)}{\vdash \{p\}\ c\ \{q\}}\ [\text{cons}]$$

$$\frac{\vdash \{G?p\}\ c_1\ \{q_1\} \quad \vdash \{(\neg G)?p\}\ c_2\ \{q_2\}}{\vdash \{p\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{q_1 + q_2\}}\ [\text{if}] \qquad \frac{\{p\}\ c_1\ \{q_1\} \quad \{p\}\ c_2\ \{q_2\}}{\{p\}\ \ c_1\ [p]\ c_2\ \ \{q_1 \oplus_p q_2\}}\ [\text{pchoice}]$$

$$\frac{\vdash \{p\}\ \texttt{if}\ \ G\ \texttt{then}\ c\ \texttt{else}\ \texttt{skip}\ \{p\} \qquad p \text{ is } \langle G, c\rangle\text{-closed}}{\vdash \{p\}\ \texttt{while}\ (G)\ \texttt{do}\ c\ \{p \wedge \mathbb{P}(G) = 0\}}\ [\text{while}]$$

Proof System pH

$$\frac{}{\vdash \{p\}\ \texttt{skip}\ \{p\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort}\ \{q\}}\ [\text{abort}] \qquad \frac{}{\vdash \{q[x/E]\}\ x := E\ \{q\}}\ [\text{assgn}]$$

$$\frac{\vdash \{p\}\ c_1\ \{q'\} \quad \vdash \{q'\}\ c_2\ \{q\}}{\vdash \{p\}\ c_1; c_2\ \{q\}}\ [\text{seq}] \qquad \frac{\models (p \Longrightarrow p') \quad \vdash \{p'\}\ c\ \{q'\} \quad \models (q' \Longrightarrow q)}{\vdash \{p\}\ c\ \{q\}}\ [\text{cons}]$$

$$\frac{\vdash \{G?p\}\ c_1\ \{q_1\} \quad \vdash \{(\neg G)?p\}\ c_2\ \{q_2\}}{\vdash \{p\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{q_1 + q_2\}}\ [\text{if}] \qquad \frac{\{p\}\ c_1\ \{q_1\} \quad \{p\}\ c_2\ \{q_2\}}{\{p\}\ \ c_1\ [p]\ c_2\ \ \{q_1 \oplus_p q_2\}}\ [\text{pchoice}]$$

$$\frac{\vdash \{p\}\ \texttt{if}\ \ G\ \texttt{then}\ c\ \texttt{else skip}\ \{p\} \qquad p \text{ is } \langle G, c\rangle\text{-closed}}{\vdash \{p\}\ \texttt{while}\ (G)\ \texttt{do}\ \ c\ \{p \wedge \mathbb{P}(G) = 0\}}\ [\text{while}]$$

$$\frac{\{p_1\}\ c\ \{q\} \quad \{p_2\}\ c\ \{q\}}{\{p_1 \vee p_2\}\ c\ \{q\}}[\text{or}] \qquad \frac{\{p\}\ c\ \{q_1\} \quad \{p\}\ c\ \{q_2\}}{\{p\}\ c\ \{q_1 \wedge q_2\}}[\text{and}]$$

$$\frac{\{p\}\ c\ \{q\} \quad j \notin FV(p)}{\{\exists j \bullet\ p\}\ c\ \{q\}}[\text{exists}] \qquad \frac{\{p\}\ c\ \{q\} \quad j \notin FV(q)}{\{p\}\ c\ \{\forall j \bullet\ q\}}[\text{forall}]$$

$$\frac{\{p\}\ c\ \{q\}}{\{r \cdot p\}\ c\ \{r \cdot q\}}[\text{lin}\cdot] \qquad \frac{\{p_1\}\ c\ \{q_1\} \quad \{p_2\}\ c\ \{q_2\}}{\{p_1 + p_2\}\ c\ \{q_1 + q_2\}}[\text{lin}+]$$

Proof System pH

Soundness of the Deductive System

The proof system **pH** generates valid Hoare triples, ie for pGCL program c

$$\vdash \{p\}\, c\, \{q\} \implies \models \{p\}\, c\, \{q\}$$

The completeness of the system is an open problem.

Proof System pH — Application Example

We want to verify

$$\models \{\mathbb{P}(\text{true})=1\}\ c\ \{\mathbb{P}(y=0)=0.7\}$$

c: $\{x := 0\}\ [0.3]\ \{x := 1\};$
$\texttt{if}\ (x=0)\ \texttt{then}\ \{y := 1\}\ \texttt{else}\ \{y := 0\}$

$$\frac{\vdash \{G?p\}\ c_1\ \{q_1\} \quad \vdash \{(\neg G)?p\}\ c_2\ \{q_2\}}{\vdash \{p\}\ \texttt{if}\ (G)\ \texttt{then}\ \{c_1\}\ \texttt{else}\ \{c_2\}\ \{q_1 + q_2\}}\ [\text{if}] \qquad \frac{\{p\}\ c_1\ \{q_1\} \quad \{p\}\ c_2\ \{q_2\}}{\{p\}\ c_1\ [p]\ c_2\ \{q_1 \oplus_p q_2\}}\ [\text{pchoice}]$$

$\langle\mathbb{P}(\text{true})=1\rangle$
$\{x := 0\}\ [0.3]\ \{x := 1\};$
$\texttt{if}\ (x=0)\ \texttt{then}$
$\quad y := 1$
$\qquad\quad \texttt{else}$
$\quad y := 0$
$\langle\mathbb{P}(y=0)=0.7\rangle$

[seq]

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

$\langle\mathbb{P}(x\neq 0)=0.7\rangle$
$\texttt{if}\ (x=0)\ \texttt{then}$
$\quad y := 1$
$\qquad\quad \texttt{else}$
$\quad y := 0$
$\langle\mathbb{P}(y=0)=0.7\rangle$

[cons]

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

[cons]

$\langle\mathbb{P}(x\neq 0)=0.7\rangle$
$\texttt{if}\ (x=0)\ \texttt{then}$
$\quad y := 1$
$\qquad\quad \texttt{else}$
$\quad y := 0$
$\langle\mathbb{P}(y=0)=0+\mathbb{P}(y=0)=0.7\rangle$

[pchoice]

$\langle\mathbb{P}(\text{true})=1\rangle$
$x := 0$
$\langle\mathbb{P}(x=0)=1\rangle$

[cons+assg]

$\langle\mathbb{P}(\text{true})=1\rangle$
$x := 1$
$\langle\mathbb{P}(x\neq 0)=1\rangle$

[cons+assg]

[if]

$\langle(x=0)?\mathbb{P}(x\neq 0)=0.7\rangle$
$\quad y := 1$
$\langle\mathbb{P}(y=0)=0\rangle$

[cons+assg]

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

Proof System pH — Loop Rule

$$\frac{\vdash \{p\}\ \texttt{if}\ G\ \texttt{then}\ c\ \texttt{else skip}\ \{p\} \qquad p \text{ is } \langle G, c\rangle\text{-closed}}{\vdash \{p\}\ \texttt{while}\,(G)\,\texttt{do}\ c\ \{p \wedge \mathbb{P}(G) = 0\}}\ [\text{while}]$$

$\langle G, c\rangle$-closedness of p

Intuition

- The sequence of probabilistic states obtained by repeated iterations of the loop from an initial state satisfying p has a least upper bound satisfying p.
- If the loop is bounded all invariants are $\langle G, c\rangle$-closed.

Formal denifition

- Far from elementary
- Requires ad hoc reasoning for being established

Agenda

- Recap on Hoare logic
- Extension of Hoare logic to probabilistic programs
- Comparison between expectation transformers and probabilistic Hoare logic
- Summary

Predicate Transformers vs Hoare Logic

Predicate transformer

✔ Allows reasoning about expected values of program variables.

✘ Probability of events appear as pre-conditions

$$0.3 \cdot [P] \Rrightarrow \mathsf{wp}[c]([Q])$$

✔ Reasoning about loops is straightforward

✘ Requires independent computations for different postconditions

$$0.3 \cdot [P] \Rrightarrow \mathsf{wp}[c]([Q])$$
$$0.8 \cdot [P] \Rrightarrow \mathsf{wp}[c]([R])$$

Hoare logic

✘ Allows reasoning only about the probability of events

✔ Hoare triples are intuitive and easy to understand

$$\{\mathbb{P}(P){=}1\}\ c\ \{\mathbb{P}(Q){\geq}0.3\}$$

✘ Closedness property of invariants is involved

✔ Allows encoding multiple assertions in one judgment

$$\{\mathbb{P}(P){=}1\}\ c\ \{\mathbb{P}(Q){\geq}0.3 \wedge \mathbb{P}(R){\geq}0.8\}$$

Agenda

- Recap on Hoare logic
- Extension of Hoare logic to probabilistic programs
- Comparison between expectation transformers and probabilistic Hoare logic
- Summary

Summary

Hoare logic meets probabilistic programs

$$\models \{\mathbb{P}(P){=}1\}\ c\ \{\mathbb{P}(Q_1){=}0.5 \wedge \mathbb{P}(Q_2){\geq}0.8\}$$