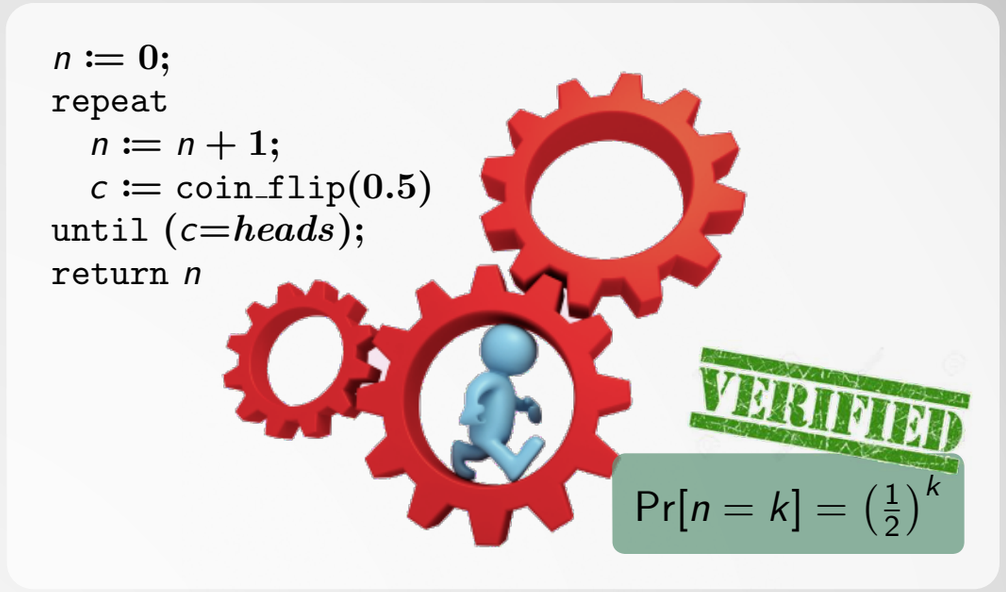
Seminar on

"Verification of Probabilistic Programs"



Lecture 5:

Probabilistic Relational Hoare Logic I

Federico Olmedo

Software Modeling and Verification Group
RWTH AACHEN UNIVERSITY

Agenda

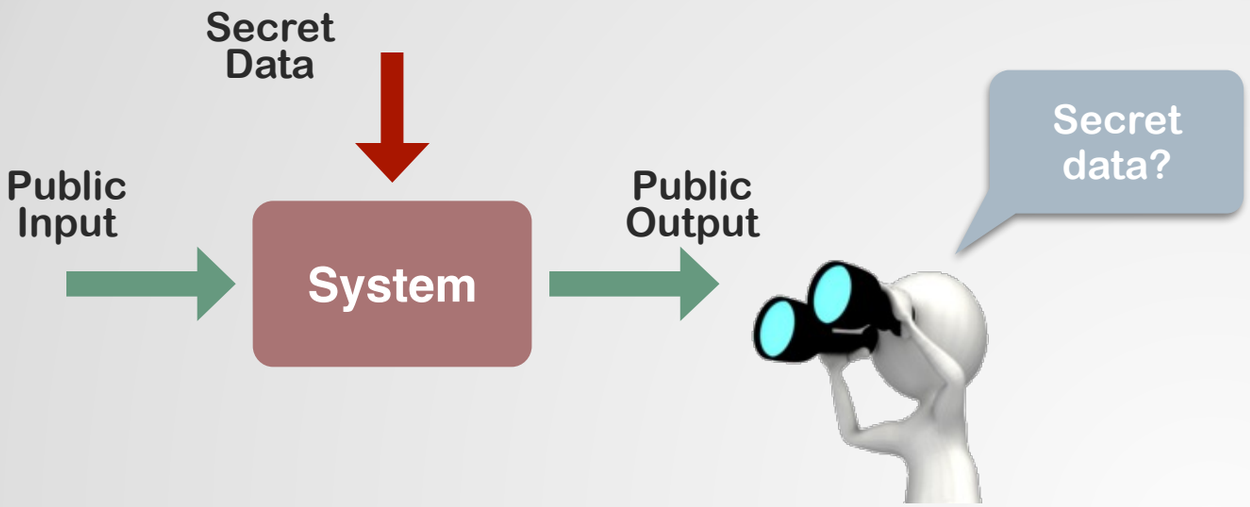
- Relational Hoare logic
- Extension of relational Hoare logic to probabilistic programs

Agenda

- Relational Hoare logic
- Extension of Relational Hoare logic to probabilistic programs

Non-Interference — Introduction

Intuition



Confidentiality Policy

There is no information flow from the **secret** part of a system to the **public** part of the system.

Examples of disallowed programs

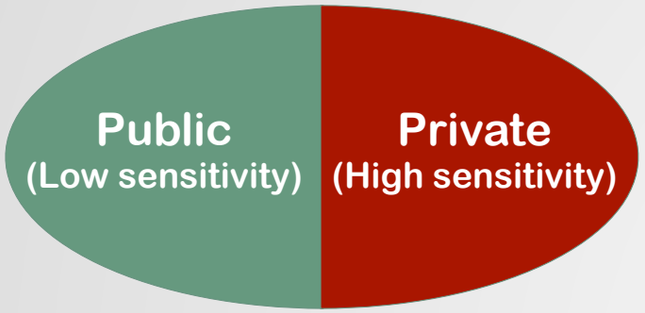
$$output := aux \,||\, secret\_key$$

$$aux := aux \oplus secret\_key;$$
$$output := aux \,||\, message$$

$$\texttt{if } (secret\_key \bmod 2 = 0) \texttt{ then}$$
$$\quad output := 0^n$$
$$\texttt{else}$$
$$\quad output := 1^n$$

Non-Interference — Formal Definition

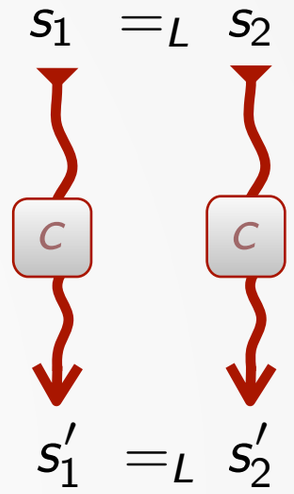
Program Variable Classification



c is non-interferent iff

$$s_1 =_L s_2 \implies s_1' =_L s_2'$$

equality on public variables



Non-interference is an Hyperproperty

Can we model non-interference through Hoare triples?

Non-interference relates **two** different **executions** of a program

Not captured by Hoare triples

Reason about **single** program **executions**

Possible solution

Non-interference is an Hyperproperty

Can we model non-interference through Hoare triples?

Non-interference relates **two** different **executions** of a program → Not captured by Hoare triples

Reason about **single** program **executions**

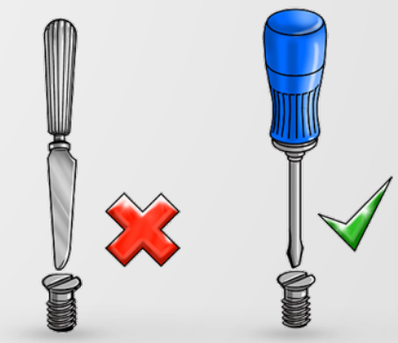
Possible solution

(1) Simulate the pair of executions using one single program *P:*

$$P = c; c'$$

Prime all variables in c

(2) Use Hoare logic to reason about *P.*

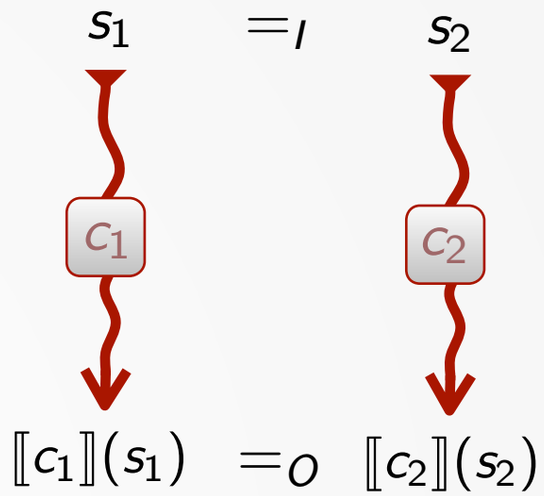


Not a satisfactory solution

Generalising Non-interference: Observational Equivalence

c_1 and c_2 are observationally equivalent wrt input set of variables I and output set of variables O iff

$$s_1 =_I s_2 \implies [\![c_1]\!](s_1) =_O [\![c_2]\!](s_2) \qquad \forall\, s_1, s_2$$



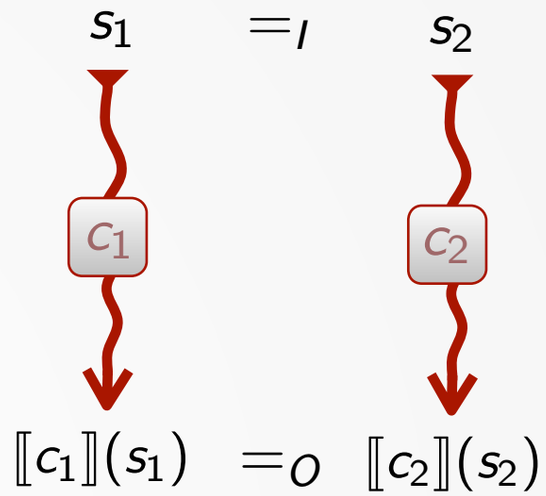
Observational equivalence is a relational property:

- Involves **two** (possibly different) **programs**;
- Pre- and post-conditions are **relations** (rather than predicates) over program states

Generalising Non-interference: Observational Equivalence

c_1 and c_2 are observationally equivalent wrt input set of variables I and output set of variables O iff

$$s_1 =_I s_2 \implies [\![c_1]\!](s_1) =_O [\![c_2]\!](s_2) \qquad \forall\, s_1, s_2$$



Observational equivalence is a relational property:

- Involves **two** (possibly different) **programs**;
- Pre- and post-conditions are **relations** (rather than predicates) over program states

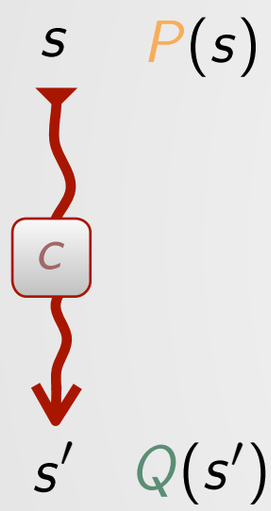
Nick Benton
[POPL '04]

RELATIONAL HOARE LOGIC

Relational Hoare Logic

Standard Hoare Logic

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



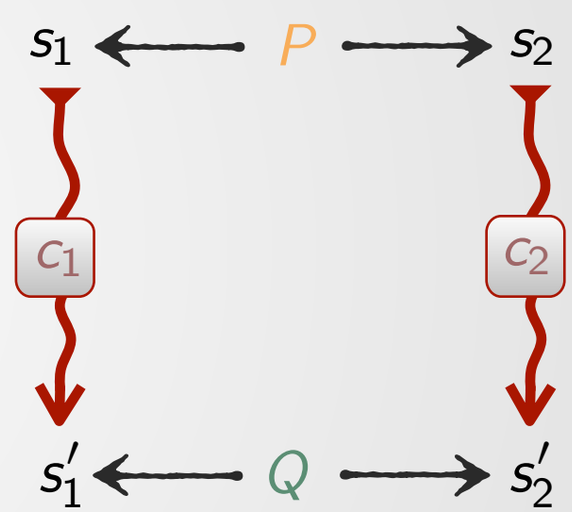
$$\models \{P\}\ c\ \{Q\}$$

iff

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

Relational Hoare Logic

$$\{P\}\ c_1 \sim c_2\ \{Q\}$$



$$\models \{P\}\ c_1 \sim c_2\ \{Q\}$$

iff

$$\forall s_1, s_2 \in \mathcal{S} \bullet\ s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ Q\ [\![c_2]\!](s_2)$$

Relational Hoare Triples

Examples

- $\models \{y_{\langle 1\rangle}+1 = x_{\langle 2\rangle}\}\ \ z := y+1 \ \sim\ z := x\ \ \{z_{\langle 1\rangle} = z_{\langle 2\rangle}\}$

- $\models \{b_{\langle 1\rangle} = \neg b_{\langle 2\rangle}\}\ \begin{array}{l}\texttt{if } b \texttt{ then } x := 0\\ \texttt{else } x := 1\end{array}\ \sim\ \begin{array}{l}\texttt{if } b \texttt{ then } y := 1\\ \texttt{else } y := 0\end{array}\ \ \{x_{\langle 1\rangle} = y_{\langle 2\rangle}\}$

- $\models \{b_{\langle 1\rangle} = b_{\langle 2\rangle}\}\ \begin{array}{l}\texttt{if } b \texttt{ then } x := 0\\ \texttt{else } x := 1\end{array}\ \sim\ \begin{array}{l}\texttt{if } b \texttt{ then } y := 1\\ \texttt{else } y := 0\end{array}\ \ \{x_{\langle 1\rangle}+y_{\langle 2\rangle} = 1\}$

- $\models \{\equiv\}\ \begin{array}{l}\texttt{while } i<N \texttt{ do}\\ \quad x := y+1\\ \quad i := i+x\end{array}\ \sim\ \begin{array}{l}x := y+1\\ \texttt{while } i<N \texttt{ do } \{\equiv\}\\ \quad i := i+x\end{array}$

Proof System RHL

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x \coloneqq A \sim y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{\underline{\text{true}}\}\ \texttt{abort} \sim \texttt{abort}\ \{Q\}}\ [\text{abort}] \qquad \frac{\vdash \{P\}\ c_1 \sim c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim c_2'\ \{Q\}}{\vdash \{P\}\ c_1; c_1' \sim c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\ c_1 \sim c_2\ \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{cons}]$$

$$\models (P \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})$$

$$\frac{\vdash \{P \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{Q\} \quad \vdash \{P \wedge \neg G_{1\langle 1\rangle}\}\ c_1' \sim c_2'\ \{Q\}}{\vdash \{P\}\ \texttt{if}\ G_1\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim \texttt{if}\ G_2\ \texttt{then}\ c_2\ \texttt{else}\ c_2'\ \{Q\}}\ [\text{if}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}] \qquad \frac{\vdash \{P\}\ c_1 \sim c_2\ \{Q\} \quad \vdash \{P'\}\ c_2 \sim c_3\ \{Q'\}}{\vdash \{P \circ P'\}\ c_1 \sim c_3\ \{Q \circ Q'\}}\ [\text{comp}]$$

Proof System — Limitations

The above proof system

- Only relates programs that are structurally equal.

$$\not\vdash \{\equiv\} \quad \begin{array}{l}\texttt{if } b \texttt{ then } x := 0\\ \texttt{else } x := 0\end{array} \quad \sim \quad x := 0 \quad \{\equiv\}$$

- There exist even pairs of structurally equal programs that cannot be related.

$$\not\vdash \{\equiv\} \quad \begin{array}{l}\texttt{if } b \texttt{ then } x := 0\\ \texttt{else } x := 1\end{array} \quad \sim \quad \begin{array}{l}\texttt{if } \neg b \texttt{ then } x := 1\\ \texttt{else } x := 0\end{array} \quad \{\equiv\}$$

Proof System — Extension

$$\frac{}{\vdash \{\underline{\mathsf{false}}\}\ c_1 \sim c_2\ \{Q\}}\ [\text{contr}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{P \wedge G_{\langle 1\rangle}\}\ c_1 \sim c_2\ \{Q\} \quad \vdash \{P \wedge \neg G_{\langle 1\rangle}\}\ c_1' \sim c_2\ \{Q\}}{\vdash \{P\}\ \texttt{if}\ G\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim c_2\ \{Q\}}\ [\text{c-branch}]$$

$$\frac{}{\vdash \{P \wedge \neg G_{\langle 1\rangle}\}\ \texttt{while}\ G\ \texttt{do}\ c \sim \texttt{skip}\ \{P \wedge \neg G_{\langle 1\rangle}\}}\ [\text{d-while}]$$

To derive

$$\vdash \{\equiv\}\ \begin{array}{l}\texttt{if}\ b\ \texttt{then}\ x := 0\\ \texttt{else}\ x := 1\end{array}\ \sim\ \begin{array}{l}\texttt{if}\ \neg b\ \texttt{then}\ x := 1\\ \texttt{else}\ x := 0\end{array}\ \{\equiv\}$$

we apply the [c-branch] rule twice (and once [inv]) to generate the following proof obligations:

$\vdash \{\equiv \wedge b_{\langle 1\rangle} \wedge b_{\langle 2\rangle}\}\ x := 0 \sim x := 0\ \{\equiv\}$
$\vdash \{\equiv \wedge \neg b_{\langle 1\rangle} \wedge \neg b_{\langle 2\rangle}\}\ x := 1 \sim x := 1\ \{\equiv\}$
] discharged by [assgn] + [cons]

$\vdash \{\equiv \wedge b_{\langle 1\rangle} \wedge \neg b_{\langle 2\rangle}\}\ x := 0 \sim x := 1\ \{\equiv\}$
$\vdash \{\equiv \wedge \neg b_{\langle 1\rangle} \wedge b_{\langle 2\rangle}\}\ x := 1 \sim x := 0\ \{\equiv\}$
] discharged by [contr] + [cons]

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$x := y+1;$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$x := y+1;$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$x := y+1;$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\qquad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\qquad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\qquad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$x := y+1;$

$i := i+x$ $\qquad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \leq 10) \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ i_{\langle 1\rangle} \leq 10 \rangle$

$x := y+1;$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \leq 10) \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\qquad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\qquad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\qquad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ i_{\langle 1\rangle} \leq 10 \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle}+x_{\langle 1\rangle} = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$i := i+x$ $\qquad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \leq 10) \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\texttt{while}\ (i \leq 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \leq 10)\ \texttt{do}$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ i_{\langle 1\rangle} \leq 10 \rangle$

$\langle i_{\langle 1\rangle}+y_{\langle 1\rangle}+1 = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle}+x_{\langle 1\rangle} = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \leq 10) \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$$

$$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \;\wedge\; y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$$

$x := y+1;$ $\quad$ $x := y+1;$

$$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$$

$z := y+1$ $\quad$ $z := x$

$$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \;\wedge\; z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\; x := A \sim y := B\; \{Q\}}\;[\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\; x := A \sim \texttt{skip}\; \{Q\}}\;[\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\; c_1 \sim c_2\; \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\; \texttt{while}\; G_1\; \texttt{do}\; c_1 \sim \texttt{while}\; G_2\; \texttt{do}\; c_2\; \{I \wedge \neg G_{1\langle 1\rangle}\}}\;[\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\; c_2 \sim c_1\; \{Q^{-1}\}}{\vdash \{P\}\; c_1 \sim c_2\; \{Q\}}\;[\text{inv}]$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$$

$x := y+1;$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$$

$\texttt{while}\ (i \le 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \le 10)\ \texttt{do}$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \;\wedge\; i_{\langle 1\rangle} \le 10 \rangle$$

$x := y+1;$

$$\langle i_{\langle 1\rangle} + x_{\langle 1\rangle} = i_{\langle 2\rangle} + x_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$$

$i := i+x$ $\quad$ $i := i+x$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \;\wedge\; x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \;\wedge\; \neg(i_{\langle 1\rangle} \le 10) \rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \;\wedge\; y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$ $\quad$ $x := y+1;$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle} \rangle$

$z := y+1$ $\quad$ $z := x$

$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ y_{\langle 2\rangle}+1 = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\texttt{while}\ (i \le 10)\ \texttt{do}$ $\quad$ $\texttt{while}\ (i \le 10)\ \texttt{do}$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ i_{\langle 1\rangle} \le 10 \rangle$

$\langle i_{\langle 1\rangle}+y_{\langle 1\rangle}+1 = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$x := y+1;$

$\langle i_{\langle 1\rangle}+x_{\langle 1\rangle} = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$i := i+x$ $\quad$ $i := i+x$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \le 10) \rangle$

$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x := A \sim y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}]\}\ x := A \sim \texttt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}]$$

$$\langle y_{\langle 1\rangle} = y_{\langle 2\rangle}\rangle$$

$$\langle y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1 \ \wedge\ y_{\langle 1\rangle}+1 = y_{\langle 2\rangle}+1\rangle$$

$x := y+1;$ $\qquad$ $x := y+1;$

$$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle}+1 = x_{\langle 2\rangle}\rangle$$

$z := y+1$ $\qquad$ $z := x$

$$\langle x_{\langle 1\rangle} = x_{\langle 2\rangle} \ \wedge\ z_{\langle 1\rangle} = z_{\langle 2\rangle}\rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle}\rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ y_{\langle 2\rangle}+1 = y_{\langle 2\rangle}+1\rangle$$

$x := y+1;$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1\rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1\rangle$$

$\texttt{while}\ (i \le 10)\ \texttt{do}$ $\qquad$ $\texttt{while}\ (i \le 10)\ \texttt{do}$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ i_{\langle 1\rangle} \le 10\rangle$$

$x := y+1;$

$$\langle i_{\langle 1\rangle}+x_{\langle 1\rangle} = i_{\langle 2\rangle}+x_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1\rangle$$

$i := i+x$ $\qquad$ $i := i+x$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1\rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle} \ \wedge\ x_{\langle 2\rangle} = y_{\langle 2\rangle}+1 \ \wedge\ \neg(i_{\langle 1\rangle} \le 10)\rangle$$

$$\langle i_{\langle 1\rangle} = i_{\langle 2\rangle} \ \wedge\ y_{\langle 1\rangle} = y_{\langle 2\rangle}\rangle$$

Proof System — Soundness and Incompleteness

Soundness and Completeness of the Deductive System

The proof system **RHL** generates valid relational Hoare triples, ie

$$\vdash \{P\}\, c_1 \sim c_2\, \{Q\} \implies \models \{P\}\, c_1 \sim c_2\, \{Q\} \qquad \textbf{(soundness)}$$

but fails to be complete. For instance the following Hoare triples are valid but not derivable:

- $\{\underline{\text{true}}\}$
  $sum \coloneqq 0;\ i \coloneqq 1;$
  $\texttt{while}\ (i{\leq}N)\ \texttt{do}$
  $\quad sum \coloneqq sum + i{\cdot}j;$
  $\quad i \coloneqq i + 1$
  $\sim$
  $j \coloneqq 1;$
  $\texttt{while}\ (j{\leq}M)\ \texttt{do}$
  $\quad sum \coloneqq sum + i{\cdot}j;$
  $\quad j \coloneqq j + 1;$
  $\{sum_{\langle 1\rangle} = sum_{\langle 2\rangle}\}$

- $\{\underline{\text{true}}\}$
  $x, y, i \coloneqq 0, 1, 0;$
  $\texttt{while}\ (i{\leq}10)\ \texttt{do}$
  $\quad i \coloneqq i{+}1;\ t \coloneqq y;$
  $\quad y \coloneqq y{+}x;\ x \coloneqq t$
  $\sim$
  $x, y, i \coloneqq 0, 1, 0;$
  $\texttt{while}\ (i{\leq}6)\ \texttt{do}$
  $\quad i \coloneqq i{+}1;\ t \coloneqq y;$
  $\quad y \coloneqq y{+}x;\ x \coloneqq t;$
  $\texttt{while}\ (6{<}i{\leq}10)\ \texttt{do}$
  $\quad i \coloneqq i{+}1;\ t \coloneqq y;$
  $\quad y \coloneqq y{+}x;\ x \coloneqq t$
  $\{y_{\langle 1\rangle} = y_{\langle 2\rangle}\}$

Logic for Total Correctness

$$\frac{}{\vdash \{\underline{\mathsf{false}}\}\ \mathtt{abort} \sim \mathtt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

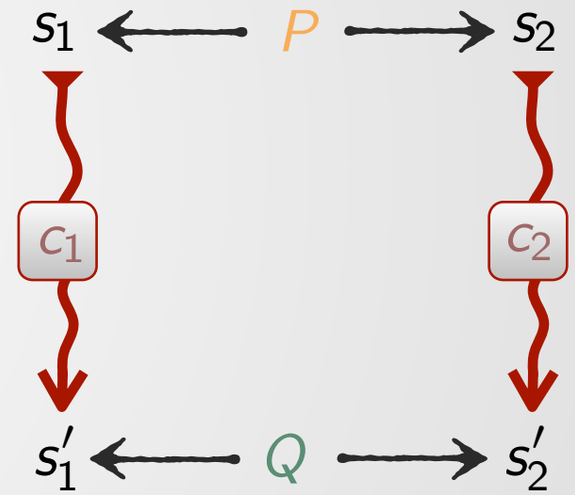
$$\frac{\begin{array}{c}\vdash \{I \wedge G_{1\langle 1\rangle} \wedge v_{\langle 1\rangle}{=}k\}\ c_1 \sim c_2\ \{I \wedge v_{\langle 1\rangle}{<}k\} \\ \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle}) \qquad \models (I \wedge G_{1\langle 1\rangle} \Longrightarrow v_{\langle 1\rangle}{\geq}0)\end{array}}{\vdash \{I\}\ \mathtt{while}\ G_1\ \mathtt{do}\ c_1 \sim \mathtt{while}\ G_2\ \mathtt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{tc-while}]$$

Agenda

- Relational Hoare logic

- Extension of relational Hoare logic to probabilistic programs

Extending the Relational Logic to Probabilistic Programs — Roadmap



Extending the Relational Logic to Probabilistic Programs — Roadmap

- Consider ordinary relations between program states as pre- and post-conditions in Hoare triples:

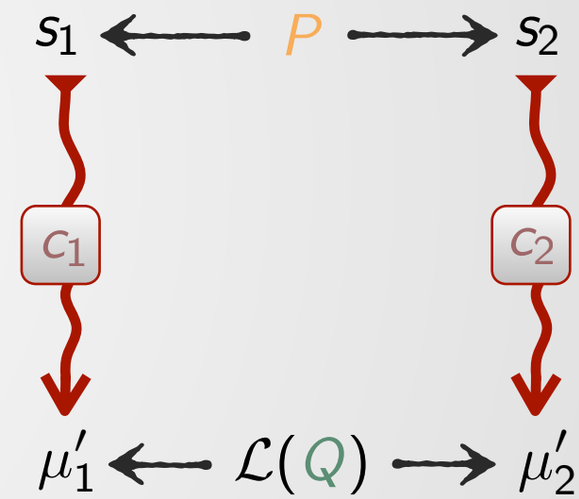
$$P, Q \in \mathcal{P}(\mathcal{S} \times \mathcal{S})$$

$$\{P\}\ c_1 \sim c_2\ \{Q\}$$

- To interprete Hoare triples, define a lifting operator

$$\mathcal{L}(\cdot)\colon \mathcal{P}(\mathcal{S} \times \mathcal{S}) \to \mathcal{P}(\mathcal{D}(\mathcal{S}) \times \mathcal{D}(\mathcal{S}))$$

that lifts relations over states to relations over distributions on states



Extending the Relational Logic to Probabilistic Programs — Roadmap

- Consider ordinary relations between program states as pre- and post-conditions in Hoare triples:

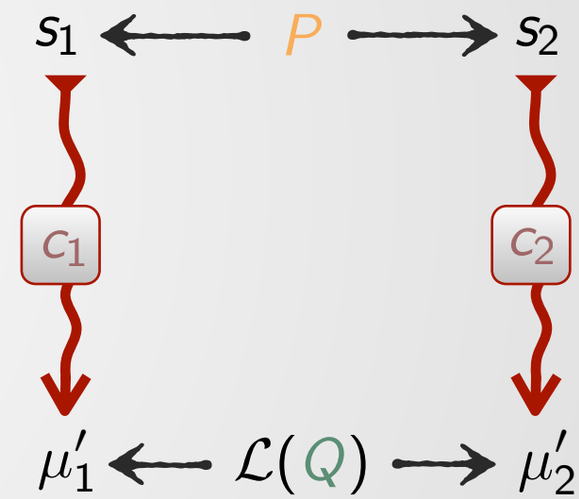
$$P, Q \in \mathcal{P}(\mathcal{S} \times \mathcal{S})$$

$$\{P\}\ c_1 \sim c_2\ \{Q\}$$

- To interprete Hoare triples, define a lifting operator

$$\mathcal{L}(\cdot)\colon \mathcal{P}(\mathcal{S} \times \mathcal{S}) \to \mathcal{P}(\mathcal{D}(\mathcal{S}) \times \mathcal{D}(\mathcal{S}))$$

that lifts relations over states to relations over distributions on states



- Adapt the proof system

Extending the Relational Logic to Probabilistic Programs — Roadmap

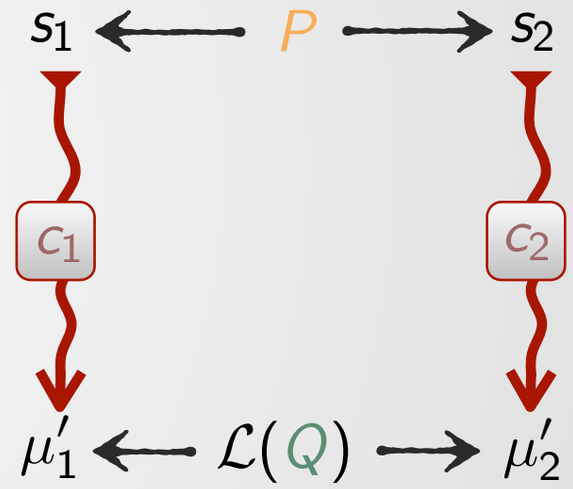
- Consider ordinary relations between program states as pre- and post-conditions in Hoare triples:

$$\{P\}\ c_1 \sim c_2\ \{Q\}$$

- To interprete Hoare triples, define a lifting operator

$$\mathcal{L}(\cdot)\colon \mathcal{P}(\mathcal{S}\times\mathcal{S}) \to \mathcal{P}(\mathcal{D}(\mathcal{S})\times\mathcal{D}(\mathcal{S}))$$

that lifts relations over states to relations over distributions on states



- Adapt the proof system

Lifting Relations to Distributions

$$\mathcal{L}(\cdot)\colon \mathcal{P}(A\times B) \to \mathcal{P}(\mathcal{D}(A)\times\mathcal{D}(B))$$

$$\mu_1\ \mathcal{L}(R)\ \mu_2 \quad\triangleq\quad \exists \mu \in \mathcal{D}(A\times B)\bullet \begin{cases} \pi_1(\mu) = \mu_1 \ \wedge\ \pi_2(\mu) = \mu_2 \\ \mathsf{support}(\mu) \subseteq R \end{cases}$$

$\in \mathcal{P}(A\times B)$

$\in \mathcal{D}(A)$

$\in \mathcal{D}(B)$

* If $\mu \in \mathcal{D}(A\times B)$ we define $\pi_1(\mu)(a) = \sum_{b\in B} \mu(a,b)$ and $\pi_2(\mu)(b) = \sum_{a\in A} \mu(a,b)$.

Lifting Relations to Distributions — Network Flow Interpretation

Decide whether μ_1 and μ_2 are related by $\mathcal{L}(R)$

μ_1	
a_1	0.33
a_2	0.12
a_3	0.22
a_4	0.33

μ_2	
b_1	0.10
b_2	0.45
b_3	0.33

$R = \{(a_1, b_1), (a_1, b_2), (a_3, b_2), (a_4, b_3)\}$

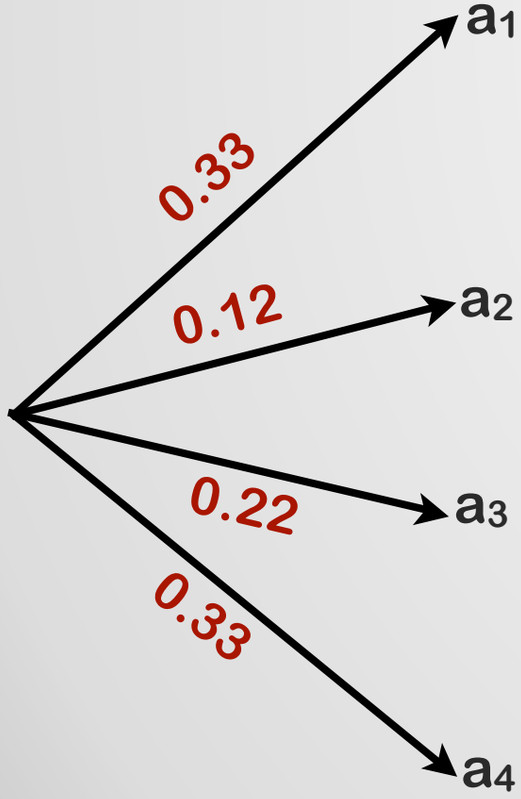
Lifting Relations to Distributions — Network Flow Interpretation

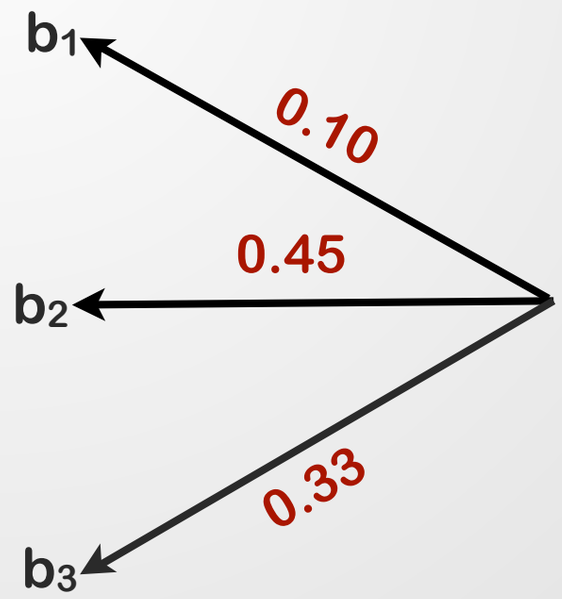
Decide whether μ_1 and μ_2 are related by $\mathcal{L}(R)$

μ_1	
a_1	0.33
a_2	0.12
a_3	0.22
a_4	0.33

μ_2	
b_1	0.10
b_2	0.45
b_3	0.33

$R = \{(a_1, b_1), (a_1, b_2), (a_3, b_2), (a_4, b_3)\}$





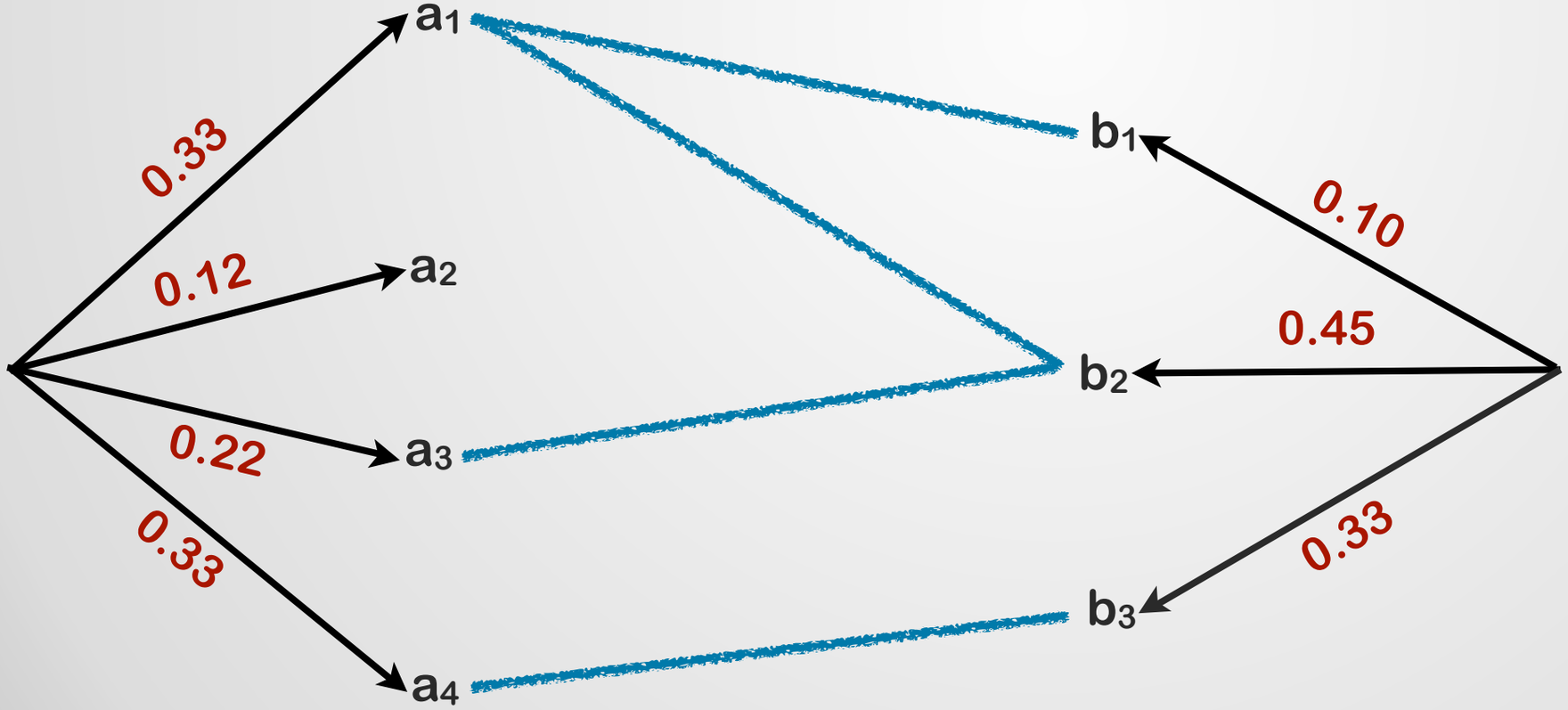
Lifting Relations to Distributions — Network Flow Interpretation

Decide whether μ_1 and μ_2 are related by $\mathcal{L}(R)$

μ_1	
a_1	0.33
a_2	0.12
a_3	0.22
a_4	0.33

μ_2	
b_1	0.10
b_2	0.45
b_3	0.33

$R = \{(a_1, b_1), (a_1, b_2), (a_3, b_2), (a_4, b_3)\}$



Lifting Relations to Distributions — Network Flow Interpretation

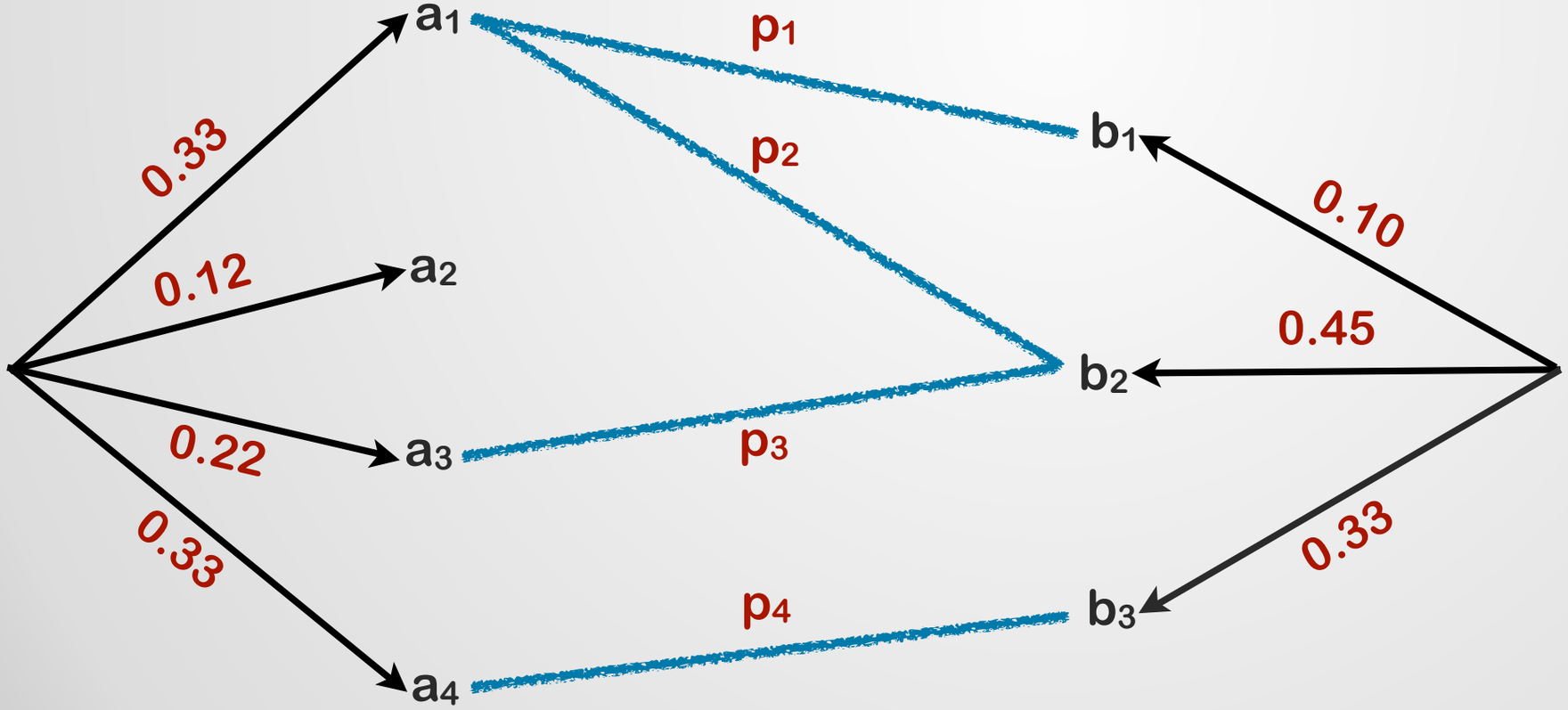
Decide whether μ_1 and μ_2 are related by $\mathcal{L}(R)$

$$0.33 = p_1 + p_2 \qquad 0.10 = p_1$$
$$0.22 = p_3 \qquad 0.45 = p_2 + p_3$$
$$0.33 = p_4 \qquad 0.33 = p_4$$
$$0 \leq p_i \text{ for } i = 1, \ldots, 4$$

μ_1	
a_1	0.33
a_2	0.12
a_3	0.22
a_4	0.33

μ_2	
b_1	0.10
b_2	0.45
b_3	0.33

$R = \{(a_1, b_1), (a_1, b_2), (a_3, b_2), (a_4, b_3)\}$



Lifting Relations to Distributions — Network Flow Interpretation

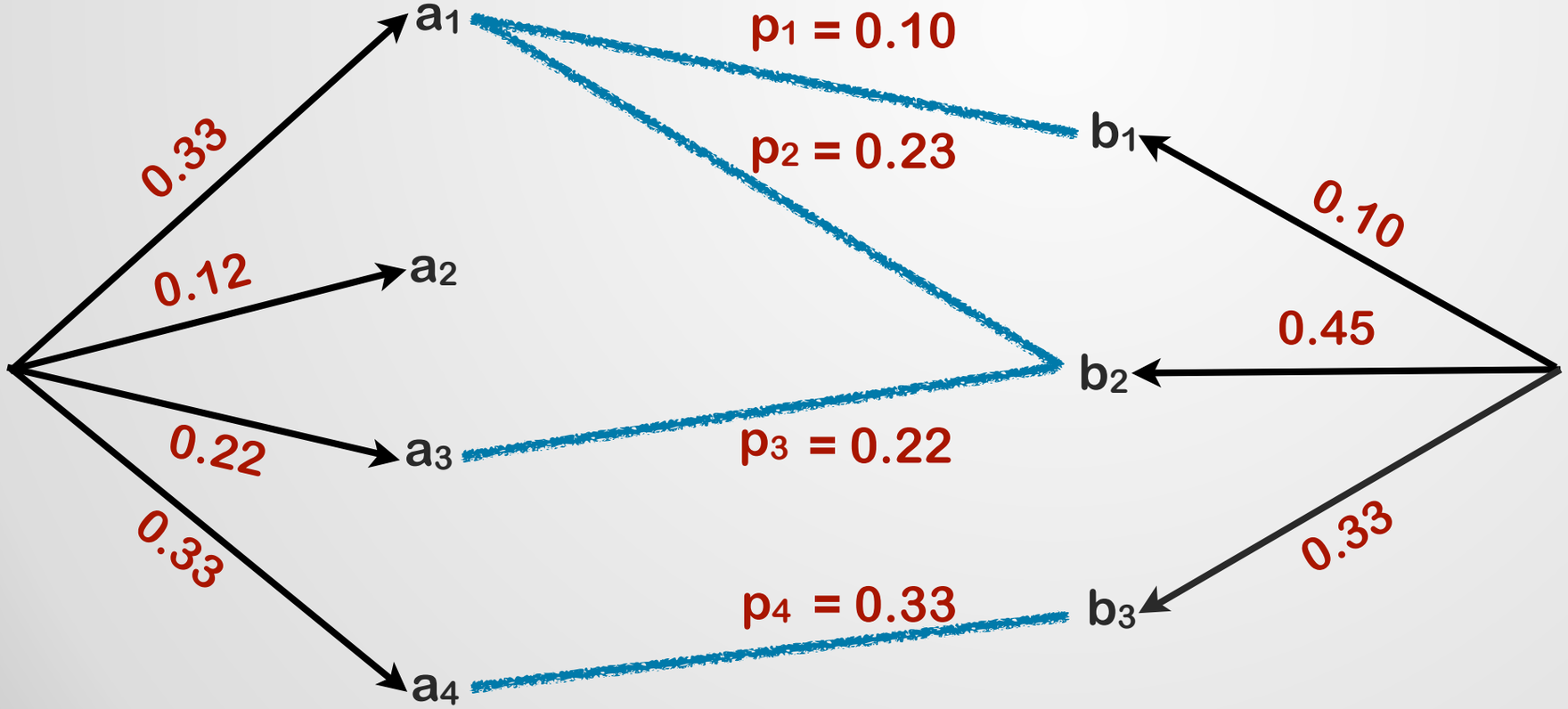
Decide whether μ_1 and μ_2 are related by $\mathcal{L}(R)$

$$0.33 = p_1 + p_2 \qquad 0.10 = p_1$$
$$0.22 = p_3 \qquad 0.45 = p_2 + p_3$$
$$0.33 = p_4 \qquad 0.33 = p_4$$
$$0 \leq p_i \text{ for } i = 1, \ldots, 4$$

μ_1	
a_1	0.33
a_2	0.12
a_3	0.22
a_4	0.33

μ_2	
b_1	0.10
b_2	0.45
b_3	0.33

$R = \{(a_1, b_1), (a_1, b_2), (a_3, b_2), (a_4, b_3)\}$



Witness distribution

μ	
(a_1,b_1)	0.10
(a_1,b_2)	0.23
(a_3,b_2)	0.22
(a_4,b_3)	0.33
…	0

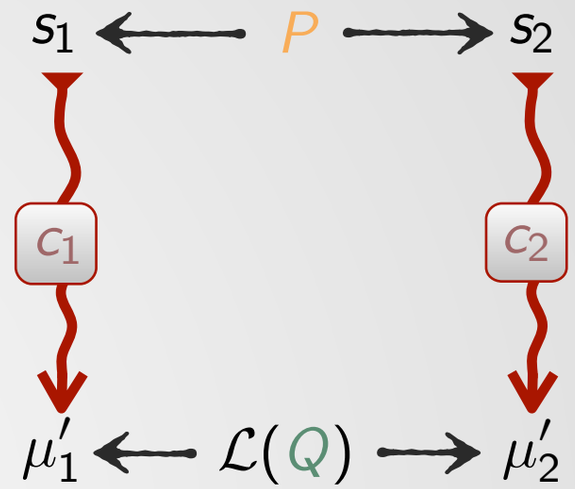
Validity of Hoare Triples

Given probabilistic programs c_1, c_2 and state relations (pre- and post-conditions) P, $Q \in \mathcal{P}(\mathcal{S} \times \mathcal{S})$ we define the **validity** of relational Hoare triple $\{P\}\ c_1 \sim c_2\ \{Q\}$ as follows:

$$\models \{P\}\ c_1 \sim c_2\ \{Q\}$$

$$\text{iff}$$

$$\forall s_1, s_2 \in \mathcal{S} \bullet\ s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ \mathcal{L}(Q)\ [\![c_2]\!](s_2)$$



Proof System pRHL

Language

$\mathcal{C}$	$:=$	$\texttt{skip}$	nop
	$\mid$	$\texttt{abort}$	abortion
	$\mid$	$x := E$	deterministic assignment
	$\mid$	$\mathbf{x :\overset{\$}{=} \mu}$	**random 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

pRHL = **RHL** + rules for random assignments

$$\frac{s_1\ P\ s_2 \ \triangleq\ (\mu_1 \blacktriangleright \lambda v \bullet \eta_{s_1[x_1/v]})\ \mathcal{L}(Q)\ (\mu_2 \blacktriangleright \lambda v \bullet \eta_{s_2[x_2/v]})}{\vdash \{P\}\ x_1 :\overset{\$}{=} \mu_1\ \sim\ x_2 :\overset{\$}{=} \mu_2\ \{Q\}}\ [\text{rand}]$$

$$\frac{s_1\ P\ s_2 \ \triangleq\ (\mu_1 \blacktriangleright \lambda v \bullet \eta_{s_1[x_1/v]})\ \mathcal{L}(Q)\ \eta_{s_2}}{\vdash \{P\}\ x_1 :\overset{\$}{=} \mu_1\ \sim\ \texttt{skip}\ \{Q\}}\ [\text{d-rand}]$$

Specialized rules for random assignments

$$\frac{f : \mathsf{supp}(\mu_1) \to \mathsf{supp}(\mu_2)\ \text{bijective} \qquad \forall v \in \mathsf{supp}(\mu_1) \bullet\ \mu_1(v) = \mu_2(f(v)) \qquad s_1\ P\ s_2\ \triangleq\ \forall v \in \mathsf{supp}(\mu_1) \bullet\ (s_1[x_1/v])\ Q\ (s_2[x_2/f(v)])}{\vdash \{P\}\ x_1 :\overset{\$}{=} \mu_1\ \sim\ x_2 :\overset{\$}{=} \mu_2\ \{Q\}}\ [\text{perm}]$$

$$\frac{\mu_1(\mathcal{S}) = 1 \qquad s_1\ P\ s_2\ \triangleq\ \forall v \in \mathsf{supp}(\mu_1) \bullet\ (s_1[x_1/v])\ Q\ s_2}{\vdash \{P\}\ x_1 :\overset{\$}{=} \mu_1\ \sim\ \texttt{skip}\ \{Q\}}\ [\text{d-perm}]$$

Application example

$$\vdash \{\underline{\mathit{true}}\}\ x_1 :\overset{\$}{=} \mathcal{U}[0 \ldots 10]\ \sim\ x_2 :\overset{\$}{=} \mathcal{U}[2 \ldots 12]\ \{x_{1\langle 1\rangle} + 2 = x_{2\langle 2\rangle}\}$$

An application of the [cons] and [perm] rule with instance $f = \lambda x \bullet\ x + 2$ generates the following proof obligations:

- $f : [0 \ldots 10] \to [2 \ldots 12]$ is bijective
- $v \in [0 \ldots 10] \implies \mathcal{U}[0 \ldots 10](v) = \mathcal{U}[2 \ldots 12](v{+}2)$
- $v \in [0 \ldots 10] \implies v{+}2 = v{+}2$

Using pRHL to Relate the Probabilities of Events

$$\frac{s_1\ P\ s_2 \qquad \models \{P\}\ c_1 \sim c_2\ \{Q\} \qquad Q \implies (A_{\langle 1\rangle} \iff B_{\langle 2\rangle})}{\Pr[c_1(s_1) : A] = \Pr[c_2(s_2) : B]}\ \text{[Pr-Eq]}$$

$$\frac{s_1\ P\ s_2 \qquad \models \{P\}\ c_1 \sim c_2\ \{Q\} \qquad Q \implies (A_{\langle 1\rangle} \implies B_{\langle 2\rangle})}{\Pr[c_1(s_1) : A] \leq \Pr[c_2(s_2) : B]}\ \text{[Pr-Le]}$$

Application examples

- Given programs

$$\begin{aligned} c_1 &= x \xleftarrow{\$} \mathcal{U}\{0,1\}^n;\ y := x \oplus z \\ c_2 &= y \xleftarrow{\$} \mathcal{U}\{0,1\}^n \end{aligned}$$

prove that for any pair of initial states s_1 and s_2 and bitstring w,

$$\Pr[c_1(s_1) : y{=}w] \ = \ \Pr[c_2(s_2) : y{=}w]$$

By rule [Pr-Eq] this follows from showing that

$$\models \{\underline{\text{true}}\}\ c_1 \sim c_2\ \{y_{\langle 1\rangle}{=}y_{\langle 2\rangle}\}$$

- Given programs

$$\begin{aligned} c_1 &= x \xleftarrow{\$} \mathcal{U}\{t,f\};\ \texttt{if}\ (x{=}f)\ \texttt{then}\ x \xleftarrow{\$} \mathcal{U}\{t,f\} \\ c_2 &= x \xleftarrow{\$} \mathcal{U}\{t,f\} \end{aligned}$$

prove that for any pair of initial states s_1 and s_2,

$$\Pr[c_1(s_1) : x{=}f] \ \leq \ \Pr[c_2(s_2) : x{=}f]$$

By rule [Pr-Le] this follows from showing that

$$\models \{\underline{\text{true}}\}\ c_1 \sim c_2\ \{x_{\langle 1\rangle}{=}f \implies x_{\langle 2\rangle}{=}f\}$$

pRHL Intricacy

- Valid judgments do not satisfy conjunctivity of their post-conditions, ie

$$\models \{P\}\, c_1 \sim c_2\, \{Q_1\} \wedge \models \{P\}\, c_1 \sim c_2\, \{Q_2\} \implies \models \{P\}\, c_1 \sim c_2\, \{Q_1 \wedge Q_2\}$$

Consider, for instance, programs

$$\begin{aligned} c_1 &= x \xleftarrow{\$} \mathcal{U}\{0,1\};\ y := 1-x \\ c_2 &= x \xleftarrow{\$} \mathcal{U}\{0,1\};\ y \xleftarrow{\$} \mathcal{U}\{0,1\} \end{aligned}$$

We have

$$\begin{aligned} &\models \{\underline{\mathsf{true}}\}\, c_1 \sim c_2\, \{x_{\langle 1\rangle} = x_{\langle 2\rangle}\} \\ &\models \{\underline{\mathsf{true}}\}\, c_1 \sim c_2\, \{y_{\langle 1\rangle} = y_{\langle 2\rangle}\} \\ &\not\models \{\underline{\mathsf{true}}\}\, c_1 \sim c_2\, \{x_{\langle 1\rangle} = x_{\langle 2\rangle} \wedge y_{\langle 1\rangle} = y_{\langle 2\rangle}\} \end{aligned}$$

- Valid judgments do, however, satisfy disjunctivity of their pre-conditions, ie

$$\models \{P_1\}\, c_1 \sim c_2\, \{Q\} \wedge \models \{P_2\}\, c_1 \sim c_2\, \{Q\} \implies \models \{P_1 \vee P_2\}\, c_1 \sim c_2\, \{Q\}$$

Summary

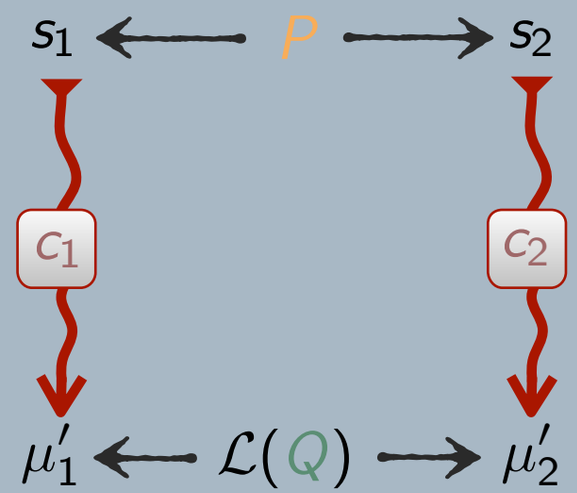
Certain properties require reasoning about **pair of** program **executions**, for instance

- Non-interference
- Observational equivalence
- Program transformation correctness

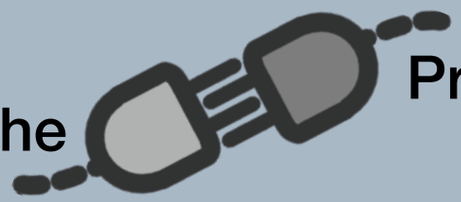
and they **cannot** be modelled through standard Hoare triples.

Relational Hoare Triples

$$\{P\}\ c_1 \sim c_2\ \{Q\}$$



World of the Logic



World of Probabilities

$$\frac{\ldots \quad \models \{P\}\ c_1 \sim c_2\ \{Q\} \quad \ldots}{\Pr[c_1(s_1) : A] = \Pr[c_2(s_2) : B]}$$

Proof System

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{Q[x_{\langle 1\rangle}/A_{\langle 1\rangle}, y_{\langle 2\rangle}/B_{\langle 2\rangle}]\}\ x \coloneqq A \sim y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{}{\vdash \{\underline{\text{true}}\}\ \texttt{abort} \sim \texttt{abort}\ \{Q\}}\ [\text{abort}] \qquad \frac{\vdash \{P\}\ c_1 \sim c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim c_2'\ \{Q\}}{\vdash \{P\}\ c_1; c_1' \sim c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$$\frac{\models (P \Longrightarrow P') \quad \vdash \{P'\}\ c_1 \sim c_2\ \{Q'\} \quad \models (Q' \Longrightarrow Q)}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{cons}]$$

$$\frac{\begin{array}{c}\models (P \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle}) \\ \vdash \{P \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{Q\} \quad \vdash \{P \wedge \neg G_{1\langle 1\rangle}\}\ c_1' \sim c_2'\ \{Q\}\end{array}}{\vdash \{P\}\ \texttt{if}\ G_1\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim \texttt{if}\ G_2\ \texttt{then}\ c_2\ \texttt{else}\ c_2'\ \{Q\}}\ [\text{if}]$$

$$\frac{\vdash \{I \wedge G_{1\langle 1\rangle}\}\ c_1 \sim c_2\ \{I\} \qquad \models (I \Longrightarrow G_{1\langle 1\rangle} = G_{2\langle 2\rangle})}{\vdash \{I\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge \neg G_{1\langle 1\rangle}\}}\ [\text{while}]$$

$$\frac{\vdash \{P^{-1}\}\ c_2 \sim c_1\ \{Q^{-1}\}}{\vdash \{P\}\ c_1 \sim c_2\ \{Q\}}\ [\text{inv}] \qquad \frac{\vdash \{P\}\ c_1 \sim c_2\ \{Q\} \quad \vdash \{P'\}\ c_2 \sim c_3\ \{Q'\}}{\vdash \{P \circ P'\}\ c_1 \sim c_3\ \{Q \circ Q'\}}\ [\text{comp}]$$