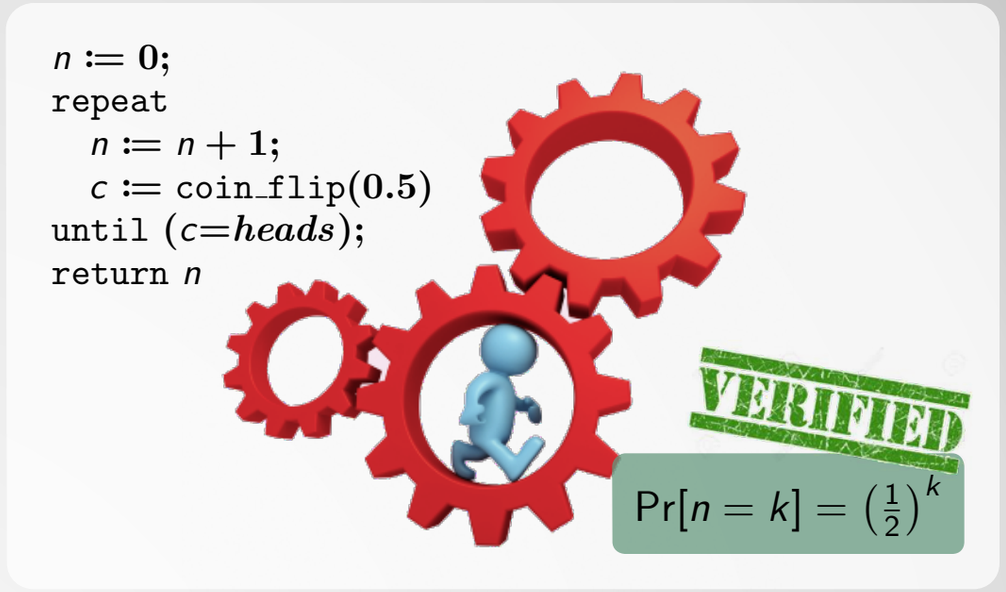
Seminar on

"Verification of Probabilistic Programs"



Lecture 6:

Probabilistic Relational Hoare Logic II

Federico Olmedo

Software Modeling and Verification Group
RWTH AACHEN UNIVERSITY

Agenda

- Recap on relational Hoare logic
- Approximate version of the relational Hoare logic
- Summary

Agenda

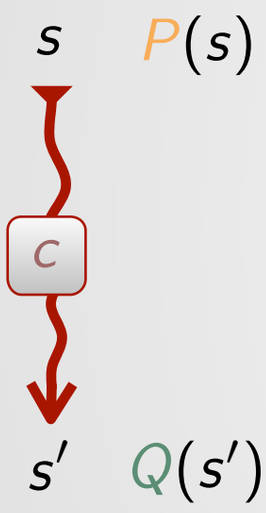
- Recap on relational Hoare logic
- Approximate version of the relational Hoare logic
- Summary

Relational Hoare Logic

Standard Hoare Logic

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

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



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

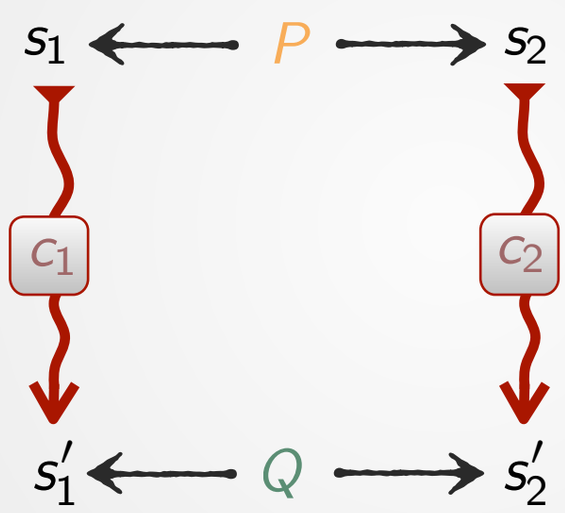
iff

$P(s) \implies Q([\![c]\!](s))$

Relational Hoare Logic

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

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



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

iff

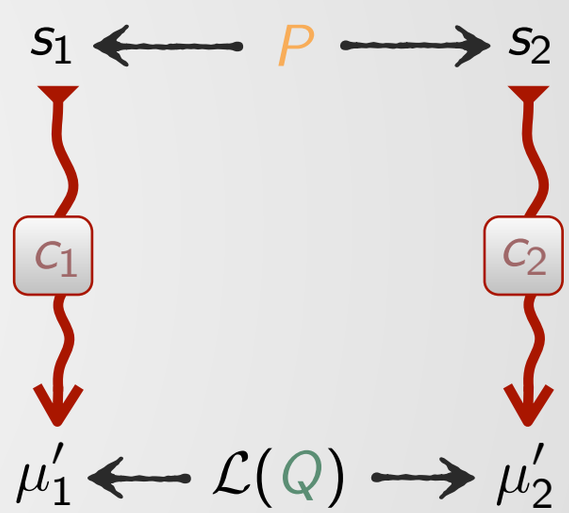
$s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ Q\ [\![c_2]\!](s_2)$

Probabilistic Relational Hoare Logic

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

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

prob. programs



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

iff

$s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ \mathcal{L}(Q)\ [\![c_2]\!](s_2)$

Lifting of Q to a relation over **distributions** on program states

Lifting Relations to Distributions

Lifting of Relations

The operator

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

that lifts relations over sets A, B to relations over distributions on these sets is defined as

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

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

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

Relational Hoare Triples

Examples

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

- $\models \{\underline{\mathit{true}}\}$ $\mathbf{x} \overset{\$}{\coloneqq} \mathcal{U}[\mathbf{0}\ldots\mathbf{10}]$ $\sim$ $x \overset{\$}{\coloneqq} \mathcal{U}[2\ldots 12]$ $\{x\langle 1\rangle + 2 = x\langle 2\rangle\}$

  random assignment

- $\models \{\underline{\mathsf{true}}\}$ $\begin{array}{l}x \overset{\$}{\coloneqq} \mathcal{U}\{t,f\};\\ \texttt{if } (x{=}f) \texttt{ then } x \overset{\$}{\coloneqq} \mathcal{U}\{t,f\}\end{array}$ $\sim x \overset{\$}{\coloneqq} \mathcal{U}\{t,f\}$ $\{x\langle 1\rangle{=}f \implies x\langle 2\rangle{=}f\}$

Proof System pRHL (Two-sided Rules)

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

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

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

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

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

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

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

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 pRHL (One-sided Rules)

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

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

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

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

Using pRHL to Relate the Probabilities of Events

$$\models \{\underline{\mathsf{true}}\} \underbrace{\begin{array}{l} x \xleftarrow{\$} \mathcal{U}[0..10]; \\ x := x+2 \end{array}}_{c_1} \sim \underbrace{x \xleftarrow{\$} \mathcal{U}[2..12]}_{c_2} \{x\langle 1\rangle = x\langle 2\rangle\}$$

$$\therefore \quad \Pr[c_1(s_1) : x \geq 5] = \Pr[c_2(s_2) : x \geq 5] \qquad \forall s_1, s_2$$

Using pRHL to Relate the Probabilities of Events

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

Application example

$$\models \{\underline{\text{true}}\} \quad \underbrace{\begin{array}{l} x \overset{\$}{:=} \mathcal{U}[0..10]; \\ x := x{+}2 \end{array}}_{c_1} \quad \sim \quad \underbrace{x \overset{\$}{:=} \mathcal{U}[2..12]}_{c_2} \quad \{x\langle 1\rangle{=}x\langle 2\rangle\}$$

$$\therefore \quad \Pr[c_1(s_1) : x{\geq}5] \;=\; \Pr[c_2(s_2) : x{\geq}5] \qquad \forall s_1, s_2$$

Approximate Relational Properties of Probabilistic Programs

Program

c_1 : $h := 1-h;$
$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$

is non—interferent $(L=\{l\}, H=\{h\})$

No information flow from *h* to *l*

$\models \{l\langle 1\rangle = l\langle 2\rangle\}\ c_1 \sim c_1\ \{l\langle 1\rangle = l\langle 2\rangle\}$

Program

c_2 : $h := 1-h;$
$l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

is interferent

$\not\models \{l\langle 1\rangle = l\langle 2\rangle\}\ c_2 \sim c_2\ \{l\langle 1\rangle = l\langle 2\rangle\}$

For all pair of initial states s_1 and s_2 such that $s_1(l) = s_2(l)$, it holds

$$\forall \varphi \bullet\ \Pr[c_1(s_1) : \varphi(l)] = \Pr[c_1(s_2) : \varphi(l)]$$

Approximate Relational Properties of Probabilistic Programs

Program

c_1 : $h := 1-h;$
$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$

is non—interferent $(L=\{l\}, H=\{h\})$

No information flow from *h* to *l*

$\models \{l\langle 1\rangle = l\langle 2\rangle\}\ c_1 \sim c_1\ \{l\langle 1\rangle = l\langle 2\rangle\}$

For all pair of initial states s_1 and s_2 such that $s_1(l) = s_2(l)$, it holds

$$\forall \varphi \bullet\ \Pr[c_1(s_1) : \varphi(l)] = \Pr[c_1(s_2) : \varphi(l)]$$

Program

c_2 : $h := 1-h;$
$l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

is ϵ-non—interferent ← APPROXIMATE NON-INTERFERENCE

$\not\models \{l\langle 1\rangle = l\langle 2\rangle\}\ c_2 \sim c_2\ \{l\langle 1\rangle = l\langle 2\rangle\}$

For all pair of initial states s_1 and s_2 such that $s_1(l) = s_2(l)$, it holds

$$\forall \varphi \bullet\ \left|\Pr[c_2(s_1) : \varphi(l)] - \Pr[c_2(s_2) : \varphi(l)]\right| \leq \epsilon$$

Agenda

- Recap on relational Hoare logic
- Approximate version of the relational Hoare logic
- Summary

Approximate Relational Properties of Probabilistic Programs

$$\models \{P\}\ c_1 \sim c_1\ \{I\langle 1\rangle = I\langle 2\rangle\}$$

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \Pr[c_1(s_1) : \varphi(I)] = \Pr[c_1(s_2) : \varphi(I)]$$

or equivalently,

$$\pi_I([\![c_1]\!](s_1)) = \pi_I([\![c_1]\!](s_2))$$

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \left|\Pr[c_2(s_1) : \varphi(I)] - \Pr[c_2(s_2) : \varphi(I)]\right| \leq \epsilon$$

Approximate Relational Properties of Probabilistic Programs

$$\models \{P\}\ c_1 \sim c_1\ \{I\langle 1\rangle = I\langle 2\rangle\}$$

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \Pr[c_1(s_1) : \varphi(I)] \;=\; \Pr[c_1(s_2) : \varphi(I)]$$

or equivalently,

$$\pi_I([\![c_1]\!](s_1)) \;=\; \pi_I([\![c_1]\!](s_2))$$

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \left|\Pr[c_2(s_1) : \varphi(I)] - \Pr[c_2(s_2) : \varphi(I)]\right| \leq \epsilon$$

or equivalently,

$$\Delta_{\mathsf{SD}}\Big(\pi_I([\![c_2]\!](s_1)), \pi_I([\![c_2]\!](s_2))\Big) \leq \epsilon$$

Statistical Distance between Distributions

$$\Delta_{\mathsf{SD}}(\cdot,\cdot) \quad : \quad \mathcal{D}(A)\times\mathcal{D}(A) \to \mathbb{R}_{\geq 0}$$

$$\Delta_{\mathsf{SD}}(\mu_1,\mu_2) \triangleq \sup_{A_0 \subseteq A} \left|\mu_1(A_0) - \mu_2(A_0)\right|$$

- $0 \leq \Delta_{\mathsf{SD}}(\mu_1,\mu_2) \leq 1$ and $\Delta_{\mathsf{SD}}(\mu_1,\mu_2) = 0$ iff $\mu_1 = \mu_2$
- $\Delta_{\mathsf{SD}}(\mu_1,\mu_2) = \Delta_{\mathsf{SD}}(\mu_2,\mu_1)$
- $\Delta_{\mathsf{SD}}(\mu_1,\mu_3) \leq \Delta_{\mathsf{SD}}(\mu_1,\mu_2) + \Delta_{\mathsf{SD}}(\mu_2,\mu_3)$

Approximate Relational Properties of Probabilistic Programs

$$\models \{P\}\ c_1 \sim c_1\ \{I\langle 1\rangle = I\langle 2\rangle\}$$

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \Pr[c_1(s_1) : \varphi(I)] \;=\; \Pr[c_1(s_2) : \varphi(I)]$$

or equivalently,

$$\pi_I([\![c_1]\!](s_1)) \;=\; \pi_I([\![c_1]\!](s_2))$$

$$\models \{P\}\ c_1 \sim_\epsilon c_1\ \{I\langle 1\rangle = I\langle 2\rangle\}$$

APPROXIMATE pRHL

For all pair of initial states s_1 and s_2 such that $s_1\ P\ s_2$, it holds

$$\forall \varphi \bullet\ \left|\Pr[c_2(s_1) : \varphi(I)] - \Pr[c_2(s_2) : \varphi(I)]\right| \leq \epsilon$$

or equivalently,

$$\Delta_{\mathsf{SD}}\Big(\pi_I([\![c_2]\!](s_1)), \pi_I([\![c_2]\!](s_2))\Big) \leq \epsilon$$

Statistical Distance between Distributions

$$\Delta_{\mathsf{SD}}(\cdot,\cdot) \quad : \quad \mathcal{D}(A)\times\mathcal{D}(A) \to \mathbb{R}_{\geq 0}$$

$$\Delta_{\mathsf{SD}}(\mu_1,\mu_2) \triangleq \sup_{A_0 \subseteq A} \left|\mu_1(A_0) - \mu_2(A_0)\right|$$

- $0 \leq \Delta_{\mathsf{SD}}(\mu_1,\mu_2) \leq 1$ and $\Delta_{\mathsf{SD}}(\mu_1,\mu_2) = 0$ iff $\mu_1 = \mu_2$
- $\Delta_{\mathsf{SD}}(\mu_1,\mu_2) = \Delta_{\mathsf{SD}}(\mu_2,\mu_1)$
- $\Delta_{\mathsf{SD}}(\mu_1,\mu_3) \leq \Delta_{\mathsf{SD}}(\mu_1,\mu_2) + \Delta_{\mathsf{SD}}(\mu_2,\mu_3)$

Approximate Relational Properties of Probabilistic Programs

$\epsilon \in \mathbb{R}_{\geq 0},\ \delta \in [0,1]$

Mining process K is **(ϵ,δ)-differentially private** iff for any pair of adjacent databases d_1 and d_2, it holds

differing in only one record

$$\Delta_{e^\epsilon}\Big(K(d_1), K(d_2)\Big) \leq \delta$$

α-Distance between Distributions

Given $\alpha \geq 1$ we define

$$\Delta_\alpha(\cdot,\cdot) \quad : \quad \mathcal{D}(A) \times \mathcal{D}(A) \to \mathbb{R}_{\geq 0}$$

$$\Delta_\alpha(\mu_1,\mu_2) \triangleq \sup_{A_0 \subseteq A} \mu_1(A_0) \dot{-} \alpha\,\mu_2(A_0)$$

- $0 \leq \Delta_\alpha(\mu_1,\mu_2) \leq 1$
- $\Delta_\alpha(\mu,\mu) = 0$ but $\Delta_\alpha(\mu_1,\mu_2) = 0 \implies \mu_1 = \mu_2$
- $\Delta_\alpha(\mu_1,\mu_2) \neq \Delta_\alpha(\mu_2,\mu_1)$
- $\Delta_{\alpha\alpha'}(\mu_1,\mu_3) \leq \Delta_\alpha(\mu_1,\mu_2) + \alpha\,\Delta_{\alpha'}(\mu_2,\mu_3)$

$^\star\ x \dot{-} y \triangleq \max\{x-y, 0\}$

Relational Properties of Probabilistic Programs — Approximate Versions

Different notions are expressed in terms of different "metrics" for comparing distributions

Judgments in approximate **pRHL** should also account for the metric between distributions at stake:

- $\{P\}\ c_1 \sim_{\mathsf{SD},\epsilon}\ c_2\ \{Q\}$ → statistical distance
- $\{P\}\ c_1 \sim_{\alpha,\epsilon}\ c_2\ \{Q\}$ → α-distance
- $\{P\}\ c_1 \sim_{\mathsf{KL},\epsilon}\ c_2\ \{Q\}$ → Kullback-Leibler distance

Relational Properties of Probabilistic Programs — Approximate Versions

Different notions are expressed in terms of different "metrics" for comparing distributions

Judgments in approximate **pRHL** should also account for the metric between distributions at stake:

- $\{P\}\ c_1 \sim_{\mathsf{SD},\epsilon}\ c_2\ \{Q\}$ → statistical distance
- $\{P\}\ c_1 \sim_{\alpha,\epsilon}\ c_2\ \{Q\}$ → α-distance
- $\{P\}\ c_1 \sim_{\mathsf{KL},\epsilon}\ c_2\ \{Q\}$ → Kullback-Leibler distance

f-DIVERGENCES

The family of f-Divergences

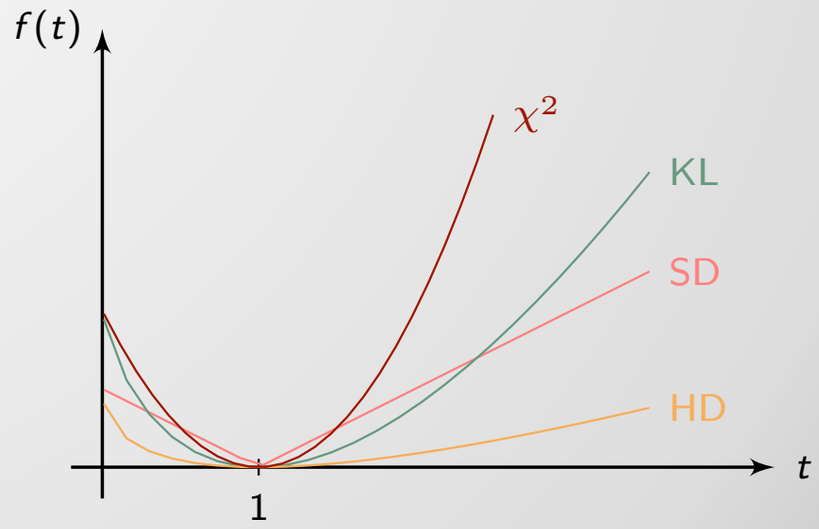
f-Divergences between Distributions

The *f*-divergence between two distributions μ_1 and μ_2 over a set A is defined as*

$$\Delta_f(\mu_1, \mu_2) \triangleq \sum_{a \in A} \mu_2(a)\, f\left(\frac{\mu_1(a)}{\mu_2(a)}\right),$$

where $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ is a continuous convex function such that $f(1) = 0$.

f-divergence	*f*
Statistical distance (Δ_{SD})	$f(t) = \frac{1}{2}\lvert t-1\rvert$
Hellinger distance (Δ_{HD})	$f(t) = \frac{1}{2}\lvert\sqrt{t}-1\rvert^2$
α-distance (Δ_α)	$f(t) = \max\{t-\alpha, 0\}$
Kullback-Leibler (Δ_{KL})	$f(t) = t\, ln(t) - t + 1$
χ^2-distance (Δ_{χ^2})	$f(t) = (t-1)^2$



* We adopt the following conventions: $0\, f(0/0) = 0$ and $0\, f(t/0) = t \lim_{x \to 0^+} x\, f(1/x)$ if $t > 0$.

Hoare Triples in Approximate Relational Hoare Logic

$\{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}$

c_1, c_2 : probabilistic programs

P, Q : relations over program states

f : function inducing the divergence

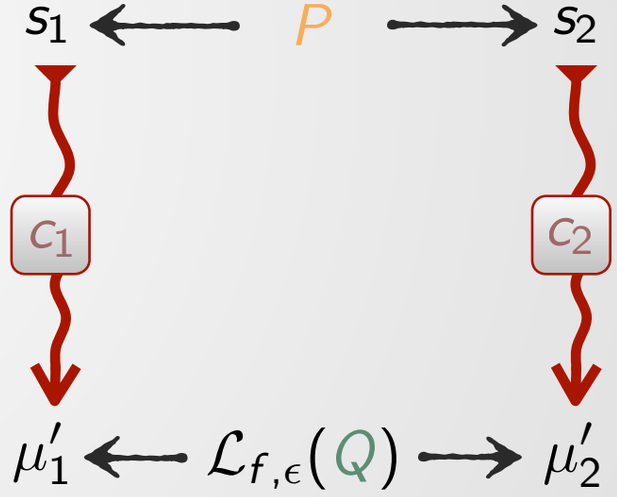
ϵ : "error" bound

$$\models \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}$$

iff

$$s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ \mathcal{L}_{f,\epsilon}(Q)\ [\![c_2]\!](s_2)$$

Approximate (f,ϵ)-Lifting of Q to a relation over distributions on program



divergence Δ_f satisfies the identity of indiscernibles

$\Delta_f(\mu_1, \mu_2) = 0 \implies \mu_1 = \mu_2$

$$\models \{P\}\ c_1 \sim_{f,0} c_2\ \{Q\} \quad \text{iff} \quad \models \{P\}\ c_1 \sim c_2\ \{Q\}$$

Hoare Triples in Approximate Relational Hoare Logic

Hoare triples

$$\{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}$$

c_1, c_2 : probabilistic programs
P, Q : relations over program states
f : function inducing the divergence
ϵ : "error" bound

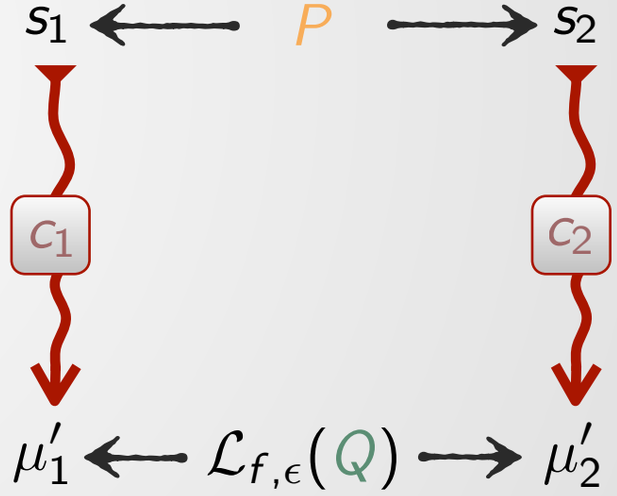
Validity of Hoare triples

$$\models \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}$$

iff

$$s_1\ P\ s_2 \implies [\![c_1]\!](s_1)\ \mathcal{L}_{f,\epsilon}(Q)\ [\![c_2]\!](s_2)$$

Approximate (f,ϵ)-Lifting of Q to a relation over distributions on program



divergence Δ_f satisfies the identity of indiscernibles

$\Delta_f(\mu_1, \mu_2) = 0 \implies \mu_1 = \mu_2$

$$\models \{P\}\ c_1 \sim_{f,0} c_2\ \{Q\} \quad \text{iff} \quad \models \{P\}\ c_1 \sim c_2\ \{Q\}$$

Approximate Lifting of Relations to Distributions

Approximate Lifting of Relations

Given a continuous convex function $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ with $f(1) = 0$ we define operator

$$\mathcal{L}_{f,\epsilon}(\cdot) : \mathcal{P}(A \times B) \to \mathcal{P}(\mathcal{D}(A) \times \mathcal{D}(B))$$

that lifts relations over sets A, B to relations over distributions on these sets as follows

$$\mu_1 \; \mathcal{L}_{f,\epsilon}(R) \; \mu_2 \quad \triangleq \quad \exists \mu_L,\, \mu_R \in \mathcal{D}(A \times B) \bullet \begin{cases} \pi_1(\mu_L) = \mu_1 \;\wedge\; \pi_2(\mu_R) = \mu_2 \\ \mathsf{supp}(\mu_L) \subseteq R \wedge \mathsf{supp}(\mu_R) \subseteq R \\ \Delta_f\,(\mu_L, \mu_R) \leq \epsilon \end{cases}$$

$\mu_1 \in \mathcal{D}(A)$ $\quad$ $\mu_2 \in \mathcal{D}(B)$ $\quad$ $R \in \mathcal{P}(A \times B)$

The lifting operator $\mathcal{L}_{f,\epsilon}(\cdot)$ also admits

- an inductive characterization:

$$\frac{a\,R\,b \quad k'\,f\left(\frac{k}{k'}\right) \leq \epsilon}{k \cdot \eta_a \;\; \mathcal{L}_{f,\epsilon_i}(R) \;\; k' \cdot \eta_b} \qquad \frac{\mu_i \;\mathcal{L}_{f,\epsilon}(R)\; \nu_i \;\; \forall i \in I \quad \sum_{i \in I} \epsilon_i \leq \epsilon}{\left(\sum_{i \in I} \mu_i\right) \;\mathcal{L}_{f,\epsilon}(R)\; \left(\sum_{i \in I} \nu_i\right)}$$

- a simpler characterization for equivalence relations:

$$\mu_1 \;\mathcal{L}_{f,\epsilon}(R)\; \mu_2 \iff \Delta_f\,(\mu_1/R, \mu_2/R) \leq \epsilon$$

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

Proof System f-pRHL (Two-sided Rules)

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim_{f,0} \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\mathsf{false}}\}\ \texttt{abort} \sim_{f,0} \texttt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x \coloneqq A \sim_{f,0} y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

Proof System f-pRHL (Two-sided Rules)

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim_{f,0} \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort} \sim_{f,0} \texttt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x \coloneqq A \sim_{f,0} y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket \mu_1 \rrbracket(s_1), \llbracket \mu_2 \rrbracket(s_2)\Big) \leq \epsilon}{\vdash \{P\}\ x \overset{\$}{\coloneqq} \mu_1\ \sim_{f,\epsilon}\ y \overset{\$}{\coloneqq} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}}\ [\text{rand}]$$

Proof System f-pRHL (Two-sided Rules)

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim_{f,0} \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort} \sim_{f,0} \texttt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x \coloneqq A \sim_{f,0} y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket \mu_1 \rrbracket(s_1), \llbracket \mu_2 \rrbracket(s_2)\Big) \leq \epsilon}{\vdash \{P\}\ x \overset{\$}{\coloneqq} \mu_1 \sim_{f,\epsilon} y \overset{\$}{\coloneqq} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}}\ [\text{rand}]$$

$$\frac{\begin{array}{c} P \implies G_1\langle 1\rangle = G_2\langle 2\rangle \\ \vdash \{P \wedge G_1\langle 1\rangle\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\} \qquad \vdash \{P \wedge \neg G_1\langle 1\rangle\}\ c_1' \sim_{f,\epsilon} c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ \texttt{if}\ G_1\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim_{f,\epsilon} \texttt{if}\ G_2\ \texttt{then}\ c_2\ \texttt{else}\ c_2'\ \{Q\}}\ [\text{if}]$$

Proof System f-pRHL (Two-sided Rules)

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim_{f,0} \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort} \sim_{f,0} \texttt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x \coloneqq A \sim_{f,0} y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon}{\vdash \{P\}\ x \overset{\$}{\coloneqq} \mu_1 \sim_{f,\epsilon} y \overset{\$}{\coloneqq} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}}\ [\text{rand}]$$

$$\frac{\begin{array}{c} P \implies G_1\langle 1\rangle = G_2\langle 2\rangle \\ \vdash \{P \wedge G_1\langle 1\rangle\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\} \qquad \vdash \{P \wedge \neg G_1\langle 1\rangle\}\ c_1' \sim_{f,\epsilon} c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ \texttt{if}\ G_1\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim_{f,\epsilon} \texttt{if}\ G_2\ \texttt{then}\ c_2\ \texttt{else}\ c_2'\ \{Q\}}\ [\text{if}]$$

$$\frac{\begin{array}{c} \Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \qquad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$$\frac{\begin{array}{c} \Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ (I \wedge v\langle 1\rangle \ge 0)\ s_2 \implies \Pr[c_1(s_1) : \text{true}] = \Pr[c_2(s_2) : \text{true}] \\ I \implies G_1\langle 1\rangle = G_2\langle 2\rangle \qquad I \wedge v\langle 1\rangle \ge n \implies \neg G_1\langle 1\rangle \\ \vdash \{I \wedge G_1\langle 1\rangle \wedge v\langle 1\rangle = k\}\ c_1 \sim_{f,\epsilon} c_2\ \{I \wedge v\langle 1\rangle > k\} \end{array}}{\vdash \{I \wedge v\langle 1\rangle \ge 0\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim_{f,n\epsilon} \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge v\langle 1\rangle \ge n \wedge \neg G_1\langle 1\rangle\}}\ [\text{tc-while}]$$

Proof System f-pRHL (Two-sided Rules)

$$\frac{}{\vdash \{P\}\ \texttt{skip} \sim_{f,0} \texttt{skip}\ \{P\}}\ [\text{skip}] \qquad \frac{}{\vdash \{\underline{\text{false}}\}\ \texttt{abort} \sim_{f,0} \texttt{abort}\ \{Q\}}\ [\text{tc-abort}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x \coloneqq A \sim_{f,0} y \coloneqq B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket \mu_1 \rrbracket(s_1), \llbracket \mu_2 \rrbracket(s_2)\Big) \le \epsilon}{\vdash \{P\}\ x \overset{\$}{\coloneqq} \mu_1 \sim_{f,\epsilon} y \overset{\$}{\coloneqq} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}}\ [\text{rand}]$$

$$\frac{\begin{array}{c} P \implies G_1\langle 1\rangle = G_2\langle 2\rangle \\ \vdash \{P \wedge G_1\langle 1\rangle\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\} \qquad \vdash \{P \wedge \neg G_1\langle 1\rangle\}\ c_1' \sim_{f,\epsilon} c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ \texttt{if}\ G_1\ \texttt{then}\ c_1\ \texttt{else}\ c_1' \sim_{f,\epsilon} \texttt{if}\ G_2\ \texttt{then}\ c_2\ \texttt{else}\ c_2'\ \{Q\}}\ [\text{if}]$$

$$\frac{\begin{array}{c} \Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) \colon \text{true}] = \Pr[c_2'(s_2) \colon \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \qquad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$$\frac{\begin{array}{c} \Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ (I \wedge v\langle 1\rangle \ge 0)\ s_2 \implies \Pr[c_1(s_1) \colon \text{true}] = \Pr[c_2(s_2) \colon \text{true}] \\ I \implies G_1\langle 1\rangle = G_2\langle 2\rangle \qquad I \wedge v\langle 1\rangle \ge n \implies \neg G_1\langle 1\rangle \\ \vdash \{I \wedge G_1\langle 1\rangle \wedge v\langle 1\rangle = k\}\ c_1 \sim_{f,\epsilon} c_2\ \{I \wedge v\langle 1\rangle > k\} \end{array}}{\vdash \{I \wedge v\langle 1\rangle \ge 0\}\ \texttt{while}\ G_1\ \texttt{do}\ c_1 \sim_{f,n\epsilon} \texttt{while}\ G_2\ \texttt{do}\ c_2\ \{I \wedge v\langle 1\rangle \ge n \wedge \neg G_1\langle 1\rangle\}}\ [\text{tc-while}]$$

$$\frac{\begin{array}{c} \vdash \{P'\}\ c_1 \sim_{f',\epsilon'} c_2\ \{Q'\} \\ P \implies P' \quad Q' \implies Q \quad f \le f' \quad \epsilon' \le \epsilon \end{array}}{\vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}}\ [\text{cons}]$$

Proof System f-pRHL (One-sided Rules)

$$\frac{}{\vdash \{\underline{\mathsf{false}}\}\ c_1 \sim_{f,0} c_2\ \{Q\}}\ [\text{contr}]$$

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle]\}\ x \coloneqq A \sim_{f,0} \mathtt{skip}\ \{Q\}}\ [\text{d-assgn}]$$

$$\frac{\vdash \{P \wedge G\langle 1\rangle\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\} \quad \vdash \{P \wedge \neg G\langle 1\rangle\}\ c_1' \sim_{f,\epsilon} c_2\ \{Q\}}{\vdash \{P\}\ \mathtt{if}\ G\ \mathtt{then}\ c_1\ \mathtt{else}\ c_1' \sim_{f,\epsilon} c_2\ \{Q\}}\ [\text{c-branch}]$$

$$\frac{}{\vdash \{P \wedge \neg G\langle 1\rangle\}\ \mathtt{while}\ G\ \mathtt{do}\ c \sim_{f,0} \mathtt{skip}\ \{P \wedge \neg G\langle 1\rangle\}}\ [\text{d-while}]$$

The proof system also include the symmetrical versions of rules [d-assgn], [c-branch] and [d-while].

Composability of f-divergences

Self-composability generalizes the notion of f-divergence additivity

$$\left.\begin{array}{l}\Delta_f\left(\mu_1, \mu_2\right) \leq \epsilon \\ \Delta_f\left(\nu_1, \nu_2\right) \leq \epsilon'\end{array}\right\} \Longrightarrow \Delta_f\left(\mu_1 \times \nu_1, \mu_2 \times \nu_2\right) \leq \epsilon + \epsilon' \qquad \text{(additivity)}$$

$\mu_1, \mu_2 \in \mathcal{D}(A)$

$\nu_1, \nu_2 \in \mathcal{D}(B)$

Self-Compostability of *f*-Divergences

Divergence Δ_f is self-composable iff

$$\left.\begin{array}{c}\Delta_f\left(\mu_1, \mu_2\right) \leq \epsilon \\ \forall a \bullet\ \Delta_f\left(M_1(a), M_2(a)\right) \leq \epsilon'\end{array}\right\} \Longrightarrow \Delta_f\left(\mu_1 \blacktriangleright M_1, \mu_2 \blacktriangleright M_2\right) \leq \epsilon + \epsilon'$$

$\mu_1, \mu_2 \in \mathcal{D}(A)$

$M_1, M_2 \in A \to \mathcal{D}(B)$

$$\begin{array}{ccc} \mu_1 & \blacktriangleright & M_1 \\ \uparrow & \uparrow & \uparrow \\ \leq \epsilon & \leq \epsilon+\epsilon' & \leq \epsilon' \\ \downarrow & \downarrow & \downarrow \\ \mu_2 & \blacktriangleright & M_2 \end{array}$$

Composability of f-divergences

Self-composability generalizes the notion of f-divergence additivity

$$\left.\begin{array}{l}\Delta_f\left(\mu_1, \mu_2\right) \leq \epsilon \\ \Delta_f\left(\nu_1, \nu_2\right) \leq \epsilon'\end{array}\right\} \Longrightarrow \Delta_f\left(\mu_1 \times \nu_1, \mu_2 \times \nu_2\right) \leq \epsilon + \epsilon' \qquad \text{(additivity)}$$

$\mu_1, \mu_2 \in \mathcal{D}(A)$

$\nu_1, \nu_2 \in \mathcal{D}(B)$

Self-Compostability of *f*-Divergences

Divergence Δ_f is self-composable iff

$$\left.\begin{array}{c}\Delta_f\left(\mu_1, \mu_2\right) \leq \epsilon \\ \forall a \bullet\ \Delta_f\left(M_1(a), M_2(a)\right) \leq \epsilon'\end{array}\right\} \Longrightarrow \Delta_f\left(\mu_1 \blacktriangleright M_1, \mu_2 \blacktriangleright M_2\right) \leq \epsilon + \epsilon'$$

$\mu_1, \mu_2 \in \mathcal{D}(A)$

$M_1, M_2 \in A \to \mathcal{D}(B)$

$$\begin{array}{ccc} [\![c_1]\!](s_1) & \blacktriangleright & [\![c_1']\!] \\ \uparrow & \uparrow & \uparrow \\ \leq \epsilon & \leq \epsilon+\epsilon' & \leq \epsilon' \\ \downarrow & \downarrow & \downarrow \\ [\![c_2]\!](s_2) & \blacktriangleright & [\![c_2']\!] \end{array}$$

Composability of f-divergences

Self-composability generalizes the notion of f-divergence additivity

$$\left.\begin{array}{l}\Delta_f\left(\mu_1,\mu_2\right)\leq\epsilon\\ \Delta_f\left(\nu_1,\nu_2\right)\leq\epsilon'\end{array}\right\}\Longrightarrow\Delta_f\left(\mu_1\times\nu_1,\mu_2\times\nu_2\right)\leq\epsilon+\epsilon'$$

$\mu_1,\mu_2\in\mathcal{D}(A)$ $\nu_1,\nu_2\in\mathcal{D}(B)$

(additivity)

Self-Compostability of *f*-Divergences

Divergence Δ_f is self-composable iff

$$\left.\begin{array}{c}\Delta_f\left(\mu_1,\mu_2\right)\leq\epsilon\\ \forall a\bullet\ \Delta_f\left(M_1(a),M_2(a)\right)\leq\epsilon'\end{array}\right\}\Longrightarrow\Delta_f\left(\mu_1\blacktriangleright M_1,\mu_2\blacktriangleright M_2\right)\leq\epsilon+\epsilon'$$

$\mu_1,\mu_2\in\mathcal{D}(A)$ $M_1,M_2\in A\to\mathcal{D}(B)$

$$\begin{array}{ccc}[\![c_1]\!](s_1) & \blacktriangleright & [\![c_1']\!]\\ \uparrow & \uparrow & \uparrow\\ \leq\epsilon & \leq\epsilon+\epsilon' & \leq\epsilon'\\ \downarrow & \downarrow & \downarrow\\ [\![c_2]\!](s_2) & \blacktriangleright & [\![c_2']\!]\end{array}$$

Theorem

Divergences Δ_{SD}, Δ_{HD} and Δ_{KL} are self-composable.

Composability of f-divergences

Divergences Δ_{χ^2} and Δ_{α} have special composability properties:

- For Δ_{χ^2} we have:

$$\left.\begin{array}{c} \Delta_{\chi^2}(\mu_1, \mu_2) \leq \epsilon \\ \forall a \bullet \Delta_{\chi^2}(M_1(a), M_2(a)) \leq \epsilon' \end{array}\right\} \implies \Delta_{\chi^2}(\mu_1 \blacktriangleright M_1, \mu_2 \blacktriangleright M_2) \leq \epsilon + \epsilon' + \epsilon\,\epsilon'$$

  Sequential composition rule for Δ_{χ^2} now looks like:

$$\frac{\begin{array}{c} \forall s_1, s_2 \bullet s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{\chi^2,\epsilon}\ c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{\chi^2,\epsilon'}\ c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ c_1; c_1' \sim_{\chi^2,\epsilon+\epsilon'+\epsilon\,\epsilon'}\ c_2; c_2'\ \{Q\}}\ [\chi^2\text{-seq}]$$

  (Rule for while loops is also adapted accordingly)

- For Δ_{α} we have:

$$\left.\begin{array}{c} \Delta_{\alpha}(\mu_1, \mu_2) \leq \epsilon \\ \forall a \bullet \Delta_{\alpha'}(M_1(a), M_2(a)) \leq \epsilon' \end{array}\right\} \implies \Delta_{\alpha\alpha'}(\mu_1 \blacktriangleright M_1, \mu_2 \blacktriangleright M_2) \leq \epsilon + \epsilon'$$

  Sequential composition rule for Δ_{α} now looks like:

$$\frac{\begin{array}{c} \forall s_1, s_2 \bullet s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{\alpha,\epsilon}\ c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{\alpha',\epsilon'}\ c_2'\ \{Q\} \end{array}}{\vdash \{P\}\ c_1; c_1' \sim_{\alpha\alpha',\epsilon+\epsilon'}\ c_2; c_2'\ \{Q\}}\ [\alpha\text{-seq}]$$

  (Rule for while loops is also adapted accordingly)

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x \overset{\$}{:=} \mu_1 \sim y \overset{\$}{:=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]\ [\text{seq}]$$

$\langle l\langle 1\rangle = l\langle 2\rangle \rangle$

$h := 1-h;$ $\qquad$ $h := 1-h;$

$\sim_{\mathsf{SD},\epsilon}$

$l \overset{\$}{:=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\qquad$ $l \overset{\$}{:=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \rangle$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle/A\langle 1\rangle, y\langle 2\rangle/B\langle 2\rangle]\}\; x := A \sim_{f,0} y := B\; \{Q\}}\;[\text{assgn}]$$

$$\frac{\forall s_1, s_2 \bullet\; s_1\, P\, s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon}{\vdash \{P\}\; x :\overset{\$}{=} \mu_1 \;\sim\; y :\overset{\$}{=} \mu_2\; \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\; P[x\langle 1\rangle/v_1, y\langle 2\rangle/v_2]\}}\;[\text{rand}]$$

$$\frac{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\; s_1\, Q'\, s_2 \implies \Pr[c_1'(s_1) : \mathsf{true}] = \Pr[c_2'(s_2) : \mathsf{true}] \\ \vdash \{P\}\; c_1 \sim_{f,\epsilon} c_2\; \{Q'\} \qquad \vdash \{Q'\}\; c_1' \sim_{f,\epsilon'} c_2'\; \{Q\}\end{array}}{\vdash \{P\}\; c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\; \{Q\}}\;[\text{seq}]$$

$$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$$

$$h := 1-h; \qquad \sim_{\mathsf{SD},0} \qquad h := 1-h;$$

$$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$$

$$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$$

$$l :\overset{\$}{=} \tfrac{1}{2}\langle l\rangle + \tfrac{1}{2}\langle 1-l\rangle \qquad \sim_{\mathsf{SD},\epsilon} \qquad l :\overset{\$}{=} \epsilon\langle h\rangle + \tfrac{1}{2}(1-\epsilon)\langle l\rangle + \tfrac{1}{2}(1-\epsilon)\langle 1-l\rangle$$

$$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$$

Proof obligations:

- Divergence Δ_{SD} is self-composable
- Programs $l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket \mu_1 \rrbracket(s_1), \llbracket \mu_2 \rrbracket(s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x :\overset{\$}{=} \mu_1 \sim y :\overset{\$}{=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]\ [\text{seq}]$$

$$h := 1-h; \qquad h := 1-h;$$

$$\langle l\langle 1\rangle = l\langle 2\rangle \rangle$$

$$l :\overset{\$}{=} \tfrac{1}{2}\langle l\rangle + \tfrac{1}{2}\langle 1-l\rangle \quad \sim_{\mathsf{SD},\epsilon} \quad l :\overset{\$}{=} \epsilon\langle h\rangle + \tfrac{1}{2}(1-\epsilon)\langle l\rangle + \tfrac{1}{2}(1-\epsilon)\langle 1-l\rangle$$

$$\langle l\langle 1\rangle = l\langle 2\rangle \rangle$$

Proof obligations:

- Divergence Δ_{SD} is self-composable
- Programs $l :\overset{\$}{=} \tfrac{1}{2}\langle l\rangle + \tfrac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \tfrac{1}{2}(1-\epsilon)\langle l\rangle + \tfrac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle/A\langle 1\rangle, y\langle 2\rangle/B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x :\overset{\$}{=} \mu_1\ \sim\ y :\overset{\$}{=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle/v_1, y\langle 2\rangle/v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) : \text{true}] = \Pr[c_2'(s_2) : \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]\ [\text{seq}]$$

$h := 1-h;$ $\quad\sim_{\mathrm{SD},0}\quad$ $h := 1-h;$

$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\quad\sim_{\mathrm{SD},\epsilon}\quad$ $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \wedge \exists v_1, v_2 \bullet\ v_1 = v_2\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$

Proof obligations:

- Divergence Δ_{SD} is self-composable
- Programs $l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour
- $s_1(l) = s_2(l) \implies \Delta_{\mathrm{SD}}\Big([\![\frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle]\!](s_1), [\![\epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle]\!](s_2)\Big) \le \epsilon$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) \colon \text{true}] = \Pr[c_2'(s_2) \colon \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\}\end{array}}{\vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \Delta_f \text{ is self-composable}\end{array}}{\vdash \{P\}\ x \xleftarrow{\$} \mu_1 \sim y \xleftarrow{\$} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}}\ [\text{rand}]$$

$h := 1-h;$ $\quad\sim_{\text{SD},0}\quad$ $h := 1-h;$

$\langle l\langle 1\rangle = l\langle 2\rangle\rangle$

$l \xleftarrow{\$} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\quad\sim_{\text{SD},\epsilon}\quad$ $l \xleftarrow{\$} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \wedge \exists v_1, v_2 \bullet\ v_1 = v_2\rangle$

Proof obligations:

- Divergence Δ_{SD} is self-composable
- Programs $l \xleftarrow{\$} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l \xleftarrow{\$} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour
- $s_1(l) = s_2(l) \implies \Delta_{\text{SD}}\Big(\Big[\!\Big[\frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle\Big]\!\Big](s_1), \Big[\!\Big[\epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle\Big]\!\Big](s_2)\Big) \le \epsilon$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x :\overset{\$}{=} \mu_1 \sim y :\overset{\$}{=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) \colon \text{true}] = \Pr[c_2'(s_2) \colon \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]\ [\text{seq}]$$

$h := 1-h;$ $\quad\sim_{\text{SD},0}\quad$ $h := 1-h;$

$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\quad\sim_{\text{SD},\epsilon}\quad$ $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \wedge \exists v_1, v_2 \bullet v_1 = v_2\rangle$

Proof obligations:

- Divergence Δ_{SD} is self-composable ✔
- Programs $l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour
- $s_1(l) = s_2(l) \implies \Delta_{\text{SD}}\Big(\Big[\!\Big[\frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle\Big]\!\Big](s_1), \Big[\!\Big[\epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle\Big]\!\Big](s_2)\Big) \le \epsilon$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x :\overset{\$}{=} \mu_1 \sim y :\overset{\$}{=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) \colon \text{true}] = \Pr[c_2'(s_2) \colon \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]\ [\text{seq}]$$

$h := 1-h;$ $\quad\sim_{\text{SD},0}\quad$ $h := 1-h;$

$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\quad\sim_{\text{SD},\epsilon}\quad$ $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \wedge \exists v_1, v_2 \bullet v_1 = v_2\rangle$

Proof obligations:

- Divergence Δ_{SD} is self-composable ✔
- Programs $l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour ✔
- $s_1(l) = s_2(l) \implies \Delta_{\text{SD}}\Big([\![\frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle]\!](s_1), [\![\epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle]\!](s_2)\Big) \le \epsilon$

Proof System — Derivation Examples

$$\frac{}{\vdash \{Q[x\langle 1\rangle / A\langle 1\rangle, y\langle 2\rangle / B\langle 2\rangle]\}\ x := A \sim_{f,0} y := B\ \{Q\}}\ [\text{assgn}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big([\![\mu_1]\!](s_1), [\![\mu_2]\!](s_2)\Big) \le \epsilon \\ \vdash \{P\}\ x :\overset{\$}{=} \mu_1 \sim y :\overset{\$}{=} \mu_2\ \{x\langle 1\rangle = y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]\}\end{array}}{\begin{array}{c}\Delta_f \text{ is self-composable} \\ \forall s_1, s_2 \bullet\ s_1\ Q'\ s_2 \implies \Pr[c_1'(s_1) \colon \text{true}] = \Pr[c_2'(s_2) \colon \text{true}] \\ \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\} \\ \hline \vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}\end{array}}\ [\text{rand}]$$

$$\frac{\vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \quad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\}}{\vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

$h := 1-h;$ $\sim_{\mathrm{SD},0}$ $h := 1-h;$

$l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ $\sim_{\mathrm{SD},\epsilon}$ $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$

$\langle l\langle 1\rangle = l\langle 2\rangle \wedge \exists v_1, v_2 \bullet v_1 = v_2\rangle$

Proof obligations:

- Divergence Δ_{SD} is self-composable ✔
- Programs $l :\overset{\$}{=} \frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle$ and $l :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle$ have the same termination behaviour ✔
- $s_1(l) = s_2(l) \implies \Delta_{\mathrm{SD}}\Big(\Big[\!\Big[\frac{1}{2}\langle l\rangle + \frac{1}{2}\langle 1-l\rangle\Big]\!\Big](s_1), \Big[\!\Big[\epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle l\rangle + \frac{1}{2}(1-\epsilon)\langle 1-l\rangle\Big]\!\Big](s_2)\Big) \le \epsilon$

$$= \Big\langle \Delta_{\mathrm{SD}}(\mu_1, \mu_2) = \textstyle\sum_{a \in A} \frac{1}{2}|\mu_1(a) - \mu_2(a)| \text{ for all } \mu_1, \mu_2 \in \mathcal{D}(A) \Big\rangle$$

$$\tfrac{1}{2}\,|0 - \epsilon| + \tfrac{1}{2}\,\big|\tfrac{1}{2} - \tfrac{1}{2}(1-\epsilon)\big| + \tfrac{1}{2}\,\big|\tfrac{1}{2} - \tfrac{1}{2}(1-\epsilon)\big|$$

$$= \langle \text{algebra} \rangle$$

$$\epsilon \quad ✔$$

Using f-pRHL to Relate the Probabilities of Events

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

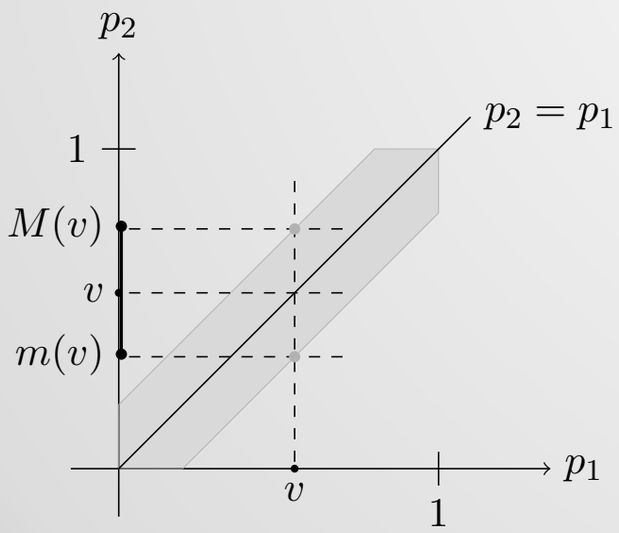
$$\frac{s_1\, P\, s_2 \quad \models \{P\}\, c_1 \sim_{f,\epsilon} c_2\, \{Q\} \quad Q \implies (A\langle 1\rangle \iff B\langle 2\rangle)}{p_B\, f\left(\frac{p_A}{p_B}\right) + p_{\overline{B}}\, f\left(\frac{p_{\overline{A}}}{p_{\overline{B}}}\right) \leq \epsilon}\ [\text{Pr-Approx}]$$

$\Pr[c_2(s_2) : B]$ $\Pr[c_1(s_1) : A]$

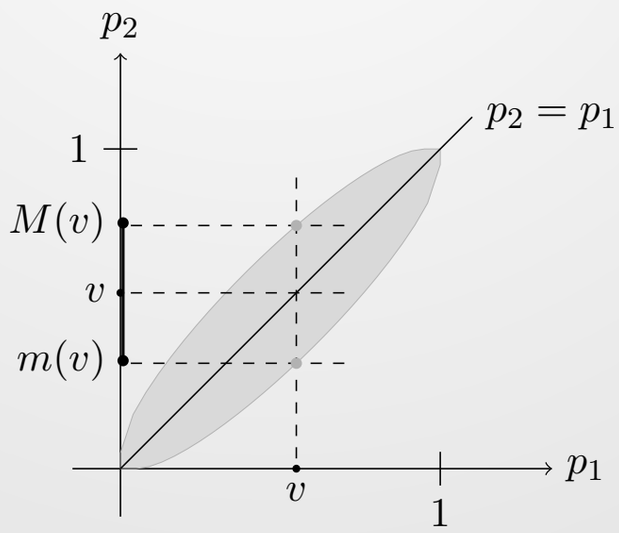
If $s_1\, P\, s_2$ entails $\Pr[c_1(s_1) : \text{true}] = \Pr[c_2(s_2) : \text{true}] = 1$, then the conclusion of the rule simplifies e.g. to

Statistical distance → $|p_A - p_B| \leq \epsilon$

Hellinger distance → $|\sqrt{p_A} - \sqrt{p_B}| + |\sqrt{1-p_A} - \sqrt{1-p_B}| \leq \epsilon$



(a) Statistical distance



(b) Hellinger distance

Using f-pRHL to Relate the Probabilities of Events

$$\frac{\begin{array}{c}\Pr[c_1(s_1)\colon \mathsf{true}] = \Pr[c_2(s_2)\colon \mathsf{true}] = 1 \\ s_1\ P\ s_2 \quad \models \{P\}\ c_1 \sim_{\mathsf{SD},\epsilon}\ c_2\ \{Q\} \quad Q \implies (A\langle 1\rangle \iff B\langle 2\rangle)\end{array}}{\left|\Pr[c_1(s_1)\colon A] - \Pr[c_2(s_2)\colon B]\right| \leq \epsilon}\ [\text{SD-Pr-Approx}]$$

Application example

c_1 **:** $h := 1-h;$
$I :\overset{\$}{=} \frac{1}{2}\langle I\rangle + \frac{1}{2}\langle 1-I\rangle$

c_2 **:** $h := 1-h;$
$I :\overset{\$}{=} \epsilon\langle h\rangle + \frac{1}{2}(1-\epsilon)\langle I\rangle + \frac{1}{2}(1-\epsilon)\langle 1-I\rangle$

From

$$\models \{I\langle 1\rangle = I\langle 2\rangle\}\ c_1 \sim_{\mathsf{SD},\epsilon}\ c_2\ \{I\langle 1\rangle = I\langle 2\rangle\}$$

we can conclude e.g. that for every pair of initial states s_1 and s_2,

$$s_1(I) = s_2(I) \implies \forall \varphi \bullet \left|\Pr[c_1(s_1) : I{=}0] - \Pr[c_2(s_2) : I{=}0]\right| \leq \epsilon$$

Applications of f-pRHL

- Bound the distance between (the output of) probabilistic programs:

$$\frac{\models \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{\equiv\}}{s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket c_1 \rrbracket(s_1), \llbracket c_2 \rrbracket(s_2)\Big) \leq \epsilon}$$

  - Applications in differential privacy (Δ_α)

- Reason about continuity (or sensitivity) of probabilistic programs:

$$\frac{\models \{\equiv\}\ c \sim_{f,\epsilon} c\ \{\equiv\} \qquad \Delta_f \text{ is self-composable}}{\Delta_f\,(\mu_1, \mu_2) \leq \epsilon' \implies \Delta_f\Big(\llbracket c \rrbracket(\mu_1), \llbracket c \rrbracket(\mu_2)\Big) \leq \epsilon + \epsilon'}$$

Applications of f-pRHL

- Bound the distance between (the output of) probabilistic programs:

$$\frac{\models \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{\equiv\}}{s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket c_1 \rrbracket(s_1), \llbracket c_2 \rrbracket(s_2)\Big) \leq \epsilon}$$

  - Applications in cryptography (Δ_{SD})
  - Applications in differential privacy (Δ_α)

- Reason about continuity (or sensitivity) of probabilistic programs:

$$\frac{\models \{\equiv\}\ c \sim_{f,\epsilon} c\ \{\equiv\} \qquad \Delta_f \text{ is self-composable}}{\Delta_f\,(\mu_1, \mu_2) \leq \epsilon' \implies \Delta_f\Big(\llbracket c \rrbracket(\mu_1), \llbracket c \rrbracket(\mu_2)\Big) \leq \epsilon + \epsilon'}$$

Variants of f-pRHL

- The proof system can be modified to reason about partial correctness

$$\frac{}{\vdash \{\underline{\mathsf{true}}\}\ \mathtt{abort} \sim_{f,0} \mathtt{abort}\ \{Q\}}\ [\text{pc-abort}]$$

$$\frac{\begin{array}{c}\forall s_1, s_2 \bullet\ s_1\ (I \wedge v\langle 1\rangle \geq 0)\ s_2 \implies \Pr[c_1(s_1) : \mathsf{true}] = \Pr[c_2(s_2) : \mathsf{true}] \\ I \implies G_1\langle 1\rangle = G_2\langle 2\rangle \qquad \Delta_f \text{ is self-composable} \\ \vdash \{I \wedge G_1\langle 1\rangle \wedge v\langle 1\rangle = k\}\ c_1 \sim_{f,\epsilon_k} c_2\ \{I \wedge v\langle 1\rangle > k\}\end{array}}{\vdash \{I \wedge v\langle 1\rangle \geq 0\}\ \mathtt{while}\ G_1\ \mathtt{do}\ c_1 \sim_{f,\sum \epsilon_k} \mathtt{while}\ G_2\ \mathtt{do}\ c_2\ \{I \wedge \neg G_1\langle 1\rangle\}}\ [\text{pc-while}]$$
$k \geq 0$

- There exists also a symmetrical version of the logic where e.g.

$$\frac{\models \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{\equiv\}}{s_1\ P\ s_2 \implies \Delta_f\Big([\![c_1]\!](s_1), [\![c_2]\!](s_2)\Big) \leq \epsilon \wedge \Delta_f\Big([\![c_2]\!](s_2), [\![c_1]\!](s_1)\Big) \leq \epsilon}$$

Agenda

- Recap on relational Hoare logic
- Approximate version of the relational Hoare logic
- Summary

Summary

Certain relational properties are expressed as **closeness conditions**

$$\left|\Pr[c_1(s_1) : A] - \Pr[c_2(s_2) : B]\right| \leq \epsilon$$

between the output of probabilistic programs and **cannot** be modelled through standard relational Hoare triples.

- Approximate Non-interference
- Differential privacy
- Program sensitivity

Approximate Relational Hoare Logic

Distance for comparing distribution

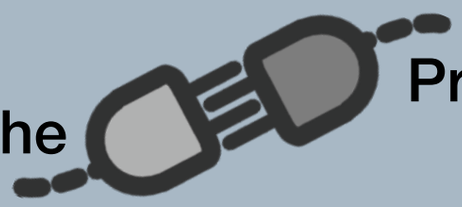
$$\{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q\}$$

Distance bound (error)

$$\frac{\forall s_1, s_2 \bullet\ s_1\ P\ s_2 \implies \Delta_f\Big(\llbracket \mu_1 \rrbracket(s_1), \llbracket \mu_2 \rrbracket(s_2)\Big) \leq \epsilon \qquad Q \triangleq x\langle 1\rangle{=}y\langle 2\rangle \wedge \exists\, v_1, v_2 \bullet\ P[x\langle 1\rangle / v_1, y\langle 2\rangle / v_2]}{\vdash \{P\}\ x \xleftarrow{\$} \mu_1\ \sim_{f,\epsilon}\ y \xleftarrow{\$} \mu_2\ \{Q\}}\ [\text{rand}]$$

$$\frac{\vdots \qquad \Delta_f \text{ is self-composable} \qquad \vdots \qquad \vdash \{P\}\ c_1 \sim_{f,\epsilon} c_2\ \{Q'\} \qquad \vdash \{Q'\}\ c_1' \sim_{f,\epsilon'} c_2'\ \{Q\}}{\vdash \{P\}\ c_1; c_1' \sim_{f,\epsilon+\epsilon'} c_2; c_2'\ \{Q\}}\ [\text{seq}]$$

World of the Logic



World of Probabilities

$$\frac{\ldots \quad \models \{P\}\ c_1 \sim_{\mathsf{SD},\epsilon} c_2\ \{Q\} \quad \ldots}{\left|\Pr[c_1(s_1) : A] - \Pr[c_2(s_2) : B]\right| \leq \epsilon}$$