A Quantitative Probabilistic Relational Hoare Logic

Martin Avanzini Gilles Barthe Davide Davoli Benjamin Grégoire

January 22nd 2025

In a nutshell...

imperative language, recursive procedures, sampling instructions

Logic for reasoning about ***pairs of* probabilistic programs** in a **quantitative way**.

mean values, probabilities, similarity metrics

In a nutshell...

imperative language, recursive procedures, sampling instructions

Logic for reasoning about ***pairs of* probabilistic programs** in a **quantitative way**.

mean values, probabilities, similarity metrics

Design goals:

- expressivity: **completeness**
- easy to use: compositional, probabilistic reasoning limited to sampling instructions

Applications:

- **cryptography**,
- differential privacy,
- machine learning

Probabilistic Programs

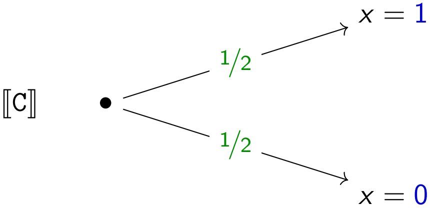
Probabilistic programs

$x \xleftarrow{\$} \{v_1, \ldots, v_k\}$ denotes *uniform* sampling from $\{v_1, \ldots, v_k\}$.

Probabilistic programs

$x \xleftarrow{\$} \{v_1, \ldots, v_k\}$ denotes *uniform* sampling from $\{v_1, \ldots, v_k\}$.

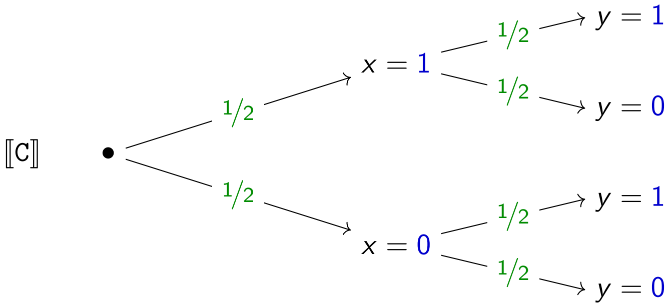
$$\mathtt{C} \triangleq \quad x \xleftarrow{\$} \{0, 1\} \quad ;$$



Probabilistic programs

$x \xleftarrow{\$} \{v_1, \ldots, v_k\}$ denotes *uniform* sampling from $\{v_1, \ldots, v_k\}$.

$$\mathtt{C} \triangleq x \xleftarrow{\$} \{0, 1\} \; ; \; y \xleftarrow{\$} \{0, 1\}$$

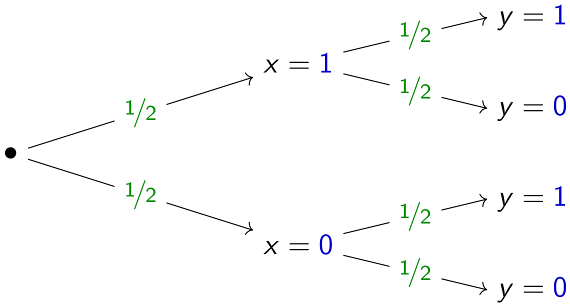


Probabilistic programs

$x \xleftarrow{\$} \{v_1, \ldots, v_k\}$ denotes *uniform* sampling from $\{v_1, \ldots, v_k\}$.

$$\mathtt{C} \triangleq \quad x \xleftarrow{\$} \{0,1\} \quad ; \quad y \xleftarrow{\$} \{0,1\} \qquad\qquad \mathbb{E}[x+y]$$

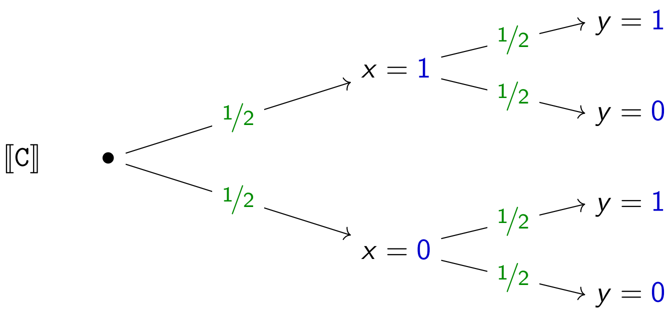
$[\![\mathtt{C}]\!]$



Probabilistic programs

$x \xleftarrow{\$} \{v_1, \ldots, v_k\}$ denotes *uniform* sampling from $\{v_1, \ldots, v_k\}$.

$$\texttt{C} \triangleq \quad x \xleftarrow{\$} \{0,1\} \quad ; \quad y \xleftarrow{\$} \{0,1\} \qquad \mathbb{E}[x+y]$$



$$
\begin{aligned}
&(1+1) \cdot 1/2 \cdot 1/2 \\
&+ \\
&(1+0) \cdot 1/2 \cdot 1/2 \\
&+ \\
&(0+1) \cdot 1/2 \cdot 1/2 \\
&+ \\
&(0+0) \cdot 1/2 \cdot 1/2 \\
\hline
&= 1
\end{aligned}
$$

Expectation based Relational Hoare Logic (eRHL)

Motivation: Probabilistic Relational Hoare Logic [Barthe et. al, 2009]

Judgments establish **qualitative** **relational** properties of probabilistic programs:

$$\vDash \{\mathcal{R}\}\ \texttt{C} \sim \texttt{D}\ \{\mathcal{S}\}$$

$\mathcal{R}, \mathcal{S} \in \mathcal{P}(\text{States} \times \text{States})$.

Motivation: Probabilistic Relational Hoare Logic [Barthe et. al, 2009]

Judgments establish **qualitative** **relational** properties of probabilistic programs:

$$\vDash \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{\mathcal{S}\}$$

$\mathcal{R}, \mathcal{S} \in \mathcal{P}(\text{States} \times \text{States})$.

$$\sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow \text{supp}(\mu) \subseteq \mathcal{S} \text{ for some } \mu\text{, coupling of } [\![\mathtt{C}]\!](\sigma_1) \text{ and } [\![\mathtt{D}]\!](\sigma_2).$$

Motivation: Probabilistic Relational Hoare Logic [Barthe et. al, 2009]

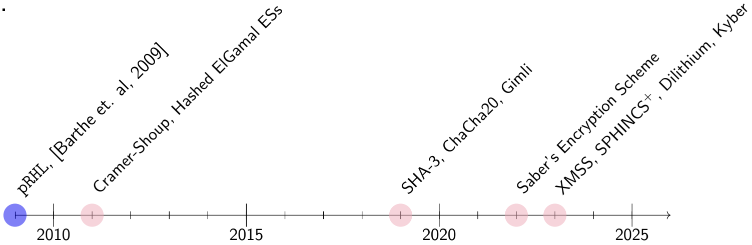
Judgments establish **qualitative** **relational** properties of probabilistic programs:

$$\models \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{\mathcal{S}\}$$

$\mathcal{R}, \mathcal{S} \in \mathcal{P}(\text{States} \times \text{States})$.

$$\sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow \text{supp}(\mu) \subseteq \mathcal{S} \text{ for some } \mu, \text{ coupling of } [\![\mathtt{C}]\!](\sigma_1) \text{ and } [\![\mathtt{D}]\!](\sigma_2).$$

Main application: Proving functional correctness and security of cryptographic applications.



Motivation: Probabilistic Relational Hoare Logic [Barthe et. al, 2009]

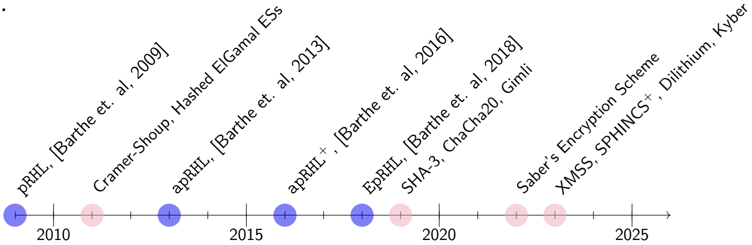
Judgments establish **qualitative** **relational** properties of probabilistic programs:

$$\vDash \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{\mathcal{S}\}$$

$\mathcal{R}, \mathcal{S} \in \mathcal{P}(\text{States} \times \text{States})$.

$$\sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow \text{supp}(\mu) \subseteq \mathcal{S} \text{ for some } \mu\text{, coupling of } [\![\mathtt{C}]\!](\sigma_1) \text{ and } [\![\mathtt{D}]\!](\sigma_2).$$

Main application: Proving functional correctness and security of cryptographic applications.



Motivation: Probabilistic Relational Hoare Logic [Barthe et. al, 2009]

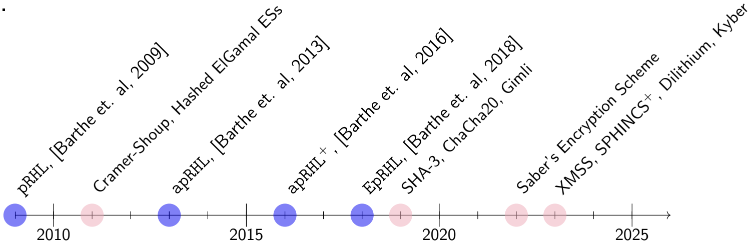
Judgments establish **qualitative** **relational** properties of probabilistic programs:

$$\vDash \{\mathcal{R}\}\ \texttt{C} \sim \texttt{D}\ \{\mathcal{S}\}$$

$\mathcal{R}, \mathcal{S} \in \mathcal{P}(\text{States} \times \text{States})$.

$$\sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow \text{supp}(\mu) \subseteq \mathcal{S} \text{ for some } \mu, \text{ coupling of } [\![\texttt{C}]\!](\sigma_1) \text{ and } [\![\texttt{D}]\!](\sigma_2).$$

Main application: Proving functional correctness and security of cryptographic applications.



Despite its success, **pRHL is incomplete.**

Incompleteness of pRHL

In pRHL:

$$\models \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{=\} \qquad \text{if and only if} \qquad \sigma_1\ \mathcal{R}\ \sigma_2 \;\Rightarrow\; [\![\mathtt{C}]\!](\sigma_1) = [\![\mathtt{D}]\!](\sigma_2)$$

Incompleteness of pRHL

In pRHL:

$$\vDash \{\mathcal{R}\}\ \texttt{C} \sim \texttt{D}\ \{=\} \qquad \text{if and only if} \qquad \sigma_1\ \mathcal{R}\ \sigma_2 \Rightarrow [\![\texttt{C}]\!](\sigma_1) = [\![\texttt{D}]\!](\sigma_2)$$

Two equivalent programs:

$$\begin{aligned} \texttt{RS} \triangleq\ & x \leftarrow 3\,\texttt{;} \\ & \texttt{while}\ (x > 2) \\ & \quad x \xleftarrow{\$} \{0,1,2,3\} \end{aligned} \qquad\qquad \texttt{DS} \triangleq x \xleftarrow{\$} \{0,1,2\}$$

Incompleteness of pRHL

In pRHL:

$$\vDash \{\mathcal{R}\}\ \texttt{C} \sim \texttt{D}\ \{=\} \qquad \text{if and only if} \qquad \sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow [\![\texttt{C}]\!](\sigma_1) = [\![\texttt{D}]\!](\sigma_2)$$

Two equivalent programs:

$$\begin{aligned} \mathrm{RS} &\triangleq x \leftarrow 3;\\ &\quad \texttt{while}\ (x > 2)\\ &\qquad x \xleftarrow{\$} \{0,1,2,3\} \end{aligned} \qquad\qquad \mathrm{DS} \triangleq x \xleftarrow{\$} \{0,1,2\}$$

$$\vDash \{\top\}\ \mathrm{RS} \sim \mathrm{DS}\ \{=\}$$

Incompleteness of pRHL

In pRHL:

$$\vDash \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{=\} \qquad \text{if and only if} \qquad \sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow [\![\mathtt{C}]\!](\sigma_1) = [\![\mathtt{D}]\!](\sigma_2)$$

Two equivalent programs:

$$\mathtt{RS} \triangleq x \leftarrow 3;\ \mathtt{while}\ (x > 2)\ x \xleftarrow{\$} \{0,1,2,3\} \qquad \mathtt{DS} \triangleq x \xleftarrow{\$} \{0,1,2\}$$

$$\vDash \{\top\}\ \mathtt{RS} \sim \mathtt{DS}\ \{=\} \qquad \nvdash \{\top\}\ \mathtt{RS} \sim \mathtt{DS}\ \{=\}$$

Expectation based Relational Hoare Logic

Judgments express **relational** **quantitative** properties of probabilistic programs:

$$\vDash \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\}$$

Expectation based Relational Hoare Logic

Judgments express **relational** **quantitative** properties of probabilistic programs:

$$\vDash \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\}$$

ϕ, ψ : States $\times$ States $\to [0, +\infty]$

Expectation based Relational Hoare Logic

Judgments express **relational** **quantitative** properties of probabilistic programs:

$$\vDash \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\}$$

ϕ, ψ : States $\times$ States $\to [0, +\infty]$

Interpretation (when $\mathtt{C}, \mathtt{D}$ terminate with probability 1):

$$\forall \sigma_1, \sigma_2.\ \phi(\sigma_1, \sigma_2) \geq \mathbb{E}_\mu[\psi] \text{ for some } \mu \text{ coupling of } [\![\mathtt{C}]\!](\sigma_1) \text{ and } [\![\mathtt{D}]\!](\sigma_2).$$

Expressivity of eRHL

Expected values:

$$\vDash \{3/2\}\ x \xleftarrow{\$} \{0,1\} \sim y \leftarrow 1\ \{x + y\}$$

Expressivity of eRHL

Expected values:

$$\vDash \{3/2\}\ x \xleftarrow{\$} \{0,1\} \sim y \leftarrow 1\ \{x + y\}$$

Probabilities:

$$\vDash \{1/2\}\ x \xleftarrow{\$} \{0,1\} \sim y \leftarrow 1\ \{[x + y = 2]\}$$

$$[P](\sigma_1, \sigma_2) = \begin{cases} 1 & \text{if } P(\sigma_1, \sigma_2) \\ 0 & \text{otherwise.} \end{cases}$$

Expressivity of eRHL

Expected values:

$$\models \{3/2\}\ x \xleftarrow{\$} \{0,1\} \sim y \leftarrow 1\ \{x + y\}$$

Probabilities:

$$\models \{1/2\}\ x \xleftarrow{\$} \{0,1\} \sim y \leftarrow 1\ \{[x + y = 2]\}$$

$$[P](\sigma_1, \sigma_2) = \begin{cases} 1 & \text{if } P(\sigma_1, \sigma_2) \\ 0 & \text{otherwise.} \end{cases}$$

Logical variables:

$$\models \{1/2 \cdot f(1) + 1/2 \cdot f(2)\}\quad x \xleftarrow{\$} \{0,1\}\ \sim\ y \leftarrow 1\quad \{f(x + y)\} \qquad f : \mathbb{N} \to [0, +\infty]$$

Selected two-sided rules of eRHL

eRHL is **compositional**:

$$\frac{\vdash \{\phi\}\,\mathtt{C}_1 \sim \mathtt{C}_2\,\{\psi\} \quad \vdash \{\psi\}\,\mathtt{D}_1 \sim \mathtt{D}_2\,\{\xi\}}{\vdash \{\phi\}\,\mathtt{C}_1\,;\,\mathtt{D}_1 \sim \mathtt{C}_2\,;\,\mathtt{D}_2\,\{\xi\}}\ \mathit{Seq}$$

Selected two-sided rules of eRHL

eRHL is **compositional**:

$$\frac{\vdash \{\phi\}\, \mathtt{C}_1 \sim \mathtt{C}_2 \,\{\psi\} \quad \vdash \{\psi\}\, \mathtt{D}_1 \sim \mathtt{D}_2 \,\{\xi\}}{\vdash \{\phi\}\, \mathtt{C}_1 \,;\, \mathtt{D}_1 \sim \mathtt{C}_2 \,;\, \mathtt{D}_2 \,\{\xi\}}\ \textit{Seq}$$

Quantitative reasoning **only for sampling** instruction:

$$\frac{\mu \text{ is a coupling of } d_1, \text{ and } d_2}{\vdash \{\mathbb{E}_{(v_1,v_2)\leftarrow\mu}[\phi[x_1/v_1][x_2/v_2]]\}\, x_1 \xleftarrow{\$} d_1 \sim x_2 \xleftarrow{\$} d_2 \,\{\phi\}}\ \textit{Sample}$$

Selected two-sided rules of eRHL

eRHL is **compositional**:

$$\frac{\vdash \{\phi\}\, \mathtt{C}_1 \sim \mathtt{C}_2\, \{\psi\} \quad \vdash \{\psi\}\, \mathtt{D}_1 \sim \mathtt{D}_2\, \{\xi\}}{\vdash \{\phi\}\, \mathtt{C}_1\, ;\, \mathtt{D}_1 \sim \mathtt{C}_2\, ;\, \mathtt{D}_2\, \{\xi\}}\ \textit{Seq}$$

Quantitative reasoning **only for sampling** instruction:

$$\frac{\mu \text{ is a coupling of } d_1, \text{ and } d_2}{\vdash \{\mathbb{E}_{(v_1,v_2)\leftarrow\mu}[\phi[x_1/v_1][x_2/v_2]]\}\, x_1 \xleftarrow{\$} d_1 \sim x_2 \xleftarrow{\$} d_2\, \{\phi\}}\ \textit{Sample}$$

These rules compare *structurally identical* programs...

Selected one-sided rules of eRHL

$$\frac{}{\vdash \{\mathbb{E}_{v\leftarrow d}[\phi[x/v]]\}\, x \xleftarrow{\$} d \sim \texttt{skip}\, \{\phi\}}\ \textit{Sample}$$

$$\frac{}{\vdash \{\phi[x/E]\}\, x \leftarrow E \sim \texttt{skip}\, \{\phi\}}\ \textit{Asgn}$$

$$\frac{\vdash \{P \mid \phi\}\, \texttt{C} \sim \texttt{skip}\, \{\phi\}}{\vdash \{\phi\}\, \texttt{while}\ (P)\ \texttt{do}\ \texttt{C} \sim \texttt{skip}\ \{\neg P \mid \phi\}}\ \textit{While}$$

Reasoning on one program at a time, in combination with:

$$\texttt{C};\, \texttt{skip} \equiv \texttt{C} \equiv \texttt{skip};\, \texttt{C}$$

Soundness and completeness

Theorem (Soundness)

$$\vdash \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\} \quad \Rightarrow \quad \models \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\}$$

What about the inverse implication?

Soundness and completeness

Theorem (Soundness)

$$\vdash \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\} \quad \Rightarrow \quad \models \{\phi\}\ \mathtt{C} \sim \mathtt{D}\ \{\psi\}$$

What about the inverse implication?

Theorem (Relative completeness)

If $\mathtt{C}$ *and* $\mathtt{D}$ *terminate with probability 1,*

$$\models \{\xi\}\ \mathtt{C} \sim \mathtt{D}\ \{\phi(\tau_1) + \psi(\tau_2)\} \quad \Rightarrow \quad \vdash \{\xi\}\ \mathtt{C} \sim \mathtt{D}\ \{\phi(\tau_1) + \psi(\tau_2)\}.$$

ϕ and ψ depend only on the output of $\mathtt{C}$ and $\mathtt{D}$, resp.

Soundness and completeness

Theorem (Soundness)

$$\vdash \{\phi\}\ \texttt{C} \sim \texttt{D}\ \{\psi\} \quad \Rightarrow \quad \models \{\phi\}\ \texttt{C} \sim \texttt{D}\ \{\psi\}$$

What about the inverse implication?

Theorem (Relative completeness)

If C *and* D *terminate with probability 1,*

$$\models \{\xi\}\ \texttt{C} \sim \texttt{D}\ \{\phi(\tau_1) + \psi(\tau_2)\} \quad \Rightarrow \quad \vdash \{\xi\}\ \texttt{C} \sim \texttt{D}\ \{\phi(\tau_1) + \psi(\tau_2)\}.$$

ϕ and ψ depend only on the output of C and D, resp.

What are the consequences of completeness?

Applications of eRHL's completeness

When $\mathtt{C}, \mathtt{D}$ terminate with probability 1:

Property	Equivalent Judgment	Complete
pRHL validity	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \ \sim\ \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin \mathcal{T}(S)]\}$	✓

pRHL validity:

$$\vDash \{\mathcal{R}\}\ \mathtt{C} \sim \mathtt{D}\ \{\mathcal{T}\}$$

Applications of eRHL's completeness

When $\mathtt{C}, \mathtt{D}$ terminate with probability 1:

Property	Equivalent Judgment	Complete
pRHL validity	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin \mathcal{T}(S)]\}$	✓
Program equivalence	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓

Program equivalence:

$$\sigma_1\ \mathcal{R}\ \sigma_2 \ \Rightarrow\ [\![\mathtt{C}]\!](\sigma_1) = [\![\mathtt{D}]\!](\sigma_2)$$

Applications of eRHL's completeness

When $\mathtt{C}, \mathtt{D}$ terminate with probability 1:

Property	Equivalent Judgment	Complete
pRHL validity	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin \mathcal{T}(S)]\}$	✓
Program equivalence	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓
Total variation	$\{1 + \delta\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓

Total variation:

$$\delta \geq \Delta_{\mathtt{TV}} = \sup_{S \subseteq \text{States}} \left| \mathbb{P}_{[\![\mathtt{C}]\!](\sigma_1)}[S] - \mathbb{P}_{[\![\mathtt{D}]\!](\sigma_2)}[S] \right|$$

Applications of eRHL's completeness

When C, D terminate with probability 1:

Property	Equivalent Judgment	Complete
pRHL validity	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin \mathcal{T}(S)]\}$	✓
Program equivalence	$\{1 + [\neg\mathcal{R}]\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓
Total variation	$\{1 + \delta\}\ \mathtt{C} \sim \mathtt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓
(ϵ, δ)-differential privacy	$\{\mathcal{R} \mid 2^{\epsilon} + \delta\}\ \mathtt{C} \sim \mathtt{C}\ \{[\tau_1 \in S] + 2^{\epsilon} \cdot [\tau_2 \notin S]\}$	✓

Differential privacy:

$$\sigma_1\ \mathcal{R}\ \sigma_2 \Rightarrow \forall S \subseteq \text{States.}\ \exp(\epsilon) \cdot \mathbb{P}_{[\![\mathtt{C}]\!](\sigma_2)}[S] + \delta \geq \mathbb{P}_{[\![\mathtt{C}]\!](\sigma_1)}[S]$$

Applications of eRHL's completeness

When C, D terminate with probability 1:

Property	Equivalent Judgment	Complete
pRHL validity	$\{1+[\neg\mathcal{R}]\}\ \texttt{C} \sim \texttt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin \mathcal{T}(S)]\}$	✓
Program equivalence	$\{1+[\neg\mathcal{R}]\}\ \texttt{C} \sim \texttt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓
Total variation	$\{1+\delta\}\ \texttt{C} \sim \texttt{D}\ \{[\tau_1 \in S] + [\tau_2 \notin S]\}$	✓
(ϵ,δ)-differential privacy	$\{\mathcal{R} \mid 2^{\epsilon}+\delta\}\ \texttt{C} \sim \texttt{C}\ \{[\tau_1 \in S] + 2^{\epsilon}\cdot[\tau_2 \notin S]\}$	✓
Kantorovich distance	$\{\mathcal{R} \mid w+h\}\ \texttt{C} \sim \texttt{D}\ \{f(\tau_1) + h - f(\tau_2)\}$	✓

Kantorovich distance:

$$w \geq W_{\Delta} \triangleq \inf_{\substack{\mu:\ \text{coupling of} \\ [\![\texttt{C}]\!](\sigma_1),\ [\![\texttt{D}]\!](\sigma_2).}} \left(\mathbb{E}_{(a_1,a_2)\leftarrow\mu}[\Delta(a_1,a_2)]\right)$$

Conclusion

Conclusion:

eRHL is a **quantitative**, relational program logic that is:

- Expressive and compositional,
- Sound and complete w.r.t. **pRHL judgments**, and $(\epsilon, \delta)-$**differential privacy**.

Conclusion

Conclusion:

eRHL is a **quantitative**, relational program logic that is:

- Expressive and compositional,
- Sound and complete w.r.t. **pRHL judgments**, and $(\epsilon, \delta)-$**differential privacy**.

In the paper:

- Rules for reasoning about **loops, recursive procedures, adversaries**.
- Case studies: PRP/PRF switching lemma, stability of SGD.

Conclusion

Conclusion:

eRHL is a **quantitative**, relational program logic that is:

- Expressive and compositional,
- Sound and complete w.r.t. **pRHL judgments**, and $(\epsilon, \delta)-$**differential privacy**.

In the paper:

- Rules for reasoning about **loops, recursive procedures, adversaries**.
- Case studies: PRP/PRF switching lemma, stability of SGD.

Thank you for your attention.