Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science

Electronic Notes in Theoretical Computer Science 325 (2016) 277–298

www.elsevier.com/locate/entcs

# Approximate Relational Hoare Logic for Continuous Random Samplings

Tetsuya Sato[1]

*Research Institute for Mathematical Sciences, Kyoto University, Kyoto, 606-8502, Japan*

**Abstract**

Approximate relational Hoare logic (apRHL) is a logic for formal verification of the differential privacy of databases written in the programming language pWHILE. Strictly speaking, however, this logic deals only with discrete random samplings. In this paper, we define the graded relational lifting of the subprobabilistic variant of Giry monad, which described differential privacy. We extend the logic apRHL with this graded lifting to deal with continuous random samplings. We give a generic method to give proof rules of apRHL for continuous random samplings.

*Keywords:* Differential privacy, Denotational semantics, Giry monad, Graded monad, Relational lifting

## 1 Introduction

Differential privacy is a *definition* of privacy of *randomised* databases proposed by Dwork, McSherry, Nissim and Smith [7]. A randomised database satisfies $\varepsilon$-differential privacy (written $\varepsilon$-differentially private) if for any two adjacent data, the difference of their output probability distributions is bounded by the privacy strength $\varepsilon$. Differential privacy guarantees high secrecy against database attacks regardless of the attackers' background knowledge, and it has the composition laws, with which we can calculate the privacy strength of a composite database from the privacy strengths of its components.

*Approximate relational Hoare logic* (apRHL) [2,17] is a probabilistic variant of the *relational Hoare logic* [4] for formal verification of the differential privacy of databases written in the programming language pWHILE. In the logic apRHL, a parametric relational lifting, which relate probability distributions, play a central role to describe differential privacy in the framework of verification. This parametric lifting is an extension of the relational lifting [10, Section 3] that captures

[1] Email:satoutet@kurims.kyoto-u.ac.jp

http://dx.doi.org/10.1016/j.entcs.2016.09.043

probabilistic bisimilarity of Markov chains [13] (see also [6, lemma 4]). The concept of differential privacy is described in the category of binary relation and mappings between them, and verified by the logic apRHL.

Strictly speaking, however, apRHL deals only with random samplings of *discrete* distributions, while the algorithms in many actual studies for differential privacy are modelled with *continuous* distributions, such as, the Laplacian distributions over real line. Therefore apRHL is desired to be extended to deal with random continuous samplings.

### *1.1 Contributions*

Main contributions of this paper are the following two points:

- We define the graded relational lifting of sub-Giry monad describing differential privacy for continuous random samplings.
- We extend the logic apRHL [2,17] for continuous random samplings (we name *continuous apRHL*) .

This graded relational lifting is developed without witness distributions of probabilistic coupling, and hence is constructed in a different way from the coupling-based parametric lifting of relations given in the studies of apRHL [1,2,17].

In the continuous apRHL, we mainly extend the proof rules for relation compositions and the frame rule. We also develop a generic method to construct proof rules for random samplings. By importing the new rules added to apRHL+ in [1], we give a formal proof of the differential privacy of the *above-threshold algorithm* for real-valued queries [8, Section 3.6].

### *1.2 Preliminaries*

We denote by **Set**, $\omega\mathbf{CPO}_{\perp}$, and **Meas** the categories of all sets and functions, all $\omega$-complete partial orders with the least element and continuous functions between them, and all measurable spaces and measurable functions respectively. The category **Meas** is complete, cocomplete, and distributive. The forgetful functor $U\colon \mathbf{Meas} \to \mathbf{Set}$ preserves limits and colimits. For each measurable space $X$, we write $\Sigma_X$ for the $\sigma$-algebra of $X$. For any $A \in \Sigma_X$, the *indicator function* $\chi_A\colon X \to [0,1]$ of $A$ is defined by $\chi_A(x) = 1$ if $X \in A$ and $\chi_A(x) = 0$ otherwise.

**The Category of Relations between Measurable Spaces**

We introduce the category **BRel**(**Meas**) of binary relations between *measurable spaces* as follows:

- An object is a triple $(X, Y, \Phi)$ consisting of measurable spaces $X$ and $Y$ and a relation $\Phi$ between $X$ and $Y$ (i.e. $\Phi \subseteq UX \times UY$). We remark that $\Phi$ does not necessary to be a measurable subset of the product space $X \times Y$.
- An arrow $(f, g)\colon (X, Y, \Phi) \to (X', Y', \Phi')$ is a pair of measurable functions $f\colon X \to X'$ and $g\colon Y \to Y'$ such that $(Uf \times Ug)(\Phi) \subseteq \Phi'$.

When we write an object $(X, Y, \Phi)$ in $\mathbf{BRel}(\mathbf{Meas})$, we omit to write the underlying spaces $X$ and $Y$ if they are obvious from the context. We write $p$ for the forgetful functor $\mathbf{BRel}(\mathbf{Meas}) \to \mathbf{Meas}^2$ extracting underlying spaces: $(X, Y, \Phi) \mapsto (X, Y)$.

The category $\mathbf{BRel}(\mathbf{Meas})$ is complete and cocomplete, and the forgetful functor $p$ preserves limits and colimits. We write $\dot{\times}$ and $\dot{+}$ for operators of the binary products and coproducts in $\mathbf{BRel}(\mathbf{Meas})$ respectively:

$$
\begin{aligned}
&(X, Y, \Phi)\dot{\times}(Z, W, \Psi) \\
&= (X \times Z, Y \times W, \{\, ((x, z), (y, w)) \mid (x, y) \in \Phi, (y, z) \in \Psi \,\}) \\
&(X, Y, \Phi)\dot{+}(Z, W, \Psi) \\
&= (X + Z, Y + W, \{\, (\iota_1(x), \iota_1(y)) \mid (x, y) \in \Phi \,\} \cup \{\, (\iota_2(z), \iota_2(w)) \mid (x, y) \in \Psi \,\}).
\end{aligned}
$$

**The Sub-Giry Monad**

The Giry monad on $\mathbf{Meas}$ is introduced in [9] to give a categorical approach to probability theory; each arrow $X \to Y$ in the Kleisli category of the Giry monad bijectively corresponds to a probabilistic transition from $X$ to $Y$, and the Chapman-Kolmogorov equation corresponds to the associativity law of the Giry monad.

We recall the sub-probabilistic variant of the Giry monad, which we call the *sub-Giry monad* (see also [18, Section 4]):

- For any measurable space $(X, \Sigma_X)$, the measurable space $\mathcal{G}X$ is defined as follows: the underlying set $U\mathcal{G}X$ of $\mathcal{G}X$ is the set of subprobability measures over $X$, and the $\sigma$-algebra $\Sigma_{\mathcal{G}X}$ of $\mathcal{G}X$ is the coarsest $\sigma$-algebra over $U\mathcal{G}X$ that makes the evaluation function $\mathrm{ev}_A \colon \mathcal{G}X \to [0, 1]$ $(\nu \mapsto \nu(A))$ measurable for any $A \in \Sigma_X$.
- For each $f \colon X \to Y$ in $\mathbf{Meas}$, $\mathcal{G}f \colon \mathcal{G}X \to \mathcal{G}Y$ is defined by $(\mathcal{G}f)(\nu) = \nu(f^{-1}(-))$.
- The unit $\eta$ is defined by $\eta_X(x) = \delta_x$, where $\delta_x$ is the *Dirac measure* centred on $x$.
- The multiplication $\mu$ is defined by $\mu_X(\Xi)(A) = \int_{\mathcal{G}X} \mathrm{ev}_A \, d(\Xi)$. The Kleisli lifting of $f \colon X \to \mathcal{G}Y$ is given by $f^\sharp(\nu)(A) = \int_X f(-)(A) \, d\nu$ $(\nu \in \mathcal{G}X)$.

The monad $\mathcal{G}$ is strong and commutative with respect to the cartesian product in $\mathbf{Meas}$. The strength $\mathrm{st}_{-,=} \colon (-) \times \mathcal{G}(=) \Rightarrow \mathcal{G}(- \times =)$ is given by the product measure $\mathrm{st}_{X,Y}(x, \nu) = \delta_x \otimes \nu$. The commutativity of $\mathcal{G}$ is shown from the Fubini theorem. The double strength $\mathrm{dst}_{-,=} \colon \mathcal{G}(-) \times \mathcal{G}(=) \Rightarrow \mathcal{G}(- \times =)$ is given by $\mathrm{dst}_{X,Y}(\nu_1, \nu_2) = \nu_1 \otimes \nu_2$.

The Kleisli category $\mathbf{Meas}_{\mathcal{G}}$ is often called the category $\mathbf{SRel}$ of *stochastic relations* [18, Section 3]. The category $\mathbf{SRel}$ is $\omega\mathbf{CPO}_\perp$-enriched (with respect to the cartesian monoidal structure) with the following pointwise order:

$$
f \sqsubseteq g \iff \forall x \in X, B \in \Sigma_Y . f(x)(B) \leq g(x)(B) \quad (f, g \colon X \to Y \text{ in } \mathbf{SRel}).
$$

The *least upper bound* $\sup_{n \in \mathbb{N}} f_n$ of any $\omega$-chain $f_0 \sqsubseteq f_1 \sqsubseteq \cdots \sqsubseteq f_n \sqsubseteq \cdots$ is given by $(\sup_n f_n)(x)(B) = \sup_n (f_n(x)(B))$. The *least function* of each $\mathbf{SRel}(X, Y)$ (written $\perp_{X,Y}$) is the constant function of the null-measure over $Y$. The *continuity* of composition is obtained from the following two facts:

- From the definition of Lebesgue integral, for any $\omega$-chain $\{\nu_n\}$ of subprobability

measures over $X$, $\int_X f\ d(\sup_n \nu_n) = \sup_n \int_X f\ d\nu_n$ holds.

- From the monotone convergence theorem, we have $\int_X \sup_n f_n\, d\nu = \sup_n \int_X f_n\, d\nu$.

This enrichment is equivalent to the partially additive structure on **SRel** [18, Section 5]: For any $\omega$-chain $\{f_n\}_{n\in\mathbb{N}}$ of $f_n \colon X \to Y$ in **SRel**, we have the summable sequence $\{g_n\}_n$ where $g_0 = f_0$ and $g_{n+1} = f_{n+1} - f_n$. Conversely, for any summable sequence $\{g_n\}_{n\in\mathbb{N}}$, the functions $f_n = \sum_{k=0}^{n} g_n$ form an $\omega$-chain.

**Differential privacy**

Throughout this paper, we define the differential privacy as follows:

**Definition 1.1** ([8, Definition 2.4], Modified) A measurable function (a query) $c \colon \mathbb{R}^m \to \mathcal{G}(\mathbb{R}^n)$ is $(\varepsilon, \delta)$-differentially private if $c(x)(A) \leq e^{\varepsilon} c(y)(A) + \delta$ holds whenever $||x - y||_1 \leq 1$ and $A \in \Sigma_{\mathbb{R}^n}$, where $||\cdot||_1$ is 1-norm of the space $\mathbb{R}^m$.

What we modify from the original definition [8, Definition 2.4] is the domain and codomain of $c$; we replace the domain from $\mathbb{N}$ to $\mathbb{R}$, and replace the codomain from a discrete probability space to $\mathcal{G}(\mathbb{R}^n)$. We apply this definition to the interpretation of pWHILE programs. The input and output spaces can be other spaces: in section 5 we consider the *above-threshold algorithm* `Above` whose output space is $\mathbb{Z}$. The above modification is essential in describing and verifying the differential privacy of this algorithm because it takes a sample from Laplace distribution over *real line*.

## 2 A Graded Monad for Differential Privacy

Barthe, Köpf, Olmedo, and Zanella-Béguelin constructed a *parametric relational lifting* describing differential privacy, and developed a framework for compositional verification of differential privacy [2]. The multiplication law of the lifting [2, Lemma 6] plays crucial role to in the formal verification of the differential privacy of queries.

Following this relational approach, we construct the parametric relational lifting of Giry monad to describe differential privacy for *continuous random samplings*. This lifting forms a graded monad on the category **BRel**(**Meas**) in the sense of [11]. The axioms of graded monad correspond to the (sequential) composition law of differential privacy.

### *2.1 Graded Monads*

**Definition 2.1** ([11, Definition 2.2-bis]) Let $\mathbb{C}$ be a category, and $(M, \cdot, 1, \preceq)$ be a *preordered* monoid. An $M$-graded (or $M$-parametric effect) monad on $\mathbb{C}$ consists of

- a collection $\{T_e\}_{e\in M}$ of endofunctors on $\mathbb{C}$,
- a natural transformation $\eta \colon \mathrm{Id} \Rightarrow T_1$,
- a collection $\{\mu^{e_1,e_2}\}_{e_1,e_2\in M}$ of natural transformations $\mu^{e_1,e_2} \colon T_{e_1}T_{e_2} \Rightarrow T_{e_1e_2}$,
- a collection $\{\sqsubseteq^{e_1,e_2}\}_{e_1\preceq e_2}$ of natural transformations $\sqsubseteq^{e_1,e_2} \colon T_{e_1} \Rightarrow T_{e_2}$

satisfying

- $\mu^{e,1} \circ T_e\eta = \mu^{1,e} \circ \eta_{T_e} = \mathrm{Id}_{T_e}$ for any $e \in M$,
- $\mu^{(e_1e_2),e_3} \circ \mu^{e_1,e_2}T_{e_3} = \mu^{e_1,(e_2,e_3)} \circ T_{e_1}\mu^{e_2,e_3}$ for all $e_1, e_2, e_3 \in M$,
- $\sqsubseteq^{e,e} = \mathrm{Id}_{T_e}$ for any $e$ and $\sqsubseteq^{e_2,e_3} \circ \sqsubseteq^{e_1,e_2} = \sqsubseteq^{e_1,e_3}$ whenever $e_1 \preceq e_2 \preceq e_3$,
- $\sqsubseteq^{(e_1e_2),(e_3e_4)} \circ \mu^{e_1,e_2} = \mu^{e_3,e_4} \circ (\sqsubseteq^{e_1,e_3} * \sqsubseteq^{e_2,e_4})$ whenever $e_1 \preceq e_3$ and $e_2 \preceq e_4$.

We call an $M$-graded monad $(\{T_e\}_{e\in M}, \eta, \mu^{e_1,e_2}, \sqsubseteq^{e_1,e_2})$ on $\mathbb{C}$ an $M$-graded lifting of a monad $(T, \eta^T, \mu^T)$ on $\mathbb{D}$ along $U\colon \mathbb{C} \to \mathbb{D}$ if $UT_e = TU$, $U(\eta) = \eta^T U$, $U(\mu^{e_1,e_2}) = \mu^T U$ $(e_1, e_2 \in M)$, and $U(\sqsubseteq^{e_1,e_2}) = \mathrm{id}_T$ $(e_1 \preceq e_2)$.

Let $T$ be a monad on **Meas**. We call an $M$-graded lifting of the product monad $T \times T$ of along the forgetful functor $p$ an *$M$-graded relational lifting* of $T$.

### *2.2 A Graded Relational Lifting of Giry Monad for Differential Privacy*

Let $M$ be the cartesian product of the monoids $([0,\infty), +, 0)$ and $([0,\infty), +, 0)$ equipped with the product order of numerical orders. The monoid $M$ is the set of parameters $(\varepsilon, \delta)$ of differential privacy. For each $(\varepsilon, \delta) \in M$, we define the following mapping of **BRel**(**Meas**)-objects by

$$\begin{aligned}&\mathcal{G}^{(\varepsilon,\delta)}(X, Y, \Phi)\\ &= (\mathcal{G}X, \mathcal{G}Y, \{\, (\nu_1, \nu_2) \mid \forall A \in \Sigma_X, B \in \Sigma_Y.\Phi(A) \subseteq B \implies \nu_1(A) \le e^{\varepsilon}\nu_2(B) + \delta \,\}).\end{aligned}$$

**Theorem 2.2** *$\{\mathcal{G}^{(\varepsilon,\delta)}\}_{(\varepsilon,\delta)\in M}$ forms an $M$-graded relational lifting of $\mathcal{G}$.*

**Proof.** Since the functor $p$ is faithful, it suffices to show:

(i) $(\mathcal{G}f, \mathcal{G}g)$ is an arrow $\mathcal{G}^{(\varepsilon,\delta)}(Z, W, \Psi) \to \mathcal{G}^{(\varepsilon,\delta)}(X, Y, \Phi)$ in **BRel**(**Meas**) for any arrow $(f, g)\colon (Z, W, \Psi) \to (X, Y, \Phi)$ in **BRel**(**Meas**) and $(\varepsilon, \delta) \in M$.

(ii) $(\mathrm{id}_{\mathcal{G}X}, \mathrm{id}_{\mathcal{G}Y})$ is an arrow $\mathcal{G}^{(\varepsilon,\delta)}(X, Y, \Phi) \to \mathcal{G}^{(\varepsilon',\delta')}(X, Y, \Phi)$ in **BRel**(**Meas**) for any $(X, Y, \Phi)$ and $(\varepsilon, \delta), (\varepsilon', \delta') \in M$ that satisfy $\varepsilon \le \varepsilon'$ and $\delta \le \delta'$.

(iii) $(\eta_X, \eta_Y)$ is an arrow $(X, Y, \Phi) \to \mathcal{G}^{(0,0)}(X, Y, \Phi)$ in **BRel**(**Meas**).

(iv) $(\mu_X, \mu_Y)$ is an arrow $\mathcal{G}^{(\varepsilon,\delta)}\mathcal{G}^{(\varepsilon',\delta')}(X, Y, \Phi) \to \mathcal{G}^{(\varepsilon+\varepsilon',\delta+\delta)}(X, Y, \Phi)$ in **BRel**(**Meas**) for any $(X, Y, \Phi)$ and $(\varepsilon, \delta), (\varepsilon', \delta') \in M$.

We prove these statements:

**(i)** Let $(\nu_1, \nu_2) \in \mathcal{G}^{(\varepsilon,\delta)}\Psi$. We have $\Psi(f^{-1}(A)) \subseteq g^{-1}(B)$ for any $A \in \Sigma_X$ and $B \in \Sigma_Y$ such that $\Phi(A) \subseteq B$. This implies $((\mathcal{G}f)(\nu_1), (\mathcal{G}g)(\nu_2)) \in \mathcal{G}^{(\varepsilon,\delta)}\Phi$.

**(ii)** We have the obvious inclusion $\mathcal{G}^{(\varepsilon,\delta)}\Phi \subseteq \mathcal{G}^{(\varepsilon',\delta')}\Phi$.

**(iii)** Let $(x, y) \in \Phi$. We have $(\eta_X(x)(A), \eta_Y(y)(B)) = (0,0), (0,1), (1,1)$ for any $A \in \Sigma_X$ and $B \in \Sigma_Y$ such that $\Phi(A) \subseteq B$. This implies $(\eta_X(x), \eta_Y(y)) \in \mathcal{G}^{(0,0)}\Phi$.

**(iv)** We first prove the following equalities:

$$\begin{aligned}\mathcal{G}^{(\varepsilon,\delta)}\Phi &\overset{(\dagger)}{=} \bigcap \left\{ (f^\sharp \times g^\sharp)^{-1}S(\varepsilon, \delta) \;\middle|\; (f, g)\colon \Phi \to (\mathcal{G}1, \mathcal{G}1, \le) \text{ in } \mathbf{BRel}(\mathbf{Meas}) \right\}\\ &\overset{(\ddagger)}{=} \bigcap \left\{ (f^\sharp \times g^\sharp)^{-1}S(\varepsilon + \varepsilon', \delta + \delta) \;\middle|\; (f, g)\colon \Phi \to S(\varepsilon', \delta') \text{ in } \mathbf{BRel}(\mathbf{Meas}) \right\}.\end{aligned}$$

where, $S(\varepsilon,\delta) = (\mathcal{G}1, \mathcal{G}1, \{\, (\alpha_1,\alpha_2) \mid \alpha_1 \le e^{\varepsilon}\alpha_2 + \delta \,\})$ and $(\mathcal{G}1, \mathcal{G}1, \le) = S(0,0)$. We remark $\mathcal{G}1 \simeq [0,1]$.

**(†)** We prove in the similar way as [12, Theorem 12]: ($\supseteq$) Suppose $(\nu_1,\nu_2) \in (f^\sharp \times g^\sharp)^{-1} S(\varepsilon,\delta)$ for any $(f,g)\colon \Phi \to \le$, and suppose that $A \in \Sigma_X$ and $B \in \Sigma_Y$ satisfy $\Phi(A) \subseteq B$. Since $(\chi_A, \chi_B)\colon \Phi \to \le$, we obtain $\nu_1(A) \le e^{\varepsilon}\nu_2(B) + \delta$. This implies $(\nu_1,\nu_2) \in \mathcal{G}^{(\varepsilon,\delta)}\Phi$. ($\subseteq$) Let $(\nu_1,\nu_2) \in \mathcal{G}^{(\varepsilon,\delta)}\Phi$ and $(f,g)\colon \Phi \to \le$. Since $\Phi(f^{-1}[\alpha,1]) \subseteq g^{-1}[\alpha,1]$ for any $\alpha \in [0,1]$, we obtain $(f^\sharp(\nu_1), g^\sharp(\nu_2)) \in S(\varepsilon,\delta)$ from

$$\begin{aligned}\int_X f d\nu_1 &= \sup\left\{ \textstyle\sum_{i=0}^n \alpha_i \nu_1(f^{-1}[\sum_{k=0}^i \alpha_i, 1]) \;\middle|\; \forall i. 0 < \alpha_i, \sum_{i=0}^n \alpha_i \le 1 \right\} \\ &\le \sup\left\{ \textstyle\sum_{i=0}^n \alpha_i (e^{\varepsilon}\nu_2(g^{-1}[\sum_{k=0}^i \alpha_i, 1]) + \delta) \;\middle|\; \forall i. 0 < \alpha_i, \sum_{i=0}^n \alpha_i \le 1 \right\} \\ &\le e^{\varepsilon} \int_Y g d\nu_2 + \delta.\end{aligned}$$

**(‡)** ($\supseteq$) Obvious. ($\subseteq$) Suppose that $(k^\sharp\nu_1, l^\sharp\nu_2) \in S(\varepsilon,\delta)$ holds for any $(k,l)\colon \Phi \to \le$. Let $(f,g)\colon \Phi \to S(\varepsilon',\delta')$. The pair $(\max(f-\delta', 0), \min(e^{\varepsilon'}g, 1))$ forms an arrow $\Phi \to \le$ in $\mathbf{BRel}(\mathbf{Meas})$ because $f - \delta' \le 1$ and $0 \le e^{\varepsilon'}g$. We have $(f^\sharp(\nu_1), g^\sharp(\nu_2)) \in S(\varepsilon+\varepsilon', \delta+\delta')$ from

$$\begin{aligned}\int_X f d\nu_1 - \delta' &\le \int_X \max(f-\delta', 0) d\nu_1 \\ &\le e^{\varepsilon} \int_Y \min(e^{\varepsilon'}g, 1) d\nu_2 + \delta \le e^{(\varepsilon+\varepsilon')} \int_Y g d\nu_2 + \delta.\end{aligned}$$

Now, we prove the inclusion $(\mu_X \times \mu_Y)(\mathcal{G}^{(\varepsilon,\delta)}\mathcal{G}^{(\varepsilon',\delta')}\Phi) \subseteq \mathcal{G}^{(\varepsilon+\varepsilon',\delta+\delta)}\Phi$.

Let $(\Xi_1,\Xi_2) \in \mathcal{G}^{(\varepsilon,\delta)}\mathcal{G}^{(\varepsilon',\delta')}\Phi$ and $(f,g)\colon \Phi \to S(\varepsilon'',\delta'')$. From the equalities (†) and (‡), we have $(f^\sharp, g^\sharp)\colon \mathcal{G}^{(\varepsilon',\delta')}\Phi \to S(\varepsilon'+\varepsilon'', \delta'+\delta'')$. We therefore obtain

$$(f^\sharp(\mu_X(\Xi_1)), g^\sharp(\mu_Y(\Xi_2))) = ((f^\sharp)^\sharp(\Xi_1), (g^\sharp)^\sharp(\Xi_2)) \in S(\varepsilon+\varepsilon'+\varepsilon'', \delta+\delta'+\delta'').$$

Since $(f,g)\colon \Phi \to S(\varepsilon'',\delta'')$ is arbitrary, $(\mu_X(\Xi_1), \mu_Y(\Xi_2)) \in \mathcal{G}^{(\varepsilon+\varepsilon',\delta+\delta)}\Phi$ holds. □

Now we characterise the differential privacy with the lifting $\{\mathcal{G}^{(\varepsilon,\delta)}\}_{(\varepsilon,\delta)\in M}$.

**Theorem 2.3** *A measurable function $c\colon \mathbb{R}^m \to \mathcal{G}(\mathbb{R}^n)$ is $(\varepsilon,\delta)$-differentially private* if and only if *$(c,c)$ is an arrow $\{\, (x,y) \mid ||x-y||_1 \le 1 \,\} \to \mathcal{G}^{(\varepsilon,\delta)}\mathrm{Eq}_{\mathbb{R}^n}$ in* $\mathbf{BRel}(\mathbf{Meas})$.

The sequential and parallel composability (see also [8,14]) of differential privacy are obtained from the following property of the $M$-graded lifting $\{\mathcal{G}^{(\varepsilon,\delta)}\}_{(\varepsilon,\delta)\in M}$:

**Proposition 2.4 (Composabilities)**

(i) *For any $(f_1,g_1)\colon \Phi_1 \to \mathcal{G}^{(\varepsilon,\delta)}\Psi_1$ and $(f_2,g_2)\colon \Phi_2 \to \mathcal{G}^{(\varepsilon',\delta')}\Psi_2$ in* $\mathbf{BRel}(\mathbf{Meas})$, *$(\mathrm{dst}\circ(f_1\times f_2), \mathrm{dst}\circ(g_1\times g_2))$ is an arrow $\Phi_1 \dot{\times} \Phi_2 \to \mathcal{G}^{(\varepsilon+\varepsilon',\delta+\delta')}(\Psi_1 \dot{\times} \Psi_2)$ in* $\mathbf{BRel}(\mathbf{Meas})$.

(ii) *For any* $(f_1, g_1)\colon \Phi_1 \to \mathcal{G}^{(\varepsilon,\delta)}\Psi$ *and* $(f_2, g_2)\colon \Phi_2 \to \mathcal{G}^{(\varepsilon',\delta')}\Psi$ *in* **BRel**(**Meas**), $([f_1, f_2], [g_1, g_2])$ *is an arrow* $\Phi_1 \dot{+} \Phi_2 \to \mathcal{G}^{(\max(\varepsilon,\varepsilon'),\max(\delta,\delta))}\Psi$ *in* **BRel**(**Meas**).

**Proof.**

**(i)** It suffices to show that $(\mathrm{st}, \mathrm{st})$ is an arrow $: \Phi_1 \dot{\times} \mathcal{G}^{(\varepsilon,\delta)}\Phi_2 \to \mathcal{G}^{(\varepsilon,\delta)}(\Phi_1 \dot{\times} \Phi_2)$ for any objects $\Phi_1$ and $\Phi_2$ in **BRel**(**Meas**). We let $\Phi_i = (X_i, Y_i, \Phi_i)$ $(i = 1, 2)$. Suppose $((x, \nu_1), (y, \nu_2)) \in \Phi_1 \dot{\times} \mathcal{G}^{(\varepsilon,\delta)}\Phi_2$, and assume that $A \in \Sigma_{X_1 \times X_2}$ and $B \in \Sigma_{Y_1 \times Y_2}$ satisfy $(\Phi_1 \dot{\times} \Phi_2)(A) \subseteq B$. We obtain $\mathrm{st}(x, \nu_1)(A) = \nu_1(A_x)$ and $\mathrm{st}(y, \nu_2)(B) = \nu_1(B_y)$. Here, $A_x = \{\, w \in X_1 \mid (x, w) \in A \,\}$ and $B_y$ is given in the same way. We have $A_x \in \Sigma_{X_1}$ and $B_y \in \Sigma_{X_2}$ from the construction of product spaces. We obtain $\Phi_2(A_x) \subseteq B_y$ by $z \in \Phi_2(A_x) \implies \exists w \in A_X.(y, z) \in (\Phi_1 \dot{\times} \Phi_2)(x, w)$ This implies $\mathrm{st}(x, \nu_1)(A) \leq e^{\varepsilon}\mathrm{st}(y, \nu_2)(B) + \delta$.

**(ii)** It suffices to prove $\mathcal{G}^{(\varepsilon,\delta)}\Phi \cap \mathcal{G}^{(\varepsilon',\delta')}\Phi \subseteq \mathcal{G}^{(\max(\varepsilon,\varepsilon'),\max(\delta,\delta'))}\Phi$ for any object $\Phi$ in **BRel**(**Meas**). This is proved from the equality (†) in the proof of Theorem 2.2 and the inclusion $S(\varepsilon, \delta) \cap S(\varepsilon', \delta') \subseteq S(\max(\varepsilon, \varepsilon'), \max(\delta, \delta'))$.

□

In fact, we have $S(\varepsilon, \delta) \cap S(\varepsilon', \delta') \subseteq S(\max(\log(\frac{1-\delta''}{1-\delta}) + \varepsilon, \log(\frac{1-\delta''}{1-\delta'}) + \varepsilon'), \delta'')$ where $\delta'' = \max(\delta, \delta')$. Hence, the parallel composability (ii) can be improved.

**The Symmetrised Lifting of $\mathcal{G}^{(\varepsilon,\delta)}$**

We recall that the relations $\{\, (x, y) \mid ||x - y||_1 \leq 1 \,\}$ and $\mathrm{Eq}_{\mathbb{R}^n}$ in Theorem 2.3 are symmetric. We hence observe that the $M$-graded lifting $\{\mathcal{G}^{(\varepsilon,\delta)}\}_{(\varepsilon,\delta)\in M}$ describes only one side of inequalities in the definition of differential privacy. By symmetrising this lifting, We obtain an $M$-graded lifting $\{\overline{\mathcal{G}^{(\varepsilon,\delta)}}\}_{(\varepsilon,\delta)\in M}$ exactly describing the differential privacy for continuous probabilities:

$$\overline{\mathcal{G}^{(\varepsilon,\delta)}} = \mathcal{G}^{(\varepsilon,\delta)}(-) \cap (\mathcal{G}^{(\varepsilon,\delta)}(-)^{\Phi})^{\Phi}.$$

### *2.3 Parametric Lifting in the Original(discrete) apRHL*

In the original works [2,3] of apRHL, the following parametric relational lifting $(-)^{\sharp(\varepsilon,\delta)}$ of the (sub)distribution monad $\mathcal{D}$ on **Set** is introduced to describe differential privacy. This lifting relates two distributions if there are intermediate distributions $d_1$ and $d_R$, called *witnesses*, whose skew distance, defined by

$$\Delta_{\varepsilon}^{X}(d_L, d_R) = \sup_{C \subseteq X} \max(d_L(C) - e^{\varepsilon}d_R(C), d_R(C) - e^{\varepsilon}d_L(C), 0).$$

**Definition 2.5** ([3, Definition 4], [17, Definition 4.3] and [1, Definition 8]) Let $\Psi$ be a relation between sets $X$ and $Y$. We define the relation $\Psi^{\sharp(\varepsilon,\delta)} \subseteq \mathcal{D}X \times \mathcal{D}Y$ as follows: $d_1 \in \mathcal{D}X$ and $d_2 \in \mathcal{D}Y$ satisfy $(d_1, d_2) \in \Psi^{\sharp(\varepsilon,\delta)}$ if and only if there are two (sub)probability distributions $d_L, d_R \in \mathcal{D}(X \times Y)$, called *witnesses*, such that

$$\mathcal{D}\pi_1(d_L) = d_1,\ \mathcal{D}\pi_2(d_R) = d_2,\ \mathrm{supp}(d_L) \subseteq \Psi,\ \mathrm{supp}(d_R) \subseteq \Psi,\ \Delta_{\varepsilon}^{X\times Y}(d_L, d_R) \leq \delta.$$

**Proposition 2.6** *For any countable discrete spaces $X$ and $Y$, and relation $\Psi \subseteq X \times Y$, we have $\Psi^{\sharp(\varepsilon,\delta)} \subseteq \overline{\mathcal{G}^{(\varepsilon,\delta)}}\Psi$.*

**Proof.** Suppose $(d_1, d_2) \in \Psi^{\sharp(\varepsilon,\delta)}$ with witnesses $d_L$ and $d_R$. For any $A \subseteq X$, since $\mathrm{supp}(d_L) \subseteq \Psi$ and $(A \times Y) \cap \Psi \subseteq X \times \Psi(A)$, we obtain:

$$\begin{aligned} d_1(A) = \mathcal{D}\pi_1(d_L)(A) = d_L(A \times Y) = d_L((A \times Y) \cap \Psi) \leq d_L(X \times \Psi(A)) \\ \leq \varepsilon d_R(X \times \Psi(A)) + \delta = e^{\varepsilon}\mathcal{D}\pi_2(d_R)(\Psi(A)) + \delta = e^{\varepsilon} d_2(\Psi(A)) + \delta. \end{aligned}$$

This implies $(d_1, d_2) \in \mathcal{G}^{(\varepsilon,\delta)}\Psi$. Since the construction of $(-)^{\sharp(\varepsilon,\delta)}$ is symmetric, we conclude $(d_1, d_2) \in \overline{\mathcal{G}^{(\varepsilon,\delta)}}\Psi$. □

We remark that we may regard $\mathcal{G}X = \mathcal{D}X$ for countable discrete space $X$. When $X$ is not countable, we have the same results by embedding each $d \in \mathcal{D}X$ in the set $\mathcal{D}X'$ of subprobability distributions over the countable *subspace* $X' = X \cap \mathrm{supp}(d)$.

**Corollary 2.7** *We have $\mathrm{Eq}_X^{\sharp(\varepsilon,\delta)} = \overline{\mathcal{G}^{(\varepsilon,\delta)}}\mathrm{Eq}_X$ for any countable discrete space $X$.*

**Proof.** ($\subseteq$) This inclusion is given from Proposition 2.6. ($\supseteq$) Suppose $(d_1, d_2) \in \overline{\mathcal{G}^{(\varepsilon,\delta)}}\mathrm{Eq}_X$. This is equivalent to $\Delta_\varepsilon^X(d_1, d_2) \leq \delta$. Hence $(d_1, d_2) \in \mathrm{Eq}_X^{\sharp(\varepsilon,\delta)}$ is proved by the witnesses given by $d_L = \sum_{x \in X} d_1(x) \cdot \delta_{(x,x)}$ and $d_R = \sum_{x \in X} d_2(x) \cdot \delta_{(x,x)}$. □

When $\Psi = \emptyset$ and $\delta > 0$, the inclusion of Proposition 2.6 is proper, because $\Psi^{\sharp(\varepsilon,\delta)}$ is the singleton $\{(0, 0)\}$, but $\overline{\mathcal{G}^{(\varepsilon,\delta)}}\Psi$ contains at least all pairs $(d_1, d_2)$ such that $d_1(X), d_2(Y) < \delta$. Thus, the lifting $\overline{\mathcal{G}^{(\varepsilon,\delta)}}$ is strictly larger than the lifting $(-)^{\sharp(\varepsilon,\delta)}$ even in the countable discrete cases. This implies that, roughly speaking, we can reuse formal proofs in the original apRHL to the continuous apRHL.

When $\varepsilon = \delta = 0$, the lifting $(-)^{\sharp(\varepsilon,\delta)}$ describes coalgebraic bisimulations between Markov chains, that is, $\mathcal{D}$-coalgebras [13] (see also [6,10]), and the lifting $\mathcal{G}^{(\varepsilon,\delta)}$ corresponds to the relational lifting (codensity lifting) of the sub-Giry monad $\mathcal{G}$ describing simulations between Markov processes [12, Theorem 12].

# 3 The Continuous apRHL

We introduce a variant of the approximate probabilistic relational Hoare logic (apRHL) to deal with continuous random samplings. We name it the *continuous apRHL*.

## *3.1 The Language pWHILE*

We recall and reformulate categorically the language pWHILE [2]. The language pWHILE is constructed in the standard way, hence we sometimes omit the details of its construction. In this paper, we mainly refer to the categorical semantics of a probabilistic language given in [5, Section 2].

### 3.1.1 Syntax

We introduce the syntax of pWHILE by the following BNF:

$$\begin{aligned}
\tau &::= \texttt{bool} \mid \texttt{int} \mid \texttt{real} \mid \dots \\
e &::= x \mid p(e_1, \dots, e_m) \\
\nu &::= d(e_1, \dots, e_m) \\
i &::= x \leftarrow e \mid x \overset{\$}{\leftarrow} \nu \mid \texttt{if } e \texttt{ then } c_1 \texttt{ else } c_2 \mid \texttt{while } e \texttt{ do } c \\
c &::= \texttt{skip} \mid \texttt{null} \mid \mathcal{I}; \mathcal{C}
\end{aligned}$$

Here, $\tau$ is a *value type*; $x$ is a *variable*; $p$ is an *operation*; $d$ is a *probabilistic operation*; $e$ is an *expression*; $\nu$ is a *probabilistic expression*; $i$ is an *imperative*; $c$ is a *command* (or program). We remark constants are 0-ary operations.

We introduce the following syntax sugars for simplicity:

$$\texttt{if } b \texttt{ then } c = \texttt{if } b \texttt{ then } c \texttt{ else skip}$$

$$[\texttt{while } b \texttt{ do } c]_n = \begin{cases} \texttt{if } b \texttt{ then null else skip}, & \text{if } n = 0 \\ \texttt{if } b \texttt{ then } c; [\texttt{while } b \texttt{ do } c]_k, & \text{if } n = k+1 \end{cases}$$

### 3.1.2 Typing Rules

We introduce a typing rule on the language pWHILE. A typing context is a finite set $\Gamma = \{x_1 \colon \tau_1, x_2 \colon \tau_2, \dots, x_n \colon \tau_n\}$ of pairs of a variable and a value type such that each variable occurs only once in the context.

We give typing rules of pWHILE as follows:

$$\frac{\Gamma \vdash^t e_1 \colon \tau_1 \ \dots \ \Gamma \vdash^t e_n \colon \tau_n \quad p \colon (\tau_1, \dots, \tau_n) \to \tau}{\Gamma \vdash^t p(e_1, \dots, e_n) \colon \tau} \qquad \frac{\Gamma, x \colon \tau \vdash^t e \colon \tau}{\Gamma, x \colon \tau \vdash x \leftarrow e} \qquad \frac{}{\Gamma \vdash \texttt{skip}}$$

$$\frac{x \colon \tau \in \Gamma \quad \Gamma \vdash^t e_1 \colon \tau_1 \ \dots \ \Gamma \vdash^t e_n \colon \tau_n \quad d \colon (\tau_1, \dots, \tau_n) \to \tau}{\Gamma \vdash x \overset{\$}{\leftarrow} d(e_1, \dots, e_n) \colon \tau} \qquad \frac{}{\Gamma \vdash \texttt{null}}$$

$$\frac{\Gamma \vdash i \quad \Gamma \vdash c}{\Gamma \vdash i; c} \qquad \frac{\Gamma \vdash^t b \colon \texttt{bool} \quad \Gamma \vdash c_1 \quad \Gamma \vdash c_2}{\Gamma \vdash \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2} \qquad \frac{\Gamma \vdash^t b \colon \texttt{bool} \quad \Gamma \vdash c}{\Gamma \vdash \texttt{while } b \texttt{ do } c}$$

Here, the type $(\tau_1, \dots, \tau_n) \to \tau$ of each operation $p$ and each probabilistic operation $d$ are assumed to be given in advance.

We easily define inductively the set of free variables of commands, expressions, and probabilistic expressions (denoted by $FV(c)$, $FV(e)$, and $FV(\nu)$).

### 3.1.3 Denotational Semantics

We introduce a denotational semantics of pWHILE in **Meas**. We give the interpretations $[\![\tau]\!]$ of the value types $\tau$:

- $[\![\texttt{bool}]\!] = \mathbb{B} = 1 + 1 = \{\texttt{true}, \texttt{false}\}$ (discrete space)
- $[\![\texttt{int}]\!] = \mathbb{Z}$ (discrete space)
- $[\![\texttt{real}]\!] = \mathbb{R}$ (Lebesgue measurable space)

We interpret a typing context $\Gamma = \{x_1 \colon \tau_1, x_2 \colon \tau_2, \dots, x_n \colon \tau_n\}$ as the product space $[\![\tau_1]\!] \times [\![\tau_2]\!] \times \cdots \times [\![\tau_n]\!]$. We interpret each operation $p \colon (\tau_1, \dots \tau_m) \to \tau$ as a measurable function $[\![p]\!] \colon [\![\tau_1]\!] \times \cdots \times [\![\tau_m]\!] \to [\![\tau]\!]$, and each probabilistic operation $d \colon (\tau_1, \dots \tau_m) \to \tau$ as $[\![d]\!] \colon [\![\tau_1]\!] \times \cdots \times [\![\tau_m]\!] \to \mathcal{G}[\![\tau]\!]$. Typed terms$\Gamma \vdash^t e \colon \tau$ and commands $\Gamma \vdash c$ are interpreted to measurable functions of the forms $[\![\Gamma]\!] \to [\![\tau]\!]$ and $[\![\Gamma]\!] \to \mathcal{G}[\![\Gamma]\!]$ respectively.

The interpretation of expressions are defined inductively by:

$$[\![\Gamma \vdash^t x \colon \tau]\!] = \pi_{x \colon \tau} \quad [\![\Gamma \vdash^t p(e_1, \dots, \mathrm{e}_m)]\!] = [\![p]\!]([\![\Gamma \vdash^t e_1]\!], \dots [\![\Gamma \vdash^t e_m]\!])$$

The interpretation of commands are defined inductively by:

$$\begin{aligned}
[\![\Gamma \vdash \texttt{skip}]\!] &= \eta_{[\![\Gamma]\!]} \quad [\![\Gamma \vdash \texttt{null}]\!] = \bot_{[\![\Gamma]\!],[\![\Gamma]\!]} \quad [\![\Gamma \vdash i; c]\!] = ([\![\Gamma \vdash c]\!])^\sharp \circ [\![\Gamma \vdash i]\!] \\
&[\![\Gamma \vdash x \xleftarrow{\$} d(e_1, \dots, \mathrm{e}_m)]\!] \\
&= \mathcal{G}(\rho_{(x \colon \tau, \Gamma)}) \circ \mathrm{st}_{[\![\tau]\!],[\![\Gamma]\!]} \circ \langle [\![d]\!]([\![\Gamma \vdash^t e_1]\!], \dots [\![\Gamma \vdash^t e_m]\!]), \mathrm{id}_{[\![\Gamma]\!]} \rangle \\
&[\![\Gamma, x \colon \tau \vdash x \leftarrow e]\!] = \eta_{[\![\Gamma, x \colon \tau]\!]} \circ \rho_{(x \colon \tau, \Gamma)} \circ \langle [\![\Gamma, x \colon \tau \vdash e]\!], \mathrm{id}_{[\![\Gamma, x \colon \tau]\!]} \rangle \\
[\![\Gamma \vdash \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2]\!] &= [[\![\Gamma \vdash c_1]\!], [\![\Gamma \vdash c_2]\!]] \circ \cong_{[\![\Gamma]\!]} \circ \langle [\![\Gamma \vdash b]\!], \mathrm{id}_{[\![\Gamma]\!]} \rangle \\
[\![\Gamma \vdash \texttt{while } b \texttt{ do } c]\!] &= \sup_{n \in \mathbb{N}} [\![\Gamma \vdash [\texttt{while } e \texttt{ do } c]_n]\!]
\end{aligned}$$

Here,

- $\rho_{(x_k \colon \tau_k, \Gamma)} = \langle f_l \rangle_{l \in \{1,2,\dots,n\}} \colon [\![\tau_k]\!] \times [\![\Gamma]\!] \to [\![\Gamma]\!]$, where $\Gamma = \{x_1 \colon \tau_1, x_2 \colon \tau_2, \dots, x_n \colon \tau_n\}$, $f_k = \pi_2$, and $f_l = \pi_l \circ \pi_2$ $(l \neq k)$.
- $\cong_X \colon 2 \times X \to X + X$ is the inverse of $[\langle \iota_1 \circ !_X,\ id \rangle, \langle \iota_2 \circ !_X,\ id \rangle] \colon X + X \to 2 \times X$, which is obtained from the distributivity of the category **Meas**.

We remark that, from the commutativity of the monad $\mathcal{G}$, if $\Gamma \vdash x \colon \tau$ and $x \notin FV(c)$ then $[\![\Gamma \vdash c]\!] \cong \mathrm{dst}_{[\![\Gamma']\!],[\![\tau]\!]}([\![\Gamma' \vdash c]\!] \times \eta_{[\![\tau]\!]})$ where $\Gamma' = \Gamma \setminus \{x \colon \tau\}$.

### *3.2 Judgements*

A judgement of apRHL is

$$c_1 \sim_{\varepsilon,\delta} c_2 \colon \Psi \Rightarrow \Phi,$$

where $c_1$ and $c_1$ are commands, and $\Psi$ and $\Phi$ are objects in **BRel**(**Meas**). We call the relations $\Psi$ and $\Phi$ the *precondition* and *postcondition* of the judgement respectively. Inspired from the validity of asymmetric apRHL [2], we introduce the validity of the judgement of apRHL.

**Definition 3.1** Let $\Psi$ and $\Phi$ be relations on the space $[\![\Gamma]\!]$. A judgement $c_1 \sim_{\varepsilon,\delta} c_2 \colon \Psi \Rightarrow \Phi$ is valid (written $\models c_1 \sim_{(\varepsilon,\delta)} c_2 \colon \Psi \Rightarrow \Phi$) when $([\![\Gamma \vdash c_1]\!], [\![\Gamma \vdash c_2]\!])$ is an arrow $\Psi \to \overline{\mathcal{G}^{(\varepsilon,\delta)}}\Phi$ in **BRel**(**Meas**).

We often write preconditions and postconditions in the following manner: Let $\Gamma = \{x_1 \colon \tau_1, x_2 \colon \tau_2, \dots, x_n \colon \tau_n\}$. Assume $\Gamma \vdash e_1 \colon \tau$ and $\Gamma \vdash e_2 \colon \tau$, and let $R$ be a relation on $[\![\tau]\!]$ (e.g. $=$, $\leq$,... ). We define the relation $e_1\langle 1 \rangle R e_2 \langle 2 \rangle$ on $[\![\Gamma]\!]$ by

$$(e_1\langle 1 \rangle R e_2 \langle 2 \rangle) = \{\ (m_1, m_2) \in [\![\Gamma]\!] \mid [\![\Gamma \vdash e_1]\!](m_1) R [\![\Gamma \vdash e_2]\!](m_2)\ \}\,.$$

To prove $(\varepsilon, \delta)$-differential privacy of a program $\Gamma \vdash c$ in (continuous) apRHL, we show the validity of judgement of the form $c \sim_{(\varepsilon,\delta)} c\colon ||x\langle 1\rangle - x\langle 2\rangle||_1 \leq 1 \Rightarrow y\langle 1\rangle = y\langle 2\rangle$, where $x$ and $y$ are variables for inputs and outputs respectively.

### *3.3 Proof Rules*

We mainly refer the proof rules of apRHL from [2,17], but we modify the [comp] and [frame] rules to verify differential privacy for continuous random samplings.

$$\frac{x_1\colon \tau_1, x_2\colon \tau_2 \in \Gamma \quad \Gamma \vdash^t e_1\colon \tau_1 \quad \Gamma \vdash^t e_2\colon \tau_2 \quad (\rho_{(x_1\colon \tau_1,\Gamma)} \circ \langle [\![e_1]\!], \mathrm{id}\rangle, \rho_{(x_2\colon \tau_2,\Gamma)} \circ \langle [\![e_2]\!], \mathrm{id}\rangle)\colon \Psi \to \Phi}{\models x_1 \leftarrow e_1 \sim_{(0,0)} x_2 \leftarrow e_2\colon \Psi \Rightarrow \Phi}\ [\mathrm{assn}]$$

$$\frac{\Gamma \vdash^t e_1^1\colon \tau_1 \ \dots\ \Gamma \vdash^t e_m^1\colon \tau_m \quad \Gamma \vdash^t e_1^2\colon \tau_1 \ \dots\ \Gamma \vdash^t e_m^2\colon \tau_m \quad x_1\colon \tau, x_2\colon \tau \in \Gamma \quad (\langle [\![e_1^1]\!], \dots, [\![e_m^1]\!]\rangle, \langle [\![e_1^2]\!], \dots, [\![e_m^2]\!]\rangle)\colon \Psi' \to \Psi \text{ in } \mathbf{BRel}(\mathbf{Meas}) \quad d\colon (\tau_1, \dots, \tau_m) \to \tau \quad ([\![d]\!], [\![d]\!])\colon \Psi \to \overline{\mathcal{G}^{(\varepsilon,\delta)}}(\mathrm{Eq}_{[\![\tau]\!]}) \text{ in } \mathbf{BRel}(\mathbf{Meas})}{\models x_1 \xleftarrow{\$} d(e_1^1, \dots, e_m^1) \sim_{(\varepsilon,\delta)} x_2 \xleftarrow{\$} d(e_1^2, \dots, e_m^2)\colon \Psi' \Rightarrow (x_1\langle 1\rangle = x_2\langle 1\rangle)}\ [\mathrm{rand}]$$

$$\frac{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \Rightarrow \Phi' \quad \models c_1' \sim_{(\varepsilon',\delta')} c_2'\colon \Phi' \Rightarrow \Phi}{\models c_1; c_1' \sim_{(\varepsilon+\varepsilon',\delta+\delta')} c_2; c_2'\colon \Psi \Rightarrow \Phi}\ [\mathrm{seq}] \qquad \frac{}{\models \mathtt{skip} \sim_{(0,0)} \mathtt{skip}\colon \Phi \Rightarrow \Phi}\ [\mathrm{skip}]$$

$$\frac{\Gamma \vdash^t b\colon \mathtt{bool} \quad \Gamma \vdash^t b\colon \mathtt{bool} \quad \Psi \Rightarrow b\langle 1\rangle = b'\langle 2\rangle \quad \models c_1 \sim_{(\varepsilon,\delta)} c_1'\colon \Psi \wedge b\langle 1\rangle \Rightarrow \Phi \quad \models c_2 \sim_{(\varepsilon,\delta)} c_2'\colon \Psi \wedge \neg b\langle 1\rangle \Rightarrow \Phi}{\models \mathtt{if}\ b\ \mathtt{then}\ c_1\ \mathtt{else}\ c_2 \sim_{(\varepsilon,\delta)} \mathtt{if}\ b'\ \mathtt{then}\ c_1'\ \mathtt{else}\ c_2'\colon \Psi \Rightarrow \Phi}\ [\mathrm{cond}]$$

$$\frac{\Gamma \vdash^t e\colon \mathtt{int} \quad \varepsilon = \sum_{k=0}^{n-1} \varepsilon_k \quad \delta = \sum_{k=0}^{n-1} \delta_k \quad \Theta \Rightarrow b_1\langle 1\rangle = b_2\langle 2\rangle \quad \Theta \wedge e\langle 1\rangle \geq n \Rightarrow \neg b_1\langle 1\rangle \quad \forall k\colon \mathtt{int}.\ \models c_1 \sim_{(\varepsilon_k,\delta_k)} c_2\colon \Theta \wedge e\langle 1\rangle = k \wedge e\langle 1\rangle \leq n \implies \Theta \wedge e\langle 1\rangle > k}{\models \mathtt{while}\ b\ \mathtt{do}\ c_1 \sim_{(\varepsilon,\delta)} \mathtt{while}\ b'\ \mathtt{do}\ c_2\colon\ \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq 0 \Rightarrow \Theta \wedge \neg b_1\langle 1\rangle}\ [\mathrm{while}]$$

$$\frac{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \wedge \Theta \Rightarrow \Phi \quad \models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \wedge \neg\Theta \Rightarrow \Phi}{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \Rightarrow \Phi}\ [\mathrm{case}]$$

$$\frac{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \Rightarrow \Phi \quad \Psi' \Rightarrow \Psi \quad \Phi \Rightarrow \Phi'}{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi' \Rightarrow \Phi'}\ [\mathrm{weak}] \qquad \frac{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \Rightarrow \Phi}{\models c_2 \sim_{(\varepsilon,\delta)} c_1\colon \Psi^{\Phi} \Rightarrow \Phi^{\Phi}}\ [\mathrm{op}]$$

The relational lifting $\overline{\mathcal{G}^{(\varepsilon,\delta)}}$ does not preserve every relation composition. However, it preserve the composition of relations if the relations are *measurable*, that is, the images and inverse images along them of measurable sets are also measurable (see

also [12, Section 3.3]). Generally speaking, it is difficult to check measurability of relations, hence the continuous apRHL is weak for dealing with relation compositions. However, we have the following two special cases:

- The *equality/diagonal* relation *on* any space is a measurable relation.
- Any relation between *discrete* spaces is automatically a measurable relation.

Hence, the following [comp] rule is an extension of the original [comp] rule in [2]:

$$\frac{\begin{array}{l}\Phi \text{ and } \Phi' \text{are measurable relations} \\ \models c_1 \sim_{(\varepsilon,\delta)} c_2 \colon \Psi \Rightarrow \Phi \quad \models c_2 \sim_{(\varepsilon',\delta')} c_3 \colon \Psi' \Rightarrow \Phi'\end{array}}{\models c_1 \sim_{(\varepsilon+\varepsilon',\min(\delta+e^{\varepsilon}\delta',\delta'+e^{\varepsilon'}\delta))} c_3 \colon \Psi \circ \Psi' \Rightarrow \Phi \circ \Phi'}\ [\text{comp}]$$

To define the [frame] rule in continuous apRHL, for any relation $\Theta$ on $[\![\Gamma]\!]$, we define the following relation $\mathrm{Range}(\Theta)$:

$$\begin{array}{l}\mathrm{Range}(\Theta) \\ = \left\{ (\nu_1,\nu_2) \;\middle|\; \exists A,B \in \Sigma_{[\![\Gamma]\!]}.(A \times B \subseteq \Theta \wedge \nu_1(A) = \nu_1([\![\Gamma]\!]) \wedge \nu_2(B) = \nu_2([\![\Gamma]\!])) \right\}.\end{array}$$

We define the [frame] rule with the construction $\mathrm{Range}(-)$:

$$\frac{\models c_1 \sim_{(\varepsilon,\delta)} c_2 \colon \Psi \Rightarrow \Phi \quad ([\![c_1]\!],[\![c_2]\!]) \colon \Theta \to \mathrm{Range}(\Theta)}{\models c_1 \sim_{(\varepsilon,\delta)} c_2 \colon \Psi \wedge \Theta \Rightarrow \Phi \wedge \Theta}\ [\text{frame}]$$

If $[\![\Gamma]\!]$ is countable discrete then the condition $(\nu_1,\nu_2) \in \mathrm{Range}(\Theta)$ is equivalent to $\mathrm{supp}(\nu_1) \times \mathrm{supp}(\nu_2) \subseteq \Theta$, and hence the above [frame] rule is an extension of the original [frame] rule in [2].

Note that if the $\sigma$-algebra of the space $[\![\tau]\!]$ contains all singleton subsets, and $\Theta$ does not restrict any variables in $FV(c_1) \cup FV(c_2)$ then $([\![c_1]\!],[\![c_2]\!]) \colon \Theta \to \mathrm{Range}(\Theta)$.

### *3.4 Soundness*

The soundness of the rules [assn] and [case] are given from the composition of arrows in **BRel**(**Meas**). The rules [skip] and [seq] are sound because $\overline{\mathcal{G}^{(\varepsilon,\delta)}}$ is an $M$-graded relational lifting of $\mathcal{G}$. The rules [weak] and [op] are sound because $\overline{\mathcal{G}^{(\varepsilon,\delta)}}$ is monotone with respect to the inclusion order of relations, and preserves opposites of relations. The soundness of [comp] is given from the measurability of the postconditions.

**Lemma 3.2** *The rule [rand] is sound.*

**Proof.** We assume that $x_1$ and $x_2$ are different variables, since the soundness is obvious if $x_1$ and $x_2$ are the same variables. We have $\Gamma = \Gamma', x_1 \colon \tau, x_2 \colon \tau$. Hence, we let $[\![\Gamma]\!] = [\![\Gamma']\!] \times [\![\tau]\!] \times [\![\tau]\!]$. From the symmetry of discussion, it suffices to show,

$$([\![\Gamma \vdash x_1 \xleftarrow{\$} d(e_1^1,\ldots,e_m^1)]\!],[\![\Gamma \vdash x_2 \xleftarrow{\$} d(e_1^2,\ldots,e_m^2)]\!]) \colon \Psi \to \mathcal{G}^{(\varepsilon,\delta)}(\Phi)$$

holds in **BRel**(**Meas**), where

$$\Phi = (x_1\langle 1\rangle = x_2\langle 2\rangle) = (\llbracket\Gamma\rrbracket, \llbracket\Gamma\rrbracket, \{\ (m_1, m_2) \mid \pi_{x_1}(m_1) = \pi_{x_2}(m_2)\ \}).$$

Let $(m_1, m_2) \in \Psi$ and $A \in \Sigma_{\llbracket\Gamma\rrbracket}$. We have $\Phi(A) = \llbracket\Gamma'\rrbracket \times \llbracket\tau\rrbracket \times A_{x_1}$, where $A_{x_1} = \{\ \pi_3(m) \mid m \in A\ \}$. Note that $A_{x_1} \in \Sigma_{\llbracket\tau\rrbracket}$, and hence $\Phi(A) \in \Sigma_{\llbracket\Gamma\rrbracket}$. We write $\nu_i = \llbracket d\rrbracket(\llbracket\Gamma \vdash^t e_1^i\rrbracket(m_i), \ldots, \llbracket\Gamma \vdash^t e_m^i\rrbracket(m_i))$ $(i = 1, 2)$, and we define $f, g\colon \llbracket\tau\rrbracket \to [0, 1]$ by $f = \chi_{(\rho_{(x_1\colon \tau,\Gamma)}(-,m_1))^{-1}(A)}$ and $g = \chi_{A_{x_1}}$. We then obtain from Fubini theorem:

$$\begin{aligned}
&\llbracket\Gamma \vdash x_1 \overset{\$}{\leftarrow} d(e_1^1, \ldots, e_m^1)\rrbracket(m_1)(A)\\
&= \mathcal{G}(\rho_{(x\colon \tau,\Gamma)}) \circ \mathrm{st}_{\llbracket\tau\rrbracket,\llbracket\Gamma\rrbracket} \circ \langle\nu_1, m_1\rangle(A) = \mathrm{st}^{\mathcal{G}}_{\llbracket\tau\rrbracket,\llbracket\Gamma\rrbracket}(\nu_1, m_1)(\rho_{(x_1\colon \tau,\Gamma)}{}^{-1}(A))\\
&= (\nu_1 \otimes \delta_{m_1})(\rho_{(x_1\colon \tau,\Gamma)}{}^{-1}(A)) = \int_{\llbracket\tau\rrbracket\times\llbracket\Gamma\rrbracket} \chi_{\rho_{(x_1\colon \tau,\Gamma)}{}^{-1}(A)}\ d(\nu_1 \otimes \delta_{m_1})\\
&= \int_{a\in\llbracket\tau\rrbracket} \left( \int_{\llbracket\Gamma\rrbracket} \chi_{\rho_{(x_1\colon \tau,\Gamma)}{}^{-1}(A)}(a, -)\ d(\delta_{m_1}) \right)\ d\nu_1 = \int_{\llbracket\tau\rrbracket} f\ d\nu_1\\
&\llbracket\Gamma \vdash x_2 \overset{\$}{\leftarrow} d(e_1^2, \ldots, e_m^2)\rrbracket(m_2)(\Phi(A))\\
&= \llbracket\Gamma \vdash x_2 \overset{\$}{\leftarrow} d(e_1^2, \ldots, e_m^2)\rrbracket(m_2)(\llbracket\Gamma'\rrbracket \times \llbracket\tau\rrbracket \times A_{x_1})\\
&= (\nu_2 \otimes \delta_{m_2})(\rho_{(x_2\colon \tau,\Gamma)}{}^{-1}(\llbracket\Gamma'\rrbracket \times \llbracket\tau\rrbracket \times A_{x_1})) = (\nu_2 \otimes \delta_{m_2})(A_{x_1}) = \int_{\llbracket\tau\rrbracket} g\ d\nu_2,
\end{aligned}$$

Since the pair $(f, g)$ is an arrow $\mathrm{Eq}_{\llbracket\tau\rrbracket} \to \leq$ in **BRel**(**Meas**), we obtain the followings:

$$\llbracket\Gamma \vdash x_1 \overset{\$}{\leftarrow} d(e_1^1, \ldots, e_m^1)\rrbracket(m_1)(A) \le e^{\varepsilon}\llbracket\Gamma \vdash x_2 \overset{\$}{\leftarrow} d(e_1^2, \ldots, e_m^2)\rrbracket(m_1)(A) + \delta.$$

Since $A$ is arbitrary, we conclude

$$(\llbracket\Gamma \vdash x_1 \overset{\$}{\leftarrow} d(e_1^1, \ldots, e_m^1)\rrbracket(m_1), \llbracket x_2 \overset{\$}{\leftarrow} d(e_1^2, \ldots, e_m^2)\rrbracket(m_2)) \in \mathcal{G}^{(\varepsilon,\delta)}(\Phi).$$

□

**Lemma 3.3** *The [cond] rule is sound.*

**Proof.** Let $(m_1, m_2) \in \Psi$. We have $\llbracket\Gamma \vdash b\rrbracket(m_1) = \llbracket\Gamma \vdash b'\rrbracket(m_2)$ from the preconditions of the [cond] rule. Since

$$\llbracket\Gamma \vdash \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\rrbracket = [\llbracket\Gamma \vdash c_1\rrbracket, \llbracket\Gamma \vdash c_2\rrbracket] \circ \cong_{\llbracket\Gamma\rrbracket} \circ \langle\llbracket\Gamma \vdash b\rrbracket, \mathrm{id}_{\llbracket\Gamma\rrbracket}\rangle,$$

we have the following two cases:

(i) If $\llbracket\Gamma \vdash b\rrbracket(m_1) = \iota_1(*)$ then we have

$$\begin{aligned}
\llbracket\Gamma \vdash \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\rrbracket(m_1) &= \llbracket\Gamma \vdash c_1\rrbracket(m_1),\\
\llbracket\Gamma \vdash \texttt{if}\ b'\ \texttt{then}\ c_1'\ \texttt{else}\ c_2'\rrbracket(m_2) &= \llbracket\Gamma \vdash c_1'\rrbracket(m_2)
\end{aligned}$$

Hence we have the following membership:

$$(\llbracket \Gamma \vdash \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \rrbracket(m_1), \llbracket \Gamma \vdash \texttt{if } b' \texttt{ then } c_1' \texttt{ else } c_2' \rrbracket(m_2)) \in \overline{\mathcal{G}^{(\varepsilon,\delta)}}\Phi.$$

(ii) If $\llbracket \Gamma \vdash b \rrbracket(m_1) = \iota_2(*)$ then the same membership holds as in the case (i).

□

**Lemma 3.4** *The [while] rule is sound.*

**Proof.** We write $c_i(n) = [\texttt{while } b_i \texttt{ do } c_i]_n$ $(i = 1, 2)$. We prove by induction on $n$:

$$\models c_1(n) \sim_{(\sum_{k=0}^{n-1}\varepsilon_k, \sum_{k=0}^{n-1}\delta_k)} c_2(n) \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq k \Rightarrow \Theta \wedge e\langle 1\rangle \geq n + k. \quad (1)$$

**case:** $n = 0$ We obtain $\models \texttt{null} \sim_{(0,0)} \texttt{null} \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq k \Rightarrow \emptyset$ since $\llbracket \Gamma \vdash \texttt{null} \rrbracket$ is the null measure over $\llbracket \Gamma \rrbracket$. We recall that the following equality:

$$c_i(0) = [\texttt{while } b_i \texttt{ do } c_i]_0 = \texttt{if } b_i \texttt{ then null else skip},$$

We obtain from the equality (1) by applying [skip], [cond], and [weak].

**case:** $n = m + 1$ From the precondition of [while] and the soundness of [case],

$$\models c_1 \sim_{(\varepsilon_m, \delta_m)} c_2 \colon \Theta \wedge (e\langle 1\rangle = k) \implies (e\langle 1\rangle > k).$$

By the induction hypothesis,

$$\models c_1(m) \sim_{(\sum_{k=0}^{m-1}\varepsilon_k, \sum_{k=0}^{m-1}\delta_k)} c_2(m) \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq k \Rightarrow \Theta \wedge e\langle 1\rangle \geq m + k.$$

From the soundness of the [seq] rule, we obtain

$$\models c_1; c_1(m) \sim_{(\sum_{k=0}^{m}\varepsilon_k, \sum_{k=0}^{m}\delta_k)} c_2; c_2(m) \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq k \Rightarrow \Theta \wedge e\langle 1\rangle \geq m+1+k.$$

From the soundness of [weak], [cond], and [skip] we conclude (1).

Next, it is obvious that $\Theta \Rightarrow b_1\langle 1\rangle = b_2\langle 2\rangle$ implies

$$\models \texttt{while } b_1 \texttt{ do } c_1 \sim_{(0,0)} \texttt{while } b_2 \texttt{ do } c_2 \colon \Theta \wedge \neg b_1\langle 1\rangle \Rightarrow \Theta \wedge \neg b_1\langle 1\rangle. \quad (2)$$

We write $\varepsilon = \sum_{k=0}^{m}\varepsilon_k$ and $\delta = \sum_{k=0}^{m}\delta_k$. From (1) and (2), we obtain by applying [cond] and [seq],

$$\models c_1(n); \texttt{while } b_1 \texttt{ do } c_1 \sim_{(\varepsilon,\delta)} c_2(n); \texttt{while } b_2 \texttt{ do } c_2 \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq 0 \Rightarrow \Theta \wedge \neg b_1\langle 1\rangle.$$

We obtain $\llbracket \Gamma \vdash c_i(n); \texttt{while } b_i \texttt{ do } c_i \rrbracket = \llbracket \Gamma \vdash \texttt{while } b_i \texttt{ do } c_i \rrbracket$ $(i = 1, 2)$ because the interpretations $\llbracket \Gamma \vdash \texttt{while } b_i \texttt{ do } c_i \rrbracket$ is the least upper bound of $\{\llbracket \Gamma \vdash c_i(n) \rrbracket\}_n$ with respect to the $\omega\mathbf{CPO}_\perp$ structure (see section 1.2). Hence we conclude,

$$\models \texttt{while } b_1 \texttt{ do } c_1 \sim_{(\varepsilon,\delta)} \texttt{while } b_2 \texttt{ do } c_2 \colon \Theta \wedge b_1\langle 1\rangle \wedge e\langle 1\rangle \geq 0 \Rightarrow \Theta \wedge \neg b_1\langle 1\rangle.$$

□

**Lemma 3.5** *The rule [frame] is sound.*

**Proof.** Let $(m_1, m_2) \in \Psi \wedge \Theta$, $\nu_1 = [\![\Gamma \vdash c_1]\!](m_1)$, and $\nu_2 = [\![\Gamma \vdash c_2]\!](m_2)$. Since $(\nu_1, \nu_2) \in \mathrm{Range}(\Theta)$, there exist $A', B' \in \Sigma_{[\![\Gamma]\!]}$ such that $A' \times B' \subseteq \Theta$, and $\nu_1(C) = \nu_1(C \wedge A')$ and $\nu_2(D) = \nu_2(D \wedge B')$ for all $C, D \in \Sigma_{[\![\Gamma]\!]}$. Suppose that $A, B \in \Sigma_{[\![\Gamma]\!]}$ satisfy $(\Phi \wedge \Theta)(A) \subseteq B$. Since $A' \times B' \subseteq \Theta$, we have $(\Phi \wedge (A' \times B'))(A) \subseteq B$. This implies $\Phi(A \wedge A') \wedge B' \subseteq B$. Thus, $\Phi(A \wedge A') \subseteq B + ([\![\Gamma]\!] \setminus (B \vee B'))$. Therefore

$$\begin{aligned}\nu_1(A) &= \nu_1(A \wedge A') \leq e^{\varepsilon}\nu_2(B + ([\![\Gamma]\!] \setminus (B \vee B')) + \delta \\ &= e^{\varepsilon}\nu_2((B + ([\![\Gamma]\!] \setminus (B \vee B')) \wedge B') + \delta \leq e^{\varepsilon}\nu_2(B \wedge B') + \delta \leq e^{\varepsilon}\nu_2(B) + \delta.\end{aligned}$$

Hence, $(\nu_1, \nu_2) \in \mathcal{G}^{(\varepsilon,\delta)}(\Theta \wedge \Phi)$. Similarly, we obtain $(\nu_1, \nu_2) \in (\mathcal{G}^{(\varepsilon,\delta)}(\Theta \wedge \Phi)^{\Phi})^{\Phi}$.□

# 4 Differentially Private Mechanisms

In this section, we give a generic method to construct the rules for random samplings, and by instantiating the method we show the soundness of the proof rules in prior researches: [Lap] for Laplacian mechanism [7], [Exp] for Exponential mechanism [15], [Gauss] for Gaussian mechanism [8, Theorem 3.22, Theorem A.1], and [Cauchy] for the mechanism by Cauchy distributions [16].

Let $f\colon X \times Y \to \mathbb{R}$ be a positive measurable function, and $\nu$ be a measure over $Y$. We define the following function $f_a\colon \Sigma_Y \to [0,1]$ by the following normalisation:

$$f_a(B) = \frac{\int_B f(a,-)\ d\nu}{\int_Y f(a,-)\ d\nu}.$$

If the function is not 'almost everywhere zero' and Lebesgue integrable, that is, $0 < \int_Y f(a,-)\ d\nu < \infty$ then the above $f_a(-)$ is a *probability measure*.

**Proposition 4.1** *Let $f\colon X \times Y \to \mathbb{R}$ be a positive measurable function, and $\nu$ be a measure over $Y$. For all $a, a' \in X$, $0 \leq \varepsilon, \varepsilon'$, $0 \leq \delta$, and $Z \in \Sigma_Y$ (window set), if the following three conditions hold then $(f_a, f_{a'}) \in \mathcal{G}^{(\varepsilon+\varepsilon',\delta)}(Y, Y, \mathrm{Eq}_Y)$:*

(i) $0 < \frac{1}{e^{\varepsilon'}} \int_Y f(a',-)\ d\nu \leq \int_Y f(a,-)\ d\nu < \infty$,

(ii) $\forall b \in Z.f(a,b) \leq e^{\varepsilon} f(a',b)$, *and*

(iii) $f_a(Y \setminus Z) \leq \delta$.

**Proof.** From the three conditions of this proposition, for each $B \in \Sigma_Y$, we obtain,

$$f_a(B) = \frac{\int_B f(a,-)\ d\nu}{\int_Y f(a,-)\ d\nu} \leq \frac{e^{\varepsilon}\int_{B\cap Z} f(a',-)\ d\nu}{\frac{1}{e^{\varepsilon'}}\int_Y f(a',-)\ d\nu} + \delta \leq e^{(\varepsilon+\varepsilon')} f_{a'}(B) + \delta$$

□

This proposition is an extension of [2, Lemma 7], and plays the central role in the construction of *sound* proof rules of (continuous) apRHL on random samplings.

**Laplacian mechanism [7].**

We give the function $f\colon \mathbb{R}\times\mathbb{R}\to\mathbb{R}$ by $f(a,b)=\frac{2}{\sigma}\exp(\frac{-|b-a|}{\sigma})$, where $\sigma>0$ is the variance of Laplacian mechanism. We introduce the probabilistic operation $\mathtt{Lap}_\sigma\colon \mathtt{real}\to\mathtt{real}$ with $[\![\mathtt{Lap}_\sigma]\!]=f_{(-)}$, whose measurability is shown from the continuity of the mapping $a\mapsto\int_\alpha^\beta f(a,x)dx$ $(\alpha,\beta\in\mathbb{R})$.

We show $(f_{(-)},f_{(-)})\colon \{\,(a,a')\mid |a-a'|<r\,\}\to\overline{\mathcal{G}^{(\frac{r}{\sigma},0)}}\mathrm{Eq}_{\mathbb{R}}$ by instantiating Proposition 4.1 as follows: If $|a-a'|<r$ then $\varepsilon=r/\sigma$, $\varepsilon'=0$, $\delta=0$, the given function $f$, the Lebesgue measure $\nu$ over $\mathbb{R}$, and $Z=\mathbb{R}$ satisfy the conditions (i)–(iii):

(i) Since the function $f(a,-)$ is the density function of Laplacian distribution, and hence $\int_{\mathbb{R}} f(a,-)d\nu=\int_{\mathbb{R}} f(a',-)d\nu=1$.

(ii) From the triangle inequality $|b-a'|\le|a-a'|+|b-a|$, we have

$$\frac{f(a,b)}{f(a',b)}=\exp\left(\frac{|b-a'|-|b-a|}{\sigma}\right)\le\exp\left(\frac{|a-a'|}{\sigma}\right)\le\exp\left(\frac{r}{\sigma}\right).$$

This implies $f(a,b)\le e^{\varepsilon}f(a',b)$.

(iii) It is obvious since $\mathbb{R}\setminus Z=\emptyset$.

Hence, $(f_{(-)},f_{(-)})\colon \{\,(a,a')\mid |a-a'|<r\,\}\to\overline{\mathcal{G}^{(\frac{r}{\sigma},0)}}\mathrm{Eq}_{\mathbb{R}}$ since $\{\,(a,a')\mid |a-a'|<r\,\}$ and $\mathrm{Eq}_{\mathbb{R}}$ are symmetric. From the [rand] rule, the following proof rule is sound:

$$\frac{\Gamma\vdash^t e_1\colon\mathtt{real}\quad\Gamma\vdash^t e_2\colon\mathtt{real}\quad m_1\Psi m_2\Rightarrow|[\![e_1]\!]m_1-[\![e_2]\!]m_2|<r}{\models x\overset{\$}{\leftarrow}\mathtt{Lap}_\sigma(e_1)\sim_{(\frac{r}{\sigma},0)}y\overset{\$}{\leftarrow}\mathtt{Lap}_\sigma(e_2)\colon\Psi\Rightarrow x\langle1\rangle=y\langle2\rangle}\ [\mathrm{Lap}].$$

**Exponential mechanism [15, Modified].**

Let $D$ be the discrete Euclidean space $\mathbb{Z}^n$, and $(R,\nu)$ be a (positive) measure space. Let $q\colon D\times R\to\mathbb{R}$ be a measurable function such that $\sup_{b\in R}|q(a,b)-q(a',b)|\le c\cdot||a-a'||_1$ for some $c>0$. Suppose $0<\int_R\exp(\gamma q(a,-))\,d\nu<\infty$ for any $a\in D$. We give the function $f\colon D\times R\to\mathbb{R}$ by $f(a,b)=\exp(\gamma q(a,b))$, where $\gamma>0$ is a constant. We add the value types $\mathtt{D}$ and $\mathtt{R}$ with $[\![\mathtt{D}]\!]=D$ and $[\![\mathtt{R}]\!]=R$ to pWHILE, and introduce the probabilistic operation $\mathtt{Exp}_{\langle q,\nu,\varepsilon\rangle}\colon\mathtt{D}\to\mathtt{R}$ with $[\![\mathtt{Exp}_{\langle q,\nu,\varepsilon\rangle}]\!]=f_{(-)}$.

We show $(f_{(-)},f_{(-)})\colon \{\,(a,a')\mid ||a-a'||_1<r\,\}\to\overline{\mathcal{G}^{(2\gamma rc,0)}}\mathrm{Eq}_R$ by instantiating Proposition 4.1 as follows: Suppose $||a-a'||_1<r$. Then $\varepsilon=\varepsilon'=\gamma cr$, $\delta=0$, the given function $f$, the given measure $\nu$, and $Z=R$ satisfy the conditions (i)–(iii):

(i) whenever $||a-a'||_1<r$, we obtain,

$$\frac{f(a,b)}{f(a',b)}\le\exp\left(\gamma|q(a,b)-q(a',b)|\right)\le\exp\left(\gamma c||a-a'||_1\right)\le\exp\left(\gamma cr\right).$$

This implies $\int_{\mathbb{R}} f(a,-)d\nu\le e^{\varepsilon}\int_{\mathbb{R}} f(a',-)d\nu$.

(ii) In the same way as (i), we have $f(a',b)\le e^{\varepsilon'}f(a,b)$.

(iii) Obvious.

From the [rand] rule, the following proof rule is sound:

$$\frac{\Gamma \vdash^t e_1 : \mathtt{D} \quad \Gamma \vdash^t e_2 : \mathtt{D} \quad m_1 \Psi m_2 \Rightarrow ||[\![e_1]\!]m_1 - [\![e_2]\!]m_2||_1 < r}{\models x \xleftarrow{\$} \mathtt{Exp}_{\langle q,\nu,\varepsilon\rangle}(e_1) \sim_{(2\gamma cr,0)} y \xleftarrow{\$} \mathtt{Exp}_{\langle q,\nu,\varepsilon\rangle}(e_2) : \Psi \Rightarrow x\langle 1\rangle = y\langle 2\rangle}\ [\mathrm{Exp}]\cdot$$

**Gaussian mechanism [8, Theorem 3.22, Theorem A.1].**

We give the function $f : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ by $f(a,b) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{(b-a)^2}{2\sigma^2})$, where $\sigma > 0$ is the variance of Gaussian mechanism. We introduce the probabilistic operation $\mathtt{Gauss}_\sigma : \mathtt{real} \to \mathtt{real}$ with $[\![\mathtt{Gauss}_\sigma]\!] = f_{(-)}$, whose continuity is easily proved.

We obtain $(f_{(-)}, f_{(-)}) : \{\, (a,a') \mid |a-a'| < r \,\} \to \overline{\mathcal{G}^{(\varepsilon,\delta)}}\mathrm{Eq}_{\mathbb{R}}$ by instantiating Proposition 4.1 as follows: If $|a-a'| < r$, $0 < \varepsilon < 1$, and $\varepsilon' = 0$ hold, and there is $(3/2) < c$ such that $2\log(1.25/\delta) \le c^2$ and $(cr/\varepsilon) \le \sigma$, then the parameters $\varepsilon$, $\varepsilon'$, and $\delta$, the given function $f$, and the Lebesgue measure $\nu$ over $\mathbb{R}$ satisfy the conditions (i)–(iii) when $Z = \{\, b \mid |b - (a+a')/2| \le (\sigma^2\varepsilon/r) \,\}$ (see [8, Theorem A.1]). From the [rand] rule, the following proof rule is sound:

$$\frac{\begin{array}{l}\exists c > \frac{3}{2}.\ (2\log(\frac{1.25}{\delta}) < c^2 \ \wedge\ \frac{cr}{\varepsilon} \le \sigma) \quad 0 < \varepsilon < 1 \\ \Gamma \vdash^t e_1 : \mathtt{real} \quad \Gamma \vdash^t e_2 : \mathtt{real} \quad m_1 \Psi m_2 \Rightarrow |[\![e_1]\!]m_1 - [\![e_2]\!]m_2| < r\end{array}}{\models x \xleftarrow{\$} \mathtt{Gauss}_\sigma(e_1) \sim_{(\varepsilon,\delta)} y \xleftarrow{\$} \mathtt{Gauss}_\sigma(e_2) : \Psi \Rightarrow x\langle 1\rangle = y\langle 2\rangle}\ [\mathrm{Gauss}]\cdot$$

We can relax the above conditions for $c$ to $((1+\sqrt{3})/2) < c$ and $2\log(0.66/\delta) < c^2$ by changing the window set $Z$.

**Lemma 4.2 ([8, Theorem A.1], Relaxed)** *Suppose $|a-a'| < r$. Assume that $((1+\sqrt{3})/2) < c$, $0 < \varepsilon < 1$, and $0 < \delta < 1$ satisfy $2\log(0.66/\delta) < c^2$ and $(cr/\varepsilon) \le \sigma$. Then $\varepsilon$, $\varepsilon' = 0$, and $\delta$, the function $f$, and the Lebesgue measure $\nu$ over $\mathbb{R}$ satisfy the conditions (i)–(iii) of Proposition 4.1 when $Z = \{\, b \mid b \le (a+a')/2 + (\sigma^2\varepsilon/r) \,\}$ if $a \le a'$ and $Z = \{\, b \mid b \ge (a+a')/2 - (\sigma^2\varepsilon/r) \,\}$ if $a' \le a$.*

**Proof.** We assume $a' \le a$. In the case of $a' > a$, we prove in the similar way.

(i) For each $a \in \mathbb{R}$ the function $f(a,-)$ is the density function of Gaussian distribution, and hence $\int_{\mathbb{R}} f(a,-)d\nu = \int_{\mathbb{R}} f(a',-)d\nu = 1$.

(ii) We have $Z = \{\, b \mid b \le (a+a')/2 + (\sigma^2\varepsilon/r) \,\}$. Take an arbitrary $b \in Z$. We then calculate as follows:

$$\begin{aligned}\frac{f(a,b)}{f(a',b)} &= \exp\left(\frac{(b-a')^2 - (b-a)^2}{2\sigma^2}\right) = \exp\left(\frac{1}{\sigma^2}(a-a')(b - \frac{a+a'}{2})\right) \\ &\le \exp\left(\frac{r}{\sigma^2}(b - \frac{a+a'}{2})\right) \le \exp\left(\frac{r}{\sigma^2}\frac{\sigma^2\varepsilon}{r}\right) \le e^\varepsilon.\end{aligned}$$

This implies $\forall b \in Z.f(a,b) \le e^\varepsilon f(a',b)$.

(iii) Let $H = \frac{a'-a}{2\sigma} + \frac{\sigma\varepsilon}{r}$. Since $((1+\sqrt{3})/2) < c$, $-r < a'-a$, and $\frac{cr}{\varepsilon} \leq \sigma$, we have $1 < c - \frac{1}{2c} < c - \frac{\varepsilon}{2c} < H$. Thus $0 < \log(H)$. We have $2\log(\frac{1}{\delta}\sqrt{\frac{e}{2\pi}}) \leq 2\log(0.66/\delta) < c^2$. Thus $2\log(\frac{1}{\delta\sqrt{2\pi}}) < c^2 - 1$. We obtain $2\log(\frac{1}{\delta\sqrt{2\pi}}) < c^2 - 1 < H^2$ from $c - \frac{1}{2c} < c - \frac{\varepsilon}{2c} < H$. Therefore, we conclude $\log(\frac{1}{\delta\sqrt{2\pi}}) < \log(H) + H^2/2$.

Let $H' = \frac{a+a'}{2} + \frac{\sigma^2\varepsilon}{r}$. We have $f_a(\mathbb{R} \setminus Z) \leq \delta$ from the following calculation:

$$\begin{aligned}
&\int_{\mathbb{R}\setminus Z} \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-a)^2}{2\sigma^2}\right)\, d\nu \\
&= \frac{1}{\sigma\sqrt{2\pi}} \int_{H'}^{\infty} \exp\left(-\frac{(x-a)^2}{2\sigma^2}\right)\, dx = \frac{1}{\sqrt{2\pi}} \int_{H}^{\infty} \exp\left(-\frac{b^2}{2}\right)\, db \\
&\leq \frac{1}{\sqrt{2\pi}} \int_{H}^{\infty} \frac{b}{H} \exp\left(-\frac{b^2}{2}\right)\, db \leq \frac{1}{\sqrt{2\pi}H} \exp\left(-\frac{H^2}{2}\right) \leq \delta.
\end{aligned}$$

□

**Mechanism of Cauchy distributions [16]**

We give the function $f\colon \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ by $f(a,b) = \frac{\rho}{\pi((a-b)^2+\rho^2)}$. We introduce the probabilistic operation $\texttt{Cauchy}_\rho\colon \texttt{real} \to \texttt{real}$ with $[\![\texttt{Cauchy}_\rho(e)]\!]^\Gamma m = f_{(-)}$, whose continuity is easily proved.

Let $\varepsilon = \log\left(1 + \frac{r^2 + r\sqrt{r^2+4\rho^2}}{2\rho^2}\right)$. We obtain $(f_{(-)}, f_{(-)})\colon \{\, (a,a') \mid |a-a'| < r \,\} \to \overline{\mathcal{G}^{(\varepsilon,0)}}\mathrm{Eq}_{\mathbb{R}}$ by instantiating Proposition 4.1 as follows: If $|a-a'| < r$ then the parameters satisfy the conditions (i)–(iii): the given $\varepsilon$, $\varepsilon' = 0$, $\delta = 0$, the Lebesgue measure $\nu$ over $\mathbb{R}$, and $Z = \mathbb{R}$.

From the [rand] rule, we obtain the following rule:

$$\frac{\Gamma \vdash^t e\colon \texttt{real} \quad m_1 \Psi m_2 \Rightarrow |[\![e_1]\!]m_1 - [\![e_2]\!]m_2| < r}{\models x \xleftarrow{\$} \texttt{Cauchy}_\rho(e_1) \sim_{(\varepsilon,0)} y \xleftarrow{\$} \texttt{Cauchy}_\rho(e_1)\colon \Psi \Rightarrow (\pi_x \times \pi_y)^{-1}(\mathrm{Eq}_{\mathbb{R}})}\ [\text{Cauchy}]$$

## 5 Example: The Above Threshold Algorithm

Barthe, Gaboardi, Grégoire, Hsu, and Strub extended the logic apRHL to the logic apRHL+ with new proof rules to describe the *sparse vector technique* (see also [8, Section 3.6]). They gave a formal proof of the differential privacy of *above threshold algorithm* in [1].

In this section, we demonstrate that the above threshold algorithm with *real-valued queries* is proved with *almost the same proof* as in [1]. The new proof rules of apRHL+ are still sound in the framework of the continuous apRHL.

We consider the following algorithm `AboveT`:

We recall the setting of this algorithm. This algorithm has two fixed parameters: the threshold $t\colon \texttt{real}$ and the set $Q\colon \texttt{queries}$ of queries where $|Q|\colon \texttt{int}$ is the number of $Q$. The input variable is $d\colon \texttt{int}$, and the output variable is $r\colon \texttt{int}$. We prepare the new value types `queries` and `data` with $[\![\texttt{data}]\!] = \mathbb{R}^N$ and `queries` =

**Algorithm 1** The Above Threshold Algorithm ([1], Modified)

```
1: AboveT(T: real, Q: queries, d: data)
2:     j ← 1; r ← |Q| + 1; T ←$ Lap_{ε/2}(t);
3:     while j < |Q| do
4:         S ←$ Lap_{ε/4}(eval(Q, i, d));
5:         if T ≤ S ∧ r = |Q| + 1 then
6:             r ← j;
7:         j ← j + 1
```

`int` (alias), and the typings $j\colon \texttt{int}$, $T\colon \texttt{real}$, and $S\colon \texttt{real}$. We assume that an operation $\texttt{eval}\colon (\texttt{queries}, \texttt{int}, \texttt{data}) \to \texttt{real}$ is given for evaluating $i$-th query in $Q$ for the input $d$. We require $[\![\texttt{eval}]\!]$ to be 1-*sensitivity* for the data $d$, that is, $||d - d'||_1 \leq 1 \Rightarrow |[\![\texttt{eval}]\!](Q, i, d) - [\![\texttt{eval}]\!](Q, i, d')| \leq 1$.

The differential privacy of `Above` is characterised as follows:

$$\models \texttt{AboveT} \sim_{\exp(\varepsilon),0} \texttt{AboveT}\colon ||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \Rightarrow r\langle 1\rangle = r\langle 2\rangle.$$

The following rules in apRHL+ are sound in the framework of continuous apRHL:

$$\frac{\forall i\colon \texttt{int}.\ \models c_1 \sim_{(\varepsilon,\delta_i)} c_2\colon \Psi \Rightarrow (x\langle 1\rangle = i \Rightarrow x\langle 2\rangle = i) \quad \sum_{i\colon \texttt{int}} [\![\delta_i]\!] = \delta}{\models c_1 \sim_{(\varepsilon,\delta)} c_2\colon \Psi \Rightarrow x\langle 1\rangle = x\langle 2\rangle}\ [\text{Forall-Eq}]$$

$$\frac{\Gamma \vdash^t e_1\colon \texttt{real} \quad \Gamma \vdash^t e_2\colon \texttt{real} \quad m_1 \Psi m_2 \Rightarrow |[\![e_1]\!]m_1 + r' - [\![e_2]\!]m_2| < r}{\models x \xleftarrow{\$} \texttt{Lap}_\sigma(e_1) \sim_{(\frac{r}{\sigma},0)} y \xleftarrow{\$} \texttt{Lap}_\sigma(e_2)\colon \Psi \Rightarrow x\langle 1\rangle + r' = y\langle 2\rangle}\ [\text{LapGen}]$$

$$\frac{\Gamma \vdash^t e_1\colon \texttt{real} \quad \Gamma \vdash^t e_2\colon \texttt{real} \qquad x \notin FV(e_1) \quad y \notin FV(e_2)}{\models x \xleftarrow{\$} \texttt{Lap}_\sigma(e_1) \sim_{(0,0)} y \xleftarrow{\$} \texttt{Lap}_\sigma(e_2)\colon \Psi \Rightarrow x\langle 1\rangle - y\langle 2\rangle = e_1\langle 1\rangle - e_2\langle 2\rangle}\ [\text{LapNull}]$$

Hence we extend the continuous apRHL by adding these rules, and therefore we construct a formal proof almost the same proof as in [1] in the extended continuous apRHL.

The soundness of the rule [Forall-Eq] is proved from the following lemma:

**Lemma 5.1 ([1, Proposition 6], Modified)** *If $x\colon \tau \in \Gamma$ and the space $[\![\tau]\!]$ is countable and discrete then*

$$\bigcap_{i \in [\![\tau]\!]} \mathcal{G}^{(\varepsilon,\delta_i)}(x\langle 1\rangle = i \Rightarrow x\langle 2\rangle = i) \subseteq \mathcal{G}^{(\varepsilon,\sum_{i\in[\![\tau]\!]}\delta_i)}(x\langle 1\rangle = x\langle 2\rangle).$$

**Proof.** Let $[\![\Gamma, x\colon \tau]\!] = [\![\tau]\!] \times [\![\Gamma]\!]$. Suppose $(\nu_1, \nu_2) \in \bigcap_{i\in[\![\tau]\!]} \mathcal{G}^{(\gamma,\delta_i)}(x\langle 1\rangle = i \Rightarrow x\langle 2\rangle = i)$. Take an arbitrary $A \in \Sigma_{[\![\Gamma, x\colon \tau]\!]}$. Since $[\![\tau]\!]$ is countable and discrete, we decompose $A = \sum_{i\in[\![\tau]\!]}(\{i\} \times A_i)$. We may assume $A_i \neq \emptyset$ because $\{i\} \times \emptyset = \emptyset$. Since $(x\langle 1\rangle = i \Rightarrow x\langle 2\rangle = i)(\{i\} \times A_i) = \{i\} \times [\![\Gamma]\!]$, we obtain $\nu_1(\{i\} \times A_i) \leq e^\varepsilon \nu_2(\{i\} \times [\![\Gamma]\!]) + \delta_i$ for each $i \in [\![\tau]\!]$. By summing them up, we obtain $\nu_1(A) \leq e^\varepsilon \nu_2((x\langle 1\rangle = x\langle 2\rangle)(A)) + \sum_{i\in[\![\tau]\!]} \delta_i$. □

The soundness of the rule [LapGen] is proved from the rules [Lap] and [assn] and the semantically equivalence $[\![x \xleftarrow{\$} \mathtt{Lap}_\sigma(e + r'); x \leftarrow x - r']\!] = [\![x \xleftarrow{\$} \mathtt{Lap}_\sigma(e)]\!]$. The soundness of [LapNull] is proved by using the [LapGen] and [Frame] rules.

**Formal Proof**

We now demonstrate that the $(\varepsilon, 0)$-differential privacy of algorithm `AboveT` is proved with almost the same proof as in [1].

From the [Forall-Eq] rule with variable $r$, it suffices to prove for all integer $i$,

$$\models \mathtt{AboveT} \sim_{(\varepsilon,0)} \mathtt{AboveT} \colon ||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \Rightarrow (r\langle 1\rangle = i \Rightarrow r\langle 2\rangle = i).$$

We denote by $c_0$ the sub-command consisting of the initialisation line 2 of `AboveT`. From the rules [assn], [LapGen] rule with $r = r' = 1$, and $\sigma = 2/\varepsilon$, [seq], and [frame] we obtain

$$\models c_0 \sim_{(\varepsilon/2,0)} c_0 \colon ||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \Rightarrow ||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \wedge \Psi.$$

where

$$\Psi = T\langle 1\rangle + 1 = T\langle 2\rangle \wedge j\langle 1\rangle = j\langle 2\rangle \wedge j\langle 1\rangle = 1 \wedge r\langle 1\rangle = r\langle 2\rangle \wedge r\langle 1\rangle = |Q| + 1.$$

We denote by $c_1$ and $c_2$ the main loop and the body of the main loop respectively (i.e. $c_1 = \mathtt{while}\ (j < |Q|)\ \mathtt{do}\ c_2$). We aim to prove the following judgement by using the [while] rule:

$$\models c_1 \sim_{(\varepsilon/2,0)} c_1 \colon (||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \wedge \Psi) \Rightarrow (r\langle 1\rangle = i \Rightarrow r\langle 2\rangle = i).$$

To prove this, it suffices to show the following cases for the loop body $c_2$:

(i) If $k < i$ then $\models c_2 \sim_{(0,0)} c_2 \colon (\Theta \wedge j\langle 1\rangle = k) \Rightarrow (\Theta \wedge j\langle 1\rangle > k)$

(ii) If $k = i$ then $\models c_2 \sim_{(\varepsilon/2,0)} c_2 \colon (\Theta \wedge j\langle 1\rangle = k) \Rightarrow (\Theta \wedge j\langle 1\rangle > k)$

(iii) If $k > i$ then $\models c_2 \sim_{(0,0)} c_2 \colon (\Theta \wedge j\langle 1\rangle = k) \Rightarrow (\Theta \wedge j\langle 1\rangle > k)$

Here, we provide the following *loop invariant* as follows:

$$\begin{aligned}\Theta =& (j\langle 1\rangle < i \Rightarrow ((r\langle 1\rangle = |Q| + 1 \Rightarrow r\langle 2\rangle = |Q| + 1) \wedge (r\langle 1\rangle = |Q| + 1 \vee r\langle 1\rangle < i))) \\ & \wedge (j\langle 1\rangle \geq i \Rightarrow (r\langle 1\rangle = i \Rightarrow r\langle 2\rangle = i)) \\ & \wedge ||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \wedge T\langle 1\rangle + 1 = T\langle 2\rangle \wedge j\langle 1\rangle = j\langle 2\rangle\end{aligned}$$

The judgement in the case (i) is proved from the rules [seq], [assn], [cond], and [frame] and the following fact obtained from the [LapNull] rule:

$$\begin{aligned}\models & S \xleftarrow{\$} \mathtt{Lap}_{\varepsilon/4}(\mathtt{eval}(Q, i, d)) \sim_{(0,0)} S \xleftarrow{\$} \mathtt{Lap}_{\varepsilon/4}(\mathtt{eval}(Q, i, d)) \colon \\ & (||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1) \wedge (T\langle 1\rangle + 1 = T\langle 2\rangle) \Rightarrow ((S\langle 1\rangle < T\langle 1\rangle) \Rightarrow (S\langle 2\rangle < T\langle 2\rangle)).\end{aligned}$$

The case (ii) is proved from the rules [seq], [assn], [cond], and [frame] and the following fact obtained from the [LapGen] rule:

$$\models S \xleftarrow{\$} \mathtt{Lap}_{\varepsilon/4}(\mathtt{eval}(Q,i,d)) \sim_{(\varepsilon/2,0)} S \xleftarrow{\$} \mathtt{Lap}_{\varepsilon/4}(\mathtt{eval}(Q,i,d)) :$$
$$(||d\langle 1\rangle - d\langle 2\rangle||_1 \leq 1 \wedge T\langle 1\rangle + 1 = T\langle 2\rangle) \Rightarrow (S\langle 1\rangle + 1 = S\langle 2\rangle \wedge T\langle 1\rangle + 1 = T\langle 2\rangle).$$

The case (iii) is proved in the similar way as (i).

## Acknowledgement

The author thanks Shin-ya Katsumata for many valuable comments and stimulating discussions, Marco Gaboardi for helpful suggestions and the introduction of his preprint of [1] in arXiv, Gilles Barthe, Masahito Hasegawa, Naohiko Hoshino, Takeo Uramoto and anonymous reviewers of MFPS for advices that contributed to improve the writing of this paper.

## References

[1] Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Jastin Hsu, and Pierre-Yves Strub. Proving Differential Privacy via Probabilistic Couplings. In *Proceedings of Thirty-First Annual ACM/IEEE Symposium on LOGIC IN COMPUTER SCIENCE (LICS)*, to appear.

[2] Gilles Barthe, Boris Köpf, Federico Olmedo, and Santiago Zanella-Béguelin. Probabilistic relational reasoning for differential privacy. In *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '12, pages 97–110, New York, NY, USA, 2012. ACM.

[3] Gilles Barthe and Federico Olmedo. Beyond differential privacy: Composition theorems and relational logic for f-divergences between probabilistic programs. In F. Fomin, R. Freivalds, M. Kwiatkowska, and D. Peleg, editors, *Automata, Languages, and Programming*, volume 7966 of *Lecture Notes in Computer Science*, pages 49–60. Springer Berlin Heidelberg, 2013.

[4] Nick Benton. Simple relational correctness proofs for static analyses and program transformations. In *Proceedings of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '04)*, number MSR-TR-2005-26, page 43. ACM, January 2004.

[5] Daniel Brown and Riccardo Pucella. Categories of timed stochastic relations. *Electronic Notes in Theoretical Computer Science*, 249:193 – 217, 2009. Proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009).

[6] E.P de Vink and J.J.M.M Rutten. Bisimulation for probabilistic transition systems: a coalgebraic approach. *Theoretical Computer Science*, 221(1 - 2):271 – 293, 1999.

[7] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer Berlin Heidelberg, 2006.

[8] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3-4):211–407, 2013.

[9] Michèle Giry. A categorical approach to probability theory. In B. Banaschewski, editor, *Categorical Aspects of Topology and Analysis*, volume 915 of *Lecture Notes in Mathematics*, pages 68–85. Springer Berlin Heidelberg, 1982.

[10] Bart Jacobs and Jesse Hughes. Simulations in coalgebra. *Electronic Notes in Theoretical Computer Science*, 82(1):128–149, 2003. CMCS'03, Coalgebraic Methods in Computer Science (Satellite Event for ETAPS 2003).

[11] Shin-ya Katsumata. Parametric effect monads and semantics of effect systems. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '14, pages 633–645, New York, NY, USA, 2014. ACM.

[12] Shin-ya Katsumata and Tetsuya Sato. Codensity Liftings of Monads. In Lawrence S. Moss and Pawel Sobocinski, editors, *6th Conference on Algebra and Coalgebra in Computer Science (CALCO 2015)*, volume 35 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 156–170, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[13] Kim Guldstrand Larsen and Arne Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991.

[14] Frank McSherry. Privacy integrated queries. Association for Computing Machinery, Inc., June 2009.

[15] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 94–103, Washington, DC, USA, 2007. IEEE Computer Society.

[16] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 75–84, New York, NY, USA, 2007. ACM.

[17] Federico Olmedo. *Approximate Relational Reasoning for Probabilistic Programs*. PhD thesis, Technical University of Madrid, 2014.

[18] Prakash Panangaden. The category of markov kernels. *Electronic Notes in Theoretical Computer Science*, 22:171 – 187, 1999. PROBMIV'98, First International Workshop on Probabilistic Methods in Verification.