⋆-Liftings for Differential Privacy and $f$-Divergences

Gilles Barthe, Thomas Espitau, Justin Hsu, Tetsuya Sato, Pierre-Yves Strub
Differential privacy: probabilistic program property

Output depends only a little on any single individual's data.

D

Alice
Bob
Chris
Donna
Ernie

Algorithm

Pr [r]
Differential privacy: probabilistic program property

Output depends only a little on any single individual's data
Differential privacy: probabilistic program property

Output depends only a little on any single individual’s data
More formally

Definition (Dwork, McSherry, Nissim, Smith)
An algorithm is \((\epsilon, \delta)\)-differentially private if, for every two adjacent inputs, the output distributions \(\mu_1, \mu_2\) satisfy:

\[
\Delta_\epsilon(\mu_1, \mu_2) \leq \delta \triangleq \text{for all sets } S, \mu_1(S) \leq e^\epsilon \cdot \mu_2(S) + \delta
\]
More formally

**Definition (Dwork, McSherry, Nissim, Smith)**
An algorithm is \((\epsilon, \delta)\)-differentially private if, for every two adjacent inputs, the output distributions \(\mu_1, \mu_2\) satisfy:

\[
\Delta_\epsilon(\mu_1, \mu_2) \leq \delta \triangleq \text{for all sets } S, \mu_1(S) \leq e^\epsilon \cdot \mu_2(S) + \delta
\]

Behaves well under composition: “\(\epsilon\) and \(\delta\) add up”

Sequentially composing an \((\epsilon, \delta)\)-private program and an \((\epsilon', \delta')\)-private program is \((\epsilon + \epsilon', \delta + \delta')\)-private.
How to verify this property?

Use ideas from probabilistic bisimulation

- $\Delta_\epsilon(\mu_1, \mu_2) \leq \delta$ means “approximately similar”
- Composition $\iff$ approximate probabilistic bisimulation
How to verify this property?

Use ideas from probabilistic bisimulation

- $\Delta_\epsilon(\mu_1, \mu_2) \leq \delta$ means “approximately similar”
- Composition $\iff$ approximate probabilistic bisimulation

Foundation for many styles of program verification

- Linear and dependent type systems
- Product program constructions
- Relational program logics
Review: Probabilistic Liftings and Approximate Liftings
Probabilistic liftings

Lift a binary relation $R$ on pairs $S \times T$ to a relation $\langle R \rangle$ on distributions $\text{Distr}(S) \times \text{Distr}(T)$

**Definition (Larsen and Skou)**

Let $R \subseteq S \times T$ be a relation. Two distributions are related $\mu_1 \langle R \rangle \mu_2$ if there exists a witness $\eta \in \text{Distr}(S \times T)$ such that:

1. $\pi_1(\eta) = \mu_1$ and $\pi_2(\eta) = \mu_2$,
2. $\eta(s, t) > 0$ only when $(s, t) \in R$. 
Lift a binary relation $R$ on pairs $S \times T$ to a relation $\langle R \rangle$ on distributions $\text{Distr}(S) \times \text{Distr}(T)$

**Definition (Larsen and Skou)**

Let $R \subseteq S \times T$ be a relation. Two distributions are related $\mu_1 \langle R \rangle \mu_2$ if there exists a witness $\eta \in \text{Distr}(S \times T)$ such that:

1. $\pi_1(\eta) = \mu_1$ and $\pi_2(\eta) = \mu_2$,
2. $\eta(s, t) > 0$ only when $(s, t) \in R$.

**Example**

$\mu_1 \langle = \rangle \mu_2$ is equivalent to $\mu_1 = \mu_2$. 
An equivalent definition via Strassen’s theorem

Theorem (Strassen 1965)
Let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R \rangle \mu_2$ if and only if:

$$\text{for all subsets } A \subseteq S, \mu_1(A) \leq \mu_2(R(A))$$
An equivalent definition via Strassen’s theorem

**Theorem (Strassen 1965)**

Let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R \rangle \mu_2$ if and only if:

**for all subsets** $A \subseteq S$, $\mu_1(A) \leq \mu_2(R(A))$
Approximate liftings

**Intuition**

- Approximately relate two distributions $\mu_1$ and $\mu_2$
- Add numeric indexes $(\epsilon, \delta)$ to lifting

**Want:**

- Given $R \subseteq S \times T$, lift to $\langle R \rangle^{(\epsilon, \delta)} \subseteq \text{Distr}(S) \times \text{Distr}(T)$
- $\mu_1 \langle = \rangle^{(\epsilon, \delta)} \mu_2$ should be equivalent to $\Delta_\epsilon(\mu_1, \mu_2) \leq \delta$
Approximate liftings

Intuition

▶ Approximately relate two distributions $\mu_1$ and $\mu_2$
▶ Add numeric indexes $(\epsilon, \delta)$ to lifting

Want:

▶ Given $R \subseteq S \times T$, lift to $\langle R \rangle^{(\epsilon, \delta)} \subseteq \text{Distr}(S) \times \text{Distr}(T)$
▶ $\mu_1 \langle = \rangle^{(\epsilon, \delta)} \mu_2$ should be equivalent to $\Delta_\epsilon(\mu_1, \mu_2) \leq \delta$
Approximate liftings

Intuition

▶ Approximately relate two distributions $\mu_1$ and $\mu_2$
▶ Add numeric indexes $(\epsilon, \delta)$ to lifting

Want:

▶ Given $R \subseteq S \times T$, lift to $\langle R \rangle^{(\epsilon, \delta)} \subseteq \text{Distr}(S) \times \text{Distr}(T)$
▶ $\mu_1 \langle = \rangle^{(\epsilon, \delta)} \mu_2$ should be equivalent to $\Delta_\epsilon(\mu_1, \mu_2) \leq \delta$
Previous definitions: “Existential”

Let $R \subseteq S \times T$ be a binary relation. Two distributions are related by $\mu_1 \langle R \rangle^{(\epsilon, \delta)} \mu_2$ if:

1. Witness (Barthe, Köpf, Olmedo, Zanella-Béguelin)
   - There exists $\eta \in \text{Distr}(S \times T)$ such that
     - $\pi_1(\eta) = \mu_1$ and $\pi_2(\eta) \leq \mu_2$,
     - $\Delta \epsilon (\mu_1, \pi_1(\eta)) \leq \delta$.

2. Witnesses (Barthe and Olmedo)
   - There exists $\eta_L, \eta_R \in \text{Distr}(S \times T)$ such that
     - $\pi_1(\eta_L) = \mu_1$ and $\pi_2(\eta_R) = \mu_2$,
     - $\eta_L(s,t), \eta_R(s,t) > 0$ only when $(s,t) \in R$,
     - $\Delta \epsilon (\eta_L, \eta_R) \leq \delta$. 

---

9
Let $R \subseteq S \times T$ be a binary relation. Two distributions are related by $\mu_1 \langle R \rangle^{(\epsilon, \delta)} \mu_2$ if:

### One witness (Barthe, Köpf, Olmedo, Zanella-Béguelin)

There exists $\eta \in \text{Distr}(S \times T)$ such that

1. $\pi_1(\eta) = \mu_1$ and $\pi_2(\eta) \leq \mu_2$,
2. $\eta(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\mu_1, \pi_1(\eta)) \leq \delta$. 

### Two witnesses (Barthe and Olmedo)

There exists $\eta^L, \eta^R \in \text{Distr}(S \times T)$ such that

1. $\pi_1(\eta^L) = \mu_1$ and $\pi_2(\eta^R) = \mu_2$,
2. $\eta^L(s, t), \eta^R(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\eta^L, \eta^R) \leq \delta$. 

### Three witnesses (Barthe, Köpf, Olmedo, Zanella-Béguelin)

There exists $\eta^L, \eta^R \in \text{Distr}(S \times T)$ such that

1. $\pi_1(\eta^L) = \mu_1$ and $\pi_2(\eta^R) = \mu_2$,
2. $\eta^L(s, t), \eta^R(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\eta^L, \eta^R) \leq \delta$. 

### Nine witnesses

There exists $\eta^L, \eta^R \in \text{Distr}(S \times T)$ such that

1. $\pi_1(\eta^L) = \mu_1$ and $\pi_2(\eta^R) = \mu_2$,
2. $\eta^L(s, t), \eta^R(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\eta^L, \eta^R) \leq \delta$. 

This provides a comprehensive framework for understanding the relationship between two distributions based on a binary relation.
Previous definitions: “Existential”

Let $R \subseteq S \times T$ be a binary relation. Two distributions are related by $\mu_1 \langle R \rangle^{(\epsilon, \delta)} \mu_2$ if:

One witness (Barthe, Köpf, Olmedo, Zanella-Béguelin)
There exists $\eta \in \text{Distr}(S \times T)$ such that
1. $\pi_1(\eta) = \mu_1$ and $\pi_2(\eta) \leq \mu_2$,
2. $\eta(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\mu_1, \pi_1(\eta)) \leq \delta$.

Two witnesses (Barthe and Olmedo)
There exists $\eta_L, \eta_R \in \text{Distr}(S \times T)$ such that
1. $\pi_1(\eta_L) = \mu_1$ and $\pi_2(\eta_R) = \mu_2$,
2. $\eta_L(s, t), \eta_R(s, t) > 0$ only when $(s, t) \in R$,
3. $\Delta_\epsilon(\eta_L, \eta_R) \leq \delta$. 
Let $R \subseteq S \times T$ be a binary relation. Two distributions are related by $\mu_1 \langle R \rangle^{(\epsilon, \delta)} \mu_2$ if:
Let $R \subseteq S \times T$ be a binary relation. Two distributions are related by $\mu_1 \langle R \rangle^{(\epsilon,\delta)} \mu_2$ if:

**No witnesses (Sato)**

For all subsets $A \subseteq S$, we have

$$\mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta$$
Which definition is the “right” one?

Definitions support different properties and constructions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1-witness</td>
<td>?</td>
<td>?</td>
<td>Yes</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>2-witness</td>
<td>Yes</td>
<td>Almost*</td>
<td>No</td>
<td>Almost*</td>
<td>Almost*</td>
<td>Yes</td>
</tr>
<tr>
<td>Universal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>?</td>
</tr>
</tbody>
</table>
Which definition is the “right” one?

Definitions support different properties and constructions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1-witness</td>
<td>?</td>
<td>?</td>
<td>Yes</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>2-witness</td>
<td>Yes</td>
<td>Almost*</td>
<td>No</td>
<td>Almost*</td>
<td>Almost*</td>
<td>Yes</td>
</tr>
<tr>
<td>Universal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>?</td>
</tr>
</tbody>
</table>

Broad tradeoff: How general?

- Less general: less compositional
- More general: harder to prove properties about
Our work: ★-Liftings, Equivalences, and an approximate Strassen’s theorem
New definition: ⋄-liftings

Generalize 2-witness lifting by adding a new point

Let $R \subseteq S \times T$ be a binary relation, and let $A^\dagger = A \cup \{\dagger\}$. Two distributions are related by $\mu_1 \langle R^\dagger \rangle^{(\epsilon,\delta)} \mu_2$ if:

There exists $\eta_L, \eta_R \in \text{Distr}(S^\dagger \times T^\dagger)$ such that

1. $\pi_1(\eta_L) = \mu_1$ and $\pi_2(\eta_R) = \mu_2$,
2. $\eta_L(s, t), \eta_R(s, t) > 0$ only when $(s, t) \in R \text{ or } s = \dagger \text{ or } t = \dagger$,
3. $\Delta_\epsilon(\eta_L, \eta_R) \leq \delta$. 

Intuition ▶ ⋄ is a default point for tracking "unimportant" mass /one.osf/three.osf
New definition: ★-liftings

Generalize 2-witness lifting by adding a new point

Let $R \subseteq S \times T$ be a binary relation, and let $A^* = A \cup \{\star\}$. Two distributions are related by $\mu_1 \langle R^* \rangle^{(\varepsilon, \delta)} \mu_2$ if:

There exists $\eta_L, \eta_R \in \text{Distr}(S^* \times T^*)$ such that

1. $\pi_1(\eta_L) = \mu_1$ and $\pi_2(\eta_R) = \mu_2$,
2. $\eta_L(s, t), \eta_R(s, t) > 0$ only when $(s, t) \in R$ or $s = \star$ or $t = \star$,
3. $\Delta_\varepsilon(\eta_L, \eta_R) \leq \delta$.

Intuition

▶ ★ is a default point for tracking "unimportant" mass
Why is $\star$-lifting a good definition?

Previously known

One-witness $\equiv$ Two-witness $\implies$ Universal
Why is \( \star \)-lifting a good definition?

Previously known

One-witness \( (??) \) Two-witness \( \Rightarrow \) Universal

\( \star \)-liftings unify known approximate liftings

One-witness \( \iff \) \( \star \)-lifting \( \iff \) Universal
Approximate version of Strassen’s theorem

\[ \star \text{-liftings are equivalent to “universal” approximate liftings} \]

**Theorem**

Let \( S, T \) be discrete (countable) sets, and let \( R \subseteq S \times T \) be a relation. Then \( \mu_1 \langle R^\star \rangle^{(\epsilon, \delta)} \mu_2 \) if and only if:

\[ \text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta \]
Approximate version of Strassen’s theorem

\[ \star \text{-liftings are equivalent to “universal” approximate liftings} \]

**Theorem**

Let \( S, T \) be discrete (countable) sets, and let \( R \subseteq S \times T \) be a relation. Then \( \mu_1 \langle R^\star \rangle^{(\epsilon, \delta)} \mu_2 \) if and only if:

\[ \text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta \]

**Theorem (Strassen 1965)**

Let \( R \subseteq S \times T \) be a relation. Then \( \mu_1 \langle R \rangle \mu_2 \) if and only if:

\[ \text{for all subsets } A \subseteq S, \mu_1(A) \leq \mu_2(R(A)) \]
Approximate version of Strassen’s theorem

\*\*-liftings are equivalent to “universal” approximate liftings

**Theorem**
Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^* \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

for all sets $A \subseteq S$, $\mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta$

**Theorem (Strassen 1965)**
Let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R \rangle \mu_2$ if and only if:

for all subsets $A \subseteq S$, $\mu_1(A) \leq \mu_2(R(A))$
Proof sketch (universal lifting implies $\star$-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1(\langle R^\star \rangle (\epsilon, \delta)) \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]
Proof sketch (universal lifting implies ⋆-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^\star \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

Define a flow network

- **Nodes**
Proof sketch (universal lifting implies ⋆-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^* \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

**Define a flow network**

- **Nodes**
  - Source/sink: $\top, \bot$
Proof sketch (universal lifting implies $\star$-lifting)

Theorem

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^\star \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

Define a flow network

- Nodes
  - Source/sink: $\top, \bot$
  - Internal nodes: $S^\star \cup T^\star$
Proof sketch (universal lifting implies ⋆-lifting)

Theorem
Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^* \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

Define a flow network

- **Nodes**
  - Source/sink: $\top, \bot$
  - Internal nodes: $S^* \cup T^*$

- **Edges**
Proof sketch (universal lifting implies ⋆-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1(R^*)^{(c, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^c \cdot \mu_2(R(A)) + \delta
\]

**Define a flow network**

- **Nodes**
  - Source/sink: $\top, \bot$
  - Internal nodes: $S^* \cup T^*$

- **Edges**
  - From source/to sink: $(\top, s), (t, \bot)$
Proof sketch (universal lifting implies $\star$-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^\star \rangle^{(e,\delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^e \cdot \mu_2(R(A)) + \delta
\]

**Define a flow network**

- **Nodes**
  - Source/sink: $\top$, $\bot$
  - Internal nodes: $S^\star \cup T^\star$

- **Edges**
  - From source/to sink: $(\top, s), (t, \bot)$
  - Internal edges: $(s, t) \in R, (\star, t), (s, \star)$
Proof sketch (universal lifting implies $\star$-lifting)

**Theorem**

Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^\star \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

\[
\text{for all sets } A \subseteq S, \quad \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

Define a flow network

- **Nodes**
  - Source/sink: $\top, \bot$
  - Internal nodes: $S^\star \cup T^\star$

- **Edges**
  - From source/to sink: $(\top, s), (t, \bot)$
  - Internal edges: $(s, t) \in R, (\star, t), (s, \star)$

- **Capacities**
Proof sketch (universal lifting implies ⋆-lifting)

Theorem
Let $S, T$ be discrete (countable) sets, and let $R \subseteq S \times T$ be a relation. Then $\mu_1 \langle R^* \rangle^{(\epsilon, \delta)} \mu_2$ if and only if:

$$\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta$$

Define a flow network

- **Nodes**
  - Source/sink: $\top, \bot$
  - Internal nodes: $S^* \cup T^*$

- **Edges**
  - From source/to sink: $(\top, s), (t, \bot)$
  - Internal edges: $(s, t) \in R, (\star, t), (s, \star)$

- **Capacities**
  - Outbound $c(\top, s)$ given by $\exp(-\epsilon) \cdot \mu_1$
Proof sketch (universal lifting implies \( \star \)-lifting)

**Theorem**

Let \( S, T \) be discrete (countable) sets, and let \( R \subseteq S \times T \) be a relation. Then \( \mu_1 \langle R^\star \rangle (\epsilon, \delta) \mu_2 \) if and only if:

\[
\text{for all sets } A \subseteq S, \mu_1(A) \leq e^\epsilon \cdot \mu_2(R(A)) + \delta
\]

Define a flow network

- **Nodes**
  - Source/sink: \( \top, \bot \)
  - Internal nodes: \( S^\star \cup T^\star \)

- **Edges**
  - From source/to sink: \( (\top, s), (t, \bot) \)
  - Internal edges: \( (s, t) \in R, (\star, t), (s, \star) \)

- **Capacities**
  - Outbound \( c(\top, s) \) given by \( \exp(-\epsilon) \cdot \mu_1 \)
  - Incoming \( c(t, \bot) \) given by \( \mu_2 \)
Proof sketch (universal lifting implies ⋆-lifting)

Universal lifting $\Rightarrow$ minimum cut large

Max-/f_low min-cut: there is a large $f_{low}$

Use $f(s,t)$ to recover ⋆-lifting witnesses $(\eta_L, \eta_R)$, conclude:

$\mu_1(\epsilon, \delta)$ /one.osf/seven.osf
Proof sketch (universal lifting implies \(*\)-lifting)

**Universal lifting implies minimum cut large**

- **Max-flow min-cut:** there is a large flow $f$ from $\top$ to $\bot$
- Use $f(s, t)$ to recover $\ast$-lifting witnesses $(\eta_L, \eta_R)$, conclude:

$$\mu_1 \langle R^\ast \rangle^{(\epsilon, \delta)} \mu_2$$
Other Results and Future Directions
See the paper for …

- Further properties of $\star$-liftings
- Symmetric $\star$-liftings and advanced composition
- $\star$-liftings for $f$-divergences
Open questions

- Generalize to continuous distributions?
- Similar equivalences for other approximate lifting?
- Which properties should approximate liftings satisfy?
Wrapping up: Future directions and other speculation

Open questions

- Generalize to continuous distributions?
- Similar equivalences for other approximate lifting?
- Which properties should approximate liftings satisfy?

Mild speculation

★-liftings are the “right” approximate version of probabilistic couplings
★-Liftings for Differential Privacy and $f$-Divergences

Gilles Barthe, Thomas Espitau, Justin Hsu, Tetsuya Sato, Pierre-Yves Strub