Liftings for Differential Privacy

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

$\star$-Liftings for Differential Privacy

Gilles Barthe[1], Thomas Espitau[2], Justin Hsu[3], Tetsuya Sato[4], and Pierre-Yves Strub[5]

1 **IMDEA Software Institute, Spain**
`gjbarthe@gmail.com`
2 **Sorbonne Universités, UPMC Paris 6, France**
`t.espitau@gmail.com`
3 **University of Pennsylvania, USA**
`justhsu@cis.upenn.edu`
4 **Research Institute for Mathematical Sciences, Kyoto University, Japan**
`satoutet@kurims.kyoto-u.ac.jp`
5 **École Polytechnique, France**
`pierre-yves@strub.nu`

Abstract

Recent developments in formal verification have identified *approximate liftings* (also known as *approximate couplings*) as a clean, compositional abstraction for proving differential privacy. There are two styles of definitions for this construction. Earlier definitions require the existence of one or more witness distributions, while a recent definition by Sato uses universal quantification over all sets of samples. These notions have different strengths and weaknesses: the universal version is more general than the existential ones, but the existential versions enjoy more precise composition principles.

We propose a novel, existential version of approximate lifting, called $\star$-*lifting*, and show that it is equivalent to Sato's construction for discrete probability measures. Our work unifies all known notions of approximate lifting, giving cleaner properties, more general constructions, and more precise composition theorems for both styles of lifting, enabling richer proofs of differential privacy. We also clarify the relation between existing definitions of approximate lifting, and generalize our constructions to approximate liftings based on f-divergences.

1998 ACM Subject Classification D.2.4 Software/Program Verification

Keywords and phrases Differential Privacy, Probabilistic Couplings, Formal Verification

Digital Object Identifier 10.4230/LIPIcs.ICALP.2017.

1 Introduction

Differential privacy [7] is a rigorous notion of statistical privacy that delivers strong individual guarantees for privacy-preserving computations. Informally, differential privacy guarantees to every individual that their (non)-participation in a database will have a small (in a rigorous, quantitative sense) effect on the results obtained by third parties when querying the database. The formal definition of differential privacy is parametrized by two non-negative real numbers, (ϵ, δ). These parameters quantify the effect of individuals on the output of the private query; smaller values give stronger privacy guarantees. The main strengths of differential privacy lie in its theoretical elegance, minimal assumptions, and flexibility for many applications.

Motivated by the importance of differential privacy, programming language researchers have developed approaches based on dynamic analysis, type systems, and program logics for formally proving differential privacy for programs. (We refer the interested reader to a recent survey [6] for an overview of this growing field.) In this paper, we consider approaches based on relational program logics [2–5, 10, 11]. To capture the quantitative nature of differential privacy, these systems rely on a quantitative generalization of probabilistic couplings (see, e.g., [9, 13, 14]), called *approximate liftings* or (ϵ, δ)-liftings. Existing works have considered several potential definitions. While all definitions support compositional reasoning and enable program logics that can verify complex examples from the privacy literature, the various notions of approximate liftings have different strengths and weaknesses.

Broadly speaking, one class of definitions require the existence of one or two *witness distributions* that "couple' the two executions of programs. The earliest definition [3] supports accuracy-based reasoning for the Laplace mechanism, while subsequent definitions [2, 10] support more precise composition principles from differential privacy and can be generalized to other notions of distance on distributions. These definitions, and their associated program logics, were designed for discrete distributions.

In the course of extending these ideas to continuous distributions, Sato [11] proposes a radically different notion of approximate lifting, which does not rely on witness distributions. Instead, it uses a universal quantification over all sets of samples. Sato shows that this definition is strictly more general than the existential versions, but it is unclear (a) whether the gap can be closed and (b) whether his construction satisfies the same composition principles enjoyed by some existential definitions.

As a consequence, there is currently no single approximate lifting with the properties needed to support all existing formalized proofs of differential privacy. Furthermore, some of the most involved privacy proofs cannot be formalized at all, as their proofs require a combination of tools from several kinds of approximate liftings.

Outline of the paper

After reviewing the necessary mathematical preliminaries in Section 2, we introduce our main technical contribution: a new, existential definition of approximate lifting. This construction, which we call ⋆-*lifting*, is a generalization of an existing definition by Barthe and Olmedo [2], Olmedo [10]. The key idea is to allow the witness distributions to have a larger domain, broadening the class of approximate liftings. By a maximum flow/minimum cut argument, we show that ⋆-liftings are equivalent to Sato's lifting over discrete distributions. This equivalence can be viewed as an approximate version of Strassen's theorem [12], a classical result in probability theory describing the existence of probabilistic couplings. We present the definition of ⋆-lifting and the proof of equivalence in Section 3.

Then, we show that ⋆-liftings satisfy desirable theoretical properties. We are able to leverage the equivalence of liftings in two ways. In one direction, Sato's definition gives simpler proofs of more general properties of ⋆-liftings. In the other direction, ⋆-liftings—like other existential definitions—can smoothly incorporate composition principles from the theory of differential privacy. Our connection shows that Sato's definition can use these principles in the discrete case. We describe the key theoretical properties of ⋆-liftings in Section 4.

Finally, we provide a thorough comparison of ⋆-lifting with existing definitions of approximate lifting in Section 5, and describe how to construct ⋆-liftings for more general version of approximate liftings based on f-divergences in Section 6.

Overall, the equivalence of ⋆-liftings and Sato's lifting, along with the natural theoretical properties satisfied by the common notion, suggest that these definitions are two views on the same concept: an approximate version of probabilistic coupling.

2 Background

To model probabilistic behavior, we work with *discrete sub-distributions*.

▶ **Definition 1.** A *sub-distribution* over a set A is defined by its mass function $\mu : A \to \mathbb{R}^+$, which gives the probability of the singleton events $a \in A$. This mass function must be s.t. $|\mu| \triangleq \sum_{a \in A} \mu(a)$ is well-defined and at most 1. In particular, the *support* $\mathrm{supp}(\mu) \triangleq \{a \in A \mid \mu(a) \neq 0\}$ must be discrete (i.e. finite or countably infinite). When the *weight* $|\mu|$ is equal to 1, we call μ a *(proper) distribution*. We let $\mathbb{D}(A)$ denote the set of sub-distributions over A. The probability of an event $E(x)$ w.r.t. μ, written $\mathbb{P}_{x \sim \mu}[E(x)]$ or $\mathbb{P}_\mu[E]$, is defined as $\sum_{x \in A | E(x)} \mu(x)$.

Simple examples of sub-distributions include the *null sub-distribution* $\mathbb{0}^A \in \mathbb{D}(A)$, which maps each element of A to 0, and the *Dirac distribution centered on* x, written $\mathbb{1}_x$, which maps x to 1 and all other elements to 0. One can equip distributions with a monadic structure using the Dirac distributions $\mathbb{1}_x$ for the unit and *distribution expectation* $\mathbb{E}_{x \sim \mu}[f(x)]$ for the bind; if μ is a distribution over A and f has type $A \to \mathbb{D}(B)$, then the bind defines a sub-distribution over B: $\mathbb{E}_{a \sim \mu}[f(a)] : b \mapsto \sum_a \mu(a) \cdot f(a)(b)$.

If $f : A \to B$, we can lift f to a function $f^\sharp : \mathbb{D}(A) \to \mathbb{D}(B)$ as follows: $f^\sharp(\mu) \triangleq \mathbb{E}_{a \sim \mu}[\mathbb{1}_{f(a)}]$ — or, equivalently, $f^\sharp(\mu) : b \mapsto \mathbb{P}_{a \sim \mu}[a \in f^{-1}(b)]$. For instance, when working with sub-distributions over pairs, this allows to obtain the probabilistic versions $\pi_1^\sharp$ and $\pi_2^\sharp$ (called *marginals*) of the usual projections π_1 and π_2. One can check that the *first* and *second marginals* $\pi_1^\sharp(\mu)$ and $\pi_2^\sharp(\mu)$ of a distribution μ over $A \times B$ are also given by the following equations: $\pi_1^\sharp(\mu)(a) = \sum_{b \in B} \mu(a, b)$ and $\pi_2^\sharp(\mu)(b) = \sum_{a \in A} \mu(a, b)$. When $f : A \to \mathbb{D}(B)$, we will abuse notation and write the lifting $f^\sharp : \mathbb{D}(A) \to \mathbb{D}(B)$ to mean $f^\sharp(\mu) \triangleq \mathbb{E}_{x \sim \mu}[f(x)]$.

Finally, if $\alpha : A \to \mathbb{R}^+$, we write $\alpha[X] \in \mathbb{R}^+ \cup \{\infty\}$ for $\sum_{x \in X} \alpha(x)$. Moreover, if $\alpha : A \times B \to \mathbb{R}^+$, we write $\alpha[X, Y]$ (resp. $\alpha[x, Y]$, $\alpha[X, y]$) for $\alpha[X \times Y]$ (resp. $\alpha[\{x\} \times Y$, $\alpha[X \times \{y\}]$). Note that for a sub-distribution $\mu \in \mathbb{D}(A)$ and an event $E \subseteq A$, $\mathbb{P}_\mu[E] = \mu[E]$.

We now review the definition of differential privacy.

▶ **Definition 2** (Dwork et al. [7])**.** A probabilistic computation $M : A \to \mathbb{D}(B)$ satisfies (ϵ, δ)-*differential privacy* w.r.t. an adjacency relation $\phi \subseteq A \times A$ iff for every pair of inputs $a, a' \in A$ such that $a \mathrel{\phi} a'$ and every subset of outputs $E \subseteq B$,

$$\mathbb{P}_{M(a)}[E] \leq e^\epsilon \cdot \mathbb{P}_{M(a')}[E] + \delta.$$

It is useful to define a notion of distance on distributions, reflecting differential privacy.

▶ **Definition 3** (Barthe and Olmedo [2], Barthe et al. [3], Olmedo [10])**.** Let $\epsilon \geq 0$. The ϵ*-DP divergence* $\Delta_\epsilon(\mu_1, \mu_2)$ between two sub-distributions $\mu_1, \mu_2 \in \mathbb{D}(B)$ is defined as

$$\sup_{E \subseteq B} \left(\mathbb{P}_{\mu_1}[E] - e^\epsilon \cdot \mathbb{P}_{\mu_2}[E]\right).$$

Then, differential privacy admits an alternative characterization based on DP divergence.

▶ **Lemma 4.** *A probabilistic computation $M : A \to \mathbb{D}(B)$ satisfies (ϵ, δ)-*differential privacy *w.r.t. an adjacency relation $\phi \subseteq A \times A$ iff $\Delta_\epsilon(M(a), M(a')) \leq \delta$ for every pair of inputs $a, a' \in A$ such that $a \mathrel{\phi} a'$.*

Our new definition of approximate lifting is inspired by a version of approximate liftings involving two witness distributions, proposed by Barthe and Olmedo [2], Olmedo [10].

▶ **Definition 5** (Barthe and Olmedo [2], Olmedo [10]). Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. An (ϵ, δ)-*approximate* 2-*lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a pair $(\mu_\triangleleft, \mu_\triangleright)$ of sub-distributions over $A \times B$ s.t.

1. $\pi_1^\sharp(\mu_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\mu_\triangleright) = \mu_2$;
2. $\Delta_\epsilon(\mu_\triangleleft, \mu_\triangleright) \leq \delta$; and
3. $\mathrm{supp}(\mu) \subseteq \mathcal{R}$.

We write $\mu_1 \; \mathcal{R}^{(2)}_{\epsilon,\delta} \; \mu_2$ if there exists an (ϵ, δ)-approximate (2-)lifting of μ_1 & μ_2 for $\mathcal{R}$; the (2) indicates that there are two witnesses in this definition of lifting.

Combined with Lemma 4, a probabilistic computation $M : A \to \mathbb{D}(B)$ is (ϵ, δ)-differentially private if and only if for every two adjacent inputs $a \; \phi \; a'$, there is an approximate lifting of the equality relation: $M(a) =^{(2)}_{\epsilon,\delta} M(a')$.

2-liftings can be generalized by varying the notion of distance given by Δ_ϵ; we will return to this point in Section 6. These liftings also satisfy useful theoretical properties, but some of the properties are not as general as we would like. For example, it is known that 2-liftings satisfy the following mapping property.

▶ **Theorem 6** (Barthe et al. [4]). *Let $\mu_1 \in \mathbb{D}(A_1)$, $\mu_2 \in \mathbb{D}(A_2)$, $f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$* surjective *maps and $\mathcal{R}$ a binary relation on B_1 & B_2. Then*

$$f_1^\sharp(\mu_1) \; \mathcal{R}^{(2)}_{\epsilon,\delta} \; f_2^\sharp(\mu_2) \iff \mu_1 \; \mathcal{S}^{(2)}_{\epsilon,\delta} \; \mu_2$$

where $a_1 \; \mathcal{S} \; a_2 \stackrel{\triangle}{\iff} f_1(a_1) \; \mathcal{R} \; f_2(a_2)$.

This property can be used to pull back an approximate lifting on two distributions over B_1, B_2 to an approximate lifting on two distributions over A_1, A_2. For applications in program logics, B_1, B_2 could be the domain of a program variable, A_1, A_2 could be the set of memories, and f_1, f_2 could project a memory to a program variable. While the mapping theorem is quite useful, it is puzzling why it only applies to surjective maps. For instance, this theorem cannot be used when the maps f_1, f_2 embed a smaller space into a larger space.

For another example, there exist 2-liftings of the following form, sometimes called the *optimal subset coupling.*

▶ **Theorem 7** (Barthe et al. [4]). *Let $\mu \in \mathbb{D}(A)$ and consider two subsets $P_1 \subseteq P_2 \subseteq A$. Suppose that P_2 is a* strict subset *of A. Then, we have the following equivalence:*

$$\mathbb{P}_\mu[P_2] \leq e^\epsilon \cdot \mathbb{P}_\mu[P_1] \iff \mu \; \mathcal{R}^{(2)}_{\epsilon,0} \; \mu,$$

where $a_1 \; \mathcal{R} \; a_2 \stackrel{\triangle}{\iff} a_1 \in P_1 \iff a_2 \in P_2$.

In this construction, it is puzzling why the larger subset P_2 must be a *strict* subset of the domain A. For example, this theorem does not apply for $P_2 = A$, but we may be able to construct the approximate lifting if we simply embed A into a larger space B—even though μ has support over A! Furthermore, it is not clear why the subsets must be nested, nor is it clear why we can only relate μ to itself.

These shortcomings suggest that the definition of 2-liftings may be problematic. While the distance condition appears to be the most constraining requirement, the marginal and support conditions are responsible for the main issues.

Witnesses can only use pairs in the relation.

For some relations $\mathcal{R}$, there may be elements a such that $a \mathcal{R} b$ does not hold for any b, or vice versa. It can be impossible find witnesses with the correct marginals on these elements, even if the distance condition can be easily satisfied. For instance, we can sometimes construct a pair $\mu_\triangleleft$ and $\mu_\triangleright$ satisfying the distance requirement, but where $\mu_\triangleright$ needs additional mass to achieve the marginal requirement for an element b. Adding this mass anywhere preserves the distance bound, but there may not be an element a such that $a \mathcal{R} b$.

No canonical choice of witnesses.

A related problem is that the marginal requirement only constrains one marginal of each witness distribution. Along the other component, the witnesses may place the mass anywhere on any pair in the relation. As a result, witnesses to an approximate lifting $\mu_1 \mathcal{R}^{(2)}_{\epsilon,\delta} \mu_2$ may have mass outside of $\mathrm{supp}(\mu_1) \times \mathrm{supp}(\mu_2)$, even though it seems that only elements in the support should be relevant to the lifting.

3 $\star$-Liftings and Strassen's Theorem

To improve the theoretical properties of 2-liftings, we propose a simple extension: allow witnesses to be distributions over a larger set.

▶ **Notation 8.** Let A be a set. We write $A^\star$ for $A \uplus \{\star\}$.

▶ **Definition 9** ($\star$-lifting)**.** Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. An (ϵ, δ)-*approximate* $\star$-*lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a pair of sub-distributions $\eta_\triangleleft \in \mathbb{D}(A \times B^\star)$ and $\eta_\triangleright \in \mathbb{D}(A^\star \times B)$ s.t.

1. $\pi_1^\sharp(\eta_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\eta_\triangleright) = \mu_2$;
2. $\mathrm{supp}(\eta_{\triangleleft|A\times B}), \mathrm{supp}(\eta_{\triangleright|A\times B}) \subseteq \mathcal{R}$; and
3. $\Delta_\epsilon(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) \leq \delta$, where $\overline{\eta_\bullet}$ is the canonical lifting of $\eta_\bullet$ to $A^\star \times B^\star$.

We write $\mu_1 \; R^{(\star)}_{\epsilon,\delta} \; \mu_2$ if there exists an (ϵ, δ)-approximate lifting of μ_1 & μ_2 for $\mathcal{R}$.

By adding an element $\star$, we address both problems discussed at the end of the previous section. First, for every $a \in A$, witnesses may place mass at $(a, \star)$; for every $b \in B$, witnesses may place mass at $(\star, b)$. Second, $\star$ can serve as a generic element where all mass that lies outside the supports $\mathrm{supp}(\mu_1) \times \mathrm{supp}(\mu_2)$ may be placed, while preserving the marginal and distance requirements, giving more control over the form of the witnesses.

▶ **Lemma 10.** *Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be distributions such that $\mu_1 \; \mathcal{R}^{(\star)}_{\epsilon,\delta} \; \mu_2$. Then, there are witnesses with support contained in* $\mathrm{supp}(\mu_1)^\star \times \mathrm{supp}(\mu_2)^\star$.

Proof. See Appendix, p. 14 ◀

3.1 Basic Properties

$\star$-liftings satisfy all basic properties satisfied by other notions of lifting. We start by proving that this new definition of lifting still characterizes differential privacy.

▶ **Lemma 11.** *A randomized algorithm $P : A \to \mathbb{D}(B)$ is (ϵ, δ)-differentially private for ϕ iff for all $a_1, a_2 \in A$, $a_1 \; \phi \; a_2$ implies $P(a_1) =^{(\star)}_{\epsilon,\delta} P(a_2)$.*

Proof. See Appendix, p. 14 ◀

The next lemma establishes several other basic properties of ⋆-liftings: monotonicity, and closure under relational and sequential composition.

▶ **Lemma 12.**
- *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$, and $\mathcal{R}$ be a binary relation over A & B. If $\mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\delta}\ \mu_2$, then for any $\epsilon' \geq \epsilon$, $\delta' \geq \delta$ and $\mathcal{S} \supseteq \mathcal{R}$, we have $\mu_1\ \mathcal{S}^{(\star)}_{\epsilon',\delta'}\ \mu_2$.*
- *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$, $\mu_2 \in \mathbb{D}(C)$ and $\mathcal{R}$ (resp. $\mathcal{S}$) be a binary relation over A & B (resp. over B & C). If $\mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\delta}\ \mu_2$ and $\mu_2\ \mathcal{S}^{(\star)}_{\epsilon',\delta'}\ \mu_3$, then $\mu_1\ (\mathcal{S} \circ \mathcal{R})^{(\star)}_{\epsilon+\epsilon',\delta+e^{\epsilon}\cdot\delta'}\ \mu_3$.*
- *For $i \in \{1,2\}$, let $\mu_i \in \mathbb{D}(A_i)$ and $\eta_i : A_i \to \mathbb{D}(B_i)$. Let $\mathcal{R}$ (resp. $\mathcal{S}$) be a binary relation over A_1 & A_2 (resp. over B_1 & B_2). If $\mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\delta}\ \mu_2$ for some $\epsilon, \delta \geq 0$ and for any $(a_1,a_2) \in\mathcal{R}$, $\eta_1(a_1)\ \mathcal{S}^{(\star)}_{\epsilon',\delta'}\ \eta_2(a_2)$ for some $\epsilon',\delta' \geq 0$, then*

$$\mathbb{E}_{\mu_1}[\eta_1]\ \mathcal{S}^{(\star)}_{\epsilon+\epsilon',\delta+\delta'}\ \mathbb{E}_{\mu_2}[\eta_2].$$

Proof. See Appendix, p. 14 ◀

3.2 Equivalence with Sato's Definition

In recent work on verifying differential privacy over general, continuous distributions, Sato [11] proposes an alternative definition of approximate lifting. In the special case of discrete distributions, where measurability of events can be forgotten, his definition can be stated as follows.

▶ **Definition 13** (Sato [11]). Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$, $\mathcal{R}$ be a binary relation over A & B and $\epsilon, \delta \geq 0$. Then, there is an (ϵ,δ)-approximate lifting of μ_1 & μ_2 for $\mathcal{R}$ if

$$\forall X \subseteq A.\, \mu_1[X] \leq e^{\epsilon} \cdot \mu_2[\mathcal{R}(X)] + \delta.$$

Notice that this definition has no witness distributions at all; instead, it uses a universal quantifier over all subsets. We can show that ⋆-liftings are equivalent to Sato's definition in the case of discrete distributions. This equivalence is reminiscent of Strassen's theorem from probability theory, which characterizes the existence of probabilistic couplings.

▶ **Theorem 14** (Strassen [12]). *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$ be two proper distributions, and $\mathcal{R}$ let be a binary relation over A & B. Then there exists a joint distribution $\mu \in \mathbb{D}(A \times B)$ with support in $\mathcal{R}$ such that $\pi_1^\sharp(\mu) = \mu_1$ and $\pi_2^\sharp(\mu) = \mu_2$ if and only if*

$$\forall X \subseteq A.\, \mu_1[X] \leq \mu_2[\mathcal{R}(X)].$$

Our result (Theorem 19) can be viewed as a generalization of Strassen's theorem to approximate couplings. The key ingredient in our proof is the *max-flow min-cut* theorem for *countable* networks; we begin by reviewing the basic setting.

▶ **Definition 15** (Flow network). A *flow network* is a structure $((V,E),\top,\bot,c)$ s.t. $\mathcal{N} = (V,E)$ is a loop-free directed graph without infinite simple path (or rays), $\top$ and $\bot$ are two distinct distinguished vertices of $\mathcal{N}$ s.t. no edge starts from $\bot$ and ends at $\top$, and $c : E \to \mathbb{R}^+ \cup \{+\infty\}$ is a function assigning to each edge of $\mathcal{N}$ a capacity. The capacity c is extended to V^2 by assigning capacity 0 to any pair (u,v) s.t. $(u,v) \notin E$.

▶ **Definition 16** (Flow). Given a flow network $\mathcal{N} \triangleq ((V,E),\top,\bot,c)$, a function $f : V^2 \to \mathbb{R}$ is a *flow* for $\mathcal{N}$ iff

1. $\forall u,v \in V.\, f(u,v) \leq c(u,v)$,
2. $\forall u,v \in V.\, f(u,v) = -f(v,u)$, and

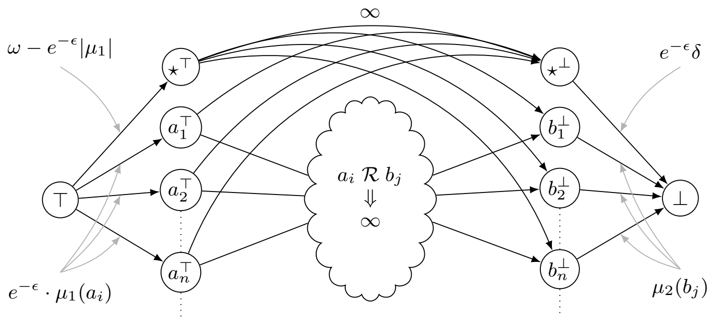

Figure 1 Flow Network in Theorem 19

3. $\forall u \in V.\, u \notin \{\top, \perp\} \implies \sum_{v \in V} f(u, v) = 0$ (Kirchhoff's Law).

The *mass* $|f|$ of a flow f is defined as $|f| \triangleq \sum_{v \in V} f(\top, v) \in \mathbb{R}\{\cup + \infty\}$.

▶ **Definition 17** (Cut). Given a flow network $\mathcal{N} \triangleq ((V, E), \top, \perp, c)$, a *cut* for $\mathcal{N}$ is any set $C \subseteq V$ that partition V s.t. $\top \in V$ but $\perp \notin V$. The *cut-set* $\mathcal{E}(C)$ of a cut C is defined as: $\{(u, v) \in E \mid u \in S, v \notin S\}$. The *capacity* $|C| \in \mathbb{R}^+ \cup \{\infty\}$ of a cut is defined as $|C| \triangleq \sum_{(u,v) \in \mathcal{E}(C)} c(u, v)$.

For flow networks with finitely many vertices an edges, the maximum flow is equal to the minimum cut. Aharoni et al. [1] consider when this is the case for a countable network. For the flow networks that we consider in this paper—where there are no infinite directed paths—equality holds.

▶ **Theorem 18** (Weak Countable Max-Flow Min-Cut). *Let $\mathcal{N}$ be a network flow. Then,*

$$\sup\{|f| \mid f \textit{ is a flow for } \mathcal{N}\} = \inf\{|C| \mid C \textit{ is a cut for } \mathcal{N}\}$$

and both the supremum and infimum are reached.

We are now ready to prove an approximate version of Strassen's theorem, thereby showing equivalence between $\star$-liftings and Sato's liftings.

▶ **Theorem 19.** *Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$, $\mathcal{R}$ be a binary relation over A & B and $\epsilon, \delta \in \mathbb{R}^+$. Then, $\mu_1\ R^{(\star)}_{\epsilon,\delta}\ \mu_2$ iff $\forall X \subseteq A.\, \mu_1(X) \leq e^\epsilon \cdot \mu_2(\mathcal{R}(X)) + \delta$.*

Proof. We only detail the reverse direction. We can assume that A and B are countable; in the case where A and B are not both countable, we first consider the restriction of μ_1 and μ_2 to their respective supports—which are countable sets—and construct witnesses to the $\star$-lifting. The witnesses can then be extended to a coupling of μ_1 and μ_2 by adding a null mass to the extra points.

Let $\omega \triangleq |\mu_2| + e^{-\epsilon} \cdot \delta$ and let $\top$ and $\perp$ be fresh symbols. For any set X, define $X^\top$ and $X^\perp$ resp. as $\{x^\top \mid x \in X\}$ and $\{x^\perp \mid x \in X\}$. Let $\mathcal{N}$ be the flow network of Figure 1 whose resp. source and sink are $\top$ and $\perp$, whose set of vertices V is $\{\top, \perp\} \uplus (A^\star)^\top \uplus (B^\star)^\perp$, and whose set of edges E is $E_\top \uplus E_\perp \uplus E_\mathcal{R} \uplus E_\star$ with

$$E_\top \triangleq \{\top \mapsto_{\mu_1(a)} a^\top \mid a \in A\} \qquad E_\perp \triangleq \{b^\perp \mapsto_{e^{-\epsilon}\mu_2(b)} \perp \mid b \in B\}$$
$$E_\mathcal{R} \triangleq \{a^\top \mapsto_\infty b^\perp \mid a \mathcal{R} b \vee a = \star \vee b = \star\} \quad E_\star \triangleq \{\top \mapsto_{(\omega - e^{-\epsilon}|\mu_1|)} \star^\top,\ \star^\perp \mapsto_{e^{-\epsilon}\delta} \perp\}.$$

Let C be a cut of $\mathcal{N}$ — in the following, we use C independently for the cut C and its cut-set $\mathcal{E}(C)$. We check $|C| \geq \omega$. If $C \cap E_\mathcal{R} \neq \emptyset$ then $|C| = \infty$. Note that $C \cap E_\star = \emptyset$ implies

$C \cap E_{\mathcal{R}} \neq \emptyset$. If $(\top, \star^{\top}) \in C$ and $(\bot, \star^{\bot}) \notin C$ then we must have $E_{\top} \subseteq C$. This implies that $|C| \geq \omega$ since $E_{\top} \uplus \{(\top, \star^{\top})\}$ is a cut with capacity ω. If $(\top, \star^{\top}) \notin C$ and $(\bot, \star^{\bot}) \in C$ then we have $|C| \geq \omega$ in the similar way as above. Otherwise (i.e. $C \cap E_{\mathcal{R}} = \emptyset$ and $E_{\star} \subseteq C$), for C to be a cut, we must have $\mathcal{R}(A - A^{\dagger}) \subseteq B^{\dagger}$ where $A^{\dagger} \triangleq \{x \in A \mid (\top, x^{\top}) \in C\}$ and $B^{\dagger} \triangleq \{y \in B \mid (y^{\bot}, \bot) \in C\}$. Thus,

$$
\begin{aligned}
|C| &= e^{-\epsilon} \cdot \mu_1[A^{\dagger}] + \mu_2[B^{\dagger}] + |E_{\star}| \\
&\geq e^{-\epsilon} \cdot \mu_1[A^{\dagger}] + \mu_2[\mathcal{R}(A - A^{\dagger})] + e^{-\epsilon} \cdot \delta + (\omega - e^{-\epsilon} \cdot |\mu_1|) \\
&\geq e^{-\epsilon} \cdot (\mu_1[A^{\dagger}] + \mu_1[A - A^{\dagger}]) + \omega - e^{-\epsilon} \cdot |\mu_1| = \omega.
\end{aligned}
$$

Hence, $E_{\top} \uplus \{(\star^{\bot}, \bot)\}$ is a minimum cut with capacity ω. By Theorem 18, we obtain a maximum flow f with mass ω. Note that the flow f saturates the capacity of all edges in $E_{\top}$, $E_{\bot}$, and $E_{\star}$. Let $\hat{f} : (a, b) \in A^{\star} \times B^{\star} \mapsto f(a^{\top}, b^{\bot})$. We now define the following distributions:

$$
\begin{aligned}
\eta_{\triangleleft} &: A \times B^{\star} \to \mathbb{R}^{+} & \eta_{\triangleright} &: A^{\star} \times B \to \mathbb{R}^{+} \\
&(a, b) \mapsto e^{\epsilon} \cdot \hat{f}(a, b) & &(a, b) \mapsto \hat{f}(a, b).
\end{aligned}
$$

We clearly have $\pi_1^{\sharp}(\eta_{\triangleleft}) = \mu_1$ and $\pi_2^{\sharp}(\eta_{\triangleright}) = \mu_2$. Moreover, by construction of the flow network $\mathcal{N}$, $\mathrm{supp}(\hat{f}_{|A \times B}) \subseteq \mathcal{R}$. Hence, $\mathrm{supp}(\eta_{\triangleleft|A \times B}), \mathrm{supp}(\eta_{\triangleright|A \times B}) \subseteq \mathcal{R}$. It remains to show that $\Delta_{\epsilon}(\overline{\eta_{\triangleleft}}, \overline{\eta_{\triangleright}}) \leq \delta$. Let X be a subset of $A^{\star} \times B^{\star}$. Let $\overline{X_a} \triangleq \{a \in A \mid (a, \star) \in X\}$, $\overline{X_b} \triangleq \{b \in B \mid (\star, b) \in X\}$ and $\overline{X} \triangleq X \cap (A \times B)$. Then,

$$
\begin{aligned}
\overline{\eta_{\triangleleft}}[X] - e^{\epsilon} \cdot \overline{\eta_{\triangleright}}[X] &= e^{\epsilon}\left(\hat{f}[\overline{X}] + \hat{f}[\overline{X_a} \times \{\star\}]\right) - e^{\epsilon}\left(\hat{f}[\overline{X}] + \hat{f}[\{\star\} \times \overline{X_b}]\right) \\
&\leq e^{\epsilon} \cdot \hat{f}[\overline{X_a} \times \{\star\}] \leq e^{\epsilon} \cdot \hat{f}[A \times \{\star\}] = \delta.
\end{aligned}
$$

The last equality holds by Kirchhoff's law: $\hat{f}[A \times \{\star\}] = \sum_{a \in A} f(a^{\top}, \star^{\bot}) = f(\star^{\bot}, \bot) = e^{-\epsilon} \cdot \delta$. ◀

4 Properties of ⋆-Liftings

Our main theorem can be used to show a variety of natural properties of ⋆-liftings. To begin, we can generalize the mapping property from Theorem 6, lifting the requirement that the maps must be surjective.

▶ **Lemma 20.** *Let $\mu_1 \in \mathbb{D}(A_1)$, $\mu_2 \in \mathbb{D}(A_2)$, $f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$ and $\mathcal{R}$ a binary relation on B_1 & B_2. Let $\mathcal{S}$ such that $a_1 \,\mathcal{S}\, a_2 \overset{\triangle}{\iff} f_1(a_1) \,\mathcal{R}\, f_2(a_2)$. Then*

$$
f_1^{\sharp}(\mu_1) \,\mathcal{R}^{(\star)}_{\epsilon,\delta}\, f_2^{\sharp}(\mu_2) \iff \mu_1 \,\mathcal{S}^{(\star)}_{\epsilon,\delta}\, \mu_2.
$$

Proof. See Appendix, p. 15 ◀

Similarly, we can generalize the existing rules for up-to-bad reasoning (cf. Barthe et al. [4, Theorem 13]), which restrict the post-condition to be equality. There are two versions: the conditional event is either on the left side, or the right side. Note that the resulting index $\overline{\delta}$ are different in the two cases.

▶ **Lemma 21.** *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$, $\theta \subseteq A$ and $\mathcal{R} \subseteq A \times B$. Assume that $\mu_1 \; (\theta_{\triangleleft} \implies \mathcal{R})^{(\star)}_{\epsilon,\delta} \; \mu_2$ for some parameters $\epsilon, \delta \geq 0$. Then, $\mu_1 \,\mathcal{R}^{(\star)}_{\epsilon,\overline{\delta}}\, \mu_2$, where $\overline{\delta} \triangleq \delta + \mu_1[\overline{\theta}]$.*

Proof. See Appendix, p. 15 ◀

▶ **Lemma 22.** *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$, $\theta \subseteq B$ and $\mathcal{R} \subseteq A \times B$. Assume that $\mu_1\ (\theta_{\triangleright} \implies \mathcal{R})^{(\star)}_{\epsilon,\delta}\ \mu_2$ for some parameters $\epsilon, \delta \geq 0$. Then, $\mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\overline{\delta}}\ \mu_2$, where $\overline{\delta} \triangleq \delta + e^{\epsilon} \cdot \mu_2[\overline{\theta}]$.*

Proof. See Appendix, p. 16 ◀

As a consequence, an approximately lifted relation can be conjuncted with a one-sided predicate if the δ parameter is increased. This principle is useful for constructing approximate liftings that express *accuracy* bounds: when $\theta_{a,\triangleleft}$ is an event that happens with high probability, we can assume that $\theta_{a,\triangleleft}$ holds if we increase the δ parameter of the approximate lifting.

▶ **Lemma 23.** *Let $\mu_1 \in \mathbb{D}(A)$, $\mu_2 \in \mathbb{D}(B)$, $\theta_a \subseteq A$, $\theta_b \subseteq B$ and $\mathcal{R} \subseteq A \times B$. Assume that $\mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\delta}\ \mu_2$. Then, $\mu_1\ (\theta_{a,\triangleleft} \wedge \mathcal{R})^{(\star)}_{\epsilon,\delta_a}\ \mu_2$ and $\mu_1\ (\theta_{b,\triangleright} \wedge \mathcal{R})^{(\star)}_{\epsilon,\delta_b}\ \mu_2$ where $\delta_a \triangleq \delta + \mu_1[\overline{\theta_a}]$ and $\delta_b \triangleq \delta + e^{\epsilon} \cdot \mu_2[\overline{\theta_b}]$.*

Proof. See Appendix, p. 16 ◀

$\star$-liftings also support a significant generalization of optimal subset coupling. Unlike the known construction for 2-liftings (Theorem 7), the two subsets need not be nested, and either subset may be the entire domain. Furthermore, the distributions μ_1, μ_2 need not be the same, or even have the same domain. Finally, the equivalence is valid for any parameters (ϵ, δ), not just $\delta = 0$.

▶ **Theorem 24.** *Let $\mu_1 \in \mathbb{D}(A_1)$, $\mu_2 \in \mathbb{D}(A_2)$ and consider two subsets $P_1 \subseteq A_1, P_2 \subseteq A_2$. Then, we have the following equivalence:*

$$\mathbb{P}_{\mu_1}[P_1] \leq e^{\epsilon} \cdot \mathbb{P}_{\mu_2}[P_2] + \delta \wedge \mathbb{P}_{\mu_1}[A_1 - P_1] \leq e^{\epsilon} \cdot \mathbb{P}_{\mu_2}[A_2 - P_2] + \delta \iff \mu_1\ \mathcal{R}^{(\star)}_{\epsilon,\delta}\ \mu_2,$$

where $a_1\ \mathcal{R}\ a_2 \overset{\triangle}{\iff} a_1 \in P_1 \iff a_2 \in P_2$.

Proof. Immediate by Theorem 19. ◀

We can then recover the existing notion of optimal subset coupling [4] for $\star$-liftings, as a special case of the previous theorem.

▶ **Corollary 25** (Barthe et al. [4])**.** *Let $\mu \in \mathbb{D}(A)$ and consider two nested subsets $P_2 \subseteq P_1 \subsetneq A$. Then, we have the following equivalence:*

$$\mathbb{P}_{\mu}[P_1] \leq e^{\epsilon} \cdot \mathbb{P}_{\mu}[P_2] \iff \mu_1\ \mathcal{R}^{(\star)}_{\epsilon,0}\ \mu_2,$$

where $a_1\ \mathcal{R}\ a_2 \overset{\triangle}{\iff} a_1 \in P_1 \iff a_2 \in P_2$.

Proof. Immediate by Theorem 24, noting that

$$\mathbb{P}_{\mu}[A - P_1] \leq e^{\epsilon} \cdot \mathbb{P}_{\mu}[A - P_2]$$

is automatic since $P_2 \subseteq P_1$ implies $\mathbb{P}_{\mu}[A - P_1] \leq \mathbb{P}_{\mu}[A - P_2]$. ◀

Finally, we can directly extend known composition theorems from differential privacy to $\star$-liftings. This connection is quite useful for lifting existing results from the privacy literature–which can be quite sophisticated—to approximate liftings.

▶ **Lemma 26.** *Pose $\mathbb{R}^+_2 \triangleq \mathbb{R}^+ \times \mathbb{R}^+$ and let $(\mathbb{R}^+_2)^*$ be the set of finite sequences over $\mathbb{R}^+_2$. Let $r : (\mathbb{R}^+_2)^* \to \mathbb{R}^+_2$ be a* DP-composition operator*, i.e. r is an operator such that for any sets A, D and family $\{f_i : D \times A \to \mathbb{D}(A)\}_{i<n}$ of functions, if for every $a \in A$ and $i < n$,*

$f_i(-,a) : D \to \mathbb{D}(A)$ is (ϵ_i, δ_i)-differentially private for some parameters $\epsilon_i, \delta_i \geq 0$ and fixed adjacency relation ϕ, then, for any $a \in A$, $F(-,a)$ is (ϵ^*, δ^*)-differentially private for ϕ, where $F : (d,a) \mapsto (\bigcirc_{i<n} (f_i(d,-))^\sharp)(\mathbb{1}_a)$ is the the n-fold composition of the $[f_i]_{i<n}$ and $(\epsilon^*, \delta^*) \triangleq r([(\epsilon_i, \delta_i)]_{i<n})$.

Let $n \in \mathbb{N}$ and assume given two families of sets $\{A_i\}_{i \leq n}$ and $\{B_i\}_{i \leq n}$, together with a family of binary relations $\{\mathcal{R}(i) \subseteq A_i \times B_i\}_{i \leq n}$. Fix two families of functions $\{g_i : A_i \to \mathbb{D}(A_{i+1})\}_{i<n}$ and $\{h_i : B_i \to \mathbb{D}(B_{i+1})\}_{i<n}$ s.t. for any $i < n$ and $(a,b) \in \mathcal{R}(i)$ we have:

1. *$g_i(a) \; \mathcal{R}(i+1)^{(\star)}_{\epsilon_i,\delta_i} \; h_i(b)$ for some parameters $\epsilon_i, \delta_i \geq 0$, and*
2. *$g_i(a)$ and $h_i(b)$ are proper distributions.*

Then, for $(a_0, b_0) \in \mathcal{R}_0$, there exists a ⋆-lifting

$$G(a_0) \; \mathcal{R}(n)^{(\star)}_{\epsilon^*,\delta^*} \; H(b_0)$$

where $(\epsilon^*, \delta^*) \triangleq r([(\epsilon_i, \delta_i)]_{i<n})$, and $G : A_0 \to \mathbb{D}(A_n)$ and $H : B_0 \to \mathbb{D}(B_n)$ are the n-fold compositions of $[g_i]_{i \leq n}$ and $[h_i]_{i \leq n}$ respectively — i.e. $G(a) \triangleq (\bigcirc_{i<n} g_i^\sharp)(\mathbb{1}_a)$ and $H(b) \triangleq (\bigcirc_{i<n} h_i^\sharp)(\mathbb{1}_b)$.

For some of the more sophisticated composition results (notably, the advanced composition theorem by Dwork et al. [8]), Lemma 26 is not quite strong enough and requires a slight adaptation of the notion of ⋆-lifting. We refer to the full version of the paper for more details.

5 Comparison with Existing Approximate Liftings

Now that we have seen ⋆-liftings, we briefly consider other definitions of approximate liftings. We have already seen 2-liftings, which involve two witnesses (Definition 5). Evidently, ⋆-liftings strictly generalize 2-liftings.

▶ **Theorem 27.** *For all binary relations $\mathcal{R}$ over A & B and parameters $\epsilon, \delta \geq 0$, we have $\mathcal{R}^{(2)}_{\epsilon,\delta} \subseteq \mathcal{R}^{(\star)}_{\epsilon,\delta}$. There exist relations and parameters where the inclusion is strict.*

Proof. The inclusion $\mathcal{R}^{(2)}_{\epsilon,\delta} \subseteq \mathcal{R}^{(\star)}_{\epsilon,\delta}$ is immediate. We have a strict inclusion $\mathcal{R}^{(2)}_{\epsilon,\delta} \subsetneq \mathcal{R}^{(\star)}_{\epsilon,\delta}$ even for $\delta = 0$ by considering the optimal subset coupling from Theorem 7. Consider a distribution μ over set A, and let $P_1 \subseteq P_2 = A$. There is an $(\epsilon, 0)$-approximate ⋆-lifting (by Theorem 24), but a $(\epsilon, 0)$-approximate 2-lifting does not exist if μ has non-zero mass outside of P_1: the first witness $\mu_\triangleleft$ must place non-zero mass at (a_1, a_2) with $a_1 \notin P_1$ in order to have $\pi_1^\sharp(\mu_\triangleleft) = \mu$, but we must have $a_2 \notin P_2$ for the support requirement, and there is no such a_2. ◀

It is more interesting to compare ⋆-liftings with the original definitions of (ϵ, δ)-approximate lifting, by Barthe et al. [3]. They introduce two notions, a symmetric lifting and an asymmetric lifting, each using a single witness distribution. We will focus on the asymmetric version.

▶ **Definition 28** (Barthe et al. [3]). Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. An (ϵ, δ)-*approximate* 1-*lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a sub-distribution $\mu \in \mathbb{D}(A \times B)$ s.t.

1. $\pi_1^\sharp(\mu) \leq \mu_1$ and $\pi_2^\sharp(\mu) \leq \mu_2$;
2. $\Delta_\epsilon(\mu_1, \pi_1^\sharp(\mu)) \leq \delta$; and
3. $\mathrm{supp}(\mu) \subseteq \mathcal{R}$.

In the first point we take the point-wise order on sub-distributions: if μ and μ' are sub-distributions over X, then $\mu \leq \mu'$ when $\mu(x) \leq \mu'(x)$ for all $x \in X$. We will write $\mu_1 \; \mathcal{R}^{(1)}_{\epsilon,\delta} \; \mu_2$ if there exists an (ϵ, δ)-approximate 1-lifting of μ_1 & μ_2 for $\mathcal{R}$; the (1) indicates that there is one witness for this lifting.

1-liftings bear a close resemblance to *probabilistic couplings* from probability theory, which also have a single witness. However, 1-liftings are less well-understood theoretically than 2-liftings—basic properties such as mapping (Theorem 20) are not known to hold; the subset coupling (Theorem 7) is not known to exist. Somewhat surprisingly, 1-liftings are equivalent to $\star$-liftings (and hence by Theorem 19, also to Sato's approximate lifting).

▶ **Theorem 29.** *For all binary relations $\mathcal{R}$ over A & B and parameters $\epsilon, \delta \geq 0$, we have* $\mathcal{R}^{(1)}_{\epsilon,\delta} = \mathcal{R}^{(\star)}_{\epsilon,\delta}$.

Proof. See Appendix, p. 16 ◀

6 $\star$-Lifting for f-Divergences

The definition of $\star$-lifting can be extended to lifting constructions based on general f-divergences, as previously proposed by Barthe and Olmedo [2], Olmedo [10]. Roughly, a f-divergence a function $\Delta_f(\mu_1, \mu_2)$ that measures the difference between two probability distributions μ_1 and μ_2. Much like we generalized their definition for (ϵ, δ)-liftings, we can define $\star$-lifting with f-divergences. Before going any further, let us first define formally f-divergences. We denote by $\mathcal{F}$ the set of non-negative convex functions vanishing at 1: $\mathcal{F} = \{f : \mathbb{R}^+ \to \mathbb{R}^+ \mid f(1) = 0\}$. We also adopt the following notational conventions: $0 \cdot f(0/0) \triangleq 0$, and $0 \cdot f(x/0) \triangleq x \cdot \lim_{t \to 0^+} t \cdot f(1/t)$; we write L_f for the limit.

▶ **Definition 30.** Given $f \in \mathcal{F}$, the f-*divergence* $\Delta_f(\mu_1, \mu_2)$ between two distributions μ_1 and μ_2 in $\mathbb{D}(A)$ is defined as:

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

Examples of f-divergences include statistical distance ($f(t) = \frac{1}{2}|t-1|$), Kullback-Leibler divergence ($f(t) = \ln(t) - t + 1$), and Hellinger distance ($f(t) = \frac{1}{2}(\sqrt{t}-1)^2$).

▶ **Definition 31** ($\star$-lifting for f-divergences)**.** Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be distributions, $\mathcal{R}$ be a binary relation over A & B, and $f \in \mathcal{F}$. An $(f; \delta)$-*approximate lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a pair of distributions $\eta_\triangleleft \in \mathbb{D}(A \times B^\star)$ and $\eta_\triangleright \in \mathbb{D}(A^\star \times B)$ s.t.

- $\pi_1^\sharp(\eta_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\eta_\triangleright) = \mu_2$;
- $\mathrm{supp}(\eta_{\triangleleft|A\times B}), \mathrm{supp}(\eta_{\triangleright|A\times B}) \subseteq \mathcal{R}$; and
- $\Delta_f(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) \leq \delta$,

where $\overline{\eta_\bullet}$ is the canonical lifting of $\eta_\bullet$ to $A^\star \times B^\star$. We will write: $\mu_1 \; R^{(\star)}_{f;\delta} \; \mu_2$ if there exists an $(f; \delta)$-approximate lifting of μ_1 & μ_2 for $\mathcal{R}$.

$\star$-liftings for f-divergences compose sequentially.

▶ **Lemma 32.** *Suppose f has divergence statistical distance, Kullback-Leibler, or Hellinger distance. For $i \in \{1, 2\}$, let $\mu_i \in \mathbb{D}(A_i)$ and $\eta_i : A_i \to \mathbb{D}(B_i)$. Let $\mathcal{R}$ (resp. $\mathcal{S}$) be a binary relation over A_1 & A_2 (resp. over B_1 & B_2). If $\mu_1 \; \mathcal{R}^{(\star)}_{f;\delta} \; \mu_2$ for some $\delta \geq 0$ and for any $(a_1, a_2) \in \mathcal{R}$ we have $\eta_1(a_1) \; \mathcal{S}^{(\star)}_{f;\delta'} \; \eta_2(a_2)$ for some $\delta' \geq 0$, then*

$$\mathbb{E}_{\mu_1}[\eta_1] \; \mathcal{S}^{(\star)}_{f;\delta+\delta'} \; \mathbb{E}_{\mu_2}[\eta_2].$$

Much like the $\star$-liftings we saw before, $\star$-liftings for f-divergences have witness distributions with support determined by the support of μ_1 and μ_2 (cf. Lemma 10).

▶ **Lemma 33.** *Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be distributions such that $\mu_1 \, R^{(\star)}_{f;\delta} \, \mu_2$. Then, there are witnesses with support contained in* $\mathrm{supp}(\mu_1)^\star \times \mathrm{supp}(\mu_2)^\star$.

Proof. See Appendix, p. 17 ◀

Finally, the mapping property from Lemma 20 holds also for these $\star$-liftings. While the proof of Lemma 20 relies on the equivalence for Sato's definition, there is no such equivalence (or definition) for general f-divergences. Therefore, we must work directly with the witnesses of the approximate lifting.

▶ **Lemma 34.** *Let $\mu_1 \in \mathbb{D}(A_1)$, $\mu_2 \in \mathbb{D}(A_2)$, $g_1 : A_1 \to B_1$, $g_2 : A_2 \to B_2$ and $\mathcal{R}$ a binary relation on B_1 & B_2. Let $\mathcal{S}$ such that $a_1 \, \mathcal{S} \, a_2 \overset{\triangle}{\iff} g_1(a_1) \, \mathcal{R} \, g_2(a_2)$. Then*

$$g_1^\sharp(\mu_1) \, \mathcal{R}^{(\star)}_{f;\delta} \, g_2^\sharp(\mu_2) \iff \mu_1 \, \mathcal{S}^{(\star)}_{f;\delta} \, \mu_2.$$

Proof. See Appendix, p. 18 ◀

7 Conclusion

We have proposed a new definition of approximate lifting that unifies existing constructions and satisfies an approximate variant of Strassen's theorem. Our notion is useful both to simplify the soundness proof of existing program logics and to strengthen some of their proof rules. We see at least two important directions for future work. First, adapting existing program logics (for instance, apRHL [3]) to use $\star$-liftings, and formalizing examples that were out of reach of previous systems. Second, our notion of $\star$-liftings only applies when distributions have discrete support. It would be interesting to see if $\star$-liftings—and the approximate Strassen's theorem—can be generalized to the continuous setting.

Acknowledgments.

We thank the anonymous reviewers for their helpful suggestions. This work is partially supported by a grant from the NSF (TWC-1513694) and a grant from the Simons Foundation (#360368 to Justin Hsu).

References

1 R. Aharoni, E. Berger, A. Georgakopoulos, A. Perlstein, and P. Sprüssel. The max-flow min-cut theorem for countable networks. *J. Comb. Theory, Ser. B*, 101(1):1–17, 2011.

2 G. Barthe and F. Olmedo. Beyond differential privacy: Composition theorems and relational logic for f-divergences between probabilistic programs. In *International Colloquium on Automata, Languages and Programming (ICALP), Riga, Latvia*, volume 7966 of *Lecture Notes in Computer Science*, pages 49–60. Springer-Verlag, 2013.

3 G. Barthe, B. Köpf, F. Olmedo, and S. Zanella-Béguelin. Probabilistic relational reasoning for differential privacy. *ACM Transactions on Programming Languages and Systems*, 35 (3):9, 2013.

4 G. Barthe, N. Fong, M. Gaboardi, B. Grégoire, J. Hsu, and P.-Y. Strub. Advanced probabilistic couplings for differential privacy. In *ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria*, 2016.

5 G. Barthe, M. Gaboardi, B. Grégoire, J. Hsu, and P.-Y. Strub. Proving differential privacy via probabilistic couplings. In *IEEE Symposium on Logic in Computer Science (LICS), New York, New York*, 2016.

6 G. Barthe, M. Gaboardi, J. Hsu, and B. C. Pierce. Programming language techniques for differential privacy. *SIGLOG News*, 3(1):34–53, 2016.

7 C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *IACR Theory of Cryptography Conference (TCC), New York, New York*, pages 265–284, 2006.

8 C. Dwork, G. N. Rothblum, and S. Vadhan. Boosting and differential privacy. In *IEEE Symposium on Foundations of Computer Science (FOCS), Las Vegas, Nevada*, pages 51–60, 2010.

9 T. Lindvall. *Lectures on the coupling method*. Courier Corporation, 2002.

10 F. Olmedo. *Approximate Relational Reasoning for Probabilistic Programs*. PhD thesis, Universidad Politécnica de Madrid, 2014.

11 T. Sato. Approximate relational Hoare logic for continuous random samplings. In *Conference on the Mathematical Foundations of Programming Semantics (MFPS), Pittsburgh, Pennsylvania*, volume 325 of *Electronic Notes in Theoretical Computer Science*, pages 277–298. Elsevier, 2016.

12 V. Strassen. The existence of probability measures with given marginals. *The Annals of Mathematical Statistics*, pages 423–439, 1965.

13 H. Thorisson. *Coupling, Stationarity, and Regeneration*. Springer-Verlag, 2000.

14 C. Villani. *Optimal transport: old and new*. Springer-Verlag, 2008.

A Detailed Proofs

In the proofs, we will sometimes refer to the witnesses of a $\star$-lifting.

▶ **Notation 35.** Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. If two distributions $\eta_\triangleleft \in \mathbb{D}(A \times B^\star)$ and $\eta_\triangleright \in \mathbb{D}(A^\star \times B)$ are witnesses to the $\star$-lifting $\mu_1 \; \mathcal{R}^{(\star)}_{\epsilon,\delta} \; \mu_2$, then we write:

$$\langle \eta_\triangleleft, \eta_\triangleright \rangle \blacktriangleleft^{\mathcal{R}}_{\epsilon,\delta} \langle \mu_1 \,\&\, \mu_2 \rangle.$$

Proof of Lemma 10. Let $\mu_\triangleleft$ and $\mu_\triangleright$ be any pair of witnesses to the approximate lifting. We will construct witnesses $\eta_\triangleleft, \eta_\triangleright$ with the desired support. For ease of notation, let $S_i \triangleq \mathrm{supp}(\mu_i)$ for $i \in \{1, 2\}$. Define:

$$\eta_\triangleleft(a,b) = \begin{cases} \mu_\triangleleft(a,b) & : (a,b) \in S_1 \times S_2 \\ \mu_\triangleleft[a, B^\star - S_2] & : \end{cases}$$

$$\eta_\triangleright(a,b) = \begin{cases} \mu_\triangleright(a,b) & : (a,b) \in S_1 \times S_2 \\ \mu_\triangleright[A^\star - S_1, b] & : a = \star \end{cases}$$

Evidently, $\eta_\triangleleft$ and $\eta_\triangleright$ have support in $S_1^\star \times S_2^\star$. Additionally, it is straightforward to check that $\pi_1^\sharp(\eta_\triangleleft) = \pi_1^\sharp(\mu_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\eta_\triangleright) = \pi_2^\sharp(\mu_\triangleright) = \mu_2$ so $\eta_\triangleleft$ and $\eta_\triangleright$ have the desired marginals.

It only remains to check the distance condition. By the definition of the distance Δ_ϵ, we know that there are non-negative values $\delta(a,b)$ such that (i) $\overline{\mu_\triangleleft}(a,b) \le e^\epsilon \overline{\mu_\triangleright}(a,b) + \delta(a,b)$ and (ii) $\sum_{a,b} \delta(a,b) \le \delta$. We can define new constants:

$$\zeta(a,b) = \begin{cases} \delta(a,b) & : (a,b) \in S_1 \times S_2 \cup \{\star\} \times B \\ \delta[a, B^\star - S_2] & : b = \star. \end{cases}$$

Since $\overline{\mu_\triangleleft}(\star, b) = \overline{\eta_\triangleleft}(\star, b) = 0$ for all $b \in B^\star$, and $\overline{\mu_\triangleright}(a,b) = \overline{\eta_\triangleright}(a,b) = 0$ for all $b \notin S_2$, point (i) holds for the witnesses $\eta_\triangleleft, \eta_\triangleright$ and constants $\zeta(a,b)$. Since $\sum_{a,b} \zeta(a,b) = \sum_{a,b} \delta(a,b) \le \delta$, point (ii) holds as well. Hence, $\Delta_\epsilon(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) \le \delta$ and we have witnesses for the desired approximate lifting. ◀

Proof of Lemma 11. **($\Longrightarrow$)** Let P be (ϵ, δ)-differentially private for ϕ and $a_1, a_2 \in A$ s.t. $a_1 \; \phi \; a_2$. Let X be a subset of B. Then, by definition of differential privacy, we have $P(x)[X] \le e^\epsilon \cdot P(a)[X] + \delta = e^\epsilon \cdot P(a)[(=)(X)] + \delta$. Hence, by application of Theorem 19, we have $P(a_1) =^{(\star)}_{\epsilon,\delta} P(a_2)$.
($\Longleftarrow$) By application of Theorem 19, we have that

$$\forall a_1, a_2 \in A, \forall X \subseteq B. \, (a_1, a_2) \in \phi \implies P(a)[X] \le e^\epsilon \cdot P(a)[X] + \delta.$$

This is the definition of P being (ϵ, δ)-differentially private for ϕ. ◀

Proof of Lemma 12. ▬ Immediate.

▬ Let $\bar{\epsilon} \triangleq \epsilon + \epsilon'$ and $\bar{\delta} \triangleq \delta + e^\epsilon \cdot \delta'$. By Theorem 19, it is sufficient to show that $\mu_1(X) \le e^{\bar{\epsilon}} \cdot \mu_1(\mathcal{S}(\mathcal{R}(X))) + \bar{\delta}$ for any set X. We have:

$$\begin{aligned} \mu_1[X] &\le e^\epsilon \cdot \mu_2[\mathcal{R}(X)] + \delta && \text{(Theorem 19)} \\ &\le e^\epsilon \cdot (e^{\epsilon'} \cdot \mu_3[\mathcal{S}(\mathcal{R}(X))] + \delta') + \delta && \text{(Theorem 19)} \\ &= e^{\epsilon+\epsilon'} \cdot \mu_3[\mathcal{S}(\mathcal{R}(X))] + e^\epsilon \cdot \delta' + \delta. \end{aligned}$$

- We know that $\exists\, \langle \mu_\triangleleft, \mu_\triangleright \rangle \blacktriangleleft^{\mathcal{R}}_{\epsilon,\delta} \langle \mu_1 \,\&\, \mu_2 \rangle$. Likewise, for $a \triangleq (a_1, a_2) \in \mathcal{R}$, $\exists\, \langle \eta_{\triangleleft,a}, \eta_{\triangleright,a} \rangle \blacktriangleleft^{\mathcal{S}}_{\epsilon',\delta'} \langle \eta_1(a_1) \,\&\, \eta_2(a_2) \rangle$. Let $\eta_\triangleleft$ and $\eta_\triangleright$ be the following distribution constructors:

$$\eta_\triangleleft : a \mapsto \begin{cases} \eta_{\triangleleft,a} & \text{if } a \in \mathcal{R} \\ \mathbb{0} & \text{otherwise} \end{cases} \qquad \eta_\triangleright : a \mapsto \begin{cases} \eta_{\triangleright,a} & \text{if } a \in \mathcal{R} \\ \mathbb{0} & \text{otherwise} \end{cases}$$

and let $\xi_\triangleleft \triangleq \mathbb{E}_{\mu_\triangleleft}[\eta_\triangleleft]$ (resp. $\xi_\triangleright \triangleq \mathbb{E}_{\mu_\triangleright}[\eta_\triangleright]$). We now prove that:

$$\langle \xi_\triangleleft, \xi_\triangleright \rangle \blacktriangleleft^{\mathcal{S}}_{\epsilon+\epsilon',\delta+\delta'} \langle \mathbb{E}_{\mu_1}[\eta_1] \,\&\, \mathbb{E}_{\mu_2}[\eta_2] \rangle.$$

The marginal and support conditions are immediate. The distance condition is obtained by an immediate application of the previous point. ◀

Proof of Theorem 19. To show the forward direction of Theorem 19, let $X \subseteq A$ and $\mathcal{R}(X)^{\complement} = B - \mathcal{R}(X)$. Then, we have

$$\begin{aligned}
\mu_1[X] &= \pi_1^\sharp(\eta_\triangleleft)[X] = \eta_\triangleleft[X, B^\star] = \overline{\eta_\triangleleft}[X, B^\star] = \overline{\eta_\triangleleft}[X, \mathcal{R}(X) \uplus \mathcal{R}(X)^{\complement} \uplus \{\star\}] \\
&= \overline{\eta_\triangleleft}[X, \mathcal{R}(X) \uplus \{\star\}] + \underbrace{\overline{\eta_\triangleleft}[X, \mathcal{R}(X)^{\complement}]}_{=\,0} \le e^\epsilon \cdot \overline{\eta_\triangleright}[X, \mathcal{R}(X) \uplus \{\star\}] + \delta \\
&\le e^\epsilon \cdot \underbrace{\overline{\eta_\triangleright}[A^\star, \mathcal{R}(X)]}_{=\,\eta_\triangleright[A^\star, \mathcal{R}(X)]} + e^\epsilon \cdot \underbrace{\overline{\eta_\triangleright}[A^\star, \{\star\}]}_{=\,0} + \delta \\
&= e^\epsilon \cdot \pi_2^\sharp(\eta_\triangleright)[\mathcal{R}(X)] + \delta = e^\epsilon \cdot \mu_2[\mathcal{R}(X)] + \delta,
\end{aligned}$$

as desired. ◀

Proof of Lemma 20. **($\Longrightarrow$)** Assume that $f_1^\sharp(\mu_1)\; \mathcal{R}^{(\star)}_{\epsilon,\delta}\; f_2^\sharp(\mu_2)$ and let $X \subseteq A_1$. Then,

$$\begin{aligned}
\mu_1[X] &\le \mu_1[f_1^{-1}(f_1(X))] = f_1^\sharp(\mu_1)[f_1(X)] \\
&\le e^\epsilon \cdot f_2^\sharp(\mu_2)[\mathcal{R}(f_1(X))] + \delta && \text{(Theorem 19)} \\
&= e^\epsilon \cdot \mu_2[\underbrace{f_2^{-1}(\mathcal{R}(f_1(X)))}_{\subseteq \mathcal{S}(X)}] + \delta \le e^\epsilon \cdot \mu_2[\mathcal{S}\;(X)] + \delta.
\end{aligned}$$

Hence, by Theorem 19, $\mu_1\; \mathcal{S}^{(\star)}_{\epsilon,\delta}\; \mu_2$.
($\Longleftarrow$) Assume that $\mu_1\; \mathcal{S}^{(\star)}_{\epsilon,\delta}\; \mu_2$ and let $X \subseteq A_2$. Then,

$$\begin{aligned}
f_1^\sharp(\mu_1)[X] &= \mu_1[f_1^{-1}(X)] \\
&\le e^\epsilon \cdot \mu_2[\underbrace{\mathcal{S}\;(f_1^{-1}(X))}_{\subseteq f_2^{-1}(\mathcal{R}(X))}] + \delta \le e^\epsilon \cdot f_2^\sharp(\mu_2)[\mathcal{R}(X)] + \delta. && \text{(Theorem 19)}
\end{aligned}$$

Hence, by Theorem 19, $f_1^\sharp(\mu_1)\; \mathcal{R}^{(\star)}_{\epsilon,\delta}\; f_2^\sharp(\mu_2)$. ◀

Proof of Lemma 21. By Theorem 19, it is sufficient to prove that

$$\mu_1[X] \le e^\epsilon \cdot \mu_2[\mathcal{R}(X)] + \mu_1[\theta^{\complement}] + \delta$$

for any $X \subseteq A$. By direct computation:

$$\begin{aligned}
\mu_1[X] &= \mu_1[X \cap \theta] + \mu_1[X \cap \theta^{\complement}] \le \mu_1[X \cap \theta] + \mu_1[\theta^{\complement}] \\
&\le e^\epsilon \cdot \mu_2[\underbrace{(\theta_\triangleleft \implies \mathcal{R})(X \cap \theta)}_{=\,\mathcal{R}(X \cap \theta)\,\subseteq\,\mathcal{R}(X)}] + \delta + \mu_1[\theta^{\complement}] \\
&\le e^\epsilon \cdot \mu_2[\mathcal{R}(X)] + \mu_1[\theta^{\complement}] + \delta.
\end{aligned}$$

◀

Proof of Lemma 22. By Theorem 19, it is sufficient to prove that

$$\mu_1[X] \leq e^\epsilon \cdot \mu_2[\mathcal{R}(X)] + e^\epsilon \cdot \mu_2[\theta^\complement] + \delta$$

for any $X \subseteq A$. Let X be such a set, then:

$$\begin{aligned}
\mu_1[X] &\leq e^\epsilon \cdot \mu_2[(\theta_\triangleright \implies \mathcal{R})(X)] + \delta \\
&\leq e^\epsilon \cdot (\mu_2[(\theta_\triangleright \implies \mathcal{R})(X) \cap \theta] + \mu_2[\theta^\complement]) + \delta \\
&\leq \mu_2[\underbrace{(\theta_\triangleright \implies \mathcal{R})(X) \cap \theta}_{\subseteq \mathcal{R}(X) \cap \theta}] + e^\epsilon \cdot \mu_2[\theta^\complement] + \delta \\
&\leq \mu_2[\mathcal{R}(X)] + e^\epsilon \cdot \mu_2[\theta^\complement] + \delta.
\end{aligned}$$

◀

Proof of Lemma 23. From $\mu_1 \ \mathcal{R}^{(\star)}_{\epsilon,\delta} \ \mu_2$ and Lemma 12, we have $\mu_1 \ \mathcal{S}^{(\star)}_{\epsilon,\delta} \ \mu_2$ where $\mathcal{S} \triangleq \theta_{a,\triangleleft} \implies \theta_{a,\triangleleft} \wedge \mathcal{R}$. Hence, by Lemma 21, we obtain $\mu_1 \ (\theta_{a,\triangleleft} \wedge \mathcal{R})^{(\star)}_{\epsilon,\delta_a} \ \mu_2$. Using similar reasoning with $\theta_{b,\triangleright} \implies \theta_{b,\triangleright} \wedge \mathcal{R}$ and Lemma 22, we have $\mu_1 \ (\theta_{b,\triangleright} \wedge \mathcal{R})^{(\star)}_{\epsilon,\delta_b} \ \mu_2$. ◀

Proof of Theorem 29. Suppose that (μ_L, μ_R) are witnesses to $\mu_1 \ \mathcal{R}^{(\star)}_{\epsilon,\delta} \ \mu_2$. Define the witness $\eta \in \mathbb{D}(A \times B)$ as the point-wise minimum: $\eta(a,b) \triangleq \min(\mu_L(a,b), \mu_R(a,b))$. We will show that η is a witness to $\mu_1 \ \mathcal{R}^{(1)}_{\epsilon,\delta} \ \mu_2$.

The support condition follows from the support condition for (μ_L, μ_R). The marginal conditions $\pi_1^\sharp(\eta) \leq \mu_1$ and $\pi_2^\sharp(\eta) \leq \mu_2$ also follow by the marginal conditions for (μ_L, μ_R). The only thing to check is the distance condition. By the distance condition on (μ_L, μ_R), there exist non-negative values $\delta(a,b)$ such that

$$\mu_L(a,b) \leq \exp(\epsilon)\mu_R(a,b) + \delta(a,b)$$

and $\sum_{a,b} \delta(a,b) \leq \delta$. So, $\mu_R(a,b) \geq \exp(-\epsilon)(\mu_L(a,b) - \delta(a,b))$. Now let $S \subseteq A$ be any subset. Then:

$$\begin{aligned}
\mu_1(S) - \exp(\epsilon)\pi_1^\sharp(\eta)(S) &= \sum_{a \in S} \mu_1(a) - \exp(\epsilon) \sum_{b \in B} \min(\mu_L(a,b), \mu_R(a,b)) \\
&\leq \sum_{a \in S} \mu_1(a) - \exp(\epsilon) \sum_{b \in B} \exp(-\epsilon)(\mu_L(a,b) - \delta(a,b)) \\
&= \sum_{a \in S, b \in B} \delta(a,b) \leq \delta.
\end{aligned}$$

Thus, η witnesses $\mu_1 \ \mathcal{R}^{(1)}_{\epsilon,\delta} \ \mu_2$, so $\mathcal{R}^{(\star)}_{\epsilon,\delta} \subseteq \mathcal{R}^{(1)}_{\epsilon,\delta}$.

The other direction is more interesting. Let $\eta \in \mathbb{D}(A \times B)$ be the witness for $\mathcal{R}^{(1)}_{\epsilon,\delta}$. By the distance condition $\Delta_\epsilon(\mu_1, \pi_1^\sharp \eta) \leq \delta$, there exist non-negative values $\delta(a)$ such that

$$\mu_1(a) \leq \exp(\epsilon)\pi_1^\sharp \eta(a) + \delta(a)$$

with equality when $\delta(a)$ is strictly positive, and $\sum_{a \in A} \delta(a) \leq \delta$. Define two witnesses $\mu_L \in \mathbb{D}(A \times B^\star), \mu_R \in \mathbb{D}(A^\star \times B)$ as follows:

$$\mu_L(a,b) \triangleq \begin{cases} \eta(a,b) \cdot \frac{\mu_1(a) - \delta(a)}{\pi_1^\sharp \eta(a)} & : b \neq \star \\ \mu_1(a) - \sum_{b \in B} \mu_L(a,b) & : b = \star \end{cases}$$

$$\mu_R(a,b) \triangleq \begin{cases} \eta(a,b) & : a \neq \star \\ \mu_2(b) - \sum_{a \in A} \mu_R(a,b) & : a = \star. \end{cases}$$

(As usual, if any denominator is zero, we take the probability to be zero as well.)

The support condition follows from the support condition of η. The marginal conditions hold by definition. Note that all probabilities are non-negative. For μ_L, note that if $\delta(a) > 0$ then $\mu_1(a) - \delta(a) = \exp(\epsilon)\pi_1^\sharp\eta(a) \geq 0$ and hence

$$\mu_L(a, \star) = \mu_1(a) - \delta(a) \geq 0.$$

assuming $\pi_1^\sharp\eta(a) > 0$; if $\pi_1^\sharp\eta(a) = 0$ then $\mu_L(a, \star) = 0$. For μ_R, non-negativity holds because $\pi_2^\sharp\eta \leq \mu_2$.

We show the distance bound. Note that when $a, b \neq \star$, by definition $\mu_L(a, b)$ and $\mu_R(a, b)$ are both strictly positive or both equal to zero, and $\eta(a, b)$ is strictly positive or equal to zero accordingly. If $\mu_L(a, b), \mu_R(a, b), \eta(a, b)$ are all strictly positive, then we know

$$\frac{\mu_L(a, b)}{\eta(a, b)} = \frac{\mu_1(a) - \delta(a)}{\pi_1^\sharp\eta(a)} \leq \exp(\epsilon).$$

Thus we always have

$$\mu_L(a, b) \leq \exp(\epsilon)\eta(a, b) = \exp(\epsilon)\mu_R(a, b).$$

We can also bound the mass on points $(a, \star)$. Let $S \subseteq A$ be any subset. Then:

$$\begin{aligned}\overline{\mu_L}(S \times \{\star\}) &= \sum_{a \in S} \mu_1(a) - \mu_1(a) \sum_{b \in B} \frac{\eta(a, b)}{\pi_1^\sharp\eta(a)} + \delta(a) \sum_{b \in B} \frac{\eta(a, b)}{\pi_1^\sharp\eta(a)} \\ &= \mu_1(S) - \mu_1(S) + \delta(S) \leq \exp(\epsilon)\overline{\mu_R}(S \times \{\star\}) + \delta.\end{aligned}$$

So $\Delta_\epsilon(\overline{\mu_L}, \overline{\mu_R}) \leq \delta$ as desired, and we have witnesses to $\mu_1 \; \mathcal{R}^{(\star)}_{\epsilon,\delta} \; \mu_2$. Hence, $\mathcal{R}^{(1)}_{\epsilon,\delta} \subseteq \mathcal{R}^{(\star)}_{\epsilon,\delta}$. ◀

Proof of Lemma 33. Let $\mu_\triangleleft$ and $\mu_\triangleright$ be any pair of witnesses to the approximate lifting. We will construct witnesses $\eta_\triangleleft, \eta_\triangleright$ with the desired support. For ease of notation, let $S_i \triangleq \mathrm{supp}(\mu_i)$ for $i \in \{1, 2\}$. Define:

$$\eta_\triangleleft(a, b) = \begin{cases} \mu_\triangleleft(a, b) & : (a, b) \in S_1 \times S_2 \\ \mu_\triangleleft[a, B^\star - S_2] & : b = \star \end{cases}$$

$$\eta_\triangleright(a, b) = \begin{cases} \mu_\triangleright(a, b) & : (a, b) \in S_1 \times S_2 \\ \mu_\triangleright[A^\star - S_1, b] & : a = \star \end{cases}$$

Evidently, $\eta_\triangleleft$ and $\eta_\triangleright$ have support in $S_1^\star \times S_2^\star$. Additionally, it is straightforward to check that $\pi_1^\sharp(\eta_\triangleleft) = \pi_1^\sharp(\mu_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\eta_\triangleright) = \pi_2^\sharp(\mu_\triangleright) = \mu_2$ so $\eta_\triangleleft$ and $\eta_\triangleright$ have the desired marginals.

It only remains to check the distance condition. We can compute:

$$\begin{aligned}\Delta_f(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) &= \sum_{(a,b) \in S_1 \times S_2} \eta_\triangleright(a, b) \cdot f\left(\frac{\eta_\triangleleft(a, b)}{\eta_\triangleright(a, b)}\right) \\ &\quad + \sum_{a \in S_1} \eta_\triangleright(a, \star) \cdot f\left(\frac{\eta_\triangleleft(a, \star)}{\eta_\triangleright(a, \star)}\right) + \sum_{b \in S_2} \eta_\triangleright(\star, b) \cdot f\left(\frac{\eta_\triangleleft(\star, b)}{\eta_\triangleright(\star, b)}\right) \\ &= \sum_{(a,b) \in S_1 \times S_2} \mu_\triangleright(a, b) \cdot f\left(\frac{\mu_\triangleleft(a, b)}{\mu_\triangleright(a, b)}\right) + \sum_{a \in S_1} \eta_\triangleleft(a, \star) \cdot L_f + \sum_{b \in S_2} \eta_\triangleright(\star, b) \cdot f(0) \\ &= \sum_{(a,b) \in S_1 \times S_2} \mu_\triangleright(a, b) \cdot f\left(\frac{\mu_\triangleleft(a, b)}{\mu_\triangleright(a, b)}\right) \\ &\quad + \sum_{a \in S_1} \sum_{b' \in B^\star - S_2} \mu_\triangleleft(a, b') \cdot L_f + \sum_{b \in S_2} \sum_{a' \in A^\star - S_1} \mu_\triangleright(a', b) \cdot f(0)\end{aligned}$$

Now, note that for all $b' \in B^\star - S_2$, we know $\mu_\triangleright(a, b') = 0$. Similarly, for all $a' \in A^\star - S_1$, we know $\mu_\triangleleft(a', b) = 0$. Hence, the last line is equal to

$$\begin{aligned}
\Delta_f(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) = &\sum_{(a,b)\in S_1\times S_2} \mu_\triangleright(a, b) \cdot f\left(\frac{\mu_\triangleleft(a, b)}{\mu_\triangleright(a, b)}\right) \\
&+ \sum_{a\in S_1} \sum_{b'\in B^\star - S_2} \mu_\triangleright(a, b') \cdot f\left(\frac{\mu_\triangleleft(a, b')}{\mu_\triangleright(a, b')}\right) \\
&\quad + \sum_{b\in S_2} \sum_{a'\in A^\star - S_1} \mu_\triangleright(a', b) \cdot f\left(\frac{\mu_\triangleleft(a', b)}{\mu_\triangleright(a', b)}\right) \\
&= \Delta_f(\overline{\mu_\triangleleft}, \overline{\mu_\triangleright}) \leq \delta.
\end{aligned}$$

Thus, $\eta_\triangleleft$ and $\eta_\triangleright$ witness the desired $\star$-lifting. ◀

Proof of Lemma 34. For the reverse direction, take the witnesses $\mu_\triangleleft, \mu_\triangleright \in \mathbb{D}(A^\star \times A^\star)$ and define witnesses $\nu_\triangleleft \triangleq (g_1^\star \times g_2^\star)^\sharp\ (\mu_\triangleleft)$ and $\nu_\triangleright \triangleq (g_1^\star \times g_2^\star)^\sharp\ (\mu_\triangleright)$, where $g_1^\star \times g_2^\star$ takes a pair (a_1, a_2) to the pair $(g_1(a_1), g_2(a_2))$ and maps $\star$ to $\star$. The support and marginal requirements are clear. The only thing to check is the distance condition, but this follows from monotonicity of f-divergences—under the mapping $g_1^\star \times g_2^\star : A^\star \times A^\star \to B^\star \times B^\star$, the f-divergence can only decrease (see, e.g., **?**]).

For the forward direction, let $\nu_\triangleleft, \nu_\triangleright \in \mathbb{D}(B^\star \times B^\star)$ be the witnesses to the second lifting. By Lemma 33, we may assume without loss of generality that $\mathrm{supp}(\nu_\triangleleft)$ and $\mathrm{supp}(\nu_\triangleright)$ are contained in

$$\mathrm{supp}(g_1^\sharp\ (\mu_1))^\star \times \mathrm{supp}(g_2^\sharp\ (\mu_2))^\star \subseteq g_1(A)^\star \times g_2(A)^\star.$$

We aim to construct a pair of witnesses $\mu_\triangleleft, \mu_\triangleright \in \mathbb{D}(A^\star \times A^\star)$ to the first lifting. The basic idea is to define $\mu_\triangleleft$ and $\mu_\triangleright$ based on equivalence classes of elements in A mapping to a particular $b \in B$, and then smooth out the probabilities within each equivalence class. To begin, for $a \in A$, define $[a]_g \triangleq g^{-1}(g(a))$ and $\alpha_i(a) \triangleq \Pr_{\mu_i}[\{a\} \mid [a]_{g_i}]$. We take $\alpha_i(a) = 0$ when $\mu_i([a]_{f_i}) = 0$, and we let $\alpha_i(\star) = 0$. We define $\mu_\triangleleft$ and $\mu_\triangleright$ as

$$\begin{aligned}
&\mu_\triangleleft : (a_1, a_2) \mapsto \alpha_\triangleleft(a_1, a_2) \cdot \nu_\triangleleft(g_1(a_1), g_2(a_2)) \\
&\mu_\triangleright : (a_1, a_2) \mapsto \alpha_\triangleright(a_1, a_2) \cdot \nu_\triangleright(g_1(a_1), g_2(a_2))
\end{aligned}$$

where

$$\alpha_\triangleleft(a_1, a_2) = \begin{cases} \alpha_1(a_1) \cdot \alpha_2(a_2) & : a_2 \neq \star \\ \alpha_1(a_1) & : a_2 = \star, \end{cases} \qquad \alpha_\triangleright(a_1, a_2) = \begin{cases} \alpha_1(a_1) \cdot \alpha_2(a_2) & : a_1 \neq \star \\ \alpha_2(a_2) & : a_1 = \star. \end{cases}$$

The support and marginal conditions follow from the support and marginal conditions of $\nu_\triangleleft$, $\nu_\triangleright$. For instance:

$$\begin{aligned}
\sum_{a_2\in A^\star} \mu_\triangleleft(a_1, a_2) &= \sum_{a_2\in A^\star} \alpha_\triangleleft(a_1, a_2)\nu_\triangleleft(g_1(a_1), g_2(a_2)) \\
&= \alpha_1(a_1)\nu_\triangleleft(g_1(a_1), \star) + \sum_{a_2\in A} \alpha_1(a_1)\alpha_2(a_2)\nu_\triangleleft(g_1(a_1), g_2(a_2)) \\
&= \alpha_1(a_1)\left(\nu_\triangleleft(g_1(a_1), \star) + \sum_{b_2\in g_2(A)} \nu_\triangleleft(g_1(a_1), b_2) \sum_{a_2\in g_2^{-1}(b_2)} \alpha_2(a_2)\right) \\
&= \alpha_1(a_1) \sum_{b_2\in B^\star} \nu_\triangleleft(g_1(a_1), b_2) = \alpha_1(a_1)\mu_1([a_1]_{g_1}) = \mu_1(a_1).
\end{aligned}$$

In the last line, we replace the sum over $b_2 \in g_2(A^\star)$ with a sum over $b_2 \in B^\star$; this holds since the support of $g_2^\sharp(\mu_2)$ is contained in $g_2(A)$, so we can assume that $\nu_\triangleleft(a, b_2) = 0$ for all b_2 outside of $g_2(A^\star)$. Then, we can conclude by the marginal condition $\pi_1^\sharp(\nu_\triangleleft) = g_1^\sharp(\mu_1)$. The second marginal is similar.

We now check the distance condition $\Delta_f(\overline{\mu_\triangleleft}, \overline{\mu_\triangleright}) \leq \delta$. We can split the f-divergence into $\Delta_f(\overline{\mu_\triangleleft}, \overline{\mu_\triangleright}) = P_0 + P_1 + P_2 + P_3$, where

$$P_0 \triangleq \mu_\triangleright(\star,\star) \cdot f\left(\frac{\mu_\triangleleft(\star,\star)}{\mu_\triangleright(\star,\star)}\right) \qquad P_1 \triangleq \sum_{(a_1,a_2)\in A\times A} \mu_\triangleright(a_1,a_2) \cdot f\left(\frac{\mu_\triangleleft(a_1,a_2)}{\mu_\triangleright(a_1,a_2)}\right)$$

$$P_2 \triangleq \sum_{a_1\in A} \mu_\triangleright(a_1,\star) \cdot f\left(\frac{\mu_\triangleleft(a_1,\star)}{\mu_\triangleright(a_1,\star)}\right) \qquad P_3 \triangleq \sum_{a_2\in A} \mu_\triangleright(\star,a_2) \cdot f\left(\frac{\mu_\triangleleft(\star,a_2)}{\mu_\triangleright(\star,a_2)}\right)$$

We will handle each term separately. Evidently $P_0 = 0$. For P_1, we have:

$$\begin{aligned}
P_1 &= \sum_{(a_1,a_2)\in A\times A} \alpha_\triangleright(a_1,a_2)\nu_\triangleright(g_1(a_1),g_2(a_2)) \cdot f\left(\frac{\alpha_\triangleleft(a_1,a_2)\nu_\triangleleft(g_1(a_1),g_2(a_2))}{\alpha_\triangleright(a_1,a_2)\nu_\triangleright(g_1(a_1),g_2(a_2))}\right) \\
&= \sum_{(a_1,a_2)|S^{=0}} \alpha_\triangleleft(a_1,a_2)\nu_\triangleleft(g_1(a_1),g_2(a_2)) \cdot L_f \\
&\quad + \sum_{(a_1,a_2)|S^{\neq 0}} \alpha_\triangleright(a_1,a_2)\nu_\triangleright(g_1(a_1),g_2(a_2)) \cdot f\left(\frac{\nu_\triangleleft(g_1(a_1),g_2(a_2))}{\nu_\triangleright(g_1(a_1),g_2(a_2))}\right)
\end{aligned}$$

where the sets $S^{=0}$ and $S^{\neq 0}$ are defined as:

$$\begin{aligned}
S^{=0} &\triangleq \{(a_1,a_2) \mid \nu_\triangleright(g_1(a_1),g_2(a_2)) = 0\} \\
S^{\neq 0} &\triangleq \{(a_1,a_2) \mid \nu_\triangleright(g_1(a_1),g_2(a_2)) \neq 0\}.
\end{aligned}$$

By further rearranging:

$$\begin{aligned}
P_1 &= \sum_{(b_1,b_2)\in(g_1\times g_2)(S^{=0})} \nu_\triangleleft(b_1,b_2) \cdot L_f \left(\sum_{a_1\in g_1^{-1}(b_1)} \alpha_1(a_1)\right)\left(\sum_{a_2\in g_1^{-1}(b_2)} \alpha_2(a_2)\right) \\
&\quad + \sum_{(b_1,b_2)\in(g_1\times g_2)(S^{\neq 0})} \nu_\triangleright(b_1,b_2) \cdot f\left(\frac{\nu_\triangleleft(b_1,b_2)}{\nu_\triangleright(b_1,b_2)}\right)\left(\sum_{a_1\in g_1^{-1}(b_1)} \alpha_1(a_1)\right)\left(\sum_{a_2\in g_1^{-1}(b_2)} \alpha_2(a_2)\right) \\
&= \sum_{(b_1,b_2)\in(g_1\times g_2)(S^{=0})} \nu_\triangleleft(b_1,b_2) \cdot L_f + \sum_{(b_1,b_2)\in(g_1\times g_2)(S^{\neq 0})} \nu_\triangleright(b_1,b_2) \cdot f\left(\frac{\nu_\triangleleft(b_1,b_2)}{\nu_\triangleright(b_1,b_2)}\right) \\
&= \sum_{(b_1,b_2)\in(g_1\times g_2)(A\times A)} \nu_\triangleright(b_1,b_2) \cdot f\left(\frac{\nu_\triangleleft(b_1,b_2)}{\nu_\triangleright(b_1,b_2)}\right) \\
&= \sum_{(b_1,b_2)\in B\times B} \nu_\triangleright(b_1,b_2) \cdot f\left(\frac{\nu_\triangleleft(b_1,b_2)}{\nu_\triangleright(b_1,b_2)}\right).
\end{aligned}$$

The final equality is because without loss of generality, we can assume (by Lemma 33) that $\nu_\triangleleft, \nu_\triangleright$ are zero outside of the support of $g_1^\sharp(\mu_1)$ and $g_2^\sharp(\mu_2)$, which have support contained in $(g_1 \times g_2)(A \times A)$.

The remaining two terms P_2 and P_3 are simpler to bound. For P_2, note that $\overline{\mu_\triangleright}(a, \star) = 0$

for all $a \in A$. Thus:

$$P_2 = \sum_{a_1 \in A} \alpha_\triangleleft(a_1, \star)\nu_\triangleleft(g_1(a_1), \star) \cdot L_f = \sum_{b_1 \in g_1(A)} \sum_{a_1 \in g_1^{-1}(b_1)} \alpha_1(a_1)\nu_\triangleleft(b_1, \star) \cdot L_f$$
$$= \sum_{b_1 \in g_1(A)} \nu_\triangleleft(b_1, \star) \cdot L_f = \sum_{b_1 \in B} \nu_\triangleleft(b_1, \star) \cdot L_f = \sum_{b_1 \in B} \overline{\nu_\triangleright}(b_1, \star) \cdot f\left(\frac{\nu_\triangleleft(b_1, \star)}{\overline{\nu_\triangleright}(b_1, \star)}\right)$$

where the last equality is because $\overline{\nu_\triangleright}(b, \star) = 0$ for all $b \in B$.

Similarly for P_3, using $\overline{\mu_\triangleleft}(\star, a) = \overline{\nu_\triangleleft}(\star, b) = 0$ for all $a \in A$ and $b \in B$, we have:

$$P_3 = \sum_{a_2 \in A} \alpha_\triangleright(\star, a_2)\nu_\triangleright(\star, g_2(a_2)) \cdot f(0) = \sum_{b_2 \in g_2(A)} \sum_{a_2 \in g_2^{-1}(b_2)} \alpha_2(a_2)\nu_\triangleright(\star, b_2) \cdot f(0)$$
$$= \sum_{b_2 \in g_2(A)} \nu_\triangleright(\star, b_2) \cdot f(0) = \sum_{b_2 \in B} \nu_\triangleright(\star, b_2) \cdot f(0) = \sum_{b_2 \in B} \nu_\triangleright(\star, b_2) \cdot f\left(\frac{\overline{\nu_\triangleleft}(\star, b_2)}{\nu_\triangleright(\star, b_2)}\right).$$

Putting everything together, we conclude

$$\Delta_f(\overline{\mu_\triangleleft}, \overline{\mu_\triangleright}) = \Delta_f(\overline{\nu_\triangleleft}, \overline{\nu_\triangleright}) \leq \delta$$

by assumption, so $\mu_\triangleleft, \mu_\triangleright$ witness the desired approximate lifting. ◀

B Symmetric $\star$-lifting

The approximate liftings we have considered so far are all *asymmetric*. For instance, the approximate lifting $\mu_1 \, \mathcal{R}^{(\star)}_{\epsilon,\delta} \, \mu_2$ may not imply the lifting $\mu_2 \, (\mathcal{R}^{-1})^{(\star)}_{\epsilon,\delta} \, \mu_1$. Given witnesses (μ_L, μ_R) to the first lifting, we may consider the witnesses $(\nu_L, \nu_R) \triangleq (\mu_R^\top, \mu_L^\top)$ where the transpose map $(-)^\top : \mathbb{D}(A \times B) \to \mathbb{D}(B \times A)$ is defined in the obvious way. Then (ν_L, ν_R) almost witness the second lifting, except that the distance bound is in the opposite direction:

$$\Delta_\epsilon(\nu_R, \nu_L) = \Delta_\epsilon(\mu_L^\top, \mu_R^\top) = \Delta_\epsilon(\mu_L, \mu_R) \leq \delta.$$

In general, we cannot bound $\Delta_\epsilon(\nu_L, \nu_R)$ and the symmetric lifting $\mu_2 \, (\mathcal{R}^{-1})^{(\star)}_{\epsilon,\delta} \, \mu_1$ may not hold. To recover symmetry, we can define a symmetric version of $\star$-lifting.

▶ **Definition 36** (Symmetric $\star$-lifting)**.** Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. An (ϵ, δ)*-approximate symmetric $\star$-lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a pair of sub-distributions $\eta_\triangleleft \in \mathbb{D}(A \times B^\star)$ and $\eta_\triangleright \in \mathbb{D}(A^\star \times B)$ s.t.

1. $\pi_1^\sharp(\eta_\triangleleft) = \mu_1$ and $\pi_2^\sharp(\eta_\triangleright) = \mu_2$;
2. $\mathrm{supp}(\eta_{\triangleleft|A \times B}), \mathrm{supp}(\eta_{\triangleright|A \times B}) \subseteq \mathcal{R}$; and
3. $\Delta_\epsilon(\overline{\eta_\triangleleft}, \overline{\eta_\triangleright}) \leq \delta, \Delta_\epsilon(\overline{\eta_\triangleright}, \overline{\eta_\triangleleft}) \leq \delta$, where $\overline{\eta_\bullet}$ is the canonical lifting of $\eta_\bullet$ to $A^\star \times B^\star$.

We write $\mu_1 \, \overline{R}^{(\star)}_{\epsilon,\delta} \, \mu_2$ if there exists an (ϵ, δ)-approximate symmetric lifting of μ_1 & μ_2 for $\mathcal{R}$.

Symmetric $\star$-lifting is a special case of $\star$-lifting that can capture differential privacy under when the adjacency relation ϕ is *symmetric*: a probabilistic computation $M : A \to \mathbb{D}(B)$ is (ϵ, δ)-differentially private if and only if for every two adjacent inputs $a \, \phi \, a'$, there is an approximate lifting of the equality relation: $M(a) \equiv^{(\star)}_{\epsilon,\delta} M(a')$. Unfortunately, the more advanced properties in Section 4 do not all hold when moving to symmetric liftings. However, we can show that symmetric $\star$-liftings are equivalent to the symmetric version of 1-witness lifting proposed by Barthe et al. [3].

▶ **Definition 37** (Barthe et al. [3]). Let $\mu_1 \in \mathbb{D}(A)$ and $\mu_2 \in \mathbb{D}(B)$ be sub-distributions, $\epsilon, \delta \in \mathbb{R}^+$ and $\mathcal{R}$ be a binary relation over A & B. An (ϵ, δ)-*approximate symmetric* 1-*lifting* of μ_1 & μ_2 for $\mathcal{R}$ is a sub-distribution $\mu \in \mathbb{D}(A \times B)$ s.t.

1. $\pi_1^\sharp(\mu) \leq \mu_1$ and $\pi_2^\sharp(\mu) \leq \mu_2$;
2. $\Delta_\epsilon(\mu_1, \pi_1^\sharp(\mu)) \leq \delta$ and $\Delta_\epsilon(\mu_2, \pi_2^\sharp(\mu)) \leq \delta$; and
3. $\mathrm{supp}(\mu) \subseteq \mathcal{R}$.

We will write $\mu_1 \overline{\mathcal{R}}^{(1)}_{\epsilon,\delta}\ \mu_2$ if there exists an (ϵ, δ)-approximate symmetric 1-lifting of μ_1 & μ_2 for $\mathcal{R}$; the (1) indicates that there is one witness for this lifting.

▶ **Theorem 38** (cf. the asymmetric result Theorem 29). *For all binary relations $\mathcal{R}$ over A & B and parameters $\epsilon, \delta \geq 0$, we have $\overline{\mathcal{R}}^{(1)}_{\epsilon,\delta} = \overline{\mathcal{R}}^{(\star)}_{\epsilon,\delta}$.*

Proof. Suppose that (μ_L, μ_R) are witnesses to $\mu_1 \overline{\mathcal{R}}^{(\star)}_{\epsilon,\delta}\ \mu_2$. Define the witness $\eta \in \mathbb{D}(A \times B)$ as the point-wise minimum: $\eta(a, b) \triangleq \min(\mu_L(a, b), \mu_R(a, b))$. We will show that η is a witness to $\mu_1 \overline{\mathcal{R}}^{(1)}_{\epsilon,\delta}\ \mu_2$.

The support condition follows from the support condition for (μ_L, μ_R). The marginal conditions $\pi_1^\sharp(\eta) \leq \mu_1$ and $\pi_2^\sharp(\eta) \leq \mu_2$ also follow by the marginal conditions for (μ_L, μ_R). The only thing to check is the distance condition. By the distance condition on (μ_L, μ_R), there exist non-negative values $\delta(a, b)$ such that

$$\mu_L(a, b) \leq \exp(\epsilon)\mu_R(a, b) + \delta(a, b)$$

and $\sum_{a,b} \delta(a, b) \leq \delta$. So, $\mu_R(a, b) \geq \exp(-\epsilon)(\mu_L(a, b) - \delta(a, b))$. Similarly, there are non-negative values $\delta'(a, b)$ such that

$$\mu_R(a, b) \leq \exp(\epsilon)\mu_L(a, b) + \delta'(a, b)$$

and $\sum_{a,b} \delta'(a, b) \leq \delta$. So, $\mu_L(a, b) \geq \exp(-\epsilon)(\mu_R(a, b) - \delta'(a, b))$.

Now let $S \subseteq A$ be any subset. Then:

$$\begin{aligned}
\mu_1(S) - \exp(\epsilon)\pi_1^\sharp(\eta)(S) &= \sum_{a \in S} \mu_1(a) - \exp(\epsilon) \sum_{b \in B} \min(\mu_L(a, b), \mu_R(a, b)) \\
&\leq \sum_{a \in S} \mu_1(a) - \exp(\epsilon) \sum_{b \in B} \exp(-\epsilon)(\mu_L(a, b) - \delta(a, b)) \\
&= \sum_{a \in S, b \in B} \delta(a, b) \leq \delta.
\end{aligned}$$

The other marginal is similar. For any subset $T \subseteq B$ we have

$$\begin{aligned}
\mu_2(T) - \exp(\epsilon)\pi_2^\sharp(\eta)(T) &= \sum_{b \in T} \mu_2(b) - \exp(\epsilon) \sum_{a \in A} \min(\mu_L(a, b), \mu_R(a, b)) \\
&\leq \sum_{b \in T} \mu_2(b) - \exp(\epsilon) \sum_{a \in A} \exp(-\epsilon)(\mu_R(a, b) - \delta'(a, b)) \\
&= \sum_{b \in T, a \in A} \delta'(a, b) \leq \delta.
\end{aligned}$$

Thus, η witnesses $\mu_1 \overline{\mathcal{R}}^{(1)}_{\epsilon,\delta}\ \mu_2$.

The other direction is more interesting. Let $\eta \in \mathbb{D}(A \times B)$ be the single witness to $\overline{\mathcal{R}}^{(1)}_{\epsilon,\delta}$. By the distance conditions $\Delta_\epsilon(\mu_1, \pi_1^\sharp \eta) \leq \delta$ and $\Delta_\epsilon(\mu_2, \pi_2^\sharp \eta) \leq \delta$, there exist non-negative values $\delta(a)$ and $\delta'(b)$ such that

$$\mu_1(a) \leq \exp(\epsilon)\pi_1^\sharp \eta(a) + \delta(a)$$
$$\mu_2(b) \leq \exp(\epsilon)\pi_2^\sharp \eta(b) + \delta'(b),$$

there is equality when $\delta(a)$ or $\delta'(b)$ are strictly positive, and both $\sum_{a \in A} \delta(a)$ and $\sum_{b \in B} \delta'(b)$ are at most δ. Define two witnesses $\mu_L \in \mathbb{D}(A \times B^\star), \mu_R \in \mathbb{D}(A^\star \times B)$ as follows:

$$\mu_L(a,b) \triangleq \begin{cases} \eta(a,b) \cdot \frac{\mu_1(a) - \delta(a)}{\pi_1^\sharp \eta(a)} & : b \neq \star \\ \mu_1(a) - \sum_{b \in B} \mu_L(a,b) & : b = \star \end{cases}$$
$$\mu_R(a,b) \triangleq \begin{cases} \eta(a,b) \cdot \frac{\mu_2(b) - \delta'(b)}{\pi_2^\sharp \eta(b)} & : a \neq \star \\ \mu_2(b) - \sum_{a \in A} \mu_R(a,b) & : a = \star. \end{cases}$$

(As usual, if any denominator is zero, we take the probability to be zero as well.)

The support condition follows from the support condition of η. The marginal conditions hold by definition. Note that all probabilities are non-negative. For instance in μ_L, note that if $\delta(a) > 0$ then $\mu_1(a) - \delta(a) = \exp(\epsilon)\pi_1^\sharp \eta(a) \geq 0$ and hence

$$\mu_L(a, \star) = \mu_1(a) - \delta(a) \geq 0.$$

assuming $\pi_1^\sharp \eta(a) > 0$; if $\pi_1^\sharp \eta(a) = 0$ then $\mu_L(a, \star) = 0$. A similar argument shows that μ_R is non-negative.

So, it remains to check the distance bounds. Note that when $a, b \neq \star$, by definition $\mu_L(a,b)$ and $\mu_R(a,b)$ are both strictly positive or both equal to zero, and $\eta(a,b)$ is strictly positive or equal to zero accordingly. If $\mu_L(a,b), \mu_R(a,b), \eta(a,b)$ are all strictly positive, then we know

$$\frac{\mu_L(a,b)}{\eta(a,b)} = \frac{\mu_1(a) - \delta(a)}{\pi_1^\sharp \eta(a)} \leq \exp(\epsilon)$$
$$\frac{\mu_R(a,b)}{\eta(a,b)} = \frac{\mu_2(b) - \delta'(b)}{\pi_2^\sharp \eta(b)} \leq \exp(\epsilon).$$

We can also lower bound the ratios:

$$\frac{\mu_L(a,b)}{\eta(a,b)} = \frac{\mu_1(a) - \delta(a)}{\pi_1^\sharp \eta(a)} \geq 1$$
$$\frac{\mu_R(a,b)}{\eta(a,b)} = \frac{\mu_2(b) - \delta'(b)}{\pi_2^\sharp \eta(b)} \geq 1;$$

for instance when $\delta(a) > 0$ then the ratio is exactly equal to $\exp(\epsilon) \geq 1$, and when $\delta(a) = 0$ then the ratio is at least 1 by the marginal property $\pi_1^\sharp \eta \leq \mu_1$. So we have $\mu_L(a,b)/\eta(a,b)$ and $\mu_R(a,b)/\eta(a,b)$ in $[1, \exp(\epsilon)]$ when all distributions are strictly positive. Thus we always have

$$\mu_L(a,b) \leq \exp(\epsilon)\mu_R(a,b)$$
$$\mu_R(a,b) \leq \exp(\epsilon)\mu_L(a,b).$$

We can also bound the mass on points $(a, \star)$. Let $S \subseteq A$ be any subset. $\overline{\mu_R}(S \times \{\star\}) \leq \exp(\epsilon)\overline{\mu_L}(S \times \{\star\}) + \delta$ is clear. For the other direction:

$$\begin{aligned}\overline{\mu_L}(S \times \{\star\}) &= \sum_{a \in S} \mu_1(a) - \mu_1(a) \sum_{b \in B} \frac{\eta(a,b)}{\pi_1^\sharp \eta(a)} + \delta(a) \sum_{b \in B} \frac{\eta(a,b)}{\pi_1^\sharp \eta(a)} \\ &= \mu_1(S) - \mu_1(S) + \delta(S) \leq \exp(\epsilon)\overline{\mu_R}(S \times \{\star\}) + \delta.\end{aligned}$$

The mass at points $(\star, b)$ can be bounded in a similar way. Let $T \subseteq B$ be any subset. Then, $\overline{\mu_L}(\{\star\} \times T) \leq \exp(\epsilon)\overline{\mu_R}(\{\star\} \times T) + \delta$ is clear. For the other direction:

$$\begin{aligned}\overline{\mu_R}(\{\star\} \times T) &= \sum_{b \in T} \mu_2(b) - \mu_2(b) \sum_{a \in A} \frac{\eta(a,b)}{\pi_2^\sharp \eta(b)} + \delta'(b) \sum_{a \in A} \frac{\eta(a,b)}{\pi_2^\sharp \eta(b)} \\ &= \mu_2(T) - \mu_2(T) + \delta'(T) \leq \exp(\epsilon)\overline{\mu_L}(\{\star\} \times T) + \delta.\end{aligned}$$

So $\Delta_\epsilon(\overline{\mu_L}, \overline{\mu_R}) \leq \delta$ and $\Delta_\epsilon(\overline{\mu_R}, \overline{\mu_L}) \leq \delta$ so we have witnesses to $\mu_1 \; \overline{\mathcal{R}}^{(\star)}_{\epsilon,\delta} \; \mu_2$. Hence, $\overline{\mathcal{R}}^{(1)}_{\epsilon,\delta} = \overline{\mathcal{R}}^{(\star)}_{\epsilon,\delta}$. ◀

The main use of symmetric approximate liftings is to support richer composition results that only apply to symmetric adjacency relations. We have the following reduction, a symmetric version of Lemma 26.

▶ **Lemma 39.** *Let n be a natural number. Suppose that there exists a function $r : (\mathbb{R}^+ \times \mathbb{R}^+)^n \to (\mathbb{R}^+ \times \mathbb{R}^+)$ such that for any sets D, A,* symmetric *adjacency relation $\phi \subseteq D \times D$, n pairs $\epsilon_i, \delta_i \geq 0$, and n functions $f_i : D \times A \to \mathbb{D}(A)$ such that for every a, $f_i(-, a) : D \to \mathbb{D}(A)$ is (ϵ_i, δ_i)-differentially private with respect to ϕ, the n-fold composition $F : D \to \mathbb{D}(A)$ is $r(\{(\epsilon_i, \delta_i)\})$-differentially private with respect to ϕ. Then for:*

1. *any relations $\{\mathcal{R}(i)\}_i$ on A_i & B_i with i ranging from $0, \dots, n$; and*
2. *any functions $\{g_i : A_i \to \mathbb{D}(A_{i+1})\}_i, \{h_i : B_i \to \mathbb{D}(B_{i+1})\}_i$ with i ranging from $0, \dots, n-1$ and for all $(a, b) \in \mathcal{R}(i)$, we have*

$$g_i(a) \; \overline{\mathcal{R}(i+1)}^{(\star)}_{\epsilon_{i+1},\delta_{i+1}} \; h_i(b)$$

and $g_i(a), h_i(b)$ proper distributions,

there is a symmetric $\star$-lifting

$$G(a_0) \; \overline{\mathcal{R}(n)}^{(\star)}_{r(\{(\epsilon_i,\delta_i)\})} \; H(b_0)$$

for every $(a_0, b_0) \in \mathcal{R}_0$, where $G : A_0 \to \mathbb{D}(A_n)$ and $H : B_0 \to \mathbb{D}(B_n)$ are the n-fold (Kleisli) compositions of $\{g_i\}$ and $\{h_i\}$ respectively.

With this reduction we hand, we can generalize the advanced composition theorem from differential privacy to $\star$-liftings.

▶ **Theorem 40** (Advanced composition, [8]). *Consider a* symmetric *adjacency relation ϕ on databases D. Let $f_i : D \times A \to \mathbb{D}(A)$ be a sequence of n functions, such that for every $a \in A$ the functions $f_i(-, a) : D \to \mathbb{D}(A)$ are (ϵ, δ)-differentially private with respect ϕ. Then, for every $a \in A$ and $\omega \in (0, 1)$, running $f_1, \dots, f_n$ in sequence is (ϵ^*, δ^*)-differentially private for*

$$\epsilon^* = \left(\sqrt{2n \ln(1/\omega)}\right)\epsilon + n\epsilon(e^\epsilon - 1) \quad \text{and} \quad \delta^* = n\delta + \omega.$$

▶ **Theorem 41.** *Let n be a natural number, $\epsilon, \delta \geq 0$, and $\omega \in (0,1)$ be real parameters. Suppose we have:*

1. *sets $\{A_i\}_i, \{B_i\}_i$ with i ranging from $0, \ldots, n$;*
2. *relations $\{\mathcal{R}(i)\}_i$ on A_i & B_i with i ranging from $0, \ldots, n$; and*
3. *functions $\{f_i : A_i \to \mathbb{D}(A_{i+1})\}_i, \{g_i : B_i \to \mathbb{D}(B_{i+1})\}_i$ with i ranging from $0, \ldots, n-1$*

such that for all $(a, b) \in \mathcal{R}(i)$, we have

$$f_i(a) \; \overline{\mathcal{R}(i+1)}^{(\star)}_{\epsilon,\delta} \; g_i(b)$$

and $f_i(a), g_i(b)$ proper distributions. Then, there is an approximate lifting of the compositions:

$$F(a_0) \; \overline{\mathcal{R}(n)}^{(\star)}_{\epsilon',\delta'} \; G(b_0)$$

for every $(a_0, b_0) \in \mathcal{R}_0$, where $F : A_0 \to \mathbb{D}(A_n)$ and $G : B_0 \to \mathbb{D}(B_n)$ are the n-fold (Kleisli) compositions of $\{f_i\}$ and $\{g_i\}$ respectively, and the lifting parameters are:

$$\epsilon' \triangleq \epsilon\sqrt{2n \ln(1/\omega)} + n\epsilon(e^\epsilon - 1) \qquad \delta' \triangleq n\delta + \omega.$$

Proof. By Lemma 39 and the advanced composition for differential privacy (Theorem 40). ◀

C An Elementary Proof of Weak Max-Flow Min-Cut Theorem

We give here an elementary proof of Max-Flow Min-Cut theorem for countable networks. We call it *weak* because it only covers graphs without rays and with a capacity function that is summable at each node. Our proof of approximate Strassen's theorem lies in this setting. Indeed, using the notations of Theorem 19, although an infinite capacity can occur on an edge of the form $a^\top \mapsto b^\perp$, we know that the flow between these two nodes cannot be above $\min\{\alpha_a, \beta_b\}$ where α_a and β_b are the respective capacities of the edges $\top \mapsto a^\top$ and $b^\perp \mapsto \perp$. Hence, we can built a network flow whose set of flows is identical to the former one and with only finite capacities. It is immediate to check that the capacity of the network flow is summable at each node, the families $\{\alpha_a\}_{a\in(A^\star)^\top}$ and $\{\beta_b\}_{b\in(B^\star)^\perp}$ being summable.

From now on, let $\mathcal{N} \triangleq ((V, E), \top, \perp, c)$ be a flow network that contains only finite capacities. Moreover, assume that for any $u \in V$, the families $\{c(u, v)\}_{v\in V}$ and $\{c(v, u)\}_{v\in V}$ are summable. In the proof, we will use the edge definition of cuts (as defined in the paper above) or the equivalent following one:

▶ **Definition 42.** Given a flow network $\mathcal{N} \triangleq ((V, E), \top, \perp, c)$, a *cut* for $\mathcal{N}$ is any subset C of V s.t. $\top \in C$ but $\perp \notin C$. The *capacity* $|C|$ of a cut C is defined as

$$|C| \triangleq \sum \{c(u, v) \mid u \in C, v \notin C\} \in \mathbb{R}^+ \cup \{+\infty\}.$$

We can now start our proof of Weak Max-Flow Min-Cut Theorem.

▶ **Lemma 43.** *There exists a flow for $\mathcal{N}$ with maximal mass.*

Proof. We assume that V, the set of vertices, is countably infinite — the finite case is already covered by the usual max-flow min-cut theorem. Let $\{[\![n]\!]\}_{n\in\mathbb{N}}$ be an enumeration of V^2.

Let $\mathcal{F} = \{f \mid f \text{ is a flow for } \mathcal{N}\}$. We order $\mathcal{F}$ by $f \preceq g$ iff $|f| \leq |g|$. We first show that $\mathcal{F}$ is an inductive set. Let $X = \{f_i\}_{i\in I}$ be a $\preceq$-chain for $\mathcal{F}$ for some countable set I. We prove that X admits an upper bound in $\mathcal{F}$. If $I = \emptyset$, we take the null flow as the upper bound of X. If I is finite but non empty, we take any f of X, that maximizes $|f|$, as the upper bound of X. Otherwise, wlog, we can assume that $X = \{f_i\}_{i \in \mathbb{N}}$ with $\forall i.\, f_i \preceq f_{i+1}$. We inductively construct a sequence $\{t_n\}_{n\in\mathbb{N}}$ of strictly increasing functions from $\mathbb{N}$ to itself. Let $n \in \mathbb{N}$ and assume that t_k is constructed for any $k < n$. Let $\tilde{t}_n \triangleq t_0 \circ \cdots \circ t_{n-1}$. The sequence t_n is chosen among all the strictly monotone sequences $\{i_n\}_n$'s s.t. $\{f_{\tilde{t}_n(i_k)}([\![n]\!])\}_k$ converges. Such a sequence exists by the Bolzano-Weierstrass theorem, $\{f_{\tilde{t}_n(k)}([\![n]\!])\}_k$ being absolutely bounded by $c([\![n]\!])$. Let $\{\omega_n\}_n$ be defined as $\omega_n \triangleq \tilde{t}_n(n)$. By construction, it is immediate that for any $k \in \mathbb{N}$, $\{f_{\omega_n}\}_n$ is a sub-sequence, at infinity, of $\{f_{\tilde{t}_k(n)}\}_n$. As such, for any e $(\triangleq [\![k]\!]) \in V^2$, $\{f_{\omega_n}(e)\}_n$ admits a limit which is equal to $\lim_{n\to\infty}[f_{\tilde{t}_{k+1}(n)}(e)]$.

We denote by f the point-wise limit of $\{f_{\omega_n}\}_n$ and prove that f is an upper bound of E. Let $u, v \in V$. Then,

$$\begin{cases} f(u,v) = \lim_{n\to\infty} \underbrace{[f_{\omega_n}(u,v)]}_{\leq c(u,v)} \leq c(u,v) \\ f(u,v) = \lim_{n\to\infty} \underbrace{[f_{\omega_n}(u,v)]}_{-f_{\omega_n}(v,u)} = -\lim_{n\to\infty}[f_{\omega_n}(v,u)] = -f(v,u). \end{cases}$$

Last, let $u \in V$ s.t. $u \notin \{\top, \bot\}$. First, note that for any $v \in V$ and $k \in \mathbb{N}$, $f^+_{\omega_k}(u,v) \leq c(u,v)$ and $f^-_{\omega_k}(u,v) \leq c(v,u)$, where $f^+_{\omega_k}$ and $f^-_{\omega_k}$ are the respective positive and negative parts of f_{ω_k}. Hence, by taking $k \to \infty$, we obtain $f^+(u,v) \leq c(u,v)$ and $f^-(u,v) \leq c(v,u)$. By summability of the in- and out-going capacities of u, we obtain that $\{f(u,v)\}_{v\in V}$ is summable. We now prove that $\sum_{v\in V} f(u,v) = 0$:

$$\sum_{v\in V} f(u,v) = \sum_{v\in V} \lim_{n\to\infty}[f_{\omega_n}(u,v)] = \lim_{n\to\infty}\left[\underbrace{\sum_{v\in V} f_{\omega_n}(u,v)}_{0}\right] = 0,$$

where the swapping lim and $\sum$ is obtained by the dominated convergence theorem. (As noted above, for any $v \in V$ and $k \in \mathbb{N}$, $f^+_{\omega_k}(u,v) \leq c(u,v)$ and $f^-_{\omega_k}(u,v) \leq c(v,u)$ with $\{c(u,v)\}_{v\in V}$ and $\{c(v,u)\}_{v\in V}$ summable families.) So, f is a flow for $\mathcal{N}$.

Finally, we show that the flow is maximal: $f \succeq g$ for any $g \in X$. Calculating,

$$|f| = \sum_{v\in V} f(\top,v) = \sum_{v\in V} \lim_{n\to\infty} f_{\omega_n}(\top,v) = \lim_{n\to\infty} f_{\omega_n}(\top,v) = \lim_{n\to\infty} |f_{\omega_n}| = \sup_{g\in X} |g|,$$

where swapping lim and $\sum$ is by the dominated convergence theorem. Hence, $\mathcal{F}$ is an inductive set, and by Zorn's lemma, it admits a maximal element. ◀

▶ **Lemma 44.** *For any cut X of $\mathcal{F}$, the mass of any flow f for $\mathcal{F}$ is equal to the flow of f going through C, i.e. to $\sum\{f(u,v) \mid (u,v) \in X^\dagger\}$ where $X^\dagger \triangleq X \times X^{\complement}$.*

Proof. The proof identical to the finite case. ◀

▶ **Theorem 45** (Weak Countable Max-Flow Min-Cut). *We have*

$$\sup\{|f| \mid f \textit{ is a flow for } \mathcal{N}\} = \inf\{|C| \mid C \textit{ is a cut for } \mathcal{N}\}$$

and both the supremum and infimum are reached.

Proof. By Lemma 43, there exists a maximal flow for $\mathcal{N}$ that we denote by $\mathfrak{f}$. Let $\mathcal{R}$ be s.t. $u \mathrel{\mathcal{R}} v \overset{\triangle}{\iff} \mathfrak{f}(u,v) < c(u,v)$ and consider the set $C \triangleq \mathcal{R}^*(\{\top\})$, where R^* is the reflexive-transitive closure of $\mathcal{R}$. Assume that $\bot \in C$. Then, there exists a path from $\top$ to $\bot$ following $\mathcal{R}$ that we can assume, wlog, simple. Let $u_0 \mathrel{\mathcal{R}} u_1 \mathrel{\mathcal{R}} \cdots \mathrel{\mathcal{R}} u_{n+1}$ be such a path — i.e. $u_0 = \top$, $u_{n+1} = \bot$ and the u_i's are pairwise disjoint. Let $\delta \triangleq \min_{i \leq n}[c(u_i, u_{i+1}) - \mathfrak{f}(u_i, u_{i+1})]$ (that is strictly positive by assumption of $\mathcal{R}$), and let $\Omega : V^2 \to \mathbb{R}$ be defined as $\Omega(u,v) = \sigma_{u,v} \cdot \delta$, where $\forall i.\, \sigma_{u_i, u_{i\pm1}} = \pm 1$ and is equal to 0 otherwise — all these cases being mutual exclusive by simplicity of the path. We consider $\mathfrak{g} = \mathfrak{f} + \Omega$ and prove that $\mathfrak{g}$ is a flow for $\mathcal{N}$ s.t. $|\mathfrak{g}| > |\mathfrak{f}|$. The two first properties of a flow are immediate. For the first one, consider $u, v \in V$ s.t. $\mathfrak{g}(u,v) > \mathfrak{f}(u,v)$. This can only happen if $\sigma_{u,v} > 0$. In that case, $u = u_k$ and $v = u_{k+1}$ for some k, and we have

$$\begin{aligned}
\mathfrak{g}(u,v) = \mathfrak{g}(u_k, u_{k+1}) &= \mathfrak{f}(u_k, u_{k+1}) + \delta \\
&\leq \mathfrak{f}(u_k, u_{k+1}) + c(u_k, u_{k+1}) - \mathfrak{f}(u_k, u_{k+1}) \\
&= c(u_k, u_{k+1}) = c(u,v).
\end{aligned}$$

For the second flow property, consider any pair (u,v) of vertices. Then,

$$\mathfrak{g}(u,v) = \mathfrak{f}(u,v) + \sigma_{u,v} \cdot \delta = -\mathfrak{f}(v,u) - \sigma_{v,u} \cdot \delta = -\mathfrak{f}(v,u).$$

For the Kirchhoff law, let $u \in V$ s.t. $u \notin \{\top, \bot\}$. If u is not part of the considered path, then $\forall v \in V$, $\mathfrak{g}(u,v) = \mathfrak{f}(u,v)$ and the flow at node u is identical for $\mathfrak{f}$ and $\mathfrak{g}$. Otherwise, there exists an index $k \in [1,n]$ s.t. $u = u_k$ and $\mathfrak{f}(u,v)$ and $\mathfrak{g}(u,v)$ only differ for $v = u_{k-1}$ and $v = u_{k+1}$. Hence, $\sum_{v \in V} \mathfrak{g}(u,v)$ converges and:

$$\sum_{v \in V} \mathfrak{g}(u,v) = \sum_{v \in V} \mathfrak{f}(u,v) + \underbrace{\sigma_{u_i, u_{i+1}}}_{+1} \cdot \delta + \underbrace{\sigma_{u_i, u_{i-1}}}_{-1} \cdot \delta = \sum_{v \in V} \mathfrak{f}(u,v) = 0.$$

We now prove that the flow $\mathfrak{g}$ has a mass strictly greater than the one of $\mathfrak{f}$:

$$|\mathfrak{g}| = \sum_{v \in V} \mathfrak{g}(\top, v) = \sum_{v \in V} \mathfrak{f}(\top, v) + \Omega(\top, u_1) = |\mathfrak{f}| + \delta > |\mathfrak{f}|.$$

By maximality of $\mathfrak{f}$, such a flow $\mathfrak{g}$ cannot exist. Hence, $\bot \notin C$ and C is a cut.

We can now conclude the proof. By Lemma 44, for any cut X, $|\mathfrak{f}| = \sum_{e \in X^\dagger} \mathfrak{f}(e) \leq \sum_{e \in X^\dagger} c(e) = |C|$. Hence, $\mathfrak{f} \preceq \inf\{|C| \mid C \text{ is a cut for } \mathcal{N}\}$. Now, by definition of C, any edge in $X^\dagger$ is saturated by $\mathfrak{f}$. Hence, for $e \in C^\dagger$, $\mathfrak{f}(e) = c(e)$ and $|\mathfrak{f}| = |C|$. This proves that C is a minimal cut and that the infimum is a minimum. ◀