Optimal Partition Selection with Rényi Differential Privacy

Charlie Harrison
Google, Austin, TX, USA

Pasin Manurangsi
Google Research, Bangkok, Thailand

Abstract

A common problem in private data analysis is the partition selection problem, where each user holds a set of partitions (e.g. keys in a GROUP BY operation) from a possibly unbounded set. The challenge here is in maximizing the set of released partitions while respecting a differential privacy constraint. Previous work [8] presented an optimal (ε, δ)-DP algorithm when each user submits only a single partition. We generalize this approach to find the optimal algorithm under δ-approximate (α, ε)-Rényi differential privacy (RDP), which allows much tighter analysis under composition. Motivated by the *non-existence* of a general optimality result in the case where users submit multiple partitions each, we present an extension of our optimal algorithm tuned for L^2 bounded weighted partition selection which can be used as a drop-in improvement over the Gaussian mechanism any time the partition frequency is not also needed. We show that our primitive can be easily plugged into state of the art partition selection algorithms (PolicyGaussian from [14] and MAD2R from [7]), improving performance both for parallel and sequential adaptive algorithms. Finally, we show that there is an inherent cost to algorithms which *do* support releasing the frequency as well as the partitions. Specifically, we formulate a basic notion of optimal approximate RDP algorithm for partition selection using additive noise, and show that there is a numerical separation between additive and non-additive noise mechanisms for this problem.

2012 ACM Subject Classification Security and privacy; Theory of computation → Design and analysis of algorithms

Keywords and phrases Differentially Privacy, Partition Selection, Renyi Differentially Privacy

Digital Object Identifier 10.4230/LIPIcs.FORC.2026.16

1 Introduction

Differential privacy [11] is a strong notion of privacy which bounds the information a worst-case attacker can learn about the output of a privacy mechanism. Since its inception, various relaxations of differential privacy have gained in popularity. In particular, Rényi differential privacy (RDP) [21] and approximate RDP [22] are most relevant to this work. These relaxations typically provide much better utility in scenarios where many mechanisms are composed together.

The problem of identifying the set of "keys" in a dataset is common in private data analysis. This comes up for instance, when determining the set of output partitions in a private GROUP BY query, or when trying to release a dataset of high dimensional items like arbitrary strings or URLs. In many cases, the set of possible outputs is exponential or even infinite, which precludes (non-trivial) mechanisms which introduce false positives. Therefore, we limit our approach to cases where the mechanism must emit only a subset of the true partitions.

1.1 Related work

Some of the earliest work in private partition selection comes from [16], who analyzed search logs to privately release the set of user queries. Their approach leveraged adding additive Laplace noise to the count of each query, and only keeping queries whose count exceeded some threshold. This basic recipe (sometimes replacing Laplace noise with Gaussian noise) became a popular approach to partition selection, and has been proposed in various private query engines [28, 2].

In the case where a user only contributes to a single partition, [8] proved the *optimal* algorithm under (ε, δ)-DP. That is, each partition is released with the maximum possible probability under the privacy constraint. Our work generalizes this result, as taking the limit $\alpha \to \infty$ under δ-approximate (α, ε)-RDP recovers (ε, δ)-DP exactly. By allowing a relaxation to finite α, we can show utility improvements when under composition (or, equivalently, to handle users contributing multiple partitions).

[14] formalized the partition selection problem as "differentially private set union", and innovated on algorithms to handle cases where users contribute more than one partitions. Their proposed algorithm is adaptive and greedy, where each user's contribution is dependent on previous users'. [6] follow a similar recipe, proceeding user-by-user in a dependent manner. While these sequential algorithms typically allow releasing the most partitions for the same privacy budget, they are difficult to scale for large datasets or query systems. [25, 7] both attempt to design adaptive algorithms that can be implemented in a highly parallelizable fashion.

Finally, our work involves numerically computing optimal additive noise mechanisms. This overall approach was used in [13] to find variance-optimal mechanisms under an RDP constraint, with the goal of improving an overall privacy guarantee under composition. Unlike their approach which attempted to minimize variance, we minimize *tail bounds*, enabling us to choose a tighter truncation threshold and therefore release more partitions.

1.2 Our contributions

Optimal partition selection (Section 3)

In Theorem 14, we present an optimal partition selection algorithm (under approximate RDP) when users only submit a single partition. Our algorithm exactly recovers the result from [8] in the limit when $\alpha \to \infty$, but for finite α we can leverage the tight composition afforded by RDP. We additionally show that when users can submit more than one partition, there is no single optimal mechanism (Theorem 16).

Weighted partition selection with the SNAPS mechanism (Section 4)

We extend our core algorithm to handle real valued weights associated with partitions. Under this framework, we derive the SNAPS algorithm (Smooth Norm-Aware Partition Selection) which satisfy the privacy constraints when the users hold vectors with sensitivities bounded by arbitrary L^r norms. In particular, when $r = 2$, we can plug our algorithm into more complex adaptive mechanisms like DP-SIPS [25], MAD2R [7], or PolicyGaussian [14] which use the Gaussian mechanism as a subroutine for partition selection.

Numerical experiments (Section 5)

We replace the Gaussian mechanism with the SNAPS mechanism described above in two weighted partition selection algorithms: MAD2R [7] and PolicyGaussian [14]. Adopting our subroutine improves performance of both of these approaches, yielding state-of-the-art approaches for partition selection in both the parallel and sequential regimes.

Optimal partition selection with additive noise (Section 6)

Motivated by the fact that [8] nearly matches utility with the truncated discrete Laplace mechanism, we present a convex program to find the optimal partition selection mechanism when a) users only submit a single partition, and b) when the algorithm must be the post-processing of an additive noise mechanism. We find a numerical separation in privacy between additive and non-additive approaches to partition selection. Since one benefit of using additive noise is that we privatize the count as well as the partition itself simultaneously, this result can be seen as the "cost of releasing the count" associated with any partition. When the count is not needed, our result demonstrates that additive-noise based techniques are (unfortunately) sub-optimal.

2 Preliminaries

For every $K \in \mathbb{N}$, we use $[K]$ to denote the set $\{1, \ldots, K\}$. For a given distribution P, we will write P_+ to denote the shift of P by one. That is, $P(x) = P_+(x-1)$. Let $\mathrm{Ber}(p)$ denote the Bernoulli distribution. For $X \sim \mathrm{Ber}(p)$, $\mathbb{P}(X = 1) = p = 1 - \mathbb{P}(X = 0)$.

2.1 Privacy tools

We will begin by defining the relevant privacy notions used in this work. Below, we define differential privacy (DP) under a generic neighboring notion. Specific neighboring notions relevant to our work will be introduced when we formalize the problem in Section 2.2.

▶ **Definition 1** (Differential privacy [11]). *A randomized algorithm $M : \mathcal{X} \to \mathcal{Y}$ satisfies (ε, δ)-differential privacy ((ε, δ)-DP) if, for all neighboring inputs $X, X' \in \mathcal{X}$, and for all $S \subseteq \mathcal{Y}$, $\mathbb{P}(M(X) \in S) \leq e^{\varepsilon} \cdot \mathbb{P}(M(X') \in S) + \delta$.*

As mentioned earlier, we are interested in variants of DP that uses (approximate) Rényi divergence to measure the divergence between $M(X)$ and $M(X')$. We start by recalling Rényi divergence and its approximate counterpart below.

▶ **Definition 2** (Rényi divergence [23]). *Let P and Q be probability distributions on Ω. Then the Rényi divergence between P and Q at order α, denoted $\mathrm{D}_\alpha(P \parallel Q)$, is*

$$\mathrm{D}_\alpha(P \parallel Q) = \frac{1}{\alpha - 1} \log \left(\int_\Omega P(x)^\alpha Q(x)^{1-\alpha} \mathrm{d}x \right),$$

where $P(\cdot), Q(\cdot)$ denote the probability mass/density functions of P and Q, respectively.[1] *The Rényi divergence at $\alpha = 1$ is defined as*

$$\mathrm{D}_1(P \parallel Q) = \lim_{\alpha \to 1} \mathrm{D}_\alpha(P \parallel Q) = D_{KL}(P||Q) = \int_\Omega P(x) \log \left(\frac{P(x)}{Q(x)} \right) \mathrm{d}x.$$

▶ **Definition 3** (Approximate Rényi divergence [22]). *Let P and Q be probability distributions over Ω and $\delta \in [0, 1]$, then*

$$\mathrm{D}_\alpha^\delta(P \parallel Q) = \inf \{ \mathrm{D}_\alpha(P' \parallel Q') : P = (1-\delta)P' + \delta P'', Q = (1-\delta)Q' + \delta Q'' \}$$

i.e. P and Q can both be expressed as a convex combination of two distributions with weights $1 - \delta$ and δ, respectively.

[1] If P is not absolutely continuous with respect to Q, we define $\mathrm{D}_\alpha(P \parallel Q) = \infty$ for all $\alpha \geq 1$.

For notational convenience, we will sometimes write random variables in place of their distributions in $\mathrm{D}_\alpha(\cdot \parallel \cdot)$ when there is no ambiguity.

The privacy notion of our interest can now be defined as follows:

▶ **Definition 4** (Approximate Rényi DP [22]). *A randomized algorithm $M : \mathcal{X} \to \mathcal{Y}$ satisfies* δ-approximate $(\alpha, \hat{\varepsilon})$-Rényi differential privacy *(denoted $(\delta, \alpha, \varepsilon)$-RDP for brevity) if, for all neighboring inputs $X, X' \in \mathcal{X}$, $\mathrm{D}_\alpha^\delta(M(x) \parallel M(x')) \leq \hat{\varepsilon}$.*

Standard Rényi differential privacy [21] is a special case of approximate RDP with $\delta = 0$, which it shares the following straightforward composition properties with.

▶ **Proposition 5** (Approximate RDP composition). *Let M_1 and M_2 satisfy $(\delta_1, \alpha, \varepsilon_1)$ and $(\delta_2, \alpha, \varepsilon_2)$ RDP, respectively. Then $M_1 \circ M_2$ satisfies $(\delta, \alpha, \varepsilon_1 + \varepsilon_2)$ RDP, where $\delta = \delta_1 + \delta_2 - \delta_1 \cdot \delta_2 \leq \delta_1 + \delta_2$.*

In particular, if we have distributions P_1, P_2, Q_1, Q_2 such that $\mathrm{D}_\alpha^{\delta_1}(P_1 \parallel Q_1) \leq \varepsilon_1$ and $\mathrm{D}_\alpha^{\delta_2}(P_2 \parallel Q_2) \leq \varepsilon_2$, then $\mathrm{D}_\alpha^{\delta_1+\delta_2}(P_1 \otimes P_2 \parallel Q_1 \otimes Q_2) \leq \varepsilon_1 + \varepsilon_2$.

Converting from approximate RDP to approximate DP is a simple extension of [5] to add the extra δ term.

▶ **Proposition 6.** *Let M satisfy $(\delta, \alpha, \varepsilon)$-RDP. Then M satisfies $(\hat{\delta}, \hat{\varepsilon})$-DP for*

$$\hat{\delta} = \delta + \frac{\exp((\alpha - 1)(\varepsilon - \hat{\varepsilon}))}{\alpha} \cdot \left(1 - \frac{1}{\alpha}\right)^{\alpha - 1}.$$

2.2 Partition selection

In this section we will formalize the problem of partition selection. Let U be a universe of elements. A dataset X is represented as a vector in $\mathbb{Z}_{\geq 0}^U$, where X_u is the number of occurrences of item u.

▶ **Definition 7** (Private partition selection). *A partition selection mechanism $M : \mathbb{Z}_{\geq 0}^U \to 2^U$ takes as input a database and returns as many partitions as possible in the database (under the privacy constraint). In other words, the output $M(X)$ must be a subset of $\{u \in U \mid X_u > 0\}$.*

We say that two datasets X, X' are neighbors under L^r norm bound Δ if $\|X - X'\|_r \leq \Delta$.

We focus on differentially private algorithms based on applying a *partition selection primitive* independently on each element, as formalized below.

▶ **Definition 8** (Differentially private partition selection primitive). *A partition selection primitive is a function $\pi : \mathbb{Z}_{\geq 0} \to [0, 1]$ where $\pi(0) = 0$. Its corresponding partition selection mechanism M_π works as follows: For every $u \in U$, include u independently in the output with probability $\pi(X_u)$.*

We say that π is $(\delta, \alpha, \varepsilon)$-RDP for $\Delta_r = \Delta$ if M_π is δ-approximate (α, ε)-RDP under the neighboring notion for L^r norm bound Δ.

We similarly define *weighted partition selection* and *weighted partition selection primitive* (denoted by a release probability function $\phi : \mathbb{R}_{\geq 0} \to [0, 1]$) identically as above, except that each dataset is now represented as a vector of non-negative *real numbers*, i.e. $X \in \mathbb{R}_{\geq 0}^U$. Here X_u denote the total weight of item u. Moreover, we also sometimes allow multiple norm bounds.

▶ Remark 9. For notational convenience, our "dataset" above already consists of total counts or weights of elements. However, this can also be a result of a function (e.g. policy from [14]) of an underlying database. As long as this function results has bounded L_r-sensitivity, we can apply our mechanisms.

Finally, we outline what we mean by *optimality* of partition selection.

▶ **Definition 10.** *A partition selection primitive π^* is optimal for $(\delta, \alpha, \varepsilon)$-RDP with $\Delta_r = \Delta$ if it satisfies $(\delta, \alpha, \varepsilon)$-RDP for $\Delta_r = \Delta$ and, additionally, for any other partition selection primitive π satisfying the same privacy constraint and all $n \in \mathbb{N}$, $\pi^*(n) \geq \pi(n)$.*

▶ **Definition 11.** *A partition selection mechanism M is optimal for $(\delta, \alpha, \varepsilon)$-RDP with $\Delta_r = \Delta$ if it satisfies $(\delta, \alpha, \varepsilon)$-RDP for $\Delta_r = \Delta$ and additionally, for any other partition selection mechanism M' satisfying the privacy constraint: $E[|M(X)|] \geq E[|M'(X)|]$ for all datasets X.*

3 Optimal partition selection

Like [8], we will start by focusing on the unweighted case where each user only contributes a single element to a single partition, i.e.[2] $\Delta_1 = 1$. In this case, we will describe a simple formula for the optimal partition selection primitive π^* for $(\delta, \alpha, \varepsilon)$-RDP.

Before we do so, it will be useful to describe how the approximate Rényi divergence between two Bernoulli random variables behaves.

▶ **Lemma 12.** *Let $P \sim \mathrm{Ber}(p), Q \sim \mathrm{Ber}(q)$ and $\alpha > 1$. Fixing p, $\mathrm{D}_\alpha(P \parallel Q)$ is decreasing in q on the interval $[0, p]$ and increasing in q on the interval $[p, 1]$. Similarly, for a fixed q, $\mathrm{D}_\alpha(P \parallel Q)$ is decreasing in p in $[0, q]$ and increasing in p on $[q, 1]$.*

Proof. Clearly, $\mathrm{D}_\alpha(P \parallel Q)$ is minimized at 0 when $p = q$. The result follows from the joint quasi-convexity of Rényi divergence for $\alpha \geq 0$ (see [26]). ◀

▶ **Lemma 13.** *Let $P \sim \mathrm{Ber}(p), Q \sim \mathrm{Ber}(q)$, and $\delta \in [0, 1)$. Then*

$$\mathrm{D}_\alpha^\delta(P \parallel Q) = \begin{cases} \mathrm{D}_\alpha\left(\mathrm{Ber}\left(\frac{p}{1-\delta}\right) \middle\| \mathrm{Ber}\left(\frac{q-\delta}{1-\delta}\right)\right) & p < q - \delta \\ \mathrm{D}_\alpha\left(\mathrm{Ber}\left(\frac{p-\delta}{1-\delta}\right) \middle\| \mathrm{Ber}\left(\frac{q}{1-\delta}\right)\right) & p > q + \delta \\ 0 & |p - q| \leq \delta. \end{cases}$$

Furthermore, fixing p, $\mathrm{D}_\alpha^\delta(P \parallel Q)$ is decreasing in q on the interval $[0, p]$ and increasing in q on the interval $[p, 1]$. Similarly for a fixed q, $\mathrm{D}_\alpha^\delta(P \parallel Q)$ is decreasing in p on $[0, q]$ and increasing in p on $[q, 1]$.

Proof. From Definition 3, we want to find distributions $P' \sim \mathrm{Ber}(p'), Q' \sim \mathrm{Ber}(q')$ that minimize $\mathrm{D}_\alpha(P' \parallel Q')$ such that $P = (1-\delta)P' + \delta P''$ and $Q = (1-\delta)Q' + \delta Q''$. From Lemma 12, it suffices to move p' and q' closer to equality. The maximum we can increase p' to is clearly $p/(1-\delta)$ by setting $P'' = 0$, and the minimum is $(p-\delta)/(1-\delta)$ by setting $P'' = 1$. The same is true for Q and the first result naturally follows by observing in cases where p' and q' would otherwise cross, they can be made equal instead.

The second observation follows directly from applying Lemma 12 to each term. ◀

[2] Since this is the unweighted case, we can also set $\Delta_r = 1$ for any $1 < r < \infty$ (or $\Delta_0 = \Delta_\infty = 1$) instead.

▶ **Theorem 14.** *Let*

$$L(q) = \max\left\{p \in [q,1] : \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(p) \parallel \mathrm{Ber}(q)\right) \le \varepsilon \wedge \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(q) \parallel \mathrm{Ber}(p)\right) \le \varepsilon\right\}$$

and

$$\pi^*(n) = \begin{cases} 0 & n = 0 \\ L(\pi^*(n-1)) & n > 0 \end{cases}.$$

Then $\pi^*(n)$ is the optimal partition selection primitive for $(\delta, \alpha, \varepsilon)$-RDP with $\Delta_1 = 1$.

Proof.

Privacy. Consider any two neighbors X, X' whose counts of a partition $u \in U$ are n, n' respectively (and the counts of other items are the same) where $n = n' - 1$. In either case, by construction we have

$$\mathrm{D}_\alpha^\delta\left(M_{\pi^*}(X) \parallel M_{\pi^*}(X')\right) = \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(\pi^*(n)) \parallel \mathrm{Ber}(\pi^*(n-1))\right) \le \varepsilon,$$

and,

$$\mathrm{D}_\alpha^\delta\left(M_{\pi^*}(X') \parallel M_{\pi^*}(X)\right) = \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(\pi^*(n-1)) \parallel \mathrm{Ber}(\pi^*(n))\right) \le \varepsilon.$$

Thus, M_{π^*} is δ-approximate (α, ε)-RDP as desired.

Optimality. First we will show that L is increasing in q. Fix any $p > q$. By Lemma 13, the divergence terms $\mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(p) \parallel \mathrm{Ber}(q)\right)$ and $\mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(q) \parallel \mathrm{Ber}(p)\right)$ are decreasing as q increases towards p. Therefore as q increases, larger values of p satisfy the divergence constraints.

Now consider any partition selection primitive π where $\pi(n_0) > \pi^*(n_0)$; let n_0 be the smallest such index, so that $\pi(n_0 - 1) \le \pi^*(n_0 - 1)$. Since $\pi^*(n_0) = L(\pi^*(n_0 - 1))$, the monotonicity of L implies that $\pi(n_0) > L(\pi(n_0 - 1))$. In other words, $\mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(\pi(n_0)) \parallel \mathrm{Ber}(\pi(n_0 - 1))\right) > \varepsilon$ or $\mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(\pi(n_0 - 1)) \parallel \mathrm{Ber}(\pi(n_0))\right) > \varepsilon$. This means that M_π is not δ-approximate (α, ε)-RDP. ◀

It is straightforward to compute π^* by with a subroutine that can compute $p_1 \leftarrow \{p_1 \in [q,1] : \mathrm{D}_\alpha\left(\mathrm{Ber}(p) \parallel \mathrm{Ber}\, q\right)\}$ and $p_2 \leftarrow \{p \in [q,1] : \mathrm{D}_\alpha\left(\mathrm{Ber}(q) \parallel \mathrm{Ber}\, p\right)\}$. Both p_1 and p_2 can be solved and guarantee convergence with simple bisection techniques, as they reduce to solving bounded convex and quasi-convex minimization problems, respectively.

3.1 General optimality of π^*

Here we will extend our optimality result to show π^* dominates mechanisms that do not necessarily consider each partition independently. Like, [8], we restrict to the $\Delta_1 = 1$ case.

▶ **Theorem 15.** *M_{π^*} is the optimal partition selection mechanism for $(\delta, \alpha, \varepsilon)$-RDP with $\Delta_1 = 1$*

Proof. Consider a single partition u, and denote $f(u) = \Pr(u \in M(X))$ the probability of releasing u under an arbitrary mechanism M under $(\delta, \alpha, \varepsilon)$-RDP. Fixing all other partitions, we have $f(u) \le \pi^*(X_u)$ by Theorem 14. Thus, $\mathbb{E}[|M(X)|] = \sum_{u \in U} f(u) \le \sum_{u \in U} \pi^*(X_u) = \mathbb{E}[|M_{\pi^*}(X)|]$. ◀

3.2 Non-existence of optimal partition selection when $\Delta_1 \neq 1$

Unlike the case $\Delta_1 = 1$, we show below that, when $\Delta_1 \neq 1$, the optimal selection mechanism does *not* exist for certain regime of parameters.

▶ **Theorem 16.** *For any $0 < \alpha, \varepsilon, \delta$ such that*[3][4] $\pi^*(2) > 3 \cdot \pi^*(1)$*, there is no optimal selection mechanism even for $\Delta_1 = 2$.*

Proof. Suppose for the sake of contradiction that there exists an optimal selection mechanism M^* for $(\delta, \alpha, \varepsilon)$-RDP with $\Delta_1 = 2$ and universe $U = \{1, 2\}$. Consider neighboring datasets $X^1 = (1, 1)$ and $X^0 = (0, 0)$. Notice that, by comparing $\mathbb{P}(M^*(X^1) \neq \emptyset)$ and $\mathbb{P}(M^*(X^0) \neq \emptyset) = 0$, we have

$$\mathbb{P}(M^*(X^1) \neq \emptyset) \leq \pi^*(1). \tag{1}$$

We consider two cases, based on $\mathbb{P}(M^*(X^1) = U)$.

- **Case I: $\mathbb{P}(M^*(X^1) = U) < \pi^*(1)$.** In this case, consider another mechanism M' where $\mathbb{P}(M'(X^1) = U) = \pi^*(1), \mathbb{P}(M'(X^1) = \emptyset) = 1 - \pi^*(1)$, and $\mathbb{P}(M'(X) = \emptyset) = 1$ for all $X \neq X^1$. It is simple to check that M is δ-approximate (α, ε)-RDP and that $\mathbb{E}[|M^*(X^1)|] < \mathbb{E}[|M'(X^1)|]$, a contradiction.
- **Case II: $\mathbb{P}(M^*(X^1) = U) \geq \pi^*(1)$.** Note that from (1), we must have $\mathbb{P}(M^*(X^1) = U) = \pi^*(1)$ and $\mathbb{P}(M^*(X^1) = \emptyset) = 1 - \pi^*(1)$. Consider another dataset $X^2 = (3, 1)$, which is a neighbor of X^1. By comparing $\mathbb{P}(M^*(X^2) \notin \{U, \emptyset\})$ with $\mathbb{P}(M^*(X^1) \notin \{U, \emptyset\}) = 0$, we have $\mathbb{P}(M^*(X^2) \notin \{U, \emptyset\}) \leq \pi^*(1)$.

Consider yet another dataset $X^3 = (3, 0)$, which is a neighbor of X^2. By the guarantee of partition selection, we must have $\mathbb{P}(M^*(X^3) = U) = 0$ Similarly, by comparing $\mathbb{P}(M^*(X^2) = U)$ with $\mathbb{P}(M^*(X^3) = U) = 0$, we have $\mathbb{P}(M^*(X^2) = U) \leq \pi^*(1)$. Together, this implies that

$$\begin{aligned}
\mathbb{E}[|M^*(X^2)|] &= 1 \cdot \mathbb{P}(M^*(X^2) = \{1\}) + 1 \cdot \mathbb{P}(M^*(X^2) = \{2\}) + 2 \cdot \mathbb{P}(M^*(X^2) = U) \\
&= \mathbb{P}(M^*(X^2) \notin \{U, \emptyset\}) + 2 \cdot \mathbb{P}(M^*(X^2) = U) \\
&\leq 3\pi^*(1) < \pi^*(2).
\end{aligned}$$

Meanwhile, consider a mechanism M'' that ignores all elements of U except for 1 and include 1 in the output with probability $\pi^*(\lceil i/2 \rceil)$. This mechanism satisfies δ-approximate (α, ε)-RDP and $\mathbb{E}[|M''(X^2)|] = \pi^*(2)$, which contradicts the optimality of M^*. ◀

It remains an interesting open question to extend the above non-optimality result to a larger regime of parameters ε, δ.

4 Weighted partition selection and the SNAPS mechanism

In this section we consider the more general weighted partition selection problem, where users hold a weight associated with each partition. We introduce a new mechanism: SNAPS (Smooth Norm-Aware Partition Selection). We remark that, due to the non-optimality result from Section 3.2, there is no optimal mechanism in this setting. Therefore, we aim to design an algorithm that provides both good utility and is practical.

[3] Here π^* is as defined in Theorem 14 for $\Delta_1 = 1$.
[4] It is simple to see that the inequality $\pi^*(2) > 3 \cdot \pi^*(1)$ holds for all sufficiently large ε and sufficiently small δ.

Our idea is to derive a weighted partition selection primitive which affords users a "smooth" privacy loss depending on how much weight they hold. This allows us to derive a composition-based mechanism where users can hold multiple partitions with a total bound on the L^r weight norm.

To define the primitive, we let

$$L(q,\varepsilon,\delta) = \max\left\{p \in [q,1] : \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(p) \parallel \mathrm{Ber}(q)\right) \le \varepsilon \wedge \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}(q) \parallel \mathrm{Ber}(p)\right) \le \varepsilon\right\}.$$

▶ **Definition 17** (Weighted partition selection primitive)**.** *Given parameters* $\varepsilon_0, \delta_0, r, \varepsilon_1, \delta_1, \Delta^{\mathrm{disc}}$, $\Delta > 0$, *first we define the* discretized weighted partition selection primitive ψ_r *over non-negative integers as follows: For* $n = 0$, *let* $\psi_r(0) = 0$. *For* $n > 0$, *let* $N_{\mathrm{disc}} = \left\lceil \frac{\Delta}{\Delta^{\mathrm{disc}}} \right\rceil$ *and*

$$\psi_r(n) = \min_{i \in [\min\{n, N_{\mathrm{disc}}\}]} L\left(\psi_r(n-i), \varepsilon_0 + \varepsilon_1 \cdot \left(\Delta^{\mathrm{disc}}(i-1)\right)^r, \delta_0 + \delta_1 \cdot \left(\Delta^{\mathrm{disc}}(i-1)\right)^r\right).$$

We define the weighted partition selection primitive ϕ_r *on non-negative real numbers as* $\phi_r(y) = \psi_r\left(\left\lfloor \frac{y}{\Delta^{\mathrm{disc}}} \right\rfloor\right)$.

We next point out that the definition of weighted partition selection primitive almost immediately gives the privacy guarantee for $\Delta_0 = 1$ setting, as shown below.[5]

▶ **Lemma 18.** *For* $\Delta_0 = 1$ *and* $\Delta_\infty \le \Delta$, *the weighted partition selection primitive* ϕ_r *satisfies* $(\delta_0 + \delta_1 \cdot \Delta_\infty^r, \alpha, \varepsilon_0 + \varepsilon_1 \cdot \Delta_\infty^r)$*-RDP.*

Proof. Consider any two neighboring datasets X, X' which differs on a single item u. Assume w.l.o.g. that $X_u \le X'_u$. By our assumption, we have $X'_u - X_u \le \Delta_\infty$. Let $z = \left\lfloor \frac{X_u}{\Delta^{\mathrm{disc}}} \right\rfloor$ and $z' = \left\lfloor \frac{X'_u}{\Delta^{\mathrm{disc}}} \right\rfloor$. We also have $i := z' - z \le \lceil \Delta_\infty / \Delta^{\mathrm{disc}} \rceil \le N_{\mathrm{disc}}$.

Let $\delta = \delta_0 + \delta_1 \cdot \Delta_\infty^r$ and $\varepsilon = \varepsilon_0 + \varepsilon_1 \cdot \Delta_\infty^r$. We have

$$\begin{aligned}
&\max\{\mathrm{D}_\alpha^\delta\left(M_{\phi_r}(X') \parallel M_{\phi_r}(X)\right), \mathrm{D}_\alpha^\delta\left(M_{\phi_r}(X) \parallel M_{\phi_r}(X')\right)\} \\
&= \max\{\mathrm{D}_\alpha^\delta\left(\phi_r(X'_u) \parallel \phi_r(X_u)\right), \mathrm{D}_\alpha^\delta\left(\phi_r(X_u) \parallel \phi_r(X'_u)\right)\} \\
&= \max\{\mathrm{D}_\alpha^\delta\left(\mathrm{Ber}\left(\psi_r(z)\right) \parallel \mathrm{Ber}\left(\psi_r(z')\right)\right), \mathrm{D}_\alpha^\delta\left(\mathrm{Ber}\left(\psi_r(z')\right) \parallel \mathrm{Ber}\left(\psi_r(z)\right)\right)\}.
\end{aligned}$$

Finally, by definition of $\psi_r(z') = \psi_r(z+i)$, it is at most $L(\psi_r(z), \varepsilon_0 + \varepsilon_1 \cdot \left(\Delta^{\mathrm{disc}}(i-1)\right)^r, \delta_0 + \delta_1 \cdot \left(\Delta^{\mathrm{disc}}(i-1)\right)^r) \le L(\psi_r(z), \varepsilon, \delta)$, where the inequality follows from $i - 1 \le \Delta_\infty / \Delta^{\mathrm{disc}}$. Thus, by definition of L, the above term is bounded above by ε as desired. ◀

The above result can be easily extended to the case $\Delta_0 > 1$ with L^r norm bound Δ_r, with the cost being a Δ_0 multiplicative factor in front of ε_0, δ_0, as formalized below.

▶ **Theorem 19** (SNAPS Mechanism)**.** *For any* $\Delta_0 \in \mathbb{N}$ *and* $\Delta_r \le \Delta$, *the weighted partition selection primitive* ϕ_r *satisfies* $(\delta_0 \cdot \Delta_0 + \delta_1 \cdot \Delta_r^r, \alpha, \varepsilon_0 \cdot \Delta_0 + \varepsilon_1 \cdot \Delta_r^r)$*-RDP. We refer to the associated weighted partition selection mechanism* M_{ϕ_r} *as the SNAPS mechanism.*

[5] We note that if we impose an additional constraint on the *minimum* weight value that a user can submit, we can avoid the need for ε_0, δ_0 params with a fine enough discretization. Furthermore, this additional restriction does indeed improve utility relative to Definition 17. We avoid this for sake of presenting an algorithm which can always replace the Gaussian mechanism for partition selection.

Proof. Consider any pair of neighboring input datasets X, X' with $\|X - X'\|_r \leq \Delta_r$ and $\|X - X'\|_0 \leq \Delta_0$. In particular, let $S \subseteq U$ denote the set of all $u \in U$ such that $X_u \neq X'_u$. Let $\varepsilon = \varepsilon_0 \cdot \Delta_0 + \varepsilon_1 \cdot \Delta_r^r$ and $\delta = \delta_0 \cdot \Delta_0 + \delta_1 \cdot \Delta_r^r$. We have

$$\mathrm{D}_\alpha^\delta \left(M_{\phi_r}(X) \parallel M_{\phi_r}(X')\right) = \mathrm{D}_\alpha^\delta \left(\bigotimes_{u \in S} \phi_r(X_u) \,\middle\|\, \bigotimes_{u \in S} \phi_r(X'_u) \right).$$

Let $\delta_u = \delta_0 + \delta_1 \cdot |X_u - X'_u|^r$ and $\varepsilon_u = \varepsilon_0 + \varepsilon_1 \cdot |X_u - X'_u|^r$. From Lemma 18, we have

$$\mathrm{D}_\alpha^{\delta_u} \left(\phi_r(X_u) \parallel \phi_r(X'_u)\right) \leq \varepsilon_u.$$

Notice that $\sum_{u \in S} \delta_u \leq \delta$ and $\sum_{u \in S} \varepsilon_u \leq \varepsilon$. Thus, applying the composition theorem (Proposition 5), we can conclude that $\mathrm{D}_\alpha^\delta \left(M_{\phi_r}(X) \parallel M_{\phi_r}(X')\right) \leq \varepsilon$. As a result, the mechanism is δ-approximate (α, ε)-RDP. ◀

We find that the SNAPS mechanism can often be parameterized to outperform the Gaussian mechanism for weighted partition selection for L^2 bounded input, and it can replace the Gaussian mechanism in all cases when the noisy weight vector output is not needed.

5 Experiments

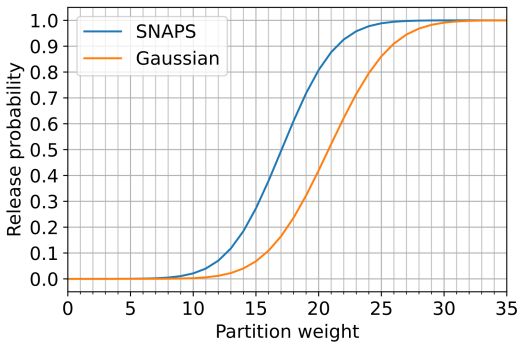

Figure 1 Gaussian and SNAPS mechanism release probabilities for $(1, 10^{-5})$-DP. SNAPS is parameterized as in Section 5. The Gaussian probabilities are determined following [14, 7], i.e. by splitting the δ budget evenly in two, one for computing the analytical Gaussian σ, and one for determining the threshold $\tau = \max_{k \in [\Delta_0]} \{1/\sqrt{k} + \sigma \cdot \Phi^{-1}\left((1 - \delta/2)^{1/k}\right)\}$.

We showcase the versatility of the SNAPS mechanism by plugging it into two adaptive partition selection mechanisms, MAD2R [7] and PolicyGaussian [14].[6] Both algorithms use an adaptive process to optimize the weight vector associated with each user while maintaining an L^2 norm bound. We replace the Gaussian mechanism with the SNAPS mechanism into the very last step in both cases.

Datasets

We consider a number of datasets commonly used in benchmarking differentially private partition selection. Reddit [14] is a dataset of posts to `r/askreddit`, Wiki [27] is a dataset of Wikipedia abstracts. Twitter [3] is a dataset of customer support tweets, Finance [1] is a

[6] We use `https://github.com/heyyjudes/differentially-private-set-union` and `https://github.com/jusyc/dp_partition_selection` for PolicyGaussian and MAD2R implementations, respectively.

dataset of stock market news data, Amazon [19, 29] is a dataset of Amazon reviews, and IMDb [18] is a dataset of movie reviews.

For each datasets, we replicate methodology in [14, 7]: each token in a document is a partition, and each document corresponds to a user. In datasets where actual users are tracked, we combine users' documents.

Algorithms and parameters

We match the benchmarking conditions of [7] by setting $\Delta_0 = 100$, and ensuring all algorithms satisfy $(1, 10^{-5})$-DP.

- **MAD2R [7].** We use a basic composition privacy split of $[.1, .9]$ across two rounds. We set $d_{max} = 50, b_{min} = 0.5, b_{max} = 2, C_{lb} = 1$, and $C_{ub} = 3$. The adaptive threshold is set to $\beta = 2$ standard deviations above the baseline threshold.
- **Policy [14].** We use only a single pass, and set the adaptive threshold to $\beta = 4$ standard deviations above the baseline threshold.
- **SNAPS.** When integrating SNAPS into the above mechanisms, we match all of the above parameters. However, rather than setting the adaptive threshold as a function of the Gaussian noise (and β), we set it so that the *release probability* under SNAPS is equalized with the Gaussian mechanism at that threshold (i.e. for $\beta = 2$ we choose a threshold that will release with probability $\sim 95\%$ under SNAPS). Furthermore in all cases we set[7] $\alpha = 18.5, \varepsilon_0 = 10^{-5}, \delta_0 = 5 \cdot 10^{-5}, \Delta^{\text{disc}} = 5 \cdot 10^{-4}$, though of course it yields different release probabilities than plotted in Figure 1.

To translate approximate RDP guarantees from our algorithm to approximate DP, we leverage Proposition 6 as implemented by [9]. In particular, to match a $(\hat{\varepsilon}, \hat{\delta})$-DP guarantee, we ensure our SNAPS mechanism satisfies $(\hat{\delta}/2, \alpha, \varepsilon)$-RDP such that the (α, ε)-RDP guarantee gives $(\hat{\varepsilon}, \hat{\delta}/2)$-DP. In other words, we use half our δ budget in RDP $\to$ DP conversion.

In Figure 1, we plot the release probabilities between the Gaussian mechanism and SNAPS for the above parameterizations. As predicted by the plot, we should expect the SNAPS experiment variants to always outperform the Gaussian variants, which is validated by the results in Table 1, showing that SNAPS improves utility (as measured by the output size) by 10-20% in all cases.

Table 1 Comparison of output size of partition selection algorithms, with $\varepsilon = 1, \delta = 10^{-5}$, and $\Delta_0 = 100$. Results for each algorithm are averaged over 5 trials, with one standard deviation reported. The best parallel result is bolded, and the best sequential result is underlined.

Dataset	PolicyGaussian	PolicySNAPS	MAD2R	MAD2R-SNAPS
Reddit	7161 (± 10)	<u>8486</u> (± 22)	6187 (± 22)	**7161** (± 20)
Wiki	11467 (± 22)	<u>13793</u> (± 47)	10431 (± 42)	**12170** (± 39)
Twitter	15814 (± 45)	<u>18407</u> (± 43)	13847 (± 29)	**15739** (± 53)
Finance	20129 (± 31)	<u>22952</u> (± 30)	17695 (± 48)	**19969** (± 33)
Amazon	77840 (± 95)	<u>89416</u> (± 71)	65273 (± 91)	**73703** (± 107)
IMDB	3582 (± 21)	<u>4447</u> (± 18)	3829 (± 23)	**4559** (± 17)

[7] While these parameters were generally selected for good utility, we did not perform an exhaustive hyperparameter search. In particular, we use the exact same parameters for the $(.9, .9 \cdot 10^{-5})$-DP stage of MAD2R.

6 Additive noise for partition selection

After exploring weighted partition selection in Section 4, we now pivot back to the notion of *optimal* partition selection. A fundamental limitation of our optimal algorithm defined by π^* (Theorem 15) is that, unlike the Laplace or Gaussian mechanism, it does not allow releasing the *total weight* of released partitions along with the set of released partitions. We observe that all mechanisms which add noise to the weight vector and then perform thresholding as a post-processing step allow releasing the weight as a byproduct, as long as the additive noise alone suffices to guarantee privacy. This is formalized below.

▶ **Definition 20.** *An additive-noise partition selection mechanism $M_{P,\tau}(n)$ is parameterized by a truncated probability distribution P with support*[8] *on $Y \subseteq (-\infty, \tau] \subseteq \mathbb{Z}$. $M_{P,\tau}(n)$ samples $Z \sim P$ and releases $n + Z$, then keeps the partition if $n + Z > \tau$. The associated partition selection primitive is $\pi_{P,\tau}(n) = \mathbb{P}_{Z\sim P}(n + Z > \tau)$.*

Since $\pi_{P,\tau}(0) = \mathbb{P}_{Z\sim P}(Z > \tau) = 0$, $\pi_{P,\tau}$ is a valid partition selection primitive. Crucially, it is also a *post-processing* of an additive noise mechanism. As such, for privacy it suffices to bound the loss associated with releasing $Z + q(D)$ where $q(D)$ is a sensitivity 1 query. This approach is precisely what allows us to release the noisy count.

The property of releasing the total partition weight "for free" is a valuable aspect of these additive noise mechanisms. For instance, a private GROUP BY followed by a SUM in private SQL can be implemented with a single additive mechanism which simultaneously releases the partitions and their sums. As such, it would be very desirable if additive noise can come close to matching the privacy of π^* for the same level of "utility".

In the $\alpha \to \infty$ regime explored in [8], the truncated discrete Laplace mechanism was shown to be nearly optimal in most regimes, and exactly optimal for certain settings of ε, δ. In this section, we show that there is an unfortunate inherent separation in privacy between additive mechanisms and the optimal mechanism in the $\alpha < \infty$ regime. Throughout section, we follow the same restrictions as Section 3 (and [8]) and only consider the $\Delta_1 = 1$ case.

6.1 Approximate RDP of truncated additive noise mechanisms

Given a discrete distribution P over the integers with finite support, our goal is to evaluate the approximate RDP guarantee of P as an additive noise mechanism. Recall from Section 2 that P_+ is the distribution of P shifted by one.

It is simple to see–by following definitions–that the additive noise mechanism is δ-approximate (α, ε)-RDP for $\varepsilon = \max\{\mathrm{D}^{\delta}_{\alpha}(P_+ \parallel P), \mathrm{D}^{\delta}_{\alpha}(P \parallel P_+)\}$, and this is tight.

Before we proceed to any specific optimization problems related to additive noise mechanisms, let us consider the generic problem of computing $\mathrm{D}^{\delta}_{\alpha}(P \parallel Q)$ for arbitrary distributions P, Q. For this problem, we first observe that the exponentiated Rényi divergence and approximate Rényi divergence is convex.

▶ **Lemma 21** ([26, Theorem 13])**.** *Let P and Q be distributions over some finite set U. Then for $\alpha > 1$, $e^{(\alpha-1)\mathrm{D}_{\alpha}(P \parallel Q)} = E_{x\sim Q}\left[\left(\frac{P(x)}{Q(x)}\right)^{\alpha}\right]$ is jointly convex in P and Q.*

[8] Defining additive-noise partition selection mechanisms this way precludes using the standard discrete Laplace / Gaussian mechanism (i.e. they need to be truncated). This is done to both simplify our subsequent optimization technique, and also to naturally define the class of mechanisms as pure post-processing of additive noise. This is fortunately without much loss of generality for our purposes (optimality for $\Delta_0 = 1$), since truncation on the right followed by normalization preserves privacy and decreases the release probability by at most δ.

▶ **Proposition 22.** *Let P and Q be distributions over some finite set U. Then for $\alpha > 1$, $e^{(\alpha-1)\mathrm{D}_\alpha^\delta(P \parallel Q)}$ is jointly convex in (P, Q, P', Q'), where P', Q' are the minimizing distributions in Definition 3:*

$$\mathrm{D}_\alpha^\delta(P \parallel Q) = \inf\{\mathrm{D}_\alpha(P' \parallel Q') : P = (1-\delta)P' + \delta P'', Q = (1-\delta)Q' + \delta Q''\}.$$

Proof. By Definition 3, $e^{(\alpha-1)\mathrm{D}_\alpha^\delta(P \parallel Q)}$ is the value of the following optimization problem:

$$\begin{aligned} \text{minimize} \quad & \sum_x P'(x)^\alpha Q'(x)^{1-\alpha} \\ \text{subject to} \quad & \sum P'(x) = \sum Q'(x) = 1, \\ & 0 \le P'(x) \le \frac{P(x)}{1-\delta}, \qquad 0 \le Q'(x) \le \frac{Q(x)}{1-\delta}. \end{aligned}$$

Let $f(P', Q') = \sum_x P'(x)^\alpha Q'(x)^{1-\alpha}$. By Lemma 21, each term in the sum is jointly convex in $(P'(x), Q'(x))$, so f is jointly convex in (P', Q'). The inequality constraints $0 \le (1-\delta)P'(x) \le P(x)$ and $0 \le (1-\delta)Q'(x) \le Q(x)$ are linear in the variables (P, Q, P', Q'). Thus, the partial minimization over the variables (P', Q') yields a function that is jointly convex in the remaining variables.[9] ◀

Fast Algorithm for Computing Approximate Rényi Divergence

From Proposition 22, it is feasible to numerically solve for the approximate Rényi divergence of two discrete distributions supported on a finite domain via standard convex optimization. However, there exists a greedy algorithm to compute this in $O(n \log n)$ time for any two discrete distributions P and Q with total support size n using a "water-filling" approach. Our approach is detailed in Appendix A.

6.2 Characterizing π^* as an additive noise mechanism

Recall that we have computed the optimal partition selection primitive π^* in Section 3. In this section, we note that this mechanism can be viewed as an additive-noise partition selection strategy, and compute its privacy guarantees using the approach in the previous subsection.

▶ **Definition 23.** *For a given optimal partition selection primitive π^*, denote by Π the discrete distribution with support on $\{0, \dots, n_d - 1\}$ where $n_d = \min\{n \in \mathbb{N} : \pi^*(n) = 1\}$ and*

$$\Pi(x) = \pi^*(n_d - x) - \pi^*(n_d - 1 - x) \qquad \forall x \in \{0, \dots, n_d - 1\}$$

It is easy to see that π^* is increasing and, for $\delta > 0$, n_d is always finite (i.e. $n_d \le \lceil 1/\delta \rceil$). Thus, Π is a valid distribution. Furthermore, the additive-noise partition selection primitive from Π with threshold $\tau = n_d - 1$ satisfies $\pi_{\Pi,\tau}(n) = \mathbb{P}_{Z\sim\Pi}(Z > \tau - n) = \sum_{x=\tau-n+1}^{n_d-1} \Pi(x) = \pi^*(n)$. In other words, the additive noise mechanism characterized by Π *precisely* matches the π^* strategy. Since π^* exactly characterizes Π up to translation, no other additive-noise distribution can both 1) exactly match the utility of π^* and 2) improve privacy over Π.

---

[9] Namely, for any solutions (P', Q') and $(\tilde{P}', \tilde{Q}')$ for (P, Q) and $(\tilde{P}, \tilde{Q})$ respectively, $\left(\frac{P'+\tilde{P}'}{2}, \frac{Q'+\tilde{Q}'}{2}\right)$ is a solution for (P, Q) with $f\left(\frac{P'+\tilde{P}'}{2}, \frac{Q'+\tilde{Q}'}{2}\right) \le \frac{f(P',Q')+f(\tilde{P}',\tilde{Q}')}{2}$.

We can numerically compute the privacy guarantee of the additive noise mechanism for Π using the approach in Section 6.1. Figure 3 shows there is a clear separation in privacy between π^* and Π, which show a separation between any additive-noise partition selection strategies which *exactly* match the selection probabilities of π^* in the $\alpha < \infty$ regime.

6.3 Optimal additive noise with a single point-wise utility

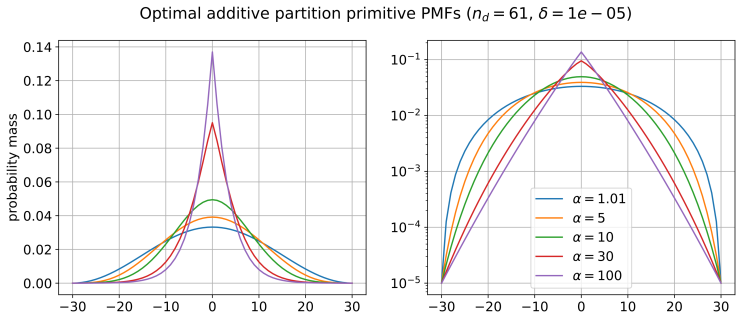

Figure 2 Probability mass functions (centered at 0) for optimal additive noise distributions satisfying $\pi(61) = 1$ at various values of α as minimized by the convex program in Theorem 26. As α grows, the optimal distribution converges to a truncated discrete Laplace (Proposition 27). At smaller α the optimal distribution becomes platykurtic, with a flatter peaks and thinner tails.

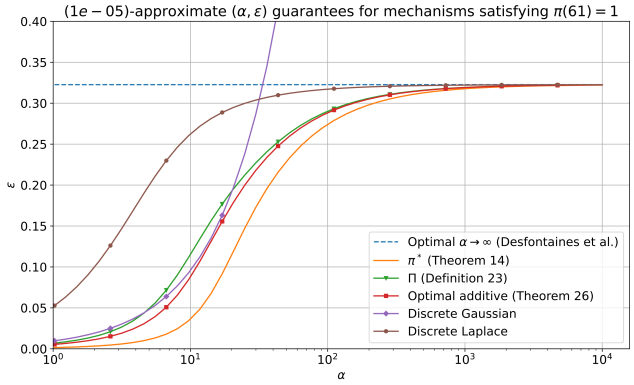

Figure 3 The privacy of various mechanisms under the constraint that $\pi(61) = 1$ i.e. additive noise must be bounded in $[0, 60]$ (or equivalently $[-30, 30]$ due to translation invariance). π^* clearly dominates all additive mechanisms for small and moderate α. The (truncated) Gaussian and Laplace plots were computed by numerically solving for the scale parameters that ensure $f(-30) = f(30) = \delta$ in their respective PMFs after truncation and normalization.

In the previous section, we showed that there is a privacy gap if we *exactly match* the selection probabilities of π^* with additive noise. In this section we will relax this to a specific point-wise guarantee: for a fixed $n_d \in \mathbb{N}$, we will find additive noise mechanisms which satisfy $\pi_{P,r}(n_d) = 1$ (i.e. those that release the partition with count at least n_d deterministically[10]), while achieving the best possible privacy guarantee (minimizing ε for fixed δ, α).

[10] By restricting to $\pi(n_d) = 1$, we simplify the optimization problem substantially to a finite convex problem. In principle this can be extended to $\pi(n_d) = \gamma$ for any $\gamma > 0$, at some increase in complexity.

Similar to Proposition 22, we can in fact find the optimal additive noise by formulating this as a convex optimization, but when P is *not* fixed apriori. The point-wise utility bound imposes a single constraint on P: that it has support only on $\{0, \dots, n_d - 1\}$. Under that constraint, it suffices to find the P that minimizes the privacy objective $\max\{\mathrm{D}_\alpha^\delta(P \parallel P_+), \mathrm{D}_\alpha^\delta(P_+ \parallel P)\}$. This can be stated equivalently as follows.

$$\begin{aligned}
&\text{minimize } \max\left\{\sum_x P_1'(x)^\alpha Q_1'(x)^{1-\alpha}, \sum_x Q_2'(x)^\alpha P_2'(x)^{1-\alpha}\right\} \qquad (2)\\
&\text{subject to } \sum P(x) = \sum P_i'(x) = \sum Q_i'(x) = 1,\\
&\qquad 0 \le P_1'(x) \le \frac{P(x)}{1-\delta}, \quad 0 \le Q_1'(x) \le \frac{P(x-1)}{1-\delta}.\\
&\qquad 0 \le P_2'(x) \le \frac{P(x)}{1-\delta}, \quad 0 \le Q_2'(x) \le \frac{P(x-1)}{1-\delta}.
\end{aligned}$$

Immediately we can show that under this optimization problem, we must have $P_1'(0) = Q_1'(0) = P_2'(n_d) = Q_2'(n_d) = 0$, otherwise either we explicitly violate the constraints, or the objective function is infinite. We can show even more structure to this problem though.

▶ **Proposition 24.** *The optimization problem to Equation* (2) *is symmetric in P. Namely, if P is an optimal solution, then $\bar{P}$ defined by $\bar{P}(x) = P(n_d - 1 - x)$ is also an optimal solution.*

Proof. Let $(P, P_1', Q_1', P_2', Q_2')$ be an optimal solution. Define $\bar{P}(x) = P(n_d - 1 - x)$ and

$$\begin{aligned}
\bar{P_1}'(x) &= Q_2'(n_d - x) \qquad & \bar{Q_1}'(x) &= P_2'(n_d - x)\\
\bar{P_2}'(x) &= Q_1(n_d - x) \qquad & \bar{Q_2}'(x) &= P_1'(n_d - x).
\end{aligned}$$

The new objective on our transformed solution becomes

$$\begin{aligned}
&\max\left\{\sum_x \bar{P_1}'(x)^\alpha \bar{Q_1}'(x)^{1-\alpha}, \sum_x \bar{Q_2}'(x)^\alpha \bar{P_2}'(x)^{1-\alpha}\right\}\\
&= \max\left\{\sum_x Q_2'(n_d - x)^\alpha P_2'(n_d - x)^{1-\alpha}, \sum_x P_1'(n_d - x)^\alpha Q_1(n_d - x)^{1-\alpha}\right\}\\
&= \max\left\{\sum_y Q_2'(y)^\alpha P_2'(y)^{1-\alpha}, \sum_y P_1'(y)^\alpha Q_1(y)^{1-\alpha}\right\},
\end{aligned}$$

which is identical to the original objective. It suffices to verify that the constraints are satisfied.

$$\begin{aligned}
\bar{P_1}'(x) &= Q_2'(n_d - x) \le \frac{P(n_d - 1 - x)}{1-\delta} = \frac{\bar{P}(x)}{1-\delta}\\
\bar{Q_1}'(x) &= P_2'(n_d - x) \le \frac{P(n_d - x)}{1-\delta} = \frac{\bar{P}(x-1)}{1-\delta},
\end{aligned}$$

and similarly the constraints on $(\bar{P_2}', \bar{Q_2}')$ hold by symmetry. ◀

When our problem is symmetrical, it gives us even more structure to exploit.

▶ **Lemma 25.** *Let P be a symmetric distribution and $Q = P + 1$ its shift by one. Then $D_\alpha^\delta(P||Q) = D_\alpha^\delta(Q||P)$.*

Proof. The proof follows from showing that (P, Q) is identical to (Q, P) under a change of variables, i.e. a re-labeling of outcomes. Assume without loss of generality (up to a shift in coordinates) that P is symmetric around 0 and $P(x) = P(-x)$. Now consider the change of variable $y = 1 - x$. Then we can show a bijection $P(y) = P(1 - x) = P(x - 1) = Q(x)$ and $Q(y) = P(-x) = P(x)$. ◀

The above results allow us to simplify Equation (2) substantially.

▶ **Theorem 26.** *For a fixed $\alpha > 1, \delta \in (0, 1), n_d \in \mathbb{N}$, let P, P' be distributions on $\{0, \dots, n_d - 1\}$ and $\{1, \dots, n_d - 1\}$ respectively which minimize the following convex program:*

$$\begin{aligned} &\text{minimize } \sum_x P'(x)^\alpha P'(n_d - x)^{1-\alpha} \\ &\text{subject to } P(x) \geq 0, \quad \sum_x P(x) = \sum_x P'(x) = 1, \\ &\qquad 0 \leq P'(x) \leq \frac{P(x)}{1-\delta}, \qquad P(x) = P(n_d - 1 - x). \end{aligned}$$

Then P minimizes ε in the $(\delta, \alpha, \varepsilon)$-RDP guarantee among all distributions X which satisfy $\pi_X(n_d) = 1$.

Proof. By Proposition 24 and convexity, there is an optimal solution to (2) that is symmetric. Moreover, by Lemma 25 it suffices to consider only one of the terms in the objective function.

We will show that the remaining problem is invariant upon reflecting and shifting P'_1 and Q'_1 in (2). Consider the following transformations:

$$\bar{P}'(x) = Q'_1(n_d - x), \qquad \bar{Q}'(x) = P'_1(n_d - x)$$

These map to the original problem constraints since $P'(0) = Q'(0) = P'(n_d) = Q'(n_d) = 0$ is implied for any feasible solution due to the symmetry of P. Substituting $y = n_d - x$ yields

$$\begin{aligned} 0 \leq \bar{P}'(x) \leq \frac{P(x)}{1-\delta} &\iff 0 \leq Q'_1(y) \leq \frac{P(y-1)}{1-\delta} \\ 0 \leq \bar{Q}'(x) \leq \frac{P(x-1)}{1-\delta} &\iff 0 \leq P'_1(y) \leq \frac{P(y)}{1-\delta}. \end{aligned}$$

Thus, if (P, P'_1, Q'_1) is feasible, then so is $(P, \bar{P}', \bar{Q}')$. Similarly, the objective function remains unchanged (Lemma 25). Now, consider averaging our optimal (P, P'_1, Q'_1) and $(\bar{P}, \bar{P}', \bar{Q}')$ to generate $(P, \tilde{P}', \tilde{Q}')$. Due to convexity, this will also be optimal. Furthermore,

$$\begin{aligned} \tilde{P}'(x) &= \frac{1}{2}(P'_1(x) + \bar{P}'(x)) = \frac{1}{2}(P'_1(x) + Q'_1(n_d - x)) \\ \tilde{Q}'(x) &= \frac{1}{2}(Q'_1(x) + \bar{Q}'(x)) = \frac{1}{2}(Q'_1(x) + P'_1(n_d - x)). \end{aligned}$$

Therefore $\tilde{Q}'(n_d - x) = \frac{1}{2}(Q'_1(n_d - x) + P'_1(n_d - (n_d - x))) = \tilde{P}'(x)$.

This allows us to further eliminate Q_1 from Equation (2) by replacing it with a shifted and reflected version of P_1. ◀

While the program in Theorem 26 is convex, its objective is not numerically stable for large α. In practice, we perform the optimization in log-probabilities (which is not convex), and certify optimality by measuring the duality gap (using complementary slackness) of the convex objective in linear space. Figure 2 plots optimal distributions at various values of α.

Furthermore, we plot the *privacy* of the optimal additive mechanism (for a specific point-wise utility guarantee) against π^* in Figure 3, showing a numerical separation even in this weaker setting where the additive noise needs to compete with π^* only at a single point n_d.

The plots suggest that as $\alpha \to \infty$, the optimal distribution for $\pi(n_d) = 1$ converges to truncated discrete Laplace. We state this convergence below, which aligns with the findings in [8]. The proof is deferred to Appendix B.

▶ **Proposition 27.** *For a fixed odd $n_d > 2$ and $\delta \in (0, 1/n_d]$, the unique distribution X supported on $\{0, \ldots, n_d - 1\}$ that minimizes ε subject to (ε, δ)-DP for $\pi_X(n_d) = 1$ is a truncated discrete Laplace distribution: $P(x) = A \cdot e^{-\varepsilon|x-\mu|}$ where $\mu = \frac{n_d-1}{2}$ and A is the constant such that $\sum P(x) = 1$.*

Furthermore, when $\delta \in (1/n_d, 1]$, the minimum ε is 0 which can be achieved when X is the uniform distribution. (However, this is not the unique distribution achieving $(0, \delta)$-DP.)

We end this section by remarking that noise with bounded support has applications in DP beyond partition selection (e.g. in multi-party DP [4]). Thus, the tools developed here might be useful elsewhere; we leave this to future work.

7 Conclusion

This work continues the direction started by [8] in deriving *optimal* mechanisms for partition selection. We generalize their result to approximate RDP. When users only submit a single partition, this result alone is of practical utility in cases where the mechanism will be composed many times due to the tighter composition properties of (approximate) RDP.

In the finite α regime we also show that there is a separation in privacy between mechanisms which are post-processing of additive noise mechanisms and those which are not; there is an inherent cost to "releasing the weight" of a partition. This differs from the $\alpha \to \infty$ regime as noted by [8], and implies that if the partition weight is not needed, analysts should strongly consider using non-additive mechanisms to maximize utility.

Furthermore, we use our recipe for the optimal mechanism to create a selection mechanism targeting L^r norm constraints on vector contributions. When $r = 1$ it gives us a drop-in replacement for the Laplace mechanism which is used as a subroutine in [6]. When $r = 2$ it gives us a drop-in replacement for the Gaussian mechanism which is used as a subroutine in [25], [14] and [7]. When injecting SNAPS into the latter two algorithms, we show improved utility across the board over a variety of datasets.

There are several interesting open questions left by our work, as highlighted below.

- **Beyond Drop-In Replacement:** Our focus has been to devise partition selection primitives that can be used as drop-in replacements for additive noise mechanisms, such as the (truncated) Gaussian and Laplace. However, some sophisticated partition selection mechanisms–including those used in our experiments [7, 14]–operate in multiple stages, which are more tailored towards L^r sensitivity. It would be interesting to see if these intermediate steps can be designed in conjunction with the optimal partition selection primitive for better compatability and overall utility.
- **Tighter Composition:** Our primary motivation for considering (approximate) RDP is due to its composition property. Another technique for tight privacy accouting which is widely used is through the so-called privacy loss distributions (PLDs) [20, 24, 17, 15, 12, 10]. Using PLD requires tracking the *dominating pairs* (aka "worst case") of neighboring output distributions [30]. For our mechanisms, there do not seem to be a tight dominating pair. Thus, it is an interesting direction to design a partition selection mechanism that is more amenable to PLD-based privacy accounting.

References

1 Miguel Aenlle. Daily financial news for 6000+ stocks. URL: https://www.kaggle.com/miguelaenlle/datasets.

2 Kareem Amin, Jennifer Gillenwater, Matthew Joseph, Alex Kulesza, and Sergei Vassilvitskii. Plume: Differential privacy at scale. *CoRR*, abs/2201.11603, 2022. arXiv:2201.11603.

3 Stuart Axelbrooke. Customer support on twitter, 2017. doi:10.34740/KAGGLE/DSV/8841.

4 James Bell, Adrià Gascón, Badih Ghazi, Ravi Kumar, Pasin Manurangsi, Mariana Raykova, and Phillipp Schoppmann. Distributed, private, sparse histograms in the two-server model. In *CCS*, pages 307–321, 2022. doi:10.1145/3548606.3559383.

5 Clément L Canonne, Gautam Kamath, and Thomas Steinke. The discrete gaussian for differential privacy. *NeurIPS*, 33:15676–15688, 2020.

6 Ricardo Silva Carvalho, Ke Wang, and Lovedeep Gondara. Incorporating item frequency for differentially private set union. In *AAAI*, 2022. URL: https://api.semanticscholar.org/CorpusID:250289456.

7 Justin Y. Chen, Vincent Cohen-Addad, Alessandro Epasto, and Morteza Zadimoghaddam. Scalable private partition selection via adaptive weighting. In *ICML*, 2025. URL: https://openreview.net/forum?id=NEfIaE4BI5.

8 Damien Desfontaines, James Voss, Bryant Gipson, and Chinmoy Mandayam. Differentially private partition selection. *PoPETS*, 2022(1):339–352, November 2021. doi:10.2478/popets-2022-0017.

9 Google Differential Privacy Team. Privacy loss distributions, 2026. URL: https://github.com/google/differential-privacy/blob/main/.

10 Vadym Doroshenko, Badih Ghazi, Pritish Kamath, Ravi Kumar, and Pasin Manurangsi. Connect the dots: Tighter discrete approximations of privacy loss distributions. *PoPETS*, 2022(4):552–570, 2022. doi:10.56553/POPETS-2022-0122.

11 Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *TCC*, pages 265–284, 2006. doi:10.1007/11681878_14.

12 Badih Ghazi, Pritish Kamath, Ravi Kumar, and Pasin Manurangsi. Faster privacy accounting via evolving discretization. In *ICML*, pages 7470–7483, 2022. URL: https://proceedings.mlr.press/v162/ghazi22a.html.

13 Atefeh Gilani, Juan Felipe Gomez, Shahab Asoodeh, Flavio P Calmon, Oliver Kosut, and Lalitha Sankar. Optimal additive noise mechanisms for differential privacy. *arXiv preprint*, 2025. arXiv:2504.14730.

14 Sivakanth Gopi, Pankaj Gulhane, Janardhan Kulkarni, Judy Hanwen Shen, Milad Shokouhi, and Sergey Yekhanin. Differentially private set union. In *ICML*, pages 3627–3636, 2020. URL: https://proceedings.mlr.press/v119/gopi20a.html.

15 Sivakanth Gopi, Yin Tat Lee, and Lukas Wutschitz. Numerical composition of differential privacy. In *NeurIPS*, pages 11631–11642, 2021. URL: https://proceedings.neurips.cc/paper/2021/hash/6097d8f3714205740f30debe1166744e-Abstract.html.

16 Aleksandra Korolova, Krishnaram Kenthapadi, Nina Mishra, and Alexandros Ntoulas. Releasing search queries and clicks privately. In *WWW*, pages 171–180, 2009. doi:10.1145/1526709.1526733.

17 Antti Koskela, Joonas Jälkö, and Antti Honkela. Computing tight differential privacy guarantees using FFT. In *AISTATS*, pages 2560–2569, 2020. URL: http://proceedings.mlr.press/v108/koskela20b.html.

18 Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, Andrew Y. Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, pages 142–150, Portland, Oregon, USA, June 2011. Association for Computational Linguistics. URL: http://www.aclweb.org/anthology/P11-1015.

19 Julian McAuley and Jure Leskovec. Hidden factors and hidden topics: understanding rating dimensions with review text. *Proceedings of the 7th ACM conference on Recommender systems*, 2013. URL: https://api.semanticscholar.org/CorpusID:6440341.

20 Sebastian Meiser and Esfandiar Mohammadi. Tight on budget? Tight bounds for r-fold approximate differential privacy. In *CCS*, pages 247–264, 2018. doi:10.1145/3243734.3243765.

21 Ilya Mironov. Rényi differential privacy. In *CSF*, pages 263–275, 2017. doi:10.1109/CSF.2017.11.

22 Nicolas Papernot and Thomas Steinke. Hyperparameter tuning with renyi differential privacy. In *ICLR*, 2022. URL: https://openreview.net/forum?id=-70L8lpp9DF.

23 Alfréd Rényi. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, 1961.

24 David M. Sommer, Sebastian Meiser, and Esfandiar Mohammadi. Privacy loss classes: The central limit theorem in differential privacy. *PoPETS*, 2019(2):245–269, 2019. doi:10.2478/POPETS-2019-0029.

25 Marika Swanberg, Damien Desfontaines, and Samuel Haney. Dp-sips: A simpler, more scalable mechanism for differentially private partition selection. *PoPETS*, 2023.

26 Tim Van Erven and Peter Harremos. Rényi divergence and kullback-leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014. doi:10.1109/TIT.2014.2320500.

27 Mark Wijkhuizen. Simple/normal wikipedia abstracts v1. URL: https://www.kaggle.com/datasets/markwijkhuizen/simplenormal-wikipedia-abstracts-v1.

28 Royce J Wilson, Celia Yuxin Zhang, William Lam, Damien Desfontaines, Daniel Simmons-Marengo, and Bryant Gipson. Differentially private sql with bounded user contribution. *PoPETS*, 2:230–250, 2020. doi:10.2478/POPETS-2020-0025.

29 Xiang Zhang, Junbo Zhao, and Yann LeCun. Character-level convolutional networks for text classification. In C. Cortes, N. Lawrence, D. Lee, M. Sugiyama, and R. Garnett, editors, *Advances in Neural Information Processing Systems*, volume 28. Curran Associates, Inc., 2015. URL: https://proceedings.neurips.cc/paper_files/paper/2015/file/250cf8b51c773f3f8dc8b4be867a9a02-Paper.pdf.

30 Yuqing Zhu, Jinshuo Dong, and Yu-Xiang Wang. Optimal accounting of differential privacy via characteristic function. In *AISTATS*, pages 4782–4817, 2022. URL: https://proceedings.mlr.press/v151/zhu22c.html.

A Fast Algorithm for Computing Approximate Rényi Divergence

In this section we will outline an improved algorithm for computing $\mathrm{D}_\alpha^\delta(P \parallel Q)$ for discrete distributions. Instead of P', Q', it will be easier to describe an algorithm for finding $\tilde{P} = (1-\delta)P'$ and $\tilde{Q} = (1-\delta)Q'$. The algorithm works as follows:

1. Compute $\tilde{P}$ by finding a cutoff λ_P such that if we clip all likelihood ratios $\tilde{P}(x)/Q(x)$ to be at most λ_P, the total mass removed from P is exactly δ. More formally, find λ_P such that

$$\sum_x \tilde{P}(x) = 1 - \delta \text{ for } \tilde{P}(x) = \min\{P(x), \lambda_P Q(x)\}$$

2. Compute $\tilde{Q}$ by finding a cutoff λ_Q such that if we clip all likelihood ratios $\tilde{P}(x)/\tilde{Q}(x)$ to be at least λ_Q, the total mass removed from Q is exactly δ. That is, find λ_Q such that

$$\sum_x \tilde{Q}(x) = 1 - \delta \text{ for } \tilde{Q}(x) = \min\{Q(x), \tilde{P}(x)/\lambda_Q\}$$

The approximate Rényi divergence between P and Q is just the Rényi divergence between the normalized versions of P' and Q'. Note that λ_P (resp. λ_Q) can be computed simply in $O(n \log n)$ time by iterating over the ratios $P(x)/Q(x)$ (resp. $\tilde{P}(x)/Q(x)$) in a sorted order, and manipulating the cumulative masses. More details and the proof of correctness are given in Appendix A.

It should be noted that, remarkably, the distributions P' and Q' do *not* depend on α at all.

We give more detail of the "water-filling" algorithm from Section 6.1. Throughout this section, we assume that the total variation distance of A, B is greater than δ (i.e. $\sum_x \min\{A(x), B(x)\} < 1 - \delta$). Otherwise, the approximate Rényi divergence is simply zero.

A.1 $O(n \log n)$ Implementation of the Algorithm

To implement the algorithm efficiently, we observe that computing the cutoffs λ_P and λ_Q requires finding a threshold that truncates exactly δ probability mass from the tail of a likelihood ratio distribution. We define a generic subprocedure ComputeCutoff to compute this threshold. This subprocedure takes as input probability distributions A, B over a discrete domain $\mathcal{X}$ of size n, and a target mass $\delta \in (0, 1)$. It then outputs a ratio $\lambda > 1$ such that $\sum_x \min\{A(x), \lambda \cdot B(x)\} = 1 - \delta$.

The subprocedure ComputeCutoff(A, B, δ) works as follows:

1. **Sort Ratios:** Compute the likelihood ratios $r(x) = \frac{A(x)}{B(x)}$ for all $x \in \mathcal{X}$. Sort the domain to $x_1, x_2, \ldots, x_n$ such that $r(x_1) \geq r(x_2) \geq \cdots \geq r(x_n)$. Define an auxiliary bound $r(x_{n+1}) = 0$.
2. **Initialize:** Set cumulative masses $S_A = 0$ and $S_B = 0$.
3. **Linear Scan:** For $k = 1, 2, \ldots, n$:
   a. Update prefix sums: $S_A \leftarrow S_A + A(x_k)$ and $S_B \leftarrow S_B + B(x_k)$.
   b. Calculate the hypothetical mass removed if the cutoff were exactly $r(x_{k+1})$:
   $$\delta_k = S_A - r(x_{k+1}) S_B$$
   c. **Termination:** If $\delta_k \geq \delta$, the exact cutoff λ lies within $[r(x_{k+1}), r(x_k)]$. Because the removed mass is strictly linear with respect to the cutoff in this interval, we simply return:
   $$\lambda = \frac{S_A - \delta}{S_B}$$

Main Algorithm

The cutoffs in our algorithm can then be computed via two independent calls to the subprocedure:

$$\lambda_P = \text{ComputeCutoff}(P, Q, \delta), \qquad \lambda_Q = \frac{1}{\text{ComputeCutoff}(Q, \tilde{P}, \delta)}.$$

This results in $O(n \log n)$-time algorithm as claimed.

A.2 Proof of Correctness

Problem Formulation. Recall that we define $\tilde{P}(x) = (1 - \delta)P'(x)$ and $\tilde{Q}(x) = (1 - \delta)Q'(x)$. The equivalent minimization problem is:

$$\begin{aligned}
\text{minimize} \quad & \sum_x \tilde{P}(x)^\alpha \tilde{Q}(x)^{1-\alpha} \\
\text{subject to} \quad & \sum_x \tilde{P}(x) = 1 - \delta, \quad \sum_x \tilde{Q}(x) = 1 - \delta, \\
& \tilde{P}(x) - P(x) \leq 0, \quad \tilde{Q}(x) - Q(x) \leq 0, \\
& -\tilde{P}(x) \leq 0, \quad -\tilde{Q}(x) \leq 0.
\end{aligned}$$

Note that, for $\alpha > 1$, the objective function $f(\tilde{P}, \tilde{Q}) = \sum_x \tilde{P}(x)^\alpha \tilde{Q}(x)^{1-\alpha}$ is strictly convex.

Lagrangian

Let $\nu_P, \nu_Q \in \mathbb{R}$ be the multipliers for the equality constraints, and $\mu_P(x), \mu_Q(x) \in \mathbb{R}$ be the multipliers for the inequality constraints. The Lagrangian is[11]:

$$\begin{aligned}\mathcal{L}(\tilde{P}, \tilde{Q}, \nu_P, \nu_Q, \mu_P, \mu_Q) = &\sum_x \tilde{P}(x)^\alpha \tilde{Q}(x)^{1-\alpha} \\ &- \nu_P \left(\sum_x \tilde{P}(x) - (1-\delta) \right) - \nu_Q \left(\sum_x \tilde{Q}(x) - (1-\delta) \right) \\ &+ \sum_x \mu_P(x)(\tilde{P}(x) - P(x)) + \sum_x \mu_Q(x)(\tilde{Q}(x) - Q(x)).\end{aligned}$$

Output Solution and Lagrangian Multipliers

Let $\tilde{P}$ and $\tilde{Q}$ be the solutions produced by the water-filling algorithm. We note that $\lambda_P \geq 1 \geq \lambda_Q$. The former inequality follows from our assumption that $\sum_x \min\{P(x), Q(x)\} < 1 - \delta$, while the latter follows from $1 - \delta = \sum_x \tilde{Q}(x) \leq \sum_x \tilde{P}(x)/\lambda_Q = (1-\delta)/\lambda_Q$.

Let $R(x) = \frac{\tilde{P}(x)}{\tilde{Q}(x)}$. The sample space can be partitioned into three regions based on the ratio $\frac{P(x)}{Q(x)}$:

- **Region 1** ($P(x)/Q(x) > \lambda_P$): We have $\tilde{P}(x) = \lambda_P Q(x)$, $\tilde{Q}(x) = Q(x) \implies R(x) = \lambda_P$.
- **Region 2** ($\lambda_Q \leq P(x)/Q(x) \leq \lambda_P$): We have $\tilde{P}(x) = P(x)$, $\tilde{Q}(x) = Q(x) \implies R(x) = \frac{P(x)}{Q(x)}$.
- **Region 3** ($P(x)/Q(x) < \lambda_Q$): We have $\tilde{P}(x) = P(x)$, $\tilde{Q}(x) = \frac{P(x)}{\lambda_Q} \implies R(x) = \lambda_Q$.

We explicitly define the Lagrangian multipliers for this proposed solution as follows:

$$\begin{aligned}\nu_P &= \alpha \lambda_P^{\alpha-1} \\ \nu_Q &= (1-\alpha)\lambda_Q^\alpha \\ \mu_P(x) &= \nu_P - \alpha R(x)^{\alpha-1} = \alpha \left(\lambda_P^{\alpha-1} - R(x)^{\alpha-1} \right) \\ \mu_Q(x) &= \nu_Q - (1-\alpha) R(x)^\alpha = (\alpha - 1) \left(R(x)^\alpha - \lambda_Q^\alpha \right)\end{aligned}$$

Verification of KKT Conditions

Since the problem is strictly convex, the KKT conditions are sufficient for global optimality. We verify that our proposed solution and multipliers satisfy all four KKT conditions:

1. **Stationarity:** By taking the gradient of $\mathcal{L}$ and substituting our defined multipliers, stationarity holds by construction for all x:

$$\begin{aligned}\frac{\partial \mathcal{L}}{\partial \tilde{P}(x)} &= \alpha R(x)^{\alpha-1} - \nu_P + \mu_P(x) = 0 \\ \frac{\partial \mathcal{L}}{\partial \tilde{Q}(x)} &= (1-\alpha) R(x)^\alpha - \nu_Q + \mu_Q(x) = 0\end{aligned}$$

[11] We only consider solutions which are interior points for the lower bounds (non-negativity strictly satisfied) and we thus omit their multipliers. Note that this is without loss of generality since our algorithm's solution satisfies this for all x such that $P(x), Q(x) > 0$. (For all other x's, we are forced to set $\tilde{P}(x) = \tilde{Q}(x) = 0$ anyway.)

2. **Primal Feasibility:** By the definition of the algorithm, $0 \le \tilde{P}(x) \le P(x)$ and $0 \le \tilde{Q}(x) \le Q(x)$. The chosen cutoffs λ_P, λ_Q explicitly guarantee $\sum \tilde{P}(x) = 1 - \delta$ and $\sum \tilde{Q}(x) = 1 - \delta$.
3. **Dual Feasibility:** As discussed above, $R(x) \in [\lambda_P, \lambda_Q]$. Since $\alpha > 1$, we thus have $\mu_P(x) = \alpha(\lambda_P^{\alpha-1} - R(x)^{\alpha-1}) \ge 0$ and $\mu_Q(x) = (\alpha-1)(R(x)^\alpha - \lambda_Q^\alpha) \ge 0$.
4. **Complementary Slackness:**
   - For $\tilde{P}$: If $\tilde{P}(x) < P(x)$, then x must be in Region 1, meaning $R(x) = \lambda_P$. Substituting this yields $\mu_P(x) = \alpha(\lambda_P^{\alpha-1} - R(x)^{\alpha-1}) = 0$. Thus, $\mu_P(x)(\tilde{P}(x) - P(x)) = 0$ for all x.
   - For $\tilde{Q}$: If $\tilde{Q}(x) < Q(x)$, then x must be in Region 3, meaning $R(x) = \lambda_Q$. Substituting this yields $\mu_Q(x) = (\alpha-1)(\lambda_Q^\alpha - \lambda_Q^\alpha) = 0$. Thus, $\mu_Q(x)(\tilde{Q}(x) - Q(x)) = 0$ for all x.

The solution generated by the sequential water-filling algorithm, coupled with the defined multipliers, satisfies the KKT sufficiency conditions. As a result, the solution is optimal. ◀

B Truncated discrete Laplace convergence

In the following proof, we use $[x]_+$ as a shorthand for $\max\{x, 0\}$. Furthermore, recall that the (ε, δ)-DP can be characterized by the hockey stick divergence, which will be more convenient for us to work with. Namely, let

$$\mathrm{D}_{e^\varepsilon}^{\mathrm{hs}}(P \parallel Q) = \int_\Omega [P(x) - e^\varepsilon \cdot Q(x)]_+ \, dx.$$

It is known that $D_\infty^\delta(P\|Q) \le \varepsilon$ if and only if $\mathrm{D}_{e^\varepsilon}^{\mathrm{hs}}(P \parallel Q) \le \delta$. We will use the latter formulation in the proof below.

Proof of Proposition 27. We will first consider the case $\delta \in (0, 1/n_d]$. Define $Z(\varepsilon) = \delta \sum_{x=0}^{n_d-1} e^{\varepsilon(\mu - |x-\mu|)}$. Let ε^* be the unique[12] non-negative real number such that $Z(\varepsilon^*) = 1$. Finally, let P^* denote the truncated discrete Laplace distribution supported on $\{0, \dots, n_d - 1\}$ with $P^*(x) = \delta \cdot e^{\varepsilon^*(\mu - |x-\mu|)}$. This is a valid distribution since $Z(\varepsilon^*) = 1$, and it is simple to check that $\mathrm{D}_{e^{\varepsilon^*}}^{\mathrm{hs}}\left(P^* \parallel P_+^*\right) = \delta$, implying that the resulting additive mechanism is (ε^*, δ)-DP as desired.

Suppose for the sake of contradiction that there is some other distribution $\tilde{P}$ supported on $\{0, \dots, n_d - 1\}$ that satisfies $(\tilde{\varepsilon}, \delta)$-DP for some $\tilde{\varepsilon} < \varepsilon$. By Proposition 24, we may assume without loss of generality that $\tilde{P}$ is symmetric around μ. Then, consider any $i \in \{1, \dots, n_d - 1\}$. Since $\tilde{P}$ satisfies $(\tilde{\varepsilon}, \delta)$-DP, we have

$$\begin{aligned}
\delta \ge \mathrm{D}_{e^{\tilde{\varepsilon}}}^{\mathrm{hs}}\left(\tilde{P} \parallel \tilde{P}_+\right) &= \sum_{x \in \{0,\dots,n_d-1\}} \left[\tilde{P}(x) - e^{\tilde{\varepsilon}} \cdot \tilde{P}(x-1)\right]_+ \\
&\ge \sum_{x \in \{0,\dots,i\}} e^{-\tilde{\varepsilon}x} \cdot \left[\tilde{P}(x) - e^{\tilde{\varepsilon}} \cdot \tilde{P}(x-1)\right]_+ \\
&\ge \sum_{x \in \{0,\dots,i\}} e^{-\tilde{\varepsilon}x} \cdot \left(\tilde{P}(x) - e^{\tilde{\varepsilon}} \cdot \tilde{P}(x-1)\right) \\
&= e^{-\tilde{\varepsilon}x} \cdot \tilde{P}(x).
\end{aligned}$$

From this and from symmetry of $\tilde{P}$, we have

$$\tilde{P}(x) \le \delta \cdot \min\{e^{\tilde{\varepsilon}x}, e^{\tilde{\varepsilon}(n_d - 1 - x)}\} = \delta \cdot e^{\tilde{\varepsilon}(\mu - |x-\mu|)} < P^*(x). \tag{3}$$

[12] The uniqueness follows from monotonicity of $Z(\varepsilon)$, $Z(0) = n_d\delta \le 1$ and $\lim_{\varepsilon\to\infty} Z(\varepsilon) = \infty$.

However, this means that

$$\sum_{x\in\{0,\dots,n_d-1\}} \tilde{P}(x) < \sum_{x\in\{0,\dots,n_d-1\}} P^*(x) = 1,$$

which is a contradiction since $\tilde{P}$ is a distribution.

To see the uniqueness of P^* for (ε^*, δ)-DP, notice that, when $\tilde{\varepsilon} = \varepsilon^*$, (3) becomes $\tilde{P}(x) \leq P^*(x)$ for all x. Since both $\tilde{P}$ and P^* are distributions, this implies that they must be the same.

For the case of $\delta \in (1/n_d, 1]$, it is simple to verify that the uniform distribution satisfies (ε, δ)-DP for $\varepsilon = 0$, and this is the smallest ε possible. ◀