# Optimal Noise Adding Mechanisms for Approximate Differential Privacy

Quan Geng and Pramod Viswanath, *Fellow, IEEE*

***Abstract*— We study the (nearly) optimal mechanisms in $(\epsilon, \delta)$-differential privacy for integer-valued query functions and vector-valued (histogram-like) query functions under a utility-maximization/cost-minimization framework. Within the classes of mechanisms oblivious of the database and the queries beyond the global sensitivity, we characterize the tradeoff between $\epsilon$ and $\delta$ in utility and privacy analysis for histogram-like query functions, and show that the $(\epsilon, \delta)$-differential privacy is a framework not much more general than the $(\epsilon, 0)$-differential privacy and $(0, \delta)$-differential privacy in the context of $\ell^1$ and $\ell^2$ cost functions, i.e., minimum expected noise magnitude and noise power. In the same context of $\ell^1$ and $\ell^2$ cost functions, we show the near-optimality of uniform noise mechanism and discrete Laplacian mechanism in the high privacy regime (as $(\epsilon, \delta) \to (0, 0)$). We conclude that in $(\epsilon, \delta)$-differential privacy, the optimal noise magnitude and the noise power are $\Theta(\min((1/\epsilon), (1/\delta)))$ and $\Theta(\min((1/\epsilon^2), (1/\delta^2)))$, respectively, in the high privacy regime.**

***Index Terms*— Data privacy, randomized algorithm.**

## I. Introduction

DIFFERENTIAL privacy is a framework to quantify to what extent individual privacy in a statistical database is preserved while releasing useful statistical information about the database [1]. The basic idea of differential privacy is that the presence of any individual data in the database should not affect the final released statistical information significantly, and thus it can give strong privacy guarantees against an adversary with arbitrary auxiliary information. For more background and motivation of differential privacy, we refer the readers to the survey [2].

The standard approach to preserve $\epsilon$-differential privacy for real-valued query function is to perturb the query output by adding random noise with Laplacian distribution. Recently, Geng and Viswanath [3] show that under a general utility-maximization framework, for single real-valued query function, the optimal $\epsilon$-differentially private mechanism is the staircase mechanism, which adds noise with staircase distribution to the query output. The optimality of the staircase mechanism is extended to the multidimensional setting for histogram-like functions in [4], where the sensitivity of the query functions is defined using the $\ell^1$ metric as in [1]. A relaxed notion of privacy, $(\epsilon, \delta)$-differential privacy, was introduced by Dwork et al. [5], and the standard approach to preserving $(\epsilon, \delta)$-differential privacy is to add Gaussian noise to the query output.

In this work, we study the (nearly) optimal mechanisms in $(\epsilon, \delta)$-differential privacy for integer-valued query functions and vector-valued (histogram-like) query functions under a utility-maximization/cost-minimization framework, and characterize the tradeoff between $\epsilon$ and $\delta$ in utility and privacy analysis. Optimality in this work is defined with respect to the class of the mechanisms which are oblivious of the database and the properties of query functions except the global sensitivity. We refer the readers to the end of Section I.A for more details about the setting considered in this work.

$(\epsilon, \delta)$-differential privacy is a relaxed notion of privacy, compared to the standard $\epsilon$-differential privacy introduced in [1]. $(\epsilon, \delta)$-differential privacy includes as special cases:

- $(\epsilon, 0)$-differential privacy; in this standard setting, the optimal mechanism for a general cost minimization framework is the *staircase* mechanism as shown in [3] and [4]. In the high privacy regime, the standard discrete Laplacian mechanism too performs well.
- $(0, \delta)$-differential privacy; this setting requires that the total variation of the conditional probability distributions of the query output for neighboring datasets should be bounded by $\delta$. In this paper we show that the uniform noise distribution is near-optimal in the $(0, \delta)$-differential privacy setting for a general class of cost functions.

While the $(\epsilon, \delta)$-differential privacy setting is more general than the two special cases – $(\epsilon, 0)$ and $(0, \delta)$-differential privacy – our main result in this work is to show that within the classes of mechanisms oblivious of the database and the queries beyond the global sensitivity, it is only more general by *very little*; this is done in the context of $\ell^1$ and $\ell^2$ cost functions. We show the near-optimality of uniform noise and discrete Laplacian mechanisms in the high privacy regime (as $(\epsilon, \delta) \to (0, 0)$) for $\ell^1$ and $\ell^2$ cost functions.

Our result is a sharp departure from the setting of $\ell^\infty$ sensitivity (modeling adaptive query compositions) where the notion of $(\epsilon, \delta)$-approximate differential privacy provides significant variance reductions (in the dimension of the query output), as compared to the standard $(\epsilon, 0)$-differential privacy [1], [6], [7]. Our main result shows that such gains

Manuscript received January 8, 2014; revised August 10, 2015; accepted November 23, 2015. Date of publication December 11, 2015; date of current version January 18, 2016. This work was supported in part by the National Science Foundation under Grant CCF-1422278 and in part by the University of Illinois at Urbana–Champaign. This paper was presented at the 2013 Workshop on Big Data and Differential Privacy, Simons Institute for Theory of Computing.

Q. Geng was with the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign, Urbana, IL 61801 USA. He is now with Google Inc., New York, NY 10011 USA (e-mail: gengquanshine@gmail.com).

P. Viswanath is with the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign, Urbana, IL 61801 USA (e-mail: pramodv@illinois.edu).

Communicated by A. Smith, Associate Editor for Complexity and Cryptography.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2015.2504972

are not available in the $\ell^1$ sensitivity model for mechanisms oblivious of the database and queries - in fact approximate differential privacy in the usual regime ($\delta \ll \epsilon$) is nearly the same (up to constants, in added noise magnitude and variance) as pure differential privacy. For completeness, we consider all relationships between $\epsilon$ and $\delta$ in this paper.

The near-optimality of the two mechanisms (designed for the special cases of $(\epsilon, 0)$ and $(0, \delta)$ differential privacy settings) is proved by demonstrating a uniform bound on the ratio between the costs of these two mechanisms and that of the optimal cost in the $(\epsilon, \delta)$ differential privacy setting in the high privacy regime, i.e., as $(\epsilon, \delta) \to (0, 0)$ for $\ell^1$ and $\ell^2$ cost functions.

### *A. Summary of Our Results*

In this work we consider a very general model for integer-valued and vector-valued (histogram-like) query functions. Unlike previous works on $(\epsilon, \delta)$-differential privacy (e.g., [8]–[10]), in this work we consider privacy mechanisms which are oblivious of the queries and the database, except for knowing the global sensitivity in the $\ell_1$ metric.[1] We implicitly assume that the local sensitivity is equal to the global sensitivity. Due to the optimality of query-output independent perturbation (under a technical condition) in a min-max cost framework as shown in [3, Th. 2], in this work we restrict ourselves to query-output independent perturbation mechanisms.[2]

We summarize our results in the following. Let $V_{LB}$ denote the lower bound we derived for the cost under differential privacy constraint (it is a different lower bound for each type of differential privacy constraints specified in the items below). Let $V_{UB}^{\text{Lap}}$ and $V_{UB}^{\text{uniform}}$ denote the upper bounds for the cost achieved by discrete Laplacian mechanism and uniform noise mechanism. In this work, we show that

- For integer-valued query functions,
  - for $(0, \delta)$-differential privacy with the global sensitivity $\Delta = 1$, the uniform noise mechanism is optimal for all generic cost funtions,
  - for $(0, \delta)$-differential privacy with arbitrary global sensitivity $\Delta$, $\lim_{\delta \to 0} \frac{V_{UB}^{\text{uniform}}}{V_{LB}} = 1$ for $\ell^1$ and $\ell^2$ cost functions,
  - for $(\epsilon, \delta)$-differential privacy with $\ell^1$ and $\ell^2$ cost functions, $\limsup_{(\epsilon,\delta)\to(0,0)} \frac{\min(V_{UB}^{\text{Lap}}, V_{UB}^{\text{uniform}})}{V_{LB}} \le C$ for some numerical constant $C$.
- For vector-valued (histogram-like) query functions,
  - for $(0, \delta)$-differential privacy with the global sensitivity $\Delta = 1$, the multi-dimensional uniform noise mechanism is optimal for $\ell^1$ and $\ell^2$ cost functions,
  - for $(0, \delta)$-differential privacy with arbitrary global sensitivity $\Delta$, $\lim_{\delta \to 0} \frac{V_{UB}^{\text{uniform}}}{V_{LB}} = 1$ for $\ell^1$ and $\ell^2$ cost functions,
  - for $(\epsilon, \delta)$-differential privacy with $\ell^1$ and $\ell^2$ cost functions, $\limsup_{(\epsilon,\delta)\to(0,0)} \frac{\min(V_{UB}^{\text{Lap}}, V_{UB}^{\text{uniform}})}{V_{LB}} \le C$ for some numerical constant $C$, which is independent of the dimension of the query function.

We conclude that in $(\epsilon, \delta)$-differential privacy, the optimal noise magnitude and noise power are $\Theta(\min(\frac{d\Delta}{\epsilon}, \frac{d\Delta}{\delta}))$ and $\Theta(\min(\frac{d\Delta^2}{\epsilon^2}, \frac{d\Delta^2}{\delta^2}))$, respectively, in the high privacy regime, and naturally, the total cost grows linearly in terms of the dimension of the query output.

We emphasize that these results are derived under the following settings:

- when the domain of the query output is the entire set of integers or $\mathbb{Z}^d$, or the mechanism is oblivious of the database;
- nothing more about the query function is known beyond its global sensitivity;
- either the local sensitivity [11] of the query function is unknown or it is the same as global sensitivity.

If any of these conditions are violated (the output domain has sharp boundaries, or the local sensitivity deviates from the global sensitivity [11], or we are restricted to specific query functions [12]), then the optimal privacy mechanism need not be data or query output independent, and the bounds derived in this work may not apply.

### *B. Related Work*

Dwork et al. [1] introduce $\epsilon$-differential privacy and show that the Laplacian mechanism, which perturbs the query output by adding random noise with Laplace distribution proportional to the global sensitivity of the query function, can preserve $\epsilon$-differential privacy. In [1], it is shown that for histogram-like query functions, where the query output has multiple components and the global sensitivity is defined using the $\ell^1$ metric, one can perturb each component independently by adding the Laplacian noise to preserve $\epsilon$-differential privacy.

Nissim *et al.* [11] show that for certain nonlinear query functions, one can improve the accuracy by adding data-dependent noise calibrated to the smooth sensitivity of the query function, which is based on the local sensitivity of the query function. McSherry and Talwar [13] introduce the *exponential mechanism* to preserve $\epsilon$-differential privacy for general query functions in an abstract setting, where the query function may not be real-valued. Dwork et al. [5] introduce $(\epsilon, \delta)$-differential privacy and show that adding random noise with Gaussian distribution can preserve $(\epsilon, \delta)$-differential privacy for real-valued query functions. Hall *et al.* [14] study how to preserve

[1] For vector-valued query function $q(\cdot) : \mathcal{D} \to \mathbb{Z}^d$, where $d$ is the dimension of the query output, we assume that for any $\mathbf{v} \in \mathbb{Z}^d$, the mechanism has to consider the case there might exist a dataset $D$ such that $q(D) = \mathbf{v}$, and for any $\mathbf{v}'$ such that $\|\mathbf{v} - \mathbf{v}'\|_1 \le \Delta$, where $\Delta$ is the global sensitivity of $q(\cdot)$, there might exist a neighboring dataset $D'$ such that $q(D') = \mathbf{v}'$.

[2] Under the setting that the query function is real-valued and the released query output is also real-valued (either scalar or vector), all privacy preserving mechanisms can be viewed as noise-adding mechanisms, where the noise can be defined as the difference between the true query output and the released query output, and the noise can be either dependent on or independent of the true query output. Specifically, a privacy preserving mechanism can be characterized by a family of probability distributions $\{\mathcal{P}_t\}_{t \in \mathbb{R}}$, where $\mathcal{P}_t$ is the probability distribution of the noise when the query output is $t$. In [3], we show that in the single dimensional setting, under the assumption that $\{\mathcal{P}_t\}_{t \in \mathbb{R}}$ is piecewise constant and periodic (the period can be arbitrary) both in terms of the index $t$, then under a min-max cost framework, query-output independent perturbation is optimal. In the multidimensional setting, under the same assumption that the family of noise probability distributions $\{\mathcal{P}_t\}_{t \in \mathbb{R}^d}$ is piecewise constant and periodic in terms of the index $t$, query-output independent perturbation is optimal.

$(\epsilon, \delta)$-differential privacy for releasing (infinite dimensional) functions, and show that adding Gaussian process noise to the released function can preserve $(\epsilon, \delta)$-differential privacy. Kasiviswanathan and Smith [15] study the semantics of $(\epsilon, \delta)$-differential privacy under a Bayesian framework. Chaudhuri and Mishra [16], and Machanavajjhala et al. [17] propose different variants of the standard $(\epsilon, \delta)$-differential privacy.

Ghosh *et al.* [18] show that for a single count query with sensitivity $\Delta = 1$, for a general class of utility functions, to minimize the expected cost under a Bayesian framework the optimal mechanism to preserve $\epsilon$-differential privacy is the geometric mechanism, which adds noise with geometric distribution. Brenner and Nissim [19] show that for general query functions no universally optimal mechanisms exist. Gupte and Sundararajan [20] derive the optimal noise probability distributions for a single count query with sensitivity $\Delta = 1$ for minimax (risk-averse) users. Gupte and Sundararajan [20] show that although there is no universally optimal solution to the minimax optimization problem in [20] for a general class of cost functions, each solution (corresponding to different cost functions) can be derived from the same geometric mechanism by randomly remapping. Geng and Viswanath [3] generalize the results of [18] and [20] to real-valued (and integer-valued) query functions with arbitrary sensitivity, and show that the optimal query-output independent perturbation mechanism is the staircase mechanism, which adds noise with a staircase-shaped probability density function (or probability mass function for integer-valued query function) to the query output. The optimality of the staircase mechanism is extended to the multidimensional setting for histogram-like functions in [4], where the sensitivity of the query functions is defined using the $\ell^1$ metric as in [1].

Differential privacy for histogram query functions has been widely studied in the literature, e.g., [8], [21]–[25], and many existing works use the Laplacian mechanism as the basic tool. For instance, Li et al. [25] introduce the matrix mechanism to answer batches of linear queries over a histogram in a differentially private way with good accuracy guarantees. Their approach is that instead of adding Laplacian noise to the workload query output directly, the matrix mechanism will design an observation matrix which is the input to the database, from perturbed output (using the standard Laplace mechanism) estimate the histogram itself, and then compute the query output directly. Li et al. [25] show that this two-stage process will preserve differential privacy and increase the accuracy. Hay et al. [22] show that for a general class of histogram queries, by exploiting the consistency constraints on the query output, which is differentially private by adding independent Laplace noises, one can improve the accuracy while still satisfying differential privacy. These existing works study how to efficiently answer a set of linear queries on the histogram, while our work addresses the problem of releasing the histogram itself, which can be viewed as the worst-case query release (without knowing which linear queries will be asked).

Hardt and Talwar [23] study the tradeoff between privacy and error for answering a set of linear queries over a histogram under $\epsilon$-differential privacy. The error is defined as the worst expectation of the $\ell^2$-norm of the noise. Hardt and Talwar [23] derives a lower bound for the error in the high privacy regime by using tools from convex geometry, and gives an upper bound by analyzing a differentially private mechanism, $K$-norm mechanism, which is an instantiation of the exponential mechanism and involves randomly sampling from a high dimensional convex body. The lower bound given in [23] depends on the volume of a convex body associated with the linear query functions, and the lower bound works for arbitrary linear query functions. In our problem setting, the linear query functions we are studying are the histogram function, which is a special case of [23] by setting $d = n$ and setting $F$ to be the identity map function. In this case, the lower bound given in [23] is $\Omega(\frac{\sqrt{d}}{\epsilon})$,[3] which matches our result, as we show that for $\epsilon$-differential privacy, in the high privacy regime, adding independent Laplacian noises to each component of the histogram is asymptotically optimal in the context of $\ell^1$ and $\ell^2$ cost functions.

Nikolov *et al.* [8] extend the result of [23] on answering linear queries over a histogram to the case of $(\epsilon, \delta)$-differential privacy. Using tools from discrepancy theory, convex geometry and statistical estimation, they derive lower bounds and upper bounds of the error, which are within a multiplicative factor of $O(\log \frac{1}{\delta})$ in terms of $\delta$. Their bounds work for any set of linear query functions over a histogram, while in our work we study only the identity function, i.e., the query output is the histogram itself. Our result shows that in the high privacy regime (as $(\epsilon, \delta) \to (0, 0)$), the optimal error scales as $\Theta(\min(\frac{1}{\epsilon}, \frac{1}{\delta}))$ and $\Theta(\min(\frac{1}{\epsilon^2}, \frac{1}{\delta^2}))$ for $\ell^1$ and $\ell^2$ cost functions, respectively. Therefore, our results significantly improve the bounds in [8] in terms of $\epsilon$ and $\delta$ in the high privacy regime where both $\epsilon$ and $\delta$ go to zero.

Kasiviswanathan *et al.* [9] derive lower bounds on the noise for releasing contingency tables under $(\epsilon, \delta)$-differential privacy constraint, where the lower bounds depend on the size and structure of the database. Our lower bounds are tighter and sharper than those of [9] in terms of $\epsilon$ and $\delta$. For instance, in [9], for $(\epsilon, \delta)$-differential privacy the lower bounds are proportional to $(1 - \frac{\delta}{\epsilon})$, which are zero whenever $\delta = \epsilon$, while our results show that the lower bound is $\Theta(\min(\frac{1}{\epsilon}, \frac{1}{\delta}))$ as $(\epsilon, \delta) \to (0, 0)$.

De [10] studies lower bound on the additive noise for Lipschitz query functions in $(\epsilon, \delta)$-differential privacy which uses a different metric for the noise, and the lower bound depends on the size of the database. Jain *et al.* [26] study how to preserve $(\epsilon, \delta)$-differential privacy for online learning algorithms, and show that the approximate differential privacy can be achieved by adding Gaussian noise to each component of the query output. They derive upper bounds on the noise, and the upper bounds can be viewed as an application of the composition theorem in [7] by Dwork, Rothblum, and Vadhan, which has been improved by Kairouz *et al.* [27] recently. The difference of [26] and other related works from our work is that the global sensitivity of the query function is defined

[3] Note that for the $d$-dimensional $\ell^1$ unit ball, the volume is $\frac{2^d}{d!}$, and thus in [23, Th. 3.4], $\text{Vol}(K)^{1/d} = \Theta(\frac{1}{d})$.

using $\ell^\infty$ metric in [7] and [26], while in our work we use $\ell^1$ metric.

### C. Organization

This paper is organized as follows. We formulate the utility-maximization/cost-minimization under the $(\epsilon,\delta)$-differential privacy constraint for a single integer-valued query function as a linear programming problem in Section II. In Section III, we study $(0,\delta)$-differential privacy, and show the near optimality of the simple uniform noise mechanism. In Section IV, we study the optimal mechanisms in $(\epsilon,\delta)$-differential privacy, and show the optimality of uniform noise mechanism and Laplacian mechanism in the regime $(\epsilon,\delta) \to (0,0)$ in the context of $\ell^1$ and $\ell^2$ cost functions. In Section V, we extend the results to the multidimensional setting for histogram-like query functions, where the query output is a vector of integers.

## II. Problem Formulation

Consider an integer-valued query function

$$q : \mathcal{D} \to \mathbb{Z}, \tag{1}$$

where $\mathcal{D}$ is the set of all possible datasets.

The sensitivity of the query function $q$ is defined as

$$\Delta \triangleq \max_{D_1,D_2\in\mathcal{D}:|D_1-D_2|\le 1} |q(D_1)-q(D_2)|, \tag{2}$$

where the maximum is taken over all possible pairs of neighboring datasets $D_1$ and $D_2$ which differ in at most one element, i.e., one is a proper subset of the other and the larger dataset contains just one additional element [2]. Clearly, $\Delta$ is an integer in this discrete setting.

*Definition 1 ($(\epsilon,\delta)$-Differential Privacy [5]): A randomized mechanism $\mathcal{K}$ gives $\epsilon$-differential privacy if for all data sets $D_1$ and $D_2$ differing on at most one element, and all $S \subset Range(\mathcal{K})$,*

$$Pr[\mathcal{K}(D_1)\in S] \le \exp(\epsilon) Pr[\mathcal{K}(D_2)\in S] + \delta. \tag{3}$$

### A. Operational Meaning of $(\epsilon,\delta)$-Differential Privacy in the Context of Hypothesis Testing

We first give an operational interpretation of differential privacy in the context of hypothesis testing. While this interpretation is not directly used for proving the results in this paper, it is a useful tool for building the intuition and is useful in other contexts [27].

As shown by [28], one can interpret the differential privacy constraint (3) in the context of hypothesis testing in terms of false alarm probability and missing detection probability. Indeed, consider a binary hypothesis testing problem over two neighboring datasets, $H_0 : D_1$ versus $H_1 : D_2$, where an individual's record is in $D_2$ only. Given a decision rule, let $S$ be the decision region such that when the released output lies in $S$, $H_1$ will be rejected, and when the released output lies in $S^C$ (the complement of $S$), $H_0$ will be rejected. The false alarm probability $P_{FA}$ and the missing detection probability $P_{MD}$ can be written as

$$P_{FA} = P(K(D_1)\in S^C), \tag{4}$$

$$P_{MD} = P(K(D_2)\in S). \tag{5}$$

Therefore, from (3) we get

$$1 - P_{FA} \le e^\epsilon P_{MD} + \delta. \tag{6}$$

Thus

$$e^\epsilon P_{MD} + P_{FA} \ge 1-\delta. \tag{7}$$

Switch $D_1$ and $D_2$ in (3), and we get

$$\Pr[\mathcal{K}(D_2)\in S] \le \exp(\epsilon)\Pr[\mathcal{K}(D_1)\in S] + \delta. \tag{8}$$

Therefore,

$$1 - P_{MD} \le e^\epsilon P_{FA} + \delta, \tag{9}$$

and thus

$$P_{MD} + e^\epsilon P_{FA} \ge 1-\delta. \tag{10}$$

In conclusion, we have

$$e^\epsilon P_{MD} + P_{FA} \ge 1-\delta, \tag{11}$$

$$P_{MD} + e^\epsilon P_{FA} \ge 1-\delta. \tag{12}$$

The $(\epsilon,\delta)$-differential privacy constraint implies that in the context of hypothesis testing, $P_{FA}$ and $P_{MD}$ can not be both too small.

We plot the regions of $P_{FA}$ and $P_{MD}$ under $(\epsilon,\delta)$-differential privacy, and under two special cases: $(\epsilon,0)$ and $(0,\delta)$-differential privacy, in Figure 1.

### B. Cost-Minimization/Utility-Maximization Formulation

The standard approach to preserving differential privacy is to add noise to the output of query function. Let $q(D)$ be the value of the query function evaluated at $D\in\mathcal{D}$, the noise-adding mechanism $\mathcal{K}$ will output

$$\mathcal{K}(D) = q(D) + X, \tag{13}$$

where $X$ is the noise added by the mechanism to the output of query function. To make the output of the mechanism be valid, i.e., $q(D)+X\in\mathbb{Z}$, $X$ can only take integer values.

Let $\mathcal{P}$ be the probability mass function of the noise $X$, and use $\mathcal{P}_i$ to denote $\Pr[X=i]$. For a set $S\subset\mathbb{Z}$, denote $\Pr[X\in S]$ by $\mathcal{P}_S$.

In the following we derive the differential privacy constraint on the probability distribution of $X$ from (3).

$$\Pr[\mathcal{K}(D_1)\in S] \le \exp(\epsilon)\Pr[\mathcal{K}(D_2)\in S] + \delta \tag{14}$$

$$\Leftrightarrow \Pr[q(D_1)+X\in S] \le \exp(\epsilon)\Pr[q(D_2)+X\in S]+\delta \tag{15}$$

$$\Leftrightarrow \mathcal{P}_{S-q(D_1)} \le \exp(\epsilon)\mathcal{P}_{S-q(D_2)} + \delta \tag{16}$$

$$\Leftrightarrow \mathcal{P}_{S'} \le \exp(\epsilon)\mathcal{P}_{S'+q(D_1)-q(D_2)} + \delta, \tag{17}$$

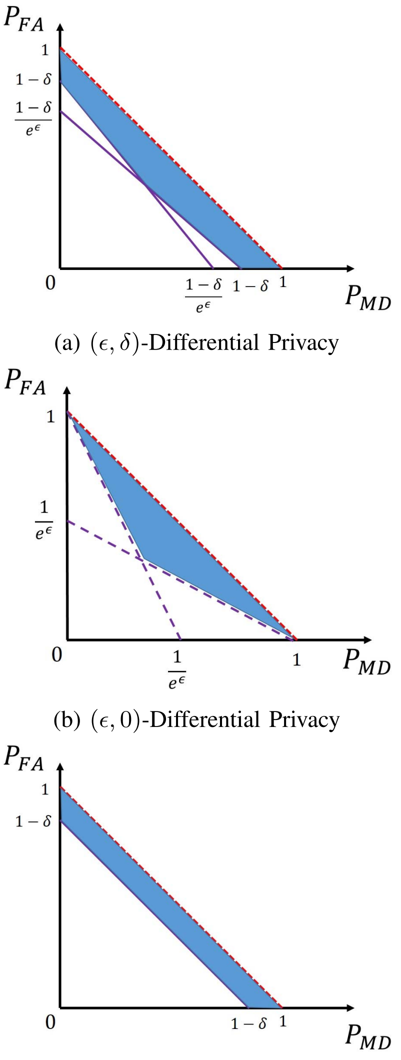
where $S' \triangleq S - q(D_1) = \{s-q(D_1) | s\in S\}$.

Since (3) holds for any set $S\subseteq\mathbb{Z}$, and $|q(D_1)-q(D_2)|\le\Delta$, from (17) we have

$$\mathcal{P}_S \le \exp(\epsilon)\mathcal{P}_{S+d} + \delta, \tag{18}$$

for any set $S\subseteq\mathbb{Z}$ and for all $|d|\le\Delta$.

Consider a cost function $\mathcal{L}(\cdot) : \mathbb{Z}\to\mathbb{R}$, which is a function of the added noise $X$. Our goal is to minimize the



(a) $(\epsilon, \delta)$-Differential Privacy

(b) $(\epsilon, 0)$-Differential Privacy

(c) $(0, \delta)$-Differential Privacy

Fig. 1. Regions of $P_{MD}$ and $P_{FA}$ in $(\epsilon, \delta)$, $(\epsilon, 0)$ and $(0, \delta)$-Differential Privacy.

expectation of the cost subject to the $(\epsilon, \delta)$-differential privacy constraint (18):

$$V^* := \min_{\mathcal{P}} \sum_{i=-\infty}^{+\infty} \mathcal{L}(i)\mathcal{P}(i)$$
$$\text{subject to } \mathcal{P}_S \leq \exp(\epsilon)\mathcal{P}_{S+d} + \delta, \quad \forall S \subset \mathbb{Z}, \quad d \in \mathbb{Z}, \ |d| \leq |\Delta|. \tag{19}$$

In this work, we restrict our attention to the scenario when the cost function $\mathcal{L}(k)$ is symmetric (around $k = 0$) and monotonically increasing for $k \geq 0$. Furthermore, without loss of generality, we assume $\mathcal{L}(0) = 0$. Using the same argument in [3, Lemma 28], we only need to consider symmetric noise probability distributions.

## III. $(0, \delta)$-Differential Privacy

We first consider the simple case when $\epsilon = 0$, i.e., $(0, \delta)$-differential privacy. The $(0, \delta)$-differential privacy constraint requires that the total variation of the conditional probability distributions of the query output for neighboring datasets should be bounded by $\delta$.

In the differential privacy constraint (18), by choosing the subset $S = S_k := \{\ell : \ell \geq k\}$ for $k \in \mathbb{N}$ and $d = \Delta$, we see that the noise probability distribution $\mathcal{P}$ must satisfy the constraints

$$\sum_{\ell=0}^{\Delta-1} \mathcal{P}_{k+\ell} \leq \delta, \quad \forall k \in \mathbb{N}. \tag{20}$$

This relaxation enables us to prove lower bounds on $V^*$.

### *A. $\Delta = 1$*

In the special case $\Delta = 1$, the constraints in (20) are particularly simple:

$$\mathcal{P}_k \leq \delta, \quad \forall k \in \mathbb{N}. \tag{21}$$

For symmetric cost functions $\mathcal{L}(k)$ that are monotonically increasing in $k \geq 0$, we can now readily argue that the *uniform* probability distribution is optimal.

To avoid integer rounding issues, assume $\frac{1}{2\delta}$ is an integer.

*Theorem 1: If $\Delta = 1$, then*

$$V^* = \sum_{k=-\frac{1}{2\delta}}^{\frac{1}{2\delta}-1} \delta\mathcal{L}(k), \tag{22}$$

*and the optimal noise probability distribution is*

$$\mathcal{P}_k = \begin{cases} \delta & -\frac{1}{2\delta} \leq k \leq \frac{1}{2\delta} - 1 \\ 0 & \textit{otherwise} \end{cases} \tag{23}$$

*Proof:* For $\Delta = 1$, the constraints in (20) become $\mathcal{P}_k \leq \delta, \quad \forall k \in \mathbb{N}$. Since the cost function $\mathcal{L}(k)$ is symmetric and monotonically increasing for $k \geq 0$, to minimize the cost we should let the noise probability mass function concentrate around $k = 0$ as much as possible, while satisfying the constraint $\mathcal{P}_k \leq \delta, \quad \forall k \in \mathbb{N}$. Therefore, the optimal noise probability mass function is (23), and it is easy to verify that it satisfies the $(0, \delta)$-differential privacy constraint (18). ■

### *B. General Lower Bound for $\Delta \geq 2$*

We now turn to understanding (near) optimal $(0, \delta)$ privacy mechanisms in terms of minimizing the expected loss when the sensitivity $\Delta \geq 2$.

Recall that in $(0, \delta)$-differential privacy, the minimum cost $V^*$ is the result of the following optimization problem, which is a linear program:

$$\begin{aligned} V^* := \min & \sum_{k=-\infty}^{+\infty} \mathcal{L}(k)\mathcal{P}_k \\ \text{s.t. } & \mathcal{P}_k \geq 0 \quad \forall k \in N \\ & \sum_{k=-\infty}^{+\infty} \mathcal{P}_k = 1 \\ & \mathcal{P}_S \leq \mathcal{P}_{S+d} + \delta, \quad \forall S \subset \mathbb{Z}, \ d \in \mathbb{Z}, \ |d| \leq |\Delta|. \end{aligned} \tag{24}$$

Since $\mathcal{L}(\cdot)$ is a symmetric function, we can assume $\mathcal{P}$ is a symmetric probability distribution. In addition, we relax the constraint (24) by choosing $d = \Delta$ and $S = S_k$ for $k \in \mathbb{N}$. Then we get a relaxed linear program, the solution of which is a lower bound for $V^*$. More precisely,

$$V_{LB} := \min \ 2\sum_{k=1}^{\infty} \mathcal{L}(k)\mathcal{P}_k \tag{25}$$

$$\text{s.t. } \mathcal{P}_k \geq 0 \quad \forall k \in N$$

$$\frac{\mathcal{P}_0}{2} + \sum_{k=1}^{\infty} \mathcal{P}_k \geq \frac{1}{2} \tag{26}$$

$$-\sum_{\ell=0}^{\Delta-1} \mathcal{P}_{k+\ell} \geq -\delta, \quad \forall k \in \mathbb{N}. \tag{27}$$

To avoid integer rounding issues, assume $\frac{1}{2\delta}$ is a positive integer.

*Theorem 2: If*

$$\mathcal{L}(1 + \frac{\Delta}{2\delta}) \geq 2\left(\mathcal{L}(1) + \sum_{i=1}^{\frac{1}{2\delta}} (\mathcal{L}(1 + i\,\Delta) - \mathcal{L}(i\,\Delta))\right), \tag{28}$$

*then*

$$V^* \geq V_{LB} = 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\,\Delta). \tag{29}$$

*Proof:* See Appendix A. ■

### *C. Uniform Noise Mechanism*

Consider the noise with the *uniform* probability distribution:

$$\mathcal{P}_k = \begin{cases} \frac{\delta}{\Delta} & \forall -\frac{\Delta}{2\delta} \leq k \leq \frac{\Delta}{2\delta} - 1 \\ 0 & \text{otherwise} \end{cases} \tag{30}$$

It is readily verified that this noise probability distribution satisfies the $(0, \delta)$ differential privacy constraint. Therefore, an upper bound for $V^*$ is

*Theorem 3:*

$$V^* \leq V_{UB} \triangleq 2 \sum_{i=1}^{\frac{\Delta}{2\delta}-1} \frac{\delta}{\Delta}\mathcal{L}(i) + \frac{\delta}{\Delta}\mathcal{L}(\frac{\Delta}{2\delta}). \tag{31}$$

### *D. Comparison of $V_{LB}$ and $V_{UB}$*

We first apply the lower bound (29) and upper bound (31) to $\ell^1$ and $\ell^2$ cost functions, i.e., $\mathcal{L}(i) = |i|$ and $\mathcal{L}(i) = i^2$, in which $V^*$ corresponds to the minimum expected noise amplitude and minimum noise power, respectively.

Note that in the case $\mathcal{L}(i) = |i|$, the condition (28) in Theorem 2 is

$$\frac{\Delta}{2\delta} \geq \frac{1}{\delta} + 1. \tag{32}$$

When $\Delta \geq 3$, (28) holds.

*Corollary 4: For the cost function $\mathcal{L}(i) = |i|$,*

$$V_{LB} = \frac{\Delta}{4\delta} + 1 - \frac{\Delta}{2}, \tag{33}$$

$$V_{UB} = \frac{\Delta}{4\delta}, \tag{34}$$

*and thus the additive gap*

$$V_{UB} - V_{LB} = \frac{\Delta}{2} - 1 \tag{35}$$

*is a constant independent of $\delta$.*

In the case $\mathcal{L}(i) = i^2$, the condition (28) in Theorem 2 is

$$\frac{\Delta}{2\delta^2}(\frac{\Delta}{2} - 1) \geq \frac{1}{\delta} + 1. \tag{36}$$

When $\Delta \geq 3$, (36) holds.

*Corollary 5: For the cost function $\mathcal{L}(i) = i^2$,*

$$V_{LB} = \frac{\Delta^2}{12\delta^2} - \frac{\Delta^2}{4\delta} + \Delta(\frac{1}{2\delta} - 1) + \frac{\Delta^2}{6} + 1, \tag{37}$$

$$V_{UB} = \frac{\Delta^2}{12\delta^2} + \frac{1}{6}, \tag{38}$$

*and thus the multiplicative gap*

$$\lim_{\delta \to 0} \frac{V_{UB}}{V_{LB}} = 1. \tag{39}$$

*Proof:* See Appendix B. ■

*Corollary 6: Given a positive integer m, consider the cost function $\mathcal{L}(i) = |i|^m$. Then*

$$\lim_{\delta \to 0} \frac{V_{UB}}{V_{LB}} = 1. \tag{40}$$

*Proof:* By induction, it is easy to show that $\sum_{i=1}^{n} i^m = \Theta(\frac{n^{m+1}}{m+1})$, and

$$\lim_{n \to +\infty} \frac{\sum_{i=1}^{n} i^m}{\frac{n^{m+1}}{m+1}} = 1. \tag{41}$$

Therefore,

$$\lim_{\delta \to 0} \frac{V_{UB}}{V_{LB}} = \lim_{\delta \to 0} \frac{2\frac{\delta}{\Delta}\sum_{i=1}^{\frac{\Delta}{2\delta}-1} i^m + \frac{\delta}{\Delta}\frac{\Delta^m}{(2\delta)^m}}{2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} (1 + i\,\Delta)^m} \tag{42}$$

$$= \lim_{\delta \to 0} \frac{2\frac{\delta}{\Delta}\frac{\frac{\Delta^{m+1}}{(2\delta)^{m+1}}}{m+1}}{2\delta\Delta^m \frac{(\frac{1}{2\delta})^{m+1}}{m+1}} \tag{43}$$

$$= 1. \tag{44}$$

■

For general cost functions, we have the following bound on the multiplicative gap between the lower bound and upper bound.

*Corollary 7: Given a cost function $\mathcal{L}(\cdot)$ satisfying*

$$\sup_{k \geq T} \frac{\mathcal{L}(k)}{\mathcal{L}(k - \Delta + 1)} \leq C, \tag{45}$$

*for some integer $T \in \mathbb{N}$, and some positive number $C \in \mathbb{R}$, then*

$$\limsup_{\delta \to 0} \frac{V_{UB}}{V_{LB}} \leq 1 + (1 + \frac{1}{2\Delta})C. \tag{46}$$

*Proof:* See Appendix C. ■

## IV. $(\epsilon, \delta)$-DIFFERENTIAL PRIVACY

Recall that since $\mathcal{L}(\cdot)$ is a symmetric function, without loss of generality, we can restrict ourselves to symmetric noise probability distributions, i.e.,

$$\mathcal{P}_k = \mathcal{P}_{-k}, \quad \forall k \in \mathbb{Z}. \tag{47}$$

The differential privacy constraint in (18) can be understood in some detail by choosing the subset $S = S_k := \{\ell : \ell \geq k\}$ for $k \in \mathbb{N}$. In this case we see that the noise probability distribution must satisfy the following constraints. For $k = 0$ and $d = \Delta$,

$$\mathcal{P}_{S_0} \leq e^{\epsilon}\mathcal{P}_{S_\Delta} + \delta. \tag{48}$$

By using the symmetry condition in (47) and the fact that $\sum_{\ell=-\infty}^{+\infty} \mathcal{P}_\ell = 1$, from (48) we get

$$\mathcal{P}_0 \frac{1+e^{\epsilon}}{2} + e^{\epsilon}\sum_{\ell=1}^{\Delta-1}\mathcal{P}_\ell \leq \delta + \frac{e^{\epsilon}-1}{2}. \tag{49}$$

For $k = 1$ and $d = \Delta$, we have

$$\mathcal{P}_{S_1} \leq e^{\epsilon}\mathcal{P}_{S_{\Delta+1}} + \delta, \tag{50}$$

and thus

$$\mathcal{P}_0 \frac{e^{\epsilon}-1}{2} + e^{\epsilon}\sum_{\ell=1}^{\Delta}\mathcal{P}_\ell \leq \delta + \frac{e^{\epsilon}-1}{2}. \tag{51}$$

For general $k \geq 2$ and $d = \Delta$, we have

$$\mathcal{P}_{S_k} \leq e^{\epsilon}\mathcal{P}_{S_{\Delta+k}} + \delta, \tag{52}$$

and thus

$$\mathcal{P}_0 \frac{e^{\epsilon}-1}{2} + (e^{\epsilon}-1)\sum_{\ell=1}^{k-1}\mathcal{P}_\ell + e^{\epsilon}\sum_{\ell=k}^{k+\Delta-1}\mathcal{P}_\ell \leq \delta + \frac{e^{\epsilon}-1}{2}. \tag{53}$$

### A. Lower Bound

By restricting the set $S$ in (18) to be $S_k := \{\ell : \ell \geq k\}$ for $k \in \mathbb{Z}$ and restricting $d$ to be $\Delta$, we get the following relaxed linear program, the solution of which is a lower bound for $V^*$:

$$\begin{aligned} V_{LB} := \min\ & 2\sum_{k=1}^{\infty}\mathcal{L}(k)\mathcal{P}_k \\ \text{s.t. } & \mathcal{P}_k \geq 0 \quad \forall k \in N \\ & \frac{\mathcal{P}_0}{2} + \sum_{k=1}^{\infty}\mathcal{P}_k \geq \frac{1}{2} && (54) \\ & \mathcal{P}_0 \frac{1+\epsilon^{\epsilon}}{2} + e^{\epsilon}\sum_{k=1}^{\Delta-1}\mathcal{P}_k \leq \delta + \frac{e^{\epsilon}-1}{2} && (55) \\ & \mathcal{P}_0 \frac{e^{\epsilon}-1}{2} + e^{\epsilon}\sum_{k=1}^{\Delta}\mathcal{P}_k \leq \delta + \frac{e^{\epsilon}-1}{2} && (56) \\ & \mathcal{P}_0 \frac{e^{\epsilon}-1}{2} + (e^{\epsilon}-1)\sum_{k=1}^{i-1}\mathcal{P}_k + e^{\epsilon}\sum_{k=i}^{i+\Delta-1}\mathcal{P}_k \\ & \leq \delta + \frac{e^{\epsilon}-1}{2}, \quad \forall i \geq 2. && (57) \end{aligned}$$

Define

$$a \triangleq \frac{\delta + \frac{e^{\epsilon}-1}{2}}{e^{\epsilon}}, \tag{58}$$

$$b \triangleq e^{-\epsilon}. \tag{59}$$

To avoid integer rounding issues, assume that there exists an integer $n$ such that

$$\sum_{k=0}^{n-1} ab^k = \frac{1}{2}. \tag{60}$$

*Theorem 8: If*

$$\sum_{i=1}^{n-1} e^{-i\epsilon}(2\mathcal{L}(i\Delta) - \mathcal{L}(1+(i-1)\Delta) - \mathcal{L}(1+i\Delta)) \geq \mathcal{L}(1), \tag{61}$$

*then we have*

$$V^* \geq V_{LB} = 2\sum_{k=0}^{n-1}\frac{\delta + \frac{e^{\epsilon}-1}{2}}{e^{\epsilon}}e^{-k\epsilon}\mathcal{L}(1+k\Delta). \tag{62}$$

*Proof:* See Appendix D. ■

### B. Upper Bound: Uniform Noise Mechanism and Discrete Laplacian Mechanism

Since $(0, \delta)$-differential privacy implies $(\epsilon, \delta)$-differential privacy, we can use the uniform noise mechanism with noise probability distribution defined in (30) to preserve $(\epsilon, \delta)$-differential privacy, and the corresponding upper bound is

*Theorem 9: For $(\epsilon, \delta)$-differential privacy, we have*

$$V^* \leq V_{UB}^{uniform} = 2\sum_{i=1}^{\frac{\Delta}{2\delta}-1}\frac{\delta}{\Delta}\mathcal{L}(i) + \frac{\delta}{\Delta}\mathcal{L}(\frac{\Delta}{2\delta}). \tag{63}$$

On the other hand, if we simply ignore the parameter $\delta$ (i.e., set $\delta = 0$), we can use a discrete variant of Laplacian distribution to satisfy the $(\epsilon, 0)$-differential privacy, which implies $(\epsilon, \delta)$-differential privacy.

More precisely, define $\lambda \triangleq e^{-\frac{\epsilon}{\Delta}}$.

*Theorem 10: The probability distribution $\mathcal{P}$ with*

$$\mathcal{P}_k \triangleq \frac{1-\lambda}{1+\lambda}\lambda^{|k|}, \quad \forall k \in \mathbb{Z}, \tag{64}$$

*satisfies the $(\epsilon, \delta)$-differential privacy constraint, and the coresonding cost is*

$$\sum_{k=-\infty}^{+\infty}\mathcal{P}_k\mathcal{L}(k) = 2\sum_{k=1}^{+\infty}\frac{1-\lambda}{1+\lambda}\lambda^k\mathcal{L}(k). \tag{65}$$

*Corollary 11:*

$$V^* \leq V_{UB}^{Lap} \triangleq 2\sum_{k=1}^{+\infty}\frac{1-\lambda}{1+\lambda}\lambda^k\mathcal{L}(k) \tag{66}$$

### C. Comparison of Lower Bound and Upper Bound

In this section, we compare the lower bound (62) and the upper bounds $V_{UB}^{\text{uniform}}$ and $V_{UB}^{\text{Lap}}$ for $(\epsilon, \delta)$-differential privacy for $\ell^1$ and $\ell^2$ cost functions, i.e., $\mathcal{L}(i) = |i|$ and $\mathcal{L}(i) = i^2$, in which $V^*$ corresponds to the minimum expected noise amplitude and minimum noise power, respectively. We show that the multiplicative gap between the lower bound and upper bound is bounded by a constant as $(\epsilon, \delta) \to (0, 0)$.

*1) $\epsilon \le \delta$ Regime:* We first compare the gap between the lower bound $V_{LB}$ and the upper bound $V_{UB}^{\text{uniform}}$ in the regime $\epsilon \le \delta$ as $\delta \to 0$.

*Corollary 12: For the cost function $\mathcal{L}(k) = |k|$, in the regime $\epsilon \le \delta$, we have*

$$\limsup_{\delta\to 0} \frac{V_{UB}^{uniform}}{V_{LB}} \le \frac{1}{4(1-2\log\frac{3}{2})} \approx 1.32 \tag{67}$$

*Proof:* See Appendix E. ■

*Corollary 13: For the cost function $\mathcal{L}(k) = k^2$, in the regime $\epsilon \le \delta$, we have*

$$\limsup_{\delta\to 0} \frac{V_{UB}^{uniform}}{V_{LB}} \le \frac{1}{12(2-4\log(\frac{3}{2})-2(\log(\frac{3}{2}))^2)} \approx \frac{5}{3}. \tag{68}$$

*Proof:* See Appendix F. ■

*2) $\delta \le \epsilon$ Regime:* We then compare the gap between the lower bound $V_{LB}$ and the upper bound $V_{UB}^{\text{Lap}}$ in the regime $\delta \le \epsilon$ as $\epsilon \to 0$.

*Corollary 14: For the cost function $\mathcal{L}(k) = |k|$, in the regime $\delta \le \epsilon$, we have*

$$\limsup_{\epsilon\to 0} \frac{V_{UB}^{Lap}}{V_{LB}} \le \frac{1}{1-2\log\frac{3}{2}} \approx 5.29. \tag{69}$$

*Proof:* See Appendix G. ■

*Corollary 15: For the cost function $\mathcal{L}(k) = k^2$, in the regime $\delta \le \epsilon$, we have*

$$\limsup_{\epsilon\to 0} \frac{V_{UB}^{Lap}}{V_{LB}} \le \frac{2}{(2-4\log(\frac{3}{2})-2(\log(\frac{3}{2}))^2)} \approx 40. \tag{70}$$

*Proof:* See Appendix H. ■

## V. $(\epsilon, \delta)$-Differential Privacy in the Multi-Dimensional Setting

In this section we consider the $(\epsilon, \delta)$-differential privacy in the multi-dimensional setting, where the query output has multiple components and the global sensitivity $\Delta$ is defined as the maximum $\ell^1$ norm of the difference of the query outputs over two neighboring datasets.

Let $d$ be the dimension of the query output. Hence, the query output $q(D) \in \mathbb{Z}^d$. Let $\mathcal{P}$ be the probability mass function of the additive noise over the domain $\mathbb{Z}^d$. Then the $(\epsilon, \delta)$-differential privacy constraint on $\mathcal{P}$ in the multi-dimensional setting is that

$$\mathcal{P}_S \le e^{\epsilon}\mathcal{P}_{S+\mathbf{v}} + \delta, \quad \forall S \subset \mathbb{Z}^d,\ \mathbf{v} \in \mathbb{Z}^d,\ \|\mathbf{v}\|_1 \le \Delta. \tag{71}$$

Consider a cost function $\mathcal{L}(\cdot) : \mathbb{Z}^d \to \mathbb{R}$, which is a function of the added noise $X$. Our goal is to minimize the expectation of the cost subject to the $(\epsilon, \delta)$-differential privacy constraint (71):

$$\begin{aligned} V^* := \min_{\mathcal{P}} \sum_{\mathbf{v}\in\mathbb{Z}^d} &\mathcal{L}(\mathbf{v})\mathcal{P}(\mathbf{v}) \\ \text{subject to } &\mathcal{P}_S \le e^{\epsilon}\mathcal{P}_{S+\mathbf{v}} + \delta, \quad \forall S \subset \mathbb{Z}^d, \\ &\mathbf{v} \in \mathbb{Z}^d,\ \|\mathbf{v}\|_1 \le \Delta. \end{aligned} \tag{72}$$

### A. $(0, \delta)$-Differential Privacy

We first consider the simple case when $\epsilon = 0$, i.e., $(0, \delta)$-differential privacy. The $(0, \delta)$-differential privacy constraint requires that the total variation of the conditional probability distributions of the query output for neighboring datasets should be bounded by $\delta$.

In the differential privacy constraint (71), by choosing the subset

$$S = S_k^m := \{(i_1, i_2, \dots, i_d) \in \mathbb{Z}^d | i_m \ge k\} \tag{73}$$

for $k \in \mathbb{N}$, $m \in \{1, 2, \dots, d\}$, and choosing $\mathbf{v}$ such that only one component is $\Delta$ and all other components are zero, we see that the noise probability distribution $\mathcal{P}$ must satisfy the constraints that $\forall k \in \mathbb{N}, \forall m \in \{1, 2, \dots, d\}$,

$$\sum_{(i_1,i_2,\dots,i_d)\in\mathbb{Z}^d : k \le i_m \le k+\Delta-1} \mathcal{P}(i_1, i_2, \dots, i_d) \le \delta. \tag{74}$$

To avoid integer-rounding issues, we assume that $\frac{1}{2\delta}$ is an integer.

*1) Lower Bound on $V^*$:* We relax the constraint (71) by choosing $S$ to be $S_k^m$ and choosing $\mathbf{v}$ such that only one component is $\Delta$ and all other components are zero. Then we get a relaxed linear program, the solution of which is a lower bound for $V^*$. More precisely,

$$\begin{aligned} V^* \ge V_{LB} := \min &\sum_{\mathbf{i}\in\mathbb{Z}^d} \mathcal{P}(\mathbf{i})\mathcal{L}(\mathbf{i}) \\ \text{s.t. } &\mathcal{P}(\mathbf{i}) \ge 0 \quad \forall \mathbf{i} \in \mathbb{Z}^d \\ &\sum_{\mathbf{i}\in\mathbb{Z}^d} \mathcal{P}(\mathbf{i}) \ge 1 \\ &\forall k \in \mathbb{N}, \quad \forall m \in \{1, 2, \dots, d\} \\ &\sum_{(i_1,i_2,\dots,i_d)\in\mathbb{Z}^d : k \le i_m \le k+\Delta-1} \mathcal{P}(i_1, i_2, \dots, i_d) \\ &\le \delta. \end{aligned} \tag{75}$$

Throughout the paper, we use the notation $\mathbf{i} := (i_1, i_2, \dots, i_d)$ to denote a $d$-dimensional vector in $\mathbb{Z}^d$.

*Theorem 16: In the case $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_1, \forall \mathbf{i} \in \mathbb{Z}^d$, we have*

$$V_{LB} \ge \frac{d\Delta}{4\delta} - \frac{\Delta - 1}{2}d. \tag{76}$$

*Proof:* See Appendix I. ■

*Theorem 17: In the case $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_2^2 = \sum_{m=1}^d i_m^2$, $\forall \mathbf{i} = (i_1, \dots, i_d) \in \mathbb{Z}^d$, we have*

$$V_{LB} \ge \frac{d\Delta^2}{12\delta^2} + (\frac{1}{\Delta} - 1)\frac{d\Delta^2}{4\delta} + \frac{1-\Delta}{2}d + \frac{d\Delta^2}{6}. \tag{77}$$

*Proof:* See Appendix J. ■

*2) Uniform Noise Mechanism in the Multi-Dimensional Setting:* Consider the noise with the *uniform* probability distribution:

$$\mathcal{P}(\mathbf{i}) = \begin{cases} \frac{\delta^d}{\Delta^d} & -\frac{\Delta}{2\delta} \le i_m \le \frac{\Delta}{2\delta} - 1,\ \forall m \in \{1, 2, \dots, d\} \\ 0 & \text{otherwise} \end{cases} \tag{78}$$

It is readily verified that this noise probability distribution satisfies the $(0, \delta)$ differential privacy constraint (71). Therefore, an upper bound for $V^*$ is

*Theorem 18:*

$$V^* \leq V_{UB} \triangleq \sum_{\{\mathbf{i}\in\mathbb{Z}^d \mid -\frac{\Delta}{2\delta} \leq i_m \leq \frac{\Delta}{2\delta}-1, \forall m \in \{1,2,\ldots,d\}\}} \frac{\delta^d}{\Delta^d}\mathcal{L}(\mathbf{i}). \tag{79}$$

*Corollary 19: In the case $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_1, \forall \mathbf{i} \in \mathbb{Z}^d$, we have*

$$V_{UB} = \frac{d\Delta}{4\delta}. \tag{80}$$

*Proof:*

$$\begin{aligned}
V_{UB} &= \sum_{\{\mathbf{i}\in\mathbb{Z}^d \mid -\frac{\Delta}{2\delta} \leq i_m \leq \frac{\Delta}{2\delta}-1, \forall m \in \{1,2,\ldots,d\}\}} \frac{\delta^d}{\Delta^d}\mathcal{L}(\mathbf{i}) &(81)\\
&= \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \cdots \sum_{i_d=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}(|i_1| + \cdots + |i_d|) &(82)\\
&= d \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \cdots \sum_{i_d=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}|i_1| &(83)\\
&= d\left(\frac{\Delta}{\delta}\right)^{d-1} \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}|i_1| &(84)\\
&= d\left(\frac{\Delta}{\delta}\right)^{d-1} \frac{\delta^d}{\Delta^d}\left(\frac{(1+\frac{\Delta}{2\delta})\frac{\Delta}{2\delta}}{2} + \frac{\frac{\Delta}{2\delta}(\frac{\Delta}{2\delta}-1)}{2}\right) &(85)\\
&= \frac{d\Delta}{4\delta}. &(86)
\end{aligned}$$

■

*Corollary 20: In the case $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_2^2 \triangleq \sum_{m=1}^d i_m^2$, $\forall \mathbf{i} = (i_1, \ldots, i_d) \in \mathbb{Z}^d$, we have*

$$V_{UB} = \frac{d\Delta^2}{12\delta^2} + \frac{d}{6}. \tag{87}$$

*Proof:*

$$\begin{aligned}
V_{UB} &= \sum_{\{\mathbf{i}\in\mathbb{Z}^d \mid -\frac{\Delta}{2\delta} \leq i_m \leq \frac{\Delta}{2\delta}-1, \forall m \in \{1,2,\ldots,d\}\}} \frac{\delta^d}{\Delta^d}\mathcal{L}(\mathbf{i}) &(88)\\
&= \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \cdots \sum_{i_d=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}(|i_1|^2 + \cdots + |i_d|^2) &(89)\\
&= d \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \cdots \sum_{i_d=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}|i_1|^2 &(90)\\
&= d\left(\frac{\Delta}{\delta}\right)^{d-1} \sum_{i_1=-\frac{\Delta}{2\delta}}^{\frac{\Delta}{2\delta}-1} \frac{\delta^d}{\Delta^d}|i_1|^2 &(91)\\
&= d\left(\frac{\Delta}{\delta}\right)^{d-1} \frac{\delta^d}{\Delta^d}\\
&\quad \times \left(\frac{\frac{\Delta}{2\delta}(1+\frac{\Delta}{2\delta})(\frac{\Delta}{\delta}+1)}{6} + \frac{(\frac{\Delta}{2\delta}-1)\frac{\Delta}{2\delta}(\frac{\Delta}{\delta}-1)}{6}\right) &(92)\\
&= \frac{d\Delta^2}{12\delta^2} + \frac{d}{6}. &(93)
\end{aligned}$$

■

*3) Comparison of Lower Bound and Upper Bound for $\ell^1$ Cost Function:*

*Corollary 21: For the cost function $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_1$,*

$$\begin{aligned}
V_{LB} &\geq \frac{d\Delta}{4\delta} - \frac{\Delta-1}{2}d, &(94)\\
V_{UB} &= \frac{d\Delta}{4\delta}, &(95)
\end{aligned}$$

*and thus the additive gap*

$$V_{UB} - V_{LB} \leq \frac{\Delta-1}{2}d, \tag{96}$$

*which is a constant independent of $\delta$.*

In the case that $\Delta = 1$, the additive gap $\frac{\Delta-1}{2}d$ is zero, and thus $V_{LB} = V_{UB}$.

*Corollary 22: For the cost function $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_1$, if $\Delta = 1$, then*

$$V^* = V_{UB} = V_{LB} = \frac{d\Delta}{4\delta}, \tag{97}$$

*and thus the uniform noise mechanism is optimal in this setting.*

*Corollary 23: For the cost function $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_2^2$,*

$$\begin{aligned}
V_{LB} &\geq \frac{d\Delta^2}{12\delta^2} + (\frac{1}{\Delta} - 1)\frac{d\Delta^2}{4\delta} + \frac{1-\Delta}{2}d + \frac{d\Delta^2}{6}, &(98)\\
V_{UB} &= \frac{d\Delta^2}{12\delta^2} + \frac{d}{6}, &(99)
\end{aligned}$$

*and thus*

$$\lim_{\delta\to 0} \frac{V_{UB}}{V_{LB}} = 1. \tag{100}$$

In the case that $\Delta = 1$,

$$V_{LB} \geq \frac{d}{12\delta^2} + \frac{d}{6} = V_{UB}, \tag{101}$$

and thus $V_{LB} = V_{UB}$.

*Corollary 24: For the cost function $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_2^2$, if $\Delta = 1$, then*

$$V^* = V_{UB} = V_{LB} = \frac{d}{12\delta^2} + \frac{d}{6}, \tag{102}$$

*and thus the uniform noise mechanism is optimal in this setting.*

### *B. $(\epsilon, \delta)$-Differential Privacy*

The $(\epsilon, \delta)$-differential privacy constraint on the probability mass function $\mathcal{P}$ in the multi-dimensional setting is that

$$\mathcal{P}_S \leq e^{\epsilon}\mathcal{P}_{S+\mathbf{v}} + \delta, \quad \forall S \subset \mathbb{Z}^d, \ \mathbf{v} \in \mathbb{Z}^d, \ \|\mathbf{v}\|_1 \leq \Delta. \tag{103}$$

We relax this constraint by choosing $S$ to be $S_k^m$ and choosing $\mathbf{v}$ such that only one component is $\Delta$ and all other components are zero. Then we get a relaxed linear program, the solution of which is a lower bound for $V^*$. More precisely,

$$\begin{aligned} V^* \geq V_{LB} := \min \ & \sum_{\mathbf{i}\in\mathbb{Z}^d} \mathcal{P}(\mathbf{i})\mathcal{L}(\mathbf{i}) \\ \text{s.t. } & \mathcal{P}(\mathbf{i}) \geq 0 \quad \forall \mathbf{i} \in \mathbb{Z}^d \\ & \sum_{\mathbf{i}\in\mathbb{Z}^d} \mathcal{P}(\mathbf{i}) \geq 1 \\ & \forall k \in \mathbb{N}, \quad \forall m \in \{1,2,\ldots,d\}, \\ & \sum_{\mathbf{i}\in\mathbb{Z}^d : k \leq i_m \leq k+\Delta-1} \mathcal{P}(\mathbf{i}) - (e^{\epsilon}-1) \\ & \times \sum_{\mathbf{i}\in\mathbb{Z}^d : i_m \geq k+\Delta} \mathcal{P}(\mathbf{i}) \leq \delta. \end{aligned} \tag{104}$$

We are interested in characterizing $V^*$ for the $\ell^1$ and $\ell^2$ cost functions in the high privacy regime when $(\epsilon, \delta) \to (0,0)$.

*1) Lower Bound for $\ell^1$ Cost Function:* The dual linear program of (104) for $\ell^1$ cost function $\mathcal{L}(\mathbf{i}) = \|\mathbf{i}\|_1$ is that

$$V_{LB} := \max \ \mu - \delta \left( \sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)} \right) \tag{105}$$

$$\text{s.t. } y_{i_1}^{(1)}, y_{i_2}^{(2)}, \ldots, y_{i_d}^{(d)} \geq 0, \quad \forall i_1 \in \mathbb{Z}, \ i_2 \in \mathbb{Z}, \ldots, i_d \in \mathbb{Z} \tag{106}$$

$$\begin{aligned} & \mu - \sum_{i_1\in[k_1-\Delta+1,k_1]} y_{i_1}^{(1)} + (e^{\epsilon}-1) \sum_{i_1\leq k_1-\Delta} y_{i_1}^{(1)} \\ & - \ldots - \sum_{i_d\in[k_d-\Delta+1,k_d]} y_{i_d}^{(d)} + (e^{\epsilon}-1) \sum_{i_d\leq k_d-\Delta} y_{i_d}^{(d)} \\ & \leq |k_1| + |k_2| + \cdots + |k_d|, \quad \forall (k_1,\ldots,k_d) \in \mathbb{Z}^d. \end{aligned} \tag{107}$$

Given the parameters $(\epsilon, \delta)$, let $\beta = \max(\epsilon, \delta)$. Since $(\beta, \beta)$-differential privacy is a relaxed version of $(\epsilon, \delta)$-differential privacy, in the above dual program we can replace both $\epsilon$ and $\delta$ by $\beta$, and the optimal value of the objecitve function will still be a lower bound of $V^*$. More precisely,

$$\begin{aligned} V^* & \geq V'_{LB} \\ & := \max \ \mu - \beta \left( \sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)} \right) \end{aligned} \tag{108}$$

$$\text{s.t. } y_{i_1}^{(1)}, y_{i_2}^{(2)}, \ldots, y_{i_d}^{(d)} \geq 0, \quad \forall i_1 \in \mathbb{Z}, \ i_2 \in \mathbb{Z}, \ldots, i_d \in \mathbb{Z} \tag{109}$$

$$\begin{aligned} & \mu - \sum_{i_1\in[k_1-\Delta+1,k_1]} y_{i_1}^{(1)} + (e^{\beta}-1) \sum_{i_1\leq k_1-\Delta} y_{i_1}^{(1)} \\ & - \ldots - \sum_{i_d\in[k_d-\Delta+1,k_d]} y_{i_d}^{(d)} + (e^{\beta}-1) \sum_{i_d\leq k_d-\Delta} y_{i_d}^{(d)} \\ & \leq |k_1| + |k_2| + \cdots + |k_d|, \quad \forall (k_1,\ldots,k_d) \in \mathbb{Z}^d. \end{aligned} \tag{110}$$

*Theorem 25: For the $\ell^1$ cost function,*

$$\liminf_{\max(\epsilon,\delta)\to 0} \frac{V'_{LB}}{\frac{d\Delta}{\max(\epsilon,\delta)}} \geq \log\frac{9}{8} \approx 0.1178 \tag{111}$$

*Proof:* See Appendix K. ■

Similarly, for the $\ell^2$ cost function, we have the lower bound

$$\begin{aligned} V^* & \geq V'_{LB} \\ & := \max \ \mu - \beta \left( \sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)} \right) \end{aligned} \tag{112}$$

$$\text{s.t. } y_{i_1}^{(1)}, y_{i_2}^{(2)}, \ldots, y_{i_d}^{(d)} \geq 0, \quad \forall i_1 \in \mathbb{Z}, \ i_2 \in \mathbb{Z}, \ldots, i_d \in \mathbb{Z} \tag{113}$$

$$\begin{aligned} & \mu - \sum_{i_1\in[k_1-\Delta+1,k_1]} y_{i_1}^{(1)} + (e^{\beta}-1) \sum_{i_1\leq k_1-\Delta} y_{i_1}^{(1)} \\ & - \ldots - \sum_{i_d\in[k_d-\Delta+1,k_d]} y_{i_d}^{(d)} + (e^{\beta}-1) \sum_{i_d\leq k_d-\Delta} y_{i_d}^{(d)} \\ & \leq |k_1|^2 + |k_2|^2 + \cdots + |k_d|^2, \quad \forall (k_1,\ldots,k_d) \in \mathbb{Z}^d. \end{aligned} \tag{114}$$

*Theorem 26: For the $\ell^2$ cost function,*

$$\liminf_{\max(\epsilon,\delta)\to 0} \frac{V'_{LB}}{\frac{d\Delta^2}{\beta^2}} \geq 0.0177. \tag{115}$$

*Proof:* See Appendix L. ■

*2) Upper Bounds: Uniform Noise Mechanism and Discrete Laplacian Mechanism:* Since $(0, \delta)$-differential privacy implies $(\epsilon, \delta)$-differential privacy and we have shown that the uniform noise mechanism defined in (78) satisfies $(0, \delta)$-differential privacy, an upper bound for $V^*$ for the $\ell^1$ cost function is

$$V^* \leq V_{UB}^{\text{uniform}} = \frac{d\Delta}{4\delta} \tag{116}$$

by Corollary 19.

In addition, $(\epsilon, 0)$-differential privacy also implies $(\epsilon, \delta)$-differential privacy, and the discrete multidimensional Laplacian mechanism, which adds independent Laplacian noise to each component of the query output, satisfies $(\epsilon, 0)$-differential privacy. Consider the discrete Laplacian mechanism in the multi-dimensional setting with probability mass function $\mathcal{P}$ defined as

$$\mathcal{P}(\mathbf{i}) = \left(\frac{1-\lambda}{1+\lambda}\right)^d \lambda^{|i_1|+|i_2|+\cdots+|i_d|}, \quad \forall \mathbf{i} \in \mathbb{Z}^d, \tag{117}$$

where $\lambda \triangleq e^{-\frac{\epsilon}{\Delta}}$.

The corresponding cost achieved by Laplacian mechanism for the $\ell^1$ cost function is

$$\begin{aligned} V_{UB}^{\text{Lap}} & = \sum_{\mathbf{i}\in\mathbb{Z}^d} \left(\frac{1-\lambda}{1+\lambda}\right)^d \lambda^{|i_1|+\cdots+|i_d|}(|i_1| + \cdots + |i_d|) && (118) \\ & = \frac{2d\lambda}{1-\lambda^2} && (119) \\ & = \frac{2de^{-\frac{\epsilon}{\Delta}}}{1-e^{-2\frac{\epsilon}{\Delta}}} && (120) \\ & = \Theta(\frac{d\Delta}{\epsilon}), && (121) \end{aligned}$$

as $\epsilon \to 0$.

Similarly, for the $\ell^2$ cost function, we have

$$V_{UB}^{\text{uniform}} = \frac{d\Delta^2}{12\delta^2} + \frac{d}{6}, \tag{122}$$

and

$$\begin{aligned} V_{UB}^{\text{Lap}} &= \sum_{\mathbf{i}\in\mathbb{Z}^d} \left(\frac{1-\lambda}{1+\lambda}\right)^d \lambda^{|i_1|+\cdots+|i_d|}(|i_1|^2+\cdots+|i_d|^2) && (123)\\ &= \frac{2d\lambda}{(1-\lambda)^2} && (124)\\ &= \Theta(\frac{2d\Delta^2}{\epsilon^2}). && (125)\end{aligned}$$

*3) Comparison of Lower Bound and Upper Bounds:* Compare the lower bound in Theorem 25 and the upper bounds (116) and (121), and we conclude that for the $\ell^1$ cost function, the multiplicative gap between the upper bound and lower bound is upper bounded by a constant as $(\epsilon, \delta) \to (0,0)$. More precisely,

*Corollary 27: For the $\ell^1$ cost function, we have*

$$V'_{LB} \le V^* \le \min(V_{UB}^{\textit{uniform}}, V_{UB}^{\textit{Lap}}), \tag{126}$$

*and as $(\epsilon, \delta) \to (0,0)$,*

$$\limsup_{(\epsilon,\delta)\to(0,0)} \frac{\min(V_{UB}^{\textit{uniform}}, V_{UB}^{\textit{Lap}})}{V'_{LB}} \le \frac{1}{\log\frac{9}{8}} \approx 8.49 \tag{127}$$

Similarly, for the $\ell^2$ cost function, we have

*Corollary 28: For the $\ell^2$ cost function, we have*

$$V'_{LB} \le V^* \le \min(V_{UB}^{\textit{uniform}}, V_{UB}^{\textit{Lap}}), \tag{128}$$

*and as $(\epsilon, \delta) \to (0,0)$,*

$$\limsup_{(\epsilon,\delta)\to(0,0)} \frac{\min(V_{UB}^{\textit{uniform}}, V_{UB}^{\textit{Lap}})}{V'_{LB}} \le \frac{2}{0.0177} \approx 113. \tag{129}$$

## APPENDIX A
## PROOF OF THEOREM 2

*Proof of Theorem 2:* Consider a feasible solution to the optimization problem (25) with primal variables

$$p_k = \begin{cases} \delta & k = 1 + i\Delta, \ \text{for } i = 0, 1, 2, \ldots, \frac{1}{2\delta} - 1 \\ 0 & \text{otherwise} \end{cases} \tag{130}$$

The corresponding value of the objective function is

$$2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\Delta). \tag{131}$$

Therefore,

$$V_{LB} \le 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\Delta). \tag{132}$$

We claim that the above primal variables are the optimal solution. We prove this claim by constructing the corresponding dual variables.

Associating dual variables $\mu$ with the constraint in (26), $y_k$ with the constraint in (27), we have the dual linear program:

$$\begin{aligned} V_{LB} = \max \ & \mu - 2\delta \sum_{k=0}^{\infty} y_k \\ \text{s.t. } & \mu \ge 0, \quad y_k \ge 0, \ \forall k \in \mathbb{N}, && (133)\\ & \frac{1}{2}\mu - y_0 \le 0, && (134)\\ & \mu - \sum_{i=\max(0,k-\Delta+1)}^{k} y_i \le \mathcal{L}(k), \quad \forall k \ge 1. && (135)\end{aligned}$$

The complementary slackness conditions require that

$$\mu - y_0 - y_1 = \mathcal{L}(1), \tag{136}$$

$$\mu - \sum_{i=2+(k-1)\Delta}^{1+k\Delta} y_i = \mathcal{L}(1+k\Delta), \quad \text{for } k = 1, 2, \ldots, \frac{1}{2\delta} - 1, \tag{137}$$

$$y_k = 0, \quad \forall k \ge (\frac{1}{2\delta} - 1)\Delta + 2. \tag{138}$$

Consider the following dual variables:

$$\mu = \mathcal{L}(1 + \frac{\Delta}{2\delta}), \tag{139}$$

$$y_k = 0, \quad \forall k \ge (\frac{1}{2\delta} - 1)\Delta + 2, \tag{140}$$

$$\forall 2 \le k \le (\frac{1}{2\delta} - 1)\Delta + 1,$$

$$y_k = \mathcal{L}(k + \Delta) - \mathcal{L}(k + \Delta - 1) + y_{k+\Delta}, \tag{141}$$

$$y_1 = \sum_{i=1}^{\frac{1}{2\delta}} (\mathcal{L}(1 + i\Delta) - \mathcal{L}(i\Delta)) \ge 0, \tag{142}$$

$$\begin{aligned} y_0 &= \mu - \mathcal{L}(1) - y_1 \\ &= \mathcal{L}(1 + \frac{\Delta}{2\delta}) - \mathcal{L}(1) - \sum_{i=1}^{\frac{1}{2\delta}} (\mathcal{L}(1 + i\Delta) - \mathcal{L}(i\Delta)) \ge 0, && (143)\end{aligned}$$

where the inequality in (143) holds due to the assumption (28).

It is easy to verify that these dual variables satisfy the constraints of the dual linear program, and the value of the objective function is

$$\begin{aligned} \mu - 2\delta \sum_{k=0}^{+\infty} y_k &= \mu - 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} (\mu - \mathcal{L}(1 + i\Delta)) && (144)\\ &= 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\Delta). && (145)\end{aligned}$$

Therefore, by weak duality we have

$$V_{LB} \ge 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\Delta). \tag{146}$$

Due to (132), we conclude

$$V_{LB} = 2\delta \sum_{i=0}^{\frac{1}{2\delta}-1} \mathcal{L}(1 + i\Delta). \tag{147}$$

■

## Appendix B
## Proof of Corollary 5

*Proof of Corollary 5:* First we compute the lower bound $V_{LB}$ via

$$\begin{aligned}
V_{LB} &= 2\sum_{i=0}^{\frac{1}{2\delta}-1} \delta\mathcal{L}(1+i\Delta) && (148)\\
&= 2\delta\sum_{i=0}^{\frac{1}{2\delta}-1} (1+i\Delta)^2 && (149)\\
&= 2\delta\sum_{i=0}^{\frac{1}{2\delta}-1} (1+2i\Delta+i^2\Delta^2) && (150)\\
&= 2\delta(\frac{1}{2\delta}+2\Delta\frac{\frac{1}{2\delta}(\frac{1}{2\delta}-1)}{2}+\Delta^2\frac{(\frac{1}{2\delta}-1)\frac{1}{2\delta}(2\frac{1}{2\delta}-1)}{6}) && (151)\\
&= 1+\Delta(\frac{1}{2\delta}-1)+\frac{\Delta^2}{12\delta^2}+\frac{\Delta^2}{6}-\frac{\Delta^2}{4\delta} && (152)\\
&= \Theta(\frac{\Delta^2}{12\delta^2}). && (153)
\end{aligned}$$

The upper bound is

$$\begin{aligned}
V_{UB} &= 2\sum_{i=1}^{\frac{\Delta}{2\delta}-1} \frac{\delta}{\Delta}\mathcal{L}(i)+\frac{\delta}{\Delta}\mathcal{L}(\frac{\Delta}{2\delta}) && (154)\\
&= 2\frac{\delta}{\Delta}\frac{(\frac{\Delta}{2\delta}-1)\frac{\Delta}{2\delta}(\frac{\Delta}{\delta}-1)}{6}+\frac{\delta}{\Delta}\frac{\Delta^2}{4\delta^2} && (155)\\
&= \frac{1}{6}(\frac{\Delta^2}{2\delta^2}+1-\frac{3\Delta}{2\delta})+\frac{\Delta}{4\delta} && (156)\\
&= \frac{\Delta^2}{12\delta^2}+\frac{1}{6} && (157)\\
&= \Theta(\frac{\Delta^2}{12\delta^2}). && (158)
\end{aligned}$$

Therefore, the multiplicative gap goes to one as $\delta \to 0$, i.e.,

$$\lim_{\delta\to 0}\frac{V_{UB}}{V_{LB}} = 1. \qquad (159)$$

■

## Appendix C
## Proof of Corollary 7

*Proof of Corollary 7:* Using the fact that $\mathcal{L}(\cdot)$ is a monotonically increasing function for $k \geq 0$, we have

$$\begin{aligned}
V_{UB}-V_{LB} &= 2\sum_{i=1}^{\frac{\Delta}{2\delta}-1} \frac{\delta}{\Delta}\mathcal{L}(i)+\frac{\delta}{\Delta}\mathcal{L}(\frac{\Delta}{2\delta})-2\delta\sum_{i=0}^{\frac{1}{2\delta}-1}\mathcal{L}(1+i\Delta) && (160)\\
&\leq -2\delta\mathcal{L}(1)+\frac{\delta}{\Delta}\mathcal{L}(\frac{\Delta}{2\delta})+2\delta\mathcal{L}(\frac{\Delta}{2\delta}-1) && (161)\\
&\leq (2+\frac{1}{\Delta})\delta\mathcal{L}(\frac{\Delta}{2\delta}). && (162)
\end{aligned}$$

Therefore,

$$\begin{aligned}
\frac{V_{UB}}{V_{LB}} &= 1+\frac{V_{UB}-V_{LB}}{V_{LB}} && (163)\\
&\leq 1+\frac{(2+\frac{1}{\Delta})\delta\mathcal{L}(\frac{\Delta}{2\delta})}{2\delta\sum_{i=0}^{\frac{1}{2\delta}-1}\mathcal{L}(1+i\Delta)} && (164)\\
&\leq 1+\frac{(2+\frac{1}{\Delta})\delta\mathcal{L}(\frac{\Delta}{2\delta})}{2\delta\mathcal{L}(1+(\frac{1}{2\delta}-1)\Delta)}, && (165)
\end{aligned}$$

and thus

$$\limsup_{\delta\to 0}\frac{V_{UB}}{V_{LB}} \leq 1+(1+\tfrac{1}{2\Delta})C. \qquad (166)$$

■

## Appendix D
## Proof of Theorem 8

*Proof of Theorem 8:* Consider the feasible primal variables $\{p_k\}_{k\in\mathbb{N}}$ defined as

$$\mathcal{P}_k = \begin{cases} ab^i & \text{for } k = 1+i\Delta,\ 0\leq i\leq n-1\\ 0 & \text{otherwise}\end{cases} \qquad (167)$$

It is straightforward to verify that the above primal variables satisfy the constraints of the relaxed linear program, and the corresponding value of the objective function is

$$2\sum_{k=0}^{n-1} ab^k\mathcal{L}(1+k\Delta). \qquad (168)$$

We prove it is also the optimal value by constructing the optimal dual variables for the corresponding dual linear program.

Associating dual variables $\mu, y_0, y_1, y_i$ with the primal constraints in (54), (55), (56) and (57), respectively, we have the dual linear program:

$$\begin{aligned}
V_{LB} := \min\ & \mu-(2\delta+e^{\epsilon}-1)\sum_{k=0}^{+\infty}y_k && (169)\\
\text{s.t. }\ & \mu\geq 0,\quad y_k\geq 0\ \ \forall k\in N && (170)\\
& \frac{1}{2}\mu-\frac{1+e^{\epsilon}}{2}y_0-\frac{e^{\epsilon}-1}{2}y_1-\frac{e^{\epsilon}-1}{2}\sum_{k=2}^{+\infty}y_k\leq 0 && (171)\\
& \mu-e^{\epsilon}y_0-e^{\epsilon}y_1-(e^{\epsilon}-1)\sum_{k=2}^{+\infty}y_k\leq\mathcal{L}(1) && (172)\\
& \forall k\geq 2,\\
& \mu-e^{\epsilon}\sum_{l=\max(0,k-\Delta+1)}^{k}y_l-(e^{\epsilon}-1)\\
& \times\sum_{l=k+1}^{+\infty}y_l\leq\mathcal{L}(k). && (173)
\end{aligned}$$

If the primal variables defined in (167) are the optimal solution, the complementary slackness conditions require that the corresponding dual variables satisfy that

$$\mu = \mathcal{L}(1) + e^{\epsilon}(y_0 + y_1) + (e^{\epsilon} - 1)\sum_{l=2}^{+\infty} y_l \tag{174}$$

$$\mu = \mathcal{L}(1+\Delta) + e^{\epsilon}\sum_{l=2}^{1+\Delta} y_l + (e^{\epsilon} - 1)\sum_{l=2+\Delta}^{+\infty} y_l \tag{175}$$

$$\forall 1 \le k \le n-1,$$

$$\mu = \mathcal{L}(1+k\Delta) + e^{\epsilon}\sum_{l=2+(k-1)\Delta}^{1+k\Delta} y_l + (e^{\epsilon} - 1)\sum_{l=2+k\Delta}^{+\infty} y_l, \tag{176}$$

$$y_l = 0, \quad \forall l \ge 2 + (n-1)\Delta. \tag{177}$$

Consider the following dual variables defined via

$$\mu = \mathcal{L}(1+(n-1)\Delta), \tag{178}$$

$$y_k = 0, \quad \forall k \ge 2 + (n-2)\Delta, \tag{179}$$

$$\forall 2 \le k \le 1 + (n-2)\Delta,$$

$$y_k = b(y_{k+\Delta} + \mathcal{L}(k+\Delta) - \mathcal{L}(k+\Delta-1)), \tag{180}$$

$$y_1 = \sum_{i=1}^{n-1} b^i(\mathcal{L}(1+i\Delta) - \mathcal{L}(i\Delta)), \tag{181}$$

$$y_0 = \sum_{i=1}^{n-1} b^i(\mathcal{L}(i\Delta) - \mathcal{L}(1+(i-1)\Delta)). \tag{182}$$

We verify that the above dual variables satisfy the inequality (171) in the following

$$(1+e^{\epsilon})y_0 + (e^{\epsilon}-1)y_1 + (e^{\epsilon}-1)\sum_{k=2}^{+\infty} y_k - \mu \ge 0 \tag{183}$$

$$\Leftrightarrow y_0 - y_1 + e^{\epsilon}(y_0 + y_1) + (e^{\epsilon}-1)\sum_{k=2}^{+\infty} y_k - \mu \ge 0 \tag{184}$$

$$\Leftrightarrow y_0 - y_1 + \mu - \mathcal{L}(1) - \mu \ge 0 \tag{185}$$

$$\Leftrightarrow y_0 - y_1 - \mathcal{L}(1) \ge 0 \tag{186}$$

$$\Leftrightarrow \sum_{i=1}^{n-1} b^i(2\mathcal{L}(i\Delta) - \mathcal{L}(1+(i-1)\Delta) - \mathcal{L}(1+i\Delta)) \ge \mathcal{L}(1). \tag{187}$$

It is easy to verify that the dual variables satisfy the constraints (170), (171), (172) and (173) in the dual linear program. Next we compute the corresponding value of the objective function

$$\mu - (2\delta + e^{\epsilon} - 1)\sum_{k=0}^{+\infty} y_k \tag{188}$$

$$= \mu - (2\delta + e^{\epsilon} - 1)(y_0 + y_1 + \frac{\mu - \mathcal{L}(1) - e^{\epsilon}(y_0+y_1)}{e^{\epsilon}-1}) \tag{189}$$

$$= \mu - \frac{2\delta + e^{\epsilon} - 1}{e^{\epsilon}-1}(\mu - \mathcal{L}(1) - y_0 - y_1) \tag{190}$$

$$= \mathcal{L}(1+(n-1)\Delta) - \frac{2\delta + e^{\epsilon} - 1}{e^{\epsilon}-1}(\mathcal{L}(1+(n-1)\Delta) - \mathcal{L}(1) - \sum_{i=1}^{n-1} b^i(\mathcal{L}(1+i\Delta) - \mathcal{L}(1+(i-1)\Delta))) \tag{191}$$

$$= 2\sum_{k=0}^{n-1} ab^k\mathcal{L}(1+k\Delta), \tag{192}$$

which is also the value of the objective function in the primal problem achieved by the primal variables defined in (167). Therefore, we conclude that

$$V_{LB} = 2\sum_{k=0}^{n-1} ab^k\mathcal{L}(1+k\Delta). \tag{193}$$

■

## Appendix E
## Proof of Corollary 12

*Proof of Corollary 12:* For the cost function $\mathcal{L}(k) = |k|$,

$$V_{LB} = 2\sum_{k=0}^{n-1} ab^k\mathcal{L}(1+k\Delta) \tag{194}$$

$$= 2\sum_{k=0}^{n-1} ab^k(1+k\Delta) \tag{195}$$

$$= 1 + 2a\Delta\sum_{k=0}^{n-1} b^k k \tag{196}$$

$$= 1 + 2a\Delta(\frac{b-b^n}{(1-b)^2} - \frac{(n-1)b^n}{1-b}). \tag{197}$$

Given $\delta > 0$, $V_{LB}$ is a decreasing function of $\epsilon$. Therefore, to lower bound $\frac{V_{UB}^{\text{uniform}}}{V_{LB}}$ in the regime $\epsilon \le \delta$, we only need to consider the case $\epsilon = \delta$. Thus, in the following we set $\epsilon = \delta$.

Since $\sum_{k=0}^{n-1} ab^k = \frac{1}{2}$, we have

$$a\frac{1-b^n}{1-b} = \frac{1}{2} \tag{198}$$

$$\Leftrightarrow b^n = 1 - \frac{1-b}{2a}. \tag{199}$$

As $\delta \to 0$, $\frac{1-b}{2a} = \frac{1-e^{-\epsilon}}{2\frac{\delta + \frac{e^{\epsilon}-1}{2}}{e^{\epsilon}}} \to \frac{1}{3}$, and thus

$$\lim_{\delta \to 0} b^n = 1 - \frac{1}{3} = \frac{2}{3}, \tag{200}$$

$$n = \Theta(\frac{\log(\frac{3}{2})}{\epsilon}). \tag{201}$$

Note that $a = \Theta(\frac{3}{2}\delta)$ as $\delta \to 0$.

Therefore, as $\delta \to 0$,

$$V_{LB} \approx 2\Delta a(\frac{1-\frac{2}{3}}{\epsilon^2} - \frac{\frac{\log(\frac{3}{2})}{\epsilon}\frac{2}{3}}{\epsilon}) \tag{202}$$

$$\approx 2\Delta\frac{3}{2}\delta(\frac{1}{3\delta^2} - \frac{\frac{2}{3}\log(\frac{3}{2})}{\delta^2}) \tag{203}$$

$$= \frac{\Delta}{\delta}(1 - 2\log\frac{3}{2}) \tag{204}$$

$$\approx 0.19\frac{\Delta}{\delta}. \tag{205}$$

Recall $V_{UB}^{\text{uniform}} = \frac{\Delta}{4\delta}$.
Therefore,

$$\lim_{\epsilon=\delta\to 0} \frac{V_{UB}}{V_{LB}} = \frac{1}{4(1-2\log\frac{3}{2})} \approx 1.32, \tag{206}$$

and thus

$$\limsup_{\epsilon\leq\delta\to 0} \frac{V_{UB}}{V_{LB}} \leq \frac{1}{4(1-2\log\frac{3}{2})} \approx 1.32, \tag{207}$$

■

## Appendix F
## Proof of Corollary 13

*Proof of Corollary 13:* Using the same argument in the proof of Corollary 12, we can set $\epsilon = \delta$.

For the cost function $\mathcal{L}(k) = k^2$,

$$V_{LB} = 2\sum_{k=0}^{n-1} ab^k \mathcal{L}(1+k\Delta) \tag{208}$$

$$= 2\sum_{k=0}^{n-1} ab^k (1+k\Delta)^2 \tag{209}$$

$$= 1 + 4a\Delta\sum_{k=0}^{n-1} b^k k + 2a\Delta^2 \sum_{k=0}^{n-1} b^k k^2 \tag{210}$$

$$\approx 2a\Delta^2 \sum_{k=0}^{n-1} b^k k^2 \tag{211}$$

$$= 2\Delta^2 \frac{\delta + \frac{e^\epsilon - 1}{2}}{e^\epsilon} \frac{-b + 2(\frac{b(1-b^{n-1})}{(1-b)^2} - \frac{(n-1)b^n}{1-b}) - \frac{b^2(1-b^{n-2})}{1-b} - (n-1)^2 b^n}{1-b} \tag{212}$$

$$\approx 2\Delta^2 \frac{3}{2}\epsilon \frac{2(\frac{1-\frac{2}{3}}{\epsilon^2} - \frac{\frac{2}{3}\log(\frac{3}{2})}{\epsilon^2}) - \frac{1}{3\epsilon} - \frac{2}{3}\frac{(\log(\frac{3}{2}))^2}{\epsilon^2}}{\epsilon} \tag{213}$$

$$\approx \frac{3\Delta^2}{\epsilon^2}(\frac{2}{3} - \frac{4}{3}\log(\frac{3}{2}) - \frac{2}{3}(\log(\frac{3}{2}))^2) \tag{214}$$

$$= \frac{\Delta^2}{\epsilon^2}(2 - 4\log(\frac{3}{2}) - 2(\log(\frac{3}{2}))^2) \tag{215}$$

$$\approx \frac{\Delta^2}{20\epsilon^2} \tag{216}$$

$$= \frac{\Delta^2}{20\delta^2} \tag{217}$$

Recall $V_{UB}^{\text{uniform}} = \frac{\Delta^2}{12\delta^2}$.
Therefore,

$$\lim_{\epsilon=\delta\to 0} \frac{V_{UB}^{\text{uniform}}}{V_{LB}} = \frac{1}{12(2-4\log(\frac{3}{2}) - 2(\log(\frac{3}{2}))^2)} \approx \frac{5}{3}, \tag{218}$$

and thus

$$\limsup_{\epsilon\leq\delta\to 0} \frac{V_{UB}^{\text{uniform}}}{V_{LB}} \leq \frac{1}{12(2-4\log(\frac{3}{2}) - 2(\log(\frac{3}{2}))^2)} \approx \frac{5}{3}. \tag{219}$$

■

## Appendix G
## Proof of Corollary 14

*Proof of Corollary 14:* For the cost function $\mathcal{L}(k) = |k|$,

$$V_{LB} = 2\sum_{k=0}^{n-1} ab^k \mathcal{L}(1+k\Delta) \tag{220}$$

$$= 2\sum_{k=0}^{n-1} ab^k (1+k\Delta) \tag{221}$$

$$= 1 + 2a\Delta\sum_{k=0}^{n-1} b^k k \tag{222}$$

$$= 1 + 2a\Delta(\frac{b-b^n}{(1-b)^2} - \frac{(n-1)b^n}{1-b}). \tag{223}$$

Given $\epsilon > 0$, $V_{LB}$ is a decreasing function of $\delta$. Therefore, to lower bound $\frac{V_{UB}^{\text{Lap}}}{V_{LB}}$ in the regime $\delta \leq \epsilon$, we only need to consider the case $\delta = \epsilon$. Thus, in the following we set $\delta = \epsilon$.

Following the same calculations in the proof of Corollary 12, we have

$$V_{LB} \approx \frac{\Delta}{\delta}(1 - 2\log\frac{3}{2}) \tag{224}$$

$$\approx 0.19\frac{\Delta}{\delta} \tag{225}$$

$$= 0.19\frac{\Delta}{\epsilon}. \tag{226}$$

On the other hand, we have

$$V_{UB}^{\text{Lap}} = 2\sum_{k=1}^{+\infty} \frac{1-\lambda}{1+\lambda}\lambda^k k \tag{227}$$

$$= \frac{2e^{-\frac{\epsilon}{\Delta}}}{1-e^{-2\frac{\epsilon}{\Delta}}} \tag{228}$$

$$\approx \frac{\Delta}{\epsilon}, \tag{229}$$

as $\epsilon \to 0$.

Therefore,

$$\lim_{\epsilon=\delta\to 0} \frac{V_{UB}^{\text{Lap}}}{V_{LB}} = \frac{1}{1-2\log\frac{3}{2}} \approx 5.29, \tag{230}$$

and thus

$$\limsup_{\delta\leq\epsilon\to 0} \frac{V_{UB}^{\text{Lap}}}{V_{LB}} \leq \frac{1}{1-2\log\frac{3}{2}} \approx 5.29. \tag{231}$$

■

## Appendix H
## Proof of Corollary 15

*Proof of Corollary 15:* Using the same argument in the proof of Corollary 14, we can set $\epsilon = \delta$.

For the cost function $\mathcal{L}(k) = k^2$, following the same calculations in the proof of Corollary 13, we have

$$V_{LB} \approx \frac{\Delta^2}{\epsilon^2}(2 - 4\log(\frac{3}{2}) - 2(\log(\frac{3}{2}))^2) \tag{232}$$

$$\approx \frac{\Delta^2}{20\epsilon^2} \tag{233}$$

On the other hand, we have

$$\begin{aligned} V_{UB}^{\text{Lap}} &= 2\sum_{k=1}^{+\infty} \frac{1-\lambda}{1+\lambda}\lambda^k k^2 && (234)\\ &= \frac{2\lambda}{(1-\lambda)^2} && (235)\\ &\approx 2\frac{\Delta^2}{\epsilon^2}, && (236)\end{aligned}$$

as $\epsilon \to 0$.

Therefore,

$$\lim_{\epsilon=\delta\to 0} \frac{V_{UB}^{\text{Lap}}}{V_{LB}} = \frac{2}{(2-4\log(\frac{3}{2})-2(\log(\frac{3}{2}))^2)} \approx 40, \quad (237)$$

and thus

$$\limsup_{\delta\le\epsilon\to 0} \frac{V_{UB}^{\text{Lap}}}{V_{LB}} \le \frac{2}{(2-4\log(\frac{3}{2})-2(\log(\frac{3}{2}))^2)} \approx 40. \quad (238)$$

■

## Appendix I
## Proof of Theorem 16

*Proof of Theorem 16:* Consider the dual program of the linear program (75),

$$\begin{aligned} V_{LB} := \max\ & \mu - \delta\left(\sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)}\right)\\ \text{s.t. } & y_{i_1}^{(1)}, y_{i_2}^{(2)}, \ldots, y_{i_d}^{(d)} \ge 0, \quad \forall i_1 \in \mathbb{Z},\\ & \qquad i_2\in\mathbb{Z},\ldots,i_d\in\mathbb{Z}\\ & \mu - \sum_{i_1\in[k_1-\Delta+1,k_1]} y_{i_1}^{(1)} - \ldots - \sum_{i_d\in[k_d-\Delta+1,k_d]} y_{i_d}^{(d)}\\ & \le |k_1|+|k_2|+\cdots+|k_d|, \quad \forall (k_1,\ldots,k_d)\in\mathbb{Z}^d.\end{aligned}$$

Consider a candidate solution with

$$\mu = \frac{d\Delta}{2\delta} \quad (239)$$

and for all $m \in \{1,2,\ldots,d\}$,

$$y_i^{(m)} = \begin{cases} \frac{\mu}{d} & i=0\\ \max(\frac{\mu}{d}-k\Delta, 0) & \\ & i=k\Delta,\ \text{for } k\in\mathbb{Z},\ k\ge 1\\ \max(\frac{\mu}{d}-(|k|-1)\Delta-1, 0) & \\ & i=k\Delta,\ \text{for } k\in\mathbb{Z},\ k\le -1\\ 0 & \text{otherwise}\end{cases} \quad (240)$$

It is easy to verify that this candidate solution satisfies the constraints, and the corresponding value of the objective function is

$$\begin{aligned} &\mu - \delta\left(\sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)}\right) && (241)\\ &= \mu - \delta d \sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} && (242)\\ &= \mu - \delta d\left(\sum_{i=0}^{\frac{\mu}{d\Delta}} (\frac{\mu}{d} - i\Delta) + \sum_{i=0}^{\frac{\mu}{d\Delta}-1} (\frac{\mu}{d} - i\Delta - 1)\right) && (243)\\ &= \mu - \delta d\left(\frac{\frac{\mu}{d}(\frac{\mu}{d\Delta}+1)}{2} + \frac{(\frac{\mu}{d}+\Delta-2)\frac{\mu}{d\Delta}}{2}\right) && (244)\\ &= \mu - \delta d(\frac{\mu^2}{d^2\Delta} + \frac{\mu}{d} - \frac{\mu}{d\Delta}) && (245)\\ &= \mu - \delta(\frac{\mu^2}{d\Delta} + \mu - \frac{\mu}{\Delta}) && (246)\\ &= \frac{d\Delta}{4\delta} - \frac{\Delta-1}{2}d. && (247)\end{aligned}$$

Therefore, we have

$$V_{LB} \ge \frac{d\Delta}{4\delta} - \frac{\Delta-1}{2}d. \quad (248)$$

■

## Appendix J
## Proof of Theorem 17

*Proof of Theorem 17:* Consider the dual program of the linear program (75),

$$\begin{aligned} V_{LB} := \max\ & \mu - \delta\left(\sum_{i_1\in\mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2\in\mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d\in\mathbb{Z}} y_{i_d}^{(d)}\right)\\ \text{s.t. } & y_{i_1}^{(1)}, y_{i_2}^{(2)}, \ldots, y_{i_d}^{(d)} \ge 0, \quad \forall i_1 \in \mathbb{Z},\\ & \qquad i_2\in\mathbb{Z},\ldots,i_d\in\mathbb{Z}\\ & \mu - \sum_{i_1\in[k_1-\Delta+1,k_1]} y_{i_1}^{(1)} - \ldots - \sum_{i_d\in[k_d-\Delta+1,k_d]} y_{i_d}^{(d)}\\ & \le |k_1|^2+|k_2|^2+\cdots+|k_d|^2, \quad \forall (k_1,\ldots,k_d)\in\mathbb{Z}^d.\end{aligned}$$

To avoid integer-rounding issues, assume that $\frac{1}{2\delta}$ is an integer. Consider a candidate solution with

$$\mu = \frac{d\Delta^2}{4\delta^2} \quad (249)$$

and for all $m \in \{1,2,\ldots,d\}$,

$$y_i^{(m)} = \begin{cases} \frac{\mu}{d} & i=0\\ \frac{\mu}{d} - k^2\Delta^2 & \\ & i=k\Delta,\ \text{for } 1\le k \ge \frac{1}{2\delta}\\ \frac{\mu}{d} - ((|k|-1)\Delta+1)^2 & \\ & i=k\Delta,\ \text{for } -\frac{1}{2\delta}\le k\le -1\\ 0 & \text{otherwise}\end{cases} \quad (250)$$

It is easy to verify that this candidate solution satisfies the constraints, and the corresponding value of the objective function is

$$\mu - \delta \left( \sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2 \in \mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d \in \mathbb{Z}} y_{i_d}^{(d)} \right) \tag{251}$$

$$= \mu - \delta d \sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} \tag{252}$$

$$= \mu - \delta d \left( \sum_{i=0}^{\frac{1}{2\delta}} (\frac{\mu}{d} - i^2 \Delta^2) + \sum_{i=0}^{\frac{1}{2\delta}-1} (\frac{\mu}{d} - (i\Delta + 1)^2) \right) \tag{253}$$

$$= \frac{d\Delta^2}{12\delta^2} + (\frac{1}{\Delta} - 1)\frac{d\Delta^2}{4\delta} + \frac{1-\Delta}{2} d + \frac{d\Delta^2}{6}. \tag{254}$$

Therefore, we have

$$V_{LB} \geq \frac{d\Delta^2}{12\delta^2} + (\frac{1}{\Delta} - 1)\frac{d\Delta^2}{4\delta} + \frac{1-\Delta}{2} d + \frac{d\Delta^2}{6}. \tag{255}$$

■

## APPENDIX K
## PROOF OF THEOREM 25

*Proof of Theorem 25:* Consider a candidate solution with $\mu = \frac{d\Delta \log \frac{3}{2}}{\beta}$ (assuming $k \triangleq \frac{\mu}{d\Delta}$ is an integer), and for all $m \in \{1, 2, \ldots, d\}$,

$$y_i^{(m)} = \begin{cases} 0 & i \leq -k\Delta \\ e^{\beta} y_{i-\Delta}^{(m)} + 1 & i \in [-k\Delta + 1, 0] \\ \max(e^{\beta} y_{i-\Delta}^{(m)} - 1, 0) & i \geq 0. \end{cases} \tag{256}$$

It is easy to verify that the above candidate solution satisfies the constraints of the dual linear program. We can derive the analytical expression for $y_i^m$, which is

$$y_i^{(m)} = \begin{cases} 0 & i \leq -k\Delta \\ \frac{e^{(k-j)\beta} - 1}{e^{\beta} - 1} & i \in [-(j+1)\Delta + 1, -j\Delta], \\ & \text{for } j \in [0, k-1] \\ \max(e^{j\beta} \frac{e^{k\beta} - 2}{e^{\beta} - 1} + \frac{1}{e^{\beta} - 1}, 0) & i \in [(j-1)\Delta + 1, j\Delta]. \end{cases} \tag{257}$$

To avoid integer-rounding issues, assume that $n \triangleq \frac{1}{\beta} \log \frac{1}{2 - e^{k\beta}} = \frac{\log 2}{\beta}$ is an integer. Then the value of the objective function with this candidate solution is

$$\mu - \beta \left( \sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2 \in \mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d \in \mathbb{Z}} y_{i_d}^{(d)} \right) \tag{258}$$

$$= \mu - \beta d \sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} \tag{259}$$

$$= \mu - \beta d \Delta \left( \sum_{i=1}^{k} \frac{e^{i\beta} - 1}{e^{\beta} - 1} + \sum_{i=1}^{n} (e^{i\beta} \frac{e^{k\beta} - 2}{e^{\beta} - 1} + \frac{1}{e^{\beta} - 1}) \right) \tag{260}$$

$$= \mu - \beta d \Delta \left( \frac{\frac{e^{\beta}(1 - e^{k\beta})}{1 - e^{\beta}} - k}{e^{\beta} - 1} + \frac{e^{k\beta} - 2}{e^{\beta} - 1} \frac{e^{\beta}(1 - e^{n\beta})}{1 - e^{\beta}} + \frac{n}{e^{\beta} - 1} \right) \tag{261}$$

$$= \frac{d\Delta \log \frac{3}{2}}{\beta} - \beta d \Delta \left( \frac{\frac{e^{\beta}(1 - \frac{3}{2})}{1 - e^{\beta}} - \frac{\log \frac{3}{2}}{\beta}}{e^{\beta} - 1} + \frac{-\frac{1}{2}}{e^{\beta} - 1} \frac{e^{\beta}(1 - 2)}{1 - e^{\beta}} + \frac{\log 2}{\beta(e^{\beta} - 1)} \right) \tag{262}$$

$$= \frac{d\Delta \log \frac{3}{2}}{\beta} - \beta d \Delta \left( \frac{e^{\beta}}{2(e^{\beta} - 1)^2} - \frac{\log \frac{3}{2}}{\beta(e^{\beta} - 1)} - \frac{e^{\beta}}{2(e^{\beta} - 1)^2} + \frac{\log 2}{\beta(e^{\beta} - 1)} \right) \tag{263}$$

$$= \Theta\left( \frac{d\Delta}{\beta} (\log \frac{3}{2} - \frac{1}{2} + \log \frac{3}{2} + \frac{1}{2} - \log 2) \right) \tag{264}$$

$$= \log \frac{9}{8} \Theta\left( \frac{d\Delta}{\beta} \right) \tag{265}$$

$$\approx \Theta\left( 0.1178 \frac{d\Delta}{\beta} \right), \tag{266}$$

as $\beta \triangleq \max(\epsilon, \delta) \to 0$.

Therefore,

$$\liminf_{\max(\epsilon,\delta) \to 0} \frac{V'_{LB}}{\frac{d\Delta}{\beta}} \geq \log \frac{9}{8} \approx 0.1178 \tag{267}$$

■

## APPENDIX L
## PROOF OF THEOREM 26

*Proof of Theorem 26:* Let $\alpha = \frac{3}{2}$. Consider a candidate solution with $\mu = \frac{d\Delta^2 \log^2 \alpha}{\beta^2}$ (assuming $k \triangleq \frac{\sqrt{\frac{\mu}{d}}}{\Delta} = \frac{\log \alpha}{\beta}$ is an integer), and for all $m \in \{1, 2, \ldots, d\}$,

$$y_i^{(m)} = \begin{cases} 0 & i \leq -k\Delta \\ e^{\beta} y_{i-\Delta}^{(m)} + 2|i| + 1 & i \in [-k\Delta + 1, 0] \\ \max(e^{\beta} y_{i-\Delta}^{(m)} - (2i + 1), 0) & i \geq 0. \end{cases} \tag{268}$$

It is easy to verify that the above candidate solution satisfies the constraints of the dual linear program.

Define

$$z_1 = \frac{2}{e^{\beta} - 1}, \tag{269}$$

$$z_2 = \frac{1 - \frac{2e^{\beta}\Delta}{e^{\beta} - 1}}{e^{\beta} - 1}, \tag{270}$$

$$z_3 = \frac{2}{1 - e^{\beta}}, \tag{271}$$

$$z_4 = \frac{1 - \frac{2e^{\beta}\Delta}{1 - e^{\beta}}}{1 - e^{\beta}}. \tag{272}$$

We can derive the analytical expression for $y_i^m$, which is $y_i^{(m)} = 0$, $\forall i \leq -k\Delta$, and $\forall i = -(k'\Delta + j)$ for $k' \in [0, k-1]$, $j \in [0, \Delta - 1]$,

$$y_i^{(m)} = e^{(k-k')\beta} (z_1(k\Delta + j) + z_2) - z_1(k'\Delta + j) - z_2 \tag{273}$$

and for $i = (m-1)\Delta + j$, where $j \in [1, \Delta]$, $m \geq 1$,

$$y_i^{(m)} = \max(a_{m,j}, 0), \tag{274}$$

where

$$\begin{aligned} a_{m,j} &\triangleq e^{m\beta}(z_1(k\Delta + \Delta - j) + z_2) \\ &\quad - z_1(\Delta - j) - z_2 - z_3(\Delta - j) + z_4) \\ &\quad - z_4 - z_3((m-1)\Delta + j). \end{aligned}$$

For each $j \in [1, \Delta]$, and we are interested in finding the number $m(j)$ such that $a_{m(j),j} = 0$. As $\beta \to 0$, from $a_{m(j),j} = 0$, we get

$$e^{m(j)\beta} e^{k\beta} (\frac{2}{\beta} k\Delta - \frac{2\Delta}{\beta^2}) = -\frac{2\Delta}{\beta^2} - \frac{2}{\beta} m(j)\Delta + o(\frac{1}{\beta^2}). \tag{275}$$

Therefore,

$$m(j) = \frac{\log \gamma}{\beta} + o(\frac{1}{\beta}), \tag{276}$$

where $\gamma$ is the solution to

$$\gamma\alpha(\log\alpha - 1) = -(1 + \log\gamma). \tag{277}$$

When $\alpha = \frac{3}{2}$, we have $\gamma \approx 1.7468$.

Therefore, the value of the objective function is

$$\begin{aligned} &\mu - \beta\left(\sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} + \sum_{i_2 \in \mathbb{Z}} y_{i_2}^{(2)} + \cdots + \sum_{i_d \in \mathbb{Z}} y_{i_d}^{(d)}\right) \\ &= \mu - \beta d \sum_{i_1 \in \mathbb{Z}} y_{i_1}^{(1)} \\ &= \mu - \beta d(\sum_{k'=0}^{k-1} \sum_{j=0}^{\Delta-1} y_{-(k'\Delta+j)}^{(1)} + \sum_{j=1}^{\Delta} \sum_{m=1}^{m(j)} y_{(m-1)\Delta+j}^{(1)}) \\ &= \frac{d\Delta^2 \log^2\alpha}{\beta^2} \\ &\quad - \beta d(\frac{1 - e^{-k\beta}}{1 - e^{-\beta}} e^{k\beta}((z_1 k\Delta + z_2)\Delta + z_1\frac{\Delta(\Delta-1)}{2}) \\ &\qquad - z_1\Delta^2\frac{k(k-1)}{2} - z_1 k\frac{\Delta(\Delta-1)}{2} - z_2 k\Delta) \\ &\quad - \beta d\sum_{j=1}^{\Delta}(\frac{e^{\beta}(1 - e^{m(j)\beta})}{1 - e^{\beta}}(e^{k\beta}(z_1(k\Delta + \Delta - j) + z_2) \\ &\qquad - z_1(\Delta - j) - z_2 - z_3(\Delta - j) + z_4) - z_4 m(j) \\ &\qquad - z_3\Delta\frac{m(j)(m(j)+1)}{2} + z_3(\Delta - j)m') \\ &= \frac{d\Delta^2}{\beta^2}(\log^2\alpha - (\alpha - 1)(2\log\alpha - 2) + \log^2\alpha - 2\log\alpha \\ &\qquad + (1-\gamma)\alpha(2\log\alpha - 2) - 2\log\gamma - \log^2\gamma) + o(\frac{1}{\beta^2}) \\ &= \frac{d\Delta^2}{\beta^2}\left(2\log^2\alpha - 2 - 2\alpha\gamma\log\alpha + 2\alpha\gamma - 2\log\gamma - \log^2\gamma\right) \\ &\quad + o(\frac{1}{\beta^2}) \\ &\approx 0.0177\frac{d\Delta^2}{\beta^2} + o(\frac{1}{\beta^2}). \end{aligned}$$

as $\beta \triangleq \max(\epsilon, \delta) \to 0$.

Therefore,

$$\liminf_{\max(\epsilon,\delta)\to 0} \frac{V'_{LB}}{\frac{d\Delta^2}{\beta^2}} \geq 0.0177. \tag{278}$$

■

## Acknowledgment

The authors would like to thank the associate editor Dr. Adam Smith and the anonymous reviewers for their insightful comments and suggestions, which help us improve the presentation of this work.

## References

[1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography* (Lecture Notes in Computer Science), vol. 3876, S. Halevi and T. Rabin, Eds. Berlin, Germany: Springer, 2006, pp. 265–284.

[2] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory Appl. Models Comput. (TAMC)*, Berlin, Germany, 2008, pp. 1–19.

[3] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2014, pp. 2371–2375.

[4] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The staircase mechanism in differential privacy," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1176–1184, Oct. 2015.

[5] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Berlin, Germany, 2006, pp. 486–503.

[6] C. Dwork and J. Lei, "Differential privacy and robust statistics," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2009, pp. 371–380.

[7] C. Dwork, G. N. Rothblum, and S. Vadhan, "Boosting and differential privacy," in *Proc. IEEE 51st Annu. Symp. Found. Comput. Sci. (FOCS)*, Washington, DC, USA, Oct. 2010, pp. 51–60.

[8] A. Nikolov, K. Talwar, and L. Zhang, "The geometry of differential privacy: The sparse and approximate cases," in *Proc. 45th Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2013, pp. 351–360.

[9] S. P. Kasiviswanathan, M. Rudelson, A. Smith, and J. Ullman, "The price of privately releasing contingency tables and the spectra of random matrices with correlated rows," in *Proc. 42nd Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2010, pp. 775–784.

[10] A. De, "Lower bounds in differential privacy," in *Proc. 9th Int. Conf. Theory Cryptogr. (TCC)*, Berlin, Germany, 2012, pp. 321–338.

[11] K. Nissim, S. Raskhodnikova, and A. Smith, "Smooth sensitivity and sampling in private data analysis," in *Proc. 39th Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2007, pp. 75–84.

[12] K. Chaudhuri and C. Monteleoni, "Privacy-preserving logistic regression," in *Proc. Adv. Neural Inf. Process. Syst.*, Vancouver, BC, Canada, 2008, pp. 289–296.

[13] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Washington, DC, USA, Oct. 2007, pp. 94–103.

[14] R. Hall, A. Rinaldo, and L. Wasserman, "Differential privacy for functions and functional data," *J. Mach. Learn. Res.*, vol. 14, no. 1, pp. 703–727, 2013.

[15] S. P. Kasiviswanathan and A. Smith, "A note on differential privacy: Defining resistance to arbitrary side information," *CoRR*, vol. abs/0803.3946, 2008. [Online]. Available: http://arxiv.org/abs/0803.3946

[16] K. Chaudhuri and N. Mishra, "When random sampling preserves privacy," in *Proc. 26th Annu. Int. Conf. Adv. Cryptol. (CRYPTO)*, Berlin, Germany, 2006, pp. 198–213.

[17] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proc. IEEE 24th Int. Conf. Data Eng. (ICDE)*, Washington, DC, USA, Apr. 2008, pp. 277–286.

[18] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2009, pp. 351–360.

[19] H. Brenner and K. Nissim, "Impossibility of differentially private universally optimal mechanisms," in *Proc. 51st Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2010, pp. 71–80.

[20] M. Gupte and M. Sundararajan, "Universally optimal privacy mechanisms for minimax agents," in *Proc. 29th ACM SIGMOD-SIGACT-SIGART Symp. Principles Database Syst.*, 2010, pp. 135–146.

[21] C. Fang and E.-C. Chang, "Adaptive differentially private histogram of low-dimensional data," in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 7384, S. Fischer-Hübner and M. Wright, Eds. Berlin, Germany: Springer, 2012, pp. 160–179.

[22] M. Hay, V. Rastogi, G. Miklau, and D. Suciu, "Boosting the accuracy of differentially private histograms through consistency," *Proc. VLDB Endowment*, vol. 3, nos. 1–2, pp. 1021–1032, Sep. 2010.

[23] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proc. 42nd ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2010, pp. 705–714.

[24] J. Xu, Z. Zhang, X. Xiao, Y. Yang, and G. Yu, "Differentially private histogram publication," in *Proc. IEEE 28th Int. Conf. Data Eng. (ICDE)*, Apr. 2012, pp. 32–43.

[25] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, "Optimizing linear counting queries under differential privacy," in *Proc. 29th ACM SIGMOD-SIGACT-SIGART Symp. Principles Database Syst. (PODS)*, New York, NY, USA, 2010, pp. 123–134.

[26] P. Jain, P. Kothari, and A. Thakurta, "Differentially private online learning," in *Proc. 25th Annu. Conf. Learn. Theory (COLT)*, 2012, pp. 1–27.

[27] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," in *Proc. 32nd Int. Conf. Mach. Learn. (ICML)*, 2015, pp. 1376–1385.

[28] L. Wasserman and S. Zhou, "A statistical framework for differential privacy," *J. Amer. Statist. Assoc.*, vol. 105, no. 489, pp. 375–389, 2010.

**Quan Geng** is a software engineer at Google Inc., New York. He received his B.S. in Electronic Engineering from Tsinghua Univeristy in 2009, M.S. in Electrical and Computer Engineering in 2011, M.S. in Mathematics in 2012, and Ph.D. in Electrical and Computer Engineering in 2013 from University of Illinois at Urbana Champaign. He has interned at Microsoft Research Asia, Qualcomm Flarion Technologies and Tower Research Capital LLC. He worked at Tower Research Capital LLC as a high-frequency quantitative analyst from January 2014 to September 2015. His research interests include information theory, wireless communication, machine learning and differential privacy.

**Pramod Viswanath** (S'98–M'03–SM'10–F'13) received the Ph.D. degree in electrical engineering and computer science from the University of California at Berkeley, Berkeley, in 2000. He was a member of technical staff at Flarion Technologies until August 2001 before joining the Electrical and Computer Engineering Department, University of Illinois at Urbana-Champaign (UIUC), Urbana. Dr. Viswanath is a recipient of the Xerox Award for Faculty Research from the College of Engineering at UIUC (2010), the Eliahu Jury Award from the Electrical Engineering and Computer Science Department of the University of California at Berkeley (2000), the Bernard Friedman Award from the Mathematics Department of the University of California at Berkeley (2000), and the National Science Foundation (NSF) CAREER Award (2003). He was an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY for the period 2006-2008.