Differentially Private Multivariate Statistics with an Application to Contingency Table Analysis

Minwoo Kim†, Jonghyeok Lee†, Seung Woo Kwak, and Sungkyu Jung‡

Department of Statistics, Seoul National University, Seoul 08826, South Korea

May 16, 2023

Abstract

Differential privacy (DP) has become a rigorous central concept for privacy protection in the past decade. We use Gaussian differential privacy (GDP) in gauging the level of privacy protection for releasing statistical summaries from data. The GDP is a natural and easy-to-interpret differential privacy criterion based on the statistical hypothesis testing framework. The Gaussian mechanism is a natural and fundamental mechanism that can be used to perturb multivariate statistics to satisfy a $\mu$-GDP criterion, where $\mu > 0$ stands for the level of privacy protection. Requiring a certain level of differential privacy inevitably leads to a loss of statistical utility. We improve ordinary Gaussian mechanisms by developing rank-deficient James-Stein Gaussian mechanisms for releasing private multivariate statistics, and show that the proposed mechanisms have higher statistical utilities. Laplace mechanisms, the most commonly used mechanisms in the pure DP framework, are also investigated under the GDP criterion. We show that optimal calibration of multivariate Laplace mechanisms requires more information on the statistic than just the global sensitivity, and derive the minimal amount of Laplace perturbation for releasing $\mu$-GDP contingency tables. Gaussian mechanisms are shown to have higher statistical utilities than Laplace mechanisms, except for very low levels of privacy. The utility of proposed multivariate mechanisms is further demonstrated using differentially private hypotheses tests on contingency tables. Bootstrap-based goodness-of-fit and homogeneity tests, utilizing the proposed rank-deficient James-Stein mechanisms, exhibit higher powers than natural competitors.

Keywords: Differential privacy, Sensitivity space, James-Stein estimator, Trade-off function, Private goodness-of-fit test

1 Introduction

Privacy has become a crucial concern in modern statistical analyses and machine learning. Data sets collected in recent years have grown exponentially in size and often contain sensitive personal information. Consequently, it has become increasingly important to prevent privacy disclosure when publicly releasing data sets containing personal information, or even when releasing statistical summaries from the data sets. In this paper, we investigate private release of multivariate statistics satisfying a pre-specified degree of privacy protection, governed by differential privacy. Differential privacy (Dwork et al. 2006b), or DP, and its variants (Mironov, 2017; Dong et al., 2022) provide formal criteria for data privacy and can be achieved by randomly perturbing the statistics to be released.

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No.2019R1A2C2002256) and Institution of Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government (MSIT) (No.2022-0-000937, Solving the problem of increasing the usability and usefulness synthetic data algorithm for statistical data).

†Equal contribution.

‡Corresponding author. Email address: sungkyu@snu.ac.kr
Let $S = (x_1, \ldots, x_n) \in \mathcal{X}^n$ be a data set collected from a sample space $\mathcal{X}$, and let $\theta(S) \in \mathbb{R}^p$ denote a multivariate summary statistic computed from the data set $S$. (We also call the map $\theta : \mathcal{X}^n \to \mathbb{R}^p$, defined for any $n \in \mathbb{N}$, a statistic.) Our development applies to any form of multivariate statistics, from the multivariate mean vector to regression coefficient estimators. Since the most common types of data release from data sets containing sensitive personal information are contingency tables and histograms, we will pay special attention to the case that $\theta$ is a contingency (or frequency) table.

Let $M : \mathcal{X}^n \to \mathbb{R}^p$ be a randomized map, called a mechanism, that outputs a randomly perturbed $\theta(S)$. A commonly used mechanism for differential privacy is an additive mechanism that adds a random noise $\xi$ to the given statistic, e.g.,

$$M(S) = \theta(S) + \xi, \quad \xi \sim N_p(0, \sigma^2 I_p),$$

(1)

where $I_p$ is the $p \times p$ identity matrix. We choose to use Gaussian differential privacy (GDP) of Dong et al. (2022) to measure the degrees of privacy protection in a mechanism $M$, and to calibrate the amount of noise infused in $M$. In the GDP framework, the level of privacy protection is summarized by a single parameter $\mu > 0$, and we say a randomized mechanism $M$ is $\mu$-GDP if determining whether any specific piece of personal information is present in the data set $S$, based on a single output $M(S)$, is as difficult as testing

$$H_0 : X \sim N(0,1) \quad \text{vs.} \quad H_1 : X \sim N(\mu,1)$$

based on a single observation of $X$. It is known that for the Gaussian mechanism (1) to satisfy $\mu$-GDP (for a pre-specified $\mu > 0$), the amount of random noise in $\xi$ should satisfy $\sigma \geq \mu^{-1} \Delta_2(\theta; \mathcal{X}^n)$, where $\Delta_2(\theta; \mathcal{X}^n)$, called $L_2$-sensitivity of $\theta$, is the largest possible $L_2$-discrepancy of $\theta$ when one individual’s record in the data is replaced by someone else’s. See Section 1.1 for a brief review of GDP.

In this work, we propose and compare various refinements on multivariate additive mechanisms stemming from adding Gaussian or Laplace-distributed noise, that are calibrated to satisfy $\mu$-GDP for each given $\mu > 0$. In particular, we propose rank-deficient James–Stein post-processed Gaussian mechanisms, denoted $M_{\text{JS}}$, and show that $M_{\text{JS}}$ has a smaller loss of statistical utility than ordinary Gaussian mechanisms of (1) in Section 2. The statistical utility of a mechanism $M$ is measured via the mean squared error of $M$ when compared to $\theta$, i.e., $L_2(M) = E\|M(S) - \theta(S)\|^2_2$. The rank-deficient James–Stein mechanism $M_{\text{JS}}$ improves upon Gaussian mechanisms in two ways.

First, $M_{\text{JS}}$ exploits the set $S_0 := \{\theta(S) - \theta(S') : S, S' \in \mathcal{X}^n, S \sim S'\} \subset \mathbb{R}^p$ (the notation $S \sim S'$ means that data sets $S$ and $S'$ differ in exactly one record) rather than using only the maximum potential difference $\Delta_2(\theta; \mathcal{X}^n) = \max_{v \in S_0} \|v\|_2$ between data sets, which was used for calibration of (1). We show that if $\text{span}(S_0)$ has dimension less than $p$, then adding Gaussian noise with a carefully chosen rank-deficient covariance matrix not only satisfies $\mu$-GDP but also has larger statistical utility than (1). The rank-deficient mechanisms are especially useful for releasing private contingency tables, since for a frequency table $\theta$ (with no overlapping categories), $\text{span}(S_0)$ has dimension $p - 1$, and is indeed a proper subspace of $\mathbb{R}^p$.

Another improvement of a Gaussian mechanism (1) is obtained by perceiving (1) for fixed $S$ as a multivariate mean $\theta(S)$ estimation problem with one observation $M(S)$. If the dimension $p$ is not small, the celebrated James–Stein shrinkage estimator provides smaller mean squared error than the ordinary least squares estimator (which is $M(S)$ itself in our context) (James and Stein, 1961; Efron, 2012; Balle and Wang, 2018). The rank-deficient James–Stein mechanism $M_{\text{JS}}$ exploits both rank-deficiency of $\text{span}(S_0)$ and the James–Stein shrinkage phenomenon, and we show that $M_{\text{JS}}$ can be calibrated to satisfy $\mu$-GDP, and has the largest statistical utility among natural competitors of the same privacy level.

In addition, we provide the optimal calibration for Laplace mechanisms of the form $M(S) = \theta(S) + \xi, \xi = (\xi_1, \ldots, \xi_p)$, where each $\xi_i$ follows independently Laplace distribution with scale parameter $b$. In Section 3, we develop several important technical lemmas that can be used to calibrate multivariate Laplace mechanisms with respect to the $\mu$-GDP criterion, which turns out to be substantially different than the case of univariate statistics. Optimal calibration of Laplace mechanisms heavily depends on the sensitivity space $S_0$, and we provide optimal calibration results
for the case where \( \Delta_1(\theta) = \max_{v \in \mathcal{S}_\theta} \|v\|_1 \) is the only information on \( \theta \), and also for the case that \( \theta \) is a contingency table.

In Section 4 we show that the statistical utility of Laplace mechanisms is typically lower than that of Gaussian mechanisms, when both mechanisms satisfy \( \mu \)-GDP. This makes sense because the GDP criterion uses the trade-off between two Gaussian distributions. However, perhaps surprisingly, Laplace mechanisms have higher utility than Gaussian mechanisms for low privacy regimes with larger \( \mu \).

The proposed mechanisms and their calibration results are demonstrated by an application of releasing differentially private contingency (or frequency) tables, and we numerically compare the statistical utilities of various mechanisms in Section 3. We also provide private hypothesis testing procedures for testing goodness-of-fit and homogeneity among different populations, using the differentially private contingency tables we have developed. The test procedure assumes that the only available information on the data set is \( M(S) \), a randomly perturbed contingency table, and uses a parametric bootstrap procedure in the computation of \( p \)-values. In a numerical study, we reveal our proposed test procedures control the type I error rates at a given significance level, and the power increases as the sample size increases. Our test procedure based on the rank-deficient James–Stein mechanism \( M_{JS} \) shows the highest empirical power among competitors.

We note that there are other types of randomized mechanisms that can be used to satisfy a DP criterion. Prominent examples are the exponential mechanism (McSherry and Talwar, 2007), staircase mechanism (Kairouz et al., 2014), randomized responses (Dwork et al., 2006b), and \( K \)-norm mechanisms (Awan and Slavković, 2021). Compositions of these mechanisms can also satisfy a given privacy criterion (Dwork et al., 2014; Abadi et al., 2016; Dong et al., 2021; Balle and Wang, 2018) proposed to use post-processing in the form of shrinkage, as we investigate in this work. While Balle and Wang (2018) demonstrated the advantage of the shrinkage empirically and also in a Bayesian perspective, we extend it to the case of shrinking towards the mean while simultaneously utilizing the structure of the sensitivity space \( S_\theta \), and show its advantage more formally. Exploiting \( S_\theta \) for maximizing statistical utilities of randomized mechanisms has been considered in Karwa et al. (2017); Avella-Medina (2021); Awan and Slavković (2021) as well. The trade-off between differential privacy and statistical utility is studied in Wasserman and Zhou (2010); Duchi et al. (2018); Cai et al. (2021). Several authors including Wasserman and Zhou (2010); Gaboardi et al. (2016); Wang et al. (2017); Kifer and Rogers (2016); Son et al. (2022) proposed differentially private procedures for contingency table analysis (or for releasing private histogram counts). All of these previous works, except (Dong et al., 2021; 2022), are developed under the original \( \epsilon \)-DP criterion, or a relaxed \((\epsilon, \delta)\)-DP criterion. On the other hand, we use the GDP criterion, since it enables a straightforward interpretation of privacy parameter \( \mu \) as the effect size in a hypothesis testing framework.

In Section 1.1 we provide a concise review of differential privacy, viewed in terms of statistical hypothesis testing. Multivariate Gaussian mechanisms and Laplace mechanisms are developed and studied in Sections 2 and 3, respectively, and their statistical utilities are compared in Section 4 with respect to the \( L_r \)-loss, \( r \geq 1 \). Applications to contingency table analysis are discussed in Section 5. Some important remarks about multivariate Laplace mechanisms are given in Section 6. Technical details and proofs of theoretical results are contained in the Appendix.

1.1 Differential privacy based on hypothesis testing

Let \( X \) be the sample space in which individual records of the data lie. For any two data sets \( S = (x_1, \ldots, x_n) \in X^n \) and \( S' = (x_1', \ldots, x_n') \in X^n \) of equal sample size, we say \( S \) and \( S' \) are neighbors if they differ by a single record, i.e., if there exists an \( i \in \{1, \ldots, n\} \) such that \( x_i \neq x_i' \) and \( x_i = x_i' \) for all \( i \neq i \). A mechanism \( M : X^n \rightarrow Y \) takes as input a data set \( S \) and releases some randomly perturbed data summary \( M(S) \) in some abstract space \( Y \). Having the data set \( S \) fixed, \( M(S) \) is a random variable taking values in \( Y \). A mechanism \( M \) is said to be differentially private at level \( \epsilon > 0 \), or \( \epsilon \)-DP (Dwork et al., 2006b), if for any neighboring data sets \( S, S' \) and for any set \( A \) of possible mechanism outputs

\[
e^{-\epsilon} \leq \frac{\mathbb{P}(M(S) \in A)}{\mathbb{P}(M(S') \in A)} \leq e^\epsilon,
\]

(2)
in which the probability is taken over the randomness of $M$, with $S$ and $S'$ being fixed. For smaller values of the privacy parameter $\varepsilon$, it is difficult to infer whether a specific private information is contained in the underlying data set $S$, just based on a perturbed observation of $M(S)$. Note that the relaxed privacy criterion of $(\varepsilon,\delta)$-DP [Dwork et al. 2006a], with an additional privacy parameter $\delta > 0$, is satisfied for a mechanism $\hat{M}$ if $P(M(S) \in A) \leq e^{\varepsilon}P(M(S') \in A) + \delta$ for all neighboring data sets $S, S'$ and for any $A$.

Differential privacy criteria can be equivalently described by the statistical hypothesis testing framework [Wasserman and Zhou 2010; Geng et al. 2015; Kairouz et al. 2015; Dong et al. 2022]. For a fixed pair of neighboring data sets $S, S'$, denote the distribution of $M(S)$ (or $M(S')$) by $P$ (or $Q$, respectively). Consider testing

$$H_0 : \text{data set is } S \text{ vs. } H_1 : \text{data set is } S',$$

or equivalently,

$$H_0 : M \sim P \text{ vs. } H_1 : M \sim Q,$$

based on a single observation $M$, where $M = M(S) \sim P$ under $H_0$ and $M = M(S') \sim Q$ under $H_1$. The difference between $P$ and $Q$ may be described by the smallest type II error rate of level-$\alpha$ tests, for each $\alpha \in (0,1)$. This amounts to quantifying the trade-off between the level of a test and its power. (Recall that requiring more strict control of type I errors (i.e., smaller level) for a test results in smaller power of the test.) Let $\phi : \mathcal{Y} \to [0,1]$ be the decision function of a (randomized) test procedure for hypotheses $\{2\}$, and write $\alpha_\phi = \mathbb{E}_{M \sim P}[\phi(M)]$ for the type I error rate, and $\beta_\phi = 1 - \mathbb{E}_{M \sim Q}[\phi(M)]$ for the type II error rate, of $\phi$. Then the trade-off function $T(P,Q) : [0,1] \to [0,1]$ between distributions $P$ and $Q$ (or between hypotheses $\{2\}$) is defined by

$$T(P,Q)(\alpha) = \inf_{\phi} \{ \beta_\phi : \alpha_\phi \leq \alpha \}.$$

Note that for any $\alpha \in (0,1)$, $T(P,Q)(\alpha)$ is the type II error rate of the most powerful test of level $\alpha$.

For two distribution pairs $(P,Q)$ and $(F,G)$, if $T(P,Q) \geq T(F,G)$ (i.e., $T(P,Q)(\alpha) \geq T(F,G)(\alpha)$ for all $\alpha \in (0,1)$), then $P$ and $Q$ are harder to distinguish than $F$ and $G$ are. That is, the indistinguishability between $M(S)$ and $M(S')$ represented by the corresponding trade-off function $T(M(S),M(S')) := T(P,Q)$ can be bounded by other trade-off functions. Based on this observation, Dong et al. (2022) proposed a general criterion of differential privacy based on trade-off functions. A function $f$ is called a trade-off function if there exist distributions $F,G$ such that $f = T(F,G)$. Generally, any $f : [0,1] \to [0,1]$ is a trade-off function if it is convex, continuous, non-increasing, $f(x) \leq 1 - x$ and is symmetric about the line $x = y$. A mechanism $M$ is said to be $f$-differentially private (or $f$-DP) for a trade-off function $f$ if

$$\inf_{S \sim S'} T(M(S),M(S')) \geq f,$$

where the infimum is taken over the family of all neighboring pairs $S$ and $S'$ in $\mathcal{X}^n$. We write $S \sim S'$ if $S$ and $S'$ are neighbors.

The $(\varepsilon,\delta)$-DP criterion can be represented by the $f$-DP framework. In particular, for any $\varepsilon > 0$, $\delta \geq 0$, a mechanism $M$ is $(\varepsilon,\delta)$-DP if and only if $M$ is $f_{\varepsilon,\delta}$-DP, where

$$f_{\varepsilon,\delta}(\alpha) = \max\{0,1 - \delta - e^{\varepsilon}\alpha, e^{-\varepsilon}(1 - \delta - \alpha)\},$$

as shown in [Wasserman and Zhou 2010; Kairouz et al. 2015; Dong et al. 2022].

A simple one-parameter family of trade-off functions is obtained by univariate Gaussian distributions differing only by the mean parameter. For $\mu \geq 0$, let $G_\mu$ be the trade-off function between $N(0,1)$ and $N(\mu,1)$. Using the Neyman–Pearson lemma, one can check that for $\alpha \in (0,1)$

$$G_\mu(\alpha) = T(N(0,1),N(\mu,1))(\alpha) = \Phi(\Phi^{-1}(1 - \alpha) - \mu),$$

where $\Phi$ is the distribution function of the standard normal distribution [Dong et al. 2022].

**Definition 1** (Dong et al. 2022). For a $\mu \geq 0$, A mechanism $M$ is $\mu$-Gaussian differentially private (or $\mu$-GDP) if

$$\inf_{S \sim S'} T(M(S),M(S')) \geq G_\mu.$$
If \( M \) is \( \mu \)-GDP, distinguishing any two neighboring data sets based solely on an observed value of \( M \) is at least as hard as distinguishing \( N(0,1) \) and \( N(\mu,1) \). Since \( 0 \leq \mu < \mu' \) if and only if \( G_{\mu} > G_{\mu'} \), the smaller the privacy parameter \( \mu \) is, the greater privacy protection is guaranteed for a mechanism satisfying \( \mu \)-GDP.

Note that an ordinary (multivariate) Gaussian mechanism in the form of

\[
M_G(S) := \theta(S) + \xi, \quad \xi \sim N_p(0, \sigma^2 I_p),
\]

(where \( \theta(S) \in \mathbb{R}^p \)) is \( \mu \)-GDP for any \( \mu \geq \mu_0 := \Delta_2/\sigma \), where \( \Delta_2 = \sup_{S \sim S'} \| \theta(S) - \theta(S') \|_2 \) is called the global \( L_2 \)-sensitivity of the multivariate statistic \( \theta(S) \). (See Theorem 4.3 in Appendix A) That is, the level of privacy protection of a Gaussian mechanism \( M_G \) in (7) is precisely described by the privacy parameter \( \mu_0 \) under the GDP criterion. On the other hand, the Gaussian mechanism (7) does not satisfy \( \varepsilon \)-DP for any \( \varepsilon > 0 \), and there is no single set of privacy parameters \((\varepsilon, \delta)\) representing the degrees of privacy protection of a Gaussian mechanism under the \((\varepsilon, \delta)\)-DP criterion. To be precise, the Gaussian mechanism (7) satisfies \((\varepsilon, \delta)\)-DP for any combination of privacy parameters \((\varepsilon, \delta) \in (0, \infty)^2\) satisfying

\[
\Phi(\frac{\Delta_2}{\sigma} - \frac{\varepsilon}{\sigma}) - e^\varepsilon \Phi(\frac{\Delta_2}{\sigma} - \frac{\varepsilon}{\sigma}) \leq \delta,
\]

where \( \Phi \) is the standard normal distribution function (Theorem 8, Balle and Wang, 2018). Therefore, when statistics to be released are perturbed by Gaussian noise, using GDP criterion in gauging the privacy protection is more convenient (and is easier to interpret) than using \((\varepsilon, \delta)\)-DP criterion. For the rest of the article, we use the GDP criterion to control the level of privacy protection in randomized mechanisms.

Verifying whether a multivariate mechanism \( M \) satisfies \( \mu \)-GDP can be done via directly comparing trade-off functions \( T(M(S), M(S')) \) with \( G_M \). In Appendix A we provide several tools that can be used to work with trade-off functions between multivariate distributions.

As seen in (7), the amount of noise in a randomized mechanism can be calibrated using the global \( L_2 \)-sensitivity of the multivariate statistic \( \theta \). The global \( L_2 \)-sensitivity, or simply \( L_2 \)-sensitivity, for \( r > 0 \), is

\[
\Delta_r = \Delta_r(\theta; X^n) := \sup_{S \sim S'} \| \theta(S) - \theta(S') \|_r,
\]

and measures the maximum amount of changes in \( \theta \) in the \( \ell_r \)-norm sense, when one record in \( S \) is replaced by any potential record in \( X \), for any \( S \). As an instance, if \( X = [0, 1]^p \), the vector average \( \theta(S) = x_n = \frac{1}{n} \sum_{i=1}^n x_i \), where \( S = \{x_1, \ldots, x_n\} \subset X^n \), has the \( L_r \)-sensitivity

\[
\Delta_r = \frac{1}{n} \| \mathbf{1}_p \|_r = (p^{1/r})/n.
\]

## 2 Improving Gaussian multivariate mechanisms

In this section, we propose rank-deficient James–Stein Gaussian mechanism \( M_{r,JS} \) and investigate under which situations \( M_{r,JS} \) leads to smaller loss of statistical utility than the ordinary Gaussian mechanism (1).

The statistical utility of a randomized mechanism \( M \), obtained by a perturbation of \( \theta \), is measured via the mean squared error of \( M \) compared to \( \theta \). For a fixed data set \( S \), the \( L_2 \)-cost of \( M(S) \) is defined to be

\[
L_2(M(S)) := \mathbb{E}_{M|S} \| M(S) - \theta(S) \|_2^2.
\]

Borrowing terminology from the theory of estimation, for mechanisms \( M \) and \( \hat{M} \) (both perturbing \( \theta \), we say \( M \) dominates \( \hat{M} \) (in the \( \ell_2 \) sense) \( \hat{M} \) if for any \( S \in X^n \)

\[
L_2(M(S)) \leq L_2(\hat{M}(S))
\]

(with strict inequality for some \( S \)), and \( M \) strictly dominates \( \hat{M} \) if, for any \( S \in X^n \), \( L_2(M(S)) < L_2(\hat{M}(S)) \). Therefore, for any pre-specified privacy level \( \mu > 0 \), if both \( M \) and \( \hat{M} \) are \( \mu \)-GDP, and \( M \) dominates \( \hat{M} \), then \( M \) is said to have higher statistical utility than \( \hat{M} \). Note that one may alternatively view the data set \( S \) as a random sample, and use the unconditional \( L_2 \)-cost of \( M \),

\[
L_2(M) := \mathbb{E} \| M(S) - \theta(S) \|_2^2 = \mathbb{E}_S(L_2(M(S))).
\]

If \( M \) dominates \( \hat{M} \), then \( L_2(M) \leq L_2(\hat{M}) \), while the converse is generally not true. (If the distribution of \( S \) leads that the strict inequality in (10) holds with a positive probability, then \( L_2(M) < L_2(\hat{M}) \)). Therefore, it is sufficient to compare the conditional \( L_2 \)-costs (10) of mechanisms, for all possible data sets \( S \in X^n \).
2.1 Rank-deficient Gaussian mechanism

When the only information we have on a multivariate statistic \( \theta \) is the \( L_2 \)-sensitivity, the ordinary Gaussian mechanism

\[
M_\sigma(S) = \theta(S) + N_p(0, \Delta_2^2/\mu^2 I_p),
\]

calibrated to satisfy \( \mu \)-GDP (for any \( \theta \) with \( \Delta_2(\theta; X^n) = \Delta_2 \)), provides the largest statistical utility among a class of \( \mu \)-GDP additive Gaussian mechanisms, as explained below.

Let \( M_{\mu}^{\Delta_2} \), for \( \mu > 0 \) and \( \Delta_2 > 0 \), be the collection of all additive Gaussian mechanisms satisfying \( \mu \)-GDP for any statistic \( \theta \) of \( \Delta_2(\theta; X^n) \leq \Delta_2 \), that are of the form \( M_{\Sigma}(S) := \theta(S) + N_p(0, \Sigma) \), where \( \Sigma \) is a \( p \times p \) symmetric non-negative definite matrix. Note that the statistical utility, or the \( L_2 \)-cost, of \( M_{\Sigma} \) is \( \mathbb{E} \| M_{\Sigma}(S) - \theta(S) \|^2 = \text{trace}(\Sigma) \). Thus, the smaller \( \text{trace}(\Sigma) \), the larger statistical utility. However, in order to ensure that \( M_{\Sigma}(S) \) is \( \mu \)-GDP, \( \Sigma \) can not be too small, as the following lemma states.

**Lemma 1.** Let \( \mu > 0 \), \( \Delta_2 > 0 \) and \( \Sigma \) be a \( p \times p \) symmetric non-negative definite matrix. The additive Gaussian mechanism \( M_{\Sigma} \) is \( \mu \)-GDP for any \( \theta \) with \( \Delta_2(\theta; X^n) \leq \Delta_2 \) if and only if \( \lambda_{\min}(\Sigma) \geq \Delta_2^2/\mu^2 \), where \( \lambda_{\min}(\Sigma) \) is the smallest eigenvalue of \( \Sigma \).

A consequence of Lemma 1 is that each mechanism in the class \( M_{\mu}^{\Delta_2} \) corresponds to a covariance matrix \( \Sigma \) satisfying \( \lambda_{\min}(\Sigma) \geq \Delta_2^2/\mu^2 \). Particularly, \( M_G \in M_{\mu}^{\Delta_2} \). Moreover, for any mechanism \( M_{\Sigma} \in M_{\mu}^{\Delta_2} \), we have

\[
L_2(M_{\Sigma}) = \text{trace}(\Sigma) \geq p\lambda_{\min}(\Sigma) \geq p\Delta_2^2/\mu^2 = L_2(M_G(S))
\]

for any data set \( S \), and both equalities hold if and only if \( \Sigma = \Delta_2^2/\mu^2 I_p \). Thus, the ordinary Gaussian mechanism \( M_G \) strictly dominates any other mechanism in \( M_{\mu}^{\Delta_2} \).

We note that when considering only the class of Gaussian mechanisms with isotropic noises, a stronger statement can be made:

**Lemma 2.** Let \( \mu > 0 \), \( \Delta_2 > 0 \) and \( \Sigma = \sigma^2 I_p \). Let \( \theta : X^n \to \mathbb{R}^p \) be a multivariate statistic with \( \Delta_2(\theta; X^n) = \Delta_2 \). Then, \( M_{\Sigma} \) is \( \mu \)-GDP if and only if \( \sigma^2 \geq \Delta_2^2/\mu^2 \).

Nevertheless, if more information about the multivariate statistic \( \theta \) is known to us, one can improve upon the ordinary Gaussian mechanism by exploiting the additional information. We assume that, for a statistic \( \theta \), the set \( S_\theta = \{ \theta(S) - \theta(S') : S, S' \in X^n, S \sim S' \} \), which may be called the sensitivity space of \( \theta \) (Awan and Slavkovic [2021]), is known to us.

For a multivariate statistic \( \theta \) taking values in \( X^n \), we say \( S_\theta \) is rank-deficient if \( d_\theta := \dim(\text{span}(S_\theta)) < p \). If \( S_\theta \) is rank-deficient, then for any \( S \), when one record of \( S \) is replaced by any element in \( X^n \), the value of the statistic \( \Pi_{S_\theta} \theta(S) \), where \( \Pi_{S_\theta} \) is the orthogonal projection operator onto the orthogonal complement of \( \text{span}(S_\theta) \), does not vary. Thus, in view of privacy protection, there is no need to add a perturbation along the orthogonal complement of \( \text{span}(S_\theta) \), as \( \theta(S) \) and \( \theta(S') \) (for \( S \sim S' \)) are already indistinguishable along the subspace. This observation motivates us to consider a rank-deficient Gaussian mechanism, defined as follows.

Suppose \( \theta \) is given, and \( S_\theta \) is rank-deficient. Let \( P_{\theta} \) be the \( p \times p \) matrix of orthogonal projection whose range is \( \text{span}(S_\theta) \). For any orthogonal basis \( u_1, \ldots, u_{d_\theta} \) for the subspace \( \text{span}(S_\theta) \), \( P_{\theta} = \sum_{i=1}^{d_\theta} u_i u_i^T \). A multivariate additive Gaussian mechanism \( M_r \), given by

\[
M_r(S) := \theta(S) + N_p(0, \sigma^2 P_{\theta})
\]

for some \( \sigma > 0 \), is called a rank-deficient Gaussian mechanism.

**Theorem 3.** Let \( \mu > 0 \). For a multivariate statistic \( \theta \) with rank-deficient \( S_\theta \), the rank-deficient Gaussian mechanism \( M_r \) is \( \mu \)-GDP if and only if \( \sigma \geq \Delta_2(\theta; X^n)/\mu \).

In the following, \( M_r \) with \( \sigma = \Delta_2(\theta; X^n)/\mu \) is referred to as the \( \mu \)-GDP rank-deficient Gaussian mechanism. It is easily checked that for any \( \mu > 0 \), \( L_2(M_r(S)) = d_\theta \Delta_2^2(\theta)/\mu^2 \) (for any \( S \)) and \( M_r \) strictly dominates \( M_G \), while both mechanisms satisfy \( \mu \)-GDP.

The advantage of \( M_r \) over \( M_G \) is realized when \( S_\theta \) is rank-deficient. In the next example we exhibit that when the statistic \( \theta \) is a frequency table (or the vector of histogram counts, or a contingency table), \( S_\theta \) is indeed rank-deficient.
Example 1. Suppose that the sample space $\mathcal{X}$ is partitioned into $p$ parts (or categories), denoted by $C_1, \ldots, C_p$. For $S = (x_1, \ldots, x_n) \in \mathcal{X}^n$, let $\mathbf{\theta}(S)$ be the frequency table $\mathbf{\theta}(S) = (\theta_1(S), \ldots, \theta_p(S))^\top$, where $\theta_i(S) = \#\{j : x_j \in C_i\}$ is the count of records in $S$ belonging to the category $C_i$. Since the categories do not overlap, if one record in $S$ is replaced by any element in $\mathcal{X}$, resulting in a neighboring data set $S'$, then $\Delta(S) = \theta(S) - \theta(S') = e_i - e_j$, for some $i, j \in \{1, \ldots, p\}$, where $\{e_1, \ldots, e_p\}$ is the standard basis of $\mathbb{R}^p$. That is, for any $S \sim S'$, $\Delta(S)$ differs from $\Delta(S')$ at most two coordinates, and the sensitivity space of $\mathbf{\theta}$ is $\mathcal{S}_\theta = \{e_i - e_j : i, j = 1, \ldots, p\}$. Thus, for any $p$ and for any partition, $\Delta_r(\mathbf{\theta}) = 2^{1/r}$ for any $r > 0$; in particular,

$$\Delta_2(\mathbf{\theta}; X^n) = \sqrt{2}, \quad \Delta_1(\mathbf{\theta}) = 2.$$ Moreover, $\mathcal{S}_\theta$ is rank-deficient since span$(\mathcal{S}_\theta)$ is orthogonal to $1_p = (1, \ldots, 1)^\top \in \mathbb{R}^p$. Therefore, the rank-deficient Gaussian mechanism for frequency table $\mathbf{\theta}$,

$$M_r(S) = \mathbf{\theta}(S) + N_p(0, \sigma^2(1_p - 1_p^\top 1_p)),$$

where $\sigma = \Delta_2(\mathbf{\theta}; X^n)/\mu = \sqrt{2}/\mu$, is $\mu$-GDP (for any $\mu$) and strictly dominates the ordinary Gaussian mechanism.

2.2 James–Stein shrinkage mechanisms

The mechanism output $M_G(S)$ of an ordinary Gaussian mechanism can be viewed as the maximum likelihood estimator of $\mathbf{\theta}(S) \in \mathbb{R}^p$ (for each given $S$) from the model $(M_G(S)), \sim N(\mathbf{\theta}(S), \sigma^2)$ ($i = 1, \ldots, n$). It is well-known that, for $p \geq 3$, the celebrated James–Stein shrinkage estimator [James and Stein, 1961] dominates $M_G(S)$ under the squared error loss in estimation of $\mathbf{\theta}(S)$. In this section, we propose two types of mechanisms derived by applications of James–Stein shrinkage, confirm that these new mechanisms can be calibrated to satisfy $\mu$-GDP (for any $\mu > 0$), and investigate under which situations the James–Stein mechanisms have high statistical utilities.

The James–Stein shrinkage Gaussian mechanisms are defined by shrinking the output of ordinary Gaussian mechanism towards a common value. For notational convenience, for a given $\sigma > 0$, write the James–Stein shrinkage operator (shrinking all elements of a vector toward zero) by $m_\sigma(\cdot; \sigma) : \mathbb{R}^p \rightarrow \mathbb{R}^p$, which is defined by

$$m_\sigma(x; \sigma) = \left(1 - \frac{(p - 2)\sigma^2}{\|x\|^2_2}\right)x.$$

Similarly, write the operator shrinking to the average $\mathbf{x} = p^{-1}1_p^\top x$ by $m_a(\cdot; \sigma) : \mathbb{R}^p \rightarrow \mathbb{R}^p$,

$$m_a(x; \sigma) = \mathbf{x} - 1_p^\top x + \left(1 - \frac{(p - 3)\sigma^2}{\|x_e\|^2_2}\right)x_e,$$

where $x_e = x - \mathbf{x}1_p$.

Definition 2. Let $\mathbf{\theta} : \mathcal{X}^n \rightarrow \mathbb{R}^p$ be a multivariate statistic, and $\sigma > 0$ be given.

(i) The James–Stein Gaussian mechanism shrinking to zero is $M_{JS0} : \mathcal{X}^n \rightarrow \mathbb{R}^p$, defined by $M_{JS0}(S) = m_\sigma(M_G(S); \sigma)$, where $M_G(S) = \mathbf{\theta}(S) + N_p(0, \sigma^21_p)$.

(ii) The James–Stein Gaussian mechanism shrinking to average is $M_{JS} : \mathcal{X}^n \rightarrow \mathbb{R}^p$, defined by $M_{JS}(S) = m_a(M_G(S); \sigma)$.

Both $M_{JS0}(S)$ and $M_{JS}(S)$ depend on the data set $S$ only through the output $M_G(S)$ of the ordinary Gaussian mechanism. In the data privacy literature, such mechanism is said to be obtained via post-processing $M_G(S)$. If a randomized mechanism $M$ satisfies a privacy criterion (e.g., it is $\mu$-GDP for some $\mu > 0$), then any information obtained via a post-processing of (the output of) $M$ retains at least the same level of privacy protection guaranteed for $M$ [Dwork et al., 2014; Dong et al., 2022]; see Lemma 3.5 in Appendix A This leads that the James–Stein mechanisms are $\mu$-GDP for any $\mu \geq \Delta_2(\mathbf{\theta}; X^n)/\sigma$. Equivalently, for any $\mu > 0$, both $M_{JS0}(S)$ and $M_{JS}(S)$ with
We have demonstrated that the ordinary Gaussian mechanisms can be improved by utilizing various mechanisms, when basis matrices for span(\(\mathcal{S}_0\)) and the orthogonal complement of span(\(\mathcal{S}_0\)), respectively, that \([U_1 U_0]\) is a \(p \times p\) orthogonal matrix. The mechanism, perturbing \(\boldsymbol{\theta}\),

\[
M_{\tau,JS}(S) = U_1 U_1^\top \boldsymbol{\theta}(S) + U_0 m_\tau(U_0^\top M_\tau(S); \sigma),
\]

where \(M_\tau(S) = \boldsymbol{\theta}(S) + N_p(0, \sigma^2 U_0 U_0^\top)\) is the rank-deficient Gaussian mechanism defined in [12], and \(m_\tau(\cdot; \sigma)\) is the James–Stein shrinkage map [13], is called a rank-deficient James–Stein mechanism.

\[
\sigma \geq \Delta_2(\theta; X^n)/\mu \text{ satisfy } \mu\text{-GDP. We say that a James–Stein mechanism is calibrated to satisfy } \mu\text{-GDP if } \sigma = \Delta_2(\theta; X^n)/\mu.
\]

We remark that post-processed Gaussian mechanisms, including \(M_{JS,0}\), have been considered in the literature; see, e.g., [Balle and Wang 2018]. Nevertheless, to the best of our knowledge, our work is the first attempt of calibrating the amount of perturbation with respect to the GDP criterion, and of investigating \(M_{JS}\), the James–Stein Gaussian mechanism shrinking to average.

The conditional \(L_2\)-costs of \(M_{JS,0}\) and \(M_{JS}\) are given as follows.

**Proposition 4.** For a multivariate statistic \(\boldsymbol{\theta} \colon X^n \to \mathbb{R}^p\) with \(\Delta_2(\theta; X^n) = \Delta_2 > 0\), let \(M_{JS,0}\) and \(M_{JS}\) be the James–Stein Gaussian mechanisms with \(\sigma > 0\), as defined in Definition 3. For any data set \(S \in X^n\),

\[
L_2(M_{JS,0}(S)) = \sigma^2 p - \sigma^2(p - 2)^2 \left\{ \frac{1}{2} e^{-\frac{1}{2} \tau(S)} \sum_{\beta=0}^{\infty} \left( \frac{\tau(S)}{2} \right)^{\beta} \frac{1}{\beta! (\frac{1}{2} p + \beta - 1)} \right\},
\]

where \(\tau(S) = ||\theta(S)||_2^2/\sigma^2\), and

\[
L_2(M_{JS}(S)) = \sigma^2 p - \sigma^2(p - 3)^2 \left\{ \frac{1}{2} e^{-\frac{1}{2} \tau_{1,\perp}(S)} \sum_{\beta=0}^{\infty} \left( \frac{\tau_{1,\perp}(S)}{2} \right)^{\beta} \frac{1}{\beta! (\frac{1}{2} (p - 1) + \beta - 1)} \right\},
\]

where \(\tau_{1,\perp}(S) = ||(I_p - \frac{1}{p} 1_p 1_p^\top) \theta(S)||_2^2/\sigma^2\).

Proposition 3 allows us to directly compare the conditional \(L_2\)-costs of \(M_{JS,0}\) and \(M_{JS}\) with the \(L_2\)-cost of the ordinary Gaussian mechanism \(M_G\), for each \(S\).

**Theorem 5.** Let \(\mu > 0\). For a multivariate statistic \(\boldsymbol{\theta} \colon X^n \to \mathbb{R}^p\) with \(\Delta_2(\theta; X^n) = \Delta_2 > 0\), let \(M_G\) be the ordinary Gaussian mechanism, and \(M_{JS,0}\) and \(M_{JS}\) be the James–Stein Gaussian mechanisms, all calibrated to satisfy \(\mu\)-GDP (i.e., with \(\sigma = \Delta_2/\mu\)).

(i) If \(p \geq 3\), \(M_{JS,0}\) strictly dominates \(M_G\).

(ii) If \(p \geq 4\), \(M_{JS}\) strictly dominates \(M_G\).

Unlike the ordinary and rank-deficient Gaussian mechanisms, \(M_G\) and \(M_{r}\), the conditional \(L_2\)-costs of \(M_{JS}\) and \(M_{JS,0}\), given \(S\), depend on the value of \(\theta(S)\). As a consequence, there is in general no simple expression for \(L_2(M_{JS}) = \mathbb{E}_S(L_2(M_{JS}))\), which depends on the distribution of the statistic \(\theta(S)\). Nevertheless, under the conditions of Theorem 5, \(L_2(M_{JS}) < L_2(M_G)\) holds for any distribution of \(\theta(S)\). In Section 4, we numerically compare the unconditioned \(L_2\)-costs of various mechanisms, when \(\theta(S)\) is a random frequency table following a multinomial distribution.

### 2.3 Rank-deficient James–Stein Gaussian mechanism

We have demonstrated that the ordinary Gaussian mechanisms can be improved by either utilizing the structure of the sensitivity space \(\mathcal{S}_0\) of \(\theta\) or using a James–Stein shrinkage of mechanism outputs. In this subsection, we combine those two ideas and propose rank-deficient James–Stein Gaussian mechanisms, \(M_{r,JS}\). The mechanism \(M_{r,JS}\) is obtained by first perturbing the statistic \(\theta(S)\) only for the span of the sensitivity space, then applying a James–Stein shrinkage for the lower dimensional subspace.

**Definition 3.** Let \(\theta \colon X^n \to \mathbb{R}^p\) be a multivariate statistic, and let \(U_0\) and \(U_1\) be orthonormal basis matrices for span(\(\mathcal{S}_0\)) and the orthogonal complement of span(\(\mathcal{S}_0\)), respectively, so that \([U_1 U_0]\) is a \(p \times p\) orthogonal matrix. The mechanism, perturbing \(\theta\),

\[
M_{r,JS}(S) = U_1 U_1^\top \theta(S) + U_0 m_\tau(U_0^\top M_r(S); \sigma),
\]

where \(M_r(S) = \theta(S) + N_p(0, \sigma^2 U_0 U_0^\top)\) is the rank-deficient Gaussian mechanism defined in [12], and \(m_\tau(\cdot; \sigma)\) is the James–Stein shrinkage map [13], is called a rank-deficient James–Stein mechanism.
In the definition above, the mechanism $M_{r,JS}$ not only depends on $\sigma$ but also depends on the choice of orthonormal basis (the columns of $U_\theta$) for $\text{span}(S_\theta)$. As we shall see shortly, the level of privacy protection guaranteed by $M_{r,JS}$ is not affected by the choice of $U_\theta$, but the conditional $L_2$-cost of $M_{r,JS}(S)$ varies for different choices of $U_\theta$, even if $\theta(S)$ is fixed.

For any choice of $U_\theta$ that does not directly depend on $\theta(S)$ or $\sigma$, the conditional $L_2$-cost of $M_{r,JS}(S)$ depends on data set $S$ only through $M_r$. This can be seen by noting that $U_\theta^T U_\theta = 0$, which in turn leads that $U_\theta^T M_r(S) = U_\theta^T \theta(S)$ for any data set $S$. Since $M_{r,JS}(S)$ is obtained via post-processing $M_r$, if $M_r$ is $\mu$-GDP for some $\mu > 0$, so is $M_{r,JS}$. By Theorem 3, $M_{r,JS}$, with any choice of $U_\theta$, is $\mu$-GDP if $\sigma \geq \Delta_2(\theta;\mathcal{X}^n)/\mu$.

On the other hand, the conditional $L_2$-cost of $M_{r,JS}$ depends on $U_\theta$. In particular, for any given $S$, $L_2(M_{r,JS}(S))$ is exactly Equation (15) with $p$ replaced by $d_\theta = \dim(\text{span}(S_\theta))$ and $\tau_1,\perp(S)$ replaced by $\tilde{\tau}(S) = \|I_{d_\theta} - \frac{1}{p} 1_{d_\theta}1_{d_\theta}^T U_\theta^T \theta(S)\|^2/\sigma^2$. (See Proposition B.1 in the appendix for the explicit expression of $L_2(M_{r,JS}(S))$.) The next result is obtained by directly comparing $L_2(M_{r,JS}(S))$ with $L_2(M_r(S)) = d_\theta\sigma^2$, for all $S \in \mathcal{X}^n$.

**Theorem 6.** Let $\mu > 0$. Suppose $\theta : \mathcal{X}^n \to \mathbb{R}^p$ is a multivariate statistic with rank-deficient $S_\theta$, i.e. $d_\theta < p$, and $\Delta_2(\theta;\mathcal{X}^n) = \Delta_2 > 0$. Let $U_\theta$ (needed to define $M_{r,JS}$) consist of any orthonormal basis of $\text{span}(S_\theta)$. Suppose $M_G$, $M_r$, and $M_{r,JS}$ are calibrated to satisfy $\mu$-GDP (i.e., with $\sigma = \Delta_2/\mu$). Then, $M_r$ strictly dominates $M_G$. If $d_\theta \geq 4$, then $M_{r,JS}$ strictly dominates each of $M_r$ and $M_G$.

We remark that one can try to choose a particular $U_\theta$ that minimizes $L_2(M_{r,JS}(S))$, but doing so requires using the unperturbed information in $\|I_{d_\theta} - \frac{1}{p} 1_{d_\theta}1_{d_\theta}^T U_\theta^T \theta(S)\|^2/\sigma^2$. Such a mechanism depends on $S$ through not only $M_r(S)$ but also $\theta(S)$, and determining the level of its privacy protection seems a difficult task.

It is natural to ask whether any mechanism among the James–Stein shrinkage mechanisms $M_{JS0}$, $M_{JS}$ and $M_{r,JS}$ dominates another. The answer is no. The conditional $L_2$-costs of these mechanisms depend on $\|\theta(S)\|_2$, $\|I_p - \frac{1}{p} 1_p1_p^T \theta(S)\|_2$ or $\|I_{d_\theta} - \frac{1}{p} 1_{d_\theta}1_{d_\theta}^T U_\theta^T \theta(S)\|_2$ (as well as $d_\theta$). As a result, $L_2(M_{JS0}(S)) < L_2(M_{JS}(S))$ is true for some $S$, but is false for other choices of $S$. Likewise, although $L_2(M_{JS}(S)) > L_2(M_{r,JS}(S))$ for most data sets, it is not true for some $S$ (for some $\theta$ and $\mathcal{X}^n$). To compare these mechanisms we simplify the situation by considering an asymptotic dimension in which the sample size $n$ of data set $S$ increases, while the dimension $p$ of statistic $\theta$ and the privacy level $\mu$ are fixed.

In Theorem 7 below, we consider any sequence of data sets $S_1, S_2, \ldots, S_n$, of increasing sample sizes, which are considered deterministic. Note that the $L_2$-sensitivity of $\theta$ may depend on the sample size $n$. For instance, for $\theta(S) = x_n$ with $\mathcal{X} = [0, 1]^p$, $\Delta_2(\theta;\mathcal{X}^n) = \sqrt{p}/n$.

**Theorem 7.** Let $\mu > 0$, and let $S_1, \ldots, S_n, \ldots$ be any sequence of data sets of increasing sample sizes such that $S_n \in \mathcal{X}^n$ for each $n$. For each $n$, $\theta : \mathcal{X}^n \to \mathbb{R}^p$ is a multivariate statistic, and the randomized mechanisms $M_G$, $M_r$, $M_{JS0}$, $M_{JS}$ and $M_{r,JS}$ satisfy $\mu$-GDP; that is, $\sigma_n := \Delta_2(\theta;\mathcal{X}^n)/\mu$ is used for all mechanisms with sample size $n$. In the statements below, $U_\theta$ is any matrix chosen for both $M_r$ and $M_{r,JS}$.

(i) If $p \geq 3$ and $\|\theta(S_n)\|_2/\Delta_2(\theta;\mathcal{X}^n) \to \infty$ as $n \to \infty$, then

$$\mathbb{E} \left\{ \|M_{JS0}(S_n) - M_G(S_n)\|^2/\sigma_n^2 \right\} \to 0, \quad \text{as } n \to \infty.$$  

(ii) If $p \geq 4$ and $\|I_p - \frac{1}{n} 1_p1_p^T \theta(S)\|_2/\Delta_2(\theta;\mathcal{X}^n) \to \infty$ as $n \to \infty$, then

$$\mathbb{E} \left\{ \|M_{JS}(S_n) - M_G(S_n)\|^2/\sigma_n^2 \right\} \to 0, \quad \text{as } n \to \infty.$$  

(iii) If $d_\theta \geq 4$ and $\|I_{d_\theta} - \frac{1}{p} 1_{d_\theta}1_{d_\theta}^T U_\theta^T \theta(S)\|_2/\Delta_2(\theta;\mathcal{X}^n) \to \infty$ as $n \to \infty$, then

$$\mathbb{E} \left\{ \|M_{r,JS}(S_n) - M_r(S_n)\|^2/\sigma_n^2 \right\} \to 0, \quad \text{as } n \to \infty.$$  

In Theorem 7, we have assumed that for any $S$, $M_{JS0}(S)$ and $M_{JS}(S)$ are obtained by post-processing $M_G(S)$ (and $M_{r,JS}(S)$ by $M_r(S)$). The conditions such as $\|\theta(S)\|_2/\Delta_2(\theta;\mathcal{X}^n) \to \infty$ hold for most applications. For example, when $\theta(S) = x_n$ with $\mathcal{X} = [0, 1]^p$, $\|\theta(S)\|_2 \leq \sqrt{p}$ is
bounded but $\Delta_2(\theta; \mathcal{X}^n) = \sqrt{p}/n$ decreases, and the condition is satisfied. Since for fixed $\mu$, $\sigma_n \asymp \Delta_2(\theta; \mathcal{X}^n)$, Theorem 7(i) yields that $E\|M_{JS0}(S_n) - M_G(S_n)\|^2 = o(n^{-2})$. As an another example, let $\theta$ be the frequency table defined in Example 1. For such cases, $\Delta_2(\theta; \mathcal{X}^n) = \sqrt{2}$ is constant over varying $n$, but $\|\theta(S)\|_2 \geq \sqrt{\|\theta(S)\|_1} = \sqrt{n}$, thus the condition is satisfied. The difference between $M_{JS0}(S_n)$ and $M_G(S_n)$ gets smaller for larger $n$, when appropriately scaled.

From Theorem 7 we conclude that while each of $M_{JS0}$ and $M_{JS}$ has strictly smaller $L_2$-cost than the $L_2$-cost of $M_G$ for each $n$, the difference becomes smaller for large $n$. Moreover, we can compare $M_{JS}$ with either $M_{JS0}$ or $M_{JS}$ in the asymptotic setting, as follows.

**Corollary 8.** Under the conditions of Theorem 7 assume further that $S_0$ is rank-deficient, i.e., $d_0 < p$. Then, for any vector sequence $S_n$, and for any basis matrix $U_0$ chosen for $M_{JS}$,

$$\limsup_{n \to \infty} L_2(M_{JS}(S_n))/\sigma_n^2 < \liminf_{n \to \infty} L_2(M_{JS0}(S_n))/\sigma_n^2,$$

which also holds if $M_{JS}$ is replaced by $M_{JS0}$.

Figure 1 summarizes our discussion in this section. Overall, $M_{JS}$ shows the largest statistical utility (or the smallest $L_2$-cost) among the Gaussian mechanisms we have considered. We have also considered a rank-deficient James–Stein Gaussian mechanism, shrinking to zero (given by replacing $m_n$ with $m_0$ in (16)), but because its empirical $L_2$-cost is typically larger than that of $M_{JS}$, we have chosen to only discuss $M_{JS}$. Other forms of post-processing can be utilized to further reduce the mechanisms’ $L_2$-cost. See Section 5.1 for an example.

### 3 Calibration of multivariate Laplace mechanisms for $\mu$-GDP

Laplace mechanisms are additive mechanisms perturbing a statistic $\theta$ with a Laplace-distributed noise, and have been commonly used as a general-purpose mechanism satisfying $\varepsilon$-DP (Dwork et al. 2014). Let $\text{Lap}(\delta, b)$ stand for the Laplace distribution with location parameter $\delta \in \mathbb{R}$ and scale parameter $b > 0$. For a random vector $X = (X_1, \ldots, X_p)$, we write $X \sim \text{Lap}(\delta, b)$, where $\delta = (\delta_1, \ldots, \delta_p)^\top \in \mathbb{R}^p$, if $X_i$ follows $\text{Lap}(\delta_i, b)$ independently for $i = 1, \ldots, p$. For a multivariate statistic $\theta$, the additive mechanism that adds a $\text{Lap}(\delta, 0)$-distributed noise,

$$M_{\text{Lap}}(S; b) = \theta(S) + \text{Lap}(\theta(S)), \quad (17)$$

is called multivariate Laplace mechanism. It is well-known that a multivariate Laplace mechanism $M_{\text{Lap}}(\cdot; b)$ with $b \geq \Delta_1/\varepsilon$ satisfies $\varepsilon$-DP (Dwork et al. 2006a), where $\Delta_1 = \Delta_1(\theta; \mathcal{X}^n)$ is the $L_1$-sensitivity of $\theta$ (see (5)).

In this section, we calibrate the amount of noise in multivariate Laplace mechanisms with respect to $\mu$-GDP, for a fair comparison with Gaussian mechanisms. We show that, in contrast to the case of Gaussian mechanisms, the optimally-calibrated scale parameter $b$ for univariate Laplace mechanisms, with respect to $\mu$-GDP criterion, turns out to be sub-optimal when used for some multivariate Laplace mechanisms. An optimal calibration of the amount of Laplace noise is achieved for the special case that $\theta$ is a multivariate frequency table.

Figure 1: Notation $M \rightarrow M'$ is used when the statistical utility of $M'$ is greater than that of $M$ (under appropriate conditions) for finite sample sizes. The dotted arrow is used when the comparison is made for large sample sizes, and the dashed arrow is used when the comparison was made empirically; see Section 5.
3.1 Universal conversion and improved Laplace mechanisms

A naive approach to determining the level of privacy protection with respect to GDP criterion in a Laplace mechanism $M_{\text{Lap}}(\cdot; b)$ is to use the fact that $M_{\text{Lap}}(\cdot; b)$ is $\varepsilon$-DP for any $\varepsilon \geq \Delta_1/b$, and then to determine $\mu(\varepsilon)$ such that any $\varepsilon$-DP mechanism satisfies $\mu(\varepsilon)$-GDP. Such a conversion from $\varepsilon$-DP to $\mu$-GDP can be obtained by comparing the trade-off function $T_{\varepsilon\text{-DP}}$ of $\varepsilon$-DP, where

$$T_{\varepsilon\text{-DP}}(\alpha) = \begin{cases} 1 - e^\varepsilon \alpha & \text{if } 0 \leq \alpha < \frac{1}{1+e^\varepsilon}, \\ e^{-\varepsilon}(1-\alpha) & \text{otherwise}, \end{cases}$$

with the trade-off function $G_\mu$ (Equation (4)) corresponding to $\mu$-GDP.

**Lemma 9** (Universal conversion). (i) Let $M$ be a mechanism satisfying $\varepsilon$-DP, for $\varepsilon > 0$. Then $M$ is $\mu$-GDP for any $\mu \geq 2\Phi^{-1}\left\{ e^\varepsilon/(e^\varepsilon+1) \right\}$, where $\Phi$ is the standard normal distribution function.

(ii) Let $\mu > 0$ be given. For any $\varepsilon \leq \varepsilon_\mu := \log\{\Phi(\mu/2)/\Phi(-\mu/2)\}$, a mechanism satisfying $\varepsilon$-DP is $\mu$-GDP.

The universal conversion in Lemma 9 can be used in determining the level $\mu$ of GDP criterion for any mechanism that is known to be $\varepsilon$-DP for some $\varepsilon > 0$. In particular, a Laplace mechanism $M_{\text{Lap}}(\cdot; b)$, satisfying $(\Delta_1/b)$-DP, is $\mu$-GDP for any $\mu \geq 2\Phi^{-1}\left\{ e^{\Delta_1/b}/(e^{\Delta_1/b}+1) \right\}$. Conversely, if a desired level $\mu > 0$ is prespecified, then choosing the scale parameter $b$ of $M_{\text{Lap}}(\cdot; b)$ to be

$$b_\mu^\varepsilon := \Delta_1/\varepsilon \mu = \Delta_1/\log\{\Phi(\mu/2)/\Phi(-\mu/2)\},$$

guarantees that $M_{\text{Lap}}(\cdot; b)$ is $\mu$-GDP, since

$$\inf_{S \sim S'} T(M_{\text{Lap}}(S; b_\mu^\varepsilon), M_{\text{Lap}}(S'; b_\mu^\varepsilon)) \geq T_{\varepsilon\text{-DP}} \geq G_\mu,$$  \hspace{1cm} (19)

in which the first inequality is given by the fact that $M_{\text{Lap}}(\cdot; b)$ is $(\Delta_1/b)$-DP, and the second inequality is from Lemma 9(ii).

Such a two-step calibration of $b$ (by $b_\mu^\varepsilon$) for Laplace mechanisms is by no means optimal. As we shall see shortly, one can choose the scale parameter $b$ strictly smaller than $b_\mu^\varepsilon$, while still satisfying $\mu$-GDP. Intuitively, this is because the equalities in (19) are not simultaneously attained. To visually confirm this fact, the three trade-off functions in (19) are plotted in Figure 2 for the univariate case on the left panel and for a multivariate case on the right panel. Let

$$\mathcal{L}_p(b) := \mathcal{L}_p(b; \theta, \mathcal{X}^\theta) = \inf_{S \sim S'} T(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b))$$

(20)
denote the trade-off function representing the worst-case Laplace trade-offs, where $p$ is the dimension of the statistic $\theta(S) \in \mathbb{R}^p$. It can be observed in Figure 2 that there exists a unique $\alpha_0 \in (0, 1)$ such that $T_{\varepsilon,-\text{DP}}(\alpha_0) = G_\mu(\alpha_0)$, but $L_p(b_\mu^n)(\alpha_0) > T_{\varepsilon,-\text{DP}}(\alpha_0)$ (for both univariate and multivariate cases).

In the two-step calibration above, we have used the $L_1$-sensitivity $\Delta_1(\theta; X^n)$ of $\theta$ only for calibration with respect to the $\varepsilon$-DP criterion. Naturally, an improvement over the two-step calibration can be obtained by directly using the $L_1$-sensitivity with respect to GDP criterion. We discuss the univariate case (i.e., the case where $p = 1$) first, and then move on to the multivariate case.

### 3.1.1 Calibration of univariate Laplace mechanisms

Let $p = 1$. For this univariate case, we write $\theta$ and $M_{\text{Lap}}(\cdot; b)$ for $\theta$ and $M_{\text{Lap}}(\cdot; b)$. In calibration of the scale parameter $b$ of $M_{\text{Lap}}(\cdot; b)$ to satisfy $\mu$-GDP (for a given $\mu > 0$), we find the smallest $b$ satisfying

$$L_1(b) \geq G_\mu,$$

where the trade-off function $L_1(b)$ is defined in (20). The expression of the trade-off function $L_1(b)$ is useful for such purpose.

**Lemma 10.** For any $b > 0$ and $\Delta_1 = \Delta_1(\theta; X^n) = \sup_{S \sim S'} |\theta(S) - \theta(S')|$, the value of the trade-off function $L_1(b) : [0, 1] \to [0, 1]$ at $\alpha \in [0, 1]$ is, for $\delta = \Delta_1/b$,

$$L_1(b)(\alpha) = \begin{cases} 1 - e^\delta \alpha, & \text{if } \alpha < \frac{1}{2} e^{-\delta}; \\ \frac{\alpha}{\alpha_0}, & \text{if } \frac{1}{2} e^{-\delta} \leq \alpha < \frac{1}{2}; \\ e^{-\delta}(1 - \alpha), & \text{otherwise}. \end{cases}$$

Using the exact expressions of $L_1(b)$ and $G_\mu$ given in (21) and (6) respectively, one can directly compare $L_1(b)(\alpha)$ with $G_\mu(\alpha)$ at $\alpha \in (0, 1)$. Such comparison leads to the following result on the optimal calibration of univariate Laplace mechanism for $\mu$-GDP. For $\mu > 0$ and $\Delta_1 > 0$, define $b_\mu^{\Delta_1} := \Delta_1/[2 \log\{2\Phi(-\frac{\mu}{2})\}]$.

**Proposition 11.** Let $\theta : X^n \to \mathbb{R}$ be any univariate statistic with $\Delta_1(\theta; X^n) = \Delta_1$, and $\Delta_1 \geq 0$.

(i) For any $\mu > 0$, the Laplace mechanism with scale parameter $b$, $M_{\text{Lap}}(\cdot; b)$, is $\mu$-GDP if and only if $b \geq b_\mu^{\Delta_1}$. Moreover, $b_\mu^{\Delta_1} < b_\mu^{\Delta_1}$.

(ii) Conversely, for any $b > 0$, $M_{\text{Lap}}(\cdot; b)$ is $\mu$-GDP if and only if $\mu \geq -2\Phi^{-1}\{\frac{1}{2} \exp\{\frac{-\alpha_0^2}{2}\}\}$.

Proposition 11 tells us that $b_\mu^{\Delta_1} = \inf\{b > 0 : L_1(b) \geq G_\mu\}$, and as a result, we may say that a univariate Laplace mechanism with scale parameter $b_\mu^{\Delta_1}$ is optimally calibrated to satisfy $\mu$-GDP. As visualized in Figure 2(a), the graph of $L_1(b_\mu^{\Delta_1})$ sits just above the graph of $G_\mu$; any $b < b_\mu^{\Delta_1}$ results in $L_1(b)(\alpha) < G_\mu(\alpha)$ for some $\alpha \in (0, 1)$.

Recall that in Lemma 2 we have established a result on an optimal calibration for a class of multivariate Gaussian mechanisms. Since Proposition 11 above states an optimality result for univariate Laplace mechanisms similar to the conclusion of Lemma 2, one may conjecture that the above result generalizes to the case of multivariate Laplace mechanisms. This conjecture is partly true, as we discuss in the next subsection.

### 3.1.2 Calibration of multivariate Laplace mechanisms

A simple-minded approach of calibrating multivariate Laplace mechanism, $M_{\text{Lap}}(\cdot; b)$, for $p \geq 2$ is to directly compare the exact expression for the trade-off function $L_p(b; \theta, X^n)$ with $G_\mu$, as done for the $p = 1$ case in Section 3.1.1. Unfortunately, the exact expression for the trade-off function $L_p(b; \theta, X^n)$ is extremely dependent on the shape of the sensitivity space $S_{\theta}$, and turns out to be quite messy even for $p = 2$. Evaluating $L_p(b; \theta, X^n) = \inf_{S \sim S'} \text{T}(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b))$ requires
an evaluation of the trade-off function between two multivariate Laplace distributions, since for any $S, S' \in \mathcal{X}^n$, $b > 0$,

$$T(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b)) = T(\text{Lap}_p(\theta(S), b), \text{Lap}_p(\theta(S'), b))$$

$$= T(\text{Lap}_p(0, 1), \text{Lap}_p(\delta, 1)), \quad (22)$$

where $\delta = \frac{1}{2}(\theta(S) - \theta(S'))$, due to the invariance of trade-off functions under simultaneous affine transformations (see Lemma A.1). A key observation that can be used for further simplifying (22) is the following.

**Lemma 12.** Let $p \geq 1$. For any $\delta = (\delta_1, \ldots, \delta_p) \in \mathbb{R}^p$, we have

$$T(\text{Lap}_p(0, 1), \text{Lap}_p(\delta, 1)) \geq T(\text{Lap}(0, 1), \text{Lap}(\|\delta\|_1, 1)). \quad (23)$$

(i) If the number of nonzero elements in $\delta$ is at most one, then the equality in (23) holds for all $\alpha \in (0, 1)$.

(ii) If at least two elements in $\delta$ are nonzero, then strict inequality in (23) holds for some $\alpha \in (0, 1)$. That is, there exists an interval $(a, b)$, $0 < a < b < 1$, such that for any $\alpha \in (a, b)$, $T(\text{Lap}_p(0, 1), \text{Lap}_p(\delta, 1))(\alpha) > T(\text{Lap}(0, 1), \text{Lap}(\|\delta\|_1, 1))(\alpha)$. Moreover, $(a, b)$ contains $\alpha_0 = \frac{1}{2}e^{-s\|\delta\|_2/2}$ which satisfies that $T(\text{Lap}(0, 1), \text{Lap}(\|\delta\|_1, 1))(\alpha_0) = \alpha_0$.

**Remark 1.** The trade-off function between multivariate Gaussian distributions can be represented exactly by a corresponding trade-off function between univariate Gaussian distributions: For any $p \geq 1$, and for any $\delta \in \mathbb{R}^p$, $T(N_p(0, 1), N_p(\delta, 1)) = T(N(0, 1), N(\|\delta\|_2, 1))$ (see Lemma A.2). In contrast, the trade-off function between multivariate Laplace distribution can only be lower-bounded by a trade-off function between univariate Laplace distributions, as stated in Lemma A.1.

As a result of Lemma 12 and using (22), the trade-off function $\mathcal{L}_p(b; \theta, \mathcal{X}^n)$ of a multivariate Laplace mechanism can be lower-bounded by a trade-off function between *univariate* Laplace distributions, as shown in the equations below:

$$\mathcal{L}_p(b; \theta, \mathcal{X}^n) = \inf_{S \sim S'} T(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b))$$

$\geq \inf_{S \sim S'} T(\text{Lap}(0, 1), \text{Lap}(\|\theta(S) - \theta(S')\|_1/b, 1))$

$= T(\text{Lap}(0, 1), \text{Lap}(\sup_{S \sim S'} \|\theta(S) - \theta(S')\|_1/b, 1))$

$= T(\text{Lap}(0, 1), \text{Lap}(\Delta_1(\theta, \mathcal{X}^n)/b, 1)).$

The above observation allows us to generalize the optimal calibration result on univariate Laplace mechanisms in Proposition 11 to multivariate cases. Recall that for $\mu > 0$ and $\Delta_1 > 0$, $b_{\mu}^{\Delta_1} = \Delta_1/[-2\log(2\Phi(-\frac{\Delta_1}{\mu}))].$

**Theorem 13.** Let $p \geq 1$, and $\Delta_1 > 0$.

(i) For any $\mu > 0$, the multivariate Laplace mechanism with scale parameter $b$, $M_{\text{Lap}}(\cdot; b)$, is $\mu$-GDP for any $\theta$ with $\Delta_1(\theta, \mathcal{X}^n) \leq \Delta_1$ if and only if $b \geq b_{\mu}^{\Delta_1}$.

(ii) Conversely, for any $b > 0$, $M_{\text{Lap}}(\cdot; b)$ is $\mu$-GDP for any $\theta$ with $\Delta_1(\theta, \mathcal{X}^n) \leq \Delta_1$ if and only if $\mu \geq -2\Phi^{-1} \left( \frac{\Delta_1}{b} \right)$.

(iii) Suppose $p \geq 2$. Then for any given $\theta$ with $\Delta_1(\theta, \mathcal{X}^n) \leq \Delta_1$, $M_{\text{Lap}}(\cdot; b)$, is $\mu$-GDP if $b \geq b_{\mu}^{\Delta_1}$.

However, there exists $\theta$ such that $\Delta_1(\theta, \mathcal{X}^n) \leq \Delta_1$ and $M_{\text{Lap}}(\cdot; b)$ is $\mu$-GDP for some $b < b_{\mu}^{\Delta_1}$.

In Theorem 13 above, parts (i) and (ii) provide an optimal calibration of Laplace mechanism (with respect to GDP criterion) when the only information we have on the multivariate statistic $\theta$ is the $L_1$-sensitivity. Part (iii), when compared to Proposition 11, reveals a subtle difference between the calibrations of univariate and multivariate Laplace mechanisms. Simply put, the Laplace mechanism $M_{\text{Lap}}(\cdot; b_{\mu}^{\Delta_1})$ is optimal in the univariate case, but is sub-optimal for some multivariate statistics $\theta$. This conclusion can be visually verified in Figure 2(b), drawn for the case where the
multivariate statistic $\theta$ is a frequency table: The trade-off function $L_p(b^n_{\mu})$ is strictly larger than $G_{\mu}$, suggesting that calibrating $b$ smaller than $b^n_{\mu}$ is possible.

Whether the multivariate Laplace mechanism $M_{\text{Lap}}(\cdot; b^n_{\mu})$ is optimal or not depends on the statistic $\theta$, and it is natural to investigate the sensitivity space $S_\theta$ for further improvement. In the next subsection, we take a full advantage of the sensitivity space in calibrating the Laplace mechanisms for the case where $\theta$ is a frequency table.

### 3.2 Laplace mechanisms for frequency tables

In this subsection, we consider the case where the multivariate statistic $\theta$ is a frequency table. As shown in Example 1, the sensitivity space of $\theta$ is

$$S_\theta = \{ \theta(S) - \theta(S') : S, S' \in X^n, S \sim S' \} = \{ e_i - e_j : i, j = 1, \ldots, p \}.$$  

Since any element in $S_\theta$ involves only two coordinates of $\mathbb{R}^p$, for any $p$, the trade-off function $L_p(b; \theta, X^n)$ of a multivariate Laplace mechanism perturbing the frequency table $\theta(S)$ with Laplace scale parameter $b$ is exactly a trade-off function between two-dimensional Laplace distributions. In particular, if $\theta$ is a frequency table, then for any $b > 0$,

$$L_p(b; \theta, X^n) = \inf_{S \sim S'} T(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b)) = \inf_{S \sim S'} T(Lap_p(0, b), Lap_p(\theta(S) - \theta(S'), b)) = T(Lap_p(0, b), Lap_p(e_1 - e_2, b)) = T(Lap(0, b), Lap(1, b)),$$

since taking $\theta(S) - \theta(S') = e_1 - e_2 = (1, -1, 0, \ldots, 0)^T \in S_\theta$ achieves the minimum of (24). To distinguish the general trade-off function $L_p(b; \theta, X^n)$ (used for any $\theta$) from the special case of frequency tables, write $L_{\text{freq}}(b) = L_p(b; \theta_0, X^n) = T(Lap(0, b), Lap(1, b))$ when $\theta_0$ is a frequency table.

An explicit expression of $L_{\text{freq}}(b)$ can be obtained by the Neyman–Pearson lemma: For $0 < \alpha \leq \frac{1}{4}e^{-\frac{x}{2}}(2 + \frac{1}{b})$,

$$L_{\text{freq}}(b)(\alpha) = \begin{cases} -e^{-\frac{x}{2}}\alpha + 1 & \text{if } 0 \leq \alpha < \frac{1}{4}e^{-\frac{x}{2}}, \\ \frac{1}{4}e^{-C_b(\alpha)}(3 + C_b(\alpha)) & \text{if } \frac{1}{4}e^{-\frac{x}{2}} \leq \alpha < \frac{1}{4}e^{-\frac{1}{2}}(1 + \frac{1}{b}), \\ \alpha + \frac{1}{4}e^{-\frac{x}{2}}(2 + \frac{1}{b}) & \text{if } \frac{1}{4}e^{-\frac{1}{2}}(1 + \frac{1}{b}) \leq \alpha \leq \frac{1}{4}e^{-\frac{x}{2}}(2 + \frac{1}{b}). \end{cases}$$

and $L_{\text{freq}}(b)(\alpha)$ for $\alpha \geq \frac{1}{4}e^{-\frac{x}{2}}(2 + \frac{1}{b})$ is given by the symmetry about the line $x = y$. In (25), $C_b(\alpha) = W(4\alpha e^{1+\frac{x}{2}}) - 1$, where $W$ is the Lambert $W$ function restricted to $[0, \infty)$, so that $W$ is the inverse of the function $w \mapsto we^w$ (Section 4.13, Olver et al. 2010). An expression for the trade-off function between more general two-dimensional Laplace distributions, $T(Lap(\delta_1, b), Lap(\delta_2, b))$, for any $\delta_1, \delta_2 \in \mathbb{R}^2$, can be found in Appendix C.1.

Using the expression (25), one can directly compare $L_{\text{freq}}(b)(\alpha)$ with $G_{\mu}(\alpha)$ at $\alpha \in (0, 1)$. For $\mu > 0$, let

$$\tilde{b}_\mu = \inf \{ b > 0 \mid L_{\text{freq}}(b) \geq G_{\mu} \}. \quad (26)$$

Choosing the scale parameter $b$ of multivariate Laplace mechanisms to be $b = \tilde{b}_\mu$ is optimal when $\theta$ is a frequency table, in the sense of the following theorem.

**Theorem 14.** Let $p \geq 2$, and suppose that the multivariate statistic $\theta : X^n \to \mathbb{R}^p$ is a frequency table, defined in Example 1. The multivariate Laplace mechanisms $M_{\text{Lap}}(\cdot; b)$ is $\mu$-GDP if and only if $b \geq \tilde{b}_\mu$.

The optimality of $M_{\text{Lap}}(\cdot; \tilde{b}_\mu)$ for frequency tables can be visually confirmed in Figure 2, in which the trade-off function $L_{\text{freq}}(\tilde{b}_\mu) = L(\tilde{b}_\mu)$ is directly above $G_{\mu}$.

The optimal scale parameter $\tilde{b}_\mu$ in (26) has no closed-form expression, and is only evaluated numerically. We propose a bisection algorithm of numerically approximating $\tilde{b}_\mu$ for given $\mu > 0$; see
Algorithm 1: Bisection algorithm for finding \( \tilde{b}_\mu \).

**Result:** Return numerically approximated \( \tilde{b}_\mu \).

1. Initialize \( b^L = b_\mu^L \) and \( b^U = 0 \)
2. while until the stopping criterion is met do
   3. \( b \leftarrow (b^L + b^U)/2 \)
   4. \( l \leftarrow \min_{a \in I}(L_{freq}(b) - G_\mu(\alpha)) \) where \( I = \left[ \frac{1}{4}e^{-\frac{\alpha}{2}}, \frac{1}{2}e^{-\frac{\alpha}{2}}(1 + \frac{1}{2}) \right] \)
   5. if \( |l| < \varepsilon_{\text{tol}} \) then
      6. Stopping criterion is met
      7. return \( b \)
   8. else if \( l > 0 \) then
      9. \( b^U \leftarrow b \)
   10. else if \( l < 0 \) then
      11. \( b^L \leftarrow b \)
   12. end
3. end

Algorithm 1. A key observation in designing such an algorithm is that \( \tilde{b}_\mu \) is the unique root of the equation \( g_\mu(b) = 0 \), where \( g_\mu(b) = \min_{a \in I}(L_{freq}(b) - G_\mu(\alpha)) = 0 \), \( b = [\frac{1}{4}e^{-\frac{\alpha}{2}}, \frac{1}{2}e^{-\frac{\alpha}{2}}(1 + \frac{1}{2})] \). This is valid since trade-off functions are symmetric about the line \( x = y \) and the function \( L_{freq}(b) \) is linear on the complement of \( I_b \).

### 4 Comparison between Gaussian and Laplace mechanisms

In this section, we compare the statistical utilities of \( \mu \)-GDP Gaussian and Laplace mechanisms, both perturbing a multivariate statistic \( \theta \). For a fair comparison, we use the \( L_r \)-cost for all \( r \geq 1 \), as opposed to just using the \( L_2 \)-cost, as done for comparison among Gaussian mechanisms.

We first compare the ordinary Gaussian mechanism \( M_G(\cdot, b_\mu^{\alpha}) \) and the multivariate Laplace mechanism \( M_{Lap}(\cdot, b_\mu^{\alpha}) \), since for any \( \mu > 0 \) and for any statistic \( \theta \), both mechanisms are \( \mu \)-GDP (see Lemma 2 and Theorem 3). Write \( M_{Lap} \) for \( M_{Lap}(\cdot, b_\mu^{\alpha}) \) for notational simplicity.

Since the conditional \( L_r \)-costs of \( M_G(S) \) and \( M_{Lap}(S) \) do not depend on the data set \( S \), we can say that \( M_G \) strictly dominates \( M_{Lap} \) in the \( \ell_r \) sense if \( L_r(M_G) > L_r(M_{Lap}) \). To investigate under which conditions the Gaussian mechanism strictly dominates the Laplace mechanism, the relative efficiency

\[
RE_r(M_G, M_{Lap}) := \frac{L_r(M_{Lap})}{L_r(M_G)} = \left( \frac{\Delta_1}{\Delta_2} \right)^r 2^r \Gamma \left( \frac{r}{2} + 1 \right) \left( \frac{\mu}{-2 \log(2\Phi(-\frac{\alpha}{2}))} \right)^r, \tag{27}
\]

where \( \Delta_r = \Delta_r(\theta; \mathcal{X}^n) \) for \( r = 1, 2 \), can be used. In particular, the Gaussian mechanism dominates the Laplace mechanism if \( RE_r(M_G, M_{Lap}) > 1 \). Observe from (27) that the relative efficiency depends on three parameters: privacy parameter \( \mu > 0 \), the ratio of sensitivities \( \Delta_1/\Delta_2 \geq 1 \), and \( r \geq 1 \). The dimension \( p \) affects the relative efficiency only through the ratio \( \Delta_1/\Delta_2 \). For each given \( r \), \( RE_r(M_G, M_{Lap}) \) increases (i.e., the Gaussian mechanism becomes more efficient than the Laplace mechanism) as \( \Delta_1/\Delta_2 \) increases or \( \mu \) decreases. (These claims are based on Lemma D.1 in Appendix D, which collects some facts about \( RE_r(M_G, M_{Lap}) \).

Figure 3 plots the region (of \( \mu, \Delta_1/\Delta_2, r \)) under which the Gaussian mechanism dominates the Laplace mechanism. We point out that for high privacy situations with smaller privacy parameter \( \mu \), the Gaussian mechanism dominates the Laplace mechanism. In particular, if \( \mu < 2.55 \) (roughly), \( RE_r(M_G, M_{Lap}) > 1 \) for any \( r \geq 1 \) and \( \Delta_1/\Delta_2 \geq 1 \). Note that the ratio \( \Delta_1/\Delta_2 \) is typically greater than 1; if \( \theta \) is a frequency table, \( \Delta_1/\Delta_2 = \sqrt{2} \), and if \( \theta \) is a multivariate mean, \( \Delta_1/\Delta_2 = \sqrt{p} \) (for \( \mathcal{X} = [0, 1]^p \)). For such typical cases, the Gaussian mechanism dominates the Laplace mechanism for a wide range of \( \mu \), and the Laplace mechanism is useful only under very low privacy situations, as shown in Figure 3(b).
can be calibrated to satisfy the randomized multivariate mechanisms developed in Sections 2 and 3 are used to release randomly perturbed contingency tables, satisfying the privacy protection level is very low (i.e., µ < 0), for high privacy situations (corresponding to µ < 3.9, approximately). We note that rank-deficient James–Stein mechanism MJS typically has a much smaller $L_2$-cost than $L_2(M_G)$. Thus, unless the privacy protection level is very low (i.e., µ is large), Gaussian mechanisms have advantages over Laplace mechanisms, when all mechanisms satisfy the µ-GDP criterion.

5 Applications to contingency table analysis

A contingency table, or a multi-way frequency table, is a fundamental data summary widely used in various fields, such as official statistics, social sciences, and genome-wide association studies. Analysis of contingency tables routinely involves hypothesis tests based on the $\chi^2$ statistics such as the goodness-of-fit (GOF) and homogeneity tests.

In this section, we demonstrate the applications of randomized mechanisms discussed in Sections 2 and 3 for private release of contingency tables, and numerically compare the statistical utilities. We also propose procedures for private GOF and homogeneity tests, that can be conducted when only the differentially private (i.e., perturbed) contingency tables are available. For this application of hypothesis tests, the power of the test serves as another measure of statistical utility.

Since a contingency table is simply the frequency table of Example 1, arranged in the form of cross-tabulation, we let $\theta : \mathcal{X}^n \rightarrow \mathbb{R}^p$ be the $r \times c$ contingency table, where $p = r \times c$ is the number of cells.

5.1 Private contingency table release

The randomized multivariate mechanisms developed in Sections 2 and 3 are used to release randomly perturbed contingency tables, satisfying the µ-GDP criterion.

The ordinary Gaussian mechanism $M_G$ and the two James–Stein mechanisms $M_{JS0}$ and $M_{JS}$ can be calibrated to satisfy µ-GDP, by choosing $\sigma = \Delta_2(\theta; \mathcal{X}^n)/\mu = \sqrt{2}/\mu$. The rank-deficient mechanisms $M_r$ and $M_{JS}$ are beneficial since the sensitivity space of contingency tables is rank-deficient, with $d_\theta = p - 1$, and they are µ-GDP if $\sigma = \sqrt{2}/\mu$. Since the output of $M_{JS}$ depends on the specific choice of the basis matrix $U_\theta$ (orthogonal to $1_\mu$), we choose to set $U_\theta$ to be the $p \times (p-1)$

![Figure 3: The partition of the set of parameters ($\mu_1, \Delta_1/\Delta_2, \mu_2$).](image)

(a) $\Delta_1/\Delta_2 = 1$.

(b) $\mu_2 = 2$.

Figure 3: The partition of the set of parameters ($\mu, \Delta_1/\Delta_2, \mu_2$), depending on whether the Gaussian mechanism dominates the Laplace mechanism or not.
The relative efficiency $\text{RE}_2(M_G, M_{\text{Lap}}(\cdot; b))$ (for three choices of $b$) as a function of $\mu$. The Gaussian mechanism $M_G$ dominates $M_{\text{Lap}}(\cdot; b)$ if the relative efficiency is greater than 1.

Helmert sub-matrix (Harville, 1998). The Helmert matrix of order $p$ is $U = [u_1, U_\theta]$, whose first column is $u_1 = 1_p/\sqrt{p}$, and the $k$th column (for $k = 2, \ldots, p$) is $u_k = [k(k-1)]^{-1/2}(1, 1, \ldots, 1, 1-k, 0, 0, \ldots, 0)$. For example, for $p = 4$, the basis matrix is

$$U_\theta = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{12} \\ -1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{12} \\ 0 & -2/\sqrt{6} & 1/\sqrt{12} \\ 0 & 0 & -3/\sqrt{12} \end{pmatrix}.$$

The multivariate Laplace mechanism with the optimal calibration $M_{\text{Lap}}(\cdot; \tilde{b}_\mu)$ can also be used to release $\mu$-GDP contingency tables (see Section 3.2).

When the amount of perturbation in each of these mechanisms is large (or equivalently $\mu$ is small), it is possible that the output of the mechanism $M(S) = \theta(S) + \xi$ contains negative values. Since it is desirable to have non-negative frequency counts, one can post-process each of mechanism outputs to have non-negative values. For any mechanism $M$, we define the truncated mechanism, obtained by truncating the output of $M(S)$ at zero, to be

$$(M^c(S))_j = \max\{0, (M(S))_j\}, j = 1, \ldots, p.$$  \hspace{1cm} (28)

By the post-processing property (Lemma A.5), if $M$ is $\mu$-GDP, so is $M^c$. We write $M^c_{JS}$ for the truncated mechanism stemming from $M_{JS}$, and use a similar notation for other mechanisms. If $\theta(S)_j \geq 0$ for any $j$ (which is the case for $\theta$ being contingency tables), $M^c$ dominates $M$.

5.2 Numerical comparison of $L_2$ costs

In this section, we numerically compare the $L_2$-costs of the mechanisms discussed in Section 5.1.

For this, we assume that the unperturbed contingency table $\theta(S) \sim \text{Multinomial}_p(n, \pi)$ is sampled from a multinomial distribution. Each $\theta(S)$ is then "sanitized" by the application of the randomized mechanisms discussed in the previous section.

We consider two models for the true probabilities $\pi = (\pi_1, \ldots, \pi_p)$. In Model I, we assume a uniform probability for each cell, i.e., we set $\pi = 1/p$ for all $i$. In Model II, we set cell probabilities to increase linearly, i.e., $\pi_i = i/(\sum_{k=1}^p k)$. For each $p = 5, 10$, and $n = 100, 200, \ldots, 3000$, a contingency table $\theta(S)$ is sampled, and perturbed to obtain an output each from the mechanisms—$M_G$, $M_r$, $M_{JS0}$, $M_{JS}$, $M_{JS}$ and $M_{\text{Lap}}(\cdot; \tilde{b}_\mu)$ and their truncated versions—satisfying $\mu$-GDP. We set $\mu = 0.1$. The squared $L_2$-loss $\|M(S) - \theta(S)\|_2^2$ for each output $M(S)$ is averaged over
\[ \pi: \text{uniform, without truncation, } \mu = 0.1, p = 5 \]

\[ \pi: \text{uniform, without truncation, } \mu = 0.1, p = 10 \]

\[ \pi: \text{increasing, without truncation, } \mu = 0.1, p = 5 \]

\[ \pi: \text{increasing, without truncation, } \mu = 0.1, p = 10 \]

Figure 5: A comparison of \( L_2 \)-costs of mechanisms without truncation, over increasing sample sizes. The first (or second) row shows results under Model I (or Model II, respectively).

\( K = 10,000 \) repetitions, for each mechanism. This is an estimate of the unconditional \( L_2 \)-cost \( \chi^2(M) \).

The simulated results are plotted in Figures 5 and 6. Results from \( MLap(\cdot; \tilde{b}_\mu) \) are omitted because their \( L_2 \)-costs are much larger than those of Gaussian mechanisms, as seen in Section 4.

See Figure 1 for a summary of the comparison between Gaussian mechanisms in this simulation study. In addition, we observe the following.

The benefit of James–Stein shrinkage eventually wears off as the sample size increases, as seen in Theorem 7. However, depending on the model, the benefit of shrinkage can be persistent. For Model I, \( E(\theta(S)) = n\pi = (n/p)1_p \) and the James–Stein mechanism \( M_{JS} \) performs best for smaller sample sizes as the model agrees with the target of the shrinkage. Nevertheless, the rank-deficient mechanisms \( Mr \) and \( MrJS \) exhibit smallest \( L_2 \)-costs for larger sample sizes. On the other hand, for Model II, while the rank-deficient James–Stein mechanism \( M_{JS} \) performs the best across different sample sizes, \( Mr \)'s \( L_2 \)-cost is also the smallest for moderately large sample sizes.

We also observe that the advantage of truncation is more pronounced for small sample sizes. The benefit of truncation is large only if there are many negative valued outputs in the untruncated mechanisms. As the sample size increases, \( E(\theta(S)) = n\pi \) increases, thus the outputs of \( M(S) \) tend to be strictly positive.

5.3 Differentially private hypothesis tests for contingency table

In this section, we discuss private \( \chi^2 \) tests based on \( \mu \)-GDP contingency tables \( M(S) \), perturbing \( \theta(S) \), for testing goodness-of-fit (GOF) and homogeneity. We consider two-way contingency tables \( \theta(S) \) of size \( r \times c \), in which \( \theta(S)_{ij} \) collects the count of observations belonging to the \((i,j)\)th category.

Classical \( \chi^2 \) tests are based on the test statistic \( T \) given by

\[
T = \sum_{i=1}^{c} \sum_{j=1}^{r} \frac{(\theta(S)_{ij} - E_{ij})^2}{E_{ij}},
\]

where \( E_{ij} \) is the expected cell count under the null hypothesis. The large-sample null distribution of \( T \) is \( \chi^2_k \) for some degrees of freedom \( k \), and this fact is used to construct a \( \chi^2 \) test. Suppose now that a sanitized contingency table \( M(S) \) is only available, in place of the original data summary.
\( \pi \): uniform, truncation, \( \mu = 0.1, p = 5 \)  
\( \pi \): uniform, truncation, \( \mu = 0.1, p = 10 \)  
\( \pi \): increasing, truncation, \( \mu = 0.1, p = 5 \)  
\( \pi \): increasing, truncation, \( \mu = 0.1, p = 10 \)

**Figure 6:** A comparison of \( L_2 \)-costs of truncated mechanisms, over increasing sample sizes. The first (or second) row shows results under Model I (or Model II, respectively).

\[ \theta(S). \] (The randomized mechanism \( M \) can be any mechanism we discussed in Sections 2 and 3.) Some researchers including [Kifer and Rogers, 2016; Gaboardi et al., 2016; Wang et al., 2017; Son et al., 2022] proposed to simply replace \( \theta(S) \) by \( M(S) \) in (29), resulting in a private statistic

\[ \tilde{T} = \sum_{i,j}^r \frac{(M(S)_{ij} - \tilde{E}_{ij})^2}{\tilde{E}_{ij}}, \]

where \( \tilde{E}_{ij} \) is obtained from \( M(S) \) under the null hypothesis. Critical values for the private test statistic \( \tilde{T} \) are obtained either by large-sample asymptotic approximations or by a bootstrap procedure. In the following, we use a parametric bootstrap procedure to approximate the null distribution of \( \tilde{T} \) for the GOF test and the homogeneity test.

In the construction of private tests, we assume the following.

1. A sanitized table \( M(S) \), satisfying \( \mu \)-GDP, is only available to us. The original table \( \theta(S) \) as well as the data set \( S \) are not accessible.
2. The exact mechanism used to produce \( M(S) \) is known.
3. The privacy level \( \mu \) (or, equivalently the scale parameters \( \sigma \) and \( b \), for Gaussian and Laplace mechanisms, respectively) is known.

Since our test procedure depends on the data set \( S \) only via \( M(S) \), if \( M(S) \) is \( \mu \)-GDP, then any conclusion made from the test procedure is also \( \mu \)-GDP.

We remark that most of private \( \chi^2 \) tests in the literature are based on Laplace mechanisms and are calibrated to satisfy \( \epsilon \)-DP. On the other hand, we calibrate our randomized mechanisms to satisfy \( \mu \)-GDP. Moreover, those previous works assume that the total sample size \( n \) is known (Gaboardi et al., 2016; Kifer and Rogers, 2016). However, when \( M(S) \) is only available, the sample size \( n \) is also hidden. Our test procedures do not assume that \( n \) is known.

### 5.3.1 Private goodness of fit test

Consider a contingency table \( \theta(S) \sim \text{Multinomial}(n, \pi) \), where \( \pi \in \mathbb{R}_+^r \times \mathbb{R}_+^c \) such that \( \sum_{i,j} \pi_{ij} = 1 \). For a given probability parameter \( \pi_0 \), the GOF test aims to test

\[ H_0 : \pi = \pi_0 \quad \text{vs.} \quad H_1 : \pi \neq \pi_0. \] (30)
In the non-private GOF test, the expected cell count under $H_0$ is simply $E_{ij} = n(\pi_0)_{ij}$ and the $\chi^2$ statistic becomes $T_{GOF} = \sum_{i=1}^r \sum_{j=1}^c \frac{(\theta_{ij} - n(\pi_0)_{ij})^2}{n(\pi_0)_{ij}}$. Suppose now that an output $\hat{\theta}$ of $M(S)$ is only available to us. The private $\chi^2$ test statistic is

$$\hat{T}_{GOF} = \sum_{i=1}^r \sum_{j=1}^c \frac{(\hat{\theta}_{ij} - \hat{n}(\pi_0)_{ij})^2}{\hat{n}(\pi_0)_{ij}},$$

where $\hat{n} = \sum_{i,j} \hat{\theta}_{ij}$.

To approximate the null distribution of $\hat{T}_{GOF}$, we use a parametric bootstrap resampling under the null hypothesis, which amounts to sampling $\hat{\theta}^{(b)} \sim \text{Multinomial}(\hat{n}, \pi_0)$ and calculate bootstrap-replicates $\hat{T}_{GOF}^{(b)}$ for some large $B$. (We used $B = 5000$ in our numerical studies.) The bootstrapped p-value of the observed statistic $\hat{T}_{GOF}$ is then the proportion of bootstrap replicates greater than $\hat{T}_{GOF}$. See Algorithm 2. In the implementation of this private GOF test, we set $0/0 = 0$, and if $\hat{n} \leq 0$, which can happen if the amount of perturbation is large, then we do not reject the null hypothesis.

**Algorithm 2:** Private parametric bootstrap test of goodness of fit

1. **Procedure** BootGOF($\hat{\theta}$, $\mu$, $M(\cdot)$, $\pi_0$, $\alpha$)
2. \[ \hat{n} \leftarrow \sum_{i=1}^r \sum_{j=1}^c \hat{\theta}_{ij} \]
3. \[ \hat{T}_{GOF} = \sum_{i=1}^r \sum_{j=1}^c \frac{(\hat{\theta}_{ij} - \hat{n}(\pi_0)_{ij})^2}{\hat{n}(\pi_0)_{ij}} \]
4. \[ \text{for } b = 1, \ldots, B \text{ do} \]
5. \[ \hat{\theta}^{(b)} \leftarrow M(\theta^{(b)}) \text{ where } \theta^{(b)} \sim \text{Multinomial}(\hat{n}, \pi_0) \]
6. \[ \hat{n}^{(b)} \leftarrow \sum_{i=1}^r \sum_{j=1}^c \hat{\theta}_{ij}^{(b)} \]
7. \[ \hat{T}_{GOF}^{(b)} = \sum_{i=1}^r \sum_{j=1}^c \frac{(\hat{\theta}_{ij}^{(b)} - \hat{n}^{(b)}(\pi_0)_{ij})^2}{\hat{n}^{(b)}(\pi_0)_{ij}} \]
8. \[ \text{end} \]
9. P-value $\leftarrow \frac{1}{\pi} \sum_{b=1}^B I(\hat{T}_{GOF}^{(b)} \geq \hat{T}_{GOF})$
10. if P-value $< \alpha$ then
11. \[ \text{return reject } H_0 \]
12. else
13. \[ \text{return do not reject } H_0 \]
14. end

5.3.2 Private homogeneity test

Consider the situation where there are $r$ populations, and the data set $S$ is the union of data sets $S_1, \ldots, S_r$ from each population. For each $i = 1, \ldots, r$, the $i$th row of the $r \times c$ contingency table $\theta(S)$ is $\theta(S_i)$. Assume that $\theta(S_i) \sim \text{Multinomial}(n_i, \pi_i)$ where $\pi_i \in \mathbb{R}^c_+$ is a vector of probabilities for the $i$th population. Testing the homogeneity among these population amounts to testing the null hypothesis $H_0 : \pi_1 = \cdots = \pi_r$ against a general alternative.

In the classical homogeneity test, the $\chi^2$ statistic is obtained from the data $\theta(S)$ as follows: Since the null probabilities $\pi_0 := \pi_1 = \cdots = \pi_r$ are unknown, an estimator $\tilde{\pi}_0 = \sum_{i=1}^r \theta(S_i)/(\sum_{i=1}^r n_i) =: (\tilde{\pi}_{01}, \ldots, \tilde{\pi}_{0c})^\top$ is used to set the expected counts $E_{ij} = n_i \tilde{\pi}_{0j}$ under the null hypothesis. The non-private $\chi^2$ statistic is $T_{Hom} = \sum_{i=1}^r \sum_{j=1}^c (\theta(S_{ij}) - E_{ij})^2/E_{ij}$.

If an output $\hat{\theta}$ of $M(S)$ is only available, then the private $\chi^2$ statistic, say $T_{Hom}$, is obtained by replacing $\theta(S)$ with $\hat{\theta}$ in the formula for the non-private statistic $T_{Hom}$. A parametric bootstrap procedure for testing the homogeneity using the private statistic $T_{Hom}$ can be constructed by following the same arguments used for the private GOF test in Section 5.3.1; see Algorithm 3.

5.4 Simulation studies for private test procedures

In this section, we numerically investigate the private GOF tests in Section 5.3, based on the $\mu$-GDP private contingency tables discussed in Section 5.1. In particular, we examine whether the
the Laplace mechanism is tightly calibrated to satisfy
\( \mu \) mechanism-based test is significantly lower than tests based on Gaussian-type mechanisms, albeit power is increasing as the sample size increases, for all cases. However, the power of the Laplace Stein mechanisms control the type I error rates successfully. From Figure 8, we observe that the in which case the amount of perturbation is huge. Nevertheless, all the tests based on the James–Stein mechanisms control the type I error rates successfully. From Figure 8 we observe that the power is increasing as the sample size increases, for all cases. However, the power of the Laplace mechanism-based test is significantly lower than tests based on Gaussian-type mechanisms, albeit the Laplace mechanism is tightly calibrated to satisfy \( \mu \)-GDP. Among Gaussian-type mechanisms, the test based on \( M^c_{JS} \) stands out in terms of empirical power. The superior performance of using

Algorithm 3: Private parametric bootstrap test of homogeneity

1. Procedure \( \text{BootHom}(\hat{\theta}, \mu, M(\cdot), \alpha) \)

   2. \( \tilde{n}_i \leftarrow \sum_{j=1}^{c} (\hat{\theta}_i)_j \) for \( i = 1, \ldots, r \)

   3. \( \tilde{n} \leftarrow \sum_{i=1}^{r} \tilde{n}_i \)

   4. \( \tilde{\pi}_0 \leftarrow (\tilde{n})^{-1} \sum_{i=1}^{r} \tilde{\theta}_i \)

   5. \( \tilde{T}_{\text{Hom}} \leftarrow \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{((\hat{\theta}_i)_j - \tilde{n}_i \tilde{\pi}_0)_j^2}{\tilde{n}_i \tilde{\pi}_0} \)

   for \( b = 1, \ldots, B \) do

      7. \( \hat{\theta}_i^{(b)} \leftarrow M(\theta_i) \) where \( \theta_i \sim \text{Multinomial}(\tilde{n}_i, \pi_0) \) for \( i = 1, \ldots, r \)

      8. \( \tilde{n}_i^{(b)} \leftarrow \sum_{j=1}^{c} (\hat{\theta}_i^{(b)})_j \) for \( i = 1, \ldots, r \)

      9. \( \tilde{n}^{(b)} \leftarrow \sum_{i=1}^{r} \tilde{n}_i^{(b)} \)

      10. \( \hat{\pi}_0^{(b)} \leftarrow (\tilde{n}^{(b)})^{-1} \sum_{i=1}^{r} \hat{\theta}_i^{(b)} \)

      11. \( \tilde{T}_{\text{Hom}}^{(b)} \leftarrow \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{((\hat{\theta}_i^{(b)})_j - \tilde{n}_i^{(b)} \hat{\pi}_0^{(b)})_j^2}{\tilde{n}_i^{(b)} \hat{\pi}_0^{(b)}} \)

   end

13. \( \text{P-value} \leftarrow \frac{1}{B} \sum_{b=1}^{B} I(\tilde{T}_{\text{Hom}}^{(b)} \geq \tilde{T}_{\text{Hom}}) \)

if \( \text{P-value} < \alpha \) then

15. return reject \( H_0 \)

else

17. return do not reject \( H_0 \)

end

test procedures control the type I error rate at the given significance level \( \alpha \), and compare the power of the tests as a measure of the statistical utility of the randomized mechanisms. We also have investigated the performance of private homogeneity tests, and the results are listed and discussed in Appendix E. The conclusions made for homogeneity tests are similar to the case of GOF tests.

Probability models for the null and alternative hypotheses are generated using real data sets from 2020 resident population demographic data of South Korea [Statistics Korea 2021] and the United States [United States Census Bureau 2020]. We set the null probabilities \( \pi_0 \) to be the \( p \times 1 \) vector \( \pi_{\text{Kor}}^{(p)} \) consisting of the age-wise population proportions, given by \( p \) age groups, from the South Korean demographic data. We use \( p = 9, 18 \) corresponding to 5-year and 10-year age groups, respectively. The alternative probabilities \( \pi_{\text{US}}^{(p)} \) consist of the \( p \) proportions from the U.S. demographic data.

We simulate under two privacy levels given by \( \mu = 0.1 \) (representing a high privacy regime) and \( \mu = 0.3 \) (moderate privacy). Type I error rates of the private GOF test (Algorithm 2) are evaluated by randomly generating contingency tables \( \theta(S) \sim \text{Multinomial}(n, \pi_{\text{Kor}}^{(p)}) \), applying a mechanism in Section 5.1, then conducting the private GOF test (Algorithm 2) with the null hypothesis \( \pi = \pi_{\text{Kor}}^{(p)} \). For the power analysis, we generate tables from \( \text{Multinomial}(n, \pi_{\text{US}}^{(p)}) \). Over a range of sample sizes \( n \), we record the proportions of rejection (with significance level \( \alpha = 0.05 \)) over \( K = 1000 \) repetitions, as estimates of the type I error rate and the power of the test.

The simulation results for the GOF test, based on the truncated Gaussian type mechanisms \( (M_G, M^c_r, M^c_{JS0}, M^c_{JS}, M^c_{JS}) \) and the truncated Laplace mechanism \( (M_{\text{Lap}}(\cdot; b_\mu)) \), are plotted in Figures 7 and 8.

Private GOF tests from all mechanisms control the type I error rate at \( \alpha = 0.05 \) for most cases, as can be seen in Figure 7. The only exception is the case of \( N \leq 500 \) with \( \mu = 0.1 \) and \( p = 18 \), in which case the amount of perturbation is huge. Nevertheless, all the tests based on the James–Stein mechanisms control the type I error rates successfully. From Figure 8 we observe that the power is increasing as the sample size increases, for all cases. However, the power of the Laplace mechanism-based test is significantly lower than tests based on Gaussian-type mechanisms, albeit the Laplace mechanism is tightly calibrated to satisfy \( \mu \)-GDP. Among Gaussian-type mechanisms, the test based on \( M^c_{JS} \) stands out in terms of empirical power. The superior performance of using
Figure 7: Graph of empirical type I error rates of GOF tests for each mechanism. The black dotted line is the level of the test, $\alpha = 0.05$. The red dotted line is the maximum empirical rejection rate value that contains 0.05 within two times of standard error.

Figure 8: Graph of empirical power of GOF tests for each mechanism.
6 Discussion

In this article, we demonstrated that the rank-deficiency of the sensitivity space $S_\theta$ and James–Stein shrinkage phenomenon can be used to improve the statistical utility of multivariate Gaussian mechanisms, which turns out to be more advantageous than using the optimally calibrated Laplace mechanism. In particular, except for the case where low levels of privacy protection are imposed, ordinary Laplace mechanisms are strictly dominated by ordinary Gaussian mechanisms. Nevertheless, one may naturally ask whether utilizing the rank-deficiency of $S_\theta$ and/or shrinkage phenomenon is beneficial for multivariate Laplace mechanisms.

Similarly to the Gaussian case, utilizing the rank-deficiency of $S_\theta$ for Laplace mechanisms is also beneficial. To see this, let $\Delta_1(\theta; X^n) = \Delta_1$ and $\dim(S_\theta) = d_\theta < p$. Let $U = [U_{S_\theta}, U_1]$ be a $p \times p$ orthogonal matrix, where $\text{span}(U_{S_\theta}) = \text{span}(S_\theta)$. Then a rank-deficient Laplace mechanism $M_{\text{Lap},r}(\cdot, b)$ may be defined as

$$M_{\text{Lap},r}(S; b) = U_{S_\theta}[U_{S_\theta}^\top \theta(S) + \text{Lap}_{d_\theta}(0, b)] + U_1 U_1^\top \theta(S).$$

Let $\Delta^U_1 := \sup_{\nu \in S_\theta} \|U_{S_\theta}^\top \nu\|_1$. An application of Theorem 13 implies that $M_{\text{Lap},r}(\cdot, b)$ for $b \geq b_{\Delta^U_1}^\theta := \Delta^U_1 / [-2 \log \{2\Phi(-\frac{b}{\sqrt{2}})\}]$ is $\mu$-GDP, Since the $L_1$-cost of $M_{\text{Lap},r}(\cdot; b)$ is proportional to $d_\theta b^r$, $M_{\text{Lap},r}(\cdot; b)$ strictly dominates $M_{\text{Lap}}(\cdot; b)$ for $d_\theta < p$. On the other hand, the smallest scale parameter $b$ of $M_{\text{Lap},r}$, satisfying $\mu$-GDP, depends on the specific choice of $U_{S_\theta}$. We suspect that $b_{\Delta^U_1}^\theta$ is smaller than $b_{\Delta^1_1}^\theta$ for some choices of $U_{S_\theta}$, but is not for other choices of $U_{S_\theta}$. We have not pursued further investigation in this direction. This is because that the statistical utility of the ordinary Gaussian mechanism far exceeds that of Laplace mechanisms, and their rank-deficient siblings are deemed to have similar relations.

We believe that an application of shrinkage for multivariate Laplace mechanisms can be beneficial. However, since the $L_1$ shrinkage is more natural for Laplace perturbations, such an investigation falls outside the scope of this article. In addition, we note that the analytical composition bounds through Edgeworth expansion [Zheng et al., 2020; Wang et al., 2022] can be applied in handling Laplace trade-off functions when $p \geq 3$, and the central limit theorem approach seems plausible when $p$ is large [Dong et al., 2022, 2021; Sommer et al., 2019]. Applications of these approximations in calibration of randomized mechanisms of high-dimensional statistics may be an interesting direction for future research.

References

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., and Zhang, L. (2016), “Deep learning with differential privacy,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 308–318.

Anderson, T. W. (2003), An Introduction to Multivariate Statistical Analysis, New York: Wiley, 3rd ed.

Avella-Medina, M. (2021), “Privacy-preserving parametric inference: a case for robust statistics,” Journal of the American Statistical Association, 116, 969–983.

Awan, J. and Dong, J. (2022), “Log-concave and multivariate canonical noise distributions for differential privacy,” arXiv preprint arXiv:2206.04572.

Awan, J. and Slavković, A. (2021), “Structure and sensitivity in differential privacy: Comparing $K$-norm mechanisms,” Journal of the American Statistical Association, 116, 935–954.

Balle, B. and Wang, Y.-X. (2018), “Improving the gaussian mechanism for differential privacy: Analytical calibration and optimal denoising,” in International Conference on Machine Learning, PMLR, pp. 394–403.
Cai, T. T., Wang, Y., and Zhang, L. (2021), “The cost of privacy: Optimal rates of convergence for parameter estimation with differential privacy,” The Annals of Statistics, 49, 2825–2850.

Dong, J., Roth, A., and Su, W. J. W. (2022), “Gaussian differential privacy,” Journal of the Royal Statistical Society: Series B (Statistical Methodology), 84, 3–37.

Dong, J., Su, W., and Zhang, L. (2021), “A central limit theorem for differentially private query answering,” Advances in Neural Information Processing Systems, 34, 14759–14770.

Duchi, J. C., Jordan, M. I., and Wainwright, M. J. (2018), “Minimax optimal procedures for locally private estimation,” Journal of the American Statistical Association, 113, 182–201.

Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., and Naor, M. (2006a), “Our data, ourselves: Privacy via distributed noise generation,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 486–503.

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006b), “Calibrating noise to sensitivity in private data analysis,” in Theory of Cryptography Conference, Springer, pp. 265–284.

Dwork, C., Roth, A., et al. (2014), “The algorithmic foundations of differential privacy,” Foundations and Trends® in Theoretical Computer Science, 9, 211–407.

Efron, B. (2012), Large-Scale Inference: Empirical Bayes Methods for Estimation, Testing, and Prediction, Cambridge University Press.

Gaboardi, M., Lim, H., Rogers, R., and Vadhan, S. (2016), “Differentially private chi-squared hypothesis testing: Goodness of fit and independence testing,” in International Conference on Machine Learning, PMLR, pp. 2111–2120.

Geng, Q., Kairouz, P., Oh, S., and Viswanath, P. (2015), “The staircase mechanism in differential privacy,” IEEE Journal of Selected Topics in Signal Processing, 9, 1176–1184.

Harville, D. A. (1998), Matrix Algebra from a Statistician’s Perspective, Taylor & Francis.

James, W. and Stein, C. (1961), “Estimation with quadratic Loss,” in Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics, University of California Press, vol. 4, pp. 361–380.

Kairouz, P., Oh, S., and Viswanath, P. (2014), “Extremal mechanisms for local differential privacy,” Advances in Neural Information Processing Systems, 27, 2879–2887.

— (2015), “The composition theorem for differential privacy,” in International Conference on Machine Learning, PMLR, pp. 1376–1385.

Karwa, V., Krivitsky, P. N., and Slavković, A. B. (2017), “Sharing social network data: differentially private estimation of exponential family random-graph models,” Journal of the Royal Statistical Society: Series C (Applied Statistics), 66, 481–500.

Kifer, D. and Rogers, R. (2016), “A new class of private chi-square tests,” in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS, vol. 17, pp. 991–1000.

Lambert, J. H. (1758), “Observationes variae in mathesin puram,” Acta Helvetica, 3, 128–168.

McSherry, F. and Talwar, K. (2007), “Mechanism design via differential privacy,” in 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS’07), IEEE, pp. 94–103.

Mironov, I. (2017), “Rényi differential privacy,” in 2017 IEEE 30th Computer Security Foundations Symposium (CSF), IEEE, pp. 263–275.

Olver, F. W., Lozier, D. W., Boisvert, R. F., and Clark, C. W. (2010), NIST Handbook of Mathematical Functions Hardback and CD-ROM, Cambridge University Press.
Paolella, M. S. (2007), *Intermediate Probability: A Computational Approach*, John Wiley & Sons.

Sommer, D., Meiser, S., and Mohammadi, E. (2019), “Privacy loss classes: The central limit theorem in differential privacy,” *Proceedings on Privacy Enhancing Technologies*, 2, 245–269.

Son, J., Park, M., and Jung, S. (2022), “A parametric bootstrap test for comparing differentially private histograms,” *The Korean Journal of Applied Statistics*, 35, 1–17.

Statistics Korea (2021), “Census questionnaire,” https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_1B040M1&conn_path=I2, accessed: 2022-11-26.

United States Census Bureau (2020), “2020 Demographic Analysis estimates by age and sex,” https://www.census.gov/data/tables/2020/demo/popest/2020-demographic-analysis-tables.html, December 2020 release.

Wang, H., Gao, S., Zhang, H., Shen, M., and Su, W. J. (2022), “Analytical composition of differential privacy via the Edgeworth accountant,” *arXiv preprint arXiv:2206.01330*.

Wang, Y., Lee, J., and Kifer, D. (2017), “Revisiting differentially private hypothesis tests for categorical data,” *arXiv preprint arXiv:1511.03376*.

Wasserman, L. and Zhou, S. (2010), “A statistical framework for differential privacy,” *Journal of the American Statistical Association*, 105, 375–389.

Zheng, Q., Dong, J., Long, Q., and Su, W. (2020), “Sharp composition bounds for Gaussian differential privacy via Edgeworth expansion,” in *International Conference on Machine Learning*, PMLR, pp. 11420–11435.
A Technical tools for working with trade-off functions

Oftentimes it is convenient to write trade-off functions with respect to random variables. For random variables $X \sim P$ and $Y \sim Q$, we write $T(X, Y) := T(P, Q)$. If the distributions $P$ and $Q$ have densities $f$ and $g$, we also denote $T(f, g) := T(P, Q)$.

Trade-off functions are invariant under simultaneous one-to-one affine transformations:

**Lemma A.1.** Suppose $f$ and $g$ are density functions, for $p$-variate random vectors $X \sim f$ and $Y \sim g$, and for any full-rank $p \times p$ matrix $A$ and $b \in \mathbb{R}^p$,

\[
T(Ax + b, Ay + b) = T(x, y) = T(f, g).
\]

**Proof of Lemma A.1.** By the Neyman-Pearson lemma, the most powerful rejection region corresponding to $T(x, y)$ is $R_\alpha = \{w : \log(g(w)/f(w)) \geq c_\alpha\}$ where $c_\alpha$ satisfies $\Pr_{M \sim f}(M \in R_\alpha) = \alpha$. The density functions of $AX + b$ and $AY + b$ are $\frac{1}{|A|} f(A^{-1}(-b))$ and $\frac{1}{|A|} g(A^{-1}(-b))$, respectively. Then the rejection region corresponding to $T(Ax + b, Ay + b)$ at level $\alpha$ is $R'_\alpha = \{z : \log g(A^{-1}(z - b)) \geq c'_\alpha\}$, where $c'_\alpha$ satisfies $\Pr(Z \in R'_\alpha) = \alpha$ for $Z \overset{d}{=} Ax + b$. It can be checked that $c'_\alpha = c_\alpha$, and that $\Pr_{M \sim f}(AM + b \notin R'_\alpha) = \Pr_{M \sim g}(M \notin R_\alpha)$ for all $\alpha \in (0, 1)$. [This lemma was used implicitly in Dong et al. 2022.]

The next few results are useful when dealing with Gaussian mechanisms.

**Lemma A.2.** Let $\mu, \mu_1, \mu_2 \in \mathbb{R}^p$ be arbitrary and $\Sigma$ be a $p \times p$ symmetric positive-definite matrix. Then,

(i) $T(N_p(0, I_p), N_p(\mu, I_p)) = T(N(0, 1), N(\|\mu\|_2, 1)) = G_{\|\mu\|_2}$.

(ii) $T(N_p(\mu_1, \Sigma), N_p(\mu_2, \Sigma)) = G_{\|\Sigma^{-1/2}(\mu_2 - \mu_1)\|_2}$.

**Proof of Lemma A.2.** (i) By the Neyman–Pearson lemma, the most powerful rejection region corresponding to $T(N_p(0, I_p), N_p(\mu, I_p))$ is $R_\alpha = \{x \in \mathbb{R}^p : x^T \mu \geq \|\mu\|_2 \Phi^{-1}(1 - \alpha)\}$. One can easily check that the type II error rate is $\Pr_{x \sim N_p(\mu_1, I_p)}(x \notin R_\alpha) = G_{\|\mu\|_2}(\alpha)$. (ii) By Lemma A.1, we have $T(N_p(\mu_1, \Sigma), N_p(\mu_2, \Sigma)) = T(N_p(0, I_p), N_p(\Sigma^{-1/2}(\mu_2 - \mu_1), I_p))$. Applying part (i) gives the desired result.

An immediate consequence of Lemmas A.1 and A.2 is the following result on the privacy guarantee of ordinary Gaussian mechanisms.

**Theorem A.3** (Ordinary Gaussian mechanism). Let $\theta$ be a multivariate statistic with $\Delta_2(\theta; x^n) = \Delta_2$. The ordinary Gaussian mechanism $M_G$, given by $M_G(S) = \theta(S) + N_p(0, \sigma^2 I_p)$, is $\mu$-GDP for any $\mu \geq \mu_0 := \Delta_2/\sigma$.

**Proof of Theorem A.3.** For any data sets $S$ and $S'$, $M_G(S) \sim N_p(\theta(S), \sigma^2 I_p)$ and $M_G(S') \sim N_p(\theta(S'), \sigma^2 I_p)$. By Lemmas A.1 and A.2,

\[
T(M_G(S), M_G(S')) = G_{\|\theta(S) - \theta(S')\|_2}.
\]

Since $0 \leq a \leq b$ if and only if $G_a \geq G_b$,

\[
\inf_{S \sim S'} T(M_G(S), M_G(S')) = \inf_{S \sim S'} G_{\|\theta(S) - \theta(S')\|_2} = G_{\sup_{S \sim S'} \|\theta(S) - \theta(S')\|_2} = G_{\Delta_2} = G_{\mu_0}.
\]

Thus, for any $\mu \geq \mu_0$, $\inf_{S \sim S'} T(M_G(S), M_G(S')) \geq G_{\mu}$. Care is needed when we compare two multivariate normal distributions with a rank-deficient covariance matrix.

26
Lemma A.4. Let \( x \sim N_p(\mu_1, \Sigma) \) and \( y \sim N_p(\mu_2, \Sigma) \), where \( \Sigma \) is a \( p \times p \) symmetric semi-definite matrix with \( \text{rank}(\Sigma) < p \). Let \( C(\Sigma) \subset \mathbb{R}^p \) be the column space of the matrix \( \Sigma \).

(a) If \( \mu_2 - \mu_1 \in C(\Sigma) \), then \( T(x, y) = G \|x\|_2^2 (\mu_2 - \mu_1) \|_2 \), where \( \Sigma^\dagger \) is the Moore-Penrose pseudo-inverse of \( \Sigma \).

(b) If \( \mu_2 - \mu_1 \notin C(\Sigma) \), then \( T(x, y)(\alpha) = 0 \) for all \( \alpha \in [0, 1] \).

Proof. By Lemma A.1, \( T(x, y) = T(x_n, y_n, x_n, y_n) = T(N_p(0, \Sigma), N_p(\mu, \Sigma)) \) for \( \mu = \mu_2 - \mu_1 \). Without loss of generality, we let \( \mu_1 = 0 \) and \( \mu_2 = \mu \).

Let \( \Sigma = U\Lambda U^\top \) be the eigendecomposition of \( \Sigma \) such that \( \Lambda = \text{diag}(\lambda_1, \ldots, \lambda_q) \) for \( q = \text{rank}(\Sigma) < p \). Let \( U_2 \) be such that \([U, U_2]\) is an orthogonal matrix. Then for

\[
\begin{align*}
    z_1 &= U^\top x, \quad w_1 = U^\top y, \\
    z_2 &= U_2^\top x, \quad w_2 = U_2^\top y,
\end{align*}
\]

we have

\[
\begin{align*}
    z_1 &\sim N_q(0, \Lambda), \quad w_1 \sim N_q(U^\top \mu, \Lambda), \\
    z_2 &= 0, \quad w_2 = U_2^\top \mu.
\end{align*}
\]

(a) Suppose \( \mu \in C(\Sigma) \), that is, \( U_2^\top \mu = 0 \). Then, testing

\[
H_0 : N_p(0, \Sigma) \quad \text{vs.} \quad H_1 : N_p(\mu, \Sigma)
\]

based on one observation from either distribution is equivalent to testing

\[
H_0 : N_q(0, \Lambda) \quad \text{vs.} \quad H_1 : N_q(U^\top \mu, \Lambda)
\]

based on one observation from either distribution. Thus,

\[
T(x, y) = T(z_1, w_1)
= T(N_q(0, \Lambda), N_q(U^\top \mu, \Lambda))
= T(N(0, 1), N(\|\Lambda^{-1/2}U^\top \mu\|_2, 1)).
\]

Since \( \|\Lambda^{-1/2}U^\top \mu\|_2 = \|UA^{-1/2}U^\top \mu\|_2 = \|(|\Sigma^\dagger|^\dagger \mu\|_2, \) the result follows.

(b) Suppose \( \mu \notin C(\Sigma) \). Then \( U_2^\top \mu \neq 0 \). This means that \( z_2 = 0 \) and \( w_2 = U_2^\top \mu \) are distinguishable with probability 1. Consider a test function \( \phi \) defined by

\[
\phi(x) = \begin{cases} 
\text{reject} & \text{if } (U_2^\top \mu)^\top \left( U_2^\top x - U_2^\top \mu/2 \right) > 0, \\
\text{do not reject} & \text{otherwise}.
\end{cases}
\]

Then the type I and II error rates are calculated as \( \alpha_\phi = \mathbb{P}(\|w_2\|^2/2 > 0) = 0 \) and \( \beta_\phi = \mathbb{P}(\|w_2\|^2/2 \leq 0) = 0 \). Since the trade-off function is non-increasing, we have

\[
T(x, y) \leq T(x, y)(0) = T(x, y)(\alpha_\phi) = \beta_\phi = 0.
\]

This completes the proof. \( \square \)

Finally, we formally state the post-processing property for the \( f \)-DP criterion, discussed in Sections 2.2 and 2.3

Lemma A.5 (Post-processing property, [Dong et al., 2022]). Let \( f \) be a trade-off function. If a mechanism \( M : X^n \rightarrow Y \) is \( f \)-DP, then \( \text{Proc} \circ M \) is also \( f \)-DP for any post-processing function \( \text{Proc} : Y \rightarrow Z \) where \( Z \) is some abstract space.
B Proofs for Section 2

Proof of Lemma 1. Assume $\lambda_{\min}(\Sigma) \geq \Delta_2^2/\mu^2 > 0$. Then $\Sigma$ is positive definite, and for any $\theta$ with $\Delta_2(\theta; X^n) \leq \Delta_2$, Lemma A.2 implies that

$$\inf_{S \sim S'} T(M_\Sigma(S), M_\Sigma(S')) = \inf_{S \sim S'} T(N(0, \Sigma), N(\theta(S) - \theta(S'), \Sigma))$$

$$= \inf_{S \sim S'} T(N(0, \Sigma), (\Sigma^{-1/2}(\theta(S) - \theta(S'))_2, 1))$$

$$= T(N(0, \Sigma), (\Sigma^{-1/2}(\theta(S) - \theta(S'))_2, 1))$$

$$\geq T(N(0, \Sigma), (\Sigma^{-1/2}\sup_{S \sim S'} \|(\theta(S) - \theta(S'))_2, 1))$$

$$= T(N(0, \Sigma), T(\Delta_2(\theta; X^n), 1)).$$

Since $\Delta_2(\theta; X^n) \leq \Delta_2/\sqrt{\lambda_{\min}(\Sigma)} \leq \mu$, we have $\inf_{S \sim S'} T(M_\Sigma(S), M_\Sigma(S')) \geq G_\mu$, as required.

The ‘only if’ part can be verified by showing the contrapositive: If $\lambda_{\min}(\Sigma) < \Delta_2^2/\mu^2$, then there exists a statistic $\theta$ with $\Delta_2(\theta; X^n) > \Delta_2$ such that $M_\Sigma$ does not satisfy $\mu$-GDP.

Let $b \in \mathbb{R}^p$ be an eigenvector of $\Sigma$ satisfying $\Sigma b = \lambda_{\min}(\Sigma) b$ and $\|b\|_2 = 1$. Let $\theta$ be such that for some $S, S' \in X^n$, $S \sim S'$, $\theta(S) - \theta(S') = \Delta_2 b$. That is, $\Delta_2 b \in \mathcal{S}_0$. The trade-off function corresponding to $M_\Sigma$ is

$$\inf_{S \sim S'} T(M_\Sigma(S), M_\Sigma(S')) = \inf_{\delta \in \mathcal{S}_0} T(N_p(\delta, \Sigma), N_p(0, \Sigma)) \leq T(N_p(\Delta_2 b, \Sigma), N_p(0, \Sigma)).$$

If $\lambda_{\min}(\Sigma) = 0$, then by Lemma A.4, $T(N_p(\Delta_2 b, \Sigma), N_p(0, \Sigma)) \leq G_\mu(\alpha) = 0 < G_\mu(\alpha)$ for all $\alpha \in (0, 1)$. Thus, $M_\Sigma$ does not satisfy $\mu$-GDP (for any $\mu > 0$).

Suppose that $\lambda_{\min}(\Sigma) > 0$. Then, we have

$$\|\Sigma^{-1/2}\Delta_2 b\|_2 = \|\Sigma^{-1/2}\|_2 \|\Delta_2 b\|_2$$

$$= \|\Sigma^{-1/2}\|_2 \|\Delta_2\|_2$$

$$= \Delta_2/\sqrt{\lambda_{\min}(\Sigma)} > \mu,$$

which in turn implies that $T(N(p(\Delta_2 b, \Sigma), N_p(0, \Sigma)) = T(N(0, 1), N(\|\Sigma^{-1/2}\Delta_2 b\|_2, 1)) < G_\mu$, as desired.

Proof of Lemma 2. Lemma 1 implies that if $\sigma^2 \geq \Delta_2^2/\mu^2$, $M_\Sigma$ is $\mu$-GDP.

For the ‘only if’ part, suppose that $\sigma^2 < \Delta_2^2/\mu^2$. Then, for any $\theta$ with $\Delta_2(\theta; X^n) = \Delta_2$,

$$\inf_{S \sim S'} T(M_\Sigma(S), M_\Sigma(S'))$$

$$= T(N(0, 1), N(\sup_{S \sim S'} \|\sigma^{-1}(\theta(S) - \theta(S'))\|_2, 1))$$

$$= G_{\Delta_2/\sigma}$$

$$< G_\mu$$

on $(0, 1)$.

Proof of Theorem 3. For any $S \sim S'$, we have $\theta(S) - \theta(S') \in C(\Theta)$. Thus, by Lemma A.4 (a),

$$T(M_r(S), M_r(S')) = G_{\|\sigma (\Theta) \|_2}$$

$$= G_{\Delta_2/\sigma}$$

$$= G_{\Delta_2/\sigma} \|\theta(S) - \theta(S')\|_2.$$
Therefore, we have
\[
\inf_{S \sim S^\prime} T(M_r(S), M_r(S^\prime)) = G_{\frac{1}{2}, \sup_{S \sim S^\prime}\|\theta(S) - \theta(S^\prime)\|_2} = G_{\Delta_2(t, x^\ast)}.
\]
The result follows as \(G_{\mu}\) strictly and uniformly (on \((0, 1)\)) decreases with respect to \(\mu\).

Next, we provide a proof of Proposition 4. We first list the related result on the conditional \(L_2\)-cost of \(M_rJS\) in Proposition B.1 and give proofs of Propositions 4 and B.1.

**Proposition B.1.** For a multivariate statistic \(\theta : X^n \to \mathbb{R}^p\) with \(\Delta_2(\theta; X^n) = \Delta_2 > 0\), let \(M_rJS\) be the rank-deficient James–Stein Gaussian mechanisms with \(\sigma > 0\), as defined in Definition 3.

For any data set \(S \in X^n\),
\[
L_2(M_rJS(S)) = \sigma^2 d_\theta - \sigma^2(d_\theta - 3)^2 \left\{ \frac{1}{2} e^{-\frac{1}{2} \tau(S)} \sum_{\beta=0}^{\infty} \left( \frac{\tau(S)}{2} \right)^\beta \frac{1}{\beta! \left( \frac{1}{2} d_\theta - 1 + \beta - 1 \right)} \right\},
\]
where \(\tau(S) = \| (I_{d_\theta} - \frac{1}{\sigma^2} 1_{d_\theta} 1_{d_\theta}^\top) U_\theta^\top \theta(S) \|_2^2 / \sigma^2\).

**Proofs of Propositions 4 and B.1.** For some deterministic \(\eta \in \mathbb{R}^p\), suppose that a random vector \(x\) follows \(N_p(\eta, \sigma^2 I_p)\). First, we verify (14) by showing that
\[
\mathbb{E} \| m_0(x; \sigma) - \eta \|_2^2 = \sigma^2 p - \sigma^2(p - 2)^2 \left\{ \frac{1}{2} e^{-\frac{1}{2} \tau} \sum_{\beta=0}^{\infty} \left( \frac{\tau}{2} \right)^\beta \frac{1}{\beta! \left( \frac{1}{2} p + \beta - 1 \right)} \right\}, \tag{32}
\]
where \(\tau = \| \eta \|_2^2 / \sigma^2\). Let \(g(t) = -\frac{(p-2)}{\| \eta \|_2^2} t\) for \(t \in \mathbb{R}^p\). We have
\[
\frac{m_0(x; \sigma)}{\sigma} = \frac{x}{\sigma} + g \left( \frac{x}{\sigma} \right),
\]
with \(x/\sigma \sim N_p(\eta/\sigma, I_p)\). Using Stein’s unbiased risk estimate lemma, we obtain
\[
\mathbb{E} \| m_0(x; \sigma) - \eta \|_2^2 = p \sigma^2 + \sigma^2 \mathbb{E} \left\| g \left( \frac{x}{\sigma} \right) \right\|^2 + 2 \nabla^\top g \left( \frac{x}{\sigma} \right) \mathbb{E} \| x \|^2.
\]
Since \(\frac{\| x \|^2}{\sigma^2} \sim \chi^2(\tau, p)\), we have (Anderson 2003)
\[
\mathbb{E} \left[ \frac{\sigma^2}{\| x \|^2} \right] = \frac{1}{2} e^{-\frac{1}{2} \tau} \sum_{\beta=0}^{\infty} \left( \frac{\tau}{2} \right)^\beta \frac{1}{\beta! \left( \frac{1}{2} p + \beta - 1 \right)}.
\]
This gives (32).

Now, we prove (15) by showing that
\[
\mathbb{E} \| m_a(x; \sigma) - \eta \|_2^2 = \sigma^2 p - \sigma^2(p - 3)^2 \left\{ \frac{1}{2} e^{-\frac{1}{2} \tau_{1,\perp}} \sum_{\beta=0}^{\infty} \left( \frac{\tau_{1,\perp}}{2} \right)^\beta \frac{1}{\beta! \left( \frac{1}{2} (p - 1) + \beta - 1 \right)} \right\}, \tag{33}
\]
where \(\tau_{1,\perp} = \| (I_p - \frac{1}{p} 1_p 1_p^\top) \eta \|_2^2 / \sigma^2\).

Take a \(p \times p\) orthogonal matrix \(U = [u_1 \ U_2]\) with \(u_1 = \frac{1}{\sqrt{p}} 1_p\). Also, let \(y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} u_1^\top x \\ U_2^\top x \end{bmatrix} \sim N_p \left( \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix}, \sigma^2 I_p \right)\).
where 
\[ \eta_1 = \frac{1}{\sqrt{p}} I_p^T \eta \in \mathbb{R}, \quad \eta_2 = U_2^\top \eta \in \mathbb{R}^{p-1}. \]

Then, 
\[
U^\top m_\sigma(x; \sigma) = \begin{bmatrix}
    u_1^T \\
    U_2^T
\end{bmatrix}
\begin{bmatrix}
    \frac{1}{\sqrt{p}} I_p^T \eta + \left(1 - \frac{(p - 3)\sigma^2}{\|x_c\|^2}\right) x_c
\end{bmatrix}
\]

\[
= \begin{bmatrix}
    \frac{1}{\sqrt{p}} I_p^T \eta + \left(1 - \frac{(p - 3)\sigma^2}{\|x_c\|^2}\right) \frac{1}{\sqrt{p}} I_p^T \eta \\
    \frac{1}{\sqrt{p}} I_p^T \eta + \left(1 - \frac{(p - 3)\sigma^2}{\|x_c\|^2}\right) (U_2^\top x - \pi U_2^\top 1_p)
\end{bmatrix}
\]

However,
\[
\|x_c\|^2 = \left\| \left( I_p - \frac{1}{p} I_p 1_p^T \right) x \right\|^2 = \left\| (UU^\top - u_1 u_1^T) x \right\|^2 = \left\| U_2 U_2^\top x \right\|^2 = \left\| U_2^\top x \right\|^2 = \|y_2\|^2.
\]

It implies that
\[
\left(1 - \frac{(p - 3)\sigma^2}{\|x_c\|^2}\right) y_2 = \left(1 - \frac{(p - 1)\sigma^2}{\|y_2\|^2}\right) y_2 = m_0(y; \sigma)
\]

with \( y_2 \sim N_{p-1}(\eta_2, \sigma^2 I_{p-1}). \) Therefore, we obtain
\[
E\|m_\sigma(x; \sigma) - \eta\|^2 = E\|U^\top m_\sigma(x; \sigma) - U^\top \eta\|^2
\]

\[
= E(y_1 - \eta_1)^2 + E\left\| \left(1 - \frac{(p - 3)\sigma^2}{\|y_2\|^2}\right) y_2 - \eta_2 \right\|^2
\]

\[
= \sigma^2 + E\|m_0(y; \sigma) - \eta_2\|^2.
\]

Here, (32) with \( \|\eta_2\|^2 = \left\| (I_p - \frac{1}{p} I_p 1_p^T) \eta \right\|^2 \) gives (33).

For Proposition B.1, note that
\[
L_2(M_{\sigma,JS}(S)) = E\left\| U_1^\top (M_{\sigma,JS}(S) - \Theta(S)) \right\|^2
\]

\[
= E\left\| m_\sigma(U_\theta^\top M_\sigma(S) ; \sigma) - U_\theta^\top \Theta(S) \right\|^2
\]

and \( U_\theta^\top M_\sigma(S) \sim N_{d_n}(U_\theta^\top \theta(S), \sigma^2 I_{d_n}) \). Therefore, by (33), we have (31). \( \square \)

**Proof of Theorem 5** Let \( p \geq 3 \). Since for any \( S \in \mathcal{X}^n \), \( L_2(M_G(S)) = p\sigma^2 \), it can be checked using (14) that \( L_2(M_{JS0}(S)) > L_2(M_G(S)) \) for any \( S \). Thus \( M_{JS0} \) strictly dominates \( M_G \). Proof for (iii) is similarly obtained. \( \square \)

**Proof of Theorem 6** The conclusion is drawn by observing that
\[
L_2(M_{\sigma,JS}(S)) < L_2(M_\sigma(S)) < L_2(M_G(S))
\]

for any \( S \), where \( L_2(M_{\sigma,JS}(S)) \) is given in Proposition B.1. \( \square \)

**Proof of Theorem 4** We give proof of (ii) and (iii) only, since (i) can be shown in a similar manner. In this proof, we wrote \( \theta_n = \theta(S_n) \).
\[ (ii) \text{ Let } \Pi_1^+ = I_p - \frac{1}{p} 1_p 1_p^T. \text{ A simple but key observation is that } \\
\begin{align*}
M_G - M_{JS} &= \frac{(p-3)\sigma^2}{\|\Pi_1^+ M_G\|_2^2} \Pi_1^+ M_G. 
\end{align*}
\]
From this, we have
\[ \|M_G - M_{JS}\|_2^2 / \sigma^2 = \frac{(p-3)^2}{\|\Pi_1^+ M_G\|_2^2}. \]

Since \( M_G(S_n) \) follows \( N_p(\theta_n, \sigma^2 I_p) \), \( \|\Pi_1^+ M_G / \sigma\|_2^2 \) follows the non-central \( \chi^2 \) distribution \( \chi^2(m, 2\lambda_N) \) where \( m = p-1 \) is a degree of freedom and \( \lambda_N = \frac{1}{2\sigma^2} \theta_n^T \Pi_1^+ \theta_N \) is the non-centrality parameter. The expectation of non-central \( \chi^2 \) distribution can be expressed by confluent hypergeometric function \( _1F_1 \). From (10.9) of Paolella (2007), it holds that
\[
\mathbb{E} \left\{ \frac{1}{\|\Pi_1^+ M_G / \sigma\|_2^2} \right\} = \frac{1}{2} \int_0^{\infty} (1-y)^{\frac{p-3}{2}} e^{-\lambda_n y} dy = \frac{1}{2} \int_0^{1} (1-y)^{\frac{p-5}{2}} e^{-\lambda_n y} dy.
\]
For the second equality, we use Kummer’s transformation: \( _1F_1(a, b; z) = e^z _1F_1(b-a, b; -z) \). Then the integral form of \( _1F_1 \), (5.27) of Paolella (2007), implies that
\[
\frac{\Gamma \left( \frac{p-3}{2} \right)}{2\Gamma \left( \frac{p-1}{2} \right)} _1F_1 \left( 1, \frac{p-1}{2}; -\lambda_n \right) = \frac{1}{2} \int_0^{1} (1-y)^{\frac{p-5}{2}} e^{-\lambda_n y} dy.
\]

First, we consider the case of \( p \geq 5 \). Since \( (1-x)^r \leq e^{-rx} \) for any \( x \in [0, 1] \) and \( r \geq 0 \), (35) has an upper bound as follows.
\[
\mathbb{E} \left\{ \frac{1}{\|\Pi_1^+ M_G / \sigma\|_2^2} \right\} = \frac{1}{2} \int_0^{1} (1-y)^{\frac{p-3}{2}} e^{-\lambda_n y} dy \leq \frac{1}{2} \int_0^{1} (1-y)^{\frac{5-p}{2}} e^{-\lambda_n y} dy = \frac{F(\sqrt{\lambda_n})}{\sqrt{\lambda_n}} < \frac{1}{\sqrt{\lambda_n}},
\]
where \( F(x) = \int_0^x e^{-y^2} dy \) is a Dawson’s integral. The last inequality of (37) comes from 7.8.7 of Olver et al. (2010). Note that \( p \) and \( \mu \) are fixed in our setting. So, the right-hand side of the inequalities (36) and (37) converge to 0 as \( n \to \infty \) under the condition \( \|\Pi_1^+ \theta_n / \Delta_2\|_2^2 \to \infty \). This proves (ii) of the theorem.

(iii) Note that
\[
M_r - M_{r,JS} = (U_1^T \Pi_1^+ + U_\theta U_\theta^T) M_r - M_{r,JS} = U_\theta (U_\theta^T M_r - m_a (U_\theta^T M_r; \sigma)).
\]
Let \( \widetilde{M}_r : = U_\theta^T M_r \sim N_q(U_\theta^T \theta_n, \sigma^2 I_{da}) \). Since the multiplication of the orthogonal matrix preserves the \( l_2 \)-norm, we have
\[
\|M_r - M_{r,JS}\|_2^2 = \|\widetilde{M}_r - m_a (\widetilde{M}_r; \sigma)\|_2^2.
\]
From the definition of JS-process,
\[
\|\widetilde{M}_r - m_a (\widetilde{M}_r; \sigma)\|_2^2 = \widetilde{M}_r^T \Pi_{1d_\theta}^+ \widetilde{M}_r
\]
and
\[
\|M_r - M_{r,JS}\|_2^2 / \sigma^2 \sim \chi^2(\hat{m}, 2\hat{\lambda}),
\]
where \( \hat{m} = d_\theta - 1 \) and \( \hat{\lambda} = \frac{1}{2\sigma^2} \theta_n^T \Pi_{1d_\theta} \theta_n \). Thus, by applying a similar argument from the proof of (ii), we get (iii).
\[ \Box \]
Proof of Corollary 3. We begin with writing \( a_n = M_{rJS}(S_n) - \theta(S_n) \), \( r_n = M_p(S_n) - \theta(S_n) \), \( g_n = M_G(S_n) - \theta(S_n) \) and \( j_n = M_{JS}(S_n) - \theta(S_n) \). Then, by the Cauchy-Schwarz inequality, we have

\[
L_2(M_{rJS}(S_n))/\sigma_n^2 = \mathbb{E}[\|a_n\|^2/\sigma_n^2] = \mathbb{E}[\|a_n - r_n\|^2/\sigma_n^2]
\]

Thus, \( \lim_{n \to \infty} \mathbb{E}[\|a_n - r_n\|^2/\sigma_n^2] = 0 \) by Theorem 7 and \( \mathbb{E}[\|r_n\|^2/\sigma_n^2] = L_2(M_r(S_n))/\sigma_n^2 = d_\theta \) for every \( n \).

Observe that \( \lim_{n \to \infty} \mathbb{E}[\|a_n - r_n\|^2/\sigma_n^2] = 0 \) by Theorem 7 and \( \mathbb{E}[\|r_n\|^2/\sigma_n^2] = L_2(M_r(S_n))/\sigma_n^2 = d_\theta \) for every \( n \).

Similarly,

\[
L_2(M_{JS}(S_n))/\sigma_n^2 = \mathbb{E}[\|j_n\|^2/\sigma_n^2] \geq \mathbb{E}[\|j_n - g_n\|^2/\sigma_n^2] - 2 \left( \mathbb{E}[\|j_n - g_n\|^2/\sigma_n^2] \right)^{1/2},
\]

and \( \lim_{n \to \infty} \mathbb{E}[\|j_n - g_n\|^2/\sigma_n^2] = 0 \) by Theorem 7 and \( \mathbb{E}[\|g_n\|^2/\sigma_n^2] = L_2(M_G(S_n))/\sigma_n^2 = p \) for every \( n \). Thus, \( \liminf_{n \to \infty} L_2(M_{JS}(S_n))/\sigma_n^2 \geq p \). This, together with (38), gives the conclusion since \( p > d_\theta \). The argument above works for \( M_{JS} \) replaced by \( M_{JS0} \) as well.

C Proofs and technical details for Section 3

In Section [C.1] we give exact expressions of trade-off functions between univariate and bivariate Laplace distributions, and the trade-off functions corresponding to Laplace mechanisms for the cases \( p = 1 \) (Lemma 10) and \( p = 2 \) (Lemma 3.3). Section [C.2] contains the proofs for Section 3. Throughout the section, we denote

\[
T_{\text{Lap}_p, \delta} := T(\text{Lap}_p(0, 1), T(\text{Lap}_p(\delta, 1))
\]

for any \( \delta \in \mathbb{R}^p \).

C.1 Trade-off functions between univariate and bivariate Laplace distributions

The exact expression of the trade-off function between univariate Laplace distributions, with a common scale parameter, is given in Proposition A.6 of Dong et al. (2022), which is derived from the log-concavity of the Laplace distribution. Below, we give an alternative proof of Proposition A.6 of Dong et al. (2022), by directly using the Neyman-Pearson lemma. It will be instructive in deriving the trade-off function between bivariate Laplace distributions.

First, we describe a general framework of using the Neyman-Pearson lemma in arbitrary dimension. For \( \delta \in \mathbb{R}^p \), the trade-off function \( T(\text{Lap}_p(0, 1), \text{Lap}_p(\delta, 1)) \) is invariant with respect to the sign changes of \( \delta_i \)’s. Moreover, switching the order of \( \delta_i \)’s also does not affect the value of the trade-off function. Thus, we only need to concern the case where \( \delta_1 \geq \cdots \geq \delta_p \geq 0 \).

Recall that the trade-off function’s value at \( \alpha \in [0, 1] \) is the type II error rate of the most powerful test with significance level \( \alpha \) on the hypotheses

\[
H_0 : X \sim \text{Lap}_p(0, 1) \quad \text{vs} \quad H_1 : X \sim \text{Lap}_p(\delta, 1).
\]

The log-likelihood ratio function is

\[
l(x) := \log \frac{f(x|\delta, b)}{f(x|0, b)} = \sum_{i=1}^{p} (|x_i| - |x_i - \delta_i|),
\]

\[32\]
where \( f(x|\delta, b) = (2b)^{-p} \exp \left( -\frac{1}{b} \sum_{i=1}^{p} |x_i - \delta_i| \right) \) is the density function of \( \text{Lap}_p(\delta, b) \). By the Neyman-Pearson lemma, the most powerful test at level \( \alpha \) has the form of

\[
\phi_{K, \gamma}(X) = 1(l(X) > K) + \gamma \cdot 1(l(X) = K)
\]

for some \( K \) and \( \gamma \in [0, 1] \). Here, \( \phi_{K, \gamma} \) is a randomized test function, and \( K \) and \( \gamma \) are determined by \( \alpha \) to satisfy \( \alpha = \frac{\gamma \cdot 1}{2} e^{-\delta} \in [0, \frac{1}{2} e^{-\delta}] \).

For \( p = 1 \) and \( p = 2 \), we derive a closed form of (39). Evaluating (39) for \( p \geq 3 \) can be done, but its expression turns out to be too complex and has little practical relevance.

**C.1.1 Univariate case**

We first consider the case of \( p = 1 \) to calibrate the univariate Laplace noise to \( L_1 \) sensitivity of \( \theta \) by calculating the trade-off function between univariate Laplace distributions. By (39), we can derive the trade-off function between univariate Laplace distributions. First, the log-likelihood ratio is

\[
l(x) = |x| - |x - \delta| = \begin{cases} \delta & \text{if } x \geq \delta, \\ 2x - \delta & \text{if } 0 \leq x < \delta, \\ -\delta & \text{otherwise}. \end{cases}
\]

Originally, \( \phi_{K, \gamma} \) was determined as the most powerful level-\( \alpha \) test given \( \alpha \). Conversely, if \( K \) and \( \gamma \in [0, 1] \) are given, \( \alpha \) is uniquely determined. With this idea, we can derive the trade-off function as follows.

(i) \( K > \delta \): The most powerful test is given as \( \phi = 0 \). In this case, the corresponding type I error is 0. So, the trade-off function value at \( \alpha = 0 \) is \( T_{\text{Lap}_1, \delta}(0) = 1 \).

(ii) \( K = \delta \): Since \( \mathbb{P}(l(X) = K) > 0 \), we need randomization. Fix a \( \gamma \in [0, 1] \). The test \( \phi_{K, \gamma} \) is the most powerful test at level \( \alpha_{\gamma} \) where

\[
\alpha_{\gamma} = \gamma \cdot \mathbb{P}_{X \sim \text{Lap}_1(0, 1)}(X \geq \delta) = \gamma \cdot \frac{1}{2} e^{-\delta} \in [0, \frac{1}{2} e^{-\delta}].
\]

Figure 9: Surface plots for \( l(x) \).

(a) Graph of \( l(x) \) for univariate case with \( \delta = 1 \).

(b) Graph of \( l(x_1, x_2) \) for bivariate case with \( \delta_1 = \delta_2 = 1 \).

The trade-off function between the two \( p \)-dimensional Laplace distributions can be written

\[
T_{\text{Lap}_p, \delta}(\alpha) = \mathbb{E}_{X \sim \text{Lap}_p(\delta, 1)} (1 - \phi_{K, \gamma}(X)) = \mathbb{P}_{X \sim \text{Lap}(\delta, 1)} (l(X) < K) + (1 - \gamma) \cdot \mathbb{P}_{X \sim \text{Lap}(\delta, 1)} (l(X) = K).
\]

For \( p = 1 \) and \( p = 2 \), we derive a closed form of (39).
Conversely, for $0 < \alpha \leq \frac{1}{2}e^{-\delta}$, let $\gamma_\alpha = 2e^\delta \alpha \in (0, 1]$. Then the most powerful test at level $\alpha \in (0, \frac{1}{2}e^{-\delta}]$ is $\phi_{K, \gamma_\alpha}$ and the trade-off function value at $\alpha$ is

$$T_{\text{Lap}_1, \delta}(\alpha) = \mathbb{P}_{X \sim \text{Lap}_1(\delta, 1)}(X < \delta) + (1 - \gamma_\alpha) \cdot \mathbb{P}_{X \sim \text{Lap}_1(\delta, 1)}(X \geq \delta)$$

$$= 1 - \frac{1}{2}\gamma_\alpha = 1 - e^\delta \alpha.$$

(iii) $-\delta < K < \delta$: Since $\mathbb{P}(l(I(X) = K) = 0, \phi_{K, 0} = 1(l(I(X) > K)$ is the most powerful test at level $\alpha_K$ where

$$\alpha_K = \mathbb{P}_{X \sim \text{Lap}_1(0, 1)}(2X - \delta > K) = \frac{1}{2}e^{\frac{K+2}{\delta}} - (\frac{1}{2}e^{-\delta} - \frac{1}{2}).$$

Conversely, for $\frac{1}{2}e^{-\delta} < \alpha < \frac{1}{2}$, $\phi_{K, 0}$ is the most powerful test at level $\alpha$ where $K_\alpha = -\delta - 2\log(2\alpha) \in (-\delta, \delta)$ and the trade-off function value at $\alpha$ is

$$T_{\text{Lap}_1, \delta}(\alpha) = \mathbb{P}_{X \sim \text{Lap}_1(\delta, 1)}(2X - \delta < K_\alpha) = \frac{1}{2}e^{\frac{K_\alpha - 2}{\delta}} = \frac{e^{-\delta}}{4\alpha}.$$

By (i)-(iii) and the symmetry of the trade-off function, $T_{\text{Lap}_1, \delta}$ is given as

$$T_{\text{Lap}_1, \delta}(\alpha) = \begin{cases} 1 - e^\delta \alpha & \text{if } \alpha < \frac{1}{2}e^{-\delta}, \\ e^{-\delta} \quad & \text{if } \frac{1}{2}e^{-\delta} \leq \alpha < \frac{1}{2}, \\ e^{\delta}(1-\alpha) & \text{otherwise.} \end{cases}$$

(40)

Remark 2. The above expression [40] was firstly presented in Proposition A.6 of [Dong et al., 2022]. In general, $T(\xi, t + \xi)(\alpha) = F(F^{-1}(1 - \alpha) - t)$ holds for every $t > 0$ if and only if the density of a random variable $\xi$ is log-concave (Proposition A.3 of [Dong et al., 2022]). Here, $F$ is the distribution function of $\xi$. Since the density of univariate Laplace distribution is log-concave, the direct calculation of $F(F^{-1}(1 - \alpha) - t)$ when $\xi \sim \text{Lap}(0, 1)$ results in $T_{\text{Lap}_1, \delta}$ of [40]. Unlike the approach of [Dong et al.], our derivation directly use the definition of trade-off function, and our approach can be applied to more higher dimensional case.

C.1.2 Bivariate Laplace mechanism

Let $p = 2$. A primary importance of this bivariate case is that the trade-off function of mechanisms perturbing contingency tables (of any dimension) can be handled using the $p = 2$ results, as argued in Section 3.2.

Following essentially the same steps used in obtaining [40], but with messier computations, we derive the following trade-off function between bivariate Laplace distributions.

Lemma C.1. For $\delta = (\delta_1, \delta_2)$ with $\delta_1 \geq \delta_2 \geq 0$,

$$T_{\text{Lap}_2, \delta}(\alpha) = \begin{cases} -e^{\delta_1 + \delta_2} \alpha + 1 & \text{if } 0 \leq \alpha \leq \frac{1}{4}e^{-\delta_1 - \delta_2}, \\ \frac{1}{4}e^{-C_\delta(\alpha)}(3 + C_\delta(\alpha)) & \text{if } \frac{1}{4}e^{-\delta_1 - \delta_2} \leq \alpha \leq \frac{1}{4}e^{-\delta_1}(1 + \delta_2), \\ -e^{\delta_1 - \delta_2} \alpha + \frac{1}{4}e^{-\delta_2}(2 + \delta_2) & \text{if } \frac{1}{4}e^{-\delta_1}(1 + \delta_2) \leq \alpha \leq \frac{1}{4}e^{-\delta_1}(2 + \delta_2), \\ \frac{1}{16\alpha}e^{-\delta_1 - \delta_2}(2 + \delta_2) & \text{if } \frac{1}{4}e^{-\delta_1}(2 + \delta_2) \leq \alpha \leq \frac{1}{4}e^{-\delta_1 - \delta_2}(2 + \delta_2), \end{cases}$$

(41)

and $T_{\text{Lap}_2, \delta}(\alpha)$ for $\alpha > \frac{1}{4}e^{-\delta_1 - \delta_2}(2 + \delta_2)$ is determined by the symmetry. Here, $C_\delta(\alpha) := W(4\alpha e^{1+\delta_1+\delta_2}) - 1$, and $W(\cdot)$ is the Lambert $W$ function.

A proof of Lemma C.1 is given in Section C.1.3.

For a given $\delta = (\delta_1, \delta_2)$ where $\delta_1 \geq \delta_2 > 0$, consider a reparameterization $\lambda_1 = \delta_1 + \delta_2 = ||\delta||_1$ and $\lambda_2 = \delta_1 - \delta_2$, so that

$$\delta^\top = (\delta_1, \delta_2) = \left(\frac{\lambda_1 + \lambda_2}{2}, \frac{\lambda_1 - \lambda_2}{2}\right).$$

Write $\tilde{T}_\lambda := T_{\text{Lap}_2, (\frac{\lambda_1 + \lambda_2}{2}, -\frac{\lambda_1 + \lambda_2}{2})^\top}$ for the trade-off function $T_{\text{Lap}_2, \delta}$, parameterized with respect to $\lambda = (\lambda_1, \lambda_2)^\top$. The following observation is useful:

34
Lemma C.2. Given \( \lambda_1 > 0 \) fixed, for any \( \alpha \in (0, 1), \tilde{T}_{\lambda}(\alpha) \) is a monotone decreasing function of \( \lambda_2 \).

A proof of Lemma C.2 is given in Section C.1.3.

We are interested in the evaluation of \( L_2(b) = \inf_{\delta \in S_b} T(Lap_2(0, 1), Lap_2(\delta, 1)) \), where \( \delta = (\theta(S) - \theta(S'))/b \). Then

\[
L_2(b) = \inf_{\delta \in S_{b_0}} T(Lap_2(0, 1), Lap_2(\delta, 1)).
\]

Without loss of generality, we can assume that any \( \delta \in S_{b_0} \) satisfies \( \delta_1 \geq \delta_2 \geq 0 \). To see this, let

\[
|S_{b_0}| := \left\{ \left( \max(\theta_1(S) - \theta_1(S')_1), \min(\theta_1(S) - \theta_1(S')) : S \sim S', S, S' \in \mathcal{X} \right) \right\},
\]

and observe that for any \( \delta \in S_{b_0} \), there exists \( \delta_0 \in |S_{b_0}| \) such that \( T(Lap_2(0, 1), Lap_2(\delta, 1)) = T(Lap_2(0, 1), Lap_2(\delta_0, 1)) \). Define

\[
S_\lambda = \{ (\delta_1 + \delta_2, \delta_1 - \delta_2) : (\delta_1, \delta_2) \in |S_{b_0}| \},
\]

which may be called the sensitivity set of \( \theta \) with respect to the “\( \lambda \)-parameterization.” If \( \Delta_1 = \Delta_1(\theta; \mathcal{X}^n) \), then for any \( (\lambda_1, \lambda_2) \in S_\lambda \), \( \lambda_1 \in [0, \Delta_1/b] \).

For each \( \lambda_1 \geq 0 \), if \( (\lambda_1, \lambda_2) \in S_\lambda \) for some \( 0 \leq \lambda_2 \leq \lambda_1 \), define \( \nabla(\lambda_1) = \sup \{ \lambda_2 : (\lambda_1, \lambda_2) \in S_\lambda \} \). Then

\[
L_2(b) = \inf_{\delta \in S_{b_0}} T(Lap_2(0, 1), Lap_2(\delta, 1)) \leq \lambda_1 \in [0, \Delta_1/b] \lambda_2 \in [0, \lambda_1] 
\]

\[
= \inf_{\lambda_1 \in [0, \Delta_1/b]} \inf_{\lambda_2 \in [0, \lambda_1]} \tilde{T}_{\lambda}(\lambda_1, \nabla(\lambda_1)) \leq \lambda_1 \in [0, \Delta_1/b] \lambda_2 \in [0, \lambda_1] 
\]

\[
= \inf_{\lambda_1 \in [0, \Delta_1/b]} \tilde{T}_{\lambda}(\lambda_1, \nabla(\lambda_1)) \leq \lambda_1 \in [0, \Delta_1/b] \lambda_2 \in [0, \lambda_1] 
\]

Summarizing the above discussion, we conclude that evaluating \( L_2(b) \) requires an exact specification of \( S_{b_0} \).

Lemma C.3. Let \( p = 2 \), and \( \theta \) and \( S_{b_0} \) be given and \( \Delta_1 = \Delta_1(\theta; \mathcal{X}^n) \). Then the value of the trade-off function \( L_2(b) : [0, 1] \to [0, 1] \) at \( \alpha \in [0, 1] \) is \( \inf_{\lambda_1 \in [0, \Delta_1/b]} \tilde{T}_{\lambda}(\lambda_1, \nabla(\lambda_1))(\alpha) \).

Note that since \( \nabla(\lambda_1) \leq \lambda_1 \) for any \( S_\lambda \), we have

\[
L_2(b) = \inf_{\lambda_1 \in [0, \Delta_1/b]} \tilde{T}_{\lambda}(\lambda_1, \nabla(\lambda_1)) \geq \inf_{\lambda_1 \in [0, \Delta_1/b]} \tilde{T}_{\lambda}(\lambda_1, \lambda_1) \geq \inf_{\delta_1 \leq \Delta_1/b} T(Lap_2(0, 1), Lap_2((\delta_1, 0), 1)) = \inf_{\delta_1 \leq \Delta_1/b} T(Lap_1(0, 1), Lap_1(\delta_1, 1)) = T(Lap_1(0, 1), Lap_2(\Delta_1/b, 1)).
\]

In the second equality above, we used the fact that \( \lambda_2 = \lambda_1 \) if and only if \( \delta_1 = \lambda_1 \) and \( \delta_2 = 0 \). This gives proof for Lemma C.3 but only for the case \( p = 2 \).

C.1.3 Proofs of Lemmas C.1 and C.2

Proof of Lemma C.2. We consider the case where \( \delta_1 > \delta_2 \geq 0 \). In the case of \( \delta_1 = \delta_2 \), it is verified in the same way, and it also can be confirmed that results are compatible with the case of \( \delta_1 > \delta_2 \).
and examples of its values by $x = (x_1, x_2)^T$ are denoted in Figure 10 with contour lines.

Let $\alpha(K, \gamma) := \mathbb{P}_{X \sim \text{Lap}_2(0, 1)}(l(X) > K) + \gamma \cdot \mathbb{P}_{X \sim \text{Lap}_2(0, 1)}(l(X) = K)$. First, we obtain $\alpha(K, \gamma)$ by the range of $K$. Next, we calculate the corresponding trade-off function value at $\alpha(K, \gamma)$ by $T_{\text{Lap}_2, \delta}(\alpha(K, \gamma)) = \mathbb{P}_{X \sim \text{Lap}_2(0, 1)}(l(X) < K) + (1 - \gamma) \cdot \mathbb{P}_{X \sim \text{Lap}_2(0, 1)}(l(X) = K)$.

(i) $K > \delta_1 + \delta_2 : \alpha(K, \gamma) = 0$, and $T_{\text{Lap}_2, \delta}(0) = 1$.

(ii) $K = \delta_1 + \delta_2 :$ For any $\gamma \in [0, 1]$,

$$\alpha(K, \gamma) = \gamma \cdot \mathbb{P}_{X \sim \text{Lap}_2(0, 1)}(X_1 \geq \delta_1, X_2 \geq \delta_2) = \frac{1}{4} e^{-\delta_1 - \delta_2} \gamma.$$

Then, $T_{\text{Lap}_2, \delta}(\alpha(K, \gamma)) = \frac{3}{4} + \frac{1}{4}(1 - \gamma)$. Conversely, for $0 \leq \alpha \leq \frac{1}{4} e^{-\delta_1 - \delta_2}$, by choosing $\gamma_\alpha = 4 e^{\delta_1 + \delta_2}$, we have

$$T_{\text{Lap}_2, \delta}(\alpha) = \frac{3}{4} + \frac{1}{4}(1 - \gamma_\alpha) = -e^{\delta_1 + \delta_2} \alpha + 1.$$

(iii) $\delta_1 - \delta_2 < K < \delta_1 + \delta_2$ :

$$\alpha(K, \gamma) = \mathbb{P}_{X \sim \text{Lap}_2(0, 1)} \left( X_1 + X_2 \geq \frac{\delta_1 + \delta_2 + K}{2}, X_1 \geq \frac{\delta_1 - \delta_2 + K}{2}, X_2 \geq \frac{-\delta_1 + \delta_2 + K}{2} \right)$$

$$= \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 + K}{2}} \left( 1 + \frac{\delta_1 + \delta_2 - K}{2} \right),$$

and

$$T_{\text{Lap}_2, \delta}(\alpha(K, \gamma)) = \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 - K}{2}} \left( 3 + \frac{\delta_1 + \delta_2 - K}{2} \right).$$
Conversely, for \( \frac{1}{4} e^{-\delta_1 - \delta_2} < \alpha < \frac{1}{4} e^{-\delta_1 (1 + \delta_2)} \),
\[
T_{\text{Lapz}, \delta}(\alpha) = \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 + K}{2} (3 + \frac{\delta_1 + \delta_2 - K}{2} \alpha)},
\]
where \( K_\alpha \) is a solution of \( \alpha = \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 + K}{2} (1 + \frac{\delta_1 + \delta_2 - K}{2})} \). By using Lambert W function, one can check that \( K_\alpha = \delta_1 + \delta_2 - 2W(4\alpha e^{1+\delta_1+\delta_2}) \). Then, \( T_{\text{Lapz}, \delta}(\alpha) = \frac{1}{4} e^{-C_\delta(\alpha) (3 + C_\delta(\alpha))} \), where \( C_\delta(\alpha) = W(4\alpha e^{1+\delta_1+\delta_2}) - 1 \).

(iv) \( K = \delta_1 - \delta_2 : \alpha(K, \gamma) = \frac{1}{4} e^{-\delta_1 (1 + \delta_2)} + \frac{1}{4} e^{-\delta_1 \gamma} \), and
\[
T_{\text{Lapz}, \delta}(\alpha(K, \gamma)) = \frac{1}{4} e^{-\delta_1 (2 + \delta_2)} + \frac{1}{4} e^{-\delta_2 (1 - \gamma)}.
\]

By using the same argument used in (ii), we have
\[
T_{\text{Lapz}, \delta}(\alpha) = -\frac{1}{4} e^{-\delta_1 - \delta_2} \alpha + \frac{1}{2} e^{-\delta_2} (2 + \delta_2)
\]
for \( \frac{1}{4} e^{-\delta_1 (1 + \delta_2)} \leq \alpha \leq \frac{1}{4} e^{-\delta_1 (2 + \delta_2)} \).

(v) \(-\delta_1 + \delta_2 < K < \delta_1 - \delta_2 : \alpha(K, \gamma) = \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 + K}{2} (2 + \delta_2)} \), and
\[
T_{\text{Lapz}, \delta}(\alpha(K, \gamma)) = \frac{1}{4} e^{-\frac{\delta_1 + \delta_2 - K}{2} (2 + \delta_2)}.
\]

Conversely, for \( \frac{1}{4} e^{-\delta_1 (2 + \delta_2)} < \alpha < \frac{1}{4} e^{-\delta_2 (2 + \delta_2)} \), it holds that
\[
T_{\text{Lapz}, \delta}(\alpha) = \frac{1}{16\alpha} e^{-\delta_1 - \delta_2} (2 + \delta_2)^2.
\]

Note that \( T_{\text{Lapz}, \delta} \) is symmetric on \( y = x \). Since
\[
\frac{1}{4} e^{-\delta_1 - \delta_2/2} (2 + \delta_2) \in \left[ \frac{1}{4} e^{-\delta_1 (2 + \delta_2)}, \frac{1}{4} e^{-\delta_2 (2 + \delta_2)} \right],
\]
(v) leads to
\[
T_{\text{Lapz}, \delta}(\frac{1}{4} e^{-\delta_1 - \delta_2/2} (2 + \delta_2)) = \frac{1}{4} e^{-\delta_1 - \delta_2/2} (2 + \delta_2).
\]

Thus, \( T_{\text{Lapz}, \delta}(\alpha) \) for \( \alpha > \frac{1}{4} e^{-\delta_1 - \delta_2/2} (2 + \delta_2) \) is determined by symmetry and (i)-(v).

\[\square\]

**Proof of Lemma [C.3]** Since the trade-off function is symmetric in the sense that it coincides with its inverse function, we need only to consider the left part where \( 0 \leq \alpha < \frac{1}{4} e^{-\frac{\lambda_2 + 2\Delta_1}{2}} (2 + \delta_2) \).

Let \( \lambda_1 \in (0, \Delta_1) \) be fixed. Rephrasing \( T_{\text{Lapz}, \delta}(\alpha) \) by \( \lambda_1 \) and \( \lambda_2 \), we get

\[
T(\lambda_2)(\alpha) := \tilde{T}_\lambda(\alpha) =
\begin{align*}
&-e^{\lambda_1 \alpha} + 1, &\text{if } \alpha \in [0, \frac{1}{4} e^{-\lambda_1}) =: I_1(\lambda_2) \equiv I_1 \\
&\frac{1}{4} e^{-C_{\lambda_1}(\alpha) (3 + C_{\lambda_1}(\alpha))}, &\text{if } \alpha \in \left[ \frac{1}{4} e^{-\lambda_1}, P_3(\lambda_2) \right) =: I_2(\lambda_2) \\
&-e^{\lambda_2 \alpha} + \frac{1}{2} e^{-\frac{\lambda_2 + 2\lambda_1}{2} (2 - \frac{\lambda_2 - \lambda_1}{2})}, &\text{if } \alpha \in [P_2(\lambda_2), P_3(\lambda_2)) =: I_3(\lambda_2) \\
&\frac{1}{16\alpha} e^{-\lambda_1 (2 - \frac{\lambda_2 - \lambda_1}{2})^2}, &\text{if } \alpha \in [P_3(\lambda_2), P_4(\lambda_2)) =: I_4(\lambda_2) \\
&\text{(symmetric part omitted)},
\end{align*}
\]

where
\[
C_{\lambda_1}(\alpha) := C_{\delta}(\alpha) = W(4\alpha e^{1+\lambda_1}) - 1 \\
P_2(\lambda_2) := \frac{1}{4} e^{-\frac{\lambda_1 + \lambda_2}{2} (1 - \frac{\lambda_2 - \lambda_1}{2})} \\
P_3(\lambda_2) := \frac{1}{4} e^{-\frac{\lambda_1 + \lambda_2}{2} (2 - \frac{\lambda_2 - \lambda_1}{2})} \\
P_4(\lambda_2) := \frac{1}{4} e^{-\frac{\lambda_1}{2} (2 - \frac{\lambda_2 - \lambda_1}{2})}.
\]

37
Now let $\lambda_2^{(1)} < \lambda_2^{(2)}$. Then, as $P_i$, $i = 2, 3, 4$ are decreasing with respect to $\lambda_2$, in particular we have that either $P_3(\lambda_2^{(0)}) \in I_3(\lambda_2^{(1)})$ or $P_3(\lambda_2^{(2)}) \in I_2(\lambda_2^{(1)})$. In both cases, we can see that

$$T(\lambda_2^{(1)})(\alpha) = T(\lambda_2^{(2)})(\alpha) \quad \text{for } \alpha \in [0, P_2(\lambda_2^{(2)})]$$

and

$$T(\lambda_2^{(1)})(\alpha) > T(\lambda_2^{(2)})(\alpha) \quad \text{for } \alpha \in I_4(\lambda_2^{(1)}) \cap I_4(\lambda_2^{(2)}) = [P_3(\lambda_2^{(1)}), P_4(\lambda_2^{(2)})].$$

Thus, we only need to check inequality for $\alpha \in [P_2(\lambda_2^{(2)}), P_3(\lambda_2^{(2)})]$.

First we regard the case where $P_3(\lambda_2^{(2)}) \in I_3(\lambda_2^{(1)})$. The trade-off functions are convex, and $T(\lambda_2^{(2)})(\alpha)$ is linear in $\alpha$ on $I_3(\lambda_2^{(2)})$. Due to (42), we obtain

$$T(\lambda_2^{(1)})(\alpha) \geq T(\lambda_2^{(2)})(\alpha) \quad \text{for } \alpha \in [P_2(\lambda_2^{(2)}), P_3(\lambda_2^{(2)})].$$

Therefore, we have $T(\lambda_2^{(1)})(P_3(\lambda_2^{(2)})) > T(\lambda_2^{(2)})(P_3(\lambda_2^{(2)}))$ and $T(\lambda_2^{(1)})(P_3(\lambda_2^{(1)})) > T(\lambda_2^{(2)})(P_3(\lambda_2^{(1)}))$. As $T(\lambda_2^{(1)})(\alpha)$ is linear on $[P_3(\lambda_2^{(2)}), P_3(\lambda_2^{(1)})]$, we get that

$$T(\lambda_2^{(1)})(\alpha) \geq T(\lambda_2^{(2)})(\alpha) \quad \text{for } \alpha \in [P_3(\lambda_2^{(2)}), P_3(\lambda_2^{(1)})].$$

For the case of $P_3(\lambda_2^{(2)}) \in I_2(\lambda_2^{(1)})$, let us show that there exists a finite sequence $\{\lambda_{2,i}\}_{i=0}^n$, $n \geq 2$ of

$$\lambda_2^{(1)} = \lambda_{2,0} \leq \lambda_{2,1} \leq \cdots \leq \lambda_{2,n-1} \leq \lambda_{2,n} = \lambda_2^{(2)}$$

such that

$$P_3(\lambda_{2,i}) \in I_3(\lambda_{2,i-1}), \quad i = 1, \ldots, n.$$  

Then we have $T(\lambda_{2,i-1})(\alpha) > T(\lambda_{2,i})(\alpha), \quad i = 1, \ldots, n$ for $\alpha \in [0, 1]$, so that $T(\lambda_2^{(1)})(\alpha) = T(\lambda_{2,0})(\alpha) > T(\lambda_{2,n})(\alpha) = T(\lambda_2^{(2)})(\alpha), \alpha \in [0, 1]$.

Consider $\lambda'_2 > \lambda_2^{(1)}$. We seek the range of $\lambda'_2$ to satisfy $P_3(\lambda'_2) \in I_3(\lambda_2^{(1)})$. Let $c := \frac{\lambda_1 - \lambda_2^{(1)}}{2} > 0$ and $\lambda'_2 = \lambda_2^{(1)} + 2c, \quad c \in (0, c)$. Then, we obtain

$$P_3(\lambda'_2) \in I_3(\lambda_2^{(1)})$$

$$\Leftrightarrow \frac{1}{4} e^{-\frac{\lambda'_2 + c}{2}} (2 + \frac{\lambda_1 - \lambda'_2}{2}) \geq \frac{1}{4} e^{-\frac{\lambda_2^{(1)} + \lambda_1}{2}} (1 + \frac{\lambda_1 - \lambda_2^{(1)}}{2})$$

$$\Leftrightarrow e^{-c} (2 + \frac{\lambda_1 - \lambda_2^{(1)}}{2} - c) \geq 1 + \frac{\lambda_1 - \lambda_2^{(1)}}{2}$$

$$\Leftrightarrow 2 + c - c \geq (1 + c)e^c$$

$$\Leftrightarrow c \leq 2 + c - W((1 + c)e^{2+c})$$

Let $h(x) := 2 + x - W((1 + x)e^{2+x})$. As $h(c) > 0$, any $\lambda'_2 \in (\lambda_2^{(1)}, \lambda_2^{(1)} + 2h(c))$ satisfies $P_3(\lambda'_2) \in I_3(\lambda_2^{(1)})$. Let $\lambda_{2,1} := \lambda_2^{(1)} + h(c)$.

We also have that

$$\frac{\partial h(x)}{\partial x} = \frac{1 - e^{h(x)}}{1 + (1 + x)e^{h(x)}} < 0$$

for all $x > 0$. This implies, as $\frac{\lambda_1 - \lambda_{2,1}}{2} < \frac{\lambda_1 - \lambda_2^{(1)}}{2} = c$, that either $\lambda_{2,1} + h(c) \geq \lambda_2^{(2)}$ or $P_3(\lambda_{2,1} + h(c)) \in I_3(\lambda_{2,1})$ by applying the logic of (44) again. In the former case, $n = 2$ and $P_3(\lambda_2^{(2)}) \in I_3(\lambda_{2,1})$ so the proof is done. In the latter case, let $\lambda_{2,2} = \lambda_{2,1} + h(c)$ and construct $\{\lambda_{2,i}\}_{i=0}^n$ inductively as $\lambda_{2,i+1} = \lambda_{2,i} + h(c)$ until $\lambda_{2,n-1} + h(c) \geq \lambda_2^{(2)}$. 

\[\square\]
C.2 Proofs for Section 3

C.2.1 Proof of Lemma 9

Proof of Lemma 9. (i) Suppose that a randomized mechanism $M$ is $\varepsilon$-DP for some $\varepsilon > 0$. Then, we have $\inf_{S \sim S'} T(M(S), M(S'))(\alpha) \geq T_{\varepsilon \text{-DP}}$. Let $\mu_\varepsilon = 2\Phi^{-1}\{e^\varepsilon/(e^\varepsilon + 1)\}$. To show $M$ is $\mu$-GDP for any $\mu \geq \mu_\varepsilon$ it is enough to show that $T_{\varepsilon \text{-DP}} \geq G_{\mu_\varepsilon}$ since $G_\mu$ is decreasing in $\mu$. Observe that

$$G_{\mu_\varepsilon} \left(\frac{1}{1 + e^\varepsilon}\right) = \Phi \left(\Phi^{-1} \left(\frac{e^\varepsilon}{1 + e^\varepsilon}\right) - 2\Phi^{-1} \left(\frac{e^\varepsilon}{1 + e^\varepsilon}\right)\right)$$

$$= \Phi \left(-\Phi^{-1} \left(\frac{e^\varepsilon}{1 + e^\varepsilon}\right)\right)$$

$$= 1 - \Phi \left(\Phi^{-1} \left(\frac{e^\varepsilon}{1 + e^\varepsilon}\right)\right)$$

$$= \frac{1}{1 + e^\varepsilon}.$$

From the convexity of any trade-off function, for any $\alpha \in [0, (1 + e^\varepsilon)^{-1}]$, we have $G_{\mu_\varepsilon}(\alpha) \leq l(\alpha)$, where $l(\alpha)$ is function of line segment passes through $(0, 1)$ to $((1 + e^\varepsilon)^{-1}, (1 + e^\varepsilon)^{-1})$. In fact, simple calculation shows that $l(\alpha) = T_{\varepsilon \text{-DP}}(\alpha)$ for $\alpha \in [0, (1 + e^\varepsilon)^{-1}]$. Finally, trade-off functions are symmetric on $y = x$, we have, for any $\alpha \in [0, 1]$

$$G_{\mu_\varepsilon}(\alpha) \leq T_{\varepsilon \text{-DP}}(\alpha).$$

(ii) Suppose that $M$ is $\varepsilon$-DP where $\varepsilon \leq \varepsilon_\mu$. Note that $e^\varepsilon/(e^\varepsilon + 1)$ is increasing in $\varepsilon > 0$, and

$$2\Phi^{-1} \left(\frac{e^\varepsilon}{1 + e^\varepsilon}\right) \leq 2\Phi^{-1} \left(\frac{e^\mu}{1 + e^\mu}\right)$$

$$= 2\Phi^{-1} \left(\frac{\Phi(\mu/2)/\Phi(-\mu/2)}{1 + \Phi(\mu/2)/\Phi(-\mu/2)}\right)$$

$$= 2\Phi^{-1} (\Phi(\mu/2))$$

$$= \mu.$$

From the part (i) of the Lemma, $M$ is $\mu$-GDP. \qed

C.2.2 Proof of Lemma 10

Proof of Lemma 10. From the previous remark, for any $t > 0$ we have $T_{\text{Lap,} t}(\alpha) = F(F^{-1}(1 - \alpha) - t)$, where $F$ is the distribution of Lap(0,1). For a fixed $\alpha \in (0, 1)$, $F(F^{-1}(1 - \alpha) - t)$ is decreasing in $t$. Thus, for any fixed $\alpha \in (0, 1)$, if $t \geq t' > 0$

$$T_{\text{Lap,} t}(\alpha) \leq T_{\text{Lap,} t'}(\alpha).$$

Since the trade-off function $L_{\text{Lap}}(b)$ is defined over the univariate Laplace mechanism, we have

$$L_{\text{Lap}}(b) = \inf_{S \sim S'} T(M_{\text{Lap}}(S; b), M_{\text{Lap}}(S'; b))$$

$$= \inf_{S \sim S'} T(\text{Lap}(0, 1), \text{Lap}(|\theta(S) - \theta(S')|/b, 1))$$

$$= T(\text{Lap}(0, 1), \text{Lap}(\sup_{S \sim S'} |\theta(S) - \theta(S')|/b, 1))$$

$$= T(\text{Lap}(0, 1), \text{Lap}(\Delta_1/b, 1))$$

$$= T(\text{Lap}(0, 1), \text{Lap}(\delta, 1)).$$

The proof is completed by \cite{40}. \qed
C.2.3 Proof of Proposition 11

Proof of Proposition 11 relies on the following lemma, which answers the question: For which values of $\delta$, $T_{\text{Lap}_1, \delta}$ is greater than $G_\mu$?

**Lemma C.4.** For a $\mu > 0$, let $\delta = -2\log\{2\Phi(-\mu/2)\}$. Then

$$T_{\text{Lap}_1, \delta}(\alpha) > G_\mu(\alpha)$$

for any $\alpha \in (0, 1)$, except for $\alpha_0 = \Phi(-\mu/2)$, where $T_{\text{Lap}_1, \delta}(\alpha_0) = G_\mu(\alpha_0)$. Moreover, For any $\delta' > \delta$, $T_{\text{Lap}_1, \delta'}(\alpha_0) < G_\mu(\alpha_0)$.

**Proof.** From (10), we have

$$T_{\text{Lap}_1, \delta}(\alpha) = \begin{cases} 1 - \frac{1}{4\Phi(-\mu/2)} & \text{if } \alpha < 2\Phi^2(-\mu/2), \\ \Phi^2(-\mu/2)/\alpha & \text{if } 2\Phi^2(-\mu/2) \leq \alpha < \frac{1}{2}, \\ 4\Phi^2(-\mu/2)(1 - \alpha) & \text{otherwise}. \end{cases}$$

(Here, $\Phi^2(t) := \{\Phi(t)\}^2$.) Since $\alpha_0 \in [2\Phi^2(-\mu/2), 1/2)$, it can be easily checked that

$$T_{\text{Lap}_1, \delta}(\alpha_0) = \alpha_0 = G_\mu(\alpha_0).$$

Next, we will show that $T_{\text{Lap}_1, \delta}(\alpha) > G_\mu(\alpha)$ for any other choice of $\alpha$.

First, consider $\alpha \in (\alpha_0, 1/2]$. The derivatives become

$$\frac{\partial T_{\text{Lap}_1, \delta}}{\partial \alpha}(\alpha) = -\frac{\Phi^2(-\mu/2)}{\alpha^2},$$

and

$$\frac{\partial G_\mu(\alpha)}{\partial \alpha}(\alpha) = -e^{\mu\Phi^{-1}(1-\alpha)} - \frac{1}{2} \mu^2.$$

From the definition of $\alpha_0$, it holds that

$$\frac{\partial T_{\text{Lap}_1, \delta}}{\partial \alpha}(\alpha_0) = \frac{\partial G_\mu(\alpha)}{\partial \alpha}(\alpha_0).$$

The difference between two derivatives is

$$\left(\frac{\partial T_{\text{Lap}_1, \delta}}{\partial \alpha} - \frac{\partial G_\mu(\alpha)}{\partial \alpha}\right)(\alpha) = -\frac{\Phi^2(-\mu/2)}{\alpha^2} + e^{\mu\Phi^{-1}(1-\alpha)} - \frac{1}{2} \mu^2.$$

Observe that

$$\left(\frac{\partial T_{\text{Lap}_1, \delta}}{\partial \alpha} - \frac{\partial G_\mu(\alpha)}{\partial \alpha}\right)(\alpha) > 0$$

if and only if

$$g(\alpha) := \log(\alpha) - \frac{1}{2} \mu \Phi^{-1}(\alpha) - \frac{1}{4} \mu^2 - \log(-\mu/2) > 0. \quad (45)$$

After some calculation, one can see that $g(\alpha_0) = 0$. The derivative of $g$ becomes

$$g'(\alpha) = \frac{2}{\alpha} - \frac{\mu}{\phi(\Phi^{-1}(\alpha))}.$$

Note that $g'(\alpha_0) = \frac{2}{\alpha_0\phi(\mu/2)} \left(\phi(-\mu/2) + (-\mu/2)\Phi(-\mu/2)\right) > 0$. The last inequality holds from the well-known fact that $\phi(x) > x(1 - \Phi(x))$ for any $x > 0$. For $\alpha \in (\alpha_0, 1/2)$, reparameterize $\alpha$ by $\eta = -2\Phi^{-1}(\alpha)$ where $\eta \in (0, \mu)$, then $g'(\alpha)$ is reparameterized by $h(\eta)$ which is defined as

$$h(\eta) := \frac{2}{\Phi(-\eta/2)} - \frac{\mu}{\phi(-\eta/2)}.$$

Note that $h(\eta) > 0$ if and only if $\tilde{h}(\eta) := 2\Phi(-\eta/2) - \mu\Phi(-\eta/2) > 0$. Observe that the derivative of $\tilde{h}$ is positive: for any $0 < \eta < \mu$,

$$\frac{\partial \tilde{h}}{\partial \eta}(\eta) = \frac{1}{2} \phi(\frac{\eta}{2})(\mu - \eta) > 0.$$
So, \( h \) is an increasing function on \((0, \mu)\). Also, \( h(\mu) = 2\phi(-\mu/2) - \mu \Phi(-\mu/2) > 0 \), and we have \( h(\mu) > 0 \).

If \( h(0) > 0 \) then \( h(\eta) > 0 \) for any \( \eta \in (0, \mu) \), and \( h(\eta) > 0 \) as a consequence, \( g'(\alpha) > 0 \) on \([\alpha_0, 1/2]\). Since \( g(\alpha_0) = 0 \), we can conclude that \( g(\alpha) > g(\alpha_0) = 0 \) for \( \alpha \in (\alpha_0, 1/2) \). By (45), we can conclude that \( \left( \frac{\partial T_{\text{Lap}, \delta}}{\partial \alpha} - \frac{\partial G_{\mu}}{\partial \alpha} \right) (\alpha) \) strictly increasing on \((\alpha_0, 1/2)\), and then

\[
T_{\text{Lap}, \delta}(\alpha) - G_{\mu}(\alpha) > T_{\text{Lap}, \delta}(\alpha_0) - G_{\mu}(\alpha_0) = 0.
\]

Otherwise, suppose that \( h(0) \leq 0 \). Then there exists a \( \eta_0 \in [0, \mu) \) such that \( h(\eta) \leq 0 \) if \( \eta \leq \eta_0 \), and \( h(\eta) > 0 \) if \( \eta > \eta_0 \). Due to the reparametrization, we have \( g'(\alpha) \leq 0 \) if \( \alpha \geq \Phi(-\eta_0/2) \), and \( g'(\alpha) > 0 \) if \( \alpha < \Phi(-\eta_0/2) \). From (45),

\[
\left( \frac{\partial T_{\text{Lap}, \delta}}{\partial \alpha} - \frac{\partial G_{\mu}}{\partial \alpha} \right) (\alpha) > 0 \quad \text{if} \quad \alpha < \Phi(-\eta_0/2),
\]

\[
\left( \frac{\partial T_{\text{Lap}, \delta}}{\partial \alpha} - \frac{\partial G_{\mu}}{\partial \alpha} \right) (\alpha) \leq 0 \quad \text{if} \quad \alpha \geq \Phi(-\eta_0/2).
\]

Thus, \( T_{\text{Lap}, \delta} - G_{\mu} \) is strictly increasing in \( \alpha < \Phi(-\eta_0/2) \), and is decreasing in \( \alpha \geq \Phi(-\eta_0/2) \). However, we know that \((T_{\text{Lap}, \delta} - G_{\mu})(\alpha_0) = 0,\) and

\[
(T_{\text{Lap}, \delta} - G_{\mu})(1/2) = 2\Phi^2(-\mu/2) - \Phi(-\mu) > 0,
\]
due to the log-concavity of \( \Phi \). This shows that \( T_{\text{Lap}, \delta}(\alpha) - G_{\mu}(\alpha) > 0 \) if \( \alpha \in (\alpha_0, 1/2) \).

Next, suppose that \( \alpha \in (1/2, 1) \). It holds that \( T_{\text{Lap}, \delta}(1) = G_{\mu}(1) = 0 \). Note that \( T_{\text{Lap}, \delta}(\alpha) = e^{-\delta}(1 - \alpha) \) is the function of line segment connecting \((1/2, T_{\text{Lap}, \delta}(1/2))\) to \((1, 0)\). By the convexity, \( G_{\mu}(\alpha) < T_{\text{Lap}, \delta}(\alpha) \) for any \( \alpha \in (1/2, 1) \).

Lastly, if \( \alpha \in [0, \alpha_0) \), then \( G_{\mu}(\alpha) \leq T_{\text{Lap}, \delta}(\alpha) \) always holds since the trade-off functions are symmetric on \( y = x \).

Proof of Proposition 77 (i) By Lemma 10

\[
\mathcal{L}_1(b) = T \left( \text{Lap}(0, 1), \text{Lap} \left( \Delta_1 \frac{b}{\Delta_1}, 1 \right) \right).
\]

If \( b \geq b_{\mu}^{\lambda_{\alpha_1}} \), then by the monotonicity of \( \mathcal{L}_1(b) \) and Lemma C.4

\[
\mathcal{L}_1(b) \geq T \left( \text{Lap}(0, 1), \text{Lap} \left( \Delta_1 \frac{b}{b_{\mu}^{\lambda_{\alpha_1}}}, 1 \right) \right) = T \left( \text{Lap}(0, 1), \text{Lap} \left( -2 \log(2\Phi(-\frac{\mu}{2})), 1 \right) \right) \geq G_{\mu}.
\]

For the ‘only if’ part, suppose that \( b < b_{\mu}^{\lambda_{\alpha_1}} \). It follows that

\[
\mathcal{L}_1(b) < T \left( \text{Lap}(0, 1), \text{Lap} \left( -2 \log(2\Phi(-\frac{\mu}{2})), 1 \right) \right).
\]

However, from Lemma C.4 \( \mathcal{L}_1(b)(\alpha_0) < G_{\mu}(\alpha_0) \) where \( \alpha_0 = \Phi(-\mu/2) \). Thus, \( M_{\text{Lap}}(\cdot, b) \) is not \( \mu \)-GDP. These prove the first part of (i).

Next, we claim that \( b_{\mu}^{\lambda_{\alpha_1}} < b_{\mu}^{\delta} \). To prove the claim, it is enough to show that

\[
\log(\Phi(\mu/2)) - \log(\Phi(-\mu/2)) < -2 \log(2\Phi(-\mu/2)).
\]

The above inequality (46) holds if

\[
\log \left( 4\Phi \left( -\frac{\mu}{2} \right) \Phi \left( \frac{\mu}{2} \right) \right) < 0.
\]

So, if we show that \( \Phi(\mu/2)\Phi(\mu/2) < \frac{1}{4} \) for any \( \mu > 0 \) the claim is proved. Let \( x = \Phi(\mu/2) \). Then \( x \in (1/2, 1) \), and

\[
\Phi \left( -\frac{\mu}{2} \right) \Phi \left( \frac{\mu}{2} \right) = (1 - x)x = -\left( x - \frac{1}{2} \right)^2 + \frac{1}{4} < \frac{1}{4}.
\]

(ii) The proof can be easily derived from the first part of the proposition. \( \square \)
Proofs for Section 3.1.2

First, we introduce a notion of tensor product of trade-off functions. For two trade-off functions $f = T(P, Q)$ and $g = T(P', Q')$, the tensor product is defined as $f \otimes g := T(P \times P', Q \times Q')$. The tensor product makes it easy to write trade-off function between multivariate distributions. The following proposition and lemma are due to Dong et al. (2022) and used in the proof of Lemma 12.

**Proposition C.5** (Proposition D.1 of Dong et al. (2022)).

1. The tensor product $\otimes$ is commutative and associative.
2. If $g_1 \geq g_2$ then $f \otimes g_1 \geq f \otimes g_2$.
3. $f \otimes Id = Id \otimes f = f$.

The following lemma is useful in handling a lower bound of composition of trade-off functions.

**Lemma C.6** (Lemma A.5 of Dong et al. (2022)). Suppose $T(P, Q) \geq f$, $T(Q, R) \geq g$, then $T(P, R)(\alpha) \geq g(1 - f(\alpha))$ for any $\alpha \in [0, 1]$.

In the proof of Lemma 12, we importantly use the following Lemma, slightly modified from Lemma A.2 of Awan and Dong (2022), and apply it to the Laplace mechanism.

**Lemma C.7.** For $\delta_1, \delta_2 \geq 0$, consider two trade-off functions $f = T(\text{Lap}(0, 1), \text{Lap}(\delta_1, 1))$ and $g = T(\text{Lap}(0, 1), \text{Lap}(\delta_2, 1))$. Then $f \otimes g \geq T(\text{Lap}(0, 1), \text{Lap}(\delta_1 + \delta_2, 1))$.

**Proof.** Let $P = \text{Lap}(0, 1) \times \text{Lap}(0, 1)$, $Q = \text{Lap}(\delta_1, 1) \times \text{Lap}(0, 1)$, and $R = \text{Lap}(\delta_1, 1) \times \text{Lap}(\delta_2, 1)$. Observe that

$$ f = f \otimes Id \quad \text{(by Proposition C.5)} $$

$$ = T(\text{Lap}(0, 1), \text{Lap}(\delta_1, 1)) \otimes T(\text{Lap}(0, 1), \text{Lap}(0, 1)) $$

$$ = T(P, Q) \quad \text{(by the definition of tensor product)} $$

and similarly, $g = T(Q, R)$. However, $(f \otimes g)(\alpha) = T(P, R)$, and then Lemma C.6 implies that

$$(f \otimes g)(\alpha) = T(P, R) \geq g(1 - f(\alpha))$$

for any $\alpha \in (0, 1)$. Let $F$ be the distribution of $\text{Lap}(0, 1)$. From Remark 2, we have

$$ g(1 - f(\alpha)) = F(F^{-1}(1 - (1 - f(\alpha))) - \delta_2) $$

$$ = F(F^{-1}(F(F^{-1}(1 - (1 - f(\alpha))) - \delta_1))) - \delta_2) $$

$$ = F(F^{-1}(1 - \alpha) - \delta_1) - \delta_2 $$

$$ = T(\text{Lap}(0, 1), \text{Lap}(\delta_1 + \delta_2, 1)). $$

This completes the proof.

Now, we are ready to prove Lemma 12.

**Proof of Lemma 12.** We first prove (23). Fix any $\delta = (\delta_1, \ldots, \delta_p) \in \mathbb{R}^p$. By symmetry of Laplace distribution and trade-off function, we may assume that $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_p \geq 0$ without loss of generality. Consider $f_1 = T(\text{Lap}(0, 1), \text{Lap}(\delta_1, 1))$ and $f = T(\text{Lap}_p(0_p, 1), \text{Lap}(\delta, 1))$. To prove the lemma, we use the mathematical induction on $p$. When $p = 1$, it holds trivially, and Lemma C.7 implies that (23) also holds when $p = 2$. Now, suppose that the lemma holds for $p = k$ ($k \geq 2$).

Then

$$ f = f_1 \otimes f_2 \otimes \cdots \otimes f_{k+1} $$

$$ = f_1 \otimes (f_2 \otimes \cdots \otimes f_{k+1}) \quad \text{(by Proposition C.5)} $$

$$ \geq f_1 \otimes T_{\text{Lap}_p(\delta_2 + \cdots + \delta_{k+1})} \quad \text{(by the induction assumption and Proposition C.5)} $$

$$ \geq T_{\text{Lap}_p(\delta_1 + \delta_2 + \cdots + \delta_{k+1})} \quad \text{(by Lemma C.7)} $$

$$ = T(\text{Lap}(0, 1), \text{Lap}(\|\delta\|_1, 1)). $$
Suppose that \( \delta = (\delta_1, 0, \ldots, 0) \) so that \( \delta_1 \neq 0 \) and other elements in \( \delta \) are all zero. Then, the trade-off function becomes

\[
T(\text{Lap}_p(0, 1), \text{Lap}_p(\delta, 1)) = T(\text{Lap}_1(0, 1), \text{Lap}_1(\delta_1, 1)) = T(\text{Lap}_1(0, 1), \text{Lap}_1(\|\delta\|_1, 1)).
\]

This proves (i).

To prove (ii), suppose that at least two elements in \( \delta = (\delta_1, \ldots, \delta_p) \) are nonzero. We may assume that \( \delta_i > 0 \) for all \( i = 1, \ldots, p \) and \( p \geq 2 \). First, consider the case of \( p = 2 \). More precisely, let \( \delta = (\delta_1, \delta_2) \) where \( \delta_1 \geq \delta_2 > 0 \). Note that \( \alpha^{(1)}_0 = \frac{1}{4}e^{-\frac{\|\delta\|_1}{4}} \), and \( \alpha^{(2)}_0 = \frac{1}{2}e^{-\frac{\|\delta\|_1}{8}}(2 + \delta_2) \) are fixed points of \( T_{\text{Lap}_1, \|\delta\|_1}, \) and \( T_{\text{Lap}_2, \delta} \), respectively, i.e., \( T_{\text{Lap}_1, \|\delta\|_1}(\alpha^{(1)}_0) = \alpha^{(1)}_0 \), and \( T_{\text{Lap}_2, \delta}(\alpha^{(2)}_0) = \alpha^{(2)}_0 \). Since \( \delta_2 > 0 \), it follows that

\[
\alpha^{(1)}_0 = \frac{1}{4}e^{-\frac{\|\delta\|_1}{4}}(2 + \delta_2) > \frac{1}{2}e^{-\frac{\|\delta\|_1}{8}} = \alpha^{(2)}_0.
\]

Then

\[
T_{\text{Lap}_1, \|\delta\|_1}(\alpha^{(1)}_0) < T_{\text{Lap}_2, \delta}(\alpha^{(2)}_0) \leq T_{\text{Lap}_2, \delta}(\alpha^{(1)}_0).
\]

By the continuity of \( T_{\text{Lap}_2, \delta} - T_{\text{Lap}_1, \|\delta\|_1} \), there exists an interval \((a, b)\) such that contains \( \alpha^{(1)}_0 \), and for any \( \alpha \in (a, b) \),

\[
(T_{\text{Lap}_2, \delta} - T_{\text{Lap}_1, \|\delta\|_1})(\alpha) > 0.
\]

Next, assume \( p \geq 3 \), and let \( \delta = (\delta_1, \ldots, \delta_p) \) where \( \delta_i > 0 \) for all \( i \). Denote \( \delta = (\delta_1, \ldots, \delta_p) \), where \( \delta_+ = (\delta_2, \ldots, \delta_p) \). Then

\[
T_{\text{Lap}_p, \delta} = T_{\text{Lap}_1, \delta_1} \otimes T_{\text{Lap}_{p-1}, \delta_+}
\geq T_{\text{Lap}_1, \delta_1} \otimes T_{\text{Lap}_{p-1}, \|\delta_+\|_1}
\geq T_{\text{Lap}_2, (\delta_1, \|\delta_+\|_1)}
\]

Since \( \delta_1 \neq 0 \) and \( \|\delta_+\|_1 \neq 0 \), from the case of \( p = 2 \), it follows that there exists an interval \((a, b)\), \( 0 < a < b < 1 \) such that, for any \( \alpha \in (a, b) \),

\[
T_{\text{Lap}_1, \|\delta_+\|_1}(\alpha) > T_{\text{Lap}_1, \|\delta_+\|_1}(\alpha) = T_{\text{Lap}_1, \|\delta\|_1}(\alpha).
\]

Thus, \( T_{\text{Lap}_1, \|\delta\|_1}(\alpha) \). Also, \((a, b)\) contains \( \|\delta\|_1 \). This completes the proof of (ii) of the lemma. \( \square \)

**Proof of Theorem 13.** (i) We first show the ‘if’ part. We have already observed that for any given \( \text{M}_{\text{Lap}_p(\cdot; b)} \) of \( \theta \),

\[
\mathcal{L}_p(b; \theta, X^n) \geq T((\text{Lap}(0, 1), \text{Lap}(\Delta_1(\theta, X^n)/b, 1))).
\]

Since \( b \geq b^\Delta_{\mu} \geq b^\Delta_{\mu}(\theta, X^n) \), Proposition 11(ii) implies \( T((\text{Lap}(0, 1), \text{Lap}(\Delta_1(\theta, X^n)/b, 1)) \geq G_\mu \), as required.

The ‘only if’ part can be verified by showing the contrapositive: If \( b < b^\Delta_{\mu} \), then there exists a statistic \( \theta \) with \( \Delta_1(\theta, X^n) = \Delta_1 \) such that \( \text{M}_{\text{Lap}_p(\cdot; b)} \) does not satisfy \( \mu \)-GDP.

Let \( \theta \) and \( X^n \) be such that for some \( S, S' \in X^n \) satisfying \( S \sim S', \theta(S) - \theta(S') = (\Delta_1, 0, \ldots, 0) \). Then

\[
\mathcal{L}_p(b; \theta, X^n) = \inf_{S \sim S'} T((\text{Lap}_p((\theta(S) - \theta(S'))/b, 1), \text{Lap}_p(0, 1)) \leq T((\text{Lap}_p((\Delta_1/b, 0, \ldots, 0, 1), \text{Lap}_p(0, 1)),
\]

and by Lemma (23), we have \( \mathcal{L}_p(b; \theta, X^n) \leq T((\text{Lap}(\Delta_1/b), \text{Lap}(0, 1)). \) By Proposition 11 for any \( b < b^\Delta_{\mu} \), there exists \( \alpha \in (0, 1) \) such that

\[
\mathcal{L}_p(b; \theta, X^n)(\alpha) \leq T((\text{Lap}(\Delta_1/b), \text{Lap}(0, 1))(\alpha) < G_\mu(\alpha).
\]

This shows that \( \text{M}_{\text{Lap}_p(\cdot; b)} \), perturbing \( \theta \), is not \( \mu \)-GDP for any \( b < b^\Delta_{\mu} \).

(ii) This can be easily derived from the first part of the theorem.
(iii) Consider a statistic $\theta$ such that the sensitivity space $S_\theta$ is

$$S_\theta = \left\{ \frac{\Delta_1}{2}(e_i + e_j) : i, j = 1, \ldots, p \right\}.$$  

Then, by the process similar to (23), we obtain

$$L_\mu(b) = T\left( \text{Lap}_2(0,1), \text{Lap}_2\left(\frac{\Delta_1}{2b}, 1, 1\right)\right)$$

From the above inequality and Lemma C.4, we have

$$L_\mu(b^b_{\Delta^1})(\alpha) > G_\mu(\alpha),$$

for any $\alpha \in (0, 1)$. Define a function $F(b, \alpha) : (0, \infty) \times [0, 1] \to \mathbb{R}$ by

$$F(b, \alpha) = L_\mu(b)(\alpha) - G_\mu(\alpha).$$

The inequality (47) is equivalent to $F(b^b_{\Delta^1}, \alpha) > 0$ for any $\alpha \in (0, 1)$. Since

$$\lim_{\alpha \to 0+} \frac{\partial G_\mu}{\partial \alpha}(\alpha) = -\infty,$$

and $L_\mu(b)(\alpha) = -e^{\Delta_1/b} + 1$ when $\alpha < \frac{1}{e} e^{-\Delta_1/b}$, there exists $c_1, c_2 > 0$ such that if $b \in (b^b_{\Delta^1} - c_1, b^b_{\Delta^1})$ and $\alpha \in (0, c_2)$ then $F(b, \alpha) > 0$. Due to the trade-off functions are symmetric on $y = x$, we have $F(b, \alpha) > 0$ if $\alpha \in (0, c_2) \cup (1 - c_2, 1)$ whenever $b \in (b^b_{\Delta^1} - c_1, b^b_{\Delta^1})$. On the other hand, since $[c_2, 1 - c_2]$ is compact, there exists a $c_3 > 0$ such that if $b \in (b^b_{\Delta^1} - c_3, b^b_{\Delta^1})$, and $\alpha \in [c_2, 1 - c_2]$, then $F(b, \alpha) > 0$.

Take $C = \min(c_1, c_3)$, and choose $b_0 \in (b^b_{\Delta^1} - C, b^b_{\Delta^1})$. Then, by the above arguments, we have $F(b_0, \alpha) > 0$ for any $\alpha \in (0, 1)$. This shows that, for any $\alpha \in (0, 1)$,

$$L_\mu(b_0)(\alpha) > G_\mu(\alpha).$$

This completes the proof of (iii). \qed

D Technical details omitted from Section 4

**Lemma D.1.** Let $\mu > 0$ Let $\theta : X^n \to \mathbb{R}^p$, and let $M_G$ and $M_{\text{Lap}} = M_{\text{Lap}}(\cdot, \Delta^1)$ be the ordinary Gaussian and Laplace mechanisms, respectively, both calibrated to satisfy $\mu$-GDP. Let $\Delta_r = \Delta_r(\theta; X^n)$ for $r \geq 1, 2$. For any $r \geq 1$,

(i) $L_r(M_{\text{Lap}}) = p(b^b_{\Delta^1})^r \Gamma(r + 1)$ and $L_r(M_G) = p(\Delta_2/\mu)^r \frac{2^r}{\sqrt{\pi}} \Gamma\left(\frac{p + 1}{2}\right)$

(ii) $\text{RE}_r(M_G, M_{\text{Lap}}) = \left(\frac{\Delta_1}{\Delta_2}\right)^r 2^{r+1} \left(\frac{1}{2} - \frac{p}{2} \log(2)\right)^r$

(iii) For each given $r$, $\text{RE}_r(M_G, M_{\text{Lap}})$ increases as $\Delta_1/\Delta_2$ increases or $\mu$ decreases.

**Proof.** (i) First, we calculate $L_r$ cost of the improved Laplace mechanism. For $Y \sim \text{Lap}(0; 1)$, the $r$th moment is

$$E|Y|^r = \int_{-\infty}^{\infty} \frac{1}{2} e^{-|y|} |y|^r dy = \int_{0}^{\infty} y^r e^{-y} dy = \Gamma(r + 1).$$

Let $\xi = (Y_1, \ldots, Y_p) \sim \text{Lap}_p(0; b^b_{\Delta^1})$. Then, the $L_r$ cost becomes

$$L_r(M_{\text{Lap}}(S; b^b_{\Delta^1})) = pE|Y_1|^r = p(b^b_{\Delta^1})^r E|Y|^r = p(b^b_{\Delta^1})^r \Gamma(r + 1).$$

In the normal case, it is well known that

$$E|X|^r = \frac{2^{r/2}}{\sqrt{\pi}} \Gamma\left(\frac{p + 1}{2}\right),$$
where $X \sim N(0, 1)$. Thus, we have

$$L_r(M_G(S)) = p(\Delta_3/\mu)\frac{\log(2\Phi(-\frac{\mu}{2}))}{\mu}.$$

(ii) From (i), the relative efficiency becomes

$$\text{RE}_r(M_G, M_{\text{Lap}}) = \frac{\sqrt{\pi}}{2^{r/2}} \left( \frac{b_{\mu}^0}{\Delta_2/\mu} \right)^r \frac{\Gamma(r+1)}{\Gamma((\frac{r}{2}+1))} = \left( \frac{\Delta_1}{\Delta_2} \right)^r \frac{\Gamma(r+1)}{\Gamma((\frac{r}{2}+1))} \left( \frac{\mu}{-2\log(2\Phi(-\frac{\mu}{2}))} \right)^r.$$

The last equality holds from the definition of $b_{\mu}^0$ and by Legendre duplication formula for gamma function (5.5.5 of Olver et al. (2010)), which says that

$$\Gamma(r+1) = \frac{2^r}{\sqrt{\pi}} \Gamma\left(\frac{r}{2}+1\right).$$

(iii) From (ii), it is obvious that $\text{RE}_r(M_G, M_{\text{Lap}})$ is increasing in $\Delta_1/\Delta_2$ for each given $r$. To check whether $\text{RE}_r(M_G, M_{\text{Lap}})$ is an increasing function of $\mu$, it is enough to show that

$$g(\mu) := \frac{-\log(2\Phi(-\frac{\mu}{2}))}{\mu}$$

increases as $\mu$ increases. Define a function $h$ on $(0, \infty)$ as $h(\mu) = -\log\left(\Phi\left(-\frac{\mu}{2}\right)\right)$. Then $g$ is expressed by using $h$ as

$$g(\mu) = \frac{-\log(\Phi(-\mu/2)) - (-\log(1/2))}{\mu} = \frac{h(\mu) - h(0)}{\mu - 0}.$$

Let $\phi$ be a density of $N(0, 1)$. Note that

$$h'(\mu) = \frac{\phi(\mu/2)}{2\Phi(-\mu/2)}.$$

and

$$h''(\mu) = \frac{\phi(\mu/2)}{4\Phi(-\mu/2)^2}\left(\phi\left(\frac{\mu}{2}\right) - \frac{\mu}{2}\Phi\left(-\frac{\mu}{2}\right)\right).$$

However, it is well known that $\Phi(-x) < \phi(x)/x$ for any $x > 0$, and thus $h''(\mu) > 0$ for any $\mu > 0$. So, $h$ is a convex function, and as a consequence, $g(\mu)$ is increasing in $\mu > 0$. \hfill \Box

### E Additional simulation results

In this section, we provide simulation results for the private homogeneity tests, as referred to in Section 5.4. We use the same model settings used for comparing GOF tests, with 5-year age groups ($p = 18$ categories) and 10-year age groups ($p = 9$ categories). In 5-year age grouped table ($p = 18$), categories are divided into age:0-4, age:5-10, ..., age:85-84 and age:85+. Similarly, we set age:0-9, age:10-19, ..., age:80+ as the categories in the case of 10-year age grouped table ($p = 9$).

For the homogeneity test (Algorithm 3), $2 \times p$ contingency table is generated, in which the rows of the table are sampled from Multinomial($n, \pi_1$) and Multinomial($n, \pi_2$) respectively. We set $\pi_1 = \pi_2 = \pi_k^{(p)}$ to simulate the type I error rate, and set $(\pi_1, \pi_2) = (\pi_k^{(p)}, \pi_{US}^{(p)})$ for the power analysis.

The simulation results for homogeneity tests are illustrated in Figures 11 and 12.

As in the GOF test, except for the case of $\mu = 0.1$ and $p = 18$, the type I errors are well controlled in homogeneity test (Figure 11). Converse to the GOF test, the James–Stein processed mechanisms do not control type I error, and one remarkable observation is that $M\text{JS}$ does not control type I error in the range of $500 \leq n \leq 1500$. We speculate that this phenomenon occurs because the shrinkage and truncation steps break the uniform distribution of empirical p-values.
Figure 11: Graph of empirical type I error rates of homogeneity tests for each mechanism. The black dotted line is the level of the test, $\alpha = 0.05$. The red dotted line is the maximum empirical rejection rate value that contains 0.05 within two times of standard error.

Figure 12: Graph of empirical power of homogeneity tests for each mechanism.
As in the GOF test, Figure 12 reveals that the Laplace mechanism has the lowest power compared to the Gaussian-type mechanisms. When $\mu = 0.3$, it is hard to say that one mechanism dominates all others with respect to the power of the test. For the analysis of the power of homogeneity test of $\mu = 0.1$ and $p = 18$, we need some care. Since $M^c_{JS}$ does not control the type I error unless $n > 1500$, we cannot conclude that $M^c_{JS}$ dominates the other mechanisms in terms of power when $n \leq 1500$ because type I error is not controlled. However, $M^c_{JS}$ still performs better than other methods for $n > 1500$. Finally, in the scenario of $\mu = 0.1$ and $p = 9$, $M^c_{JS}$ and $M^c_{rJS}$ perform better than other mechanisms.