Journal of Privacy and Confidentiality
Vol. 14 (1) 2024

Submitted Nov. 2022
Published Feb. 2024

THE BOUNDED GAUSSIAN MECHANISM FOR DIFFERENTIAL PRIVACY

BO CHEN AND MATTHEW HALE

University of Florida, Gainesville, Florida, USA
e-mail address: bo.chen@ufl.edu

University of Florida, Gainesville, Florida, USA
e-mail address: matthewhale@ufl.edu

Abstract. The Gaussian mechanism is one differential privacy mechanism commonly used to protect numerical data. However, it may be ill-suited to some applications because it has unbounded support, and thus can produce invalid numerical answers to queries, such as negative ages or human heights in the tens of meters. One can project such private values onto valid ranges of data, but such projections lead to the accumulation of private query responses at the boundaries of ranges, thereby harming accuracy. Motivated by the need for both privacy and accuracy over bounded domains, we present a bounded Gaussian mechanism for differential privacy, which has support only on a given region. We present both univariate and multivariate versions of this mechanism, and illustrate a significant reduction in variance relative to comparable existing work.

Introduction

As many engineering applications have become increasingly reliant on user data, data privacy has become a concern that data aggregators and curators must take into consideration. In numerous applications, such as healthcare [Yang et al., 2018], energy systems [Asghar et al., 2017], transportation systems [Zhang and Zhu, 2018], and the Internet of Things (IoT) [Medaglia and Serbanati, 2010], the data gathered to support system operation often contain sensitive individual information. Differential privacy [Dwork and Roth, 2014] has emerged as a standard privacy framework that can be used in such applications to protect sensitive data while allowing the resultant privatized data to remain useful. Differential privacy is a statistical notion of privacy that provides privacy guarantees by adding carefully calibrated noise to sensitive data or functions of sensitive data. Its key features include: (i) it is robust to side information, in that any additional knowledge about data-producing entities does not weaken their privacy by much [Kasiviswanathan and Smith, 2014], and (ii) it is

Key words and phrases: Differential privacy, Gaussian mechanism, bounded mechanism, multivariate distribution, truncated distribution.

This work was supported by the NSF under CAREER Grant 1943275, by AFOSR under grant FA9550-19-1-0169, and by ONR under grant N00014-21-1-2502.

JPrivacy Confidentiality
www.journalprivacyconfidentiality.org
DOI:10.29012/jpc.850

immune to post-processing, in that any transformation of private data stays private [Dwork and Roth, 2014].

Well-known mechanisms implementing differential privacy include the Laplace mechanism [Dwork et al., 2016], the Gaussian mechanism [Dwork and Roth, 2014], and the exponential mechanism [McSherry and Talwar, 2007, McSherry, 2009]. Other mechanisms have been developed for specific applications, in some cases by building upon or modifying these well-known mechanisms. A representative sample includes the Dirichlet mechanism on the unit simplex [Gohari et al., 2021], mechanisms for sensitive words of symbolic data [Chen et al., 2023], the matrix-variate Gaussian mechanism for matrix-valued queries [Chanyaswad et al., 2018], and the XOR mechanism for binary-valued data [Ji et al., 2021]. As the use of differential privacy has grown, these and other mechanisms have been asked to respond to privacy needs in settings with constraints on allowable data.

The Gaussian mechanism has been used for some classes of numerical data, although it may also require modifications for some types of sensitive data because the Gaussian mechanism adds unbounded noise. For example, the Gaussian mechanism may generate negative values for data such as ages, salaries, and weights, and such negative values are not meaningful in these contexts. One attempt to solve this problem is through projecting out-of-domain results back to the closest value in the given domain. Although this procedure does not weaken differential privacy because it is only post-processing on private data, it has been observed to lead to low accuracy in applications [Holohan et al., 2019] and thus is undesirable. Nonetheless, the Gaussian mechanism has been used in numerous applications, including deep learning [Abadi et al., 2016, Yu et al., 2019], convex optimization [Bassily et al., 2014], filtering and estimation problems [Le Ny and Pappas, 2014], and cloud control [Hale and Egerstedt, 2018], all of which can use data that are inherently bounded in some way.

On the other hand, compared to the Laplace mechanism, which is another popular privacy mechanism designed for numerical data, the Gaussian mechanism is able to use lower-variance noise to provide the same privacy level for high-dimensional data. This is because the variance of privacy noise is an increasing function of the sensitivity of a given query, and the Gaussian mechanism allows the use of the L_2 sensitivity, which, in applications such as federated learning [Wei et al., 2020] and deep learning [Abadi et al., 2016], is much lower than the L_1 sensitivity used in Laplace mechanism.

Therefore, in this paper we develop a new type of Gaussian mechanism that accounts for the boundedness of semantically valid data in a given application. In the univariate case we consider data confined to a closed interval, and in the multivariate case we consider data confined to a product of closed intervals. For both cases, we show that the bounded Gaussian mechanism provides ϵ-differential privacy, rather than (ϵ, δ)-differential privacy, as is provided by the ordinary Gaussian mechanism. We also present algorithms for finding the minimum variance necessary to enforce ϵ-differential privacy using the bounded Gaussian mechanism. The mechanisms we develop do not rely on projections, and thus avoid the harms to accuracy that can accompany projection-based approaches.

In addition, Balle and Wang [2018] point out that the original Gaussian mechanism's variance bound is far from tight when the privacy parameter ϵ approaches 0, and cannot be extended when ϵ approaches ∞. This is because the original Gaussian mechanism calibrates noise with a worst-case bound that is only tight for a small range of ϵ. In this work, we present bounded mechanisms that address this limitation by leveraging the boundedness of the domains we consider. This boundedness excludes the tail of each Gaussian distribution from our analysis and allows for the development of tight bounds on the variance of noise required for all ϵ.

Related work in Holohan et al. [2019] developed a bounded Laplace mechanism, and in this work we bring the ability to bound private data to the Gaussian mechanism. Developments in Liu [2019] include a generalized Gaussian mechanism with bounded support, and we show in Section 4 that the mechanism developed in this paper requires significantly lower variance of noise to attain differential privacy and thus provides improved accuracy.

Notation. Let $\mathbb{N}$ denote the set of all positive integers and let I denote the identity matrix. We use letters to denote scalars, e.g., $a \in \mathbb{R}$, and we use arrows over letters to denote vectors, e.g., $\vec{b} \in \mathbb{R}^n$, where the superscript denotes the dimension of the vectors. All intervals of the form $[l, u]$ are assumed to have $l < u$. We use $[l, u]^m = [l_1, u_1] \times [l_2, u_2] \times \cdots \times [l_m, u_m] = [\vec{l}, \vec{u}]$ to denote the m-dimensional bounded sets, where $\times$ denotes the Cartesian product. Let $\{n\}$ denote a set $\{1, 2, \ldots, n\}$. We use $\ln(\cdot)$ to denote the natural logarithm. We also use the special functions

$$\begin{aligned} \operatorname{erf}(z) &= \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2} dt, \\ \phi(x) &= \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2}x^2\right), \end{aligned} \tag{0.1}$$

and

$$\Phi(x) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{x}{\sqrt{2}}\right)\right). \tag{0.2}$$

1. Preliminaries and Problem Statement

This section gives background on differential privacy and problem statements that are the focus of the remainder of the paper.

1.1. Differential Privacy Background.

Differential privacy is enforced by a *mechanism*, which is a randomized map. We let S denote the space of sensitive data of interest. For nearby pieces of sensitive data, a mechanism must produce outputs that are approximately indistinguishable. The definition of "nearby" is given by an adjacency relation.

Definition 1.1 (Adjacency)**.** Databases $d, d' \in S^n$ are adjacent, denoted $d \sim d'$, if they differ in at most k rows, where $k \in \mathbb{N}$ is a user-specified parameter. ◊

For numerical queries $Q : S^n \to \mathbb{R}^m$, $m \in \mathbb{N}$, the sensitivity of a query Q, denoted ΔQ, is used to calibrate the distribution of privacy noise used to implement privacy. Throughout this paper, we will use the ℓ_2-sensitivity.

Definition 1.2 (ℓ_2-Sensitivity)**.** The ℓ_2-sensitivity of a query $Q : S^n \to \mathbb{R}^m$ is defined as $\Delta Q = \max_{d \sim d'} ||Q(d) - Q(d')||_2$. ◊

The ℓ_2 sensitivity captures the largest magnitude by which the outputs of Q can change across two adjacent databases.

We next introduce the definition of differential privacy itself.

Definition 1.3 (Differential Privacy)**.** Fix a probability space $(\Omega, \mathfrak{F}, \mathbb{P})$. Let the adjacency parameter $k \in \mathbb{N}$ and the privacy parameter $\epsilon > 0$ be given. A mechanism $M : \Omega \times S^n \to \mathbb{R}^m$ is (ϵ, δ)-differentially private if for all adjacent databases $d, d' \in S^n$ it satisfies $\mathbb{P}\big[M(d) \in A\big] \leq e^{\epsilon} \cdot \mathbb{P}\big[M(d') \in A\big] + \delta$ for all sets A in a sigma-algebra over $\mathbb{R}^m$. ♢

The privacy parameter ϵ sets the strength of privacy protections, and a smaller ϵ implies stronger privacy. The parameter δ can be interpreted as a relaxation parameter, in the sense that it is the probability that ϵ-differential privacy fails to hold [Beimel et al., 2013] (although it may hold with a different value of ϵ). If $\delta = 0$, then a mechanism is said to be ϵ-differentially private.

In the literature, ϵ has ranged from 0.01 to 10 [Hsu et al., 2014]. A differential privacy mechanism guarantees that the randomized outputs of two adjacent databases will be made approximately indistinguishable to any recipient of their privatized forms, including any eavesdroppers. One widely used differential privacy mechanism is the Gaussian mechanism. The standard Gaussian mechanism is as follows:

Definition 1.4 (Standard Gaussian Mechanism)**.** Let $\epsilon, \delta \in (0, 1)$ and $k \in \mathbb{N}$ be given. For a query $Q : S^n \to \mathbb{R}^m$ on a database d, the Gaussian mechanism $M_G(d) = Q(d) + \eta$, where $\eta \sim \mathcal{N}(\vec{0}, \sigma^2 I)$, is (ϵ, δ)-differentially private if $\sigma = \Delta Q \sqrt{2 \log(1.25/\delta)}/\epsilon$. ♢

As discussed in the introduction, the Gaussian mechanism has been favored over the Laplace mechanism in several applications, including deep learning, empirical risk minimization, and various problems in control theory and optimization. Simultaneously, these applications may have bounds on the data they use, such as bounds on training data for a learning algorithm or bounds on states in a control system. Despite bounds, the Gaussian mechanism, because it has infinite support, produces unbounded private outputs.

1.2. Problem Statement.

In this work, we seek a Gaussian mechanism that respects given bounds on outputs of queries, and we formalize the development of this mechanism in the next two problem statements.

Problem 1.5 (Univariate bounded Gaussian mechanism)**.** Given a query $Q : S^n \to D$, where $D = [l, u] \subset \mathbb{R}$ ($l < u$, both finite) is a constrained domain, and a privacy parameter $\epsilon > 0$, develop a mechanism $M_{UB} : \Omega \times S^n \to D$ that is an ϵ-differentially private approximation of Q and generates outputs in D with probability 1. ♢

Problem 1.6 (Multivariate bounded Gaussian mechanism)**.** Given a query $Q : S^n \to D^m$, where $D^m = [l, u]^m \subset \mathbb{R}^m$ ($l_i < u_i$, both finite for all $i \in \{m\}$) is a bounded m-dimensional domain, and a privacy parameter $\epsilon > 0$, develop a mechanism $M_{MB} : \Omega \times S^n \to D^m$ that is an ϵ-differentially private approximation of Q and generates outputs in D^m with probability 1. ♢

We solve Problem 1.5 in Section 2, and Problem 1.6 in Section 3.

2. Univariate Bounded Gaussian mechanism

In this section, we develop the bounded Gaussian mechanism for a bounded domain $D = [l, u] \subset \mathbb{R}$. We now give a formal statement of the univariate bounded Gaussian mechanism, which will be the focus of the rest of this section:

Definition 2.1 (Univariate Bounded Gaussian Mechanism)**.** Let a query $Q : S^n \to D$ be given, where $D = [l, u] \subset \mathbb{R}$, and suppose that each $d \in S^n$ generates the output $Q(d) = q \in D$. Then the univariate bounded Gaussian mechanism $M_{UB} : \Omega \times S^n \to D$ is given by the probability density function

$$p_{UB}(x) = \begin{cases} \frac{1}{\sigma} \frac{\phi((x-q)/\sigma)}{\Phi((u-q)/\sigma) - \Phi((l-q)/\sigma)} & \text{if } x \in D, \\ 0 & \text{otherwise,} \end{cases} \tag{2.1}$$

with $\sigma > 0$, where $\phi(\cdot)$ is from (0.1) and $\Phi(\cdot)$ is from (0.2). ♢

Since $Q(d) = q$, the density function $p_{UB}(x)$ is not the same for each database, and data-dependent noise is known to be problematic in general for differential privacy [Nissim et al., 2007]. Therefore using the parameters of the standard Gaussian mechanism is no longer guaranteed to satisfy differential privacy for the bounded Gaussian mechanism. We next derive the parameters required for the bounded Gaussian mechanism to provide differential privacy, but first introduce some preliminary results.

2.1. **Preliminary Results.**

Lemma 2.2. *For a database $d \in S^n$, a query $Q : S^n \to D$ with $Q(d) = q$ and $D = [l, u] \subset \mathbb{R}$, let*

$$C(q, \sigma \mid l, u) = \Phi\left(\frac{u-q}{\sigma}\right) - \Phi\left(\frac{l-q}{\sigma}\right),$$

where $\sigma > 0$. Then for any adjacent database $d' \in S^n$ such that $d' \sim d$ in the sense of Definition 1.1 with $Q(d') = q'$, we have

$$\max_{q,q'} \frac{\Phi\left(\frac{u-q'}{\sigma}\right) - \Phi\left(\frac{l-q'}{\sigma}\right)}{\Phi\left(\frac{u-q}{\sigma}\right) - \Phi\left(\frac{l-q}{\sigma}\right)} = \max_{q,q'} \frac{C(q', \sigma \mid l, u)}{C(q, \sigma \mid l, u)} = \left.\frac{C(q+c, \sigma \mid l, u)}{C(q, \sigma \mid l, u)}\right|_{q=l},$$

where $c = |q - q'| \leq \Delta Q$.

Proof. See Appendix A. □

This leads to the following lemma.

Lemma 2.3. *For adjacent databases $d \sim d' \in S^n$ in the sense of Definition 1.1, and a query $Q : S^n \to D$ with a bounded support $D = [l, u] \subset \mathbb{R}$,*

$$\Delta C(\sigma) = \max_{c \in [0, \Delta Q]} \left(\left.\frac{C(q+c, \sigma \mid l, u)}{C(q, \sigma \mid l, u)}\right|_{q=l} \right) = \begin{cases} \left.\frac{C(q+c,\sigma|l,u)}{C(q,\sigma|l,u)}\right|_{q=l, c=\Delta Q} & \textit{if } \Delta Q < \frac{u-l}{2}, \\ \left.\frac{C(q+c,\sigma|l,u)}{C(q,\sigma|l,u)}\right|_{q=l, c=(u-l)/2} & \text{otherwise,} \end{cases}$$

where $\sigma > 0$, $Q(d) = q$, and $Q(d') = q'$.

Proof. See Appendix B. □

2.2. **Main Result on the Univariate Bounded Gaussian Mechanism.** We now proceed to the main result of this section, which bounds the variance required for the bounded Gaussian mechanism to provide ϵ-differential privacy.

Theorem 2.4. *Given a query $Q : S^n \to D$ with bounded support $D = [l, u] \subset \mathbb{R}$, for any $\epsilon > 0$, the univariate bounded Gaussian mechanism M_{UB} provides ϵ-differential privacy if*

$$\sigma^2 \geq \frac{\left((u-l) + \frac{\Delta Q}{2}\right)\Delta Q}{\epsilon - \ln(\Delta C(\sigma))}, \tag{2.2}$$

where ΔQ is the sensitivity in the sense of Definition 1.2.

Proof. See Appendix C. □

We observe that in Equation (2.2) the privacy noise scale parameter σ appears on both sides of the equation. Given a value of $\epsilon > 0$, it is desirable to use the smallest σ as this corresponds to using the smallest variance of privacy noise for a given privacy level. To do so, in the next section, we form a zero finding problem to find the minimum σ that satisfies Equation (2.2).

2.3. **Calculating the minimum σ.** Let σ^* be the smallest admissible value of σ. The calculation of σ^* can be formulated as a zero-finding problem, where we require

$$f(\sigma^*) = (\sigma^*)^2 - \frac{\left((u-l) + \frac{\Delta Q}{2}\right)\Delta Q}{\epsilon - \ln(\Delta C(\sigma^*))} = 0. \tag{2.3}$$

We now present some technical lemmas concerning the function f evaluated at

$$\sigma_0 = \sqrt{\frac{\left((u-l) + \frac{\Delta Q}{2}\right)\Delta Q}{\epsilon}}. \tag{2.4}$$

Lemma 2.5. *For all $\epsilon > 0$, $\epsilon - \ln(\Delta C(\sigma_0)) > 0$.*

Proof. See Appendix D. □

Lemma 2.6. *For all $\sigma \in (0, \infty)$, $\ln(\Delta C(\sigma)) > 0$.*

Proof. See Appendix E. □

Next, Lemma 2.7 calculates the value of $f(\sigma_0)$ and Lemma 2.8 shows that f is a monotonically increasing function on $[\sigma_0, \infty)$.

Lemma 2.7. *For the point $\sigma_0 = \sqrt{([(u-l) + \Delta Q/2]\,\Delta Q)/\epsilon}$, $f(\sigma_0) < 0$.*

Proof. By substituting σ_0,

$$f(\sigma_0) = \frac{\left[(u-l) + \frac{\Delta Q}{2}\right]\Delta Q}{\epsilon} - \frac{\left[(u-l) + \frac{\Delta Q}{2}\right]\Delta Q}{\epsilon - \ln(\Delta C(\sigma_0))}.$$

By Lemma 2.5 and Lemma 2.6 we have $\epsilon > \epsilon - \ln(\Delta C(\sigma_0)) > 0$. Therefore $f(\sigma_0) < 0$. □

Lemma 2.8. *For any $\sigma \in [\sigma_0, \infty)$, $(\partial/\partial\sigma) f(\sigma) > 0$.*

Proof. See Appendix F. □

Algorithm 1: A Zero Finding Algorithm

```
Input  : Function $f$ given in Equation (2.3), initial condition for privacy noise
         variance $\sigma_0$ given in Equation (2.4)
Output : Optimal privacy parameter $(\sigma^*)^2$
left= $\sigma_0^2$;
right= $\frac{[(u-l)+\frac{\Delta Q}{2}]\Delta Q}{\epsilon-\ln(\Delta C(\sigma_0))}$;
intervalSize= (left+right)/2;
while intervalSize>right−left do
    intervalSize = right − left;
    $(\sigma^*)^2 = \frac{\text{left+right}}{2}$;
    if $\frac{[(u-l)+\frac{\Delta Q}{2}]\Delta Q}{\epsilon-\ln(\Delta C(\sigma^*))} \geq (\sigma^*)^2$ then
        left = $(\sigma^*)^2$;
    else
        right = $(\sigma^*)^2$ ;
    end
end
return $(\sigma^*)^2$
```

By combining Lemma 2.7 and Lemma 2.8, we can use Algorithm 1 in Holohan et al. [2019], given below as Algorithm 1, to find the exact fixed point of f, which in our case is σ^*. The output of Algorithm 1 can be used in Definition 2.1 to form the univariate bounded Gaussian mechanism, and Theorem 2.4 shows that doing so provides ϵ-differential privacy. We next present an analogous mechanism for multi-variate query responses.

3. Multivariate Bounded Gaussian mechanism

We begin by formally defining the multivariate bounded Gaussian mechanism, which is the focus of the remainder of this section.

Definition 3.1 (Multivariate Bounded Gaussian Mechanism)**.** Let a query $Q : S^n \to D^m$ be given, where $D^m = [l, u]^m \subset \mathbb{R}^m$, and suppose that each $d \in S^n$ generates the output $Q(d) = \vec{q} \in D^m$. Then the multivariate bounded Gaussian mechanism $M_{MB} : \Omega \times S^n \to D^m$ is given by the probability density function

$$p_{MB}(\vec{x}) = \begin{cases} \prod_{i=1}^{m} \frac{1}{\sigma_m} \frac{\phi((x_i-q_i)/\sigma_m)}{\Phi((u_i-q_i)/\sigma_m)-\Phi((l_i-q_i)/\sigma_m)} & \text{if } \vec{x} \in D^m, \\ 0 & \text{otherwise,} \end{cases} \tag{3.1}$$

with $\sigma_m > 0$, where $\phi(\cdot)$ is from (0.1) and $\Phi(\cdot)$ is from (0.2). ♢

Before deriving this mechanism's differential privacy guarantee we require some preliminary results.

3.1. Preliminary Results.

Lemma 3.2. *For a database $d \in S^n$, a query $Q : S^n \to D^m$ with $Q(d) = \vec{q}$ and $D = [l, u]^m \subset \mathbb{R}$, let*

$$C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u}) = \prod_{i=1}^{m} \Phi\left((u_i - q_i)/\sigma_m\right) - \Phi\left((l_i - q_i)/\sigma_m\right),$$

where $\sigma_m > 0$. Then for any adjacent database $d' \in S^n$ such that $d' \sim d$ in the sense of Definition 1.1 with $Q(d') = \vec{q}\,'$, we have

$$\max_{\vec{q},\vec{q}\,'} \prod_{i=1}^{m} \frac{\Phi\left(\frac{u_i - q_i'}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i'}{\sigma_m}\right)}{\Phi\left(\frac{u_i - q_i}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i}{\sigma_m}\right)} = \max_{\vec{q},\vec{q}\,'} \frac{C_m(\vec{q}\,', \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})} = \left.\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right|_{\vec{q}=\vec{l}},$$

where $\vec{c} = ||\vec{q} - \vec{q}\,'||_2 \leq \Delta Q$.

Proof. See Appendix G. □

Now we define $\Delta C_m(\sigma_m, \vec{c}^{\,*})$, where

$$\Delta C_m(\sigma_m, \vec{c}^{\,*}) = \left.\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right|_{\vec{q}=\vec{l}, \vec{c}=\vec{c}^{\,*}},$$

where $\vec{c}^{\,*} \in \mathbb{R}^m$ is the optimal value of $\vec{c} = (c_1, \ldots, c_m)^T$ in the following optimization problem:

$$\begin{aligned} \max_{\vec{c}} \quad & \left.\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right|_{\vec{q}=\vec{l}} \\ \text{subject to} \quad & 0 \leq c_i \leq u_i - l_i \text{ for each } i \\ & ||\vec{c}||_2 \leq \Delta Q. \end{aligned} \tag{3.2}$$

Remark 3.3. The optimization problem in (3.2) is a concave maximization problem. In general, the value of c^* does not have a closed form, but it can be efficiently computed numerically using standard optimization software such as CVX or CasADi.

3.2. Main Results.

We now proceed to the main result of this section, which bounds the variance required for the multivariate bounded Gaussian mechanism to provide ϵ-differential privacy.

Theorem 3.4. *Given a query $Q : S^n \to D^m$ with bounded support $D^m = [l, u]^m \subset \mathbb{R}^m$, for any $\epsilon > 0$, the multivariate bounded Gaussian mechanism M_{MB} provides ϵ-differential privacy if*

$$\sigma_m^2 \geq \frac{\left[||\vec{u} - \vec{l}||_2 + \Delta Q/2\right] \Delta Q}{\epsilon - \ln(\Delta C_m(\sigma_m, \vec{c}^{\,*}))}, \tag{3.3}$$

where ΔQ is the sensitivity in the sense of Definition 1.2.

Proof. See Appendix H. □

As with the univariate bounded Gaussian mechanism, we see that σ_m appears on both sides of (3.3). Hence, we will use numerical methods to compute it.

3.3. Calculating the minimum σ_m.

We will follow similar steps to those in Section 2.3. Let σ_m^* be the minimal admissible value of σ_m that satisfies (3.3). Then for $D \subset \mathbb{R}^m$,

$$f_m(\sigma_m^*) = (\sigma_m^*)^2 - \frac{\left[||\vec{u}-\vec{l}||_2 + \Delta Q/2\right] \Delta Q}{\epsilon - \ln(\Delta C_m(\sigma_m^*, \vec{c}^*))} = 0. \tag{3.4}$$

We now present some lemmas concerning the function f_m with respect to the point

$$\sigma_{m,0} = \sqrt{\frac{\left[||\vec{u}-\vec{l}||_2 + \Delta Q/2\right] \Delta Q}{\epsilon}}. \tag{3.5}$$

Lemma 3.5. *For any $\epsilon > 0$, $\epsilon - \ln(\Delta C_m(\sigma_{m,0}, \vec{c}^*)) > 0$, where $\vec{c}^*$ can be derived by solving the optimization problem (3.2).*

Proof. See Appendix I. □

Lemma 3.6. *For $\sigma_{m,0} = \sqrt{\frac{[||\vec{u}-\vec{l}||_2+\Delta Q/2]\Delta Q}{\epsilon}}$, $\ln(\Delta C_m(\sigma_{m,0}, \vec{c}^*)) > 0$.*

Proof. See Appendix J. □

Lemma 3.7. *For $\sigma_{m,0} = \sqrt{\frac{[||\vec{u}-\vec{l}||_2+\Delta Q/2]\Delta Q}{\epsilon}}$, $f_m(\sigma_{m,0}) < 0$.*

Proof. By plugging in $\sigma_{m,0}$ we have

$$f_m(\sigma_{m,0}) = \frac{\left[||\vec{u}-\vec{l}||_2 + \frac{\Delta Q}{2}\right] \Delta Q}{\epsilon} - \frac{\left[||\vec{b}-\vec{a}||_2 + \frac{\Delta Q}{2}\right] \Delta Q}{\epsilon - \ln(\Delta C_m(\sigma_{m,0}, \vec{c}^*))}.$$

With Lemma 3.5 and Lemma 3.6 we have $\epsilon > \epsilon - \ln(\Delta C_m(\sigma_{m,0}, \vec{c}^*)) > 0$. Therefore $f_m(\sigma_{m,0}) < 0$. □

Lemma 3.8. *For any $\sigma_m \in [\sigma_{m,0}, \infty)$, we have $(\partial/\partial\sigma_m) f_m(\sigma_m) > 0$.*

Proof. See Appendix K. □

By combining Lemma 3.7 and Lemma 3.8 we can use Algorithm 1 in Holohan et al. [2019] to find the exact fixed point of f_m, namely σ_m^*, which is shown in Algorithm 2. The output of Algorithm 2 can be combined with the mechanism in Definition 3.1, and Theorem 3.4 shows that this combination gives ϵ-differential privacy for multivariate queries.

4. Numerical Results

This section presents simulation results. We consider queries of the properties of a graph. Specifically, the bounded data we consider is (i) the average degree in an undirected graph, and (ii) the second-smallest eigenvalue of the Laplacian of an undirected graph. This eigenvalue is also called the Fiedler value [Fiedler, 1973] of the graph. It is known that an undirected graph is connected if and only if its Fiedler value is positive [Fiedler, 1973], and the Fiedler value also sets the rate of convergence of various dynamical processes over graphs [Mesbahi and Egerstedt, 2010].

Algorithm 2: A Zero Finding Algorithm for Multivariate Bounded Gaussian Mechanism

```
Input  : Function $f_m$ given in Equation (3.4), Initial privacy parameter $\sigma_{m,0}$ given
         in Equation (3.5).
Output : Optimal privacy parameter $(\sigma_m^*)^2$.
left= $\sigma_{m,0}^2$;
Compute $c^*$ from the optimization problem in (3.2);
rignt= $\frac{[||\vec{u}-\vec{l}||_2+\Delta Q/2]\Delta Q}{\epsilon-\ln(\Delta C_m(\sigma_{m,0},\vec{c}^*))}$;
intervalSize= (left+right)/2;
while intervalSize>right−left do
    intervalSize = right − left;
    $(\sigma_m^*)^2$ = (left + right/2;
    Compute $c^*$ from the optimization problem in (3.2);
    if $\frac{[||\vec{u}-\vec{l}||_2+\Delta Q/2]\Delta Q}{\epsilon-\ln(\Delta C_m(\sigma_m^*,\vec{c}^*))} \geq (\sigma_m^*)^2$ then
        left = $(\sigma_m^*)^2$;
    else
        right = $(\sigma_m^*)^2$;
    end
end
return $(\sigma_m^*)^2$
```

We let $G = (V, E)$ denote a connected, undirected graph on 10 nodes. In this experiment we have a two-dimensional query Q to compute (i) the algebraic connectivity, equal to the second smallest eigenvalue λ_2 of the Laplacian matrix of G, which satisfies $\lambda_2 \in [0, 10]$ here, and (ii) the degree of a fixed but arbitrary node i, denoted N^i, which satisfies $N^i \in [1, 9]$ here. Therefore, for a graph G, we have $Q(G) = [\lambda_2, N_{\text{out}}]^T \in D^2$, where $D^2 = [l, u]^2 \subset \mathbb{R}^2$, with $l_1 = 0, l_2 = 1$ and $u_1 = 10, u_2 = 9$. For fixed $k \in \mathbb{N}$, we say that two graphs are adjacent if they have the same node set but differ in k edges. Let ΔQ_{λ_2} denote the sensitivity of λ_2, let ΔQ_{N^i} denote the sensitivity of node i's degree, and let $\Delta Q = ||(\Delta Q_{\lambda_2}, \Delta Q_{N^i})^T||_2$ denote the sensitivity of the query Q. From [Chen et al., 2021, Lemma 1], $\Delta Q_{\lambda_2} = 2k$ and $\Delta Q_{N^i} = k$. Thus, $\Delta Q = \sqrt{5}k$. In our simulations we set $k = 2$. Table 1 gives some example variances computed for using the multivariate bounded Gaussian mechanism. In Figure 1, there is a general decrease in the variance of the bounded Gaussian mechanism as ϵ grows. This decrease agrees with intuition because a larger ϵ implies weaker privacy protection and thus the private output distribution has a higher peak on the true query answer.

We now compare the proposed mechanism with generalized Gaussian mechanism [Liu, 2019]. Let σ_{GG}^2 be the variance of generalized Gaussian mechanism and σ_{BG}^2 be the bounded Gaussian mechanism. Then we define the Percent Reduction in variance as

$$\text{Percent Reduction} = \frac{\sigma_{GG}^2 - \sigma_{BG}^2}{\sigma_{GG}^2} \times 100\%.$$

Both Figure 1 and Table 1 show that the bounded Gaussian mechanism always generates smaller variance, i.e., $\sigma_{BG}^2 < \sigma_{GG}^2$ and the Percent Reduction > 0 for all ϵ. In other words, compared to the generalized Gaussian mechanism [Liu, 2019], the bounded Gaussian

ϵ	Generalized Gaussian σ^2_{GG}	Bounded Gaussian σ^2_{BG}	Percent Reduction
0.1	1320.0	857.5	35.0%
0.5	264.0	170.3	35.5%
1.0	132.0	84.3	36.1%
1.5	88	55.8	36.6%
2.0	66	41.5	37.2%
2.5	52.8	32.9	37.7%
3.0	44	27.2	38.2%

Table 1: Some example values of σ_{BG} with different values of ϵ. The last column shows the percentage reduction in variance attained by using the bounded Gaussian mechanism we develop.

mechanism generates private outputs with less noise but with the same level of privacy protection.

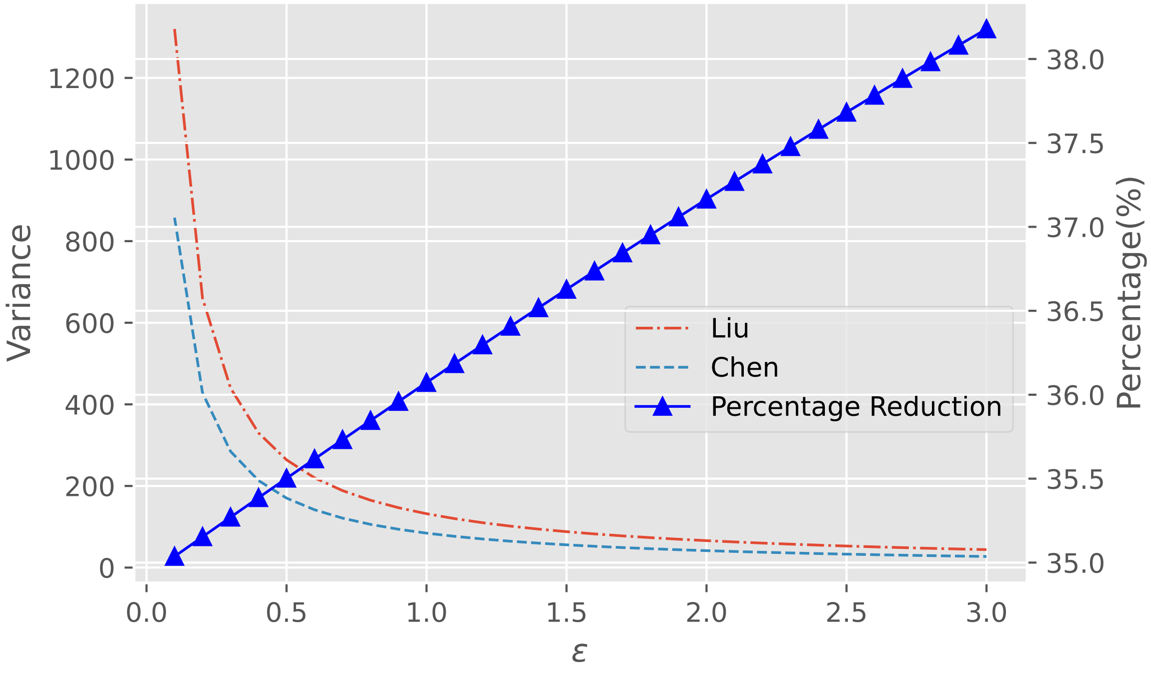

Figure 1: The variance comparison of proposed machanism and Liu's mechanism from [Liu, 2019, Definition 5]. With a larger ϵ, which gives weaker privacy, the variance of bounded Gaussian mechanism decreases quickly and is always smaller than that of the generalized Gaussian mechanism. This means that the bounded Gaussian mechanisms require less noise and provide better accuracy while maintaining the same level of protection. In addition, the blue triangles ascent from left to right, indicating that the reduction in variance grows as ϵ grows.

5. Conclusion

This paper presented two differential privacy mechanisms, namely the univariate and multivariate bounded Gaussian mechanisms, for bounded domain queries of a database of sensitive data. Compared to the existing generalized Gaussian mechanism, the bounded Gaussian mechanisms we present generate private outputs with less noise and better accuracy for the same privacy level. Future work will apply this mechanism to real-world applications, such as privately forecasting epidemic propagation, federated learning and optimization, and exploring privacy and performance trade-offs. Future work will design a de-noisingpost-processing procedure to generate more accurate private outputs.

References

M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 308–318, New York, NY, USA, 2016. Association for Computing Machinery.

M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac. Smart meter data privacy: A survey. *IEEE Communications Surveys and Tutorials*, 19(4):2820–2835, 2017.

B. Balle and Y.-X. Wang. Improving the Gaussian mechanism for differential privacy: analytical calibration and optimal denoising. In *Proceedings of the 35th International Conference on Machine Learning*, volume 80, pages 394–403. PMLR, Jul. 2018.

R. Bassily, A. Smith, and A. Thakurta. Private empirical risk minimization: efficient algorithms and tight error bounds. In *Proceedings of 55th Annual Symposium on Foundations of Computer Science*, pages 464–473. IEEE, 2014.

A. Beimel, K. Nissim, and U. Stemmer. Private learning and sanitization: Pure vs. approximate differential privacy. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 363–378. Springer Berlin Heidelberg, 2013.

T. Chanyaswad, A. Dytso, H. V. Poor, and P. Mittal. MVG mechanism: differential privacy under matrix-valued query. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 230–246, 2018.

B. Chen, C. Hawkins, K. Yazdani, and M. Hale. Edge differential privacy for algebraic connectivity of graphs. In *Proceedings of 60th IEEE Conference on Decision and Control (CDC)*, pages 2764–2769. IEEE, 2021.

B. Chen, K. Leahy, A. Jones, and M. Hale. Differential privacy for symbolic systems with application to Markov chains. *Automatica*, 152:110908, 2023.

C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3–4):211–407, Aug. 2014.

C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3):17–51, 2016. (Preliminary version in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC* 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3, pp. 265-284. Springer, Berlin Heidelberg, 2006.).

M. Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2): 298–305, 1973.

P. Gohari, B. Wu, C. Hawkins, M. Hale, and U. Topcu. Differential privacy on the unit simplex via the Dirichlet mechanism. *IEEE Transactions on Information Forensics and Security*, 16:2326–2340, 2021.

M. T. Hale and M. Egerstedt. Cloud-enabled differentially private multiagent optimization with constraints. *IEEE Transactions on Control of Network Systems*, 5(4):1693–1706, 2018.

N. Holohan, S. Antonatos, S. Braghin, and M. Aonghusa. The bounded Laplace mechanism in differential privacy. *Journal of Privacy and Confidentiality*, 10(1), Dec. 2019.

J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, B. C. Pierce, and A. Roth. Differential privacy: An economic method for choosing epsilon. *2014 IEEE 27th Computer Security Foundations Symposium*, Jul. 2014.

T. Ji, P. Li, E. Yilmaz, E. Ayday, Y. Ye, and J. Sun. Differentially private binary-and matrix-valued data query: an XOR mechanism. In *Proceedings of the VLDB Endowment*, volume 14(5), pages 849–862. VLDB Endowment, 2021.

S. P. Kasiviswanathan and A. Smith. On the 'semantics' of differential privacy: a Bayesian formulation. *Journal of Privacy and Confidentiality*, 6, Jun. 2014.

J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Control*, 59(2):341–354, 2014.

F. Liu. Generalized Gaussian mechanism for differential privacy. *IEEE Transactions on Knowledge and Data Engineering*, 31(4):747–756, 2019.

F. McSherry and K. Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 94–103, 2007.

F. D. McSherry. Privacy integrated queries: An extensible platform for privacy-preserving data analysis. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data*, page 19–30. Association for Computing Machinery, 2009.

C. M. Medaglia and A. Serbanati. An overview of privacy and security issues in the Internet of Things. *The Internet of Things*, pages 389–395, 2010.

M. Mesbahi and M. Egerstedt. Graph theoretic methods in multiagent networks. In *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.

K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, page 75–84. Association for Computing Machinery, 2007.

K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 15:3454–3469, 2020.

Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang. Privacy-preserving fusion of IoT and big data for e-health. *Future Generation Computer Systems*, 86:1437–1455, 2018.

L. Yu, L. Liu, C. Pu, M. E. Gursoy, and S. Truex. Differentially private model publishing for deep learning. In *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*, pages 332–349, 2019.

T. Zhang and Q. Zhu. Distributed privacy-preserving collaborative intrusion detection systems for vanets. *IEEE Transactions on Signal and Information Processing over Networks*, 4(1):148–161, 2018.

Appendix A. Proof of Lemma 2.2

Let $q' = q + c$. The same result can be derived by setting $q = q' + c$, due to symmetry. We proceed by showing that $C(q + c, \sigma \mid l, u)/C(q, \sigma \mid l, u)$ is monotonically decreasing with respect to q: $(\partial/\partial q)\left(C(q + c, \sigma \mid l, u)/C(q, \sigma \mid l, u)\right) < 0$. We first note that

$$\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)} = \frac{\Phi\left(\frac{u-q-c}{\sigma}\right) - \Phi\left(\frac{l-q-c}{\sigma}\right)}{\Phi\left(\frac{u-q}{\sigma}\right) - \Phi\left(\frac{l-q}{\sigma}\right)} = \frac{\int_{l-q}^{u-q} \exp\left(-\frac{1}{2}\left(\frac{y-c}{\sigma}\right)^2\right)dy}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-q}{\sigma}\right)^2\right)dx}, \tag{A.1}$$

where $y = x - q$. We now introduce the Leibniz rule used later in the proof.

Theorem A.1 (Leibniz Integral Rule)**.** *Let $g(x, t)$ be a function such that both $g(x, t)$ and its partial derivative $g_x(x, t)$ are continuous in t and x in some region of the xt-plane, including $f_1(x) \le t \le f_2(x)$, $x_0 \le x \le x_1$. Also suppose that the functions $f_1(x)$ and $f_2(x)$ are both continuous and both have continuous derivatives for $x_0 \le x \le x_1$. Then for $x_0 \le x \le x_1$,*

$$\frac{d}{dx}\left(\int_{f_1(x)}^{f_2(x)} g(x,t)dt\right) = g(x, f_2(x)) \cdot \frac{d}{dx}f_2(x) - g(x, f_1(x)) \cdot \frac{d}{dx}f_1(x) + \int_{f_1(x)}^{f_2(x)} \frac{d}{dx}g(x,t)dt.$$

Let $p_0 = \int_l^u \exp\left(-(1/2)(((x-q)/\sigma)^2\right)dx$. Using Theorem A.1, the derivative of Equation (A.1) becomes

$$\begin{aligned}
\frac{\partial}{\partial q}\left(\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)}\right) &= \frac{\left(\exp(-\frac{(l-q-c)^2}{2\sigma^2}) - \exp(-\frac{(u-q-c)^2}{2\sigma^2})\right) \cdot p_0}{p_0^2} \\
&\quad - \frac{\left(\exp(-\frac{(l-q)^2}{2\sigma^2}) - \exp(-\frac{(u-q)^2}{2\sigma^2})\right) \cdot \int_l^u \exp(-\frac{(x-q-c)^2}{2\sigma^2})dx}{p_0^2}, \\
&= \frac{p_1}{p_0} - \frac{p_2 \cdot p_3}{p_0^2},
\end{aligned} \tag{A.2}$$

where

$$\begin{aligned}
p_1 &= \exp\left(-\frac{(l-q-c)^2}{2\sigma^2}\right) - \exp\left(-\frac{(u-q-c)^2}{2\sigma^2}\right), \\
p_2 &= \exp\left(-\frac{(l-q)^2}{2\sigma^2}\right) - \exp\left(-\frac{(u-q)^2}{2\sigma^2}\right), \\
p_3 &= \int_l^u \exp\left(-\frac{(x-q-c)^2}{2\sigma^2}\right)dx.
\end{aligned}$$

We next introduce the mean value theorem of integrals.

Theorem A.2 (Mean Value Theorem of Integrals)**.** *For a continuous function $h : (a, b) \to \mathbb{R}$ and an integrable function g that does not change sign on $[a, b]$, there exists $\alpha \in [a, b]$ such that*

$$\int_a^b h(x)g(x)dx = h(\alpha)\int_a^b g(x)dx.$$

Using Theorem A.2,

$$\begin{aligned} p_3 &= \int_l^u \exp\left(-\frac{1}{2\sigma^2}((x-q)^2 - 2(x-q)c + c^2)\right) dx \\ &= \exp\left(-\frac{c^2}{2\sigma^2}\right) \int_l^u \exp\left(-\frac{(x-q)^2}{2\sigma^2}\right) \exp\left(\frac{(x-q)c}{\sigma^2}\right) dx \\ &= \exp\left(-\frac{c^2}{2\sigma^2}\right) \exp\left(\frac{(e-q)c}{\sigma^2}\right) p_0, \end{aligned} \tag{A.3}$$

where $e \in [l, u]$. Then we plug Equation (A.3) into the Equation (A.2), and we have

$$\frac{\partial}{\partial q}\left(\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)}\right) = \frac{p_1 - \left(p_2 \cdot \exp\left(-\frac{c^2}{2\sigma^2}\right)\exp\left(\frac{(e-q)c}{\sigma^2}\right)\right)}{p_0}. \tag{A.4}$$

Additionally, we can split the term p_1 by

$$\begin{aligned} p_1 = \exp&\left(-\frac{c^2}{2\sigma^2}\right) \\ &\cdot \left[\exp\left(-\frac{(l-q)^2}{2\sigma^2}\right)\exp\left(\frac{(l-q)c}{\sigma^2}\right) - \exp\left(-\frac{(u-q)^2}{2\sigma^2}\right)\exp\left(\frac{(u-q)c}{\sigma^2}\right)\right]. \end{aligned} \tag{A.5}$$

Combining Equation (A.4) and (A.5),

$$\frac{\partial}{\partial q}\left(\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)}\right) = \frac{\exp\left(-\frac{c^2}{2\sigma^2}\right)\left(\exp\left(-\frac{(l-q)^2}{2\sigma^2}\right)\cdot p_4 + \exp\left(-\frac{(u-q)^2}{2\sigma^2}\right)\cdot p_5\right)}{p_0}, \tag{A.6}$$

where

$$p_4 = \exp\left(\frac{(l-q)c}{\sigma^2}\right) - \exp\left(\frac{(e-q)c}{\sigma^2}\right) \le 0,$$

with equality if and only if e=l, and

$$p_5 = \exp\left(\frac{(e-q)c}{\sigma^2}\right) - \exp\left(\frac{(u-q)c}{\sigma^2}\right) \le 0,$$

with equality if and only if e=u.

Since p_4 and p_5 cannot be 0 at the same time, therefore

$$\frac{\partial}{\partial q}\left(\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)}\right) < 0.$$

Finally, since $q \in [l, u]$,

$$\max_q \frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)} = \left.\frac{C(q+c,\sigma \mid l,u)}{C(q,\sigma \mid l,u)}\right|_{q=l}.$$

■

Appendix B. Proof of Lemma 2.3

We proceed with this proof by forming a maximization problem and then using the Lagrangian multipliers method to solve it. By symmetry, we assume $c > 0$. Use Lemma 2.2 we have

$$\max_c \left(\frac{C(q+c, \sigma \mid l, u)}{C(q, \sigma \mid l, u)}\bigg|_{q=l} \right) = \max_c \frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c}{\sigma}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx}$$

$$\text{subject to} \quad c \in [0, \Delta Q].$$

Because this is a maximization problem, the Lagrangian function can be formed as

$$\mathcal{L}(c, \lambda_1, \lambda_2) = \frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c}{\sigma}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx} - \lambda_1 \cdot (0-c) - \lambda_2 \cdot (c - \Delta Q),$$

where λ_1,$\lambda_2 \geq 0$ are Lagrange multipliers. We then set $\partial\mathcal{L}(c, \lambda_1, \lambda_2)/\partial c = 0$ and apply the Karush–Kuhn–Tucker (KKT) conditions to find that

$$\frac{\partial}{\partial c}\left(\frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c}{\sigma}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx} \right) + \lambda_1 - \lambda_2 = 0 \tag{B.1}$$

$$\lambda_1(0-c) = 0 \tag{B.2}$$

$$\lambda_2(c - \Delta Q) = 0. \tag{B.3}$$

The derivative term in Equation (B.1) can be further simplified as

$$\frac{\partial}{\partial c}\left(\frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c}{\sigma}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx} \right) \tag{B.4}$$

$$= \frac{1}{p_6}\left(\frac{\partial}{\partial c}\int_{l-c}^{u-c} \exp\left(-\frac{1}{2}\left(\frac{z-l}{\sigma}\right)^2\right)dz \right)$$

$$= \frac{1}{p_6}\left(\exp\left(-\frac{c^2}{2\sigma^2}\right) - \exp\left(-\frac{(c-(u-l))^2}{2\sigma^2}\right) \right), \tag{B.5}$$

where $z = x - c$ and $p_6 = \int_l^u \exp\left[-(1/2)\left((x-l)/\sigma\right)^2\right]dx$. Equation (B.5) comes by using Theorem A.1. We now consider two cases.

Case 1: $\Delta Q < (u-l)/2$. Now if $c \leq \Delta Q < (u-l)/2$, then $\exp\left(-c^2/2\sigma^2\right) > \exp\left(-(c-(u-l))^2/2\sigma^2\right)$. Therefore based on Equation (B.5),

$$\frac{\partial}{\partial c}\left(\frac{C(q+c, \sigma \mid l, u)}{C(q, \sigma \mid l, u)}\Big|_{q=l} \right) > 0.$$

Therefore Equations (B.1)-(B.3) are satisfied simultaneously if and only if $\lambda_2 > 0$ and $\lambda_1 = 0$. Hence, the optimal value is $c^* = \Delta Q$.

Case 2: $(u-l)/2 \leq \Delta Q \leq u-l$ Now if $(u-l)/2 \leq \Delta Q \leq u-l$, then Equation (B.1)-(B.3) are satisfied simultaneously if and only if $c^* = (u-l)/2$ with $\lambda_1 = 0$ and $\lambda_2 = 0$.

Thus, we can conclude this proof by setting c to

$$c^* = \begin{cases} \Delta Q, & \text{if } \Delta Q < (u-l)/2, \\ (u-l)/2, & \text{otherwise,} \end{cases} \tag{B.6}$$

which is the optimal solution of Equations (B.1) and (B.3). ■

Appendix C. Proof of Theorem 2.4

For adjacent databases $d \sim d' \in S^n$, let $Q(d) = q$ and $Q(d') = q'$ such that $q' = q + c$ and by Definition 1.2 we have $|c| \leq \Delta Q$. Without loss of generality we take $c \geq 0$. To prove differential privacy we examine the ratio of the probabilities that the bounded Gaussian mechanism outputs some element $z \in D$ on q and q', namely

$$\begin{aligned} \left| \frac{\Pr[M_{UB}(d) = z]}{\Pr[M_{UB}(d') = z]} \right| &= \left| \frac{\phi\left(\frac{z-q}{\sigma}\right)}{\phi\left(\frac{z-q'}{\sigma}\right)} \cdot \frac{\Phi\left(\frac{u-q'}{\sigma}\right) - \Phi\left(\frac{l-q'}{\sigma}\right)}{\Phi\left(\frac{u-q}{\sigma}\right) - \Phi\left(\frac{l-q}{\sigma}\right)} \right| \\ &\leq \Delta C(\sigma) \cdot |g(z, q, c|\sigma)|, \end{aligned}$$

where

$$|g(z, q, c|\sigma)| = \left| \frac{\phi\left(\frac{z-q}{\sigma}\right)}{\phi\left(\frac{z-q-c}{\sigma}\right)} \right| = \left| \frac{\exp\left(-\frac{x^2}{2\sigma^2}\right)}{\exp\left(-\frac{(x+c)^2}{2\sigma^2}\right)} \right| \leq \left| \exp\left(\frac{(2x\Delta Q + (\Delta Q)^2)}{2\sigma^2} \right) \right|,$$

with $x = q - z$. As in Dwork and Roth [2014], for $\epsilon' > 0$, if $x < \sigma^2\epsilon/\Delta Q - \Delta Q/2$, then

$$|g(z, q, c|\sigma)| \leq \exp(\epsilon').$$

Since $x \in [l-u, u-l]$, we let

$$\frac{\sigma^2\epsilon'}{\Delta Q} - \frac{\Delta Q}{2} \geq u - l.$$

Then, solving for σ^2 gives

$$\sigma^2 \geq \frac{\left[(u-l) + \frac{\Delta Q}{2}\right] \Delta Q}{\epsilon'}.$$

Now we let

$$\left| \frac{\Pr[M_B(d) = z]}{\Pr[M_B(d') = z]} \right| \leq \Delta C(\sigma) \cdot |g(z, q, c|\sigma)| \leq \Delta C(\sigma) \exp(\epsilon').$$

To satisfy the differential privacy guarantee, we let $\exp(\epsilon) = \Delta C(\sigma) \exp(\epsilon')$. Then $\epsilon' = \epsilon - \ln(\Delta C(\sigma))$. As a result, the scale parameter σ must satisfy

$$\sigma^2 \geq \frac{\left[(u-l) + \frac{\Delta Q}{2}\right] \Delta Q}{\epsilon - \ln(\Delta C(\sigma))}. ■$$

Appendix D. Proof of Lemma 2.5

By definition of σ_0,

$$\Delta C(\sigma_0) = \begin{cases} \dfrac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-\Delta Q}{\sigma_0}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma_0}\right)^2\right)dx} & \text{if } \Delta Q \leq \frac{u-l}{2} \\ \dfrac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-\frac{u-l}{2}}{\sigma_0}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma_0}\right)^2\right)dx} & \text{otherwise.} \end{cases}$$

We first consider $\Delta Q \leq (u-l)/2$. Note that $\Delta C(\sigma_0)$ can be further simplified as

$$\begin{aligned} \Delta C(\sigma_0) &= \frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma_0}\right)^2\right)\exp\left(\frac{1}{2}\left(\frac{2(x-l)\Delta Q}{\sigma_0^2}\right)\right)\exp\left(-\frac{1}{2}\frac{(\Delta Q)^2}{\sigma_0^2}\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma_0}\right)^2\right)dx} \\ &= \exp\left(\frac{1}{2}\left(\frac{2(\delta-l)\Delta Q}{\sigma_0^2}\right)\right)\exp\left(-\frac{1}{2}\frac{(\Delta Q)^2}{\sigma_0^2}\right), \end{aligned} \tag{D.1}$$

where Equation (D.1) holds by using Theorem A.2 with $\delta \in [l,u]$. We can now substitute $\sigma_0 = \sqrt{[(u-l)+\Delta Q/2]\,\Delta Q/\epsilon}$ and get:

$$\begin{aligned} \Delta C(\sigma_0) &= \exp\left(\frac{1}{2}\left(\frac{2(\delta-l)\Delta Q\epsilon}{\left(u-l+\frac{\Delta Q}{2}\right)\Delta Q}\right)\right)\exp\left(-\frac{1}{2}\left(\frac{(\Delta Q)^2\epsilon}{\left(u-l+\frac{\Delta Q}{2}\right)\Delta Q}\right)\right) \\ &= \exp\left(\frac{(2(\delta-l)-\Delta Q)\epsilon}{(2(u-l)+\Delta Q)}\right) \\ &< \exp(\epsilon), \end{aligned}$$

where the last inequality holds since $\delta \in [l,u]$ and $2(\delta-l)-\Delta Q \leq 2(u-l)+\Delta Q$.

Now consider $\Delta Q > (u-l)/2$, and further simplify $\Delta C(\sigma_0)$ with

$$\Delta C(\sigma_0) = \frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-\frac{u-l}{2}}{\sigma_0}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma_0}\right)^2\right)dx} = \exp\left(\frac{1}{2}\left(\frac{2(\delta-l)\frac{u-l}{2}}{\sigma_0^2}\right)\right)\exp\left(-\frac{1}{2}\frac{\left(\frac{u-l}{2}\right)^2}{\sigma_0^2}\right)$$

We can now substitute $\sigma_0 = \sqrt{([(u-l)+\Delta Q/2]\,\Delta Q)/\epsilon}$ to get

$$\Delta C(\sigma_0) = \exp\left(\frac{\left(2(\delta-l)-\frac{u-l}{2}\right)\frac{u-l}{2}}{(2(u-l)+\Delta Q)\Delta Q}\epsilon\right) \leq \exp\left(\frac{\left(2(\delta-l)-\frac{u-l}{2}\right)\Delta Q}{(2(u-l)+\Delta Q)\Delta Q}\epsilon\right) \leq \exp(\epsilon),$$

where the first inequality holds since $(u-l)/2 \leq \Delta Q$, and the second inequality holds since $2(\delta-l)-(u-l)/2 < 2(u-l)+\Delta Q$. ■

Appendix E. Proof of Lemma 2.6

According to Definition 1.2 and Equation (B.6) we have $c^* \in (0, (u-l)/2]$. Then

$$\Delta C(\sigma) = \frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c^*}{\sigma}\right)^2\right)dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx}.$$

Since $c^* \in (0, (u-l)/2]$, we have $l + c^* \in [l, u]$ and $u - c^* \in [l, u]$, so that

$$\begin{aligned}\Delta C(\sigma) &= \frac{\int_l^{l+c^*} \exp\left(-\frac{1}{2}\left(\frac{x-l-c^*}{\sigma}\right)^2\right)dx + \int_{l+c^*}^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c^*}{\sigma}\right)^2\right)dx}{\int_l^{u-c^*} \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx + \int_{u-c^*}^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx} \\ &= \frac{\int_{-c^*}^0 \exp\left(-\frac{1}{2}\left(\frac{x}{\sigma}\right)^2\right)dx + \int_l^{u-c^*} \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx}{\int_{-c^*}^0 \exp\left(-\frac{1}{2}\left(\frac{x+u-l}{\sigma}\right)^2\right)dx + \int_l^{u-c^*} \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right)dx}.\end{aligned}$$

To proceed in the proof we introduce the comparison property of definite integrals.

Theorem E.1 (Comparison Property of Definite Integrals)**.** *If $f(m) \geq g(m)$ for $\underline{m} \leq m \leq \bar{m}$, then*

$$\int_{\underline{m}}^{\bar{m}} f(m)dm \geq \int_{\underline{m}}^{\bar{m}} g(m)dm.$$

Since

$$\exp\left(-\frac{1}{2}\left(\frac{x}{\sigma}\right)^2\right) \geq \exp\left(-\frac{1}{2}\left(\frac{x+u-l}{\sigma}\right)^2\right)$$

for $x \in [-c^*, 0]$ and $c^* \in (0, (u-l)/2]$, it follows that

$$\int_{-c^*}^0 \exp\left(-\frac{1}{2}\left(\frac{x}{\sigma}\right)^2\right)dy \geq \int_{-c^*}^0 \exp\left(-\frac{1}{2}\left(\frac{x+u-l}{\sigma}\right)^2\right)dz.$$

Consequently, the numerator of $\Delta C(\sigma)$ is greater than its denominator. As a result, $\Delta C(\sigma) > 1$ and $\ln(\Delta C(\sigma)) > 0$. ■

Appendix F. Proof of Lemma 2.8

Taking the derivative of $f(\sigma)$,

$$\frac{\partial}{\partial\sigma} f(\sigma) = 2\sigma - \frac{\left((u-l) + \frac{\Delta Q}{2}\right)\Delta Q}{(\epsilon - \ln(\Delta C(\sigma))^2} \cdot \frac{1}{\Delta C(\sigma)} \cdot \frac{\partial \Delta C(\sigma)}{\partial \sigma} = 2\sigma + h(\sigma),$$

where

$$h(\sigma) = -\frac{\left((u-l) + \frac{\Delta Q}{2}\right)\Delta Q}{(\epsilon - \ln(\Delta C(\sigma))^2} \cdot \frac{1}{\Delta C(\sigma)} \cdot \frac{\partial \Delta C(\sigma)}{\partial \sigma}.$$

According to Lemma 2.6, $\Delta C(\sigma) > 1$ for all $\sigma \in (0, \infty]$. We next prove that $\partial \Delta C(\sigma)/\partial \sigma < 0$, which implies that $h(\sigma) > 0$. By taking the derivative and using Theorem A.1,

$$\frac{\partial \Delta C(\sigma)}{\partial \sigma} = \frac{\partial}{\partial \sigma}\left(\frac{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l-c^*}{\sigma}\right)^2\right) dx}{\int_l^u \exp\left(-\frac{1}{2}\left(\frac{x-l}{\sigma}\right)^2\right) dx}\right) = \beta_1(\sigma) + \beta_2(\sigma),$$

where

$$\beta_1(\sigma) = \frac{\frac{1}{\sigma^2}\exp\left(-\frac{(c^*)^2}{2\sigma^2}\right) \cdot \left(-\exp\left(-\frac{(u-l)^2-2(u-l)c^*}{2\sigma^2}\right) \cdot (u-l-c^*) - c^*\right)}{p_6} \tag{F.1}$$

$$\beta_2(\sigma) = -\frac{\left(\exp\left(-\frac{1}{2}\left(\frac{u-l}{\sigma}\right)^2\right) \cdot \frac{-(u-l)}{\sigma^2}\right) \cdot \int_l^u \exp\left(-\frac{1}{2}\left(\frac{(x-l)^2-2(x-l)c^*+(c^*)^2}{\sigma^2}\right)\right) dx}{p_6^2},$$

with $p_6 = \int_l^u \exp\left(-(1/2\left((x-l)/\sigma\right)^2\right) dx$. We can further simplify $\beta_2(\sigma)$ by applying Theorem A.2 with $\delta \in (a, b)$:

$$\beta_2(\sigma) = \frac{\frac{1}{\sigma^2}\exp\left(-\frac{(c^*)^2}{2\sigma^2}\right)\left(\exp\left(-\frac{1}{2}\left(\frac{u-l}{\sigma}\right)^2\right)(u-l) \cdot \exp\left(\frac{(\delta-l)c^*}{\sigma^2}\right)\right)}{p_6}. \tag{F.2}$$

Combining Equation (F.1) and Equation (F.2),

$$\begin{aligned}\beta_1(\sigma) + \beta_2(\sigma) = {} & \frac{\frac{1}{\sigma^2}\exp\left(-\frac{(c^*)^2}{2\sigma^2}\right)}{p_6} \cdot \left(c^*\left(\exp\left(-\frac{(u-l)^2-2(u-l)c^*}{2\sigma^2}\right) - 1\right) + \right. \\ & \left. (u-l) \cdot \left(\exp\left(-\frac{(u-l)^2-2(\delta-l)c^*}{2\sigma^2}\right) - \exp\left(-\frac{(u-l)^2-2(u-l)c^*}{2\sigma^2}\right)\right)\right) \\ = {} & \frac{\frac{1}{\sigma^2}\exp\left(-\frac{(c^*)^2}{2\sigma^2}\right)}{p_6} \cdot (\gamma_1(\sigma) + \gamma_2(\sigma)),\end{aligned}$$

where

$$\gamma_1(\sigma) = c^*\left(\exp\left(-\frac{(u-l)^2-2(u-l)c^*}{2\sigma^2}\right) - 1\right) = c^*\left(\exp\left(-\frac{(u-l)(u-l-2c^*)}{2\sigma^2}\right) - 1\right)$$

and

$$\gamma_2(\sigma) = (u-l) \cdot \left(\exp\left(-\frac{(u-l)^2-2(\delta-l)c^*}{2\sigma^2}\right) - \exp\left(-\frac{(u-l)^2-2(u-l)c^*}{2\sigma^2}\right)\right).$$

Since $c^* \in (0, (u-l)/2]$, we have $\gamma_1(\sigma) \leq 0$. Moreover, since $\delta \in (l, u)$, $\gamma_2(\sigma) < 0$. Therefore, $\partial \Delta C(\sigma)/\partial \sigma = \beta_1(\sigma) + \beta_2(\sigma) < 0$. And then we have $h(\sigma) > 0$ and $(\partial/\partial \sigma) f(\sigma) > 0$ on $[\sigma_0, \infty)$. ■

Appendix G. Proof of Lemma 3.2

By symmetry we assume $\vec{q}' = \vec{q} + \vec{c}$. We let $\vec{q} = (q_1, q_2, \dots, q_m)^T$. We proceed by showing that $C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})/C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})$ is monotonically decreasing with respect to each q_i, $i \in \{1, 2, \dots, m\}$. That is, we will show that

$$\frac{\partial}{\partial q_i}\left(\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right) < 0.$$

In fact, we only show that

$$\frac{\partial}{\partial q_1}\left(\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right) < 0,$$

because the proof for $q_2, \dots, q_m$ proceeds in the same way. We first note that

$$\begin{aligned}\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})} &= \prod_{i=1}^{m} \frac{\Phi\left(\frac{u_i - q_i'}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i'}{\sigma_m}\right)}{\Phi\left(\frac{u_i - q_i}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i}{\sigma_m}\right)} &\text{(G.1)}\\ &= h_1(q_1, c_1)h_2(q_2, \dots, q_m, c_2, \dots, c_m), &\text{(G.2)}\end{aligned}$$

where

$$h_1(q_1, c_1) = \frac{\int_{l_1}^{u_1} \exp\left(-\frac{1}{2\sigma_m^2}(x_1 - q_1 - c_1)^2\right) dx_1}{\int_{l_1}^{u_1} \exp\left(-\frac{1}{2\sigma_m^2}(x_1 - q_1)^2\right) dx_1}$$

and

$$h_2(q_2, \dots, q_m, c_2, \dots, c_m) = \prod_{i=2}^{m} \frac{\Phi\left(\frac{u_i - q_i'}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i'}{\sigma_m}\right)}{\Phi\left(\frac{u_i - q_i}{\sigma_m}\right) - \Phi\left(\frac{l_i - q_i}{\sigma_m}\right)}.$$

We also note that $h_2(\cdot)$ is a function that is independent of q_1. Therefore, $\partial h_2(\cdot)/\partial q_1 = 0$, so that

$$\frac{\partial}{\partial q_1}\left(\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right) = \left(\frac{\partial h_1(q_1, c_1)}{\partial q_1}\right) \cdot h_2(q_2, \dots, q_m, c_2, \dots, c_m).$$

We also have $h_2(\cdot) > 0$, so to show that

$$\frac{\partial}{\partial q_1}\left(\frac{C_m(\vec{q} + \vec{c}, \sigma_m \mid \vec{l}, \vec{u})}{C_m(\vec{q}, \sigma_m \mid \vec{l}, \vec{u})}\right) \leq 0,$$

we only need to show $\partial h_1(q_1, c_1)/\partial q_1 \leq 0$, which can be proved by using the same technique as in Appendix A. ■

Appendix H. Proof of Theorem 3.4

For adjacent databases $d \in S^n$ and $d' \in S^n$, along with a query Q, suppose that $Q(d) = \vec{q}$ and $Q(d') = \vec{q}\,'$ such that $\vec{q}\,' = \vec{q} + \vec{c}$ and $||\vec{c}||_2 \leq \Delta Q$. To prove that the multivariate mechanism provides differential privacy, we examine

$$\begin{aligned}\left|\frac{\Pr[M_{MB}(d)=\vec{z}]}{\Pr[M_{MB}(d')=\vec{z}]}\right| &= \left|\prod_{i=1}^{m}\frac{\phi\left(\frac{z_i-q_i}{\sigma_m}\right)}{\phi\left(\frac{z_i-q_i'}{\sigma_m}\right)}\cdot\frac{\Phi\left(\frac{u_i-q_i'}{\sigma_m}\right)-\Phi\left(\frac{l_i-q_i'}{\sigma_m}\right)}{\Phi\left(\frac{u_i-q_i}{\sigma_m}\right)-\Phi\left(\frac{l_i-q_i}{\sigma_m}\right)}\right| \\ &\leq \Delta C_m(\sigma_m,\vec{c}^{\,*})\cdot\left|\prod_{i=1}^{m}\frac{\phi\left(\frac{z_i-q_i}{\sigma_m}\right)}{\phi\left(\frac{z_i-q_i'}{\sigma_m}\right)}\right|,\end{aligned}$$

where

$$\left|\prod_{i=1}^{m}\frac{\phi\left(\frac{z_i-q_i}{\sigma_m}\right)}{\phi\left(\frac{z_i-q_i'}{\sigma_m}\right)}\right| = \left|\frac{\exp\left(-\frac{||\vec{z}-\vec{q}||_2^2}{2\sigma_m^2}\right)}{\exp\left(-\frac{||\vec{z}-\vec{q}-\vec{c}||_2^2}{2\sigma_m^2}\right)}\right| = \left|\frac{\exp\left(-\frac{||\vec{x}||_2^2}{2\sigma_m^2}\right)}{\exp\left(-\frac{||\vec{x}+\vec{c}||_2^2}{2\sigma_m^2}\right)}\right| \leq \left|\exp\left(\frac{2||\vec{x}||_2\Delta Q+(\Delta Q)^2}{2\sigma_m^2}\right)\right|,$$

with $\vec{x} = \vec{q} - \vec{z}$. Based on Appendix A in Dwork and Roth [2014], for $\epsilon' > 0$, if $||\vec{x}||_2 < \sigma_m^2\epsilon'/\Delta Q - \Delta Q/2$, then

$$\left|\exp\left(\frac{2||\vec{x}||_2\Delta Q+(\Delta Q)^2}{2\sigma_m^2}\right)\right| \leq \exp(\epsilon'). \tag{H.1}$$

Since $||\vec{x}||_2 \in \left[0, ||\vec{u}-\vec{l}||_2\right]$, then we choose the following inequality to ensure that Equation (H.1) always holds:

$$\frac{\sigma_m^2\epsilon'}{\Delta Q} - \frac{\Delta Q}{2} \geq ||\vec{u}-\vec{l}||_2. \tag{H.2}$$

By rearranging Equation (H.2),

$$\sigma_m^2 \geq \frac{\left(||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right)\Delta Q}{\epsilon'}.$$

Now we let

$$\begin{aligned}\left|\frac{\Pr[M_{MB}(d)=\vec{z}]}{\Pr[M_{MB}(d')=\vec{z}]}\right| &\leq \Delta C_m(\sigma_m,\vec{c}^{\,*})\cdot\left|\exp\left(\frac{2||\vec{x}||_2\Delta Q+(\Delta Q)^2}{2\sigma_m^2}\right)\right| \\ &\leq \Delta C_m(\sigma_m,\vec{c}^{\,*})\exp(\epsilon').\end{aligned}$$

To satisfy the differential privacy guarantee, we let $\exp(\epsilon) = \Delta C_m(\sigma_m,\vec{c}^{\,*})\exp(\epsilon')$. Then $\epsilon' = \epsilon - \ln(\Delta C_m(\sigma_m,\vec{c}^{\,*}))$. As a result, the scale parameter σ_m has to satisfy

$$\sigma_m^2 \geq \frac{\left[||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right]\Delta Q}{\epsilon-\ln(\Delta C_m(\sigma_m,\vec{c}^{\,*}))}. \blacksquare$$

Appendix I. Proof of Lemma 3.5

We proceed in this proof by showing that $\ln\left(\Delta C_m(\sigma_{m,0},\vec{c}^*)\right) < \epsilon$. For $\sigma_{m,0}$,

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) = \prod_{i=1}^{m} \frac{\int_{l_i}^{u_i} \exp\left(-\frac{1}{2}\left(\frac{x-l_i}{\sigma_{m,0}}\right)^2\right)\exp\left(\frac{1}{2}\left(\frac{2(x-l_i)c_i^*}{\sigma_{m,0}^2}\right)\right)\exp\left(-\frac{1}{2}\frac{(c_i^*)^2}{\sigma_{m,0}^2}\right)dx}{\int_{l_i}^{u_i} \exp\left(-\frac{1}{2}\left(\frac{x-l_i}{\sigma_{m,0}}\right)^2\right)dx},$$

Now we use Theorem A.2. There exists $\vec{\delta} = (\delta_1,\ldots,\delta_m)^T \in \mathbb{R}^m$ such that for each $i \in \{1,2,\ldots,m\}$ we have $\delta_i \in [l_i,u_i]$, so that

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) = \exp\left(-\frac{1}{2\sigma_{m,0}^2}\left((\vec{c}^*)^T\vec{c}^* - (\vec{c}^*)^T(\vec{\delta}-\vec{l})\right)\right),$$

We now substitute $\sigma_{m,0}^2 = \left[||\vec{u}-\vec{l}||_2 + \frac{\Delta Q}{2}\right]\Delta Q/\epsilon$ to obtain

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) = \exp\left(\frac{(\vec{c}^*)^T(2(\vec{\delta}-\vec{l})-\vec{c}^*)}{2\left(||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right)\Delta Q}\epsilon\right).$$

Using the Cauchy–Schwarz inequality,

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) = \exp\left(\frac{(\vec{c}^*)^T(2(\vec{\delta}-\vec{l})-\vec{c}^*)}{2\left(||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right)\Delta Q}\epsilon\right) \leq \exp\left(\frac{||\vec{c}^*||_2||2(\vec{\delta}-\vec{l})-\vec{c}^*||_2}{2\left(||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right)\Delta Q}\epsilon\right).$$

With $\delta_i \in (l_i,u_i)$, $||\vec{c}^*||_2 \leq \Delta Q$, by the triangle inequality,

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) \leq \exp\left(\frac{(||2(\vec{\delta}-\vec{l})||_2 + ||\vec{c}^*||_2)}{2\left[||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right]}\epsilon\right) \leq \exp(\epsilon).$$

■

Appendix J. Proof of Lemma 3.6

We can simplify $\Delta C_m(\sigma_{m,0},\vec{c}^*)$ with

$$\Delta C_m(\sigma_{m,0},\vec{c}^*) = \prod_{i=1}^{m} \frac{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i-c_i^*)^2}{2\sigma_{m,0}^2}\right)dx_i}{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i)^2}{2\sigma_{m,0}^2}\right)dx_i}, \tag{J.1}$$

where $\vec{c}^* = (c_1^*,\ldots,c_m^*)^T$. By Appendix E, we have for each $i \in \{1,2,\ldots,m\}$,

$$\frac{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i-c_i^*)^2}{2\sigma_{m,0}^2}\right)}{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i)^2}{2\sigma_{m,0}^2}\right)} > 1.$$

Therefore $\Delta C_m(\sigma_{m,0},\vec{c}^*) > 1$ and $\ln(\Delta C_m(\sigma_{m,0},\vec{c}^*)) > 0$. ■

Appendix K. Proof of Lemma 3.8

We take the derivative of f_m at σ_m:

$$\begin{aligned}\frac{\partial}{\partial\sigma_m}f_m(\sigma_m) &= 2\sigma_m - \frac{\left[||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right]\Delta Q}{(\epsilon-\ln(\Delta C_m(\sigma_m,\vec{c}^*))^2}\cdot\frac{1}{\Delta C_m(\sigma_m,\vec{c}^*)}\cdot\frac{\partial}{\partial\sigma_m}(\Delta C_m(\sigma_m,\vec{c}^*))\\ &= 2\sigma_m + h_m(\sigma_m),\end{aligned}$$

where

$$h_m(\sigma_m) = -\frac{\left[||\vec{u}-\vec{l}||_2+\frac{\Delta Q}{2}\right]\Delta Q}{(\epsilon-\ln(\Delta C_m(\sigma_m,\vec{c}^*))^2}\cdot\frac{1}{\Delta C_m(\sigma_m,\vec{c}^*)}\cdot\frac{\partial}{\partial\sigma_m}(\Delta C_m(\sigma_m,\vec{c}^*)).$$

Since $\Delta C_m(\sigma_m,\vec{c}^*)>0$ for all $\sigma_m\in(0,\infty]$, then if $(\partial/\partial\sigma_m)(\Delta C_m(\sigma_m,\vec{c}^*))<0$, we will have $h_m(\sigma_m)>0$. From Equation (J.1),

$$\Delta C_m(\sigma_m,\vec{c}^*) = \prod_{i=1}^{m}\frac{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i-c_i^*)^2}{2\sigma_m^2}\right)}{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i)^2}{2\sigma_m^2}\right)}.$$

Then,

$$\frac{\partial(\Delta C_m(\sigma_m,\vec{c}^*))}{\partial\sigma_m} = \sum_{i=1}^{m}\left(\left(\frac{\partial}{\partial\sigma_m}\frac{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i-c_i^*)^2}{2\sigma_m^2}\right)}{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i)^2}{2\sigma_m^2}\right)}\right)\cdot\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\int_{l_j}^{u_j}\exp\left(-\frac{(x_j-l_j-c_j^*)^2}{2\sigma_m^2}\right)}{\int_{l_j}^{u_j}\exp\left(-\frac{(x_j-l_j)^2}{2\sigma_m^2}\right)}\right).$$

From Appendix F, for each $i\in\{1,2,\ldots,m\}$,

$$\frac{\partial}{\partial\sigma_m}\frac{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i-c_i^*)^2}{2\sigma_m^2}\right)}{\int_{l_i}^{u_i}\exp\left(-\frac{(x_i-l_i)^2}{2\sigma_m^2}\right)}<0.$$

Therefore $(\partial/\partial\sigma_m)\Delta C_m(\sigma_m,\vec{c}^*)<0$ and $(\partial/\partial\sigma_m)f_m(\sigma_m)>0$. ■