A closed form scale bound for the \((\epsilon, \delta)\)-differentially private Gaussian Mechanism valid for all privacy regimes

Staal A. Vinterbo

Abstract

The standard closed form lower bound on \(\sigma\) for providing \((\epsilon, \delta)\)-differential privacy by adding zero mean Gaussian noise with variance \(\sigma^2\) is \(\sigma > \Delta \sqrt{2e^{-1}} \sqrt{\log (5/4 \delta^{-1})}\) for \(\epsilon \in (0, 1)\). We present a similar closed form bound \(\sigma \geq \Delta (\sqrt{2} \epsilon)^{-1} (\sqrt{z} + \sqrt{z} + \epsilon)\) for \(z = -\log (\delta (2 - \delta))\) that is valid for all \(\epsilon > 0\) and is always lower (better) for \(\epsilon < 1\) and \(\delta \leq 0.946\). Both bounds are based on fulfilling a particular sufficient condition. For \(\delta < 1\), we present an analytical bound that is optimal for this condition and is necessarily larger than \(\Delta / \sqrt{2e}\).

1 Introduction

Differential privacy \([4]\) is an emerging standard for individual data privacy. In essence, differential privacy is a bound on any belief update about an individual on receiving a result of a differentially private randomized computation. Critical for the utility of such results is minimizing the random perturbation required for a given level of privacy. In Theorem 5 we present a closed form bound on the amount of perturbation needed for privacy in the Gaussian Mechanism. This bound improves on the current closed form standard in two ways: smaller perturbation and wider applicability. Both our and the current standard bound are based on fulfilling a certain sufficient condition for privacy. In Lemma 3 we also describe the smallest possible perturbation for this condition.

Formally, let a database \(d\) be a collection of record values from some set \(V\). Two databases \(d\) and \(d'\) are neighboring if one can be obtained from the other by adding one record. Let \(N\) be the set of all pairs of neighboring databases. Then following Dwork et al. \([4, 5]\) we define differential privacy as follows.

\textbf{Definition 1} \((\epsilon, \delta)\)-differential privacy \([4, 5]\). A randomized algorithm \(M\) is called \((\epsilon, \delta)\)-differentially private if for any measurable set \(S\) of possible outputs and all \((d, d') \in N\)

\[Pr(M(d) \in S) \leq e^\epsilon Pr(M(d') \in S) + \delta,\]

where the probabilities are over randomness used in \(M\). By \(\epsilon\)-differential privacy we mean \((\epsilon, 0)\)-differential privacy.

A standard mechanism for achieving \((\epsilon, \delta)\)-differential privacy is that of adding zero mean Gaussian noise to a statistic, called the Gaussian Mechanism. A primary reason for the popularity of
the Gaussian Mechanism is that the Gaussian distribution is closed under addition. However, Gaussian noise requires $\delta > 0$, which represents a relaxation of the stronger $(\epsilon, 0)$-differential privacy that is not uncontroversial [7]. On the positive side, a non-zero $\delta$ allows, among others, for better composition properties than $(\epsilon, 0)$-differential privacy [6]. The exploitation of the composition benefits of using Gaussian noise can be observed in an application to deep learning by Abadi et al.[1].

To achieve $(\epsilon, \delta)$-differential privacy, the variance $\sigma^2$ is carefully tuned taking into account the sensitivity $\Delta$ of the statistic, i.e., the maximum change in the statistic resulting from adding or removing any individual record from any database. Of prime importance is to minimize $\sigma$ while still achieving $(\epsilon, \delta)$-differential privacy as higher $\sigma$ generally decreases the utility of the now noisy statistic.

A well known sufficient condition for $(\epsilon, \delta)$-differential privacy when adding Gaussian noise that has been described as folklore [3] is

$$\Pr \left( \frac{|Z|}{\Delta} > \frac{\sigma \epsilon}{2\sigma} \right) \leq \delta.$$  \hspace{1cm} (1)

In the following, we are interested in closed form expressions relating $\sigma$, to $\epsilon$, $\delta$, and $\Delta$ that fulfil the criterion above. The simple closed form relationships we are after can be implemented using simple algorithms with low implementation and computational complexity. The benefit of this is a lower potential for errors, as well as decreasing power consumption in low power devices whenever the alternative is using iterative numerical algorithms to compute analytical solutions. Furthermore, closed form relationships can be potentially useful in the analysis of larger systems where the Gaussian Mechanism is a component.

In their Theorem A.1 [3], Dwork and Roth derive a closed form relationship between $\sigma$, $\epsilon$, $\delta$, and $\Delta$ by substituting the tail bound $\Pr(|Z| > x) \leq 2\phi(x)/x$, where $\phi$ is the standard Gaussian density, into (1) and subsequently manipulating the result to determine that $(\epsilon, \delta)$-differential privacy is achieved for $\epsilon \in (0, 1)$ if

$$\sigma > s(\epsilon, \delta, \Delta) = \frac{\Delta \sqrt{2}}{\epsilon} \sqrt{\log \left( \frac{5}{4 \delta} \right)}.$$  \hspace{1cm} (2)

The above bound (2) is essentially the standard closed form used for the Gaussian Mechanism, and we will refer to it as such in the following. Notably, the restriction $\epsilon \in (0, 1)$ can present non-obvious pitfalls in addition to the explicit restriction to privacy regimes with $\epsilon < 1$. For example consider the representation of $\epsilon$ as a function derived from the standard bound (2) (ignoring strict inequalities)

$$\epsilon(\delta, \sigma, \Delta) = \frac{\Delta \sqrt{2}}{\sigma} \sqrt{\log \left( \frac{5}{4 \delta} \right)}.$$  \hspace{1cm} (3)

A use of the above function can, for example, be found in [10], Section 4. As the magnitude of $\delta$ is associated with the failure of guaranteeing strong $\epsilon$-differential privacy, it is usually stated that $\delta$ should be cryptographically small. Now, the function in (3) increases as $\delta > 0$ decreases, and for fixed $\sigma$ and $\Delta$, even a relatively large $\delta$ could result in $\epsilon(\delta, \sigma, \Delta) \geq 1$, which might not be obvious. For example, $\epsilon(10^{-1}, 1, 1) > 2.24$.

Below in Theorem 5, we present the bound (12) that holds for all $\epsilon > 0$, $1 \geq \delta > 0$, $\Delta > 0$. Like the standard bound (2), this bound is closed form, very simple, and is based on fulfilling condition
We analyze this condition, present an optimal analytical bound, and show that any bound satisfying this condition must satisfy $\sigma > \frac{\Delta}{\sqrt{2\epsilon}}$ (Lemma 3). Restricted to $\epsilon \in (0,1)$, our bound (12) allows smaller $\sigma$ than the standard bound (2) whenever $\delta \leq 0.946$.

2 A few more preliminaries

We briefly recapitulate known results. In the following, we will let $\Phi$ and $\phi$ denote the standard Gaussian distribution function and density, respectively. For completeness, we provide proofs in Section A.

Definition 2. The global sensitivity of a real-valued function $q$ on databases is

$$\Delta_q = \max_{(d,d') \in \mathcal{N}} |q(d) - q(d')|.$$ 

Theorem 1. Let $X$ be a random variable distributed according to density $f$, and let $q$ be a real valued function on databases with global sensitivity $\Delta$. The algorithm that outputs a variate of $q(d) + X$ is $\epsilon$-differentially private if

$$f(x) \leq e^\epsilon f(y) \quad (4)$$

for all $x, y$ such that $|x - y| \leq \Delta$.

Applying the above theorem requires us to check that (4) holds for all $|x - y| \leq \Delta$. For certain densities we need only check for $|x - y| = \Delta$.

Corollary 1. If $f$ in Theorem 1 is strictly positive everywhere and log-concave, then the algorithm that outputs a variate of $q(d) + X$ is $\epsilon$-differentially private for $\epsilon > 0$ if for all $x$ and $s \in \{-1, +1\}$

$$\frac{f(x)}{f(x + s\Delta)} \leq e^\epsilon. \quad (5)$$

Remark 1. The density of a Gaussian distribution is strictly positive everywhere and log-concave.

Lemma 2. Let $Z$ be a random variable distributed according to the standard Gaussian distribution. Then for a real-valued function $q$ on databases with global sensitivity $\Delta$ and a database $d$, the mechanism returning a variate of $q(d) + \sigma Z$ is $(\epsilon, \delta)$-differentially private if

$$\Pr\left( |Z| > \frac{\sigma \epsilon}{\Delta} - \frac{\Delta}{2\sigma} \right) \leq \delta. \quad (1)$$

3 The theorem

We are now ready to present our main contributions.

Lemma 3. Let $Z$ be a random variable distributed according to the standard Gaussian distribution. Then for $\epsilon > 0$, $\Delta > 0$, and $\delta < 1$

$$\Pr\left( |Z| > \frac{\sigma \epsilon}{\Delta} - \frac{\Delta}{2\sigma} \right) \leq \delta, \quad (1)$$
holds if and only if $\sigma \geq b$ for

$$b = \frac{\Delta}{2 \epsilon} \left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) + \sqrt{\left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) \right)^2 + 2 \epsilon} \right) > \frac{\Delta}{\sqrt{2 \epsilon}} \quad (6)$$

where $\Phi^{-1}$ is the standard Gaussian quantile function.

**Proof.** Let

$$v(\sigma) = \frac{\sigma \epsilon}{\Delta} - \frac{\Delta}{2 \sigma}.$$ 

Then, requirement (1) can be written $\Pr(|Z| > v(\sigma)) \leq \delta$. Since $\delta < 1$, we must have that $\Pr(|Z| > v(\sigma)) < 1$ which is only the case if $v(\sigma) > 0$. Therefore, we need only consider this case in the remainder of this proof.

Then

$$l(\sigma) = \Pr(|Z| > v(\sigma)) = 2(1 - \Phi(v(\sigma)))$$

$$\iff$$

$$\Phi(v(\sigma)) = 1 - \frac{l(\sigma)}{2}$$

$$\iff$$

$$v(\sigma) = \Phi^{-1} \left( 1 - \frac{l(\sigma)}{2} \right). \quad (7)$$

Recall that we want to find a lower bound for $\sigma$ such that $l(\sigma) \leq \delta < 1$. We note that $l(\sigma)$ is decreasing in $\sigma$ if $v$ is increasing in $\sigma$. This is the case since

$$v'(\sigma) = \frac{2 \sigma^2 \epsilon + \Delta^2}{2 \Delta \sigma^2}$$

is positive for all $\sigma$ and $\Delta > 0$, $\epsilon > 0$. Hence, we can find the sought lower bound by solving $l(\sigma) = \delta$ for $\sigma$. We do this by substituting $\delta$ for $l(\sigma)$ in (7) and solving for $\sigma > 0$, yielding

$$\sigma = \frac{\Delta}{2 \epsilon} \left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) + \sqrt{\left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) \right)^2 + 2 \epsilon} \right). \quad (8)$$

We now conclude the proof by showing that the right-hand side of the equation above is larger than $\frac{\Delta}{\sqrt{2 \epsilon}}$. First, we note that $z + \sqrt{z^2 + 2 \alpha}$ is monotonically increasing in $z \geq 0$. This means that for $z \geq 0$

$$\frac{\Delta(z + \sqrt{z^2 + 2 \epsilon})}{2 \epsilon} \quad (9)$$

achieves its minimum $\frac{\Delta}{\sqrt{2 \epsilon}}$ at $z = 0$. Noting that substituting $\Phi^{-1}(1 - \delta/2)$ for $z$ in (9) yields the right-hand side of (8) and that $\delta < 1$ yields $1 - \delta/2 > 1/2$ and therefore $\Phi^{-1}(1 - \delta/2) > 0$. Hence, this right hand side is always larger than $\frac{\Delta}{\sqrt{2 \epsilon}}$.

**Remark 2.** A $\delta \geq 1$ eliminates any protection of privacy as the release of the original data is $(\epsilon,1)$-differentially private. In this light, Lemma 3 is a generalization and sharpening of Theorem 4 in [2] that claims $\sigma \geq \frac{\Delta}{\sqrt{2 \epsilon}}$ for the standard bound. As $\delta \to 1$ from below we have that the right side of (8) approaches $\frac{\Delta}{\sqrt{2 \epsilon}}$ from above.
Lemma 4. Let $\Phi^{-1}$ be the standard Gaussian quantile function. Then for $p \geq 1/2$

$$\Phi^{-1}(p) \leq \sqrt{2}\sqrt{-\log(-(2p - 1)^2 + 1)}. \quad (10)$$

Proof. It is well known that $\text{erf}(x) = \text{sign}(x)P(\frac{1}{2}, x^2)$, where $P$ is the regularized gamma function $P(s, x) = \frac{\gamma(s, x)}{\Gamma(s)}$ in which $\Gamma$ and $\gamma$ are the Gamma and lower incomplete Gamma functions, respectively (see, e.g., [8] 7.11.1). From [8] (8.10.11) we have that

$$1 - e^{-\alpha a x} \leq P(a, x) \leq (1 - e^{-\beta a x})$$

for

$$\begin{align*}
\alpha_a &= \begin{cases} 1, & 0 < a < 1, \\
da, & a > 1,
\end{cases} \\
\beta_a &= \begin{cases} d_a, & 0 < a < 1, \\
1, & a > 1,
\end{cases} \\
d_a &= (\Gamma(1 + a))^{-1/a}.
\end{align*}$$

Since $a = 1/2$ in our case, get that for $x \geq 0$

$$\text{erf}(x) \geq (1 - e^{-x^2})^{1/2},$$

and consequently

$$\text{erf}^{-1}(x) \leq \sqrt{-\log(-x^2 + 1)}$$

when $x \geq 0$. As $\Phi^{-1}(p) = \sqrt{2}\text{erf}^{-1}(2p - 1)$, the Lemma follows by substituting the upper bound for $\text{erf}^{-1}$.

Theorem 5 (Gaussian mechanism $(\epsilon, \delta)$-differential privacy). Let $q$ be a real valued function on databases with global sensitivity $\Delta$, and let $Z$ be a standard Gaussian random variable. Then for $\delta \leq 1$ and $\epsilon > 0$, the mechanism that returns a variate of $q(d) + \sigma Z$ is $(\epsilon, \delta)$-differentially private if $\sigma \geq b$ where

$$b = \frac{\Delta}{2\epsilon} \left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) + \sqrt{\left( \Phi^{-1} \left( 1 - \frac{\delta}{2} \right) \right)^2 + 2\epsilon} \right) \quad (11)$$

$$\leq \frac{\Delta \sqrt{2}}{2\epsilon} \left( \sqrt{\log \left( \frac{1}{\delta(2 - \delta)} \right)} + \sqrt{\log \left( \frac{1}{\delta(2 - \delta)} \right) + \epsilon} \right) \quad (12)$$

$$\leq \frac{\Delta \sqrt{2}}{\epsilon} \sqrt{\log \left( \frac{1}{\delta(2 - \delta)} \right)} + \frac{\Delta}{\sqrt{2\epsilon}} \quad (13)$$

where $\Phi^{-1}$ is the standard Gaussian quantile function.

Proof. Note that for $\delta = 1$, any mechanism fulfills $(\epsilon, \delta)$-differential privacy, and so does the one with $\sigma \geq b$ in particular. We also achieve equality for the upper bounds. Now let $\delta < 1$. Then, differential privacy and (11) follows from Lemmas 2 and 3. As $1 - \delta/2 \geq 1/2$, we apply Lemma 4 to get $\Phi^{-1}(1 - \delta/2) \leq \sqrt{-2\log(\delta(2 - \delta))}$. Substituting this bound for $\Phi^{-1}(1 - \delta/2)$ in (11), yields the bound (12) in the Theorem. Bound (13) is achieved by applying the fact that $\sqrt{a} + \sqrt{b} \leq \sqrt{a + b}$ for non-negative $a, b$ to the right hand side of (12). \qed
Remark 3. Theorem 5 can be extended unchanged to the multidimensional case using the exact argument Dwork and Roth use in their proof of Theorem A.1. in their monograph [3].

4 Illustrating constraints of the standard bound

Here we graphically illustrate that constraining \( \epsilon \) from above for the standard bound is indeed needed, both for meeting condition (1) and providing \((\epsilon, \delta)\)-differential privacy.

Recall from Lemma 2 that the sufficient condition for adding Gaussian noise to achieve \((\epsilon, \delta)\)-differential privacy is

\[
\Pr(|Z| > v(\sigma, 2)) \leq \delta
\]

for the standard Gaussian variable \( Z \) and

\[
v(\sigma, y) = \frac{\sigma \epsilon - \Delta}{y \sigma}.
\]

We further have that for \( s \) defined in (2),

\[
w(\epsilon, \delta) = v(s(\epsilon, \delta, \Delta), 2) = \frac{\sqrt{2} \left( 4 \log \left( \frac{s}{\epsilon \sigma} \right) - \epsilon \right)}{\nu \log \left( \frac{s}{\epsilon \sigma} \right)}
\]

which does not depend on \( \Delta \). Let

\[
g(\epsilon, \delta) = \delta - 2(1 - \Phi(w(\epsilon, \delta))) = \delta - \Pr(|Z| > w(\epsilon, \delta)).
\]

Now, the sign of \( g \) determines whether the condition (1) in Lemma 2 is met. A plot of \( g(\epsilon, \delta) \) can be seen in Figure 1a. Interestingly, there exist \( 0 < \delta < 1 \) and \( 0 < \epsilon < 1 \) such that (1) is violated as \( g(0.97, 0.97) < -0.005 \), suggesting that technically a constraint on \( \delta \) is needed to avoid violating (1).

However, as Balle et al. [2] point out, violating (1) is not the same as violating \((\epsilon, \delta)\)-differential privacy. They show that \((\epsilon, \delta)\)-differential privacy is achieved if and only if

\[
\Phi \left( \frac{\Delta}{2\sigma} - \frac{\epsilon \sigma}{\Delta} \right) - e^\epsilon \Phi \left( -\frac{\Delta}{2\sigma} - \frac{\epsilon \sigma}{\Delta} \right) \leq \delta.
\]

(14)

They do not provide a closed form bound based on (14) but provide a numerical algorithm to compute the smallest \( \sigma > 0 \) for which the above holds.

Substituting \( s(\epsilon, \delta, \Delta) \) for \( \sigma \) in the left side of (14), and subtracting this from \( \delta \) yields

\[
d(\epsilon, \delta) = \delta - (\Phi(-v(s(\epsilon, \delta, \Delta), 2)) - e^\epsilon \Phi(-v(s(\epsilon, \delta, \Delta), -2)))
\]

which does not depend on \( \Delta \). Analogous to \( g \) above, the sign of \( d \) determines whether (14) and \((\epsilon, \delta)\)-differential privacy is violated. A plot of \( d(\epsilon, \delta) \) can be seen in Figure 1b. Negative values indicate failure to be \((\epsilon, \delta)\)-differential privacy. The plot suggests that even if the inequality of the standard bound (2) is strict, it is safe to consider it non-strict for \( \epsilon \in (0, 1) \). What the plot also shows, is that the standard bound does not yield \((\epsilon, \delta)\)-differential privacy for all \( \epsilon > 0 \).
5 Comparing the two bounds

Dwork and Roth developed the bound by substituting the Cramér–Chernoff style tail bound $\Pr(\{|Z| > x\}) \leq 2\phi(x)/x$ into (1) and subsequently manipulating the result to determine the bound. This differs from the approach above resulting in our bound that is based on bounding the (inverse) error function. Furthermore, the standard bound is constrained to $\epsilon \in (0, 1)$, while our bound is valid for all $\epsilon > 0$.

We now compare these for the common interval $\epsilon \in (0, 1)$.

The ratio of the standard bound (2) and our bound (12) is

$$r(\epsilon, \delta) = \frac{2\sqrt{\log \left(\frac{5}{4\delta}\right)}}{\sqrt{\log \left(\frac{1}{\pi^2-\delta}\right)} + \sqrt{\log \left(\frac{1}{\pi^2-\delta}\right)} + \epsilon}.$$ (15)

A value for $r > 1$ means that the standard bound is larger than ours. A plot of the ratio $r$ can be seen in Figure 2a. Furthermore, the above ratio is 1 when

$$\epsilon = \epsilon(\delta) = 4 \log \left(\frac{5}{4\delta}\right) - 4\sqrt{\log \left(\frac{5}{4\delta}\right)} \sqrt{\log \left(\frac{1}{\delta(2-\delta)}\right)}.$$ (16)

A plot of $\epsilon(\delta)$ can be seen in Figure 2b.

The partial derivative of $r$ in (15) with respect to $\epsilon$ is

$$-\frac{\sqrt{\log \left(\frac{5}{4\delta}\right)}}{\left(\sqrt{\log \left(\frac{1}{\pi^2-\delta}\right)} + \sqrt{\log \left(\frac{1}{\pi^2-\delta}\right)} + \epsilon\right)^2 \sqrt{\log \left(\frac{1}{\pi^2-\delta}\right)} + \epsilon}.$$ (17)
This derivative is negative for $\delta > 0$ and $\epsilon > 0$, meaning that the ratio $r$ decreases as $\epsilon$ increases, which in turn means that the shaded area strictly under the curve of $\epsilon(\delta)$ in Figure 2b represents values $(\delta, \epsilon)$ for which $r > 1$, indicating that our bound (12) allows a smaller $\sigma$ than the standard bound (2). Numerical calculation yields that $\epsilon(0.946) > 1$, and looking at the curve in Figure 2b we see that $r > 1$ for $\epsilon \in (0, 1)$ and $\delta \in (0, 0.946)$.

Inspecting $r$, we see that as $\epsilon \to 0$ we get that $r \to \rho(\delta)$ where

$$
\rho(\delta) = \frac{\log \left( \frac{\delta}{1+\epsilon} \right)}{\log \left( \frac{1}{\delta(2-\delta)} \right)}.
$$

Since $r$ is decreasing in $\epsilon$, the function $\rho(\delta)$ provides an upper bound on $r$ for a given value of $\delta$. The function $\rho$ is increasing in $0 < \delta < 1$ and as $\delta \to 0$ we have that $\rho \to 1$. A plot of $\rho$ can be seen in Figure 2c. As $\rho(10^{-8}) < 1.026$, we see that for small $\delta$, the ratio $r$ is not that big. In other words, while our bound (12) is better than the standard bound for $\delta \in (0, 0.946)$, it is only slightly better for $\delta$ that can be considered small.

## 6 Conclusion

In Theorem 5 and by Remark 3 we presented a closed form lower bound (12) on $\sigma$ in terms of $\epsilon$ and $\delta$ needed to achieve $(\epsilon, \delta)$-differential privacy using the Gaussian Mechanism. Compared to the standard bound (2), our bound (12) has the following benefits:

a. it is valid for all $\epsilon > 0$, and
b. it allows a smaller $\sigma$ whenever $\epsilon \in (0, 1)$ and $\delta \in (0, 0.946)$.

While our bound is better for the above ranges of $\epsilon$ and $\delta$, we suggest that the main advantage of our bound is that it is valid for all $\epsilon > 0$ and that it can effectively be used without loss respective to the standard bound.

Like the standard bound (2), our bound (12) is based on the sufficient condition (1). Under this condition, the best possible $\sigma$ for $\delta < 1$ is given by (11) and must be larger than $\frac{\Delta}{\sqrt{2\epsilon}}$ (Lemma
3). As Balle et al. [2] demonstrate, the above condition is not necessary, and smaller \( \sigma \) can be gotten through numerically optimizing (14). A question we leave unaddressed for now is whether suitable closed form bounds on \( \Phi \) can be substituted into (14) to find an even better closed form bound on \( \sigma \).

References

[1] Martín Abadi et al. “Deep Learning with Differential Privacy”. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16 (2016), pp. 308–318. DOI: 10.1145/2976749.2978318. arXiv: 1607.00133. url: http://arxiv.org/abs/1607.00133 (visited on 03/01/2019).

[2] Borja Balle and Yu-Xiang Wang. “Improving the Gaussian Mechanism for Differential Privacy: Analytical Calibration and Optimal Denoising”. In: ed. by Jennifer Dy and Andreas Krause. Vol. 80. Proceedings of Machine Learning Research. Stockholmsmässan, Stockholm Sweden: PMLR, July 10–15, 2018, pp. 394–403. url: http://proceedings.mlr.press/v80/balle18a.html.

[3] Cynthia Dwork and Aaron Roth. “The Algorithmic Foundations of Differential Privacy”. In: Foundations and Trends® in Theoretical Computer Science 9.3–4 (Aug. 11, 2014), pp. 211–407. issn: 1551-305X, 1551-3068. doi: 10.1561/0400000042. url: http://www.nowpublishers.com/article/Details/TCS-042 (visited on 07/28/2017).

[4] Cynthia Dwork et al. “Calibrating Noise to Sensitivity in Private Data Analysis”. In: Proceedings of the Conference on Theory of Cryptography. 2006. doi: 10.1007/11681878_14.

[5] Cynthia Dwork et al. “Our Data, Ourselves: Privacy Via Distributed Noise Generation”. In: Advances in Cryptology (EUROCRYPT 2006). Vol. 4004. Saint Petersburg, Russia: Springer Verlag, May 2006, pp. 486–503. url: https://www.microsoft.com/en-us/research/publication/our-data-ourselves-privacy-via-distributed-noise-generation/.

[6] P. Kairouz, S. Oh, and P. Viswanath. “The Composition Theorem for Differential Privacy”. In: IEEE Transactions on Information Theory 63.6 (2017), pp. 4037–4049.

[7] Frank McSherry. How Many Secrets Do You Have? Feb. 8, 2017. url: https://github.com/frankmcsherry/blog/blob/master/posts/2017-02-08.md.

[8] F. W. J. Olver et al. NIST Digital Library of Mathematical Functions. 2020. url: http://dlmf.nist.gov/.

[9] Adrien Saumard and Jon A. Wellner. Log-Concavity and Strong Log-Concavity: A Review. 2014. arXiv: 1404.5886 [math.ST].

[10] Yu-Xiang Wang, Borja Balle, and Shiva Prasad Kasiviswanathan. “Subsampled Renyi Differential Privacy and Analytical Moments Accountant”. In: ed. by Kamalika Chaudhuri and Masashi Sugiyama. Vol. 89. Proceedings of Machine Learning Research. PMLR, Apr. 16–18, 2019, pp. 1226–1235. url: http://proceedings.mlr.press/v89/wang19b.html.

A Proofs from Section 2

Proof of Theorem 1. Let \( T = (a, b) \subseteq \mathbb{R} \) for some \( a < b \), let \( f(x) \leq e^\epsilon f(y) \) for all \( |x - y| \leq \Delta \), and let \( |v - w| \leq \Delta \). Then, \( \Pr(X + v \in T) = \int_{x \in T} f(x - v)dx \leq \int_{x \in T} e^\epsilon f(x - w)dy = e^\epsilon \int_{x \in T} f(x - w)dy = e^\epsilon \Pr(X + w \in T) \) since \( |v - w| \leq \Delta \) implies \( |(x - v) - (x - w)| \leq \Delta \) for any \( x \in T \). Since we can decompose any measurable \( S \) into a countable union of disjoint open intervals \( T \), we get \( \Pr(X + x \in S) \leq e^\epsilon \Pr(X + y \in S) \) for any \( |x - y| \leq \Delta \). The theorem then follows from \( |q(d) - q(d')| \leq \Delta \) for any \( (d, d') \in \mathcal{N} \). □
Proof of Corollary 1. Since \( f \) is strictly positive (and therefore also defined) everywhere, \( f(x)/f(x + d) \) is well defined for any \( x, y, d \in \mathbb{R} \). Furthermore, since \( f \) is also log-concave, \( f \) is unimodal, continuous, and for any \( d > 0 \) (\( d < 0 \)) we have that \( f(x)/f(x + d) \) is monotone and non-decreasing (non-increasing) in \( x \) (see, e.g., [9]). Since \( f \) is log-concave and positive everywhere, it decreases away from the mode \( x_m \) on both sides, and \( f(x + d) \) does the same for its mode \( x_m - d \).

Let \( 0 \leq z \leq \Delta \). We first show that \( f(x)/f(x + \Delta) \leq e^\epsilon \) implies \( f(x) \leq e^\epsilon f(x + z) \). Let \( z = 0 \), then since \( e^\epsilon > 1 \), we have that \( f(x) \leq e^\epsilon f(x + z) \) for all \( x \). Therefore, assume \( z > 0 \). Now, there exists \( x^* \in (x_m - z, x_m) \) such that \( f(x) \leq f(x + z) \) for \( x \leq x^* \) and \( f(x) \geq f(x + z) \) for \( x \geq x^* \). For \( x \leq x^* \), it follows that \( f(x) \leq e^\epsilon f(x + z) \). Now assume that \( x > x^* \). For \( x \geq x_m \), \( f(x) \geq f(x^*) \geq f(x + z) \), and consequently \( f(x) \leq e^\epsilon f(x + \Delta) \) implies \( f(x) \leq e^\epsilon f(x + z) \). Also, \( f(x + z) \geq f(x_m + \Delta) \), which means that \( f(x_m)/f(x_m + z) \leq f(x_m)/f(x_m + \Delta) \). Since \( f(x)/f(x + z) \) is non-decreasing and for \( x^* < x \leq x_m \) attains its maximum at \( f(x_m)/f(x_m + z) \leq f(x_m)/f(x_m + \Delta) \leq e^\epsilon \), we must have that \( f(x) \leq e^\epsilon f(x + z) \) also for \( x^* < x < x_m \). We now established that \( f(x_m)/f(x + \Delta) \leq e^\epsilon \) implies \( f(x) \leq e^\epsilon f(x + z) \). The case for \( f(x)/f(x - \Delta) \leq e^\epsilon \) implying \( f(x) \leq e^\epsilon f(x - z) \) follows from a mirrored argument.

Collecting the above, we now have \( f(x)/f(x + s\Delta) \leq e^\epsilon \) implies \( f(x) \leq e^\epsilon f(x + sz) \) for \( 0 \leq z \leq \Delta \) and all \( x \). Noting that \( |x - y| \leq \Delta \) if and only if \( y = x + sz \) for some \( s \in \{-1, 1\} \) and \( z \in [0, \Delta] \), we obtain that \( f(x)/f(x + s\Delta) \leq e^\epsilon \) implies \( f(x) \leq e^\epsilon f(y) \) for all \( x \) and \( y \) such that \( |x - y| \leq \Delta \). The corollary now follows from Theorem 1. \( \square \)

Proof of Lemma 2. Following Corollary 1 and Remark 1, we investigate

\[
\frac{\phi(x/\sigma)}{\phi((x + s\Delta)/\sigma)} \leq e^\epsilon,
\]

for \( s \in \{-1, 1\} \) and \( \phi = \Phi' \). The above holds as long as \( |x| \leq \frac{\sigma^2 + \Delta^2}{2} \). Define \( S_{\text{bad}} = \{ x \mid |x| > \frac{\sigma^2 + \Delta^2}{2} \} \) and \( S_{\text{good}} = \mathbb{R} - S_{\text{bad}} \). We now show that \( \Pr(\sigma Z \in S_{\text{bad}}) \leq \delta \) implies \((\epsilon, \delta)\)-differential privacy of \( q(d) + \sigma Z \). First, define

\[
S^+ = q(d) + S_{\text{good}}
\]

\[
S^- = q(d) + S_{\text{bad}}.
\]

Now, for any \( S' \subseteq S^+ \) and neighboring database \( d' \) we have

\[
\Pr(q(d) + \sigma Z \in S') \leq e^\epsilon \Pr(q(d') + \sigma Z \in S').
\]

Then for fixed measurable \( S \subset \mathbb{R} \)

\[
\Pr(q(d) + \sigma Z \in S \cap S^-) \leq \Pr(q(d) + \sigma Z \in S^-) = \Pr(\sigma Z \in S_{\text{bad}}) \leq \delta
\]

\[
\Pr(q(d) + \sigma Z \in S \cap S^+) \leq e^\epsilon \Pr(q(d') + \sigma Z \in S \cap S^+) \leq e^\epsilon \Pr(q(d') + \sigma Z \in S)
\]

and

\[
\Pr(q(d) + \sigma Z \in S) = \Pr(q(d) + \sigma Z \in S \cap S^+) + \Pr(q(d) + \sigma Z \in S \cap S^-)
\]

\[
\leq \Pr(q(d) + \sigma Z \in S \cap S^+) + \delta
\]

\[
\leq e^{-\epsilon} \Pr(q(d') + \sigma Z \in S) + \delta.
\]
For $\sigma > 0$

$$\Pr \left( |\sigma Z| \leq \frac{\sigma^2 \epsilon}{\Delta} - \frac{\Delta}{2} \right) = \Pr \left( |Z| \leq \frac{\sigma \epsilon}{\Delta} - \frac{\Delta}{2\sigma} \right),$$

from which the Lemma follows.