Full proof on the differential privacy property of $\mathcal{M}_{\mathcal{H}}$

ABSTRACT

KEYWORDS

Differential privacy, Bayesian inference, Hellinger distance

1 PRELIMINARIES

Bayesian Inference.

Given a prior belief $\Pr(\theta)$ on some parameter θ, and an observation $\mathbf{x}$, the posterior distribution on θ given $\mathbf{x}$ is computed as:

$$\Pr(\theta|\mathbf{x}) = \frac{\Pr(\mathbf{x}|\theta) \cdot \Pr(\theta)}{\Pr(\mathbf{x})}$$

where the expression $\Pr(\mathbf{x}|\theta)$ denotes the *likelihood* of observing $\mathbf{x}$ under a value of θ. Since we consider $\mathbf{x}$ to be fixed, the likelihood is a function of θ. For the same reason $\Pr(\mathbf{x})$ is a constant independent of θ. Usually in statistics the prior distribution $\Pr(\theta)$ is chosen so that it represents the initial belief on θ, that is, when no data has been observed. In practice though, prior distributions and likelihood functions are usually chosen so that the posterior belongs to the same *family* of distributions. In this case we say that the prior is conjugate to the likelihood function. Use of a conjugate prior simplifies calculations and allows for inference to be performed in a recursive fashion over the data.

Beta-binomial System.

In this work we will consider a specific instance of Bayesian inference and one of its generalizations. specifically, a Beta-binomial mode. We will consider the situation the underlying data is binomial distribution ($\sim$ *binomial*(θ)), where θ represents the parameter –informally called *bias*– of a Bernoulli distributed random variable. The prior distribution over $\theta \in [0, 1]$ is going to be a beta distribution, $\mathrm{beta}(\alpha, \beta)$, with parameters $\alpha, \beta \in \mathbb{R}^+$, and with p.d.f:

$$\Pr(\theta) \equiv \frac{\theta^{\alpha}(1-\theta)^{\beta}}{\mathrm{B}(\alpha, \beta)}$$

where $\mathrm{B}(\cdot,\cdot)$ is the beta function. The data $\mathbf{x}$ will be a sequence of $n \in \mathbb{N}$ binary values, that is $\mathbf{x} = (x_1, \ldots x_n), x_i \in \{0, 1\}$, and the likelihood function is:

$$\Pr(\mathbf{x}|\theta) \equiv \theta^{\Delta\alpha}(1-\theta)^{n-\Delta\alpha}$$

where $\Delta\alpha = \sum_{i=1}^{n} x_i$. From this it can easily be derived that the posterior distribution is:

$$\Pr(\theta|\mathbf{x}) = \mathsf{beta}(\alpha + \Delta\alpha, \beta + n - \Delta\alpha)$$

Dirichlet-multinomial Systems.

The beta-binomial model can be immediately generalized to Dirichlet-multinomial, with underlying data multinomially distributed. The *bias* is represented by parameter $\boldsymbol{\theta}$, the vector of parameters of a categorically distributed random variable. The prior distribution over $\boldsymbol{\theta} \in [0, 1]^k$ is given by a Dirichelet distribution, $\mathsf{DL}(\boldsymbol{\alpha})$, for $k \in \mathbb{N}$, and $\boldsymbol{\alpha} \in (\mathbb{R}^+)^k$, with p.d.f:

$$\Pr(\boldsymbol{\theta}) \equiv \frac{1}{\mathrm{B}(\boldsymbol{\alpha})} \cdot \prod_{i=1}^{k} \theta_i^{\alpha_i - 1}$$

where $\mathrm{B}(\cdot)$ is the generalized beta function. The data $\mathbf{x}$ will be a sequence of $n \in \mathbb{N}$ values coming from a universe $\mathcal{X}$, such that $\mid \mathcal{X} \mid = k$. The likelihood function will be:

$$\Pr(\mathbf{x}|\boldsymbol{\theta}) \equiv \prod_{a_i \in \mathcal{X}} \theta_i^{\Delta\alpha_i},$$

with $\Delta\alpha_i = \sum_{j=1}^{n} [x_j = a_i]$, where $[\cdot]$ represents Iverson bracket notation. Denoting by $\Delta\boldsymbol{\alpha}$ the vector $(\Delta\alpha_1, \ldots \Delta\alpha_k)$ the posterior distribution over $\boldsymbol{\theta}$ turns out to be

$$\Pr(\boldsymbol{\theta}|\mathbf{x}) = \mathsf{DL}(\boldsymbol{\alpha} + \Delta\boldsymbol{\alpha}).$$

where $+$ denotes the componentwise sum of vectors of reals.

Differential Privacy.

Definition 1.1. $\epsilon-$differential privacy.

A randomized mechanism $\mathcal{M} : \mathcal{X} \to \mathcal{Y}$ is differential privacy, iff for any adjacent input $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$, a metric H over $\mathcal{Y}$ and a $B \subseteq H(\mathcal{Y})$, $\mathcal{M}$ satisfies:

$$\mathbb{P}[H(\mathcal{M}(\mathbf{x})) \in B] = e^{\epsilon}\mathbb{P}[H(\mathcal{M}(\mathbf{x}')) \in B],$$

where $\mathbf{x} = (x_i)_{i=1}^{n}$ and $\mathbf{x} = (x_i')_{i=1}^{n}$ is adjacent if there is only one j that $x_j \neq x_j'$ and $x_i = x_i'$ for $i = 1, 2, \cdots, n; i \neq j$.

Definition 1.2. $(\epsilon, \delta)-$differential privacy.

A randomized mechanism $\mathcal{M} : \mathcal{X} \to \mathcal{Y}$ is differential privacy, iff for any adjacent input $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$, a metric H over $\mathcal{Y}$ and a $B \subseteq H(\mathcal{Y})$, $\mathcal{M}$ satisfies:

$$\mathbb{P}[H(\mathcal{M}(\mathbf{x})) \in B] = e^{\epsilon}\mathbb{P}[H(\mathcal{M}(\mathbf{x}')) \in B] + \delta,$$

vwhere $\mathbf{x} = (x_i)_{i=1}^{n}$ and $\mathbf{x} = (x_i')_{i=1}^{n}$ is adjacent if there is only one j that $x_j \neq x_j'$ and $x_i = x_i'$ for $i = 1, 2, \cdots, n; i \neq j$.

2 MECHANISM PROPOSITION

Given a prior distribution $\boldsymbol{\beta}_{\text{prior}} = \mathsf{beta}(\alpha, \beta)$ and a sequence of n observations $\mathbf{x} \in \{0, 1\}^n$, we define the follwing set:

$$\mathcal{R}_{\text{post}} \equiv \{\mathsf{beta}(\alpha', \beta') \mid \alpha' = \alpha + \Delta\alpha, \beta' = \beta + n - \Delta\alpha\},$$

where $\Delta\alpha$ is as defined in Section1. Notice that $\mathcal{R}_{\text{post}}$ has $n + 1$ elements, and the Bayesian Inference process will produce an element from $\mathcal{R}_{\text{post}}$ that we denote by $\mathsf{BI}(\mathbf{x})$ – we don't explicitely parametrize the result by the prior, which from now on we consider fixed and we denote it by $\boldsymbol{\beta}_{\text{prior}}$.

2.1 $\mathcal{M}_{\mathcal{H}}$: Smoothed Hellinger Distance Based Exponential Mechanism

Definition 2.1. The mechanism $\mathcal{M}_{\mathcal{H}}(x)$ outputs a candidate $r \in \mathcal{R}_{\text{post}}$ with probability

$$\Pr_{z \sim \mathcal{M}_{\mathcal{H}}}[z = r] = \frac{exp\left(\frac{-\epsilon \cdot \mathcal{H}(\mathsf{BI}(\mathbf{x}), r)}{2 \cdot S(\mathbf{x})}\right)}{\sum_{r \in \mathcal{R}_{\text{post}}} exp\left(\frac{-\epsilon \cdot \mathcal{H}(\mathsf{BI}(\mathbf{x}), r)}{2 \cdot S(\mathbf{x})}\right)}.$$

where $S_{\beta}(x)$ is the smooth sensitivity of $\mathcal{H}(\mathsf{BI}(x), -)$, calculated by:

$$S(\mathbf{x}) = \max_{\mathbf{x}' \in \{0,1\}^n} \left\{ LS(\mathbf{x}') \cdot e^{-\gamma \cdot d(\mathbf{x}, \mathbf{x}')} \right\}, \tag{1}$$

where d is the Hamming distance between two datasets, and $\beta = \beta(\epsilon, \delta)$ is a function of ϵ and δ.

This mechanism is based on the basic exponential mechanism [1], with $\mathcal{R}_{\text{post}}$ as the range and $\mathcal{H}(\cdot, \cdot)$ as the scoring function. The difference is that in this mechanism we don't calibrate the noise w.r.t. to the global sensitivity of the scoring function but w.r.t. to the smooth sensitivity $S(\mathbf{x})$ – defined by Nissim, Raskhodnikova, and Smith [2]– of $\mathcal{H}(\mathsf{BI}(\mathbf{x}), \cdot)$.

$\gamma = \gamma(\epsilon, \delta)$ is a function of ϵ and δ to be determined later, and where $LS(\mathbf{x}')$ denotes the local sensitivity at $\mathsf{BI}(\mathbf{x}')$, or equivalently at $\mathbf{x}'$, of the scoring function used in our mechanism.

This mechanism also extends to the Dirichlet-multinomial system $\mathsf{DL}(\boldsymbol{\alpha})$ by rewriting the Hellinger distance as:

$$\mathcal{H}(\mathsf{DL}(\boldsymbol{\alpha}_1), \mathsf{DL}(\boldsymbol{\alpha}_2)) = \sqrt{1 - \frac{\mathrm{B}(\frac{\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2}{2})}{\sqrt{\mathrm{B}(\boldsymbol{\alpha}_1)\mathrm{B}(\boldsymbol{\alpha}_2)}}},$$

and by replacing the $\mathcal{R}_{\text{post}}$ with set of posterior Dirichlet distributions candidates. Also, the smooth sensitivity $S(\mathbf{x})$ in (1) will be computed by letting $\mathbf{x}'$ range over all the elements in $\mathcal{X}^n$ adjacent to $\mathbf{x}$. Notice that $\mathcal{R}_{\text{post}}$ has $\binom{n+1}{m-1}$ elements in this case. We will denote by $\mathcal{M}^D_{\mathcal{H}}$ the mechanism for the Dirichlet-multinomial system.

By setting the γ as $\ln(1 - \frac{\epsilon}{2\ln(\frac{\delta}{2(n+1)})})$ (or $\ln(1 - \frac{\epsilon}{2\ln(\frac{\delta}{2|\mathcal{R}_{\text{post}}|})})$ when generalized to Dirichlet-multinomial System), $\mathcal{M}_{\mathcal{H}}$ is (ϵ, δ)−differentially private.

3 PRIVACY ANALYSIS

3.1 Privacy Analysis for $\mathcal{M}_{\mathcal{H}}$

The differential privacy property of $\mathcal{M}_{\mathcal{H}}$ is proved based on the holds of the two properties: *sliding property* and *dilation property*.

Sliding Property of $\mathcal{M}_{\mathcal{H}}$

Lemma 3.1. *Given $\mathcal{M}_{\mathcal{H}}(x)$ calibrated on the smooth sensitivity. Let $\lambda = f(\epsilon, \delta)$, $\epsilon \geq 0$ and $|\delta| < 1$. Then, the following* sliding property *holds:*

$$\Pr_{r \sim \mathcal{M}_{\mathcal{H}}(x)}[u(r, x) = \hat{s}] \leq e^{\frac{\epsilon}{2}} \Pr_{r \sim \mathcal{M}_{\mathcal{H}}(x)}[u(r, x) = (\Delta + \hat{s})] + \frac{\delta}{2},$$

Proof. In what follows, we will use a correspondence between the probability $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r]$ of every $r \in \mathcal{R}_{\text{post}}$ and the probability $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[\mathcal{H}(\mathsf{BI}(x), z) = \mathcal{H}(\mathsf{BI}(x), r)]$ for the utility score for r. In particular, for every $r \in \mathcal{R}_{\text{post}}$ we have:

$$\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r] = \frac{1}{2}\left(\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[\mathcal{H}(\mathsf{BI}(x), z) = \mathcal{H}(\mathsf{BI}(x), r)] \right)$$

To see this, it is enough to notice that: $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r]$ is proportional too $\mathcal{H}(\mathsf{BI}(x), r)$, i.e., $u(x, z)$. We can derive, if $u(r, x) = u(r', x)$ then $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r] = \Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r']$. We assume the number of candidates $z \in \mathcal{R}$ that satisfy $u(z, x) = u(r, x)$ is $|r|$, we have $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[u(z, x) = u(r, x)] = |r| \Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r]$. Because Hellinger distance $\mathcal{H}(\mathsf{BI}(x), z)$ is axial symmetry, where the $\mathsf{BI}(x)$ is the symmetry axis. It can be infer that $|z| = 2$ for any candidates, apart from the true output, i.e., $\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[u(z, x) = u(r, x)] = 2 \Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[z = r]$. This parameter can be eliminate in both sides in proof.

We denote the normalizer of the probability mass in $\mathcal{M}_{\mathcal{H}}(x)$: $\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon u(r', x)}{2S(x)})$ as $NL(x)$:

$$\begin{aligned} LHS = \Pr_{r \sim \mathcal{M}_{\mathcal{H}}(x)}[u(r, x) = \hat{s}] &= \frac{exp(\frac{\epsilon \hat{s}}{2S(x)})}{NL(x)} \\ &= \frac{exp(\frac{\epsilon(\hat{s} + \Delta - \Delta)}{2S(x)})}{NL(x)} \\ &= \frac{exp(\frac{\epsilon(\hat{s} + \Delta)}{2S(x)} + \frac{-\epsilon\Delta}{2S(x)})}{NL(x)} \\ &= \frac{exp(\frac{\epsilon(\hat{s} + \Delta)}{2S(x)})}{NL(x)} \cdot e^{\frac{-\epsilon\Delta}{2S(x)}}. \end{aligned}$$

By bounding the $\Delta \geq -S(x)$, we can get:

$$\begin{aligned} \frac{exp(\frac{\epsilon(\hat{s} + \Delta)}{2S(x)})}{NL(x)} \cdot e^{\frac{-\epsilon\Delta}{2S(x)}} &\leq \frac{exp(\frac{\epsilon(\hat{s} + \Delta)}{2S(x)})}{NL(x)} \cdot e^{\frac{\epsilon}{2}} \\ &= e^{\frac{\epsilon}{2}} \Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[u(r, x) = (\Delta + \hat{s})] \leq RHS \end{aligned}$$

□

Dilation Property of $\mathcal{M}_{\mathcal{H}}$

Lemma 3.2. *for any exponential mechanism $\mathcal{M}_{\mathcal{H}}(x)$, $\lambda < |\beta|$, ϵ, $|\delta| < 1$ and $\beta \leq \ln(1 - \frac{\epsilon}{2\ln(\frac{\delta}{2(n+1)})})$, the dilation property holds:*

$$\Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[u(z, x) = c] \leq e^{\frac{\epsilon}{2}} \Pr_{z \sim \mathcal{M}_{\mathcal{H}}(x)}[u(z, x) = e^{\lambda}c] + \frac{\delta}{2},$$

where the sensitivity in mechanism is still smooth sensitivity as above.

Proof. The sensitivity is always greater than 0, and our utility function $-\mathcal{H}(\mathsf{BI}(x), z)$ is smaller than zero, i.e., $u(z, x) \leq 0$, we need to consider two cases where $\lambda < 0$, and $\lambda > 0$:

We set the $h(c) = Pr[u(\mathcal{M}_{\mathcal{H}}(x)) = c] = 2\frac{exp(\frac{\epsilon z}{2S(x)})}{NL(x)}$.

We first consider $\lambda < 0$. In this case, $1 < e^{\lambda}$, so the ratio $\frac{h(c)}{h(e^{\lambda}c)} = \frac{exp(\frac{\epsilon c}{2S(x)})}{exp(\frac{\epsilon(c \cdot e^{\lambda})}{2S(x)})}$ is at most $\frac{\epsilon}{2}$.

Next, we proof the dilation property for $\lambda > 0$, The ratio of $\frac{h(c)}{h(e^{\lambda}c)}$ is $\exp(\frac{\epsilon}{2} \cdot \frac{u(\mathcal{M}_{\mathcal{H}}(x))(1-e^{\lambda})}{S(x)})$. Consider the event $G = \{\mathcal{M}_{\mathcal{H}}(x) : u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})}\}$. Under this event, the log-ratio above is at most $\frac{\epsilon}{2}$. The probability of G under density $h(c)$ is $1 - \frac{\delta}{2}$. Thus, the probability of a given event z is at most $Pr[c \cap G] + Pr[\overline{G}] \leq e^{\frac{\epsilon}{2}} Pr[e^{\lambda}c \cap G] + \frac{\delta}{2} \leq e^{\frac{\epsilon}{2}} Pr[e^{\lambda}c] + \frac{\delta}{2}$.

Detail proof:

By simplification, we get this formula: $u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})}$

- $\lambda < 0$

  The left hand side will always be smaller than 0 and the right hand side greater than 0. This will always holds, i.e.

  $$u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})}$$

  is always true when $\lambda < 0$

- $\lambda > 0$

  Because $\hat{s} = u(r)$ where $r \sim \mathcal{M}_{\mathcal{H}}(x)$, we can substitute $\hat{s}$ with $u(\mathcal{M}_{\mathcal{H}}(x))$. Then, what we need to proof under the case $\lambda > 0$ is:

  $$u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})} \tag{2}$$

  Based on the accuracy property of exponential mechanism:

  $$Pr[u(\mathcal{M}_E(x, u, \mathcal{R}_{\text{post}})) \leq c] \leq \frac{|\mathcal{R}|exp(\frac{\epsilon c}{2GS})}{|\mathcal{R}_{OPT}|exp(\frac{\epsilon OPT_{u(x)}}{2GS})}$$

  we derived the accuracy bound for $\mathcal{M}_{\mathcal{H}}$:

  $$Pr[u(\mathcal{M}_{\mathcal{H}}(x)) \leq c] \leq |\mathcal{R}_{\text{post}}|exp(\frac{\epsilon c}{2S(x)})$$

  In Beta-binomial system, $|\mathcal{R}_{\text{post}}| = n + 1$, apply this bound to eq. 2:

  $$\begin{aligned} Pr[u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})}] &= (n+1)exp(\frac{\epsilon S(x)}{(1-e^{\lambda})}/2S(x)) \\ &= (n+1)exp(\frac{\epsilon}{2(1-e^{\lambda})}) \end{aligned}$$

  When we set $\lambda \leq \ln(1 - \frac{\epsilon}{2\ln(\frac{\delta}{2(n+1)})})$, it is easily to derive that $Pr[u(\mathcal{M}_{\mathcal{H}}(x)) \leq \frac{S(x)}{(1-e^{\lambda})}] \leq \frac{\delta}{2}$.

  In Dirichlet-multinomial system, λ is set as $\leq \ln(1 - \frac{\epsilon}{2\ln(\frac{\delta}{2|\mathcal{R}_{\text{post}}|})})$ since $|\mathcal{R}_{\text{post}}| \neq n + 1$ any more.

□

(ϵ, δ)−Differential Privacy of $\mathcal{M}_{\mathcal{H}}$

Lemma 3.3. *$\mathcal{M}_{\mathcal{H}}$ is (ϵ, δ)-differential privacy.*

Proof. of Lemma 3.3: For all neighboring $x, y \in D^n$ and all sets $\mathcal{S}$, we need to show that:

$$\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[z \in \mathcal{S}] \leq e^{\epsilon} \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(y)}[z \in \mathcal{S}] + \delta.$$

Given that $2\Big(\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[z \in \mathcal{S}]\Big) = \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[u(x,z) \in \mathcal{U}]$, let $\mathcal{U}_1 = \frac{u(y,z)-u(x,z)}{S(x)}$, $\mathcal{U}_2 = \mathcal{U} + \mathcal{U}_1$ and $\mathcal{U}_3 = \mathcal{U}_2 \cdot \frac{S(x)}{S(y)} \cdot \ln(\frac{NL(x)}{NL(y)})$. Then,

$$\begin{aligned} 2\Big(\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[z \in \mathcal{S}]\Big) &= \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[u(x,z) \in \mathcal{U}] \\ &\leq e^{\epsilon/2} \cdot \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[u(x,z) \in \mathcal{U}_2] \\ &\leq e^{\epsilon} \cdot \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[u(x,z) \in \mathcal{U}_3] + e^{\epsilon/2} \cdot \frac{\delta'}{2} \\ &= e^{\epsilon} \cdot \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(y)}[u(y,z) \in \mathcal{U}] + \delta = 2\Big(e^{\epsilon} \cdot \Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[z \in \mathcal{S}]\Big) \end{aligned}$$

The first inequality holds by the sliding property, since the $\mathcal{U}_1 \geq -S(x)$. The second inequality holds by the dilation property, since $\frac{S(x)}{S(y)} \cdot \ln(\frac{NL(x)}{NL(y)}) \leq 1 - \frac{\epsilon}{2\ln(\frac{\delta}{2(n+1)})}$.

□

4 ACCURACY ANALYSIS

4.1 Accuracy Bound for Baseline Mechanisms

4.2 Accuracy Bound for $\mathcal{M}_{\mathcal{H}}$

We explored three accuracy bounds for our exponential mechanism with smooth sensitivity.

First is the tight bound with very accurate calculation.

$$\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[\mathcal{H}(\mathsf{BI}(x), z) \geq c] = \sum_{\{z|\mathcal{H}(\mathsf{BI}(x),z)\geq c\}} \frac{e^{\frac{-\epsilon\mathcal{H}(\mathsf{BI}(x),z)}{S(x)}}}{NL_x}.$$

In order to be more efficient, we designed the second accuracy bound which is slightly looser than the first one:

$$\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[\mathcal{H}(\mathsf{BI}(x), z) \geq c] \leq \frac{|R| \exp(\frac{-\epsilon c}{S(x)})}{NL_x}.$$

In the second bound, we still need to calculate the normaliser every time. So we want make further improvements on efficiency like follows:

$$\Pr_{z\sim\mathcal{M}_{\mathcal{H}}(x)}[\mathcal{H}(\mathsf{BI}(x), z) \geq c] \leq \frac{|R| \exp(\frac{-\epsilon c}{S(x)})}{N(n)},$$

where we replace the NL_x with a value only related to the size of the data. However, we haven't figured out the formula of this $N(n)$.

Moreover, based on the accuracy bound in Sec. **??**, we can derive a loose bound:

$$Pr[u(\mathcal{M}_{\mathcal{H}}(x)) \leq c] \leq |\mathcal{R}_{\text{post}}|exp(\frac{\epsilon c}{2S(x)}),$$

which has been used in the dilation property proof.

REFERENCES

[1] Frank McSherry and Kunal Talwar. Mechanism Design via Differential Privacy. In *FOCS, 2007.*

[2] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *STOC, 2007.* 75–84.