

# Notes of DP - Bayesian Inference

## 1 Setting up

The Bayesian inference process is denoted as  $\text{BI}(x, \text{prior})$  taking an observed data set  $x \in \mathcal{X}^n$  and a prior distribution as input, outputting a posterior distribution *posterior*. For conciseness, when prior is given, we use  $\text{BI}(x)$ .

For now, we already have a prior distribution *prior*, an observed data set  $x$ .

### 1.1 Exponential Mechanism with Global Sensitivity

#### 1.1.1 Mechanism Set up

In exponential mechanism, candidate set  $R$  can be obtained by enumerating  $y \in \mathcal{X}^n$ , i.e.

$$R = \{\text{BI}(y) \mid y \in \mathcal{X}^n\}.$$

Hellinger distance  $H$  is used here to score these candidates. The utility function:

$$u(x, r) = -H(\text{BI}(x), r); r \in R. \quad (1)$$

Exponential mechanism with global sensitivity selects and outputs a candidate  $r \in R$  with probability proportional to  $\exp(\frac{\epsilon u(x, r)}{2\Delta_g u})$ :

$$P[r] = \frac{\exp(\frac{\epsilon u(x, r)}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})},$$

where global sensitivity is calculated by:

$$\Delta_g u = \max_{\{|x', y'| \leq 1; x', y' \in \mathcal{X}^n\}} \max_{\{r \in R\}} |H(\text{BI}(x'), r) - H(\text{BI}(y'), r)|$$

#### 1.1.2 Security Analysis

It can be proved that exponential mechanism with global sensitivity is  $\epsilon$ -differentially private. We denote the BI with privacy mechanism as  $\text{PrivInfer}$ . For adjacent data set  $\|x, y\|_1 = 1$ :

$$\begin{aligned} \frac{P[\text{PrivInfer}(x, u, R) = r]}{P[\text{PrivInfer}(y, u, R) = r]} &= \frac{\frac{\exp(\frac{\epsilon u(x, r)}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})}}{\frac{\exp(\frac{\epsilon u(y, r)}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r')}{2\Delta_g u})}} \\ &= \left( \frac{\exp(\frac{\epsilon u(x, r)}{2\Delta_g u})}{\exp(\frac{\epsilon u(y, r)}{2\Delta_g u})} \right) \cdot \left( \frac{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r')}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})} \right) \\ &= \exp\left(\frac{\epsilon(u(x, r) - u(y, r))}{2\Delta_g u}\right) \cdot \left( \frac{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r')}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})} \right) \\ &\leq \exp\left(\frac{\epsilon}{2}\right) \cdot \exp\left(\frac{\epsilon}{2}\right) \cdot \left( \frac{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_g u})} \right) \\ &= \exp(\epsilon). \end{aligned}$$

Then,  $\frac{P[\text{PrivInfer}(x, u, R) = r]}{P[\text{PrivInfer}(y, u, R) = r]} \geq \exp(-\epsilon)$  can be obtained by symmetry.

## 1.2 Exponential Mechanism with Local Sensitivity

### 1.2.1 Mechanism Set up

Exponential mechanism with local sensitivity share the same candidate set and utility function as it with global sensitivity. This outputs a candidate  $r \in R$  with probability proportional to  $\exp(\frac{\epsilon u(x, r)}{2\Delta_l u})$ :

$$P[r] = \frac{\exp(\frac{\epsilon u(x, r)}{2\Delta_l u})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_l u})},$$

where local sensitivity is calculated by:

$$\Delta_l u(x) = \max_{\{x, y' | \leq 1; y' \in \mathcal{X}^n\}} \max_{\{r \in R\}} |H(\text{Bl}(x), r) - H(\text{Bl}(y'), r)|$$

### 1.2.2 Security Analysis

We will then prove that exponential mechanism with local sensitivity is non-differentially private.

$$\begin{aligned} \frac{P[\text{PrivInfer}(x, u, R) = r]}{P[\text{PrivInfer}(y, u, R) = r]} &= \exp\left(\frac{\epsilon u(x, r)}{2\Delta_l u(x)} - \frac{\epsilon u(y, r)}{2\Delta_l u(y)}\right) \cdot \left(\frac{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r')}{2\Delta_l u(y)})}{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r')}{2\Delta_l u(x)})}\right) \\ &= \frac{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r)}{2\Delta_l u(x)} + \frac{\epsilon u(y, r')}{2\Delta_l u(y)})}{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r)}{2\Delta_l u(y)} + \frac{\epsilon u(x, r')}{2\Delta_l u(x)})}. \end{aligned}$$

Without loss of generality, we consider the case that  $\Delta_l u(y) < \Delta_l u(x)$ ,  $r = \arg(\max_{r' \in R} \{u(x, r')\}) = \arg(\min_{r' \in R} \{u(y, r')\})$  and  $\Delta_l u(y) = u(x, r) - u(y, r)$ . We have:

$$\begin{aligned} \frac{\sum_{r' \in R} \exp(\frac{\epsilon u(x, r)}{2\Delta_l u(x)} + \frac{\epsilon u(y, r')}{2\Delta_l u(y)})}{\sum_{r' \in R} \exp(\frac{\epsilon u(y, r)}{2\Delta_l u(y)} + \frac{\epsilon u(x, r')}{2\Delta_l u(x)})} &> \frac{\sum_{r' \in R} \exp(\frac{\epsilon(u(x, r) + u(y, r'))}{2\Delta_l u(x)})}{\sum_{r' \in R} \exp(\frac{\epsilon(u(y, r) + u(x, r'))}{2\Delta_l u(y)})} \\ &> \frac{|R| \exp(\frac{\epsilon(u(x, r) + u(y, r))}{2\Delta_l u(x)})}{|R| \exp(\frac{\epsilon(u(y, r) + u(x, r))}{2\Delta_l u(y)})} \\ &= \exp\left(\frac{\epsilon}{2} \left(\frac{u(x, r) + u(y, r)}{\Delta_l u(x)} - \frac{u(x, r) + u(y, r)}{\Delta_l u(y)}\right)\right). \end{aligned}$$

From Eq. 1,  $\{u(x, r') \leq 0 | r' \in R\}$  and  $\{u(y, r') \leq 0 | r' \in R\}$ , we can infer that  $r = \arg(\max_{r' \in R} \{u(x, r')\}) = \text{Bl}(x)$  and  $u(x, r) = 0$ . From  $\Delta_l u(y) = u(x, r) - u(y, r)$ , we can also infer that  $\Delta_l u(y) = -u(y, r)$ . Then, the following relationship between  $u(x, r)$ ,  $u(y, r)$ ,  $\Delta_l u(x)$  and  $\Delta_l u(y)$ :

$$\begin{aligned} -\Delta_l u(x) &< \Delta_l u(y) \\ \Delta_l u(x) - \Delta_l u(y) &< 2\Delta_l u(x) \\ -\Delta_l u(y)(\Delta_l u(y) - \Delta_l u(x)) &< 2\Delta_l u(x)\Delta_l u(y) \\ u(y, r)(\Delta_l u(y) - \Delta_l u(x)) &< 2\Delta_l u(x)\Delta_l u(y) \\ \frac{u(x, r) + u(y, r)}{\Delta_l u(x)} - \frac{u(x, r) + u(y, r)}{\Delta_l u(y)} &> 2. \end{aligned}$$

holds.

Then we can have:

$$\begin{aligned}
& \exp\left(\frac{\epsilon}{2}\left(\frac{u(x, r) + u(y, r)}{\Delta_l u(y)} - \frac{u(x, r) + u(y, r)}{\Delta_l u(x)}\right)\right) \\
& > \exp\left(\frac{\epsilon}{2} * 2\right) \\
& = \exp(\epsilon),
\end{aligned}$$

i.e.

$$\frac{P[\text{PrivInfer}(x, u, R) = r]}{P[\text{PrivInfer}(y, u, R) = r]} > \exp(\epsilon).$$

Since there are cases where exponential mechanism with local sensitivity's privacy loss is greater than  $e^\epsilon$ , we can say it is non-differentially private.

### 1.3 Exponential Mechanism of Varying Sensitivity

#### 1.3.1 Mechanism Setting up

#### 1.3.2 Security Analysis

### 1.4 Exponential Mechanism of Smooth Sensitivity

#### 1.4.1 Mechanism Setting up

#### 1.4.2 Security Analysis

## 2 Privacy Fix

### 2.1 Propositions

Assume we have a prior distribution  $\text{beta}(1, 1)$ , an observed data set  $x \in \{0, 1\}^n$ ,  $n > 0$ . We use the  $x + 1$  and  $x - 1$  to denote:

$$\begin{aligned}
& \text{if } \text{BayesInfer}(x) = \text{beta}(a_1 + 1, b_1 + 1) \\
& \text{then } \text{BayesInfer}(x + 1) = \text{beta}((a_1 + 1) + 1, (b_1 - 1) + 1) \\
& \quad \text{BayesInfer}(x - 1) = \text{beta}((a_1 - 1) + 1, (b_1 + 1) + 1),
\end{aligned}$$

$x_0$  to denote:

$$\begin{aligned}
& \text{if } n \text{ is even} \\
& \text{then } \text{BI}(x_0) = \text{beta}\left(\frac{n}{2} + 1, \frac{n}{2} + 1\right) \\
& \text{else } \text{BI}(x_0) = \left\{ \text{beta}\left(\frac{n+1}{2} + 1, \frac{n-1}{2} + 1\right), \right. \\
& \quad \left. \text{beta}\left(\frac{n-1}{2} + 1, \frac{n+1}{2} + 1\right) \right\}
\end{aligned}$$

$\text{beta}(\alpha, \beta)$  is the beta function with two arguments  $\alpha$  and  $\beta$ .

Then, we have the following three statements, and proofs of the statements.

I  $\text{H}(\text{BI}(x), \text{BI}(x + 1)) < \text{H}(\text{BI}(x + 1), \text{BI}(x + 2)) \ \forall x \geq x_0$ ;  
or  $\text{H}(\text{BI}(x), \text{BI}(x + 1)) > \text{H}(\text{BI}(x + 1), \text{BI}(x + 2)) \ \forall x \leq x_0$ .

II  $\Delta_l u(x) = \text{H}(\text{BI}(x), \text{BI}(x + 1)), \forall x \geq x_0$ ;  
 $\Delta_l u(x) = \text{H}(\text{BI}(x), \text{BI}(x - 1)), \forall x \leq x_0$ .

III  $\forall x \neq x_0 : \Delta_l u(x) > \Delta_l u(x_0)$ .

## 2.2 proof

### 2.2.1 Statement I

We use the MI (Mathematical Induction) method to prove the first statement.

*Proof.* Since the Hellinger distance is symmetric, if we prove the  $H(BI(x), BI(x+1)) < H(BI(x+1), BI(x+2)) \forall x \geq x_0$ , the other part when  $\forall x \leq x_0$  also holds.

1. if  $x = x_0$ ,  $H(BI(x_0), BI(x_0+1)) < H(BI(x_0+1), BI(x_0+2))$  holds:

$$\begin{aligned}
& H(beta(\frac{n}{2}+1, \frac{n}{2}+1), beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1)) < H(beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1), beta(\frac{n}{2}+1+2, \frac{n}{2}+1-2)) \\
& \sqrt{1 - \frac{beta(\frac{\frac{n}{2}+1+\frac{n}{2}+1+1}{2}, \frac{\frac{n}{2}+1+\frac{n}{2}+1-1}{2})}{\sqrt{beta(\frac{n}{2}+1, \frac{n}{2}+1)beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1)}}} < \sqrt{1 - \frac{beta(\frac{\frac{n}{2}+1+1+\frac{n}{2}+1+2}{2}, \frac{\frac{n}{2}+1-1+\frac{n}{2}+1-2}{2})}{\sqrt{beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1)beta(\frac{n}{2}+1+2, \frac{n}{2}+1-2)}}} \\
& \sqrt{1 - \frac{beta(\frac{n+3}{2}, \frac{n+1}{2})}{\sqrt{beta(\frac{n}{2}+1, \frac{n}{2}+1)beta(\frac{n}{2}+2, \frac{n}{2})}}} < \sqrt{1 - \frac{beta(\frac{n+5}{2}, \frac{n-1}{2})}{\sqrt{beta(\frac{n}{2}+2, \frac{n}{2})beta(\frac{n}{2}+3, \frac{n}{2}-1)}}} \\
& \frac{beta(\frac{n+3}{2}, \frac{n+1}{2})}{\sqrt{beta(\frac{n}{2}+1, \frac{n}{2}+1)beta(\frac{n}{2}+2, \frac{n}{2})}} > \frac{beta(\frac{n+5}{2}, \frac{n-1}{2})}{\sqrt{beta(\frac{n}{2}+2, \frac{n}{2})beta(\frac{n}{2}+3, \frac{n}{2}-1)}} \\
& \frac{beta(\frac{n+3}{2}, \frac{n-1}{2}) \frac{\frac{n-1}{2}}{\frac{n-1}{2} + \frac{n+3}{2}}}{\sqrt{beta(\frac{n}{2}+1, \frac{n}{2}-1) \frac{\frac{n-1}{2}}{\frac{n-1}{2} + \frac{n+3}{2}}}} > \frac{beta(\frac{n+3}{2}, \frac{n-1}{2}) \frac{\frac{n+3}{2}}{\frac{n+3}{2} + \frac{n-1}{2}}}{\sqrt{beta(\frac{n}{2}+1, \frac{n}{2}-1) \frac{\frac{n+3}{2}}{\frac{n+3}{2} + \frac{n-1}{2}}}} \\
& \frac{\frac{n-1}{2}}{\sqrt{(\frac{n}{2}-1)(\frac{n}{2})}} > \frac{\frac{n+3}{2}}{\sqrt{(\frac{n}{2}+1)(\frac{n}{2}+2)}} \\
& (n-1)^2(n+2)(n+4) > (n+3)^2n(n-2) \\
& n > -1.
\end{aligned}$$

Since  $n > 0$ , it always holds.

2. if  $x = x_0 + m$  holds, then also  $x = x_0 + m + 1$  holds:

i.e  $H(beta(\frac{n}{2}+1+m, \frac{n}{2}+1-m), beta(\frac{n}{2}+1+m+1, \frac{n}{2}+1-m-1)) < H(beta(\frac{n}{2}+1+m+1, \frac{n}{2}+1-m-1), beta(\frac{n}{2}+1+m+2, \frac{n}{2}+1-m-2))$  is what we know:

$$\begin{aligned}
& \sqrt{1 - \frac{beta(\frac{\frac{n}{2}+1+m+\frac{n}{2}+1+m+1}{2}, \frac{\frac{n}{2}+1-m+\frac{n}{2}+1-m-1}{2})}{\sqrt{beta(\frac{n}{2}+1+m, \frac{n}{2}+1-m)beta(\frac{n}{2}+2+m, \frac{n}{2}-m)}}} < \sqrt{1 - \frac{beta(\frac{\frac{n}{2}+1+m+1+\frac{n}{2}+1+m+2}{2}, \frac{\frac{n}{2}+1-m-1+\frac{n}{2}+1-m-2}{2})}{\sqrt{beta(\frac{n}{2}+2+m, \frac{n}{2}-m)beta(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}}} \\
& \frac{beta(\frac{n+2m+3}{2}, \frac{n-2m+1}{2})}{\sqrt{beta(\frac{n}{2}+1+m, \frac{n}{2}+1-m)beta(\frac{n}{2}+2+m, \frac{n}{2}-m)}} > \frac{beta(\frac{n+2m+5}{2}, \frac{n-2m-1}{2})}{\sqrt{beta(\frac{n}{2}+2+m, \frac{n}{2}-m)beta(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}}
\end{aligned}$$

Now, we need to proof  $H(beta(\frac{n}{2}+1+m+1, \frac{n}{2}+1-m-1), beta(\frac{n}{2}+1+m+2, \frac{n}{2}+1-m-2)) < H(beta(\frac{n}{2}+1+m+2, \frac{n}{2}+1-m-2), beta(\frac{n}{2}+1+m+3, \frac{n}{2}+1-m-3))$  by using what we know.

From  $x = x_0 + m$  and property of  $beta(\alpha, \beta)$  function, we know:

$$\frac{beta(\frac{n+2m+5}{2}, \frac{n-2m-1}{2}) \frac{n-2m-1}{n+2m+3}}{\sqrt{beta(\frac{n}{2}+2+m, \frac{n}{2}-m)beta(\frac{n}{2}+3+m, \frac{n}{2}-m-1) \frac{n-2m-1}{n+2m+3}}} > \frac{beta(\frac{n+2m+7}{2}, \frac{n-2m-3}{2}) \frac{n-2m-3}{n+2m+5}}{\sqrt{beta(\frac{n}{2}+2+m, \frac{n}{2}-m)beta(\frac{n}{2}+3+m, \frac{n}{2}-m-1) \frac{n-2m-3}{n+2m+5}}}$$

$$\frac{\text{beta}(\frac{n+2m+5}{2}, \frac{n-2m-1}{2})}{\sqrt{\text{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\text{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}} > \frac{\text{beta}(\frac{n+2m+7}{2}, \frac{n-2m-3}{2})}{\sqrt{\text{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\text{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}}$$

$$\sqrt{1 - \frac{\text{beta}(\frac{n+2m+5}{2}, \frac{n-2m-1}{2})}{\sqrt{\text{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\text{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}}} < \sqrt{1 - \frac{\text{beta}(\frac{n+2m+7}{2}, \frac{n-2m-3}{2})}{\sqrt{\text{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\text{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)}}}$$

$$H(\text{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m), \text{beta}(\frac{n}{2}+3+m, \frac{n}{2}-1-m)) < H(\text{beta}(\frac{n}{2}+m+3, \frac{n}{2}-1-m), \text{beta}(\frac{n}{2}+m+4, \frac{n}{2}-m-2))$$

i.e.  $x = x_0 + m + 1$  also holds when  $x = x_0 + m$  is valid.  $\square$

### 2.2.2 Statement II

*Proof.*

$$\begin{aligned} \therefore^1 \quad \Delta_l u(x) &= \max_{\{|x, y'| \leq 1; y' \in \mathcal{X}^n\}} \max_{\{r \in R\}} |H(\text{BI}(x), r) - H(\text{BI}(y'), r)|, \\ \therefore \quad H(\text{BI}(x), r) - H(\text{BI}(y'), r) &\leq H(\text{BI}(x), \text{BI}(y')); \\ \therefore^2 \quad \Delta_l u(x) &= \max_{\{|x, y'| \leq 1; y' \in \mathcal{X}^n\}} H(\text{BI}(x), \text{BI}(y')), \\ \therefore \quad \Delta_l u(x) &= \max\{H(\text{BI}(x), \text{BI}(x+1)), H(\text{BI}(x), \text{BI}(x-1))\}; \\ &\text{According to Statement I :} \\ \text{if } x > x_0 & \\ \text{then } H(\text{BI}(x), \text{BI}(x-1)) &< H(\text{BI}(x), \text{BI}(x+1)); \\ \text{then } \Delta_l u(x) &= H(\text{BI}(x), \text{BI}(x+1)); \\ \text{if } x < x_0 & \\ \text{then } H(\text{BI}(x), \text{BI}(x-1)) &> H(\text{BI}(x), \text{BI}(x+1)); \\ \text{then } \Delta_l u(x) &= H(\text{BI}(x), \text{BI}(x-1)); \\ \text{else } \Delta_l u(x_0) &= H(\text{BI}(x_0), \text{BI}(x_0-1)) = H(\text{BI}(x_0), \text{BI}(x_0+1)). \end{aligned}$$

From above, we can conclude the Statement II.  $\square$

### 2.2.3 Statement III

*Proof.* From Statement I and Statement II, we can conclude that:

$$\begin{aligned} \text{when } x > x_0 & \\ H(\text{BI}(x), \text{BI}(x+1)) &> H(\text{BI}(x_0), \text{BI}(x_0+1)); \\ \text{i.e. } \Delta_l u(x) &> \Delta_l u(x_0) \\ \text{when } x < x_0 & \\ H(\text{BI}(x), \text{BI}(x-1)) &> H(\text{BI}(x_0), \text{BI}(x_0-1)); \\ \text{i.e. } \Delta_l u(x) &> \Delta_l u(x_0). \end{aligned}$$

i.e.  $\forall x \neq x_0, \Delta_l u(x) > \Delta_l u(x_0)$ .  $\square$

### 3 Smooth sensitivity

#### 3.1 Dilation Property of Laplace Noise

**Lemma 3.1.** *For 1-dimensional Laplace distribution:  $h(z) = \frac{1}{2}e^{-|z|}$ ,  $\alpha = \frac{\epsilon}{2}$ ,  $\beta = \frac{\epsilon}{2\rho_{\delta/3}(|z|)}$  or  $\frac{\epsilon}{2\ln(2/\delta)}$  and  $|\lambda| \leq \beta$ , the dilation property holds for any  $z$  sampled from  $h$ :*

$$Pr[z \in S] \leq e^{\frac{\epsilon}{2}} Pr[z \in e^\lambda S] + \frac{\delta}{2}$$

*Proof.* From the integral substitution property, we have:

$$\begin{aligned} \frac{Pr[z \in e^\lambda S]}{Pr[z \in S]} &= \frac{\int_{e^\lambda S} \frac{1}{2} e^{-|z|} dz}{\int_S \frac{1}{2} e^{-|z|} dz} \\ &= \frac{\int_S \frac{1}{2} e^{-|e^\lambda z|} e^\lambda dz}{\int_S \frac{1}{2} e^{-|z|} dz} \\ &= \frac{e^{-|e^\lambda z|} e^\lambda}{e^{-|z|}} \\ &= \frac{e^\lambda h(e^\lambda z)}{h(z)} \end{aligned}$$

Then, we proof the dilation property in cases of  $\lambda > 0$  and  $\lambda < 0$  separately:

**case 1:**  $\lambda > 0$

$$\begin{aligned} \because h(e^\lambda z) &= \frac{1}{2} e^{-|e^\lambda z|} < \frac{1}{2} e^{-|z|} = h(z) \\ \therefore \frac{Pr[z \in e^\lambda S]}{Pr[z \in S]} &= \frac{e^\lambda h(e^\lambda z)}{h(z)} \leq e^\lambda \\ \therefore \ln\left(\frac{e^\lambda h(e^\lambda z)}{h(z)}\right) &\leq \lambda \\ \therefore \lambda &\leq \beta = \frac{\epsilon}{2\ln(3/\delta)}, \delta < 1 \\ \therefore \lambda &\leq \frac{\epsilon}{2} \\ \therefore \frac{Pr[z \in e^\lambda S]}{Pr[z \in S]} &\leq \frac{\epsilon}{2} \end{aligned}$$

• **case 2:**  $\lambda < 0$

From integral property, we firstly have:

$$\frac{Pr[z \in e^\lambda S]}{Pr[z \in S]} = \frac{e^{-|e^\lambda z|} e^\lambda}{e^{-|z|}} = \frac{h(e^\lambda z) e^\lambda}{h(z)} = e^\lambda e^{|z|(1-e^\lambda)}$$

$$\begin{aligned} \because 1 - e^\lambda &\leq |\lambda| \\ \therefore \ln\left(\frac{h(e^\lambda z) e^\lambda}{h(z)}\right) &\leq \lambda + |z||\lambda| \\ \because \lambda &< 0 \\ \therefore \ln\left(\frac{h(e^\lambda z) e^\lambda}{h(z)}\right) &\leq |z||\lambda| \end{aligned}$$

By setting  $h'(z) = e^\lambda h(e^\lambda z)$ , we can get:

$$\begin{aligned} \ln\left(\frac{h'(z)}{h(z)}\right) &\leq |z||\lambda| \\ \Rightarrow h'(z) &\leq e^{|z||\lambda|} h(z) \end{aligned}$$

By exchanging the notation of  $h'$  and  $h$ , we have:

$$h(z) \leq e^{|z||\lambda|} h'(z)$$

i.e.

$$Pr_{z \sim h}[z \in S] \leq e^{|z||\lambda|} Pr_{z \sim h'}[z \in S] = e^{|z||\lambda|} Pr_{z \sim h}[z \in e^\lambda S]$$

We consider an event  $G = \{z \mid |z| \leq \log(\frac{2}{\delta})\}$ . Under this event, we have:

$$\begin{aligned} |z||\lambda| &\leq \log\left(\frac{2}{\delta}\right)|\lambda| \\ &\leq \log\left(\frac{2}{\delta}\right)\beta \\ &\leq \log\left(\frac{2}{\delta}\right) \frac{\epsilon}{2\log(\frac{3}{\delta})} \\ &\leq \frac{\epsilon}{2}. \end{aligned}$$

Then:

$$\begin{aligned} Pr_{z \sim h}[z \in S \cap G] &\leq e^{|z||\lambda|} Pr_{z \sim h'}[z \in S \cap G] \\ &\leq e^{\frac{\epsilon}{2}} Pr_{z \sim h'}[z \in S \cap G] \end{aligned}$$

We also have:

$$Pr[\overline{G}] = Pr[|z| > \log(\frac{2}{\delta})] = \exp(-\log(\frac{2}{\delta})) = \frac{\delta}{2}$$

Then, we can get

$$\begin{aligned} Pr_{z \sim h}[z \in S] &\leq Pr_{z \sim h}[z \in S \cap G] + Pr_{z \sim h}[z \in \overline{G}] \\ &\leq e^{\frac{\epsilon}{2}} Pr_{z \sim h'}[z \in S \cap G] + \frac{\delta}{2} \\ &\leq e^{\frac{\epsilon}{2}} Pr_{z \sim h'}[z \in S] + \frac{\delta}{2} \\ &= e^{\frac{\epsilon}{2}} Pr_{z \sim h}[z \in e^\lambda S] + \frac{\delta}{2} \end{aligned}$$

i.e. the dilation property.

□

### 3.2 Sliding Property of Exponential Mechanism

**Lemma 3.2.** *for any exponential mechanism  $\mathcal{M}_E(x, u, \mathcal{R})$ ,  $\lambda = f(\epsilon, \delta)$ ,  $\epsilon$  and  $|\delta| < 1$ , the sliding property holds:*

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

where the sensitivity in mechanism is smooth sensitivity  $S(x)$ , calculated by:

$$S_\beta(x) = \max(\Delta_I u(x), \max_{y \neq x; y \in D^n} (\Delta_I u(y) \cdot e^{-\beta d(x, y)})),$$

where  $\beta = \beta(\epsilon, \delta)$ .

*Proof.* We denote the normalizer of the probability mass in  $\mathcal{M}_E(x, u, \mathcal{R})$ :  $\sum_{r' \in \mathcal{R}} \exp(\frac{\epsilon u(r', x)}{2S(x)})$  as  $NL_x$ :

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

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

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

□

### 3.3 Dilation Property of Exponential Mechanism

**Lemma 3.3.** *for any exponential mechanism  $\mathcal{M}_E(x, u, \mathcal{R})$ ,  $\lambda = f(\epsilon, \delta)$ ,  $\epsilon$  and  $|\delta| < 1$ , the dilation property holds:*

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

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

*Proof.* The sensitivity is always greater than 0, and we are using  $-H(\text{Bl}(x), r)$  for utility function, i.e.,  $u(r) \leq 0$ , we need to consider two cases that  $\lambda < 0$ , and  $\lambda > 0$ :

We set the  $h(z) = \Pr[u(\mathcal{M}_E(x, u, \mathcal{R})) = z] = \frac{\exp(\frac{\epsilon z}{2S(x)})}{NL_x}$ .

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

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



- $\lambda < 0$

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

- $\lambda > 0$

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

$$u(\mathcal{M}_E(x, u, \mathcal{R})) \leq \frac{S(x)}{(1 - e^\lambda)}$$

By applying the accuracy property of exponential mechanism, we bound the probability that the equation holds with probability:

$$Pr[u(\mathcal{M}_E(x, u, \mathcal{R})) \leq \frac{S(x)}{(1 - e^\lambda)}] \leq \frac{|\mathcal{R}| \exp(\frac{\epsilon S(x)}{(1 - e^\lambda)} / 2S(x))}{|\mathcal{R}_{OPT}| \exp(\epsilon OPT_{u(x)} / 2S(x))}$$

In our Bayesian Inference mechanism, the size of the candidate set  $\mathcal{R}$  is equal to the size of observed data set plus 1, i.e.,  $n + 1$ , and  $OPT_{u(x)} = 0$ , then we have:

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

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

□

## 4 Experimental Evaluations

We got some results from these mechanisms.