Notes of DP - Bayesian Inference

1 Setting up

The Bayesian inference process is denoted as $\mathsf{BI}(x, prior)$ 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 $\mathsf{BI}(x)$.

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.

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

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

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

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

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

where global sensitivity is calculated by:

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

1.1.2 Security Analysis

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

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

Then, $\frac{P[\mathsf{PrivInfer}(x,u,R)=r]}{P[\mathsf{PrivInfer}(y,u,R)=r]} \geqslant exp(-\epsilon)$ 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 $exp(\frac{\epsilon u(x,r)}{2\Delta_l u})$:

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

where local sensitivity is calculated by:

$$\Delta_l u(x) = \max_{\{|x,y'|\leqslant 1; y'\in\mathcal{X}^n\}} \max_{\{r\in R\}} .\mathsf{H}(\mathsf{BI}(x),r) - \mathsf{H}(\mathsf{BI}(y'),r)|$$

1.2.2 Security Analysis

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

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

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

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

From Eq. 1, $\{u(x,r') \leqslant 0 | r' \in R\}$ and $\{u(y,r') \leqslant 0 | r' \in R\}$, we can infer that $r = arg(\max\limits_{r\in R}\{u(x,r')\}) = \mathsf{BI}(x)$ 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:

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

i.e.

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

Since there are cases where exponential mechanism with local sensitivity's privacy loss is greater than e^{ϵ}. 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 $beta(1,1)$, an observed data set $x \in \{0,1\}^n$, $n > 0$. We use the $x+1$ and $x-1$ to denote:

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

x_0 to denote:

$$\begin{aligned}
&\text{if } n \textit{ is even}\\
&\text{then } \mathsf{BI}(x_0) = beta(\frac{n}{2}+1, \frac{n}{2}+1)\\
&\text{else } \mathsf{BI}(x_0) = \{beta(\frac{n+1}{2}+1, \frac{n-1}{2}+1),\\
&\qquad\qquad beta(\frac{n-1}{2}+1, \frac{n+1}{2}+1)\}
\end{aligned}$$

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

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

I $\mathsf{H}(\mathsf{BI}(x), \mathsf{BI}(x+1)) < \mathsf{H}(\mathsf{BI}(x+1), \mathsf{BI}(x+2))\ \forall x \geqslant x_0$;
or $\mathsf{H}(\mathsf{BI}(x), \mathsf{BI}(x+1)) > \mathsf{H}(\mathsf{BI}(x+1), \mathsf{BI}(x+2)) \forall x \leqslant x_0$.

II $\Delta_l u(x) = \mathsf{H}(\mathsf{BI}(x), \mathsf{BI}(x+1)), \forall x \geqslant x_0$;
$\Delta_l u(x) = \mathsf{H}(\mathsf{BI}(x), \mathsf{BI}(x-1)), \forall x \leqslant x_0$.

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 $\mathsf{H}(\mathsf{BI}(x), \mathsf{BI}(x+1)) < \mathsf{H}(\mathsf{BI}(x+1), \mathsf{BI}(x+2))$ $\forall x \geqslant x_0$, the other part when $\forall x \leqslant x_0$ also holds.

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

$$\mathsf{H}(beta(\frac{n}{2}+1, \frac{n}{2}+1), beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1)) < \mathsf{H}(beta(\frac{n}{2}+1+1, \frac{n}{2}+1-1), beta(\frac{n}{2}+1+2, \frac{n}{2}+1-2))$$

$$\sqrt{1 - \frac{\mathsf{beta}(\frac{\frac{n}{2}+1+\frac{n}{2}+1+1}{2}, \frac{\frac{n}{2}+1+\frac{n}{2}+1-1}{2})}{\sqrt{\mathsf{beta}(\frac{n}{2}+1, \frac{n}{2}+1)\mathsf{beta}(\frac{n}{2}+1+1, \frac{n}{2}+1-1)}}} < \sqrt{1 - \frac{\mathsf{beta}(\frac{\frac{n}{2}+1+1+\frac{n}{2}+1+2}{2}, \frac{\frac{n}{2}+1-1+\frac{n}{2}+1-2}{2},)}{\sqrt{\mathsf{beta}(\frac{n}{2}+1+1, \frac{n}{2}+1-1)\mathsf{beta}(\frac{n}{2}+1+2, \frac{n}{2}+1-2)}}}$$

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

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

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

$$\frac{\frac{n-1}{2}}{\sqrt{(\frac{n}{2}-1)(\frac{n}{2})}} > \frac{\frac{n+3}{2}}{\sqrt{(\frac{n}{2}+1)(\frac{n}{2}+2)}}$$

$$(n-1)^2(n+2)(n+4) > (n+3)^2 n(n-2)$$

$$n > -1.$$

Since $n > 0$, it always holds.

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

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

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

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

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

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

$$\frac{\mathsf{beta}(\frac{n+2m+5}{2}, \frac{n-2m-1}{2})\frac{n-2m-1}{n+2m+3}}{\sqrt{\mathsf{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\mathsf{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)\frac{n-2m}{n+2m+2}}} > \frac{\mathsf{beta}(\frac{n+2m+7}{2}, \frac{n-2m-3}{2})\frac{n-2m-3}{n+2m+5}}{\sqrt{\mathsf{beta}(\frac{n}{2}+2+m, \frac{n}{2}-m)\mathsf{beta}(\frac{n}{2}+3+m, \frac{n}{2}-m-1)\frac{n-2m-2}{n+2m+6}}}$$

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

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

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

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

2.2.2 Statement II

Proof.

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

From above, we can conclude the Statement II.

□

2.2.3 Statement III

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

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

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

□

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* $\frac{\epsilon}{2ln(2/\delta)}$ *and* $|\lambda| \leqslant \beta$, *the dilation property holds for any* z *sampled from* h*:*

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

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: $\lambda > 0$

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

- **case 2:** $\lambda < 0$

  From integral property, we firstly have:

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

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

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

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

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

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

i.e.

$$\underset{z \sim h}{Pr}[z \in S] \leqslant e^{|z||\lambda|} \underset{z \sim h'}{Pr}[z \in S] = e^{|z||\lambda|} \underset{z \sim h}{Pr}[z \in e^{\lambda} S]$$

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

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

Then:

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

We also have:

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

Then, we can get

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

i.e. the dilation property.

□

3.2 Sliding Property of Exponential Mechanism

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

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

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

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

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:

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

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

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

□

3.3 Dilation Property of Exponential Mechanism

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

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

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

Proof.

$$\begin{aligned} \frac{exp(\frac{\epsilon\hat{s}}{2S(x)})}{NL_x} &\leqslant \frac{exp(\frac{\epsilon(\hat{s}\cdot e^\lambda)}{2S(x)})}{NL_x} \\ exp(\frac{\epsilon\hat{s}}{2S(x)}) &\leqslant exp(\frac{\epsilon(\hat{s}\cdot e^\lambda)}{2S(x)}) \\ \frac{\epsilon\hat{s}}{2S(x)} &\leqslant \frac{\epsilon}{2} + \frac{\epsilon\hat{s}\cdot e^\lambda}{2S(x)} \\ \hat{s} &\leqslant S(x) + \hat{s}\cdot e^\lambda \\ (1-e^\lambda)\cdot\hat{s} &\leqslant S(x) \end{aligned}$$

To proof this, we discuss some cases:

Since the sensitivity is always greater than 0, but the utility function and λ can be positive or negative. That's what we need to discuss.

- $\lambda > 0$
  - $u(r) > 0$
    The left hand side will always be smaller than 0 and the right hand side greater than 0. This will always holds.
  - $u(r) < 0$
- $\lambda < 0$
  - $u(r) > 0$
  - $u(r) \leqslant 0$
    The left hand side will always be smaller than 0 and the right hand side greater than 0. This will always holds.

In our case, we are using $-\mathsf{H}(\mathsf{BI}(x), r)$ for utility function, we only need to consider the case $u(r) \leqslant 0$.

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 event $G = \{\lambda > 0, u(r) \leqslant 0\}$ is:

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

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

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

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:

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

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

□

4 Experimental Evaluations

We got some results from these mechanisms.