Differentially Private Bayesian Inference

Anonymous Authors[1]

Abstract

1. Setting up

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

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.

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

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

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

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:

$$\Delta_g u = \mathsf{Hlg}(\mathsf{BayesInfer}(x'), r) - \mathsf{Hlg}(\mathsf{BayesInfer}(y'), r)| \max_{\{|x',y'| \le 1; x',y' \in \mathcal{X}^n\}} \max_{\{r \in R\}}.$$

[1]Anonymous Institution, Anonymous City, Anonymous Region, Anonymous Country. Correspondence to: Anonymous Author <anon.email@domain.com>.

Preliminary work. Under review by the International Conference on Machine Learning (ICML). Do not distribute.

1.1.2. Security Analysis

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

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

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

$$\Delta_g u(x) = \mathsf{Hlg}(\mathsf{BayesInfer}(x), r) - \mathsf{Hlg}(\mathsf{BayesInfer}(y'), r)| \max_{\{|x,y'|\le 1; y' \in \mathcal{X}^n\}} \max_{\{r \in R\}}.$$

1.2.2. Security Analysis

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

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

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:

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

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

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

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:

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

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

I $\mathsf{Hlg}(\mathsf{BayesInfer}(x), \mathsf{BayesInfer}(x+1)) < \mathsf{Hlg}(\mathsf{BayesInfer}(x+1), \mathsf{BayesInfer}(x+2)) \; \forall x \ge x_0$;

or $\mathsf{Hlg}(\mathsf{BayesInfer}(x), \mathsf{BayesInfer}(x+1)) > \mathsf{Hlg}(\mathsf{BayesInfer}(x+1), \mathsf{BayesInfer}(x+2)) \forall x \le x_0$.

II $\Delta_l u(x) = \mathsf{Hlg}(\mathsf{BayesInfer}(x), \mathsf{BayesInfer}(x+1)), \forall x \geq x_0$;

$\Delta_l u(x) = \mathsf{Hlg}(\mathsf{BayesInfer}(x), \mathsf{BayesInfer}(x-1)), \forall x \leq x_0$.

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 $\mathsf{Hlg}(\mathsf{BayesInfer}(x), \mathsf{BayesInfer}(x+1)) < \mathsf{Hlg}(\mathsf{BayesInfer}(x+1), \mathsf{BayesInfer}(x+2))$ $\forall x \geq x_0$, the other part when $\forall x \leq x_0$ also holds.

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

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

Since $n > 0$, it always holds.

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

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

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

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

$$
\frac{\mathsf{beta}(,)}{\sqrt{\mathsf{beta}(,)\mathsf{beta}(,)}}
$$

$$
> \frac{\mathsf{beta}(,)}{\sqrt{\mathsf{beta}(,)\mathsf{beta}(,)}}
$$

Now, we want to proof $\mathsf{Hlg}(beta(\frac{n}{2}+1+m+1, \frac{n}{2}+1-m-1), beta(\frac{n}{2}+1+m+2, \frac{n}{2}+1-m-2)) < \mathsf{Hlg}(beta(\frac{n}{2}+1+m+2, \frac{n}{2}+1-m-2), beta(\frac{n}{2}+1+m+3, \frac{n}{2}+1-m-3))$ by using what we know: □

2.2.2. Statement II

2.2.3. Statement III

3. Experimental Evaluations

We got some results from these mechanisms.

References