CS591S1 Homework 2: More on Differential Privacy

Jiawen Liu
Collaborators: none.

1 Problem 1

1. (Sensitivity)

   Given data set $\mathbf{x}$, for arbitrary $y \in \{1, \cdots, R\}$ and adjacent dataset $\mathbf{x}'$ by insertion or deletion of one data point x_k, we have following cases for insertion (deletion will be symmetric):

   - $y = x_k$:

   $$q(y;\mathbf{x}') = -|\sum_{i=0}^{n} sign(y-x_i)+sign(y-x_k)| = -|\sum_{i=0}^{n} sign(y-x_i)+0| = -|\sum_{i=0}^{n} sign(y-x_i)| = q(y;\mathbf{x})$$

   - $y < x_k$

   $$\begin{aligned} q(y;\mathbf{x}') &= -|\textstyle\sum_{i=0}^{n} sign(y-x_i) + sign(y-x_k)| \\ &= -|\textstyle\sum_{i=0}^{n} sign(y-x_i) - 1| \ (\star) \end{aligned}$$

   By triangle inequality, we have:

   $$\begin{aligned} (\star) &\leq -|\textstyle\sum_{i=0}^{n} sign(y-x_i)| + 1 = q(y;\mathbf{x}) + 1 \\ (\star) &\geq -|\textstyle\sum_{i=0}^{n} sign(y-x_i)| - 1 = q(y;\mathbf{x}) - 1 \end{aligned}$$

   Then we can get:

   $$-1 \leq q(y;\mathbf{x}') - q(y;\mathbf{x}) \leq 1$$

   - $y > x_k$

   $$\begin{aligned} q(y;\mathbf{x}') &= -|\textstyle\sum_{i=0}^{n} sign(y-x_i) + sign(y-x_k)| \\ &= -|\textstyle\sum_{i=0}^{n} sign(y-x_i) + 1| \ (\star) \end{aligned}$$

   By triangle inequality, we have:

   $$\begin{aligned} (\star) &\leq -|\textstyle\sum_{i=0}^{n} sign(y-x_i)| + 1 = q(y;\mathbf{x}) + 1 \\ (\star) &\geq -|\textstyle\sum_{i=0}^{n} sign(y-x_i)| - 1 = q(y;\mathbf{x}) - 1 \end{aligned}$$

   Then we can get:

   $$-1 \leq q(y;\mathbf{x}') - q(y;\mathbf{x}) \leq 1$$

   The Deletion is symmetric where we can get: $-1 \leq q(y;\mathbf{x}) - q(y;\mathbf{x}') \leq 1$ in the same way. Then, we can conclude from all cases, the $|q(y;\mathbf{x}) - q(y;\mathbf{x}')| \leq 1$, i.e., the sensitivity be at most 1.

2. *Proof.* By the definition of $rank_{\mathbf{x}}(y)$, we have:

$$|rank_{\mathbf{x}}(y) - \frac{n}{2}| = -q(y;\mathbf{x}).$$

Then, we know:

$$\begin{aligned} Pr_{y\sim A_\epsilon(\mathbf{x})}[|rank_{\mathbf{x}}(y) - \tfrac{n}{2}| > c \cdot \tfrac{\ln(R)+\ln(1/\beta)}{\epsilon}] &\equiv Pr_{y\sim A_\epsilon(\mathbf{x})}[-q(y;\mathbf{x}) > c \cdot \tfrac{\ln(R)+\ln(1/\beta)}{\epsilon}] \\ &= Pr_{y\sim A_\epsilon(\mathbf{x})}[q(y;\mathbf{x}) \le -c \cdot \tfrac{\ln(R)+\ln(1/\beta)}{\epsilon}] \end{aligned}$$

By definition of exponential mechanism, we have:

$$\begin{aligned} Pr_{y\sim A_\epsilon(\mathbf{x})}[q(y;\mathbf{x}) \le -c \cdot \tfrac{\ln(R)+\ln(1/\beta)}{\epsilon}] &= \sum_{y|q(y;\mathbf{x})<-c\cdot\frac{\ln(R)+\ln(1/\beta)}{\epsilon}} \frac{\exp\left(q(y;\mathbf{x})\epsilon/2S\right)}{\sum_y \exp\left(q(y;\mathbf{x})\epsilon/2S\right)} \\ &\le R\frac{\exp\left(-c\cdot\frac{\ln(R)+\ln(1/\beta)}{\epsilon}\frac{\epsilon}{2S}\right)}{\sum_y \exp\left(q(y;\mathbf{x})\epsilon/2S\right)} \\ &= R\frac{\exp\left(\frac{c}{2}(\ln(\frac{1}{R})+\ln(\beta))\right)}{\sum_y \exp\left(q(y;\mathbf{x})\epsilon/2S\right)} \quad (\star) \end{aligned}$$

Since the only one optimal output candidate is the median value where $q(y,\mathbf{x}) = 0$, so we have:

$$(\star) \quad \le \quad \frac{\exp\left(\frac{c}{2}(\ln(\frac{1}{R})+\ln(\beta))\right)}{\exp(0)}$$

In order to have this probability be at most β, we take the equality and get:

$$\begin{aligned} \frac{\exp\left(\frac{c}{2}(\ln(\frac{1}{R})+\ln(\beta))\right)}{\exp(0)} &= \beta \\ R^{1-\frac{c}{2}} &= \beta^{1-\frac{c}{2}} \end{aligned}$$

Since we have $R \ge 1$ and $\beta \in (0,1)$, there exists $c = 2$ which can make the equation holds. □

2 Problem 2

Proof. The proof are developed by two symmetric cases: insertion and deletion.

case Insertion

Taking two adjacent data sets $\mathbf{x}$, $\mathbf{x}'$ where $\mathbf{x}'$ contains one more data point. For any output set S, there are following cases by output space:

- $S \subseteq E_{bad}$ Inserting one data that makes an empty bin ($k \in \mathcal{X}$) be nonempty and this bin is contained in the output set S.

$$\begin{aligned} Pr[A(\mathbf{x}') = S] &= Pr[\tilde{c'_k} > \tau] \le \tfrac{\delta}{2} \\ Pr[A(\mathbf{x}) = S] &= 0 \end{aligned}$$

- $S \subseteq E_0$ Inserting one data that makes an empty bin ($k \in \mathcal{X}$) be nonempty and this bin is not contained in the output set.The probability ratio

$$\begin{aligned} 1 > \frac{Pr[A(\mathbf{x}')\in S]}{Pr[A(\mathbf{x})\in S]} &= \frac{Pr[A(\mathbf{x})\in S \wedge \tilde{c'_k} < \tau]}{Pr[A(\mathbf{x})\in S]} \\ &= \frac{Pr[A(\mathbf{x})\in S]\cdot Pr[\tilde{c'_k} < \tau]}{Pr[A(\mathbf{x})\in S]} \\ &= Pr[\tilde{c'_k} = 1 + Lap(\tfrac{1}{\epsilon}) < \tau] \\ &\ge (1 - \tfrac{\delta}{2}) \end{aligned}$$

- $S \subseteq E_1$ Inserting one data that doesn't change non-empty bins:

$$
\begin{aligned}
e^{-\epsilon} \leq \frac{Pr[A(\mathbf{x}') \in S]}{Pr[A(\mathbf{x}) \in S]} &= \frac{Pr[A(\mathbf{x}\backslash k) \in S\backslash k \wedge \tilde{c'_k} \in S \cap k]}{Pr[A(\mathbf{x}'\backslash k) \in S\backslash k \wedge \tilde{c_k} \in S \cap k]} \\
&= \frac{Pr[A(\mathbf{x}\backslash k) = S\backslash k] \cdot Pr[\tilde{c'_k} \in S \cap k]}{Pr[A(\mathbf{x}\backslash k) = S\backslash k] \cdot Pr[\tilde{c'_k} \in S \cap k]} \\
&= \frac{Pr[\tilde{c'_k} \in S \cap k]}{Pr[\tilde{c_k} \in S \cap k]} \\
&\leq e^{\epsilon}
\end{aligned}
$$

By summarization, we have following equations:

$$
\begin{aligned}
Pr[A(\mathbf{x}') \in S] &= Pr[A(\mathbf{x}') \in S \cap E_0] + Pr[A(\mathbf{x}') \in S \cap E_1] + Pr[A(\mathbf{x}') \in S \cap E_{Bad}] \\
&\leq e^{\epsilon} Pr[A(\mathbf{x}) \in S \cap E_0] + Pr[A(\mathbf{x}) \in S \cap E_1] + \frac{\delta}{2} \\
&\leq e^{\epsilon} Pr[A(\mathbf{x}) \in S \cap E_0] + e^{\epsilon} Pr[A(\mathbf{x}) \in S \cap E_1] + \frac{\delta}{2} \\
&= e^{\epsilon} Pr[A(\mathbf{x}) \in S \cap (E_0 \cup E_1)] + \frac{\delta}{2} \\
&\leq e^{\epsilon} Pr[A(\mathbf{x}) \in S] + \frac{\delta}{2}
\end{aligned}
$$

On the other side, we have:

$$
\begin{aligned}
Pr[A(\mathbf{x}') \in S] &= Pr[A(\mathbf{x}') \in S \cap E_0] + Pr[A(\mathbf{x}') \in S \cap E_1] + Pr[A(\mathbf{x}') \in S \cap E_{Bad}] \\
&\geq e^{-\epsilon} Pr[A(\mathbf{x}) \in S \cap E_0] + (1 - \frac{\delta}{2}) Pr[A(\mathbf{x}) \in S \cap E_1] \\
&\geq \min(e^{-\epsilon}, 1 - \frac{\delta}{2}) Pr[A(\mathbf{x}) \in S \cap E_0] + \min(e^{-\epsilon}, 1 - \frac{\delta}{2}) Pr[A(\mathbf{x}) \in S \cap E_1] \\
&= \min(e^{-\epsilon}, 1 - \frac{\delta}{2}) Pr[A(\mathbf{x}) \in S \cap (E_0 \cup E_1)] \\
&= \min(e^{-\epsilon}, 1 - \frac{\delta}{2}) Pr[A(\mathbf{x}) \in S]
\end{aligned}
$$

case deletion.

By deletion, we have exactly the symmetric cases as insertion.

By summarization, the probability of failure would be δ in both cases. So we have the algorithm be $(\max(\epsilon, \ln(\frac{1}{1-\frac{\delta}{2}})), \delta)$-DP. When δ is small, we have $\ln(\frac{1}{1-\frac{\delta}{2}}) \sim 0$ and $\epsilon > 0$, then $(\max(\epsilon, \ln(\frac{1}{1-\frac{\delta}{2}})), \delta)$-DP is (ϵ, δ)-DP. $\square$