中国科学技术大学计算机学院
《数据隐私的方法伦理和实践》作业

2021.06.06

学生姓名：胡毅翔

学生学号：PB18000290

计算机实验教学中心制

2019 年 9 月

1 Concept of DP

1.1

Prove that the Laplace mechanism preserves (ϵ, 0)-DP.

Proof. Let $x \in \mathbb{N}^{|\mathcal{X}|}$ and $y \in \mathbb{N}^{|\mathcal{X}|}$ be such that $\|x-y\|_1 \leq 1$, and let $f(\cdot)$ be some function $f : \mathbb{N}^{|\mathcal{X}|} \to \mathbb{R}^k$. Let p_x denote the probability density function of $\mathcal{M}_L(x, f, \varepsilon)$, and let p_y denote the probability density function of $\mathcal{M}_L(y, f, \varepsilon)$. We compare the two at some arbitrary point $z \in \mathbb{R}^k$

$$
\begin{aligned}
\frac{p_x(z)}{p_y(z)} &= \prod_{i=1}^{k} \left(\frac{\exp\left(-\frac{\varepsilon|f(x)_i - z_i|}{\Delta f}\right)}{\exp\left(-\frac{\varepsilon|f(y)_i - z_i|}{\Delta f}\right)} \right) \\
&= \prod_{i=1}^{k} \exp\left(\frac{\varepsilon\left(|f(y)_i - z_i| - |f(x)_i - z_i|\right)}{\Delta f} \right) \\
&\leq \prod_{i=1}^{k} \exp\left(\frac{\varepsilon\,|f(x)_i - f(y)_i|}{\Delta f} \right) \\
&= \exp\left(\frac{\varepsilon \cdot \|f(x) - f(y)\|_1}{\Delta f} \right) \\
&\leq \exp(\varepsilon)
\end{aligned}
$$

where the first inequality follows from the triangle inequality, and the last follows from the definition of sensitivity and the fact that $\|x-y\|_1 \leq 1$. That $\frac{p_x(z)}{p_y(z)} \geq \exp(-\varepsilon)$ follows by symmetry. □

1.2

Please explain the difference between $(\epsilon, 0) -$ DP and (ϵ, δ) -DP. Typically, what range of δ we're interested in? Explain the reason.

Solution. Even δ is negligible, there are theoretical distinctions between $(\varepsilon, 0)$ - and (ε, δ) - differential privacy.

$(\varepsilon, 0)$ -differential privacy: for every run of the mechanism $M(x)$, the output observed is (almost) equally likely to be observed on every neighboring database, simultaneously.

(ε, δ) - differential privacy: given an output $\xi \sim M(x)$ it may be possible to find a database y such that ξ is much more likely to be produced on y than it is when the database is x. The privacy loss (divergence) incurred by observation ξ :

$$
\mathcal{L}^{(\xi)}_{\mathcal{M}(x)\|\mathcal{M}(y)} = \ln\left(\frac{\Pr[\mathcal{M}(x) = \xi]}{\Pr[\mathcal{M}(y) = \xi]} \right)
$$

(ε, δ) - differential privacy ensures that for all adjacent x, y, the absolute value of the privacy loss will be bounded by ε with probability at least $1 - \delta$.

Typically, we are interested in values of δ that are less than the inverse of any polynomial in the size of the database.

Because, for each piece of data in data set, there is a probability that it will be released. Each piece of different data in this ralease is independent, so this mechanism can release $n\delta$ sample. So in order to prevent such leakage, it must be less than $1/n$.

□

1.3

Please explain the difference between DP and Local DP.

Solution. Definition of ϵ -local differential privacy is that a randomized function f satisfies ϵ local differential privacy if and only if for any two input tuples t and t' in the domain of f, and for any output t^* of f, we have:

$$\Pr\left[f(t)=t^*\right] \leq \exp(\epsilon) \cdot \Pr\left[f\left(t'\right)=t^*\right]$$

1. The notation $\Pr[\cdot]$ means probability. If f 's output is continuous, $\Pr[\cdot]$ is replaced by the probability density function.
2. Basically, local differential privacy is a special case of differential privacy where the random perturbation is performed by the users, not by the aggregator.
3. According to the above definition, the aggregator, who receives the perturbed tuple t, cannot distinguish whether the true tuple is t or another tuple t' with high confidence (controlled by parameter ϵ), regardless of the background information of the aggregator.
4. This provides plausible deniability to the user.

While the definition of differential privacy is that A randomized algorithm M with domain $\mathbb{N}^{|X|}$ is (ϵ, δ) -differentially private if for all $S \subset$ Range (M) and for all $x, y \in \mathbb{N}|X|$ such that $\|x-y\|_1 \leq 1$:

$$\Pr[M(x) \in S] \leq \exp(\epsilon) \Pr[M(y) \in S]+\delta$$

where the probability space is over the coin flips of the mechanism M. If $\delta=0$, we say that M is δ -differentially private.

We can find out the difference between LDP and DP is that DP restrictions on tuple $x, y \in \mathbb{N}|X|$ such that $\|x-y\|_1 \leq 1$, while LDP restrictions on any two input tuples t and t'.

□

2 Basics of DP

ID	Sex	Chinese	Mathematics	English	Physics	Chemistry	Biology
1	Male	96	58	80	53	56	100
2	Male	60	63	77	50	59	75
3	Female	83	86	98	69	80	100
...							
2000	Female	86	83	98	87	82	92

Table 1: Scores of students in School A

Table 2 is the database records scores of students in School A in the final exam. We need to help teacher query the database while protecting the privacy of students' scores. The domain of this database is $\{$ Male, Female $\} \times \{0, 1, 2, \ldots, 100\}^6$. In this question, assume that two inputs X and Y are neighbouring inputs if X can be obtained from Y by removing or adding one element. Answer the following questions.

2.1

What is the sensitivity of the following queries:

1. $q_1 = \frac{1}{2000} \sum_{ID=1}^{2000}$ Mathematics $_{ID}$
2. $q_2 = \max_{ID \in [1,2000]}$ English $_{ID}$

2.2

Design ϵ -differential privacy mechanisms corresponding to the two queries in 2.1 where $\epsilon = 0.1$. (Using Laplace mechanism for q_1, Exponential mechanism for q_2.)

2.3

Let $M_1, M_2, \ldots, M_{100}$ be 100 Gaussian mechanisms that satisfy $(\epsilon_0, \delta_0) - \mathrm{DP}$, respectively, with respect to the database. Given $(\epsilon, \delta) = (1.25, 10^{-5})$, calculate σ for every query with the composition theorem (Theorem 3.16 in the textbook) and the advanced composition theorem (Theorem 3.20 in the textbook, choose $\delta' = \delta$) such that the total query satisfies (ϵ, δ) - DP.