DataPrivacy HW2

PB18111760 王嘉梁

一:

1 Concept of DP(15')

1.1

Prove that the Laplace mechanism preserves $(\epsilon, 0)$-DP.

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.

1.3

Please explain the difference between DP and Local DP.

1.1

考虑任意相邻数据集x、$y \in \mathbb{N}^{|k|}$, $(||x-y||_1 \le 1)$

设f是$\mathbb{N}^{|k|} \to \mathbb{R}^k$的映射函数，用$p_x$代表概率密度函数$M_L(x,f,\epsilon)$，用$p_y$代表概率密度函数$M_L(y,f,\epsilon)$

比较两个概率密度函数在任意点$z \in \mathbb{R}^k$的大小：

$$\frac{p_x(z)}{p_y(z)} = \prod_{i=1}^{k}(\frac{exp(-\frac{\epsilon|f(x)_i - z_i|}{\Delta f})}{exp(-\frac{\epsilon|f(y)_i - z_i|}{\Delta f})})$$

$$= \prod_{i=1}^{k} exp(\frac{\epsilon(|f(y)_i - z_i| - |f(x)_i - z_i|)}{\Delta f})$$

由三角不等式$(|f(y)_i - z_i| - |f(x)_i - z_i|) \le |f(x)_i - f(y)_i|$

$$\le \prod_{i=1}^{k} exp(\frac{\epsilon|f(x)_i - f(y)_i|}{\Delta f})$$

$$= exp(\frac{\epsilon \sum_{i=1}^{n} |f(x)_i - f(y)_i|}{\Delta f})$$

由定义，$\sum_{i=1}^{n} |f(x)_i - f(y)_i| = ||f(x) - f(y)||_1$且$\Delta f = max_{x、y \in \mathbb{N}^{|k|}, ||x-y||_1 = 1} ||f(x) - f(y)||_1$

$$= exp(\frac{\epsilon \cdot ||f(x) - f(y)||_1}{\Delta f})$$

$$\le exp(\epsilon)$$

同理，可以得到$\frac{p_x(z)}{p_y(z)} \ge exp(-\epsilon)$

综上所述，$Laplace\ \ mechanism$ 满足$(\epsilon, 0) - DP$

1.2

一个算法M满足$(\epsilon,0)-DP$，即对所有相邻的输入D，D'，对所有的度量S，$Pr[M(D) \in S] \le e^{\epsilon} Pr[M(D) \in S]$

一个算法M满足$(\epsilon,\delta)-DP$，即对所有相邻的输入D，D'，对所有的度量S，$Pr[M(D) \in S] \le e^{\epsilon} Pr[M(D) \in S] + \delta$

也即是，$(\epsilon,0)-DP$在所有时候都严格控制相邻数据集输出的相似性，但$(\epsilon,\delta)-DP$允许在δ的情况下，相邻数据集的输出不同

$(\epsilon,0)-DP$虽然对于隐私数据的保护比$(\epsilon,\delta)-DP$好，但与之相对的，需要付出数据可用性更差的代价

$(\epsilon,\delta)-DP$虽然只在$(1-\delta)$的概率下保证了（ϵ，0）隐私条件，但可以获得更好的$loss$

一般的，对于一个共n条记录的敏感数据集，我们选择$\delta << \frac{1}{n}$，因为这样可以保证$\delta * n << 1\ record$，保证每条记录的安全

1.3

DP中存在一个可信的数据中心，将所有用户的数据收集到数据中心后，针对每个查询，对原始数据进行处理后返回查询结果。

然而现实中很难存在一个让所有人都相信的第三方数据中心，所以$Local-DP$应运而生。

在$Local-DP$中，不存在这样的可信数据中心，每个用户在上传自己的数据之前，都要进行加噪，以防自己的隐私大规模泄露。

二者对于隐私保护的定义都是相同的，即对于任意两个相邻数据集x, y，他们对于查询的输出相似程度由(ϵ,δ)控制：

$$P[f(x)=t] \le e^{\epsilon} P[f(y)=t] + \delta$$

不同之处在于，DP中x, y来源是所有用户的数据总集，而LDP中x, y来源是每个用户自己的数据集。

二、

2 Basics of DP(30')

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 1 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 $\{Male, Female\} \times$

$\{0, 1, 2, ..., 100\}^6$. 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 $M_1, M_2, ..., M_{100}$ be 100 Gaussian mechanisms that satisfy (ϵ_0, δ_0)-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.

2.1

$$(1)q_1 = \frac{1}{2000}\sum_{ID=1}^{2000} Mathematics_{ID}$$

$$sensitivity = \frac{100}{2000} = \frac{1}{20}$$

$$(2)q_2 = max_{ID\in[1,2000]} English_{ID}$$

$$sensitivity = 100(\text{某个学生}English = 100, \text{其余学生}English\text{均为}0)$$

2.2

(1)对于q_1,使用$Laplace$机制$,\Delta f = sensitivity(q_1) = \frac{1}{20}, \epsilon = 0.1$

所以$\frac{\Delta f}{\epsilon} = 0.5$，所以$q_1$需要对数据加上$Lap(0.5)$的噪声

(2)对于q_2,使用指数机制$,\Delta f = GS(q_2) = max_{r\in R, ||D-D'||_1 \le 1}(q_2(D,r) - q_2(D',r))$

在这个问题中，我们关心的是成绩的最大值，所以可用性函数$q_2(D,r)$应该取$English - score$

所以$\Delta f = 100, \epsilon = 0.1$

所以$\frac{\epsilon}{2\Delta f} = \frac{1}{2000}$，所以$q_1$需要对数据加上$E(\frac{1}{2000})$的噪声

2.3

Theorem 3.16. Let $\mathcal{M}_i : \mathbb{N}^{|\mathcal{X}|} \to \mathcal{R}_i$ be an $(\varepsilon_i, \delta_i)$-differentially private algorithm for $i \in [k]$. Then if $\mathcal{M}_{[k]} : \mathbb{N}^{|\mathcal{X}|} \to \prod_{i=1}^k \mathcal{R}_i$ is defined to be $\mathcal{M}_{[k]}(x) = (\mathcal{M}_1(x), \ldots, \mathcal{M}_k(x))$, then $\mathcal{M}_{[k]}$ is $(\sum_{i=1}^k \varepsilon_i, \sum_{i=1}^k \delta_i)$-differentially private.

Theorem 3.20 (Advanced Composition). For all $\varepsilon, \delta, \delta' \ge 0$, the class of (ε, δ)-differentially private mechanisms satisfies $(\varepsilon', k\delta + \delta')$-differential privacy under k-fold adaptive composition for:

$$\varepsilon' = \sqrt{2k \ln(1/\delta')}\varepsilon + k\varepsilon(e^\varepsilon - 1).$$

(1)对于q_1使用$Theorem3.16$:

$M_i(i \in [1,100])$满足$(\epsilon_o, \delta_0) - DP$,根据$Theorem\ 3.16$:

$M_{[100]}$ 满足 $(\sum_{i=1}^{100} \epsilon_i, \sum_{i=1}^{100} \delta_i) - DP = (100\epsilon_o, 100\delta_0) - DP$

我们想要$M_{[100]}$去满足的是$(1.25, 10^{-5}) - DP$,则$\epsilon_0 = 1.25 * 10^{-2}, \delta_0 = 10^{-5} * 10^{-2}$

因为q_1所查询是均值,所以$L2$距离与$L1$距离相同$,\Delta f = 0.05$

$$\sigma = \frac{\sqrt{2ln(\frac{1.25}{\delta_0})} * \Delta f}{\epsilon_0} \frac{\sqrt{2ln(\frac{1.25}{10^{-7}})} * \frac{1}{20}}{1.25 * 10^{-2}} = 22.8674$$

对于q_1使用$Theorem3.20$:

即$\epsilon' = 1.25, 100\delta + \delta' = 10^{-5}$

又有$\delta' = \delta_0$,故$\epsilon' = 1.25 = \sqrt{2 * 100 * ln(\frac{1}{\delta'})} * \epsilon_0 + 100 * \epsilon_0(e^{\epsilon_0} - 1), \delta' = \frac{10^{-5}}{101} \approx 10^{-7}$

解方程得到$\epsilon_0 = 0.021208738, \delta_0 = 10^{-7}, \sigma = \frac{\sqrt{2ln(\frac{1.25}{\delta_0})} * \Delta f}{\epsilon_0}$

对于$Gaussian\ Machanisms, \Delta f = max_{D,D'} ||f(D) - f(D')||_2$

因为q_1所查询是均值,所以$L2$距离与$L1$距离相同$,\Delta f = 0.05$

$$\sigma = \frac{\sqrt{2ln(\frac{1.25}{\delta_0})} * \Delta f}{\epsilon_0} \approx \frac{\sqrt{2ln(\frac{1.25}{10^{-7}})} * \frac{1}{20}}{0.021208738} = 13.4776$$

(2)对于q_2使用$Theorem 3.16$:

$$M_i(i \in [1,100])满足(\epsilon_o,\delta_0)-DP,根据Theorem\ 3.16:$$

$$M_{[100]}\ 满足\quad (\sum_{i=1}^{100}\epsilon_i,\sum_{i=1}^{100}\delta_i)-DP=(100\epsilon_o,100\delta_0)-DP$$

$$我们想要M_{[100]}去满足的是(1.25,10^{-5})-DP,则\epsilon_0=1.25*10^{-2},\delta_0=10^{-5}*10^{-2}$$

$$因为q_2所查询是最大值,所以L2距离与L1距离相同,\Delta f=100$$

$$\sigma=\frac{\sqrt{2ln(\frac{1.25}{\delta_0})}*\Delta f}{\epsilon_0}=\frac{\sqrt{2ln(\frac{1.25}{10^{-7}})}*100}{1.25*10^{-2}}=45734$$

对于q_2使用$Theorem 3.20$:

$$又有\delta'=\delta,故\epsilon'=1.25=\sqrt{2*100*ln(\frac{1}{\delta'})}*\epsilon_0+100*\epsilon_0(e^{\epsilon_0}-1),\delta'=\frac{10^{-5}}{101}\approx 10^{-7}$$

$$解方程得到\epsilon_0=0.021208738,\delta_0=10^{-7},\sigma=\frac{\sqrt{2ln(\frac{1.25}{\delta_0})}*\Delta f}{\epsilon_0}$$

$$对于Gaussian\ Machanisms,\Delta f=max_{D,D'}||f(D)-f(D')||_2$$

$$因为q_2所查询是最大值,所以L2距离与L1距离相同,\Delta f=100$$

$$\sigma=\frac{\sqrt{2ln(\frac{1.25}{\delta_0})}*\Delta f}{\epsilon_0}\approx\frac{\sqrt{2ln(\frac{1.25}{10^{-7}})}*100}{0.021208738}=26955$$

三、

3 Local DP(30')

This question focuses on the problem of estimating the mean value of a numeric attributes by collecting data from individuals under ϵ-LDP. Assume that each user u_i's data record t_i contains a single numeric attribute whose value lies in range $[-1,1]$. Answer the following questions.

3.1

Prove that Algorithm 1 satisfies ϵ-LDP.

3.2

Prove that given an input value t_i, Algorithm 1 returns a noisy value t_i^* with $\mathbb{E}[t_i^*]=t_i$ and $Var[t_i^*]=\frac{t_i^2}{e^{\epsilon/2}-1}+\frac{e^{\epsilon/2}+3}{3(e^{\epsilon/2}-1)^2}$.

Algorithm 1

Input: tuple $t_i \in [-1,1]$ and privacy parameter ϵ.
Output: tuple $t_i^* \in [-C,C]$;

Sample x uniformly at random from [0,1];
$C=\frac{exp(\epsilon/2)+1}{exp(\epsilon/2)-1}$;
$l(t_i)=\frac{C+1}{2}\cdot t_i-\frac{C-1}{2}$;
$r(t_i)=l(t_i)+C-1$;
if $x<\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}$ **then**
    Sample t_i^* uniformly at random from $[l(t_i),r(t_i)]$;
else
    Sample t_i^* uniformly at random from $[-C,l(t_i)]\cup[r(t_i),C]$;
end if
return t_i^*;

3.1

由题意：

$-C = \frac{C+1}{2} * -1 - \frac{C-1}{2} \le l(t_i) \le \frac{C+1}{2} * 1 - \frac{C-1}{2} = 1$

$-1 = -C + C - 1 \le r(t_i) = l(t_i) + C - 1 \le 1 + C - 1 = C$

即$l(t_i) \in [-C, 1], r(t_i) \in [-1, C]$,且二者取值是线性映射,$r(t_i) > l(t_i)$

(1)从$[0,1]$均匀分布中选择x

(2)计算概率密度函数$p_{t_i^*}(t_i^* = x|t_i)$

$x \in [l(t_i), r(t_i)]$时，$t_i^* = x$发生在$x < \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}$时,而$P(x < \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}) = \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}$

此时t^*在$[l(t_i), r(t_i)]$服从均匀分布，故$P(t_i^* = x) = \frac{1}{r(t_i) - l(t_i)} = \frac{1}{C-1} = \frac{e^{\frac{\epsilon}{2}}-1}{2}$

$$
\begin{aligned}
\text{所以} p_{t_i^*}(t_i^* = x|t_i) &= P(x < \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}) * P(t_i^* = x) \\
&= \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1} * \frac{e^{\frac{\epsilon}{2}}-1}{2} \\
&= \frac{e^{\epsilon} - e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2} \qquad x \in [l(t_i), r(t_i)]
\end{aligned}
$$

$x \in [-C, l(t_i)] \cup [r(t_i), C]$时,$t_i^* = x$发生在$x \ge \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}$时，而$P(x \ge \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}) = 1 - \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1} = \frac{1}{e^{\frac{\epsilon}{2}}+1}$

此时t^*在$[-C, l(t_i)] \cup [r(t_i), C]$中服从均匀分布

故$P(t_i^* = x) = \frac{1}{l(t_i) - (-C) + C - r(t_i)} = \frac{1}{C+1} = \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\frac{\epsilon}{2}}}$

$$
\begin{aligned}
\text{所以} p_{t_i^*}(t_i^* = x|t_i) &= P(x \ge \frac{e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}+1}) * P(t_i^* = x) \\
&= \frac{1}{e^{\frac{\epsilon}{2}}+1} * \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\frac{\epsilon}{2}}} \\
&= \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}} \qquad x \in [-C, l(t_i)] \cup [r(t_i), C]
\end{aligned}
$$

$$
\text{综上所述}, p_{t_i^*}(t_i^* = x|t_i) = \begin{cases} \frac{e^{\epsilon} - e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2} & x \in [l(t_i), r(t_i)] \\ \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}} & x \in [-C, l(t_i)] \cup [r(t_i), C] \end{cases}
$$

(3)$\forall t^* \in [-C, C]$ and $\forall input$ $t_i, t_i^* \in [-1, 1]$

$$
\frac{p(t^*|t)}{p(t^*|t')} \le \frac{\frac{e^{\epsilon} - e^{\frac{\epsilon}{2}}}{2e^{\epsilon}+2}}{\frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}}} = e^{\epsilon}
$$

证毕!

3.2

$$
\begin{aligned}
(1)\mathbb{E}[t_i^*] &= \int_{-C}^{l(t_i)} x * p(t_i^* = x)dx + \int_{l(t_i)}^{r(t_i)} x * p(t_i^* = x)dx + \int_{r(t_i)}^{C} x * p(t_i^* = x)dx \\
&= \int_{-C}^{l(t_i)} x * \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}}dx + \int_{l(t_i)}^{r(t_i)} x * \frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}dx + \int_{r(t_i)}^{C} x * \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}}dx \\
&= \frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2} * \frac{1}{2e^{\epsilon}} * [l^2(t_i) - r^2(t_i)] + \frac{\frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}}{2}[r^2(t_i) - l^2(t_i)] \\
&= \frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}(-\frac{1}{2e^{\epsilon}} + \frac{1}{2}) * \frac{2e^{\frac{\epsilon}{2}}}{e^{\frac{\epsilon}{2}}-1} * t_i * \frac{2}{e^{\frac{\epsilon}{2}}-1} \\
&= t_i
\end{aligned}
$$

$$
\begin{aligned}
(2)Var[t_i^*] &= E[(t_i^*)^2] - E[t_i^*]^2 \\
&= \int_{-C}^{l(t_i)} x^2 * \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}}dx + \int_{l(t_i)}^{r(t_i)} x^2 * \frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}dx + \int_{r(t_i)}^{C} x^2 * \frac{e^{\frac{\epsilon}{2}}-1}{2e^{\epsilon}+2e^{\frac{\epsilon}{2}}}dx - t_i^2 \\
&= \frac{\frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}}{3e^{\epsilon}}[l^3(t_i) - r^3(t_i) + 2C^3] + \frac{\frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}}{3}[r^3(t_i) - l^3(t_i)] - t_i^2 \\
&= \frac{e^{\epsilon}-e^{\frac{\epsilon}{2}}}{2e^{\frac{\epsilon}{2}}+2}[(\frac{1}{3} - \frac{1}{3e^{\epsilon}})\frac{6e^{\epsilon}t_i^2+2}{(e^{\frac{\epsilon}{2}}-1)^3} + \frac{2}{3e^{\epsilon}}(\frac{e^{\frac{\epsilon}{2}}+1}{e^{\frac{\epsilon}{2}}-1})^3] - t_i^2 \\
&= \frac{t_i^2}{e^{\frac{\epsilon}{2}}-1} + \frac{e^{\frac{\epsilon}{2}}+3}{3(e^{\frac{\epsilon}{2}}-1)^2}
\end{aligned}
$$

证毕!

四、

4 Random Subsampling(25')

Given a dataset $x \in \mathcal{X}^n$, and $m \in \{0, 1, ..., n\}$, a *random m-sumsample of* x is a new (random) dataset $x' \in \mathcal{X}^m$ formed by keeping a random subset of m rows from x and throwing out the remaining $n - m$ rows.

4.1

Show that for every $n \in \mathbb{N}$, $\mathcal{X} \geq 2$, $m \in \{1, ..., n\}$, $\epsilon > 0$ and $\delta < m/n$, the mechanism $M(x)$ that outputs a random m-subsample of $x \in \mathcal{X}^n$ is not (ϵ, δ)-DP.

4.2

Although random subsamples do not ensure differential privacy on their own, a random subsample dose have the effect of "amplifying" differential privacy. Let $M : \mathcal{X}^m \rightarrow \mathcal{R}$ be any algorithm. We define the algorithm $M' : \mathcal{X}^n \rightarrow \mathcal{R}$ as follows: choose x' to be a random m-subsample of x, then output $M(x')$.

Prove that if M is (ϵ, δ)-DP, then M' is $((e^\epsilon - 1) \cdot m/n, \delta m/n)$-DP. Thus, if we have an algorithm with the relatively weak guarantee of 1-DP, we can get an algorithm with ϵ-DP by using a random subsample of a database that is larger by a factor of $1/(e^\epsilon - 1) = O(1/\epsilon)$.

4.1

反例如下：

取$\mathcal{X} = 0, 1$，这是满足$|\mathcal{X}| \geq 2$的；$\forall n$，令$x = 1^n, x' = 0 \cdot 1^{n-1}$，这是满足$x, x' \in \mathcal{X}$的；

令$S = \{z = \{0,1\}^m | z \neq 1^m\}$，对$\forall \epsilon$和$\forall \delta < \dfrac{m}{n}$，有：

$$e^\epsilon Pr[M(x) \in S] + \delta = \delta < \frac{m}{n} = Pr[M(x') \in S]$$

这与$(\epsilon, \delta) - DP$的要求：$e^\epsilon Pr[M(x) \in S] + \delta = Pr[M(x') \in S]$相悖

对于其他任意$|\mathcal{X}| \geq 2$，均可使用相同方法构造反例

4.2

对于M'算法而言，它的输出相对于原始数据的随机性来源于M算法引入的(ϵ, δ)随机性以及M'算法本身带来的$m - subsample$的随机性

使用随机变量$index \subseteq \{0, 1, 2, \ldots, n\}$，代表$M'$算法中随机选择留下来的$row$是哪些，使用$x, x'$代表相邻数据集，二者相差某一个$row$，记为 t

使用x_t, x'_t代表从x, x'中随机采样的新数据集；令S是M'值域的任意子集

欲证明M'满足$((e^{\epsilon}-1)*\frac{m}{n},\delta\frac{m}{n})-DP$,即要证：$Pr[M'(x)\in S]\leq e^{(e^{\epsilon}-1)*\frac{m}{n}}Pr[M'(x')\in S]+\delta\frac{m}{n}$

为简洁表达，令$q=\frac{m}{n}$,即证$\frac{Pr[M'(x)\in S]-q\delta}{Pr[M'(x')\in S]}\leq e^{q(e^{\epsilon}-1)}$

将上式左值替换成有关算法M的表达式，x和x'将通过$m-subsample$变成x_t和x'_t(规模从n维变成m维)

记x_t的随机变量为$i\subseteq\{0,1,2,\ldots,n\}$,因为$m-subsample$随机从规模为$n$的$x$中选取$m$个$row$组成新的$m$维$x_t$,

故x_t的$newindex$，即i有q的概率在$index$中，$(1-q)$的概率不在$index$中

同理x'_t的$newindex$，即i也有q的概率在$index$中，$(1-q)$的概率不在$index$中

故可以得到：

$$\frac{Pr[M'(x)\in S]-q\delta}{Pr[M'(x')\in S]}=\frac{qPr[M(x_t)\in S|i\in index]+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta}{qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index]}$$

因为M算法是满足$(\epsilon,\delta)-DP$的，所以我们可以得到$M\leq e^{\epsilon}min\{Pr[M(x'_t)\in S|i\in index],Pr[M(x'_t)\in S|i\notin index]\}+\delta$

所以$qPr[M(x_t)\in S|i\in index]+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta$

$$\begin{aligned}
&\leq q(e^{\epsilon}min\{Pr[M(x'_t)\in S|i\in index],Pr[M(x'_t)\in S|i\notin index]\}+\delta)+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta\\
&\leq q(min\{Pr[M(x'_t)\in S|i\in index],Pr[M(x'_t)\in S|i\notin index]\}\\
&\qquad+(e^{\epsilon-1})min\{Pr[M(x'_t)\in S|i\in index],Pr[M(x'_t)\in S|i\notin index]\}+\delta)\\
&\quad+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta
\end{aligned}$$

由$min\{x,y\}\leq ax+(1-a)y\ where\ a\in[0,1]$,得

$$\begin{aligned}
&\leq q(min\{Pr[M(x'_t)\in S|i\in index],Pr[M(x'_t)\in S|i\notin index]\}\\
&\qquad+(e^{\epsilon-1})(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])+\delta)\\
&\quad+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta\\
&\leq q(Pr[M(x'_t)\in S|i\in index]+(e^{\epsilon-1})(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])+\delta)\\
&\quad+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta\\
&\leq q(Pr[M(x'_t)\in S|i\in index]+(e^{\epsilon-1})(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index]))\\
&\quad+(1-q)Pr[M(x_t)\in S|i\notin index]\\
&\leq(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])\\
&\quad+(q(e^{\epsilon-1}))(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])\\
&\leq(1+q(e^{\epsilon-1}))(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])
\end{aligned}$$

由$e^x\geq 1+x$，得

$$\leq e^{q(e^{\epsilon-1})}(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])$$

即得到：

$$\begin{aligned}
&qPr[M(x_t)\in S|i\in index]+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta\\
&\leq e^{q(e^{\epsilon-1})}(qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index])
\end{aligned}$$

即是：

$$\frac{qPr[M(x_t)\in S|i\in index]+(1-q)Pr[M(x_t)\in S|i\notin index]-q\delta}{qPr[M(x'_t)\in S|i\in index]+(1-q)Pr[M(x'_t)\in S|i\notin index]}\leq e^{q(e^{\epsilon-1})}$$

即是：

$$\frac{Pr[M'(x)\in S]-q\delta}{Pr[M'(x')\in S]}\leq e^{q(e^{\epsilon}-1)}$$

即是：

$$Pr[M'(x)\in S]\leq e^{(e^{\epsilon}-1)*\frac{m}{n}}Pr[M'(x')\in S]+\delta\frac{m}{n}$$

证毕！