数据隐私HW2

范翔宇 PB18000006

Q1

1.1

使$x \in N^{|x|}$和$y \in N^{|x|}$满足$||x-y||_1 \le 1$，定义$f(\cdot)$为某个$N^{|x|} \to R^k$的函数，p_x代表$M_l(x,f,\epsilon)$的概率密度函数，p_y代表$M_l(y,f,\epsilon)$的概率密度函数，我们在同一点$z \in R^k$比较这$p_x, p_y(x,y,z$均为任取)

$\frac{p_x(z)}{p_y(z)} = \prod_{i=1}^{k}(\frac{exp(-\frac{\epsilon|f(x)_i-z_i|}{\Delta f})}{exp(-\frac{\epsilon|f(y)_i-z_i|}{\Delta f})})$
$= \prod_{i=1}^{k} exp(\frac{\epsilon(|f(y)_i-z_i|-|f(x)_i-z_i|)}{\Delta f})$
$\le \prod_{i=1}^{k} exp(\frac{\epsilon|f(x)_i-f(y)_i|}{\Delta f})$
$= exp(\frac{\epsilon||f(x)-f(y)||_1}{\Delta f})$
$\le exp(\epsilon)$

上述推导过程中，第一个不等式利用了三角不等式，最后一个不等式基于$l_1-sensitivity$的定义以及$||x-y||_1 \le 1$的事实，$\frac{p_x(z)}{p_y(z)} \ge exp(-\epsilon)$也可以对称推出。综上即得，$Laplacemechanism$可以保证$(\epsilon,0)-DP$

1.2

$(\epsilon,0)-DP$:对于$M(x)$机制的每一次运行，所观察到的输出在每个相邻的数据库上被观察到的可能性几乎相等；

$(\epsilon,\delta)-DP$:给定的一个$\xi \sim M(x)$输出，可能找到一个数据库y，使得从y产生的ξ可能比从另一个数据库x产生的更大。而由观察ξ导致的$PrivacyLoss$为$\mathcal{L}^{\xi}_{M(x)||M(y)} = ln(\frac{Pr[M(x)=\xi]}{Pr[M(y)=\xi]})$;

另外$(\epsilon,\delta)-DP$确保了对于所有邻近的x,y，$PrivacyLoss$的绝对值能以至少$1-\delta$的概率被ξ所限制。

1.3

DP与$LocalDP$的差别如下：

- 主要用途不同：DP用于数据发布或者查询，处理的是针对整个数据库的数据；而$LocalDP$用于收集用户信息，处理的是针对单个用户的数据。
- 对第三方数据收集方的信任要求程度不同：DP需要第三方可以信任，因为第三方能够看到真实的原始数据，而$LocalDP$则无论第三方是否可信任，用户都可以自己在本地给原始数据加噪，再将加噪处理后的数据交给第三方，另外后者要加的噪声通常比前者的噪声要大；
- 加噪机制不同：DP加噪机制以拉普拉斯机制和指数机制为主。而$LocalDP$噪声机制以随机响应为主；

Q2

2.1

(1)

q_1不是很敏感，即使是只有一位同学考了100分，其他同学全部考了0分，即使我们将考100分的同学记录删除，q_1的敏感度此时也只有0.05，q_1也处在很小的波动范围内，整体仍具有参考性。

(2)

q_2较为敏感，想象一下这场英语考试难度特别大，只有一位同学超常发挥考了100分， 而其他同学都考了0分，第二名(这里均指英语单科排名，下同)同样也只考了0分。那么如果我们将第一名的成绩记录删除，这时q_2反而指向第二名的0分，敏感度为100，整体不再具有可信赖的参考性。

2.2

- $f(x) = q_1(x), \Delta f(x) = 0.05, \frac{\Delta f}{\epsilon} = 0.5$

则$LaplaceMechanism: M_L(x,f,\epsilon)=f(x)+Y$，其中$Y\sim Lap(0.5)$

- 设$\mathcal{X}()$为示性函数，$e(x,r)=\mathcal{X}(r=max(x))$为期望收益函数，由定义可知$\Delta u=100$；

  $ExponentialMechanism$:用与$exp(\frac{\epsilon e(x,r)}{2\Delta u})=exp(\frac{e(x,r)}{2000})$成比例的概率输出元素$r\in\{0,1,\dots,100\}$

2.3

由定理3.22，即

Theorem 3.22. Let $\varepsilon\in(0,1)$ be arbitrary. For $c^2>2\ln(1.25/\delta)$, the Gaussian Mechanism with parameter $\sigma\geq c\Delta_2(f)/\varepsilon$ is (ε,δ)-differentially private.

可知$\sigma^2\geq 2ln(1.25/\delta)/\epsilon^2$时，有$GaussianMechanism$是$(\epsilon,\delta)-DP$的。

- $the\ composition\ theorem$

  由定理3.16，即

  > **Theorem 3.16.** Let $\mathcal{M}_i:\mathbb{N}^{|\mathcal{X}|}\to\mathcal{R}_i$ be an (ε_i,δ_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 $\mathcal{M}_{[k]}(x)=(\mathcal{M}_1(x),\dots,\mathcal{M}_k(x))$, then $\mathcal{M}_{[k]}$ is $(\sum_{i=1}^k\varepsilon_i,\sum_{i=1}^k\delta_i)$-differentially private.

  得每次更新是$(\frac{\epsilon}{100},\frac{\delta}{100})-DP$的，代入数据即$(1.25\times10^{-2},10^{-7})-DP$的，方能确保总查询满足$(\epsilon,\delta)-DP$，即$\sigma^2\geq 2.1\times10^5$

- $the\ advanced\ composition\ theorem$

  由定理3.20，即

  > **Theorem 3.20** (Advanced Composition). For all $\varepsilon,\delta,\delta'\geq0$, the class of (ε,δ)-differentially private mechanisms satisfies $(\varepsilon',k\delta+\delta')$-differential privacy under k-fold adaptive composition for:
  >
  > $$\varepsilon'=\sqrt{2k\ln(1/\delta')}\varepsilon+k\varepsilon(e^{\varepsilon}-1).$$

  结合$\delta^{'}=\delta$知总查询应该满足$(\epsilon^{'},101\delta_0)-DP$的，其中$\epsilon^{'}=\sqrt{200ln(1/\delta^{'})}\epsilon_0+100\epsilon_0(e^{\epsilon_0}-1)$，代入$\epsilon^{'}=1.25$和$101\delta_0=10^{-5}$，有$\epsilon_0=0.021$和$\delta_0=9.9\times10^{-8}$，则$\sigma^2\geq7.416\times10^4$

Q3

3.1

设$[l(t_i),r(t_i)]$为区间A，$[-C,l(t_i)]\cup[r(t_i),C]$为区间B，A区间长度为C-1，B区间长度为C+1。

结合题意，有四种情况，每种情况对应概率密度为：

$$P[f(t)=t^*]=\begin{cases}\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}\frac{C-1}{2C},x<\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in A\\ \frac{1}{e^{\epsilon/2}+1}\frac{C-1}{2C},x\geq\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in A\\ \frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}\frac{C+1}{2C},x<\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in B\\ \frac{1}{e^{\epsilon/2}+1}\frac{C+1}{2C},x\geq\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in B\end{cases}$$

则$\forall t_0,t_1$，均有：

$$\frac{Pr[f(t_0)=t^*]}{Pr[f(t_1)=t^*]}=\frac{P[f(t_0)=t^*]}{P[f(t_1)=t^*]}\leq\frac{P[x<\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in B]}{P[x\geq\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1},t^*\in A]}=\frac{\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}\frac{C+1}{2C}}{\frac{1}{e^{\epsilon/2}+1}\frac{C-1}{2C}}=\frac{e^{\epsilon/2}(C+1)}{C-1}=\frac{e^{\epsilon/2}(\frac{e^{\epsilon/2}+1}{\epsilon/2-1}+1)}{\frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1}-1}=\frac{e^{\epsilon/2}(e^{\epsilon/2}+1+e^{\epsilon/2}-1)}{e^{\epsilon/2}+1-e^{\epsilon/2}+1}=\frac{2e^{\epsilon/2}}{2}=e^{\epsilon}$$

即证。

3.2

(吐槽一下，这题真的就纯概率论硬算呗？)

先求期望，设$x < \frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}$为C，设$x \geq \frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}$为D

$E[t_i^*] = E[t_i^*|C]P(C) + E[t_i^*|D]P(D)$

分别求$E[t_i^*|C]$和$E[t_i^*|D]$

$E[t_i^*|C] = \int_{l(t_i)}^{r(t_i)} \frac{1}{r(t_i)-l(t_i)} xdx = \frac{r(t_i)+l(t_i)}{2}$

$E[t_i^*|D] = \int_{-C}^{l(t_i)} \frac{1}{2C-r(t_i)+l(t_i)} xdx + \int_{r(t_i)}^{C} \frac{1}{2C-r(t_i)+l(t_i)} xdx = \frac{l^2(t_i)-r^2(t_i)}{2(2C-r(t_i)+l(t_i))}$

而结合$r(t_i)$、$l(t_i)$、C，知三者关系为$r(t_i) - l(t_i) = C - 1$，$r(t_i) + l(t_i) = (C+1)t_i$

则有

$E[t_i^*|C] = \frac{(C+1)t_i}{2}$

$E[t_i^*|D] = -\frac{(C-1)(C+1)t_i}{2(2C-(C-1))} = -\frac{(C-1)t_i}{2}$

又$P(C)$、$P(D)$均已知

则

$E[t_i^*] = \frac{(C+1)t_i}{2}\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1} - \frac{(C-1)t_i}{2}\frac{1}{e^{\epsilon/2}+1} = \frac{\frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1}+1}{2}\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}t_i - \frac{\frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1}-1}{2}\frac{1}{e^{\epsilon/2}+1}t_i = \frac{e^{\epsilon/2}(e^{\epsilon/2}+1+e^{\epsilon/2}-1)-(e^{\epsilon/2}+1-e^{\epsilon/2}+1)}{2(e^{\epsilon/2}+1)(e^{\epsilon/2}-1)}t_i = \frac{2e^{\epsilon}-2}{2(e^{\epsilon}-1)}t_i = t_i$

再求方差，先陈列一些已知条件，$r(t_i)$、$l(t_i)$、C三者关系在此就不赘述，补充一下$P(C)$、$P(D)$、C三者之间的关系，显然有：$P(C) = \frac{e^{\epsilon/2}}{e^{\epsilon/2}+1} = \frac{1+C}{2C}$，$P(D) = \frac{C-1}{2C}$，另外还要补充$l(t_i) = \frac{C+1}{2}t_i - \frac{C-1}{2}$，$r(t_i) = \frac{C+1}{2}t_i + \frac{C-1}{2}$，下面先求$E[t_i^{*2}]$，同样有：$E[t_i^{*2}] = E[t_i^{*2}|C]P(C) + E[t_i^{*2}|D]P(D)$。

分别求$E[t_i^{*2}|C]$和$E[t_i^{*2}|D]$

$E[t_i^{*2}|C] = \int_{l(t_i)}^{r(t_i)} \frac{x^2}{r(t_i)-l(t_i)}dx = \frac{r^3(t_i)-l^3(t_i)}{3(r(t_i)-l(t_i))} = \frac{(r(t_i)-l(t_i))(r^2(t_i)+r(t_i)l(t_i)+l^2(t_i))}{3(r(t_i)-l(t_i))} = \frac{r^2(t_i)+r(t_i)l(t_i)+l^2(t_i)}{3}$
$= \frac{1}{3}(\frac{(C+1)^2}{4}t_i^2 - \frac{(C^2-1)}{2}t_i + \frac{(C-1)^2}{4} + \frac{(C+1)^2}{4}t_i^2 - \frac{(C-1)^2}{4} + \frac{(C+1)^2}{4}t_i^2 + \frac{(C^2-1)}{2}t_i + \frac{(C-1)^2}{4})$
$= \frac{1}{3}(\frac{3(C+1)^2}{4}t_i^2 + \frac{(C-1)^2}{4})$
$= \frac{(C+1)^2}{4}t_i^2 + \frac{(C-1)^2}{12}$

$E[t_i^{*2}|D] = \int_{-C}^{l(t_i)} \frac{x^2}{2C-(r(t_i)-l(t_i))}dx + \int_{r(t_i)}^{C} \frac{x^2}{2C-(r(t_i)-l(t_i))}dx = \frac{2C^3+l^3(t_i)-r^3(t_i)}{3(2C-(C-1))} = \frac{2C^3+l^3(t_i)-r^3(t_i)}{3(C+1)} = \frac{2C^3+(l(t_i)-r(t_i))(l^2(t_i)+l(t_i)r(t_i)+r^2(t_i))}{3(C+1)}$
$= \frac{(2C^3-(C-1)(\frac{(C+1)^2}{4}t_i^2-\frac{(C^2-1)}{2}t_i+\frac{(C-1)^2}{4}+\frac{(C+1)^2}{4}t_i^2-\frac{(C-1)^2}{4}+\frac{(C+1)^2}{4}t_i^2+\frac{(C^2-1)}{2}t_i+\frac{(C-1)^2}{4}))}{3(C+1)} = \frac{2C^3-(C-1)(\frac{3(C+1)^2}{4}t_i^2+\frac{(C-1)^2}{4})}{3(C+1)}$
$= \frac{2C^3}{3(C+1)} - \frac{(C-1)(C+1)}{4}t_i^2 - \frac{(C-1)^3}{12(C+1)} = \frac{2C^3}{3(C+1)} - \frac{(C-1)(C+1)}{4}t_i^2 - \frac{C^3-3C^2+3C-1}{12(C+1)}$
$= \frac{7C^3+3C^2-3C+1}{12(C+1)} - \frac{C^2-1}{4}t_i^2$

$E[t_i^{*2}] = E[t_i^{*2}|C]P(C) + E[t_i^{*2}|D]P(D)$
$= \frac{(C+1)^2}{4}t_i^2 \times \frac{1+C}{2C} + \frac{(C-1)^2}{12} \times \frac{1+C}{2C} + \frac{7C^3+3C^2-3C+1}{12(C+1)} \times \frac{C-1}{2C} - \frac{C^2-1}{4}t_i^2 \times \frac{C-1}{2C}$
$= (\frac{(C+1)^3}{8C} - \frac{(C-1)^2(C+1)}{8C})t_i^2 + \frac{(C-1)^2(C+1)^2+(7C^3+3C^2-3C+1)(C-1)}{24C(C+1)}$
$= (\frac{(C+1)(C^2+2C+1-C^2+2C-1)}{8C})t_i^2 + \frac{(C-1)(C^3+C^2-C-1+7C^3+3C^2-3C+1)}{24C(C+1)}$
$= \frac{C+1}{2}t_i^2 + \frac{(C-1)(2C^2+C-1)}{6(C+1)} = \frac{C+1}{2}t_i^2 + \frac{(C-1)(2C-1)(C+1)}{6(C+1)}$
$= \frac{C+1}{2}t_i^2 + \frac{(C-1)(2C-1)}{6}$

则有

$Var[t^*] = E[t^{*2}] - E[t]^2 = \frac{C+1}{2}t_i^2 + \frac{(C-1)(2C-1)}{6} - t_i^2$
$= \frac{C-1}{2}t_i^2 + \frac{(C-1)(2C-1)}{6} = \frac{1+\frac{2}{e^{\epsilon/2}-1}-1}{2}t_i^2 + \frac{(1+\frac{2}{e^{\epsilon/2}-1}-1)(2+\frac{4}{e^{\epsilon/2}-1}-1)}{6} = \frac{2}{2(e^{\epsilon/2}-1)}t_i^2 + \frac{2(e^{\epsilon/2}+3)}{6(e^{\epsilon/2}-1)^2}$
$= \frac{1}{e^{\epsilon/2}-1}t_i^2 + \frac{e^{\epsilon/2}+3}{3(e^{\epsilon/2}-1)^2}$

证毕。

Q4

4.1

使得$X = \{0,1\}$，并考虑两个数据库$x = 0^n$和$x^* = 10^{n-1}$，现定义$S = \{z \in \{0,1\}^m | z \neq 0^m\}$。然后对于任意$\epsilon$和$\delta < m/n$有$e^\epsilon Pr[M(x) \in S] + \delta = \delta < \frac{m}{n} = Pr[M(x^*) \in S]$，与$(\epsilon, \delta) - DP$中的$M$相矛盾。

4.2

使用$T \subseteq \{1, \ldots, n\}$来表示m-样本的行数。注意到$T$是一个随机变量，而且$M^{'}$的随机性包括样本$T$的随机性和$M$的随机硬币。令$x \sim x^{'}$为相邻的数据库并假设$x$和$x^{'}$仅有某行$t$不同。使$x_T$为$x$包含$T$中一些行的子样本。令$S$为$M^{'}$的任意子集。为了方便，令$p = \frac{m}{n}$。为了体现$(p(e^\epsilon - 1), p\delta) - DP$，我们用$e^{p(e^{\epsilon - 1})}$来约束比例$\frac{Pr[M'(x) \in S] - p\delta}{Pr[M^{'}(x^{'}) \in S]} = \frac{pPr[M(x_T) \in S | i \in T] + (1-p)Pr[M(x_T) \in S | i \notin T] - p\delta}{pPr[M(x^{'}_T) \in S | i \in T] + (1-p)Pr[M(x^{'}_T) \in S | i \notin T]}$，同时为了方便，定义$C = Pr[M(x_T) \in S | i \in T], C^{'} = Pr[M(x^{'}_T \in S | i \in T)], D = Pr[M(x_T) \in S | i \notin T] = Pr[M(x^{'}_T \in S | i \notin T)]$，则可将比例重新写成$\frac{Pr[M^{'}(x) \in S]}{Pr[M^{'}(x) \in S]} = \frac{pC + (1-p)D - p\delta}{pC^{'} + (1-p)D}$，然后利用$(\epsilon, \delta) - DP, M \leq e^\epsilon min\{C^{'}, D\} + \delta$的事实，然后进行如下运算：

$$pC + (1-p)D - p\delta$$
$$\leq p(e^\epsilon min\{C^{'}, D\} + \delta) + (1-p)D - p\delta$$
$$\leq p(min\{C^{'}, D\} + (e^\epsilon - 1)min\{C^{'}, D\} + \delta) + (1-p)D - p\delta$$
$$\leq p(min\{C^{'}, D\} + (e^\epsilon - 1)(pC^{'} + (1-p)D) + \delta) + (1-p)D - p\delta$$
$$① \leq p(C^{'} + (e^\epsilon - 1)(pC^{'} + (1-p)D)) + (1-p)D - p\delta$$
$$② \leq p(C^{'} + (e^{\epsilon - 1})(pC^{'} + (1-p)D)) + (1-p)D$$
$$\leq (pC^{'} + (1-p)D) + (p(e^\epsilon - 1))(pC^{'} + (1-p)D)$$
$$\leq (1 + p(e^\epsilon - 1))(pC^{'} + (1-p)D)$$
$$\leq e^{p(e^{\epsilon - 1})}(pC^{'} + (1-p)D)$$

①因为对于任意$0 \leq \alpha \leq 1$，则 $min\{x, y\} \leq \alpha x + (1-\alpha)y$

②因为$min\{x, y\} \leq x$

这样就成功地限制了必要的概率比。