Data Privacy Homework 1

傅申　PB20000051

1. (15′) Laplace Mechanism

(a) (5′) Given the function $f(x) = \frac{1}{6}\sum_{i=1}^{6} x_i$, where $x_i \in \{1, 2, ..., 10\}$ for $i \in \{1, 2, ..., 6\}$, compute the global sensitivity and local sensitivity when $x = \{3, 5, 4, 5, 6, 7\}$.

(b) (10′) Given a database x where each element is in $\{1, 2, 3, 4, 5, 6\}$, design ε-differentially private Laplace mechanisms corresponding to the following queries, where $\varepsilon = 0.1$:

1. $q_1(x) = \sum_{i=1}^{6} x_i$
2. $q_2(x) = \max_{i\in\{1,2,...,6\}} x_i$

In this anwser, neighboring databases are those that differ in one and only one element.

The probability density function of Laplace distribution with scale b is $\text{Lap}(x \mid b) = \frac{1}{2b}\exp\left(-\frac{|x|}{b}\right)$. In this answer, a random variable X denoted as $\text{Lap}(b)$ satisfies the Laplace distribution with scale b.

(a) Global Sensitivity Since $\max|x_i - x_i'| = 9$, the global sensitivity $\Delta f = \frac{9}{6} = 1.5$

Local Sensitivity For all neighboring database x' of x, the maximum difference in sum of x and x' is 7, where $x_1 = 3$ and $x_1{}' = 10$. Thus, the local sensitivity $\text{LS}(f, x) = \frac{7}{6}$

(b) 1. The sensitivity of q_1 is $\Delta q_1 = 6 - 1 = 5$ (consider two neighboring datasets where the different elements are 1 and 6). Thus, the 0.1-differentially private Laplace mechanism is

$$\mathscr{M}_L(x, q_1(\cdot), 0.1) = \sum_{i=1}^{6} x_i + \text{Lap}(50)$$

2. The sensitivity of q_2 is $\Delta q_2 = 6 - 1 = 5$ (consider dataset $\{1, 1, ..., 1\}$ and $\{6, 1, ..., 1\}$). Thus, the 0.1-differentially private Laplace mechanism is

$$\mathscr{M}_L(x, q_2(\cdot), 0.1) = \max_{i\in\{1,2,...,6\}} x_i + \text{Lap}(50)$$

2. (15′) Exponential mechanism

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
				...			
4000	Female	86	83	98	87	82	92

Table 1: Scores of students in School A

Table 1 records the scores of students in School A in the final exam. We need to help the teacher query the database while protecting the privacy of students' scores. The domain of this database is $\{\text{Male}, \text{Female}\} \times \{0, 1, 2, ..., 100\}^6$. Answer the following questions.

(a) (5′) What is the sensitivity of the following queries:

1. $q_1(x) = \frac{1}{4000}\sum_{\text{ID}=1}^{4000} \text{Physics}_{\text{ID}}$
2. $q_2(x) = \max_{\text{ID}\in\{1,2,...,4000\}} \text{Biology}_{\text{ID}}$

(b) (10′) Design ε-differentially privacy mechanisms corresponding to the two queries in (a), where $\varepsilon = 0.1$. (Using Laplace mechanism for q_1 and exponential mechanism for q_2)

In this anwser, neighboring databases are those that differ in one and only one element.

(a) 1. Since the range of Physics score is $[0, 100]$, the maximum difference in sum of Physics score is 100. Thus, the sensitivity of q_1 is $\Delta q_1 = \frac{100}{4000} = \frac{1}{40} = 0.025$.

2. Consider Biology scores of two neighboring datasets: $\{0, 0, ..., 0\}$ and $\{100, 0, ..., 0\}$, which makes the maximum difference in query q_2. Thus, the sensitivity of q_2 is $\Delta q_2 = 100$.

(b) 1. The 0.1-differentially private Laplace mechanism for q_1 is

$$\mathscr{M}_L(x, q_1(\cdot), 0.1) = \frac{1}{4000} \sum_{\text{ID}=1}^{4000} \text{Physics}_{\text{ID}} + \text{Lap}(40)$$

2. First, define the scoring function $u(x, r) = \mathbb{I}(r = \max(x))$, where $\mathbb{I}(\cdot)$ is the indicator function. Thus, the sensitivity of u is $\Delta u = 1$. The 0.1-differentially private exponential mechanism for q_2 outputs $r \in \{0, 1, ..., 100\}$ with probability proportional to

$$\exp\left(0.1 \times \frac{u(x, r)}{2}\right) = \exp\left(\frac{u(x, r)}{20}\right).$$

3. (20′) Composition

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

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

$$\varepsilon' = \varepsilon\sqrt{2k \ln\left(\frac{1}{\delta'}\right)} + k\varepsilon(\exp(\varepsilon) - 1)$$

(a) **(10′)** Given a database $x = \{x_1, x_2, ..., x_{2000}\}$ where $x_i \in \{0, 1, 2, ..., 100\}$ for each i and privacy parameters $(\varepsilon, \delta) = \left(1.25, 10^{-5}\right)$, apply the Gaussian mechanism to protect 100 calls to the query $q_1(x) = \frac{1}{2000} \sum_{i=1}^{2000} x_i$. Determine the noise variances σ^2 of the Gaussian mechanism to ensure (ε, δ)-DP based on the composition and advanced composition theorems, respectively.

(b) **(10′)** Determine the noise variances σ^2 of the Gaussian mechanism to protect 100 calls to the query $q_2(x) = \max_{i \in \{1,2,...,2000\}} x_i$ to ensure $\left(1.25, 10^{-5}\right)$-DP based on the composition and advanced composition theorems, respectively, where x is the database in (a).

(a) First calculate the ε_0 and δ_0 for each call of q_1:

- For composition, $\varepsilon = 100\varepsilon_0$, $\delta = 100\delta_0$. Thus, $\varepsilon_0 = \frac{\varepsilon}{100} = 0.0125$, $\delta_0 = \frac{\delta}{100} = 10^{-7}$.
- For advanced composition,

$$\varepsilon = \varepsilon_0\sqrt{2k \ln\left(\frac{1}{\delta_0}\right)} + k\varepsilon_0(\exp(\varepsilon_0) - 1)$$
$$\delta = k\delta_0 + \delta_0 = (k + 1)\delta_0,$$

where $k = 100$. The solution of the above equation is

$$\delta_0 = \frac{1}{101} \times 10^{-5}$$
$$\varepsilon_0 \approx 0.0212.$$

To ensure $(\varepsilon_0, \delta_0)$-DP, the noise variance σ^2 of the Gaussian mechanism should be $2 \ln\left(\frac{1.25}{\delta_0}\right) \cdot \frac{(\Delta q_1)^2}{\varepsilon_0^2}$. The sensitivity of q_1 is $\Delta q_1 = \frac{100}{2000} = 0.05$. Thus,

- For composition, the noise variance σ^2 of the Gaussian mechanism should be

$$\sigma^2 = 2\ln\left(\frac{1.25}{10^{-7}}\right) \times \left(\frac{0.05}{0.0125}\right)^2 \approx 522.92$$

- For advanced composition, the noise variance σ^2 of the Gaussian mechanism should be

$$\sigma^2 = 2\ln\left(1.25 \times 101 \times 10^5\right) \times \left(\frac{0.05}{0.0212}\right)^2 \approx 181.91$$

(b) The sensitivity of q_2 is $\Delta q_2 = 100$. Thus,

- For composition, the noise variance σ^2 of the Gaussian mechanism should be

$$\sigma^2 = 2\ln\left(\frac{1.25}{10^{-7}}\right) \times \left(\frac{100}{0.0125}\right)^2 \approx 2.09 \times 10^9$$

- For advanced composition, the noise variance σ^2 of the Gaussian mechanism should be

$$\sigma^2 = 2\ln\left(1.25 \times 101 \times 10^5\right) \times \left(\frac{100}{0.0212}\right)^2 \approx 7.28 \times 10^8$$

4. (25′) Randomized Response for Local DP

Consider a population of n users, where the true proportion of males is denoted as π. Our objective is to gather statistics on the proportion of males, prompting a sensitive question: "Are you male?" Each user responds with either a yes or no, but due to privacy concerns, they refrain from directly disclosing their true gender. Instead, they employ a biased coin with a probability of landing heads denoted as p, and tails as $1 - p$. When the coin is tossed, a truthful response is given if heads appear, while the opposite response is provided if tails come up.

(a) (10′) Demonstrate that the aforementioned randomized response adheres to local differential privacy and determine the corresponding privacy parameter, ε.

(b) (15′) Employing the perturbation method outlined above to aggregate responses from the n users yields a statistical estimate for the number of males. Assuming the count of "yes" responses is n_1, construct an unbiased estimate π for based on n, n_1, p. Calculate the variance associated with this estimate.

(a) To make this randomized response mechanism satisfy local differential privacy, the probability of responding truthfully should be $p = \frac{\exp(\varepsilon)}{1+\exp(\varepsilon)}$. Thus, the privacy parameter ε is

$$\varepsilon = \ln\left(\frac{p}{1-p}\right).$$

(b) The probability of a user responding "yes" is

$$\Pr[\text{yes}] = p\pi + (1-p)(1-\pi) = (2p-1)\pi - p + 1.$$

Since $n_1 \sim \mathrm{B}(n, \Pr[\text{yes}])$, the expectation of n_1 is $\mathbb{E}(n_1) = n\Pr[\text{yes}]$. Thus, the unbiased estimate of π is

$$\hat{\pi} = \frac{n_1/n + p - 1}{2p-1} = \frac{n_1 + (p-1)n}{(2p-1)n}.$$

The variance associated with this estimate is

$$\begin{aligned}\mathrm{Var}(\hat{\pi}) &= \mathrm{Var}\left(\frac{n_1}{(2p-1)n}\right)\\ &= \frac{\Pr[\text{yes}](1-\Pr[\text{yes}])}{(2p-1)^2 n}\\ &= \frac{(2p\pi - p - \pi + 1)(p + \pi - 2p\pi)}{(2p-1)^2 n}.\end{aligned}$$

5. (10′) Accuracy Guarantee of DP

Consider the application of an (ε, δ)-differentially private Gaussian mechanism denoted by $\mathscr{M}$ to protect the mean estimator $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ of a d-dimensional input database x, where $x_i \in \{0, 1, ..., 100\}^d$ for each i. Let $\mathscr{M}(x)$ represent the output of this Gaussian mechanism. Utilize both the tail bound and the union bound to derive the L_∞-norm error bound of $\mathscr{M}$, denoted by $\|\mathscr{M}(x) - \bar{x}\|_\infty$, ensuring a probability of at least $1 - \beta$. Specifically, solve for the bound $\mathscr{B}$ such that

$$\Pr[\|\mathscr{M}(x) - \bar{x}\|_\infty \le \mathscr{B}] \ge 1 - \beta$$

Hint: Refer to Zhihu link for descriptions of statistical inequalities.

Denote Y_i as the noise added to the i-th dimension of the mean estimator, then $\mathscr{M}(x) = \bar{x} + Y$. Thus,

$$\|\mathscr{M}(x) - \bar{x}\|_\infty = \max_{i\in[d]}|Y_i| \Rightarrow \Pr[\|\mathscr{M}(x) - \bar{x}\|_\infty \le \mathscr{B}] = \Pr\left[\max_{i\in[d]}|Y_i| \le \mathscr{B}\right].$$

Since Y_i is i.i.d. random variables following the Gaussian distribution $\mathbb{N}(0, \sigma^2)$, there is

$$\Pr[\|\mathscr{M}(x) - \bar{x}\|_\infty \le \mathscr{B}] = \Pr\left[\max_{i\in[d]}|Y_i| \le \mathscr{B}\right] = \prod_{i=1}^{d}\Pr[|Y_i| \le \mathscr{B}] = p^d,$$

where p stands for the probability that a random variable following $\mathbb{N}(0, \sigma^2)$ is in the interval $[-\mathscr{B}, \mathscr{B}]$. It is obvious that if the inequality in the question holds, then $p \ge \sqrt[d]{1-\beta}$.

The tail bound (Chernoff-style bound) of Gaussian distribution can be written as

$$\Pr[X - \mu \ge t] \le \exp\left(-\frac{t^2}{2\sigma^2}\right), X \sim \mathbb{N}(\mu, \sigma^2).$$

So p satisfies

$$p = \Pr[|X| \le \mathscr{B}] = 1 - 2\Pr[X \ge \mathscr{B}] \ge 1 - 2\exp\left(-\frac{\mathscr{B}^2}{2\sigma^2}\right).$$

Then, the inequality in the question holds if

$$1 - 2\exp\left(-\frac{\mathscr{B}^2}{2\sigma^2}\right) \ge \sqrt[d]{1-\beta},$$

which is equivalent to

$$\mathscr{B}^2 \ge 2\sigma^2 \ln\frac{2}{1-\sqrt[d]{1-\beta}} \Leftrightarrow \mathscr{B} \ge \sqrt{2\sigma^2 \ln\frac{2}{1-\sqrt[d]{1-\beta}}}.$$

Since the Gaussian mechanism is (ε, δ)-DP, the noise variance σ^2 should satisfy

$$\Delta_2^2(\bar{x}) = \left\| \left(\frac{100}{n}, \frac{100}{n}, \frac{100}{n}, ..., \frac{100}{n} \right) \right\|_2^2 = \frac{10000d}{n^2}$$

$$\sigma^2 \geq 2 \cdot \frac{\Delta_2^2(\bar{x})}{\varepsilon^2} \ln \frac{1.25}{\delta} = \frac{20000d}{\varepsilon^2 n^2} \ln \frac{1.25}{\delta}.$$

So the bound of $\mathscr{B}$ is $\mathscr{B} \geq \sqrt{2\sigma^2 \ln \frac{2}{1 - \sqrt[d]{1-\beta}}} \geq \frac{200}{\varepsilon n} \sqrt{d \ln \frac{1.25}{\delta} \cdot \ln \frac{2}{1 - \sqrt[d]{1-\beta}}}$.

6. (15′) Personalized Differential Privacy

Consider an n-element dataset D where the i-th element is owned by a user $i \in [n]$, where $[n] = \{1, 2, ..., n\}$ and the privacy requirement of user i is ε_i-DP. A randomized mechanism $\mathscr{M}$ satisfies $\{\varepsilon_i\}_{i\in[n]}$-personalized differential privacy (or $\{\varepsilon_i\}_{i\in[n]}$-PDP) if, for every pair of neighboring datasets D, D' differing at the j-th element for an arbitrary $j \in [n]$, and for all sets S of possible outputs,

$$\Pr[\mathscr{M}(D) \in S] \leq \exp(\varepsilon_j) \Pr[\mathscr{M}(D') \in S].$$

(a) (5′) Prove the composition theorem of PDP: if a mechanism is $\left\{\varepsilon_i^{(1)}\right\}_{i\in[n]}$-PDP and another is $\left\{\varepsilon_i^{(2)}\right\}_{i\in[n]}$-PDP, then publishing the result of both is $\left\{\varepsilon_i^{(1)} + \varepsilon_i^{(2)}\right\}_{i\in[n]}$-PDP.

(b) (10′) Given a dataset D and a privacy requirement set $\{\varepsilon_i\}_{i\in[n]}$, the *Sample mechanism* works as follows:

1) We pick an arbitrary threshold value $t > 0$;
2) We sample a subset $D_S \subset D$ where the probability that the i-th element of D is contained in D_S equals $\frac{\exp(\varepsilon_i)-1}{\exp(t)-1}$ if $\varepsilon_i < t$ and 1 otherwise;
3) We output $\mathscr{M}(D_S)$, where $\mathscr{M}$ is a t-differentially private mechanism.

Prove that the Sample mechanism with any $t > 0$ is $\{\varepsilon_i\}_{i\in[n]}$-PDP.
Hint: Use the Bayes formula.

In this answer,

- $\{\varepsilon_i\}_{i\in[n]}$ is abbreviated as $\mathscr{E}$, and $\left\{\varepsilon_i^{(k)}\right\}_{i\in[n]}$ is abbreviated as $\mathscr{E}^{(k)}$;
- $D \sim D'$ stands for D and D' are neighboring datasets, and $D \overset{j}{\sim} D'$ stands for D and D' are neighboring datasets that differ at the j-th element;
- The notation D' represents a neighboring dataset of D that differs at the j-th element, i.e. $D \overset{j}{\sim} D'$;
- Function $\pi_t(\cdot)$ is defined as

$$\pi_t(x) = \begin{cases} \frac{\exp(x)-1}{\exp(t)-1} & \text{if } x < t \\ 1 & \text{otherwise} \end{cases}$$

- Sampling mechanism is denoted as $\mathscr{S}$, while the sampling procedure in it is denoted as SP.

(a) Let $\mathscr{M}_1$ and $\mathscr{M}_2$ denote two mechanisms that satisfy PDP for $\mathscr{E}^{(1)}$ and $\mathscr{E}^{(2)}$, respectively. Mechanism $\mathscr{M}_3$ publishes the result of both $\mathscr{M}_1$ and $\mathscr{M}_2$, i.e. $\mathscr{M}_3(D) = (\mathscr{M}_1(D), \mathscr{M}_2(D))$. For any set S of im $\mathscr{M}_3$, there is

$$\Pr[\mathscr{M}_3(D) \in S] = \sum_{(s_1,s_2)\in S} \Pr[\mathscr{M}_1(D) = s_1] \cdot \Pr[\mathscr{M}_2(D) = s_2]$$

Let $D \overset{j}{\sim} D'$ be an arbitrary pair of neighboring datasets. Applying the definition of PDP for both D and D' gives

$$\begin{aligned}\Pr[\mathscr{M}_3(D) \in S] &\leq \sum_{(s_1,s_2)\in S} \exp\left(\varepsilon_j^{(1)}\right) \Pr[\mathscr{M}_1(D') = s_1] \cdot \exp\left(\varepsilon_j^{(2)}\right) \Pr[\mathscr{M}_2(D') = s_2] \\ &= \exp\left(\varepsilon_j^{(1)} + \varepsilon_j^{(2)}\right) \sum_{(s_1,s_2)\in S} \Pr[\mathscr{M}_1(D') \in S] \cdot \Pr[\mathscr{M}_2(D') \in S] \\ &= \exp\left(\varepsilon_j^{(1)} + \varepsilon_j^{(2)}\right) \Pr[\mathscr{M}_3(D') \in S]\end{aligned}$$

for any set S of im $\mathscr{M}_3$. By the definition of PDP , $\mathscr{M}_3$ satisfies PDP for $\mathscr{E} = \mathscr{E}^{(1)} + \mathscr{E}^{(2)}$. □

(b) The subject of this proof is to demonstrate that for any $D \overset{j}{\sim} D'$ and any set S of im $\mathscr{S}$,

$$\Pr[\mathscr{S}(D) \in S] \leq \exp(\varepsilon_j) \Pr[\mathscr{S}(D') \in S].$$

Note that all of the possible outputs of the sampling procedure $SP(D)$ can be divided into those in which the j-th element is contained and in which the j-th element is not contained. Thus, $\Pr[\mathscr{S}(D) \in S]$ can be rewritten as

$$\begin{aligned}\Pr[\mathscr{S}(D) \in S] = \pi_t(\varepsilon_j) &\Pr\big[\mathscr{M}(SP(D)) \in S \mid D_j \in SP(D)\big] \\ &+\big(1 - \pi_t(\varepsilon_j)\big) \Pr\big[\mathscr{M}(SP(D)) \in S \mid D_j \notin SP(D)\big], \\ \Pr[\mathscr{S}(D') \in S] = \pi_t(\varepsilon_j) &\Pr\big[\mathscr{M}(SP(D')) \in S \mid D_j{}' \in SP(D')\big] \\ &+\big(1 - \pi_t(\varepsilon_j)\big) \Pr\big[\mathscr{M}(SP(D')) \in S \mid D_j{}' \notin SP(D')\big].\end{aligned}$$

Since $\mathscr{M}$ satisfies t-DP, there is

$$\Pr\big[\mathscr{M}(SP(D)) \in S \mid D_j \notin SP(D)\big] \leq \exp(t) \Pr\big[\mathscr{M}(SP(D')) \in S \mid D_j{}' \in SP(D')\big].$$

Thus,

$$\begin{aligned}\Pr[\mathscr{S}(D) \in S] \leq \exp(t)\pi_t(\varepsilon_j) &\Pr\big[\mathscr{M}(SP(D')) \in S \mid D_j{}' \in SP(D')\big] \\ &+\big(1 - \pi_t(\varepsilon_j)\big) \Pr\big[\mathscr{M}(SP(D')) \in S \mid D_j{}' \notin SP(D')\big].\end{aligned}$$

There are two cases:

- If $\varepsilon_j \geq t \Leftrightarrow \pi_t(\varepsilon_j) = 1$, there is

$$\Pr[\mathscr{S}(D) \in S] \leq \exp(t) \Pr[\mathscr{S}(D') \in S] \leq \exp(\varepsilon_j) \Pr[\mathscr{S}(D') \in S].$$

- If $\varepsilon_j < t \Leftrightarrow \pi_t(\varepsilon_j) = \frac{\exp(\varepsilon_j)-1}{\exp(t)-1}$, there is

$$\begin{aligned}\exp(t)\pi_t(\varepsilon_j) + 1 - \pi_t(\varepsilon_j) &= \frac{\exp(t+\varepsilon_j) - \exp(\varepsilon_j)}{\exp(t) - 1} = \exp(\varepsilon_j) \\ \Rightarrow \Pr[\mathscr{S}(D) \in S] &\leq \exp(\varepsilon_j) \Pr[\mathscr{S}(D') \in S].\end{aligned}$$

Thus, $\mathscr{S}$ satisfies $\mathscr{E}$-PDP.