9-)

According to the sequential composition, if we are given A_1, $A_2, A_3, A_4, \ldots, A_n$ as the algorithms and if each of these algorithms satisfy ε_j-DP for $0 < j \leq n$, then the combinations of the outputs of these algorithms satisfy ε-DP where the $\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \ldots + \varepsilon_n = \sum_{j=1}^{n} \varepsilon_j$ (from Lecture-06)

In this question, we are given $A_1, A_2, A_3, \ldots, A_n$ as n independent algorithms. We need to show that whether their sequential composition satisfies the following inequality for showing whether or not their composition satisfies ε-DP where $\varepsilon = \sum_{j=1}^{n} \varepsilon_j$: $\sum_{j=1}^{n} \varepsilon_j = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \ldots + \varepsilon_n = \varepsilon$

$A \rightarrow$ randomized algorithm
$D \rightarrow$ original dataset
$D' \rightarrow$ neighboring dataset
$O \rightarrow$ any output of A

$$\frac{Pr[A(D)=O]}{Pr[A(D')=O]} \leq e^{\varepsilon} \text{ (need to be shown)}$$

Since each of $A_1, A_2, A_3, \ldots, A_n$ satisfy ε_j-DP where $1 \leq j \leq n$, we can write following inequalities:

$$\frac{Pr[A_1(D)=O_1]}{Pr[A_1(D')=O_1]} \leq e^{\varepsilon_1}$$

$$\frac{Pr[A_2(D)=O_2]}{Pr[A_2(D')=O_2]} \leq e^{\varepsilon_2}$$

$$\frac{Pr[A_3(D)=O_3]}{Pr[A_3(D')=O_3]} \leq e^{\varepsilon_3}$$

$$\vdots$$

$$\frac{Pr[A_n(D)=O_n]}{Pr[A_n(D')=O_n]} \leq e^{\varepsilon_n}$$

$\Rightarrow$ Let's multiply those side-by-side:

$$\frac{Pr[A_1(D)=O_1]}{Pr[A_1(D')=O_1]} \cdot \frac{Pr[A_2(D)=O_2]}{Pr[A_2(D')=O_2]} \cdots \leq e^{\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_n}$$

$$\Rightarrow \frac{Pr[A_1(D)=O_1]}{Pr[A_1(D')=O_1]} \cdot \frac{Pr[A_2(D)=O_2]}{Pr[A_2(D')=O_2]} \cdots \leq e^{\varepsilon}$$

If X and Y are independent events or algorithms, then the following equality should hold:

$$P(X \cap Y) = P(X) \cdot P(Y)$$

For n algorithms, this formula becomes:

$$P(K_1 \cap K_2 \cap K_3 \cap \ldots K_n) = P(K_1) \cdot P(K_2) \cdots P(K_n)$$

Note: $K_1, K_2, K_3, K_4, \ldots, K_n$ are independent algorithms.

$$\Rightarrow \frac{Pr[A_1(D)=O_1]}{Pr[A_1(D')=O_1]} \cdot \frac{Pr[A_2(D)=O_2]}{Pr[A_2(D')=O_2]} \cdots\cdots \cdot \frac{Pr[A_n(D)=O_n]}{Pr[A_n(D')=O_n]} \leq e^{\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n}$$

$$\Rightarrow \varepsilon_1+\varepsilon_2+\varepsilon_3+\cdots+\varepsilon_n=\varepsilon=\sum_{j=1}^{n}\varepsilon_j$$

$$\Rightarrow \frac{Pr[A_1(D)=O_1]}{Pr[A_1(D')=O_1]} \cdot \frac{Pr[A_2(D)=O_2]}{Pr[A_2(D')=O_2]} \cdots\cdots \cdot \frac{Pr[A_n(D)=O_n]}{Pr[A_n(D')=O_n]} \leq e^{\varepsilon}$$

$$\Rightarrow \frac{(Pr[A_1(D)=O_1] \cdot Pr[A_2(D)=O_2] \cdots\cdots \cdot Pr[A_n(D)=O_n])}{(Pr[A_1(D')=O_1] \cdot Pr[A_2(D')=O_2] \cdots\cdots \cdot Pr[A_n(D')=O_n])} \leq e^{\varepsilon}$$

Since $A_1, A_2, A_3, \ldots, A_n$ are independent, we can apply the following formula to numerator and denumerator:

$$P(X_1) \cdot P(X_2) \cdot P(X_3) \cdots\cdots P(X_n) = P(X_1 \cap X_2 \cap X_3 \ldots \cap X_n)$$

Note: $X_1, X_2, \ldots, X_n$ are independent algorithms here.

If we apply this formula to numerator and denominator, we get the following:

$$\frac{Pr\left[(A_1(D)=O_1) \cap (A_2(D)=O_2) \cap (A_3(D)=O_3) \cdots\cdots \cap (A_n(D)=O_n)\right]}{Pr\left[(A_1(D')=O_1) \cap (A_2(D')=O_2) \cap (A_3(D')=O_3) \cdots\cdots \cap (A_n(D')=O_n)\right]} \leq e^{\varepsilon}$$

$\Rightarrow$ We can see in the numerator of the left-hand side of above inequality that the individual outputs $O_1, O_2, O_3, \ldots, O_n$ of the independent algorithms $A_1, A_2, A_3, \ldots, A_n$ which act on the original dataset D are combined. However; for the denominator, the individual outputs $O_1, O_2, O_3, \ldots, O_n$ of the independent algorithms $A_1, A_2, \ldots, A_n$ which act on the neighboring dataset D' are combined. Since $A_1, A_2, A_3, \ldots, A_n$ are independent algorithms, the combination of the individual outputs of $A_1, A_2, A_3, A_4, \ldots\ldots, A_n$ has taken by using the intersection symbol ($\cap$). We can represent this process of combining the outputs with an algorithm named S which includes at least n different variables and gives the accumulated version of the individual outputs $O_1, O_2, \ldots\ldots, O_n$.

⇒ Therefore, we can write the following:

Let O be $(O_1 \cup O_2 \cup O_3 \cup \dots \cup O_n)$

$$\Rightarrow \frac{Pr[(A_1(D)=O_1) \cap (A_2(D)=O_2) \cap \dots (A_n(D)=O_n)]}{Pr[(A_1(D')=O_1) \cap (A_2(D')=O_2) \cap \dots (A_n(D')=O_n)]} \leq e^{\varepsilon}$$

$$\Rightarrow \frac{Pr[S(D) = (O_1 \cup O_2 \cup \dots \cup O_n)]}{Pr[S(D') = (O_1 \cup O_2 \cup \dots \cup O_n)]} \leq e^{\varepsilon}$$

$O = (O_1 \cup O_2 \dots \cup O_n)$. So, plug O to $(O_1 \cup O_2 \dots \cup O_n)$.

$$\Rightarrow \frac{Pr[S(D)=O]}{Pr[S(D')=O]} \leq e^{\varepsilon}$$

This inequality is same with the one that we should prove in order to prove ε-DP. Therefore, we can say that this version of sequential composition satisfies ε-DP where ε is equal to $\sum_{i=1}^{n} \varepsilon_i$.

b-) Let the number of records in the dataset D be $\|D\|$

⇒ We are given an algorithm A. If $\|D\|$ is bigger than e^{ε}, then A prints "large" as output. If $\|D\|$ is smaller than or equal to e^{ε}, then A prints "small" as output.

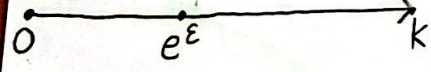
if $\|D\| > e^{\varepsilon} \Rightarrow$ "large"

else if $\|D\| \leq e^{\varepsilon} \Rightarrow$ "small"

Note: While checking whether the algorithm A is ε-DP or not, I have picked "small" as an output O of the algorithm A.

In order to show whether or not this algorithm satisfies ε-DP, we need to show whether or not the following inequality satisfies:

If D is the original dataset and D' is the neigboring dataset, then $\frac{Pr[A(D)=O]}{Pr[A(D')=O]} \leq e^{\varepsilon}$ where A is a randomized algoritm and O is any output of A. Let's represent the maximum possible number of records in dataset D with k.



for $[0, e^{\varepsilon}]$, $\|D\| \leq e^{\varepsilon}$

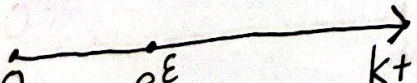
for $(e^{\varepsilon}, k]$, $\|D\| > e^{\varepsilon}$

Therefore; $Pr[A(D) = \text{"small"}] = \frac{(e^{\varepsilon}-0)}{(k-0)} = \frac{e^{\varepsilon}}{k}$

Let's define the neighbouring dataset with the addition or removal of one row to dataset. Then, the sensitivity S(q) is equal to 1.

⇒ Sensitivity = S(q) = 1.

If we define D' with one row addition:



$\Rightarrow$ for $[0, e^{\varepsilon}] \Rightarrow \|D\| \leq e^{\varepsilon}$

for $(e^{\varepsilon}, k+1] \Rightarrow \|D\| > e^{\varepsilon}$

Therefore; $Pr[A(D') = \text{"small"}] = \frac{e^{\varepsilon}}{k+1}$

⇒ Since the value of k will approach (be near to) to ∞, we can send k to ∞ in the probability calculations.

Continuation of b-)

$Pr[A(D) = \text{"small"}] = \frac{e^{\varepsilon}}{k}$

$Pr[A(D') = \text{"small"}] = \frac{e^{\varepsilon}}{k+1}$

} If D' is defined with one row addition

$$\Rightarrow \frac{Pr[A(D) = \text{"small"}]}{Pr[A(D') = \text{"small"}]} = \lim_{k\to\infty} = \left[\frac{(e^{\varepsilon}/k)}{(e^{\varepsilon}/(k+1))}\right] = \lim_{k\to\infty}\left[\frac{e^{\varepsilon}}{k} \cdot \frac{k+1}{e^{\varepsilon}}\right] = \underbrace{\lim_{k\to\infty}\left[\frac{e^{\varepsilon}}{e^{\varepsilon}}\right]}_{1} \cdot \lim_{k\to\infty}\left[\frac{k+1}{k}\right]$$

$\frac{(k+1)}{k}$

$$\Rightarrow \lim_{k\to\infty}\left[\frac{(k+1)}{k}\right] = \lim_{k\to\infty}\left[\frac{k\cdot(1+\frac{1}{k})}{k}\right] = \lim_{k\to\infty}\left[\frac{k}{k}\right] \cdot \lim_{k\to\infty}\left[1+\frac{1}{k}\right] =$$

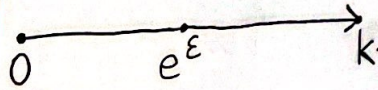
$$\Rightarrow 1 \cdot \lim_{k\to\infty}\left[1+\frac{1}{k}\right] = \lim_{k\to\infty}\left[1+\frac{1}{k}\right] = \lim_{k\to\infty}[1] + \lim_{k\to\infty}\left[\frac{1}{k}\right] = 1+0=1 \overset{?}{\hookrightarrow} (1 \leq e^{\varepsilon})$$

$\varepsilon \geq 0$ (By definition of ε), $e > 0$. So, e^{ε} is trivially at least equal to 1. In other words, $1 \leq e^{\varepsilon}$ holds for D' defined by adding one row to the dataset D.

⇒ Since $1 \leq e^{\varepsilon}$ holds, we can say that this algorithm is ε differentially private (ε-DP) for D' defined by adding one row to the dataset D.

we should check whether $1 \leq e^{\varepsilon}$ holds!

If we define D' with one row removal: → Sensitivity = $S(q) = 1$



for $[0, e^{\varepsilon}]$, $\|D\| \leq e^{\varepsilon}$

for $(e^{\varepsilon}, k-1]$, $\|D\| > e^{\varepsilon}$

Therefore; $Pr[A(D') = \text{"small"}] = \frac{(e^{\varepsilon}-0)}{(k-1-0)} = \frac{e^{\varepsilon}}{k-1}$

⇒ Since the value of k will approach to (be near to) ∞ infinity, we can send k to ∞ in probability calculations.

$$\Rightarrow \frac{Pr[A(D) = \text{"small"}]}{Pr[A(D') = \text{"small"}]} = \lim_{k\to\infty}\left[\frac{(e^{\varepsilon}/k)}{(e^{\varepsilon}/(k-1))}\right] = \lim_{k\to\infty}\left[\frac{e^{\varepsilon}}{k} \cdot \frac{k-1}{e^{\varepsilon}}\right]$$

$$\Rightarrow \lim_{k\to\infty}\left[\frac{e^{\varepsilon}}{e^{\varepsilon}}\right] \cdot \lim_{k\to\infty}\left[\frac{k-1}{k}\right] = 1 \cdot \lim_{k\to\infty}\left[\frac{(k-1)}{k}\right] = \lim_{k\to\infty}\left[\frac{(k-1)}{k}\right]$$

Continuation of b-)

$$\frac{Pr[A(D)="small"]}{Pr[A(D')="small"]} = \lim_{k\to\infty}\left[\frac{k-1}{k}\right] = \lim_{k\to\infty}\left[\frac{k\cdot(1-\frac{1}{k})}{k}\right] =$$

$$\Rightarrow \lim_{k\to\infty}\left[\frac{k}{k}\right]\cdot\lim_{k\to\infty}\left[(1-\frac{1}{k})\right] = 1\cdot\lim_{k\to\infty}\left[(1-\frac{1}{k})\right] =$$

$$\Rightarrow \lim_{k\to\infty}\left[(1-\frac{1}{k})\right] = \lim_{k\to\infty}[1] - \lim_{k\to\infty}\left[\frac{1}{k}\right] = 1-0 = 1$$

$$\frac{Pr[A(D)="small"]}{Pr[A(D')="small]} = 1 \overset{?}{\leq} e^{\varepsilon}$$ (We should check whether $1 \leq e^{\varepsilon}$ holds!)

$\varepsilon \geq 0$ (By definition of epsilon), $e > 0 \Rightarrow e^{\varepsilon} \geq 1$

Therefore, A satisfies ϵ-DP for D' defined by removal of one row. (Since we found $1 \leq e^{\varepsilon}$ at the end, A satisfies ϵ-DP also for D' defined by removal of one row)

Note-1: Since we removed one row in removal case, maximum possible number of record spaces decreased and become k-1. Since we added one row in the row addition case, maximum possible number of record spaces increased and become k+1.

Finally, since A satisfies ϵ-DP for both definitions of D', we can say A satisfies ϵ-DP.

The definitions of D' → By removing one row from D
The definitions of D' → By adding one row to D

⇒ Note-2: All of (lines) I have drawn represent the possible value ranges for (the number of records in the dataset D. → such as 0 → 5.

c-)

General formula of the probability density function (PDF) of the laplace distribution:

$$f(x|\mu, b) = \frac{1}{(2.b)} \cdot \exp\left(-\frac{|x-\mu|}{b}\right)$$

In this question, the mean (μ) is given as 0 and the scale (b) is given as ε. When we plug these values, we get:

$$\Rightarrow f(x|\mu, \varepsilon) = \frac{1}{(2.\varepsilon)} \cdot \exp\left(-\frac{|x-0|}{\varepsilon}\right) = \frac{1}{(2.\varepsilon)} \cdot \exp\left(-\frac{|x|}{\varepsilon}\right)$$

In order to prove ε-DP property, we should show that the below inequality holds:

D = Original Dataset
D' = Neighbouring Dataset
O = Any output of A

$$\frac{Pr[A(D)=O]}{Pr[A(D')=O]} \leq e^{\varepsilon}$$

$$\Rightarrow \frac{Pr[A(D)=O]}{Pr[A(D')=O]} = \frac{Pr[q(D)+r=O]}{Pr[q(D')+z=O]} = \frac{Pr[r=O-q(D)]}{Pr[z=O-q(D')]}$$

$$\Rightarrow Pr[z=O-q(D')] = \frac{1}{2.\varepsilon} \cdot e^{\frac{-|O-q(D')|}{\varepsilon}} \quad (*)$$

$$\Rightarrow Pr[r=O-q(D)] = \frac{1}{2.\varepsilon} \cdot e^{\frac{-|O-q(D)|}{\varepsilon}} \quad (**)$$

Find the ratio of $\frac{(**)}{(*)}$

$$\Rightarrow \frac{Pr[r=O-q(D)]}{Pr[z=O-q(D')]} = \frac{\left(\frac{1}{2.\varepsilon}\right) \cdot e^{\frac{-|O-q(D)|}{\varepsilon}}}{\left(\frac{1}{2.\varepsilon}\right) \cdot e^{\frac{-|O-q(D')|}{\varepsilon}}} = \frac{e^{\frac{-|O-q(D)|}{\varepsilon}}}{e^{\frac{-|O-q(D')|}{\varepsilon}}}$$

$$\Rightarrow e^{\frac{-|O-q(D)| + |O-q(D')|}{\varepsilon}}$$

$$\Rightarrow e^{\frac{(|O-q(D')| - |O-q(D)|)}{\varepsilon}}$$

Reversed Triangle Inequality
↳ $|c|-|d| \leq |c-d|$

let $c = O-q(D')$ and $d = O-q(D)$. Then, $c-d = (O-q(D')) - (O-q(D))$

$\Rightarrow c-d = O-q(D')-O+q(D) = q(D)-q(D')$

$O-q(D)$

$$\Rightarrow e^{\frac{(|0-q(D')|)-(|0-q(D)|)}{\varepsilon}} \leq e^{\frac{|q(D)-q(D')|}{\varepsilon}}$$ } From reverse triangle inequality

$\Rightarrow S(q) = |q(D)-q(D')|$

$\Rightarrow$ Scale parameter $= b = \frac{S(q)}{\varepsilon}$

$\Rightarrow$ In this question, the value of b parameter is given as ε.

$$\Rightarrow \frac{Pr[r=0-q(D)]}{Pr[z=0-q(D')]} \leq e^{\frac{S(q)}{\varepsilon}}$$

$b = \frac{S(q)}{\varepsilon}$, Since the value of b is given as ε in the question, $b = \varepsilon$.

$\varepsilon = \frac{S(q)}{\varepsilon} \Rightarrow S(q) = \varepsilon^2$

$\frac{\varepsilon^2}{\varepsilon} = \frac{\varepsilon^2}{\varepsilon^1} = \varepsilon^{2-1} = \varepsilon^1 = \varepsilon$

$$\Rightarrow \frac{Pr[r=0-q(D)]}{Pr[z=0-q(D')]} \leq e^{\frac{\varepsilon^2}{\varepsilon}} \Rightarrow \frac{Pr[r=0-q(D)]}{Pr[z=0-q(D')]} \leq e^{\varepsilon}$$

$$\Rightarrow \frac{Pr[q(D)+r=0]}{Pr[q(D')+z=0]} \leq e^{\varepsilon}$$

Note: r and z are different noise values which are added to q(D) and q(D') respectively.

$A(D) = q(D) + r$
$A(D') = q(D') + z$ } $\Rightarrow$ $\frac{Pr[A(D)=0]}{Pr[A(D')=0]} \leq e^{\varepsilon}$ ✓

This inequality is same as the inequality which we are supposed to prove. Therefore, we can say that the algorithm A satisfies ε-DP.