Part 1 Privacy Proofs

Question A

$$\frac{Pr[A_1(D)=o]}{Pr[A_1(D')=o]}, \quad \frac{Pr[A_2(D)=o]}{Pr[A_2(D')=o]} \quad \ldots \quad \frac{Pr[A_n(D)=o]}{Pr[A_n(D')=o]}$$

The n independent A algorithm's sequential composition satisfy $(\sum_{i=1}^{n} \varepsilon_i)$-DP
Their independent sequential composition kind a like parallel composition. Difference is execution time and they are not using disjoint datasets. Their sequential composition satisfy $\max(\varepsilon_i)$-DP. But this maximum epsilon lower than $(\sum_{i=1}^{n} \varepsilon_i)$-DP so that's why from the DP formula their sequential composition also satisfies $(\sum_{i=1}^{n} \varepsilon_i)$-DP.

$$\boxed{\frac{Pr[A_1(D)=o]}{Pr[A_1(D')=o]} + \frac{Pr[A_2(D)=o]}{Pr[A_2(D')=o]} + \ldots} \leq \max(\varepsilon_i)\text{-DP} \leq (\sum_{i=1}^{n} \varepsilon_i)\text{-DP}$$

Question B

Let number of records in D be $e^{\varepsilon}-1$ then, let the number of records in neighbor D' be $e^{\varepsilon}+1$!

- From the formula, these algorithms should give same output on both D, D'

$$\frac{Pr[A(D)=o]}{Pr[A(D')=o]} \leq e^{\varepsilon} \quad \text{output}$$

- With our assumed D and D' in the begining, it doesn't give the same output

$$\frac{Pr[A(D)=o]}{Pr[A(D')=o]} \leq e^{\varepsilon} \Rightarrow \frac{Pr[A(D)=\text{"small"}]}{Pr[A(D')=\text{"small"}]} = \frac{1}{0} \quad \text{or}$$

$$\frac{Pr[A(D)=\text{"large"}]}{Pr[A(D')=\text{"large"}]} = \frac{0}{1}$$

A satisfy ε-DP if the number of records in dataset D and number of records in Dataset D' should be both lower than e^{ε} or greater than e^{ε}

Question C

$$\frac{Pr[q(D)+r=o]}{Pr[q(D')+r'=o]} \rightarrow \frac{Pr[r=o-q(D)]}{Pr[r'=o-q(D')]} \rightarrow \frac{1}{2b} * e^{-\frac{|o-q(D')|}{b}}$$

$$\frac{\frac{1}{2\varepsilon} * e^{-\frac{|o-q(D)|}{b}}}{\frac{1}{2\varepsilon} * e^{-\frac{|o-q(D')|}{b}}} = e^{-\frac{|o-q(D)|}{\varepsilon} + \frac{|o-q(D')|}{\varepsilon}} = e^{\frac{\overbrace{|o-q(D')|}^{a} - \overbrace{|o-q(D)|}^{b}}{\varepsilon}}$$

$|a| - |b| \leq |a-b|$

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

A satisfy ε-DP if the sensitivity [S(q)] is equals to ε^2. In other cases, it does not satisfy the ε-DP