Quiz 2

Name and KAUST ID

November 14, 2022

1. Consider the following statements. Judge whether each of them is true or false. You dont need to explain the reason.

   - For (ϵ, δ)-DP algorithms, the privacy budget δ must satisfy $\delta \ll \frac{1}{n}$. Equivalently, there is an $(\epsilon = 0, \delta)$-DP algorithm such that if $\delta \gg \frac{1}{n}$ then with high probability its output will reveal individuals information.
   - Consider the following the statement:
     For a mechanism $A : \mathcal{X}^n \mapsto \mathcal{Y}$, a pair of neighboring data $D \sim D'$, defines the sets

     $$\text{Good} = \{y \in \mathcal{Y} : \frac{\mathbb{P}(A(D) = y)}{\mathbb{P}(A(D') = y} \leq e^{\epsilon}\}, \text{Bad} = \mathcal{Y} - \text{Good}. \tag{1}$$

     Then A is (ϵ, δ)-DP if and only if $\mathbb{P}(A(D) \in \text{Bad}) \leq \delta$ for every pair of neighboring datasets. Note that is $A(D)$ and $A(D')$ are continuous distributions then we just replace the probability to the probability density functions.
   - For a given privacy budget ϵ, the error of Laplacian mechanism to achieve ϵ-DP is always smaller than the error of Gaussian mechanism to achieve $(\epsilon, \delta = \frac{1}{n})$-DP.
   - We know that Differential privacy has the subsampling property. However, different subsampling approaches may lead different level of privacy guarantees.
   - Like the approximate (or (ϵ, δ)) DP, Rényi-DP also has a similar form the advanced composition theorem.