Quiz 1

Name and KAUST ID

November 14, 2022

1. Consider the following statements. Judge whether each of them is true or false. You don't need to explain the reason.

   - Consider the Generalized Random Response (Algorithm 1). Each Y_i is a unbiased estimator of $\phi(x_i)$.

Algorithm 1 Generalized Random Response

Require: Dataset $D = \{x_1, \cdots, x_n\}$, predicate $\phi : \mathcal{X} \mapsto \{0, 1\}$ and parameter $\epsilon > 0$
Ensure: Bits $(Y_1, \cdots, Y_n)$
1: **for** $i = 1, \cdots, n$ **do**
2: Let $Y_i = \phi(x_i)$ w.p $\frac{e^\epsilon}{e^\epsilon+1}$ and $Y_i = 1 - \phi(x_i)$ otherwise.
3: **end for**

   - Consider the following definition: A randomized algorithm M is is called ϵ-differentially private (DP) if for all neighboring datasets D, D' and every particular output s in the output space (if the output space is discrete) we have $\mathbb{P}(A(D) = s) \leq e^\epsilon \mathbb{P}(A(D') = s)$.

     The previous definition is equivalent to the original definition of ϵ-DP (if the output space is discrete).
   - In the definition of ϵ-DP, in practice ϵ could be an extremely small number such as $1/2^{10}$.
   - The definition of the ℓ_1-norm global sensitivity must be the maximum $\|f(D) - f(D')\|_1$ for all the pairs of neighboring datasets $D \sim D'$.
   - The exponential mechanism could be not well defined. For example, when the possible outputs is infinite.