AMMI Privacy and Fairness Course, Rwanda, May 2019
Assignment 1

Answer three out of the following four questions.
Please turn in by Noon on Thursday, May 14.

1a. Prove that the following two definitions of $(\epsilon, 0)$-DP are the same.

- For every two neighboring databases x, y and for each element $r \in R$, $Pr[M(x) = r] \leq e^{\epsilon} Pr[M(y) = r]$.
- For every two neighboring databases x, y, and for every subset $S \subseteq R$, $Pr[M(x) \in S] \leq e^{\epsilon} Pr[M(y) \in S]$.

1b. What happens in the case of (ϵ, δ)-DP?

2. Prove that if $M_1, ..., M_k$ are (ϵ, δ)-DP mechanisms, then any convex combination is also a (ϵ, δ)-DP mechanism. (A convex combination is defined by a distribution p over $\{1, \ldots, k\}$. The convex combination mechanism first picks $i \in [k]$ according to p, and then runs mechanism M_i on x.)

3. Prove that any mechanism M that is deterministic is not differentially private.

4a. (Group Privacy.) Let M be a mechanism mapping $\mathbb{N}^{|X|}$ to R, Prove that any $(\epsilon, 0)$-DP mechanism M is $(k\epsilon, 0)$-DP for groups of size k i.e. for all x, y such that $||x - y||_1 \leq k$, $Pr[M(x) \in S] \leq e^{\epsilon k} Pr[M(y) \in S]$.

4b Prove the following approximate group privacy property. Any (ϵ, δ)-DP mechanism M is $(k\epsilon, k \cdot e^{k \cdot \epsilon} \cdot \delta)$-DP for groups of size k. Note that both ϵ and δ are nonnegative.