Assignment 4
CS260B: Algorithmic Machine Learning, Spring 2021
Due: May 25, 10PM

Guidelines for submitting the solutions:

- The assignments need to be submitted on Gradescope. Make sure you follow all the instructions - they are simple enough that exceptions will not be accepted.
- Start each problem or sub-problem on a separate page even if it means having a lot of white-space and write/type in large font.
- The solutions need to be submitted by 10 PM on the due date. No late submissions will be accepted.
- Please adhere to the code of conduct outlined on the class page.

1. Consider the following alternative to potentially achieve ϵ-differential privacy for releasing the mean of a database $X \in \{0,1\}^n$. So we have n users each with one attribute and we want to release the count of users with this attribute so $f(X) = \sum_i X_i$. As studied in class, this query has $S_1(f) = 1$ so we can use Laplacian noise. But what if instead of Laplacian noise we consider the following strategy for achieving privacy: 1. Sample a uniform real-value in the interval $[-C/\epsilon, C/\epsilon]$ (for some constant C). 2. Release $f(X) + Z$.

   Is the above mechanism ϵ-differentially private? (For some fixed constant C.) [4 points]

   Solution The scheme will not be differentially private. As an example, consider a case where $f(X) = N$ and we have a neighboring database X' with sum $f(X') = N - 1$. Now, the distribution of $M(X)$ is uniform in the interval $[N - C/\epsilon, N + C/\epsilon]$ whereas $M(X')$ is uniform in the interval $[N-1-C/\epsilon, N-1+C/\epsilon]$. So in particular, $Pr[M(X) \in [N-1+C/\epsilon, N+C/\epsilon]] \neq 0$, whereas the same probability for X', $Pr[M(X') \in [N-1+C/\epsilon, N+C/\epsilon]] = 0$ which violates the definition of privacy.

2. In class we stated without proof that the exponential mechanism gets a reasonable guarantee for preserving the utility of the released id. In particular, we stated in class without proof that (using notation from class), if we use exponential mechanism for a utility function with sensitivity Δu,

$$Pr[u(X, M_E(X, u, R)) \leq OPT_u(X) - \frac{\Delta u}{\epsilon} \cdot (\ln |R| + t)] \leq e^{-t}.$$

Prove the above statement. [4 points]

[Hint: Try to reason that every item with as small utility as above is quite unlikely, and then use that the total number of items is at most $|R|$.]

Solution For brevity of notation, let $B = OPT_u(X) - \Delta u(\ln |R| + t)/\epsilon$. Let r^* be an item with $u(X, r^*) = OPT_u(X)$. Now, for any other item r, we have

$$Pr[M_E(X, u, R) = r] = \frac{exp(\epsilon u(X, r)/\Delta u)}{\sum_s exp(\epsilon u(X, s)/\Delta u)} \leq \frac{exp(\epsilon u(X, r)/\Delta u)}{exp(\epsilon u(X, r^*)/\Delta u)}$$
$$= \exp(\frac{\epsilon}{\Delta u}(u(X, r) - u(X, r^*))).$$

In particular, for any item r with $u(X, r) \leq B$, we have

$$Pr[M_E(X, u, R) = r] \leq \exp(-(\ln |R| + t)) = \frac{e^{-t}}{|R|}.$$

Therefore,

$$Pr[u(X, M_E(X, u, R)) \leq B] = \sum_{r:u(X,r)\leq B} Pr[M_E(X, u, R) = r] \leq \sum_{r:u(X,r)\leq B} \frac{e^{-t}}{|R|} \leq e^{-t}. \quad (1)$$

3. Suppose your database is the income numbers of n individuals. What scheme would you use to release the median income in the dataset to satisfy ϵ-differential privacy while achieving a good guarantee on error?

   Concretely, suppose the each persons income is an integer in $\{0, 1, 2, \ldots, N\}$. So the database $X \in [N]^n$ and the query we are trying to release privately is $Median(X)$. While this is not needed, if it helps for you, you can suppose that all incomes are distinct and that n is odd.

   - What is the sensitivity of this query as a function of N? [2 points]

     Solution The sensitivity could be very high. Let $n = 2k+1$ Consider a scenario where X has the first $\lfloor n/2 \rfloor$ incomes are $0, 1, 2, \ldots, \lfloor k-1$, the next income is k, and the last k incomes are $N-k+1, N-k+2, \ldots, N$. In this case, $Median(X) = k$. However, if we consider a neighboring database X' where the income of the $k+1$'st person changes to $N-k$, then the we would have $Median(X') = N-k$. So the sensitivity is at least $|Median(X) - Median(X')| = N - 2k$.

   - What would happen if you use Laplacian mechanism given this sensitivity bound? [2 points]

     Solution Given the above sensitivity, to maintain differential privacy with Laplacian mechanism, we would need to add noise at least $(N-2k)/\epsilon$ which would be very high.

   - Describe a *score function* or *utility function* for which the arg max would exactly be the median and one whose sensitivity (i.e., Δu as defined in class for utility) can be bounded independently of N, n. Note the remarkable gains you would get by now using exponential mechanism with this score function to release the median instead! [2 points]

Solution There are many choices for a score function. For an income r in the database, $u(X, r) = min(|$number of people with income at most $r|$,$|$number of people with income at least $r|)$.

The maximum utility is achieved by the median with a value of $\lfloor n/2 \rfloor + 1$.

The sensitivity of the above score function is at most 1 as changing one income can only change the counts by at most 1.

- Describe a *score function* for which the arg max would exactly be the 90'th percentile income level among the people in the database and one whose sensitivity is still independent of N, n. [2 points]

Solution Generalizing the above idea, you can take $u(X, r) = min(|$number of people with income at most $r|/9$,$|$number of people with income at least $r|)$.