# Lecture : Specialized Statistics : The Exponential Mechanism and Threshold Queries

In this lecture, we shall focus on the data analysis task of releasing a statistic that can be framed as the "maximizer" of a certain reward/utility function. Our objective is to argue that there exist $\epsilon$-DP mechanisms fine-tuned to this task, which incur small error.

Example : Consider an election that we wish to conduct for choosing the chairman of a political outfit. Clearly, the $N$ members of the political party do not desire their votes to be leaked to others. Call the database of votes $\underline{x} = (x_1, \ldots, x_N) \in [k]^N$ ; our objective is to release an $\epsilon$-DP estimate of $\arg\max_{i=1}^{k} \#\{j : x_j = i\} \triangleq f(\underline{x})$.

More generally, consider the following data release task:

There exists a dataset $\underline{x} \in \mathbb{D}_N$ and a collection $\mathcal{Y}$ of candidate "outputs".
The "goodness" of any output $y \in \mathcal{Y}$ w.r.t. the dataset $\underline{x}$ is measured via a "score" or "utility" function $q: \mathcal{Y} \times \mathbb{D}_N \to \mathbb{R}$.

Our objective is to release $\hat{y} \in \mathcal{Y}$ that is an estimate of $\underset{y \in \mathcal{Y}}{\arg\max}\ q(y, \underline{x})$, privately.

<u>Example</u>: In our previous example, $\mathcal{Y} = \{\text{candidates}\}$ and $q(\cdot,\cdot)$ is such that $q(y, \underline{x}) = \#\{j : x_j = y\}$.

<u>Def 1</u>: We let $\Delta_q \triangleq \sup_{y} \sup_{\underline{x} \sim \underline{x}'} |q(y, \underline{x}) - q(y, \underline{x}')|$ denote the sensitivity of $q$.

## <u>The Exponential Mechanism</u> (EM)

The EM simply returns

$$\hat{y} \sim P^{EM}_{\epsilon, \underline{x}},$$

where

$$P^{EM}_{\epsilon, \underline{x}}(y) = \frac{\exp\left(\frac{\epsilon}{2\Delta} \cdot q(y, \underline{x})\right)}{\sum_{y'} \exp\left(\frac{\epsilon}{2\Delta} \cdot q(y', \underline{x})\right)}, \text{ for } y \in \mathcal{Y}.$$

**Theorem 1** : The EM is $\epsilon$-DP.

**Proof** : Fix $\underline{x} \sim \underline{x}'$. We simply need to show that $\dfrac{P_{\epsilon,\underline{x}}(y)}{P_{\epsilon,\underline{x}'}(y)} \leq e^{\epsilon}$.

To this end, observe that
$$\frac{\exp\left(\frac{\epsilon}{2\Delta}\cdot q(y,\underline{x})\right)}{\exp\left(\frac{\epsilon}{2\Delta}\cdot q(y,\underline{x}')\right)} \leq \exp\left(\frac{\epsilon}{2\Delta}\cdot\Delta\right) = \exp(\epsilon/2).$$
[Why?]

Moreover, we have
$$\frac{\sum_{y'} \exp\left(\frac{\epsilon}{2\Delta}\cdot q(y',\underline{x}')\right)}{\sum_{y'} \exp\left(\frac{\epsilon}{2\Delta}\cdot q(y',\underline{x})\right)} \leq \sup_{y'}\left(\exp\left(\frac{\epsilon}{2\Delta}\cdot\left(q(y',\underline{x}) - q(y',\underline{x}')\right)\right)\right)$$
[Why?]
$$\leq \exp(\epsilon/2).$$

Putting these two observations together completes the proof. $\blacksquare$

Our next result bounds the utility of the EM.

HW: Argue that for our example above, we have $\Delta_q = 1$.

Let $q_{max}(\underline{x}) \triangleq \max_{y \in \mathcal{Y}} q(y, \underline{x})$.

<u>Theorem 2</u>: We have for <u>any $\underline{x} \in \mathbb{D}_N$</u> and any $t > 0$ that for $Y \sim p^{EM}_{\epsilon, \underline{x}}$,

$$\Pr\left[ q(Y, \underline{x}) < q_{max}(\underline{x}) - \frac{2\Delta}{\epsilon}(\ln|\mathcal{Y}| + t) \right] \leq e^{-t}.$$

<u>Proof</u>: Let $q_{max} \triangleq q_{max}(\underline{x})$ and $q(y) \triangleq q(y, \underline{x})$. We wish to show that the collection

$$B \triangleq \left\{ y \in \mathcal{Y} : q(y) < q_{max} - \frac{2\Delta}{\epsilon}(\ln|\mathcal{Y}| + t) \right\}$$

is s.t. $P(B) \leq e^{-t}$.

Let $y^* \in \mathcal{Y}$ be an element with $q(y^*) = q_{max}$. Then,

why?

$$P(B) \leq \frac{P(B)}{P(y^*)} = \frac{\sum_{y \in B} \exp\left(\frac{\epsilon}{2\Delta} \cdot q(y)\right)}{\exp\left(\frac{\epsilon}{2\Delta} \cdot q_{max}\right)} \leq \frac{|B| \cdot \exp\left(\frac{\epsilon}{2\Delta} q_{max} - \ln|\mathcal{Y}| - t\right)}{\exp\left(\frac{\epsilon}{2\Delta} \cdot q_{max}\right)}$$

$$= |B| \cdot \frac{1}{|\mathcal{Y}|} \cdot e^{-t} \leq e^{-t}.$$

why? ∎

<u>Remark</u>: For our specific example, one can add Laplace noise to each count $q(y, \underline{x}) \triangleq \#\{j : x_j = y\}$, i.e., one can compute

$$\hat{q}(y, \underline{x}) = q(y, \underline{x}) + \mathrm{Lap}(1/\epsilon)$$

and release $\arg\max_{y \in \mathcal{Y}} \hat{q}(y, \underline{x})$. Intuitively, it is likely that

$\max_{y \in \mathcal{Y}} \hat{q}(y, \underline{x})$ is "close"$_\epsilon$ to $q_{max}$, with error at most $O\left(\frac{\ln d}{\epsilon}\right)$.

This is a particular version of the "Report Noisy Max" (RNM) mechanism.

[Can you provide a heuristic explanation for this? Use the properties of the Laplace distribution we encountered earlier.]

However, there are other settings (such as releasing the optimal price of an item in a single-item auction) where natural extensions of the Laplace mechanism do not work, due to its property of producing continuous-valued outputs.

## Threshold Queries

We next move on to another important statistic for practical data analysis: the histogram of data samples. Clearly, such a "meta-statistic" allows for the computation of other statistics (e.g. mean, mode, higher moments) of interest. We assume that the data samples have been suitably quantized into finitely many "bins" or intervals.

The histogram is only one of several such meta-statistics, all of which can be computed from range/threshold queries.

Formally, consider a dataset $\underline{x} = (x_1, \cdots, x_N) \in [K]^N$. An interval query asks for the count

$$c_{ij} \triangleq \#\{t : i \le x_t \le j\},$$

for some $1 \le i \le j \le K$. A threshold query asks for $c_{1,j}$, for some $1 \le j \le K$ (this is also called a range query).

HW: Argue that the cumulative distribution function (CDF)

$$\underline{F} = \left( \frac{c_{1,j}}{N} : j \in [K] \right)$$

can be used to compute any given interval query.

In the next lecture, we shall focus on the $\epsilon$-DP release of CDFs and discuss an important mechanism — the binary tree mechanism — which yields far smaller $\ell_2$-errors compared to standard application of the Laplace mechanism.