Privacy in Statistics and Machine Learning — Spring 2023
In-class Exercises for Lecture 16 (Projection Mechanism)
March 23, 2023

Adam Smith (based on materials developed with Jonathan Ullman)

Problems with marked with an asterisk **(*)** *are more challenging or open-ended.*

1. (Exploring Projection) It's a little magical why the projection mechanism is able to take answers that are so noisy as to seemingly contain no information about the true answers, and somehow produce very accurate answers. Here is an example that we think demystifies it a bit.

   Suppose we have k copies of the exact same count query $f_1, \ldots, f_k$, so that $\mathbf{F} \in \{0,1\}^{k \times m}$ is a matrix whose rows are all the same. Suppose you compute noisy answers $\hat{\mathbf{a}} \in \mathbb{R}^k$ with the Gaussian mechanism and project into the set of feasible answers C.

   (a) What is the set of consistent answers C?

   (b) Given noisy answers $\hat{\mathbf{a}}$, what is the projection $\tilde{\mathbf{a}} = \Pi_C(\hat{\mathbf{a}})$?

   (c) What is the error of the noisy answers $\hat{\mathbf{a}}$, and the projected answers $\tilde{\mathbf{a}}$? Does it increase with k?

2. (Understanding the bounds) Suppose our data comes from the universe $\mathcal{U} = \{0,1\}^d$ and we are interested in releasing all *3-way marginal queries*—namely, for every triple of indices $i_1, i_2, i_3 \in [d]$, and for every three bits b_1, b_2, b_3, we want to estimate the fraction of records x in the data set with $x_{i_1} = b_1$ and $x_{i_2} = b_2$ and $x_{i_3} = b_3$.

   What are m and k here? What error bounds do we get for the regular Gaussian mechanism and the projection mechanism respectively?

   How do these answer change if we look at 1-way marginals, 2-way marginals, or 4-way marginals (instead of 3-way marginals)?

3. (Projection for Monotone Queries) This question explores the special case of the projection mechanism that arises from threshold queries over the domain $\mathcal{U} = \{1, \ldots, D\}$. Here there are $D-1$ non-trivial queries[1]

   (a) When $D = 3$, there are 2 non-trivial queries, and the feasible set is

   $$C = \left\{(a_1, a_2) \in \mathbb{R}^2 : 0 \le a_1 \le a_2 \le 1\right\}$$

   Write (or illustrate) the projection operation $\Pi_C(a_1, a_2)$ for this specific set C.

   (b) **(*)** Suppose the data happens to be such that all the entries of the true answer $a_1, ..., a_{D-1}$ are the same. Projecting a noisy version of this vector onto the set C in (1) will eliminate much of noise. How good a bound can you give on the ℓ_2 error after projection?

[1] The query $f_D(\mathbf{x}) = \#\{i : x_i \le D\}$ evaluates to 1 for every dataset.

(c) **(*)** For the general case, the feasible set has the form

$$C = \{(a_1, \ldots, a_{D-1}) : 0 \le a_1 \le \cdots \le a_{D-1} \le 1\} \tag{1}$$

Design an explicit polynomial time algorithm for computing projection into the set C (i.e. without relying on general linear programming as a tool).

[***Hints:*** (1) Dynamic programming! (2) It's a bit easier if we further require that all the projected answers are integer multiples of some discretization parameter $\gamma > 0$.]

4. (Bias and Variance) Unlike the Gaussian mechanism which is *unbiased*, meaning $\mathbb{E}(\hat{\mathbf{a}}) = \mathbf{a}$, the projection mechanism is not necessarily unbiased.

   (a) Consider the case of a single count query, for which the feasible set is just $C = \{a : 0 \le a \le 1\}$. Compute an upper bound on the bias $\mathbb{E}(\hat{a} - a)$ of the projection mechanism on any dataset. How does the bias compare to the standard deviation of the noise?

   (b) **(*)** For a single count query, show that *every* (ε, δ)-differentially private mechanism whose output is always in the range $[0, 1]$ must have bias $\Omega(1/\varepsilon n)$, at least when δ is sufficiently small.

5. (Projection as Maximum-Likelihood Estimation) A common paradigm in statistical estimation is *maximum-likelihood*. Here we are given a family of distributions $\{P_\theta\}_{\theta \in \Theta}$ and an observation y that is drawn from some distribution P_θ, and our goal is to estimate the hidden parameter θ. To do so, we're given an observation $y \sim P_\theta$ and we estimate

$$\tilde{\theta} = \arg\max_{\theta' \in \Theta} P_{\theta'}(y)$$

Show that the projection mechanism is an instance of maximum likelihood estimation. What is the family of distributions P_θ and what is $P_\theta(y)$?