STOR 390: HOMEWORK 7

Riley Harper

April 19, 2024

Abstract: This homework explores optimization methods in machine learning, specifically Gradient Descent (GD) and Stochastic Gradient Descent (SGD), and their fundamental differences, particularly in the context of the update step. Additionally, it delves into the FedAve algorithm, presenting a proof of equivalence between two of its formulations and offering an intuitive explanation of its federated learning approach. Lastly, it examines the harm principle's relevance to machine learning, questioning the agency of ML models and their potential to limit user autonomy through the unintended consequences of their application.

Question 1

Recall that in class we showed that for randomized response differential privacy based on a fair coin (that is a coin that lands heads up with probability 0.5), the estimated proportion of incriminating observations $\widehat{P}$ (in class this was the estimated proportion of students having actually cheated) was given by $\widehat{P} = 2\pi - \frac{1}{2}$ where π is the proportion of people answering affirmative to the incriminating question. I want you to generalize this result for a potentially biased coin. That is, for a differentially private mechanism that uses a coin landing heads up with probability $0 \leq \theta \leq 1$, find an estimate $\widehat{P}$ for the proportion of incriminating observations. This expression should be in terms of θ and π.

To generalize the result of the randomized response mechanism for a biased coin, we follow the methodology applied with a fair coin but adjust it to account for the bias in the coin flip probability.

Randomized Response Mechanism Setup:

1. **Options for Each Respondent:**

   - **Truthfully answer** the question (e.g., such as having not cheated).
   - **Lie** according to the outcome of a coin flip.

   For a biased coin:

   - Probability of flipping heads (θ) – the respondent lies.
   - Probability of flipping tails $(1 - \theta)$ – the respondent answers truthfully.

2. **If the coin comes up heads**, the respondent answers ”Yes” or ”No” irrespective of the truth and solely based on the result of the second coin flip.

3. **If the coin comes up tails**, the respondent answers truthfully.

Modeling Responses:

- Let π be the proportion of people who answer ”Yes” to the question.
- When asked the question under this mechanism,
  - The probability of a respondent saying ”Yes” because they are telling the truth (coin lands tails and they are in the truthful group): $(1 - \theta)\widehat{P}$.
  - The probability of a respondent saying ”Yes” because they are lying (coin lands heads twice): θ^2.

So, the total probability of receiving a ”Yes” response, denoted $\widehat{P}$, is given by the addition of the two outcomes: $\pi = \theta^2 + (1 - \theta)\widehat{P}$

Solving for π:

We want to express π in terms of P and θ. Rearranging the above equation: