IN-STK5000 Project 2 - Project 5

Anders Bredesen Hatlelid
Even Tronstad
Jacob Nicolai Arthur Sjødin
Torgeir Ladstein Waagbø

December 8, 2021

There is a lot of text, but I have stated to questions in red and tried to be specific

Two separate privacy questions

I interpret the privacy questions as two separate cases: One where you are asked to protect the identities of the people in the training set (just the storage of the data, without taking the experiment into account). It is this question we shall address when answering:

- Does the existence of this database raise any privacy concerns?
- Explain how you would protect the data of the people in the training set.

This we shall only describe, and not implement.

The second questions is how to can protect the people in the training set from being identified based on the published data in the report. This we shall address in the questions:

- If the database was secret, but your analysis public, how would that affect privacy?
- In particular, given that your policy and model are obtained from some 'training' data set, how would you guarantee that release or use, of the policy and model does not leak private information about the individual?
- Explain how you would protect the data of the people that obtained treatment?

- How would you then ensure that the private information of the treated individual is not leaked?

Q1: Have I somewhat understood the questions we shall answer?

Implementation of privacy

Based on the two type of questions, I interpret the point

- Implement a private decision making mechanism for (b)

as being asked to implement a privacy mechanism NOT to hide the individual in the database from being identifiable, but to make sure the individuals can not be identified based on our analysis, assuming the database to be secret in the first place.
Q2: Is this correct?

Privacy when using bandits

We have chosen to stick with the bandit model using Thompson sampling. We have three bandits, one for each vaccine. Thus we disregard the features, but we will address this limitation. (We considered changing the bandits to model the probability of death given comorbidities, but we stuck to vaccines as we find this model simple and we understand it.)

Here is my thoughts on how to use privacy using bandits: We add Laplace noise when updating the parameters for the bandits. If we use a Local privacy model we would get

$$\theta_i \sim \mathrm{Beta}(a_i, b_i) \quad i = 1, 2, 3$$

We choose the argmax and observe the reward r_i (whether or not we get a critical symptom). When we update the parameters we add the noise $\omega \sim$ Laplace. Or we could use a centralised privacy model we we batch the updates and add noise for each batch.
Q3: Is this a sufficient privacy mechanism? Or do we need to we also need to add noise to the observed symptom (response) when 'pulling' a bandit?
Q4: And if we need to add noise to the symptom, can we use randomized response?

The exponential mechanism

We have considered trying the exponential mechanism, but we find it hard to grasp.

In Dirk's lecture he had an example where he used the exponential mechanism to change the frequencies of the values in a 'education'-column. However, the definition in the book (3.4.6)

$$\pi(a|x) := \frac{e^{\epsilon U(q,a,x)/\mathbb{L}(U(q))}}{e^{\sum_{a'} \epsilon U(q,a',x)/\mathbb{L}(U(q))}}$$

defines the probability of a policy.

When answering the question:

- Estimate the amount of loss in utility as you change the privacy guarantee

my initial though was to add Laplace noise to the beta parameter updates, and then estimate the accumulated utility. This would probably be sub optimal and result in loss in utility.

Q5: If you think the exponential mechanism is a good idea, could you give us a hint on how we use it in the bandit setting?