University of Tartu
Institute of Computer Science
Cybersecurity Curriculum

Joosep Parts

Homework 5: Differential privacy

Privacy-preserving Technologies LTAT.04.007

Tartu 2023

Contents

1 Differential privacy of query Q1

```
SELECT COUNT(*) FROM votes
GROUP BY candidate;
```

Figure 1. Q1: The histogram of vote counts of all candidates.

1.1 Choosing the epsilon

1.1.1 What is the global sensitivity of the query Q1?

The global sensitivity of a query is the maximum possible change in the output of the query when a single entry in the dataset is changed. In the case of query Q1, it is a histogram of vote counts for all candidates. We will analyze the possible changes in the output when a single entry in the dataset is changed:

1. A citizen adds a vote for one candidate: In this case, the vote count of one candidate will increase by 1, and the vote count of another candidate remain the same.
2. A citizen changes their vote from one candidate to another: In this case, the vote count of one candidate will increase by 1, and the vote count of another candidate will decrease by 1.

In both cases, the maximum change in the output is 1. Therefore, the global sensitivity of the query Q1 is 1:

$$\Delta f(Q1) = 1 \tag{1}$$

1.1.2 Which epsilon should be taken so that the probability of getting the correct result is at least 0.9?

We are given that the probability of getting the correct result must be at least 0.9. We need to find the value of the noise scale parameter b for the Laplace distribution. Recall that for the Laplace distribution, the probability density function is given by:

$$f(x|\mu, b) = \frac{1}{2b} \exp\left(-\frac{|x-\mu|}{b}\right) \tag{2}$$

where μ is the location parameter and b is the scale parameter. We need to find b such that the probability of the noisy result being equal to the true result is at least 0.9. Since we are using the Laplace mechanism with rounding, we need to find the probability of

the noise being within $(-0.5, 0.5)$, which corresponds to rounding to the nearest integer. Since the Laplace distribution is symmetric [1, p. 294] around the location parameter, can find the scale parameter (b) that corresponds to the desired probability:

$$\int_{-0.5}^{0.5} f(x|0, b)dx \geq 0.9 \tag{3}$$

Since there are 3 candidates, we want the probability of getting the correct result for each candidate to be at least $\sqrt[3]{0.9}$, which is ≈ 0.9659.

$$\begin{aligned} P(|\text{noise}| \leq 0.5) &= 0.9659 \\ 1 - e^{-\frac{0.5}{b}} &= 0.48295 \\ e^{-\frac{0.5}{b}} &= 0.51705 \\ -\frac{0.5}{b} &= \ln(0.51705) \\ b &\approx 0.692 \end{aligned} \tag{4}$$

Now, we can find ε using the formula for the Laplace distribution's scale parameter:

$$\begin{aligned} b &= \frac{\Delta f}{\varepsilon} \\ \varepsilon &= \frac{\Delta f}{b} \\ \varepsilon &\approx \frac{1}{0.692} \\ \varepsilon &\approx 1.445 \end{aligned} \tag{5}$$

In this case, we should choose an ε value of approximately 1.445 to ensure the probability of getting the correct result for all candidates is at least 0.9. If I choose a larger ε, the noise added to the vote counts will be smaller, which makes the results more accurate but may also compromise privacy.

1.2 Dealing with negative counts

The post-processing theorem states that if a function is applied to the output of an ε-differentially private mechanism, the result is still ε-differentially private. "The post-processing property means that it's always safe to perform arbitrary computations on the

output of a differentially private mechanism - there's no danger of reversing the privacy protection the mechanism has provided" [2]. Lets evaluate each modifcation option:

1. Sampling only positive noise, i.e., from the interval $[0, \infty)$: This modifcation is not differentially private because it may make it easier to infer the original vote counts by observing the published results. For differential privacy, the noise should be sampled symmetrically around zero, so that it doesn't introduce bias in the results.

2. If the true vote count of some candidate is some value y, sample the noise from the interval $[-y, \infty)$: This modifcation does not maintain ε-differential privacy because it's dependent on the true vote count, which introduces a potential privacy breach. The noise should be sampled independently of the true vote count to ensure that the privacy guarantee is preserved.

3. If the noisy vote count of some candidate is negative, then re-sample the noise until the result becomes positive: This modifcation does not preserve ε-differential privacy either. Re-sampling the noise based on the output (noisy vote count) creates a potential for bias and compromises the privacy guarantee.

4. If the noisy vote count of some candidate is negative, then round this negative count up to 0: This modifcation is consistent with the post-processing theorem and maintains ε-differential privacy. Clipping the negative vote count to zero does not depend on the true vote count and does not introduce any bias in the results. It's a form of post-processing that does not compromise the privacy guarantee.

Therefore, option 4 is the only modifcation that keeps the system ε-differentially private with the same value of ε due to the post-processing theorem.

2 Differential privacy of query Q2

```
SELECT MAX(score) (
SELECT COUNT(*) AS score FROM votes
GROUP BY candidate
) ORDERED BY score DESC LIMIT 1;
```

Figure 2. Q2: The histogram of vote counts of all candidates.

2.1 Choosing the epsilon

Given the sensitivity $\Delta f = 1$ and the probability of selecting the true candidate $P(T) \geq 0.9$, we want to find the suitable ϵ value for the exponential mechanism [3]. We can write the inequality for the probability of selecting a different candidate $P(C)$:

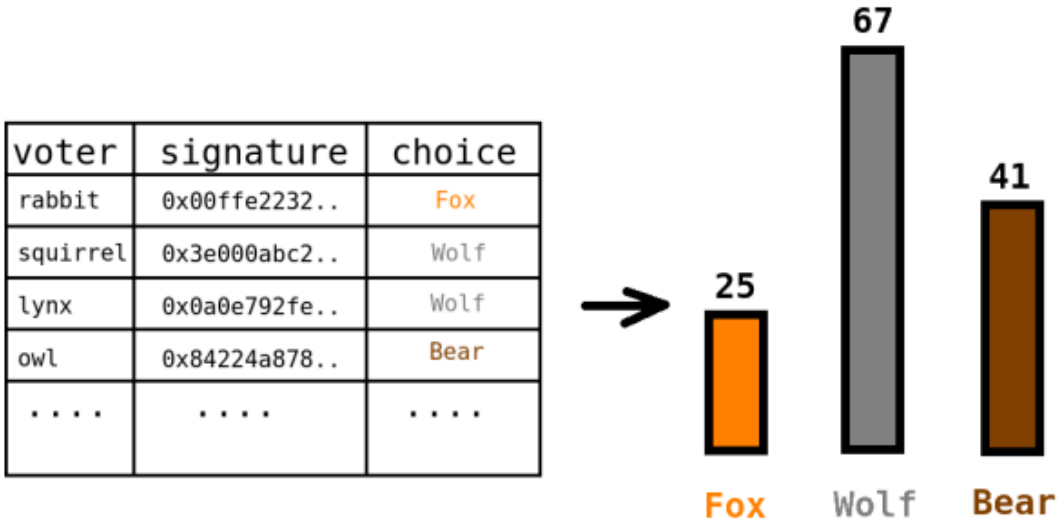

Figure 3. Example vote dataset (left) and the corresponding election result (right) taken from Differential Privacy Homework

$$P(C) \leq 0.1 \tag{6}$$

Assuming the worst-case scenario where the difference in score between the true candidate and the next highest candidate is 1, we can solve for ϵ:

$$\exp\left(\frac{\epsilon(-1)}{2}\right) \leq 0.1$$
$$\epsilon(-1) = 2\ln(0.1)$$
$$\epsilon \approx 4.605$$

Therefore, the programmer should choose $\epsilon \approx 4.605$ to ensure the probability of getting the correct result is at least 0.9.

Using the computed $\epsilon \approx 4.605$ and the dataset in Figure 3 of the provided example (Fox – 25, Wolf – 67 , Bear – 41), we can calculate the probability that the system will output the actual winner (Wolf) using the exponential mechanism. I use Z to ensure that the probabilities of all possible outcomes sum up to 1, so thhe probabilities for each candidate are given by:

$$P(\text{Fox}) = \frac{\exp\left(\frac{4.605(25-67)}{2}\right)}{Z}$$
$$P(\text{Wolf}) = \frac{\exp\left(\frac{4.605(67-67)}{2}\right)}{Z}$$
$$P(\text{Bear}) = \frac{\exp\left(\frac{4.605(41-67)}{2}\right)}{Z}$$

The normalization constant Z is $1.000000000000000000000000114400000101$ [4]:

$$Z = \exp\left(\frac{4.605(25-67)}{2}\right) + \exp\left(\frac{4.605(67-67)}{2}\right) + \exp\left(\frac{4.605(41-67)}{2}\right) \quad (7)$$

The probability of selecting the true winner (Wolf) is:

$$P(\text{Wolf}) = \frac{\exp\left(\frac{4.605(67-67)}{2}\right)}{Z} \approx 0.99997 \quad (8)$$

2.2 The goodness of epsilon

1. For the group of 10 rabbits (out of 25 votes for the Fox), we need to find the ϵ-DP that is actually guaranteed for the group of 10 rabbits such that the Fox won't find sensitive

information about the rabbits. Recall from above, we computed an $\epsilon \approx 4.605$ to ensure the probability of getting the correct result is at least 0.9. This means that the group of 10 rabbits is guaranteed ϵ-DP with $\epsilon \approx 4.605$. If we wanted to give the rabbits more privacy, we would need to increase the value of ϵ and increase the noise, but then we would fall short on the 0.9 probability of getting the correct result. So for now rabbits would have to accept their privacy being $\epsilon \approx 4.605$.

2. Let's consider the definition of ϵ-differential privacy [5, p. 3]:

$$\forall t, t' \in \mathcal{D}, \forall y \in \mathcal{R}, \frac{Pr[Mq(t) = y]}{Pr[Mq(t') = y]} \leq e^{\epsilon} \tag{9}$$

where t and t' are neighboring datasets, y is the output of the mechanism, and Mq is the exponential mechanism applied to the query.

We previously obtained $\epsilon \approx 4.605$. Now, we want to show that this value of ϵ does not give any privacy guarantees for at least one output $y \in Fox, Wolf, Bear$.

Consider the true dataset t and an arbitrary neighboring dataset t' that differ by one vote, such that the vote count for the true candidate (Wolf) is decreased by one, and the vote count for one of the other candidates (Fox or Bear) is increased by one.

Given this, the probabilities for each candidate in the true dataset t are:

$$P_t(\text{Fox}) = \frac{\exp\left(\frac{4.605(25-67)}{2}\right)}{Z_t} \quad P_t(\text{Wolf}) = \frac{\exp\left(\frac{4.605(67-67)}{2}\right)}{Z_t} \quad P_t(\text{Bear}) = \frac{\exp\left(\frac{4.605(41-67)}{2}\right)}{Z_t}$$

And the probabilities for each candidate in the neighboring dataset t' are:

$$P_{t'}(\text{Fox}) = \frac{\exp\left(\frac{4.605(26-66)}{2}\right)}{Z_{t'}} \quad P_{t'}(\text{Wolf}) = \frac{\exp\left(\frac{4.605(66-66)}{2}\right)}{Z_{t'}} \quad P_{t'}(\text{Bear}) = \frac{\exp\left(\frac{4.605(41-66)}{2}\right)}{Z_{t'}}$$

Check ϵ-DP condition for Fox. Since $0.00676 \leq e^{4.605}$, the condition is satisfied for $y = Fox$.

$$\frac{P_t(\text{Fox})}{P_{t'}(\text{Fox})} = \frac{\exp\left(\frac{4.605(25-67)}{2}\right)}{\exp\left(\frac{4.605(26-66)}{2}\right)} \approx 0.00676 \tag{10}$$

Check ϵ-DP condition for Wolf. Since $1 \leq e^{4.605}$, the condition is satisfied for $y = Wolf$.

$$\frac{P_t(\text{Wolf})}{P_{t'}(\text{Wolf})} = \frac{\exp\left(\frac{4.605(67-67)}{2}\right)}{\exp\left(\frac{4.605(66-66)}{2}\right)} = 1 \tag{11}$$

Check ϵ-DP condition for Bear. Since $7.389 > e^{4.605}$, the condition is not satisfied for $y = Bear$

$$\frac{P_t(\text{Bear})}{P_{t'}(\text{Bear})} = \frac{\exp\left(\frac{4.605(41-67)}{2}\right)}{\exp\left(\frac{4.605(41-66)}{2}\right)} \approx 7.389 \tag{12}$$

This means that the previously obtained $\epsilon \approx 4.605$ does not give privacy guarantees for the output $y = Bear$.

3. When I use 10 times smaller ϵ, which means that $\epsilon' = \frac{4.605}{10} \approx 0.4605$. Let's analyze affects of this change by computing new probailityes:

$$P_t(\text{Fox}) = \frac{\exp\left(\frac{0.4605(25-67)}{2}\right)}{Z'_t} \quad P_t(\text{Wolf}) \quad = \frac{\exp\left(\frac{0.4605(67-67)}{2}\right)}{Z'_t} \quad P_t(\text{Bear}) = \frac{\exp\left(\frac{0.4605(41-67)}{2}\right)}{Z'_t}$$

The new normalization constant is $Z'_t \approx 1.0025783$ [6]

$$Z'_t = \exp\left(\frac{0.4605(25-67)}{2}\right) + \exp\left(\frac{0.4605(67-67)}{2}\right) + \exp\left(\frac{0.4605(41-67)}{2}\right) \tag{13}$$

The new probability of selecting the true winner (Wolf) is:

$$P_t(\text{Wolf}) = \frac{\exp\left(\frac{0.4605(67-67)}{2}\right)}{Z'_t} \approx 0.824 \tag{14}$$

As we can see, the probability of getting the correct result (Wolf) is now approximately 0.824, which is lower than the previous probability (≈ 0.99997) obtained with $\epsilon \approx 4.605$. This reduction in accuracy is a trade-off for stronger privacy guarantees. Even though the accuracy has decreased, a probability of 0.824 for selecting the true winner can still be considered reasonable in my opinion.

4. I am not entierly sure if the programmer overreacted by taking a smaller ϵ. From $\epsilon \approx 4.605$ to 10x drop into $\epsilon \approx 0.4605$ in that sense is quite a big change relative to the original value. Even though I just concluded that change was reasonable... Reminder that Wolf had ≈ 0.824 change with the $\epsilon \approx 0.4605$, Fox had ≈ 0.090(not in formula) and Bear had ≈ 0.086(not in formula) respectivley, I think that the programmer should have taken a smaller steps to decide what would be the appropriate ϵ to stop at. Having a near $8 - 9\%$ chance to pick the wrong candidate(Fox or Bear) in the election might just be a bit too high of a chance in my opinion. Perhaps trying different levels of privacy budgets ϵ and seeing how the usefulness of the data vs. privacy changes in the output might give more insight into what ϵ level is appropriate.

3 Decision

As an election organizer I would choose Q2 using the exponential mechanism. The exponential mechanism is more siutable for finding the most popular candidate, which is the primary goal of the election organizer. For Q2, to achieve a probability of getting the correct result was for Wolf with $\epsilon \approx 4.605$ was ≈ 0.99997 chance (very high probability). But then again I also guess that's not very secure from a privacy perspective. And our programmers attempt to add more privacy by changing query Q2 to $\epsilon \approx 0.4605$ might have been also a bit overreaction.

As a voter (interested in privacy) I would choose Q1 using rounding mechanism. From a privacy perspective, Q1 using the Laplace mechanism with rounding could be a better choice. In this scenario, the global sensitivity of the query Q1 is 1, considering there are three candidates. To ensure the probability of getting the correct result at least 0.9 for each candidate we found that with $\varepsilon \approx 1.445$ it was ≈ 0.9659 chance of selecting the right candidate.

To conclude, it is essential to consider the trade-off between privacy and utility in both mechanisms. With Q2, there might be a higher chance of losing privacy. On the other hand, with Q1, there might be a higher chance of getting inaccurate results due to rounding. In either case, it's crucial to weigh the trade-offs between privacy and utility in both scenarios.

References

[1] "Laplace distribution," in *The Concise Encyclopedia of Statistics*. New York, NY: Springer New York, 2008, pp. 294–295, ISBN: 978-0-387-32833-1. DOI: 10.1007/978-0-387-32833-1_219. [Online]. Available: https://doi.org/10.1007/978-0-387-32833-1_219.

[2] *Programming differential privacy*. [Online]. Available: https://programming-dp.com/ch4.html#post-processing.

[3] *Programming differential privacy*. [Online]. Available: https://programming-dp.com/ch9%20.html#equation-274ce7f7-b2d6-46cc-85e4-34d24cc412b4.

[4] "The normalization constant Z." (), [Online]. Available: https://www.wolframalpha.com/input?i=%5Cexp%5Cleft%28%5Cfrac%7B4.605%2825+-+67%29%7D%7B2%7D%5Cright%29+%2B+%5Cexp%5Cleft%28%5Cfrac%7B4.605%2867+-+67%29%7D%7B2%7D%5Cright%29+%2B+%5Cexp%5Cleft%28%5Cfrac%7B4.605%2841+-+67%29%7D%7B2%7D%5Cright%29 (visited on 2023-04-22).

[5] M. Aitsam, "Differential privacy made easy," in *2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)*, 2022, pp. 1–7. DOI: 10.1109/ETECTE55893.2022.10007322.

[6] "The normalization constant Z'." (), [Online]. Available: https://www.wolframalpha.com/input?i=%5Cexp%5Cleft%28%5Cfrac%7B0.4605%2825+-+67%29%7D%7B2%7D%5Cright%29+%2B+%5Cexp%5Cleft%28%5Cfrac%7B0.4605%2867+-+67%29%7D%7B2%7D%5Cright%29+%2B+%5Cexp%5Cleft%28%5Cfrac%7B0.4605%2841+-+67%29%7D%7B2%7D%5Cright (visited on 2023-04-22).