The privacy course students have had a quite harsh exam this year. After grading the exam, the teacher has created a table with attributes \( \text{id}, \text{faculty}, \text{grade} \) listing grades of the students, using pseudonymous identifiers \( \text{id} \). No one can see this table besides the teacher himself.

The teacher decided to publish some summarizing statistics of the exam results. First of all, he decided to report the total number of students who got the grade 'A', and also the most popular grade. To compare success of students with different background knowledge, he also reported the average grade per faculty. For these purposes, he computed the following aggregation queries:

Q1: \( \text{SELECT COUNT(*) FROM exam WHERE grade = 'A';} \)

Q2: \( \text{SELECT grade FROM exam GROUP BY grade ORDER BY COUNT(*) DESC LIMIT 1;} \)

Q3: \( \text{SELECT AVG(grade) FROM exam GROUP BY faculty;} \)

The starting point for this exercise, containing some useful functions (including implementation of queries Q1, Q2, Q3), can be found in \texttt{dpLab_init.py}.

1.1 Demonstrate privacy issues

The attacker wants to learn the grades of Alice, Bob, and Chris. He knows that:

- Alice is one of the three math students registered to the course.
- Alice got the same grade as the math student Bob.
- Alice got a different grade from the math student Chris.

The dataset of the records \( \text{id}, \text{faculty}, \text{grade} \) is given in the file \texttt{dpLab_data.csv}. The attacker should come up with the answers \textit{without} looking at the data, but just by observing the outputs of Q1-Q3 applied to this data.
1.2 Add differential privacy to Q1 and Q3 using Laplacian mechanism

1. Estimate the global sensitivity of queries Q1 and Q3.

2. Apply Laplacian mechanism that ensures $\epsilon$-DP of Q1 for $\epsilon = 1.0$.

3. What the attacker may think after seeing a single noisy output? 10 noisy outputs? 20? 100? How is this number related to $\epsilon$?

4. Generate 10000 samples of noisy outputs of Q1. Based on these samples, predict the true output and the $\epsilon$.

   *Hint:* It is known that Laplace distribution with scaling $b$ has variance $2b^2$.

5. Estimate the accuracy of the output for $\epsilon = 1.0$. What is the probability that the added noise is at most $\pm1$?

1.3 Add differential privacy to Q2 using exponential mechanism

1. Propose a score function $Q$ for Q2.

2. Estimate the global sensitivity of $Q$.

3. Apply exponential mechanism that ensures $\epsilon$-DP for $\epsilon = 1.0$.

4. Generate 10000 samples of noisy outputs of Q2 for $\epsilon \in \{0.01, 1.0, 10.0\}$. What can an attacker infer about:
   - The most popular grade?
   - The true counts?
   - The $\epsilon$?

5. Estimate the accuracy of the output for $\epsilon = 1.0$. What is the probability that the added noise is at most $\pm5$?

1.4 Composition and group privacy

1. Let us assume that the attacker is allowed to execute each of the queries Q1, Q2, Q3 exactly once. How should one add noise to these queries, so that the differential privacy of the entire system would be $\epsilon$?

2. The attacker knows that Alice, Bob and Chris always learn together, and their grades are strongly correlated. How to ensure $\epsilon$-differential privacy for a group of 3 people?