Final Project Write-up

Advanced data privacy

Ryan Symons and Harry Sharman

In our project, we aimed to determine the impact of Laplace and Gaussian mechanisms on privacy and data accuracy. In other words, the problem we wanted to solve was to determine where these mechanisms are efficient in securing privacy of our data set.

The data set we chose to apply privacy to is a file containing identifying information for 200 students. It contains relevant columns such as Name, Student ID, GPA, Age, Email, Department (major), and graduation year. Ou default parameters are as follows: epsilon = 0.5, sensitivity = 1.0, and delta = 1e-5.

Our first section of our project tests both Laplace and Gaussian mechanisms on our data set with multiple queries. The column we applied privacy to is the GPA column, and we used 10 queries in our testing on the true mean of the column. We stored the results from each mechanism in separate data sets and calculated the errors for each, using the default parameters. After comparing the errors to the true answers, we see that the errors are greater for the Gaussian mechanism, so we can say that the Gaussian mechanism preserves privacy more aggressively while the Laplace mechanism has greater accuracy.

Next, we analyze how the sensitivity parameter influences accuracy for our tests. We varied the sensitivity to be either 0.1, 2, or 20. Similar to our test above, we used the true mean of the GPA column for testing. After applying both mechanisms separately, we see that the Gaussian mechanism is able to adapt to higher sensitivities and produce lower errors, however the Laplace mechanism is less able to adapt as sensitivity values grow, leading to lower accuracy.

After testing the impact of varying the sensitivity parameter, we then vary the epsilon values and test both mechanisms. We chose epsilons of 0.1, 0.5, and 1, and applied them to each mechanism on the true mean of the GPA column. We kept track of the errors for each iteration and compared them for each mechanism. As suspected, the errors are generally higher with lower epsilons, but the Gaussian mechanism yields substantially higher errors over the Laplace mechanism.

In our next section, we test each mechanism’s flexibility with the introduction of outliers. We clone the GPA column, replace the first two entries with 0.1 and 4.5 respectively, which are extreme GPA values. Then, we calculate a new mean and test each mechanism on the new column with outliers, using the default parameters, and record the output errors. With the outliers, the Laplace mechanism can adapt and produce lower errors, while the Gaussian mechanism produces higher errors from the true mean.

In the following section we used our data set as training data and preformed machine learning to create privacy. Specifically, we had X = GPA and an encoded version of the department (major) columns, and Y = students graduating after 2024. We applied both mechanisms to our machine learning set up with our default parameters to see how they would act with training data rather than the raw data. They both produced classification accuracy of around 0.8 steadily, so both mechanisms performed reasonably with the training data.

Next, we test the Gaussian mechanism with varying delta values. We use 1e-4, 1e-5, and 1e-6 deltas values to apply the Gaussian mechanism on the true mean of the GPA column and record the errors. Looking at the results, we see that – as suspected – smaller delta values produce greater privacy and less noise added as the delta value rises. However, the errors can fluctuate from the randomness of the mechanism.

After altering the delta values for the gaussian mechanism, we started testing the mechanisms with categorical data rather than numerical data. We decided to use the Student ID column, and use both mechanisms on the true mean of it. We used our default parameters and compared this tests output to the output of the GPA column to determine if this categorical column should be treated with differential privacy. From the output, the mechanisms seem to handle the categorical data well and produce reasonable errors that are comparable to the errors with the GPA column.

In our second to last section, we created line graphs to visualize the errors for each mechanism using varying epsilon values, illustrating the privacy-accuracy tradeoff. Using our default parameters on the true mean of the GPA column, we see the graph shows that privacy is generally more aggressive with smaller epsilon values, and then accuracy is better with greater epsilon values. The visualization is helpful as it shows the Gaussian mechanism is much more aggressive with privacy for smaller epsilon values but both mechanisms smooth out as epsilon values grow. Using the graph to make decisions on how much privacy to use will be effective, there is no one-size-fits-all epsilon value for every data set. This can change based on the size of the data set and type of data one wants to apply differential privacy to.

Lastly, we cloned the GPA column and replaced the first 10 rows with missing values. We calculated the new true mean of the column and applied both mechanisms on the new data set with our default parameters to see how they would handle a column with missing values. The errors for the Laplace mechanism are generally smaller than the Gaussian mechanism, but both handle the new column reasonably.

In conclusion, both mechanisms bring great attributes to the table for our data set. The Laplace mechanism is better for scenarios with multiple queries, higher epsilon parameters, outliers, and missing values. Gaussian mechanism shows to be better for higher sensitivity parameters, and both mechanisms handle training data and categorical data reasonably.