COMS453 - hw2 report

Benjamin Lee, Feifei Cheng, Marios Tsekitsidis

1. *Task (a)*
   Number of mislabeled points out of a total 30 points : 2
   Non-private test accuracy : 93.33333333333333

   Task (b)
   Results:
   epsilon: 1.0
   Number of mislabeled points out of a total 30 points : 9
   Differentially private test accuracy : 70.0

   Explanation:
   Deriving Sensitivity
   In the case of numeric attributes, the probability $P(X = x'|c)$ depends on the mean μ_j and standard deviation σ_j, where the mean μ_j and variance σ_j^2 are calculated for class j based on the values of attribute X from the training set. Therefore, we need to derive the sensitivity for both the mean and standard deviation.

   Algorithm
   Now that we have derived how to compute the sensitivity, the actual differentially private Naive Bayes procedure is quite simple. As described earlier, the key idea is to derive the sensitivity for each attribute appropriately. Following this, Laplacian noise is added to the parameters. The parameters are then used to classify the test dataset using Naive Bayes.

   Task (c)
   To prove epsilon-differential privacy for the algorithm in part b, we need to show that for every pair of input that differ in one row, let's say given D_1 and D_2, and for every output, the adversary should not be able to distinguish between any D_1 and D_2, based on any output O. From class lecture notes, the formula below must be fulfilled in order to ensure epsilon-differential privacy.

   $$\log\left(\frac{\Pr[A(D_1) = O]}{\Pr[A(D_2) = O]}\right) \leq \epsilon, \text{ such that } \epsilon > 0$$

   From part b, we use epsilon = 1 to test on the classifier.

   $$\log\left(\frac{\Pr[A(D_1) = O]}{\Pr[A(D_2) = O]}\right) \leq \epsilon, \text{ such that } \epsilon > 0$$

   $$0.0953101798043249 \leq \epsilon$$

   This shows the maximum calculated differential privacy probabilistic between pairs of inputs, which is 0.09531, which is less than epsilon, since epsilon used here is equal to 1. Therefore, this ensures that the algorithm is epsilon-differential private.

   Task (d)
   epsilon: 0.5
   Number of mislabeled points out of a total 30 points : 18
   Differentially private test accuracy : 40.0
   Precision: 0.3858363858363858

```
Recall: 0.39999999999999997

epsilon: 1.0
Number of mislabeled points out of a total 30 points : 9
Differentially private test accuracy : 70.0
Precision: 0.7111111111111111
Recall: 0.7000000000000001

epsilon: 2.0
Number of mislabeled points out of a total 30 points : 7
Differentially private test accuracy : 76.66666666666667
Precision: 0.7859362859362861
Recall: 0.7666666666666666

epsilon: 4.0
Number of mislabeled points out of a total 30 points : 5
Differentially private test accuracy : 83.33333333333334
Precision: 0.8350168350168351
Recall: 0.8333333333333334

epsilon: 8.0
Number of mislabeled points out of a total 30 points : 4
Differentially private test accuracy : 86.66666666666667
Precision: 0.875
Recall: 0.8666666666666667

epsilon: 16.0
Number of mislabeled points out of a total 30 points : 2
Differentially private test accuracy : 93.33333333333333
Precision: 0.9333333333333332
Recall: 0.9333333333333332
```

Figure below illustrates the graph of differentially private Naive Bayes classification accuracy with different epsilon for part d.

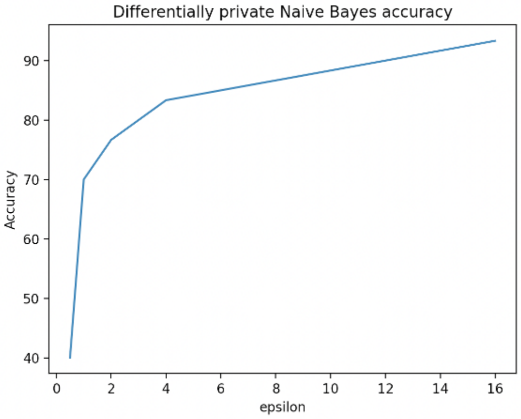

Figure 1: Classification accuracy for different values of epsilon

Summary
We can see that the differential privacy works best as the epsilon with value 16 because it is similar to the non-private test accuracy, only having two mislabeled data. As the epsilon gets larger, the better the classifier is able to predict the data. However, as the epsilon increases, the less privacy is preserved and data accuracy gets better. However, if epsilon is small, the more privacy is preserved and data accuracy gets worse.

2. Below are the experiment results of two LDP protocals: generalized random response and unary coding on domain size of 16. From 2, we see that the l1 distance of true response and noised response are getting smaller as the epsilon grows. Theoretically, unary is supposed to perform better than RR but since the privacy budget is halved in unary, they have similar performance. However, when epsilon is less than 2, unary is better than generalized RR.

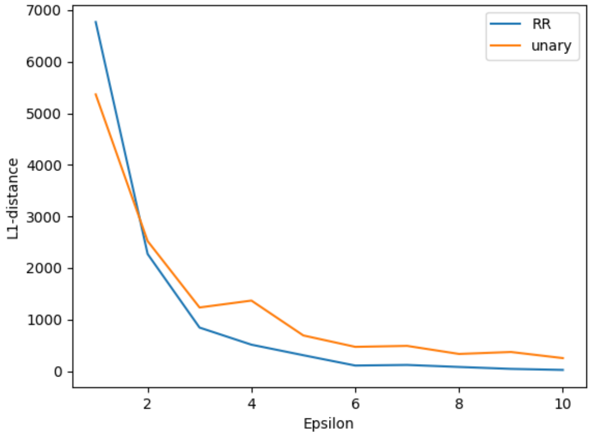

Figure 2: Experiments on different values of epsilon

From 3, we see that the l1 distance of true response and noised response are getting smaller as the number of records grows. This is expected as the more users, the more noise when aggregates.

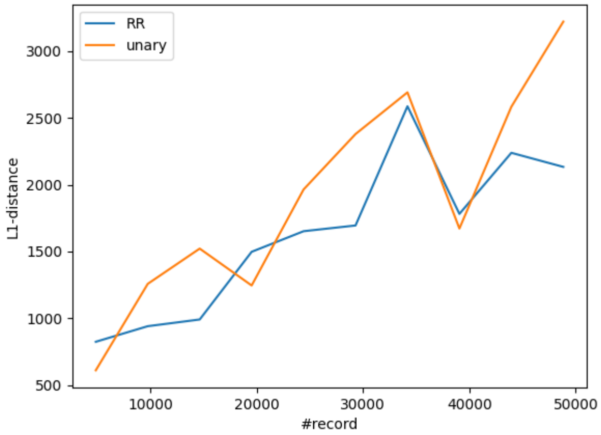

Figure 3: Experiments on different values of records