Hw 7

Marin Mato

1/5/2024

Recall that in class we showed that for randomized response differential privacy based on a fair coin (that is a coin that lands heads up with probability 0.5), the estimated proportion of incriminating observations $\hat{P}$ [1] was given by $\hat{P} = 2\hat{\pi} - \frac{1}{2}$ where $\hat{\pi}$ is the proportion of people answering affirmative to the incriminating question.

I want you to generalize this result for a potentially biased coin. That is, for a differentially private mechanism that uses a coin landing heads up with probability $0 \leq \theta \leq 1$, find an estimate $\hat{P}$ for the proportion of incriminating observations. This expression should be in terms of θ and $\hat{\pi}$.

$\hat{\pi} = (1-\theta)\theta + \theta\hat{P}$

Next, show that this expression reduces to our result from class in the special case where $\theta = \frac{1}{2}$.

First, we sub in $\theta = \frac{1}{2}$ Then, the expression becomes $\hat{\pi} = \frac{1}{2}\hat{P} + (1 - \frac{1}{2})\frac{1}{2}$ Then, we are left with the result that was shown in class $\hat{\pi} = \frac{1}{2}\hat{P} + \frac{1}{4}$

Part of having an explainable model is being able to implement the algorithm from scratch. Let's try and do this with `KNN`. Write a function entitled `chebychev` that takes in two vectors and outputs the Chebychev or L^∞ distance between said vectors. I will test your function on two vectors below. Then, write a `nearest_neighbors` function that finds the user specified k nearest neighbors according to a user specified distance function (in this case L^∞) to a user specified data point observation.

```
#student input
#chebychev function
cheby <- function(x, y) {
  max(abs(x-y))
}
#nearest_neighbors function
nearest_neighbors = function(x, obs, k, df){
  distance = apply(x, 1, df, obs)
  distances = sort(distance)[1:k]
  neighbors_list = which(distance %in% sort(distance)[1:k])
  return(list(neighbors_list, distances))
}
```

[1] in class this was the estimated proportion of students having actually cheated

```r
x<- c(3,4,5)
y<-c(7,10,1)
cheby(x,y)
```

```
## [1] 6
```

Finally create a `knn_classifier` function that takes the nearest neighbors specified from the above functions and assigns a class label based on the mode class label within these nearest neighbors. I will then test your functions by finding the five nearest neighbors to the very last observation in the `iris` dataset according to the `chebychev` distance and classifying this function accordingly.

```r
library(class)
df <- data(iris)
#student input
knn_classifier = function(x, y){
  groups = table(x[,y])
  return(groups[groups == max(groups)])
}

#data less last observation
x = iris[1:(nrow(iris)-1),]
#observation to be classified
obs = iris[nrow(iris),]

#find nearest neighbors
ind = nearest_neighbors(x[,1:4], obs[,1:4],5, cheby)[[1]]
as.matrix(x[ind,1:4])
```

```
##     Sepal.Length Sepal.Width Petal.Length Petal.Width
## 71           5.9         3.2          4.8         1.8
## 84           6.0         2.7          5.1         1.6
## 102          5.8         2.7          5.1         1.9
## 127          6.2         2.8          4.8         1.8
## 128          6.1         3.0          4.9         1.8
## 139          6.0         3.0          4.8         1.8
## 143          5.8         2.7          5.1         1.9
```

```r
obs[,1:4]
```

```
##     Sepal.Length Sepal.Width Petal.Length Petal.Width
## 150          5.9           3          5.1         1.8
```

```r
knn_classifier(x[ind,], 'Species')
```

```
## virginica
##         5
```

```r
obs[,'Species']
```

```
## [1] virginica
## Levels: setosa versicolor virginica
```

Interpret this output. Did you get the correct classification? Also, if you specified $K = 5$, why do you have 7 observations included in the output dataframe?

Yes, the KNN classifier correctly predicted the species of the last observation in the iris dataset. Although K=5, 7 observations appeared in the output because, using the Chebyshev distance metric, multiple observations (specifically the 5th to 7th nearest neighbors) had the same minimum distance. As a result, all these equally distant neighbors need to be included to ensure an accurate and fair classification.

Earlier in this unit we learned about Google's DeepMind assisting in the management of acute kidney injury. Assistance in the health care sector is always welcome, particularly if it benefits the well-being of the patient. Even so, algorithmic assistance necessitates the acquisition and retention of sensitive health care data. With this in mind, who should be privy to this sensitive information? In particular, is data transfer allowed if the company managing the software is subsumed? Should the data be made available to insurance companies who could use this to better calibrate their actuarial risk but also deny care? Stake a position and defend it using principles discussed from the class.

Even though developers at the Google's DeepMind have designed algorithms to advance and enhance the efficiency in the medical field, its use must be restricted to a great extent. In this particular example, transferring the data to insurance companies or Google will be a direct breach of privacy for a patient admitted to a certain hospital. The data should only be exposed to algorithms if the patient's explicit consent is given, after a representative from the company explains in detail how the data will be used. By transferring the data to insurance companies, there is a real danger that they could use the data to deny coverage or increase premiums for individuals who are already vulnerable. Algorithms should be focused on minimizing the harm for the already disadvangated groups, not advance it even further. Moreover, from the Kantian ethics standpoint, individuals have inherent dignity and must be treated as ends in themselves, not merely as means to an end.

I have described our responsibility to proper interpretation as an *obligation* or *duty*. How might a Kantian Deontologist defend such a claim?

Student Answer A Kantian deontologist might argue that we have a moral duty to provide proper interpretations because misinterpretation cannot be universalized without leading to a breakdown in trust and rational communication, violating the Categorical Imperative. Additionally, accurate interpretation respects others as ends in themselves by allowing them to make informed decisions. However, as I mentioned above, misinterpretation uses them merely as means to an end, which is morally impermissible in Kantian ethics.