Hw 7

Mackie Jackson

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 $\hat{\pi}$.

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

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

$\hat{P} = \frac{\hat{\pi} - (1-\frac{1}{2})\frac{1}{2}}{\frac{1}{2}}$

$\hat{P} = 2(\hat{\pi} - (1 - \frac{1}{2})\frac{1}{2})$

$\hat{P} = 2(\hat{\pi} - \frac{1}{2} - \frac{1}{2})$

$\hat{P} = 2\hat{\pi} - 2(\frac{1}{4})$

$\hat{P} = 2\hat{\pi} - \frac{1}{2}$

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
#nearest_neighbors function


chebychev <- function(a, b) {
max(abs(a - b))
```

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

```r
}

nearest_neighbors <- function(x, obs, k, dist_func){
dist = apply(x, 1, dist_func, obs)
distances = sort(dist) [1: k]
neighbor_list = which(dist %in% sort(dist)[1:k])
return( list (neighbor_list, distances))
}

x <- c(3,4,5)
y <-c(7,10,1)
chebychev(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])
pred = groups[groups == max(groups)]
return(pred)
}

#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, chebychev)[[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
```

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

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

```
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?

The KNN function classified row 150 as virginica, which is accurate. I specified $K = 5$, but there were likely several observations that were of equal distance to the last observation in the dataset, thus leading to the function returning seven rows.

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.

In healthcare data ethics, tacit consent is not equivalent to true consent. We discussed the conflict between the harm principle and paternalism in class in the case of health data management, and I would appeal to deontological ethics to argue that an individual's sensitive information should be available only to parties whom have been given explicit consent. If the company managing data/software is subsumed, the merger company is essentially buying data from the original data manager. In this case, the individual whose data is transferred is treated as a means to increase profit and algorithmic accuracy at the expense of their autonomy. This holds true for insurance companies as well–people, not corporations, are moral agents. In any case where we are choosing between the potential financial gain of a corporate entity and treating a person as an end objective, Kant would likely agree that the person's wellbeing and autonomy comes first.

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

A Kantian Deontologist might argue that failure to properly interpret results to an audience violates both formulations of the categorical imperative, so proper interpretation is an ethical obligation. You cannot universalize presenting results that are improperly interpreted. In many, or most cases, making claims that are not accurate is not morally defensible. Furthermore, presenting results that distort reality to further one's own interests treat the audience of moral agents as an end, not a mean.