Hw 7

Mason Boyles

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 $\hat{\pi}$.

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

$\hat{\pi} = \theta - \theta^2 + \hat{p}\theta)$

$\hat{\pi} - \theta + \theta^2 = \hat{p}\theta$

$\hat{p} = \frac{\hat{\pi}}{\theta} - 1 + \theta$

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

When $\theta = \frac{1}{2}$ we have:

$\hat{p} = \frac{\hat{\pi}}{1/2} - 1 + 1/2 = 2\hat{\pi} - 1 + 1/2 = 2\hat{\pi} - 1/2$

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.

```r
#student input
#chebychev function
chebychev <- function(x, y) {
  distance <- max(abs(x - y))
  return(distance)
}
#nearest_neighbors function
nearest_neighbors <- function(x, obs, k, dist_func){
```

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

```
  dist = apply(x, 1, dist_func, obs) #apply along the rows
  distances = sort(dist)[1: k]
  neighbor_list = which(dist %in% sort(dist)[1:k])
  return(list(neighbor_list, distances))
}
euclid <- function(x, y) {
  distance = sqrt(sum((x-y)^2))
  return(distance)
}
taxi <- function(x,y){
  distance = sum(abs(x-y))
  return(distance)
}


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.

```
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
```

```
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 reason there are 7 observations is because there are ties. Chebychev distance simply takes the minimum of each of the distances of features and for each of those 7 nearest neighbors, there is a feature that has the exact same value as our observation. I believe we did get the correct classification, I confirmed by using taxi and euclidean distance as our distance function and ended up with the same results.

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.

From the perspective of a utilitarian, I would argue that it is justified to give the sensitive information to any and everyone who could engineer benefit to the masses. This is because in the end, if you tally up the consequences will be negative for the people who have their health care data collected, and it will be positive for all of the people who may be helped by the use of that data (presumably a higher number of people in the long run as each persons data can help people for years to come). In addition, the pain that affects the people getting data collected on them will be a lower order one (not life or death) whereas the pleasure for the field of health care have the potential to actually save lives.

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 would be against the sharing of the data. This is because Kant emphasized how it is unethical to use someone as a mere means to an end. In this case, using peoples data would be using them as a mere means to an end rather than an end in and of themselves, which would violate his second formulation of the second imparative.