Hw 7

Ruby Ashman

11/28/2024

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 $\hat{\pi}$.

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

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

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

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.

```
cheby <- function(a,b) {max(abs(a-b))}
nearest_neighbors = function(x, obs, k, dist_func){
  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))
}


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

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

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)

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, cheby)[[1]]
as.matrix(x[ind,1:4])
obs[,1:4]
knn_classifier(x[ind,], 'Species')
obs[,'Species']
```

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?

Based on the it's five nearest neighbors, the chosen data point was classified correctly as virginica. While I specified to only classify based on 5 of the nearest neighbors, the output data frame includes the observation to be classified, as well as the data less last observation for a total of 7 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.

I do not believe any company, including those who were presented with the sensitive information willingly, should be able to utilize the sensitive information at hand for a purpose that was not listed in the consent agreement with the user, such as a study regarding acute kidney injury. However if the benefit to the patient, such as the progress made in this study, outweighs the harm, a form of tacit consent could be acquired, given the user is now receiving at least half the benefits of the social exchange. If this form of consent is determined appropriate, all data should be privatized, through a mechanism that will protect individuals identities that

the data was trained on, in the event of a data extraction attack. After all data has been privatized, only researchers that train the model on this data set should have access to the user data. No one outside this group is at all privy to this information, considering the nature of intimacy of the data set. I do not think this data transfer is acceptable in the scenario of a company being subsumed, given the user explicitly bestowed the information to the company they made contact with at the time. The data should absolutely not be made available to insurance companies, because in this case users would likely be negatively affected in the social exchange, and any argument for tacit consent would therefore be overturned.

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

Kantian deontology is heavily reliant on two principles: the universal maxim formulation, and the ends-not-means formulation. The universal maxim formulation, which states an act is only moral if it can be universalized to all of humanity, is violated heavily by the misinterpretation of an outcome, given if the general rule for interpreting outcomes was misinterpretation, all data prediction software would be useless. Additionally, by deceiving those that will receive the observations developed from the misinterpreted data, the ends-not-means formulation is being violated, as convincing others of an untrue interpretation of outcome is treating them as means and not ends, despite being a separate moral agent.