Hw 7

Jonathan Zhao

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 $\hat{\pi}$.

Student Answer

if θ is the chance that the coin lands on heads, then θ-1 is the chance that it lands on tails. We can then use that to create the equation $\pi = \theta P + (1-\theta)P$, which is the proportion of stdents that flipped heads that actually cheated and the proportion of students that flipped tails that actually cheated.vNext, it can be changed to $\pi = \theta\hat{P} + (1-\theta)\theta$, which simplifies to $\hat{p} = (\hat{\pi} - (1-\theta)\theta)/\theta$.

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

Student Answer If you plug in 1/2 as the theta, you end with $2\hat{\pi} - \frac{1}{2}$

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.

```r
#student input
#chebychev function
cheby <- function(vec1, vec2) {
  return(max(abs(vec1 - vec2)))
}
```

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

```r
#nearest_neighbors function
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] 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])
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?

Student Answer

I got the correct classification here, as the species is Virginica. The reason I have more than 5 observations in the output dataframe is probably because there are ties in the Chebyshev distance, so it shows more than 5.Since there are 7, I am assuming there are 2 ties.

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.

Student Answer

The sensitive data of patients should be used only by those that are directly involved with patient care, and assisting the health care sector to benefit the patients. Google's DeepMind should be allowed to use the data on the principle of paternalism, since what they are doing is in the best interest of the patients. However, this data should be closely guarded and should require explicit consent if it is to be transferred. If explicit consent can't be gotten, then the data should be anonymized as much as possible.Insurance companies should not have access to this data based on the harm principle. Because they can use the data to deny care, which will directly harm patients, they should not be given access to it, unless explicit consent from patients are given.

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 Deontlogist would defend this claim by saying that we have a moral duty for proper interpretation because it prevents individuals from being used as just a means to an end. For example, if we use a model without being able to interpret how it gets to the results, then the data from people would be used as tools, which goes against the principle of deontology. Only through proper interpretation can data be used ethically in a way that upholds the moral duty of treating moral agents as ends themselves.