HW 7

Razmin Bari

12/3/2024

1

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 $\hat{\pi}$.

The two ways that result in people give an affirmative answer is (1) the respondent lands a heads and actually tells the truth, and (2) the respondent lands a tails-head. The probability of (1) is $\theta\hat{P}$ and that of (2) is $(1-\theta)\theta$.

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

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

2

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

Substituting θ with $\frac{1}{2}$:

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

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

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

3

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.

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

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

# testing chebychev function (given)
x<- c(3,4,5)
y<-c(7,10,1)
chebychev(x,y)
```

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

```r
# nearest_neighbors function
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))
}
```

4

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)

#knn_classifier
knn_classifier = function(x,y){
  groups = table(x[,y])
  pred = groups[groups == max(groups)]
  return(pred)
}

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

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

```
##     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') # predicted class
```

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

```
obs[,'Species'] # actual class
```

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

5

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 test data point was correctly classified as virginica. The reason for 7 observations instead of 5 may be that the extra 2 observations had the exact same chebychev distance to some of the other 5. The algorithm just kept all of them instead of arbitrarily dropping one and inducing bias.

6

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.

The data should not be made available to any entity the participants did not give fully informed consent to. This includes any entity that later subsumes the team that originally had consent to use the data. I assert that it is similar to IRB procedures, and how a new researcher needs to get approval to use the data even if their superior had prior access/consent.

From a deontological point of view, it is imperative to treat moral agents not merely as the means to an end. Going against the wishes of the people who initially shared their data for a specific purpose denies those people the dignity of moral agents. The insurance companies are the ones profiting here while parcipants' rights to informed consent and privacy are being breached. And so it can be argued that the people whose data was used are being used as the means to an end.

7

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

If a statistician interprets their results in a way to push their own agenda, then that is a misrepresentation meant to manipulate the person making any decisions based on that analysis. One of the formulations of the categorical imperative in Deontology is that an act is not permissible if it cannot be universalized without a logical contradiction. Purposefully manipulating somebody cannot be universalized as that would lead to people not being able to trust anybody but themselves. It would break down on itself since if people become distrusting, they can no longer even be manipulated. As statisticians with access to the 'truth', we yield a sort of power that morally should not be abused for the betterment of human society. This makes proper interpretation not just the better choice, but also our duty.