Hw 7

Anna Fetter

12/1/2024

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

generalized response for a potentially biased coin from class notes:

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

rearrange to solve for $\hat{P}$

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

$\hat{\pi}/\theta = 1 - \theta + \hat{P}$

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

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

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

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

Student Answer

when $\theta = \frac{1}{2}$

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

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

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

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

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: max absolute distance
chebychev <- function(vec1, vec2) {
  max(abs(vec1 - vec2))
}
#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))
}


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

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

```
#test
```

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 = names(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')
```

```
## [1] "virginica"
```

```
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?

Student Answer

Yes, I got the correct observation because I predicted virginica and also got vigrinica. I have 7 observations in the dataframe because the nearest neighbor function when worded this wat akkiws duplicates. Three observations have the same values.

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

Sensitive patient data should only be shared with explicit patient consent. Sensitive patient information should only be only used private models that can't be accessed by the public. Going forward, patient data should not be allowed to be sold in corporate mergers without explicit consent. In the future, I could see healthcare start-ups getting acquired by health insurance companies for the sole purpose of more patient health data if data privacy protections are not upheld. Health insurance companies already deny care based on the data they have, but using the algorithm should not be the sole decider and practioners should be able to appeal the health insurances' denial of care based on an algorithm. This is similar to how the court ruled on COMPAS.

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 deontologist would apply the universal maxim to this claim. Under this case, a deontologist would allow the sharing of patient data if this happened to all patients in the database and the data was used equally for all patients to predict patient outcomes. Kantian deontologists also follow the ends not means formulation. They would be against purely instrumentalizing the moral agents for this data or for the insurance companies' benefits. The obligation or duty would be to apply this data sharing fairly and if the data is shared to have a reason beyond pure instrumentalization.