Hw 7

Lynn Check

1/5/2024

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 $\hat{\pi}$.

Student Answer

Isolating $\hat{P}$:

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

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

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

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

2

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

Student Answer

Substituting $\frac{1}{2}$ for θ in $\hat{P} = \frac{\hat{\pi}}{\theta} \text{ - } 1 + \theta$

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

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

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
#student input
#chebychev function
chebychev = function(x,y){
  max(abs(x-y))
}

#nearest_neighbors function
nearest_neighbors = function(data, obs, k, dist_function){
  dist = apply(data, 1, dist_function, obs)
  distances = sort(dist[1:k])
  kneighbor = which(dist %in% sort(dist)[1:k])
  return(list(kneighbor, distances))
}

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

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

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)
#student input
knn_classifier = function(x,y){
  labels = table(x[,y])
  prediction = labels[labels == max(labels)]
  return(prediction)
}

#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
```

```r
obs[,1:4]
```

```
##     Sepal.Length Sepal.Width Petal.Length Petal.Width
## 150          5.9           3          5.1         1.8
```

```r
knn_classifier(x[ind,], 'Species')
```

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

```r
obs[,'Species']
```

```
## [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?

Student Answer

The classification algorithm was correct. It correctly classified the observation as virginica, matching its actual class. There was 7 observations included in the output dataframe instead of returning exactly 5 nearest neighbors ($k = 5$) because they all have a Chebyshev distance of 0 from the test point. What this mean is that at least one of the features (i.e Sepal.Length, Sepal.Width, etc.) is identical between the test points and each of these 7 observations.

The idea behind the `nearest_neighbors` function is to include all the points that have the same minimum distances, even if it exceeds k. Specifically, the line `kneighbor = which(dist %in% sort(dist)[1:k])` retrieves all the indices with distances that are equal to the smallest k distances. The significance of this line of code is to ensure the algorithm's fairness as shown by the inclusion of all 7 observations.

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.

Student Answer

The parties the should be privy to this sensitive information are those directly involved with patient care, such as the healthcare providers, and the patients themselves. These sensitive data holds information about the patient's private life and well-being that should not be shared without fully-informed consent. Therefore, data transfer should not be allowed under any circumstances. This includes in siutations where the company is subsumed. The insurance companies also should not have access to sensitive healthcare data even if they claim that by having access to such data would help with calibrating actuarial risk. If insurance companies have access to healthcare data, it opens up for the possibility of discriminatory practices. For example, insurance companies could start denying coverage or increasing plans for high-risk individuals. This appeals to the moral framework of Deontology. Granting insurance companies access to these sensitive healthcare data would by violating the duty to protect patients from potential harm and discriminaiton. Furthermore, access to these data would greater benefit the insurance companies rather than for the benefit of the entire society. It would prioritize insurance companies' financial goals over the patients' rights, hence failing to justify the action under the deontological lens. Deontology emphasizes that individuals have inherent rights that must be respected, which denying coverage, increasing coverage plans, transferring healthcare data are all examples of the patients' autonomy is being denied and violated.

7

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 defend the claim that proper interpretation as an *obligation* or *duty* by formulating the argument rooted in Immanuel Kant's principles of the categorical imperative. According to this framework, individuals must act in a way in which their actions could be universalized as a moral law. Proper interpretation aligns with this because it ensures that the truth is respective and communication and understanding is not undermined. For example, one may say proper interpretation is "interpreting information truffully and responsibly". However, a Kantian Deontologist could argue that it can be universalized as misinterpretation, regardless if it is deliberate or negligent, which would lead to a breakdown in trust and fairness. It could also case rational discourse. Furthermore, the categorical imperative requires treating humanity never as a means to an end. As discussed in class, data that is used without informed consent would be "to use the owner of the data as a mere means to an end rather than an end in-and-of themselves". Misinterpretation would be violating this principle as it is using others as a mere tool, manipulating their understanding decisions for selfish purposes, hence undermining their autonomy as rational beings. Therefore, proper interpretation is a statistician's obligation or duty.