# CSCI 567 Fall 2022, Quiz 2 

Instructor: Vatsal Sharan
Time limit: 2 hour and 40 minutes

| Problem | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Total |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| Max | 8 | 8 | 15 | 12 | 17 | 10 | 30 | 100 |

Please read the following instructions carefully:

- Please go ahead and fill in your name and Student ID in the space above.
- The exam has 20 pages (including this cover page), numbered 1-20. Once you are permitted to open your exam (and not before), you should make sure you are not missing any pages.
- Answers should be concise and written down legibly. You must answer each question on the space provided below the question. You likely won't need all the provided space to answer most of the questions.
- There are 4 pages provided for scratch work at the end. These pages will not be graded.
- This is a closed-book/notes exam. Consulting any resource is NOT permitted. Do not use your phones during the exam.
- Any kind of cheating will lead to score 0 for the entire exam and be reported to SJACS.


## $1 k$-means clustering

Recall the $k$-means objective function $F\left(\left\{\gamma_{i j}\right\},\left\{\boldsymbol{\mu}_{j}\right\}\right)(\mathrm{Eq} 1)$, and the $k$-means algorithm (in the box below):

$$
\begin{equation*}
F\left(\left\{\gamma_{i j}\right\},\left\{\mu_{j}\right\}\right)=\sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{i j}\left\|\boldsymbol{x}_{i}-\boldsymbol{\mu}_{j}\right\|_{2}^{2} \tag{1}
\end{equation*}
$$

Step 0 Initialize $\boldsymbol{\mu}_{1}, \ldots, \boldsymbol{\mu}_{k}$
Step 1 For the centers $\boldsymbol{\mu}_{1}, \ldots, \boldsymbol{\mu}_{k}$ being fixed, assign each point to the closest center:

$$
\gamma_{i j}=\mathbb{I}\left[j=\underset{c}{\operatorname{argmin}}\left\|\boldsymbol{x}_{i}-\boldsymbol{\mu}_{c}\right\|_{2}^{2}\right]
$$

Step 2 For the assignments $\left\{\gamma_{i j}\right\}$ being fixed, update the centers

$$
\boldsymbol{\mu}_{j}=\frac{\sum_{i} \gamma_{i j} \boldsymbol{x}_{i}}{\sum_{i} \gamma_{i j}}
$$

Step 3 Return to Step 1 if not converged (convergence means that all the assigments $\gamma_{i j}$ are unchanged in Step 1).

Now consider the following data points in a 2-D plane:

(a) Suppose you run $k$-means with $k=2$ and the initial cluster centers being $(4,0)$ and $(0,3)$. What are the final cluster centers when $k$-means converges?
(b) Prove that the above initialization converges to the global minimum for $k=2$. (Hint: Enumerate over all possible cluster assignments.)
(4 points)
(c) Suppose we uniformly randomly pick two distinct data points (out of the three datapoints) as the cluster centers at initialization. What is the probability that $k$-means converges to the global minimum? (2 points)

## 2 Linear discriminant analysis (LDA) in 1-D

In this question we will explore a simple generative model for classifying 1-D data with a Gaussian assumption (the generalization of the approach to higher dimensions is known as linear discriminant analysis (LDA), hence the name of the question).

Consider a binary classification task on one dimensional data with labels $\{1,2\}$. We have $n_{1}$ datapoints with label 1 and these are denoted as $\left\{x_{1}^{(1)}, \ldots, x_{n_{1}}^{(1)}\right\}$. Similarly, we have $n_{2}$ datapoints $\left\{x_{1}^{(2)}, \ldots, x_{n_{2}}^{(2)}\right\}$ with label 2. We will use a generative model to predict the labels of the datapoints. Recall that a generative model will output the label given by $\operatorname{argmax}_{j \in[2]} p(x, y=j)$. For $j \in\{1,2\}$, we model $p(x \mid y=j)$ as

$$
p(x \mid y=j)=\frac{1}{\sqrt{2 \pi} \sigma} \exp \left(-\frac{\left(x-\mu_{j}\right)^{2}}{2 \sigma^{2}}\right)
$$

for parameters $\mu_{j} \in \mathbb{R}$. We assume $\sigma \in \mathbb{R}^{+}$is some appropriately chosen constant and is not a parameter of the model (and is also the same for all $j$ ).
(a) What is the maximum likelihood estimate (MLE) of $\left\{\mu_{j}\right\}_{j=\{1,2\}}$ given the data? Write down the expression for the log-likelihood, and show your derivation.
(4 points)
(b) Suppose $n_{1}=n_{2}$. What is the MLE estimate for $p(y)$ ? Use this to show that the final predictor has the following form,

$$
\underset{j \in[2]}{\operatorname{argmax}} p(x, y=j)=\left\{\begin{array}{l}
1, \text { if }\left|x-\mu_{1}\right| \leq\left|x-\mu_{2}\right| \\
2, \text { otw }
\end{array}\right.
$$

## 3 Backpropagation and Vanishing Gradients

Consider the 152-layer neural network in the figure below. Throughout the question, we assume that the training example is $(\boldsymbol{x}, y)$ where $\boldsymbol{x}=\left(x_{1}, x_{2}\right) \in \mathbb{R}^{2}$ and $y \in \mathbb{R}$ (all activations and gradients are with respect to this training example). The network has no bias terms, and it is fully-connected only for the final output node (i.e. the input $x_{1}$ is not connected to the red node in the next layer and so on, except for the last output node).


Notation: The notation for the weights is as described in the figure above. The notation for the inputs and outputs to the nodes is analogous. For e.g., the red node has input $a_{2}^{(1)}=w_{2}^{(1)} x_{2}$ and output $o_{2}^{(1)}=h\left(a_{2}^{(1)}\right)$. Similarly, the final output node has input $a_{1}^{(152)}=w_{1}^{(152)} o_{1}^{(151)}+w_{2}^{(152)} o_{2}^{(151)}$ and output $o_{1}^{(152)}=h\left(a_{1}^{(152)}\right)$.

Activation functions: The network uses some activation function $h(\cdot)$ for all nodes in all layers.
Loss function: The network is trained on the standard squared loss, so that $L(\boldsymbol{w})=\frac{1}{2}\left(o_{1}^{(152)}-y\right)^{2}$ for the example $(\boldsymbol{x}, y)$, where $\boldsymbol{w}$ is the vector of all the weights in the network.

For questions (a) and (b), you can use $h^{\prime}(a)$ to represent the derivative of the activation function $h(\cdot)$ with respect to some input $a$ in your answer.
(a) Derive expressions for $\frac{\partial L(\boldsymbol{w})}{\partial o_{1}^{(152)}}$ and $\frac{\partial L(\boldsymbol{w})}{\partial w_{1}^{(152)}}$.
(b) Derive expressions for $\frac{\partial L(\boldsymbol{w})}{\partial o_{1}^{(l)}}$ and $\frac{\partial L(\boldsymbol{w})}{\partial w_{1}^{(l)}}$ for all hidden layers $l=1, \ldots, 151$ in the network.
(Hint: Use the chain rule, for example, $\frac{\partial o_{1}^{(l+1)}}{\partial o_{1}^{(l)}}=\frac{\partial o_{1}^{(l+1)}}{\partial a_{1}^{(l+1)}} \frac{\partial a_{1}^{(l+1)}}{\partial o_{1}^{(l)}}$.)
(5 points)
(c) Suppose we use the sigmoid activation $h(a)=\frac{1}{1+e^{-a}}$ for all nodes in this neural network. The gradient of $h(a)$ is $h^{\prime}(a)=h(a)(1-h(a))$. Using your expression from the previous part, describe what the gradients $\frac{\partial L(\boldsymbol{w})}{\partial w_{1}^{(l)}}$ for the weights in the earlier layers of the network would be like, and explain why (earlier layers refers to small $l$ ). (Hint: You don't need to actually use the expression for the sigmoid activation, just think about the range of values the gradient of the activation takes. The range of $h(a)$ is $[0,1]$. What is the range of $\left.h^{\prime}(a) ?\right)$
(d) Suppose we use ReLU as the activation function for all nodes, i.e. $h(a)=\max (0, a)$. When would the gradients $\frac{\partial L(\boldsymbol{w})}{\partial w_{1}^{(I)}}$ for the weights for some layer of the network be zero? If we continue with the ReLU activation function but modify the network to be fully connected for all layers (i.e. add all cross-connections by connecting $x_{1}$ and the red node and so on), when would the gradients of the weights be zero? Describing one case where the gradient is zero for each of these questions is enough.
(3 points)

## 4 PCA

Consider the usual PCA setup. There is a dataset with $n$ datapoints $\left\{\boldsymbol{x}_{i}, i \in[n]\right\} \in \mathbb{R}^{d}$. Assume that the data is 0 mean. The data is represented as a matrix $\boldsymbol{X} \in \mathbb{R}^{n \times d}$ as usual, with each row being the (transpose) of the corresponding datapoint. Let the covariance matrix $\boldsymbol{X}^{\mathrm{T}} \boldsymbol{X}$ have the eigendecomposition $\boldsymbol{X}^{\mathrm{T}} \boldsymbol{X}=\boldsymbol{Q} \boldsymbol{D} \boldsymbol{Q}^{\mathrm{T}}$. Here $\boldsymbol{D}$ is a diagonal matrix containing the eigenvalues $\left(\lambda_{1}, \ldots, \lambda_{d}\right)$ as diagonal entries, sorted in decreasing order (assume all the eigenvalues are unique). $\boldsymbol{Q}$ is an orthogonal matrix $\left(\mathbf{Q}^{T} \mathbf{Q}=\mathbf{Q} \mathbf{Q}^{T}=\mathbf{I}\right)$, and consists of the eigenvectors. We proved in class that the $j^{\text {th }}$ principal component $\boldsymbol{v}_{j}$ is equal to the eigenvector corresponding to the $j^{\text {th }}$ eigenvalue, which is the $j^{\text {th }}$ column $\boldsymbol{q}_{j}$ of $\boldsymbol{Q}$.

In this question we will prove some properties of PCA for data compression which we have already implicitly stated in class. We first note that we can represent any datapoint $\boldsymbol{x}_{i}$ by using all the $d$ principal components,

$$
\begin{equation*}
\boldsymbol{x}_{i}=\sum_{j=1}^{d} \alpha_{i, j} \boldsymbol{v}_{j} \tag{2}
\end{equation*}
$$

where $\alpha_{i, j}$ are some coefficients. If we only use the top $k$ principal components (for some $k \leq d$ ), we can get an approximation $\hat{\boldsymbol{x}}_{i}$ of the $i^{\text {th }}$ datapoint $\boldsymbol{x}_{i}$ as follows:

$$
\begin{equation*}
\hat{\boldsymbol{x}}_{i}=\sum_{j=1}^{k} \alpha_{i, j} \boldsymbol{v}_{j} . \tag{3}
\end{equation*}
$$

Consider the overall reconstruction error if we use the top $k$ principal components:

$$
\begin{equation*}
E=\sum_{i=1}^{n}\left\|\boldsymbol{x}_{i}-\hat{\boldsymbol{x}}_{i}\right\|_{2}^{2}=\sum_{i=1}^{n}\left(\boldsymbol{x}_{i}-\hat{\boldsymbol{x}}_{i}\right)^{\mathrm{T}}\left(\boldsymbol{x}_{i}-\hat{\boldsymbol{x}}_{i}\right) \tag{4}
\end{equation*}
$$

(a) Show that for all $i \in[n]$ and $j \in[k]$, choosing the coefficients $\alpha_{i, j}=\boldsymbol{x}_{i}^{\mathrm{T}} \boldsymbol{v}_{j}$ in Eq. 3 minimizes the reconstruction error $E$ in Eq. 4. To do this, follow the following steps,

- Step 1: First consider the case when $k=1$. Expand out Eq. 4 using Eq. 3, and then find the best value of $\alpha_{i, j}$.
(3 points)
- Step 2: Then, consider the case of general $k$. Here, use the fact that $\boldsymbol{v}_{j}=\boldsymbol{q}_{j}$ and $\boldsymbol{Q}$ is an orthogonal matrix.
(2 points)
(b) Prove that $E=\sum_{j=k+1}^{d} \lambda_{j}$. To show this, you should follow the following three steps. ${ }^{1}$ If you get stuck on some step, feel free to try out the next one using the conclusion of the previous step.
- Step 1: Plug Eq. 2 and 3 into the expression for $E$ in Eq. 4. Next, use the fact that $\boldsymbol{v}_{j}=\boldsymbol{q}_{j}$ and $\boldsymbol{Q}$ is orthogonal to simpify the expression. You should be able to show that $E=\sum_{i=1}^{n} \sum_{j=k+1}^{d} \alpha_{i, j}^{2}$. points)
- Step 2: Use the fact that $\alpha_{i, j}=\boldsymbol{x}_{i}^{\mathrm{T}} \boldsymbol{v}_{j}$ for all $i \in[n]$ and $j \in[d]$ to simplify the expression from Step 1. Finally, you should be able to show that $E=\sum_{j=k+1}^{d}\left\|\boldsymbol{X} \boldsymbol{v}_{j}\right\|_{2}^{2}$.
(2 points)
- Step 3: Prove that $\left\|\boldsymbol{X} \boldsymbol{v}_{j}\right\|_{2}^{2}=\lambda_{j}$ to finish the proof (use the fact that $\boldsymbol{v}_{j}=\boldsymbol{q}_{j}$, and that $\boldsymbol{X}^{\mathrm{T}} \boldsymbol{X}=$ $\left.\boldsymbol{Q} \boldsymbol{D} \boldsymbol{Q}^{\mathrm{T}}\right)$.
(2 points)

[^0](you can use this page to finish the previous PCA question, just in case you run out of space)

## 5 Short answer questions

### 5.1 Decision boundary for decision trees

(3 points)
Consider the decision tree in Fig. 1a. The tree takes $\boldsymbol{x}=\left(x_{1}, x_{2}\right)$ as input, and outputs a label $y \in\{-1,+1\}$. The internal nodes are solid black, the leaves are shaded if the label is -1 , and white if the label is 1 . Draw the decision boundary for this decision tree in Fig. 1b. You can represent -1 as shaded, and 1 as solid white.


Figure 1: Decision boundary for decision trees

### 5.2 Boosting decision stumps

Consider the following dataset with 2-dimensional inputs $\left(x_{1}, x_{2}\right)$ and binary outputs $\{-1,+1\}$.

| Datapoint | Label |
| :--- | :--- |
| $(-2,-1)$ | +1 |
| $(0,0)$ | -1 |
| $(1,-1)$ | +1 |
| $(3,3)$ | +1 |
| $(-2,3)$ | +1 |

Consider running AdaBoost with a decision stump as the base classifier on this dataset. Recall that a decision stump is just a decision tree with a root and two leaves as children. More formally, it is of the form

$$
f(\boldsymbol{x})=\left\{\begin{array}{l}
b_{1}, \text { if } x_{i} \geq \theta  \tag{5}\\
b_{2}, \text { if } x_{i}<\theta
\end{array}\right.
$$

where $b_{1}, b_{2} \in\{-1,+1\}, i \in\{1,2\}$ and $\theta \in \mathbb{R}$. Recall that the boosted classifier at the end of $T$ iterations be given by $f_{\text {boost }}^{(T)}(\boldsymbol{x})=\operatorname{sign}\left(\sum_{t=1}^{T} \beta_{t} f_{t}(\boldsymbol{x})\right)$. Here $f_{t}(\boldsymbol{x})$ is the weak classifier found by the AdaBoost algorithm at the $t^{\text {th }}$ iteration.
(a) Which datapoint(s) will have their weights increased at the end of the first iteration of AdaBoost $(T=1)$ for this dataset? (Hint: You might find it helpful to draw out the dataset. Is it possible to classify
(b) Is it possible for the algorithm to classify all datapoints correctly after $T=2$ iterations? Explain. (Hint: You can reason about it directly, and don't need the formulae for AdaBoost).
(3 points)

## $5.3 n$-gram models for language

Recall that a 3-gram language model uses a second-order Markov assumption to model the data:

$$
P\left(X_{t+1} \mid X_{t}, \ldots, X_{1}\right)=P\left(X_{t+1} \mid X_{t}, X_{t-1}\right)
$$

Suppose we train the second-order Markov model on the following text corpus. (For the purpose of this question, assume that any punctuation marks are part of the word, so "Jude," is one word.)

Hey Jude, don't make it bad. Take a sad song and make it better. Hey Jude, don't be afraid. You were made to go out and get her. Hey Jude, refrain. Don't carry the world upon your shoulders.

We can now use the trained Markov model to predict the distribution of the next word following any sequence of words. What is the distribution of the next word in the following text (to fill in the $\qquad$ ), as predicted by the trained Markov model?

And don't you know that it's just you, hey Jude, you'll do, the movement you need is on your shoulder. Hey Jude, $\qquad$

### 5.4 Neural networks for language modelling

Continuing with the text corpus from the previous question, suppose we now want to train a standard fullyconnected neural network for the task. The network should take the previous two words as input and predict the distribution of the next word.
(a) Describe how to convert the prediction task to a standard supervised ML problem. To do this, describe the input and output which will be used to train the model (you should provide an example of a training datapoint, with the input and desired output).
(b) Write the name, and the mathematical expression for the loss function that we can use to train the model on this task. You can assume that the model has a softmax layer and outputs a probability distribution for the word (let the predicted probability of word $w$ at the $t$-th time step be $\hat{y}_{w}^{(t)}$ ). (Hint: the answer is one of the following: $-\log \hat{y}_{w_{t}}^{(t)}, \log \hat{y}_{w_{t}}^{(t)}, \log \left(1-\hat{y}_{w_{t}}^{(t)}\right),-\log \left(1-\hat{y}_{w_{t}}^{(t)}\right)$, where you also need to say what $w_{t}$ is.)
(2 points)

## 6 Adventures of a CSCI567 graduate: The Saga Continues points)

In the last quiz, we told a few stories about your adventures in the world of ML. This question continues those chronicles.

### 6.1 Evaluating ML models

A rare kind of blood disorder whose consequences are controllable if diagnosed early affects $\mathbf{0 . 1} \%$ of the population. The condition has so far been expensive to diagnose, but you are working on a ML-based approach that uses the result of an inexpensive lab test as features and predicts if the person has the disorder. In which of the following scenarios can you conclude that your ML model is doing a good job? Explain each answer in 1-2 sentences.
(a) The model predicts if a person has the disorder with accuracy $99.9 \%$.
(b) The model predicts if a person has the disorder with precision $0.1 \%$ and recall $100 \%$.
(Hint: Let positive instances refer to the person having the disorder. Then

$$
\begin{aligned}
& \text { Precision }=\frac{\# \text { true positive instances caught by algorithm }(\mathrm{TP})}{\# \text { instances flagged by algorithm as positive }(\mathrm{TP}+\mathrm{FP})}, \\
& \text { Recall }=\frac{\# \text { true positive instances caught by algorithm }(\mathrm{TP})}{\# \text { instances which are positive in the entire data }(\mathrm{TP}+\mathrm{FN})} .
\end{aligned}
$$

Here TP, FP and FN refer to true positive, false positive and false negative respectively.)
(c) The model predicts if a person has the disorder with precision $10 \%$ and recall $90 \%$.

### 6.2 ML advice

As you gain more experience, you start to advise and help other teams with their ML projects. What advice would be provide in the following scenarios? Write your recommendation, along with the explanation (2-3 sentences total).
(a) "I want to build a ML based model to predict if a customer will return a loan. I have collected several features (whether the person took a loan previously, employment status, income etc.) for this task. I want the model to ideally have some interpretability since the customer may demand an explanation for the decision."
(b) "I run a retail website and want to optimize the presentation of items on my website, so that items which are more likely to be purchased draw more attention. I have limited data/features regarding these items at present, but can collect statistics of clicks/purchases of different items. Ideally, the model should improve without manual intervention and get better over time as more users visit the website."

## 7 Multiple choice questions

IMPORTANT: Select ALL options among $\{A, B, C, D\}$ that you think are correct (no justification needed). You get 0.5 point for selecting each correct option and similarly 0.5 point for not selecting each incorrect option. You get 1 additional point for selecting all four options correctly.
(1) Which of the following are best practices for responsible ML?
(A) It is important to identify the right metrics to quantify the performance of the ML model (such as accuracy, precision, recall, performance on sub-groups etc.)
(B) The model may latch onto spurious correlations to make their predictions, so should be tested extensively in use cases which directly impact large populations.
(C) The model should be tested on diverse data which reflects the use cases in deployment.
(D) The model should not be monitored or updated after deployment.

Your answer (select all among A,B,C,D which are true):
(2) Suppose we have a fully-connected neural network with 1 hidden layer with $\operatorname{ReLU}$ activations $(h(a)=$ $\max (0, a))$ for a binary classification task. Which of the following statements are true about the behavior of the network at training and test time?
(A) The total training time is usually the fastest for the smallest possible batch size, since each gradient step takes less time.
(B) Early stopping may lead to poorer training accuracy, but can improve test accuracy.
(C) Adding a momentum term can help the network converge faster, but too much momentum can be harmful.
(D) Multiplying all the weights and biases in the network by a factor of 10 after training the network will not change its classification accuracy.

Your answer (select all among A,B,C,D which are true):
(3) Consider a convolution layer which takes a $10 \times 10 \times 3$ dimensional input and convolves it with 5 filters of size $3 \times 3$ filters with stride 1 and no zero padding. Which of the following statements are true about this layer? (Recall that the output volume as a result of convolving a $N \times N \times 3$ image with one filter of size $F \times F$ with stride $S$ and zero padding $P$ is $D \times D \times 1$ dimensional, where $D=(N+2 P-F) / S+1)$.
(A) The output volume is $8 \times 8 \times 5$ dimensional.
(B) The output volume is $8 \times 8 \times 3$ dimensional.
(C) If the layer was fully connected, it would have more than 10 times as many parameters as currently in the convolution layer.
(D) Without zero-padding the input, we cannot use stride $S=2$ instead of $S=1$ in this layer.

Your answer (select all among A,B,C,D which are true):
(4) Which of the following classifiers could have been used to generate the decision boundary in the binary classification task on the right?
(A) A one hidden layer fully connected neural network with ReLU activation functions $(h(a)=\max (0, a))$.
(B) A one hidden layer fully connected neural network with linear activation functions $(h(a)=a)$.
(C) A three hidden layer fully connected neural network with linear activation functions $(h(a)=a)$.
(D) A decision stump (decision tree of depth 1 ).


Your answer (select all among A,B,C,D which are true):
(5) Consider a binary dataset with 50 positive examples 50 negative examples. Decision stump $\mathcal{T}_{1}$ splits this dataset into two children where the left one has 10 positive examples and 50 negative examples, while another decision stump $\mathcal{T}_{2}$ results in a left child with 0 positive examples and 50 negative examples. Which of the following is correct?
(A) The entropy of the left child of $\mathcal{T}_{1}$ is $\frac{1}{6} \ln 6+\frac{5}{6} \ln \frac{6}{5}$. (Hint: Entropy of a random variable $X$ taking value over some domain $\mathcal{X}$ and having density $p(x)$ is $\left.\sum_{x \in \mathcal{X}} p(x) \log (1 / p(x))\right)$.
(B) The entropy of the right child of $\mathcal{T}_{1}$ is 0 .
(C) The entropy of either child of $\mathcal{T}_{2}$ is the minimum possible entropy for two classes.
(D) Based on conditional entropy, $\mathcal{T}_{2}$ is a better split than $\mathcal{T}_{1}$.

Your answer (select all among A,B,C,D which are true):
(6) Figure 2 shows various training/test classification error curves as parameters for training decision trees are varied. Select all options which represent reasonable relationships between the considered parameters and obtained error(s).


Figure 2: Possible curves for decision trees (select all which are reasonable)
(A) Fig 2a is a reasonable plot of training error as the maximum depth of the decision tree is increased.
(B) Fig 2 b is a reasonable plot of test error as the maximum depth of the decision tree is increased.
(C) Fig 2c is a reasonable plot of training error as the minimum number of samples to be a leaf node is increased.
(D) Fig 2d is a reasonable plot of training \& test errors as the total size of the training set used to train a decision tree with maximum depth 5 is increased.
Your answer (select all among A,B,C,D which are true):
(7) Consider the problem of learning a mixture of $k=2$ Gaussians on some one-dimensional data. Let the mean, covariance and clusters weight of the two Gaussians be $\mu_{j}, \sigma_{j}$ and $\pi_{j}$ (respectively), for $j \in\{1,2\}$. Which of the following statements are true about the problem?
(A) The problem of finding the parameters which maximize the log-likelihood is non-concave.
(B) Suppose EM finds the parameters $\mu_{1}=-1, \sigma_{1}=1, \pi_{1}=0.8$ and $\mu_{2}=1, \sigma_{2}=1, \pi_{2}=0.2$. Then for a datapoint with $x=0$ (equidistant from the two centers), its posterior probability of being in cluster 1 is 0.5 .
(C) The learned GMM can be used to flag outliers/anomalies in the data.
(D) The learned GMM can be used to generate synthetic data.

Your answer (select all among A,B,C,D which are true):
(8) Figure 3 shows executions of the EM algorithm with different values of the number of Gaussian components $k$ and different initializations. The code is generated using the same demo as shown in class: the histogram of the data is in blue, the true density is given by the dashed red line and the model learned by EM is given by the solid green line. In which of the figures is it possible that the EM algorithm has converged?


Figure 3: EM algorithm runs

Your answer (select all among A,B,C,D where EM has possibly converged):
(9) Which of the following statements are true about Principal Component Analysis (PCA)?
(A) In PCA, the first principal component is the direction where the projection of the dataset has the largest variance.
(B) In Fig. 4a, the red line represents the first principal component of the data.
(C) PCA will not work very well to discover the underlying structure for the dataset in Fig. 4b.
(D) The results of PCA are invariant to re-scaling the coordinates of the data.

(a) Centered data with candidate first principal component in red.

(b) Data with some underlying structure given by the blue and orange points.

Figure 4: Datasets for PCA

Your answer (select all among A,B,C,D which are true):
(10) Consider the dataset of 5 examples shown in Table 1. Each example corresponds to an email and has two features "Domain" and "Length", and one label "Label", which denotes or not that email was spam. All columns all have two possible values: "internal" or "external" for Domain, "long" or "short" for Length, and "not spam" or "spam" for Label.

| $i$ | Domain | Length | Label |
| :---: | :---: | :---: | :---: |
| 1 | internal | long | not spam |
| 2 | internal | short | not spam |
| 3 | external | short | not spam |
| 4 | external | long | spam |
| 5 | external | long | spam |

Table 1: Training set for Naive Bayes
Which of the following statements are true about Naive Bayes applied to this data? (Hint: Naive Bayes predicts using $\operatorname{argmax}_{j} p(\boldsymbol{x}, y=j)$, where the Naive Bayes assumption is then used to expand out the joint probability).
(A) $p(\mathrm{~L}=$ "spam" $)=2 / 5$.
(B) $p($ Domain="internal" $\mid \mathrm{L}=$ "spam" $)=0$.
(C) A new datapoint with Domain="external" and Length="short" is classified as "spam".
(D) A new datapoint with Domain="internal" and Length="long" is classified as "spam".

Your answer (select all among A,B,C,D which are true):


[^0]:    ${ }^{1}$ You can also attempt a completely different proof, but will get limited partial credits for incomplete or incorrect attempts.

