## CS480/680: Introduction to Machine Learning

Homework 4

Due: 11:59 pm, July 23, 2021, submit on CrowdMark.

Submit your writeup in pdf and all source code in a zip file (with proper documentation). Write a script for each programming exercise so that the TAs can easily run and verify your results. Make sure your code runs!

[Text in square brackets are hints that can be ignored.]

## Exercise 1: Gaussian Mixture Model (GMM) (10 pts)

**Notation**: For a matrix A, |A| denotes its determinant. For a diagonal matrix diag(s),  $|\operatorname{diag}(s)| = \prod_i s_i$ .

```
Algorithm 1: EM for GMM.
    Input: X \in \mathbb{R}^{n \times d}, K \in \mathbb{N}, initialization for model
    // model includes \pi \in \mathbb{R}_+^K and for each 1 \leq k \leq K, m{\mu}_k \in \mathbb{R}^d and S_k \in \mathbb{S}_+^d
    // \pi_k \geq 0, \sum_{k=1}^K \pi_k = 1, S_k symmetric and positive definite.
    // random initialization suffices for full credit.
    // alternatively, can initialize r by randomly assigning each data to one of the K
          components
    Output: model, \ell
 1 for iter = 1: Maxiter do
         // step 2, for each i = 1, \ldots, n
         for k = 1, \ldots, K do
 2
           [r_{ik} \leftarrow \pi_k | S_k |^{-1/2} \exp[-\frac{1}{2} (\mathbf{x}_i - \boldsymbol{\mu}_k)^{\top} S_k^{-1} (\mathbf{x}_i - \boldsymbol{\mu}_k)] 
                                                                                                              // compute responsibility
         // for each i=1,\ldots,n
         r_{i.} \leftarrow \sum_{k=1}^{K} r_{ik}
         // for each k=1,\ldots,K and i=1,\ldots,n
                                                                                                                                      // normalize
         r_{ik} \leftarrow r_{ik}/r_{i}
          // compute negative log-likelihood
         \ell(iter) = -\sum_{i=1}^{n} \log(r_{i.})
 6
         if iter > 1 && |\ell(iter) - \ell(iter - 1)| \le \text{TOL} * |\ell(iter)| then
 7
           break
          // step 1, for each k=1,\ldots,K
         r_{.k} \leftarrow \sum_{i=1}^{n} r_{ik}
 9
         \pi_k \leftarrow r_{.k}/n
10
         \begin{aligned} & \boldsymbol{\mu}_k^n = \sum_{i=1}^n r_{ik} \mathbf{x}_i / r_{.k} \\ & S_k \leftarrow \left( \sum_{i=1}^n r_{ik} \mathbf{x}_i \mathbf{x}_i^\top / r_{.k} \right) - \boldsymbol{\mu}_k \boldsymbol{\mu}_k^\top \end{aligned}
11
```

a) (5 pts) Derive and implement the EM algorithm for the diagonal Gaussian mixture model, where all covariance matrices are constrained to be diagonal. Algorithm 1 recaps all the essential steps and serves as a hint rather than a verbatim instruction. In particular, you must change the highlighted steps accordingly (with each  $S_k$  being a diagonal matrix), along with formal explanations. Analyze the space and time complexity of your implementation.

[You might want to review the steps we took in class for a simpler case, and ensure you can derive the updates in Algorithm 1. Then adapt the steps to the simpler diagonal case. The solution should look like  $s_j = \frac{\sum_{i=1}^n r_{ik}(x_{ij} - \mu_j)^2}{\sum_{i=1}^n r_{ik}} = \frac{\sum_{i=1}^n r_{ik}x_{ij}^2}{\sum_{i=1}^n r_{ik}} - \mu_j^2$  for the *j*-th diagonal. Multiplying an  $n \times p$  matrix with a  $p \times m$  matrix costs O(mnp). Do not maintain a diagonal matrix explicitly; using a vector for its diagonal suffices.

[Warning: Either in this part or the next one, you may run into issues involving NaNs. You will have to diagnose these issues and fix them.]

To stop the algorithm, set a maximum number of iterations (say MAXITER = 500) and also monitor the

change of the negative log-likelihood  $\ell$ :

$$\ell = -\sum_{i=1}^{n} \log \left[ \sum_{k=1}^{K} \pi_k |2\pi S_k|^{-1/2} \exp\left[-\frac{1}{2} (\mathbf{x}_i - \boldsymbol{\mu}_k)^{\top} S_k^{-1} (\mathbf{x}_i - \boldsymbol{\mu}_k)\right] \right], \tag{1}$$

where  $\mathbf{x}_i$  is the *i*-th column of  $X^{\top}$ . As a debug tool, note that  $\ell$  should decrease from step to step, and we can stop the algorithm if the decrease is smaller than a predefined threshold, say  $TOL = 10^{-5}$ .

Run your algorithm on  $gmm_dataset.csv$ , for k=1 to 10. Generate a plot with k on the x-axis and the negative log-likelihood of the data under the final trained model on the y-axis. What do you think the most appropriate choice of k is? Explain and justify how and why you chose this value. [You may want to focus on more than just maximizing the log-likelihood.] For your chosen value of k, report the parameters (mixing weights, mean vectors, and vectors corresponding to the diagonals of the covariance matrices) of your trained model. When reporting them, sort the components in increasing order of mixing weights.

## Ans:

Derive the EM algorithm for the diagnoal Gaussian mixture model: First of all, the probability density function of a given vector x in n-dimension is:

$$p(x) = \frac{1}{(2\pi)^{\frac{n}{2}} |S_k|^{\frac{1}{2}}} \exp[-\frac{1}{2} (\mathbf{x} - \boldsymbol{\mu})^{\top} S_k^{-1} (\mathbf{x} - \boldsymbol{\mu})]$$

And we know that the Mixture-of-Gaussian distribution can be written as:

$$PM(x) = \sum_{i=1}^{k} \alpha_i * p(x|\mu, S_k)$$

Since the sum of coefficients should be 1 (they represents the probability of chosen the ith component) and the coefficient should larger than 0, we can rewritten the two equation above to get the response:

$$r_{ik} = \pi_k |S_k|^{-1/2} \exp\left[-\frac{1}{2}(\mathbf{x}_i - \boldsymbol{\mu}_k)^{\top} S_k^{-1}(\mathbf{x}_i - \boldsymbol{\mu}_k)\right]$$

where  $\pi_k \geq 0$ ,  $\sum_{k=1}^K \pi_k = 1$ . Then, we do the normalization to  $r_{ik}$ :

$$r_{ik} = \frac{r_{ik}}{\sum_{j=1}^{K} r_{jk}}$$

To solve PM(x), we can use maximum likelihood estimation:

$$LL(D) = \ln(\prod_{i=1}^{n} PM(x_i))$$
$$= \sum_{i=1}^{n} \ln(\sum_{k=1}^{k} \pi_k * p(x_i | \mu_k, S_k))$$

To maximize, we will have  $\frac{\partial LL(D)}{\partial \mu_k} = 0$ :

$$\sum_{i=1}^{n} \frac{\pi_k * p(x_i | \mu_k, S_k)}{\sum_{l=1}^{k} \pi_l * p(x_i | \mu_l, S_l)} (x_i - u_i) = 0$$

Rewrite the equation:

$$\sum_{i=1}^{n} r_{ik}(x_i - \mu_k) = 0$$

$$\mu_k = \frac{\sum_{i=1}^{n} r_{ik} x_i}{\sum_{i=1}^{n} r_{ik}}$$

$$= \frac{\sum_{i=1}^{n} r_{ik} x_i}{r_{.k}}$$

Since we also need to satisfy  $\pi_k \geq 0$ ,  $\sum_{i=1}^k \pi_k = 1$ . Using the Lagrange:

$$\frac{\partial LL(D)}{\partial \pi_k} + \frac{\partial \lambda(\sum_{i=1}^k \pi_k - 1)}{\partial \pi_k} = 0$$
$$\sum_{i=1}^n \frac{p(x_i|\mu_k, S_k)}{\sum_{l=1}^k \pi_l * p(x_i|\mu_l, S_l)} + \lambda = 0$$

We multiply  $pi_k$  on both side:

$$\sum_{i=1}^{n} r_{ik} - n\pi_k = 0$$
$$\pi_k = \frac{1}{n} \sum_{i=1}^{n} r_{ik} = \frac{r_{.k}}{n}$$

Finally, we get  $S_k$  (from how we compute the covarince matrix):

$$S_k = \frac{\sum_{i=1}^n r_{ik} (x_i - \mu_k) (x_i - \mu_k)^\top}{\sum_{i=1}^n r_{ik}}$$

Simplify this equation, we can get:

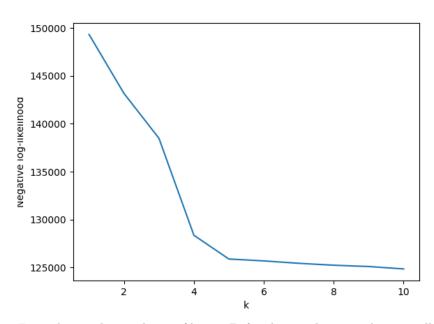
$$S_k = \frac{\sum_{i=1}^n r_{ik} x_{ij}^2}{\sum_{i=1}^n r_{ik}} - \mu_j^2$$

Space complexity: n \* k + k \* d \* d + k \* d

Which came from responsibility  $r_{ik}$ ,  $S_k$  and mean, respectively.

Time complexity:  $O(2 * n_{iter} * k)$ 

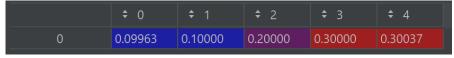
My code uses dynamic programming to record all the responsibility in compute\_log\_likelihood(), which use a for loop in range of k. I call this function in estep() to get the log\_likelihood. And I call estep() in fit() with in a for loop of n\_iter, so  $O(n_{iter} * k)$  for now. I also call mstep() in the for loop, which consists of a for loop of k, where I update  $S_k$ . Thus, the time complexity is  $O(2 * n_{iter} * k)$ .



From the graph, my choice of k is 5. Before k = 5, there is a dramatically drop in negative log likelihood. After that, negative log likelihood just gradually drops. Thus, k = 5 is a turning point and we kind of want this in GMM, a balance of loss and the number of clusters exist.

 $Parameters: (random\ seed\ =\ 24)$ 

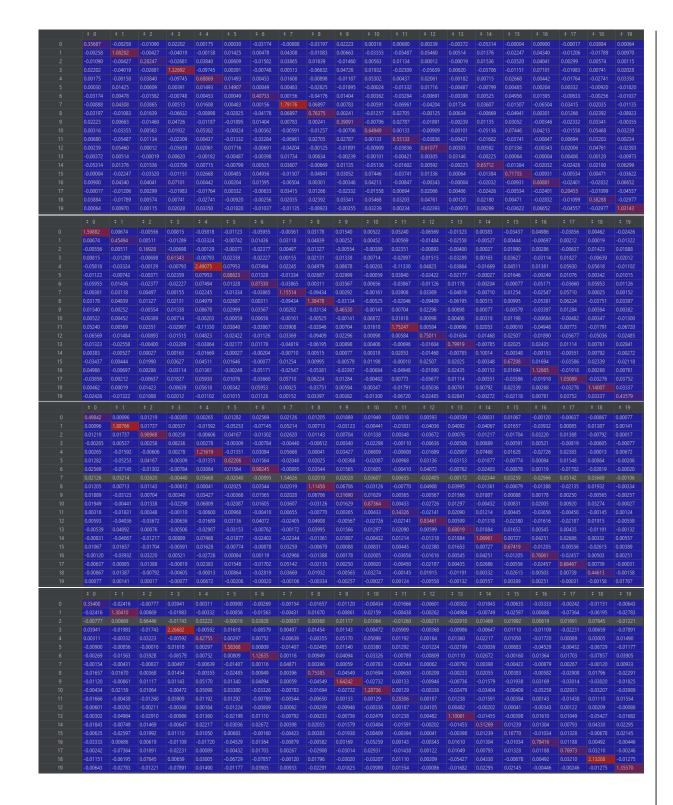
mixing weights:



mean vectors:																		
0																		
1																		
2											-0.89480							
3	-0.66420						-1.64448		-0.94520						0.43648			0.05545
4									-1.05649									0.39975

diagnoals of the covariance matrices:





b) (5 pts) Next, we apply (the adapted) Algorithm 1 in part a) to the MNIST dataset. For each of the 10 classes (digits), we can use its (only its) training images to estimate its (class-conditional) distribution by fitting a GMM (with say K = 5, roughly corresponding to 5 styles of writing this digit). This gives us the density estimate  $p(\mathbf{x}|y)$  where  $\mathbf{x}$  is an image (of some digit) and y is the class (digit). We can now

classify the test set using the Bayes classifier:

$$\hat{y}(\mathbf{x}) = \arg\max_{c=0,\dots,9} \quad \underbrace{\Pr(Y=c) \cdot p(X=\mathbf{x}|Y=c)}_{\propto \Pr(Y=c|X=\mathbf{x})},\tag{2}$$

where the probabilities  $\Pr(Y=c)$  can be estimated using the training set, e.g., the proportion of the c-th class in the training set, and the density  $p(X=\mathbf{x}|Y=c)$  is estimated using GMM for each class c separately. Report your error rate on the test set as a function of K (if time is a concern, using K=5 will receive full credit).

[Optional: Reduce dimension by PCA may boost accuracy quite a bit. Your running time should be on the order of minutes (for one K), if you do not introduce extra for-loops in Algorithm 1.]

[In case you are wondering, our classification procedure above belongs to the so-called plug-in estimators (plug the estimated densities to the known optimal Bayes classifier). However, note that estimating the density  $p(X = \mathbf{x}|Y = c)$  is actually harder than classification. Solving a problem (e.g. classification) through some intermediate harder problem (e.g. density estimation) is almost always a bad idea.]

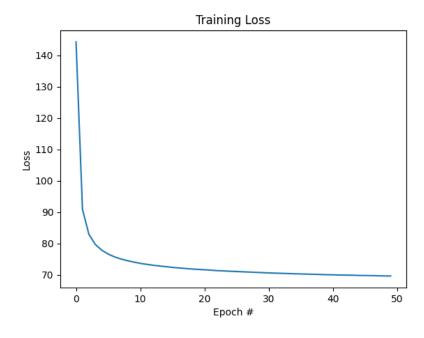
Ans: I have implement PCA of dimension = 20, and the test accuracy is 0.9627 for K=5 (error rate: 0.0373).

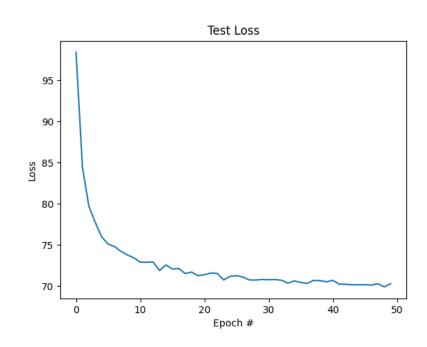
## Exercise 2: VAEs and GANs (10 pts)

Code provided for this exercise is assuming a PyTorch solution, you may change it as necessary if you prefer to use TensorFlow or JAX. You may find this tutorial for GANs helpful.

a (4.5 pts) Complete the implementation of a VAE in vae.py. In your solution writeup, include the two produced graphs (corresponding to the training and test sets), with the epoch number on x-axis and the loss on the y-axis. Further include the produced samples from every 10th epoch (after epochs 10, 20, 30, 40, and 50).

Ans:







10 epochs



20 epochs



30 epochs



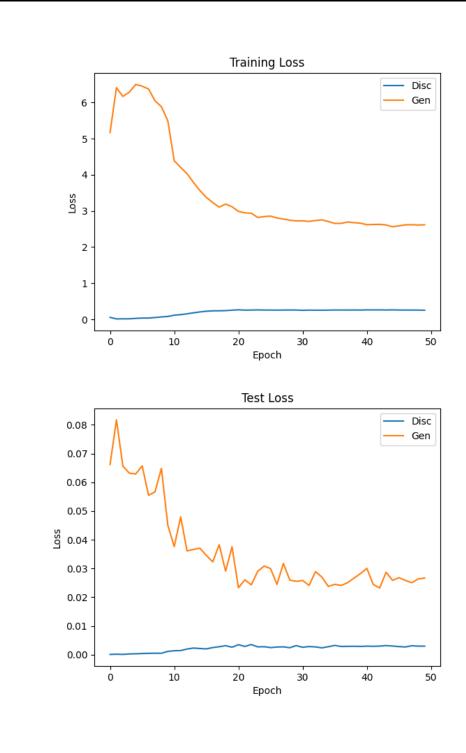
40 epochs

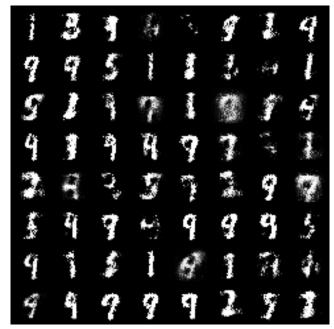


50 epochs

b (4.5 pts) Complete the implementation of a GAN in gan.py. In your solution writeup, include the two produced graphs (corresponding to the training and test sets), with the epoch number on x-axis and the losses (both generator and discriminator) on the y-axis. Further include the produced samples from every 10th epoch (after epochs 10, 20, 30, 40, and 50).

Ans:





10 epochs



20 epochs



30 epochs



40 epochs



50 epochs

c (1 pt) Describe, compare, and constrast your produced results and experiences with GANs and VAEs in this exercise.

Ans: For VAEs' results, the training loss and test loss decrease rapidly in first few epochs, then gradually decreases (with small fluctuations in test loss) during the rest epochs. Basically, the VAE loss plots show the model is well trained and not suffering from overfitting. While in GAN's loss curves, for training, the generator loss rises at the beginning and starts decreasing at around epoch 10. Again, it rapidly decreases in the next few epochs then gradually decreases. This can be interpreted as that the images generated by generator cannot fool the discriminator at the beginning, as we trained it more, it gradually generate images that can fool the discriminator (which is what we want, faked real images), so the generator loss goes down. For the discriminator loss, it is relatively low at the beginning compared to the generator loss, and only gain very little increase during 50 epochs. This can be interpreted as the discriminator is good at distinguishing the real images from the fake images at first (which should be easy at first). Then our generator keep generated more "realistic" fake images which sometimes fool the discriminator, so the loss goes up but not to very high because our discriminator is still learning and try to be capable doing its job. That's why it is called adversarial learning. The disc and gen loss for test is basically the same trend but with more fluctuations.

Regarding to the images VAE and GAN generated, VAE can generate different numbers, but for many of them, it is kind of hard for a human to tell what the number is. Besides, some of them are even not numbers to me, they are very weird symbols. While for GAN, the numbers it generated are most 1 and 9, as these numbers could be easier to fool the discriminator as I imaged. We can still see 3, 4, 5, 7, 8 as well. There are some blur and meaningless symbol as well, but for the numbers I can recognized, they are more clear compared to VAE's.

For the experience with VAE and GAN, I think VAE is relatively simpler to implement, while for GAN, you have to notice many details, such as how generator loss and discriminator loss is calculated; when calculating discriminator loss, there are two parts: the loss to tell the real is real and the loss to tell fake is fake; when pass the generated data into the discriminator to get the fake loss, we have to add .detach() so that the loss will not back-propagated. We want to do this because we are not training the generator but the discriminator. We have to be more careful to details like those when implementing GAN.