

CS 446 MJT — Homework 5

junzhew3haoruans8

Version 1

Instructions.

- Homework is due **Tuesday, April 16, at 11:59pm**; no late homework accepted.
- Everyone must submit individually at Gradescope under **hw5** and **hw5code**.
- The “written” submission at **hw5** **must be typed**, and submitted in any format Gradescope accepts (to be safe, submit a PDF). You may use L^AT_EX, markdown, google docs, MS word, whatever you like; but it must be typed!
- When submitting at **hw5**, Gradescope will ask you to mark out boxes around each of your answers; please do this precisely!
- Please make sure your NetID is clear and large on the first page of the homework.
- Your solution **must** be written in your own words. Please see the course webpage for full academic integrity information. Briefly, you may have high-level discussions with at most 3 classmates, whose NetIDs you should place on the first page of your solutions, and you should cite any external reference you use; despite all this, your solution must be written in your own words.
- We reserve the right to reduce the auto-graded score for **hw5code** if we detect funny business (e.g., rather than implementing an algorithm, you keep re-submitting the assignment to the auto-grader, eventually completing a binary search for the answers).
- There are **no regrade requests** on **hw5code**, which is the code auto-grader; however, you can re-submit and re-grade as many times as you like before the deadline! Start early and report any issues on piazza!
- Methods and functions in the template and utility code include docstrings describing the inputs and outputs. The autograder relies on correct implementations of these methods. Follow the docstrings to avoid failing tests.
- In this homework, you cannot use any of the SciPy or SciKit methods. Importing these libraries or their sublibraries, except for those already imported in **hw5_utils.py** will raise an error.

1. k -means and PCA.

Let $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n \in \mathbb{R}^d$ be n data points in a k -means problem. Let $\mathbf{X} \in \mathbb{R}^{n \times d}$ denote the data matrix with rows $\mathbf{x}_1^\top, \dots, \mathbf{x}_n^\top$. For centers $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \dots, \boldsymbol{\mu}_k \in \mathbb{R}^d$, define the matrix \mathbf{C} with the centers as its rows. Let $\mathbf{A} \in \{0, 1\}^{n \times k}$ denote an assignment matrix, meaning there is a single 1 per row, and all other entries are zeros. The notation $\mathcal{C}_{d,k} = \mathbb{R}^{k \times d}$ for matrices of k centers in d dimensions, and the notation $\mathcal{A}_{n,k} \subseteq \{0, 1\}^{n \times k}$ for all possible assignment matrices. Let $\mathbf{X} = \mathbf{U}\mathbf{S}\mathbf{V}^\top$ be the full singular value decomposition of \mathbf{X} with the diagonal of \mathbf{S} being sorted in decreasing order. Define \mathbf{V}_l as the first l columns of \mathbf{V} , corresponding to the l largest singular values.

(a) Prove that for any orthonormal matrix \mathbf{M} ,

$$\|\mathbf{X} - \mathbf{AC}\|_{\text{F}}^2 = \|(\mathbf{X} - \mathbf{AC})\mathbf{M}\mathbf{M}^\top\|_{\text{F}}^2 + \|(\mathbf{X} - \mathbf{AC})(\mathbf{I} - \mathbf{M}\mathbf{M}^\top)\|_{\text{F}}^2.$$

(b) Prove that for any fixed assignment matrix \mathbf{A} , the row space of the optimal \mathbf{C} is a subset of the row space of \mathbf{X} .

Hint. The matrix \mathbf{V}_r is orthonormal, where r denotes rank of \mathbf{X} .

(c) Prove that $\|\mathbf{X} - \mathbf{AC}\|_{\text{F}}^2 \geq \sum_{i=k+1}^r s_i^2$, for any assignment matrix and any choice of the k centers, where $(s_i)_i$ is the decreasing sequence of singular values of \mathbf{X} .

(d) Let $(\mathbf{A}_l, \mathbf{C}_l) = \arg \min_{\substack{\mathbf{A} \in \mathcal{A}_{n,k} \\ \mathbf{C} \in \mathcal{C}_{d,k}}} \|\mathbf{X}\mathbf{V}_l\mathbf{V}_l^\top - \mathbf{AC}\|_{\text{F}}^2$. Then

$$\|\mathbf{X}\mathbf{V}_l\mathbf{V}_l^\top - \mathbf{A}_l\mathbf{C}_l\|_{\text{F}}^2 \leq \min_{\substack{\mathbf{A} \in \mathcal{A}_{n,k} \\ \mathbf{C} \in \mathcal{C}_{d,k}}} \|\mathbf{X} - \mathbf{AC}\|_{\text{F}}^2 \leq \|\mathbf{X}\mathbf{V}_l\mathbf{V}_l^\top - \mathbf{A}_l\mathbf{C}_l\|_{\text{F}}^2 + \sum_{i=l+1}^r s_i^2.$$

Remark. This means that if PCA down to some dimension doesn't incur too much error, then we can solve k -means there without things changing too much.

Solution. (Your solution here.)

(a) Set $\mathbf{X} - \mathbf{AC} = \mathbf{N}$, so $\|\mathbf{X} - \mathbf{AC}\|_{\text{F}}^2 = \|\mathbf{N}\|_{\text{F}}^2 = \text{tr}(\mathbf{N}\mathbf{N}^\top)$

\mathbf{M} is orthonormal, $\mathbf{M}^\top\mathbf{M} = \mathbf{I}$. So:

$$\|(\mathbf{X} - \mathbf{AC})\mathbf{M}\mathbf{M}^\top\|_{\text{F}}^2 = \text{tr}(\mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) = \text{tr}(\mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) \quad (1)$$

$$\|(\mathbf{X} - \mathbf{AC})(\mathbf{I} - \mathbf{M}\mathbf{M}^\top)\|_{\text{F}}^2 = \text{tr}((\mathbf{N} - \mathbf{N}\mathbf{M}\mathbf{M}^\top)(\mathbf{N}^\top - \mathbf{M}\mathbf{M}^\top\mathbf{N}^\top)) \quad (2)$$

$$= \text{tr}(\mathbf{N}\mathbf{N}^\top - \mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top - \mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top + \mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) = \text{tr}(\mathbf{N}\mathbf{N}^\top - \mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) \quad (3)$$

So:

$$\|(\mathbf{X} - \mathbf{AC})\mathbf{M}\mathbf{M}^\top\|_{\text{F}}^2 + \|(\mathbf{X} - \mathbf{AC})(\mathbf{I} - \mathbf{M}\mathbf{M}^\top)\|_{\text{F}}^2 = \text{tr}(\mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) + \text{tr}(\mathbf{N}\mathbf{N}^\top - \mathbf{N}\mathbf{M}\mathbf{M}^\top\mathbf{N}^\top) \quad (4)$$

$$= \text{tr}(\mathbf{N}\mathbf{N}^\top) = \|\mathbf{N}\|_{\text{F}}^2 = \|\mathbf{X} - \mathbf{AC}\|_{\text{F}}^2 \quad (5)$$

So it is proved.

(b) According to the proof in the kmeans slide:

$$\min_{C \in \mathcal{C}_{d,k}} \phi(C; \mathbf{A}) = \sum_{j=1}^k \min_{\mu_j \in \mathbb{R}^d} \sum_{i=1}^n A_{ij} \|\mathbf{x}_i - \mu_j\| \quad (6)$$

Taking the gradient with respect to μ_j and setting to 0:

$$\sum_{i=1}^n 2A_{i,j} (\mathbf{x}_i - \mu_j) = 0, \text{ so } \mu_j = \frac{\sum_{i=1}^n \mathbf{x}_i \mathbb{1}_{[A_{ij}=1]}}{\sum_{i=1}^n \mathbb{1}_{[A_{ij}=1]}} = \text{mean}(\{\mathbf{x}_i : A_{ij} = 1\}) \quad (7)$$

So the row space $\mu_1, \mu_2, \dots, \mu_k \in \mathbb{R}^d$ of the optimal C is the mean of points in X with common assignment. So for any fixed assignment matrix A , the row space of the optimal C is a subset of the row space of X .

(c) Since $r(A) \leq k$ and $r(C) \leq k$, $r(AC) \leq k$.

since $X = USV^\top$, We assume rank k approximation to X is given by $X_k = \sum_{i=1}^k s_i u_i v_i^\top$

By the triangle inequality with the spectral norm, we can know that if $X = X' + X''$ then

$s_1(X) \leq s_1(X') + s_1(X'')$. Suppose X'_k and X''_k respectively denote the rank k

approximation to X' and X'' . So for any $i, j \geq 1$:

$$\begin{aligned} s_i(X') + s_j(X'') &= s_1(X' - X'_{i-1}) + s_1(X'' - X''_{j-1}) \\ &\geq s_1(X - X'_{i-1} - X''_{j-1}) \\ &\geq s_1(X - X_{i+j-2}) \left(\text{rank}(X'_{i-1} + X''_{j-1}) \leq \text{rank}(X_{i+j-2}) \right) \\ &\geq s_{i+j-1}(X) \end{aligned}$$

since $r(AC) \leq k$, $s_{k+1}(AC) = 0$. So we can set $X' = X - AC$ and $X'' = AC$, and for

$i \geq 1, j = k + 1$: $s_i(X - AC) \geq s_{k+i}(X)$. So:

$$\|X - AC\|_F^2 = \sum_{i=1}^r s_i(X - AC)^2 \geq \sum_{i=k+1}^r s_i(X)^2 = \sum_{i=k+1}^r s_i^2 \quad (8)$$

So the problem is proved.

(d) Since the row space of the optimal C is a subset of the row space of X and the A, C are optimal,

$$CV_l V_l^\top = C$$

Since V_l is orthonormal, using the conclusion from problem (a):

$$\begin{aligned} \min_{\substack{A \in \mathcal{A}_{n,k} \\ C \in \mathcal{C}_{d,k}}} \|X - AC\|_F^2 &= \min_{\substack{A \in \mathcal{A}_{n,k} \\ C \in \mathcal{C}_{d,k}}} \left\| (X - AC) V_l V_l^\top \right\|_F^2 + \min_{\substack{A \in \mathcal{A}_{n,k} \\ C \in \mathcal{C}_{d,k}}} \left\| (X - AC) (I - V_l V_l^\top) \right\|_F^2 \\ &\geq \min_{\substack{A \in \mathcal{A}_{n,k} \\ C \in \mathcal{C}_{d,k}}} \left\| (X - AC) V_l V_l^\top \right\|_F^2 = \min_{\substack{A \in \mathcal{A}_{n,k} \\ C \in \mathcal{C}_{d,k}}} \left\| X V_l V_l^\top - A C V_l V_l^\top \right\|_F^2 \\ &= \|X V_l V_l^\top - A_l C_l\|_F^2 \end{aligned}$$

Moreover:

$$\begin{aligned}
\min_{A \in \mathcal{A}_{\mathcal{A},k}} \|\mathbf{X} - \mathbf{A}\mathbf{C}\|_F^2 &\leq \|\mathbf{X} - \mathbf{A}_l \mathbf{C}_l\|_F^2 \\
&= \left\| \mathbf{X} - \mathbf{X} \mathbf{V}_l \mathbf{V}_l^\top + \mathbf{X} \mathbf{V}_l \mathbf{V}_l^\top - \mathbf{A}_l \mathbf{C}_l \right\|_F^2 \\
&\leq \left\| \mathbf{X} - \mathbf{X} \mathbf{V}_l \mathbf{V}_l^\top \right\|_F^2 + \left\| \mathbf{X} \mathbf{V}_l \mathbf{V}_l^\top - \mathbf{A}_l \mathbf{C}_l \right\|_F^2 \quad \text{So the problem is proved.} \\
&= \left\| \mathbf{X} \mathbf{V}_l \mathbf{V}_l^\top - \mathbf{A}_l \mathbf{C}_l \right\|_F^2 + \sum_{i=l+1}^r s_i^2
\end{aligned}$$

2. k -means.

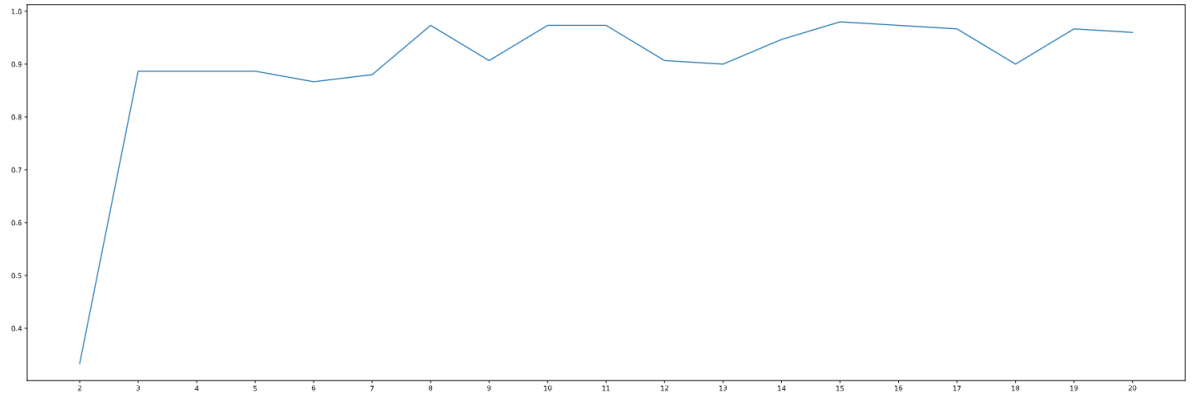
In this problem you will deal with the Iris dataset by Ronald Fisher. The dataset consists of measurements of various classes of Iris flowers and the goal is to group the points into classes. The dataset provides four features of the flowers. They are sepal length, sepal width, petal length and petal width, respectively, measured in centimeters. You can access these data by calling the method `load_iris_data()`. The function returns two NumPy arrays of shape $(150, 4)$ and $(150, 1)$. The first array contains 150 datapoints with 4 features each and the latter array contains the corresponding label of datapoints. Note that your solution is not allowed to directly invoke `sklearn` or `scipy`.

- (a) Implement Lloyd's method inside the `k_means(X, k)` method, which takes as input a NumPy array of shape (n, d) of n datapoints of dimension d and a positive integer k . The method should return a $k \times d$ matrix in which each row corresponds to one of the k centers. For the initialization, use a random (valid) assignment matrix. You don't need to write anything in the hand-in solutions for this part.
- (b) Implement the `get_purity_score(X, Y, C)` method. The method takes a data matrix \mathbf{X} of shape (n, d) , a label array \mathbf{Y} of shape $(n, 1)$, and a matrix \mathbf{C} of shape (k, d) with rows corresponding to the k centers. The purity score of a clustering is defined as the percentage of data points whose label matches the plurality label of the cluster they are placed in. The function should return a number in range $[0, 1]$, that is the purity score of the clustering induced on \mathbf{X} by the centers \mathbf{C} . Ties can be broken arbitrarily. You don't need to write anything in the hand-in solutions for this part.
- (c) Load the Iris dataset using the `load_iris_data()` method and apply your implementation of k -means to it with different values of k . Plot the purity score of the classification as a function of k . You can use the `line_plot(data1, ..., min_k=2, output_file='plot.pdf')` to draw the plot. This method takes as input an array of purity scores and prints the corresponding line plot to a PDF file. The optional argument `min_k` indicates the first label along the x axis and `output_file` indicates the output file location. Describe the behavior of purity score as k increases. At what point does purity reach 1?
- (d) In the next three parts, you will use k -means centers to learn features of a dataset. For a data matrix \mathbf{X} of shape (n, d) and centers matrix \mathbf{C} of shape (k, d) , let \mathbf{A} be the (n, k) matrix of assignments in the i -th row equals e_j^\top if the j -th center is the closest center to the i -th datapoint. You may break ties arbitrarily. Run the `logistic_regression(X, Y)` method given in `hw5_utils.py` on the rows of \mathbf{A} . The output of the function is of type `sklearn.linear_model.LogisticRegression` and in particular supports the method `predict_proba(x)` that returns the probability of a given data point \mathbf{x} having each of the four labels. See the documentation at https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LogisticRegression.html. Implement the function `classify_using_k_means(X, Y, k)` that takes and input the data matrix \mathbf{X} and labels \mathbf{Y} and the integer k indicating the number of centers, and returns a function f that takes a point $x \in \mathbb{R}^d$ and returns a label in $\{0, 1, 2, 3\}$. You don't need to write anything in the hand-in solutions for this part.
- (e) In this part you will repeat the previous problem, except instead of the matrix \mathbf{A} , you should construct the matrix \mathbf{A}_l that has exactly l ones in each row i , that correspond to the l closest centers to the i -th datapoint. Ties can be broken arbitrarily. Implement `classify_using_k_means(X, Y, k, l=1)` as in the previous part, for all positive integer l . You don't need to write anything in the hand-in solutions for this part.
- (f) The method `load_iris_data(ratio=0)` takes a value `ratio` in range $[0, 1]$ and returns the matrices $\mathbf{X}_{\text{train}}$, \mathbf{X}_{test} , $\mathbf{Y}_{\text{train}}$ and \mathbf{Y}_{test} where \mathbf{X}_{test} , \mathbf{Y}_{test} is a test set with $\lfloor n \times \text{ratio} \rfloor$ points and $\mathbf{X}_{\text{train}}$, $\mathbf{Y}_{\text{train}}$ is the training dataset and contains the rest the points. Use this method to train a classifiers using `classify_using_k_means(X, Y, k, 1)` with training/test ratio of 0.8 and $k \in 2, 3, \dots, 20$. Plot the training error and test error of the classifier against k once for $l = 1$ and once for $l = 3$, and describe your explanation for the trends in a few sentences. Again, you can use the method `line_plot(data1, ..., min_k=2, output_file='plot.pdf')` to plot the data.

- (g) Train a k -means model with 4 centers. Plot the data and group them by the closest center. To draw the plot, you can use the method `scatter_plot_2d_project(X1, ..., output_file='output.pdf', ncol=3)`. This method takes multiple matrices $X1, \dots$ of size $n_i \times d$ each corresponding to one cluster. It generates $\binom{d}{2}$ plots, one for every pair of dimensions. The output is then saved to the file indicated by `output_file`.

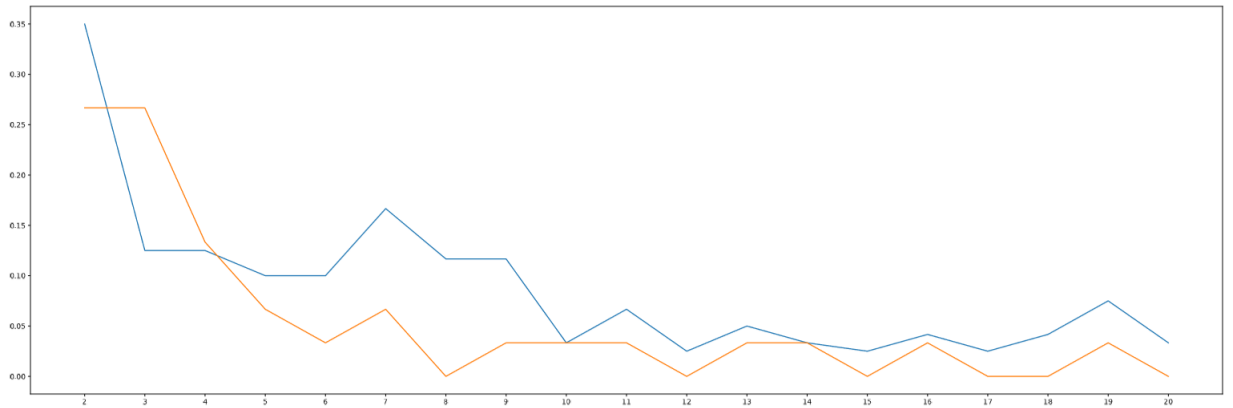
Solution. *(Your solution here.)*

(c)

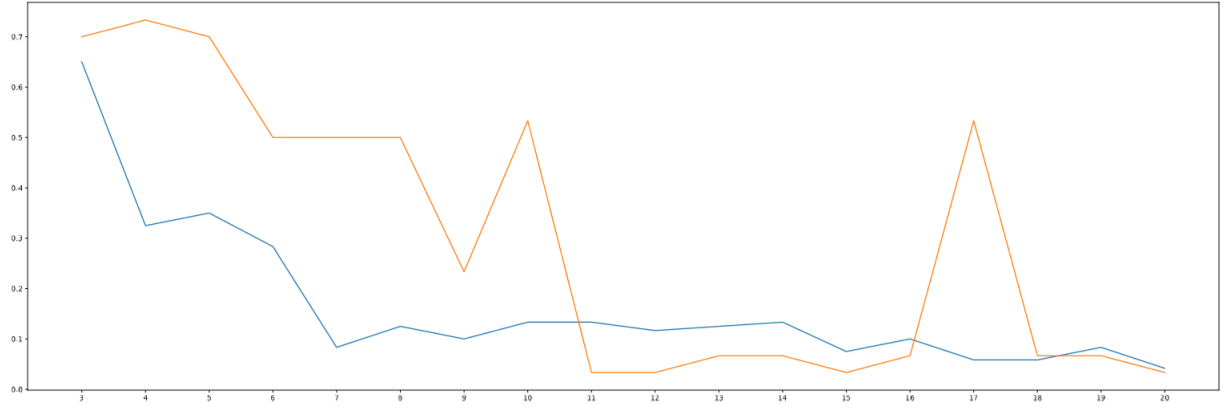


The purity scores fluctuate since the random initialization in the k -means algorithm. Overall, the purity scores show an upward trend as k increases. And at no point the purity reach 1 but the purity scores of some points are really closed to 1.

(f)



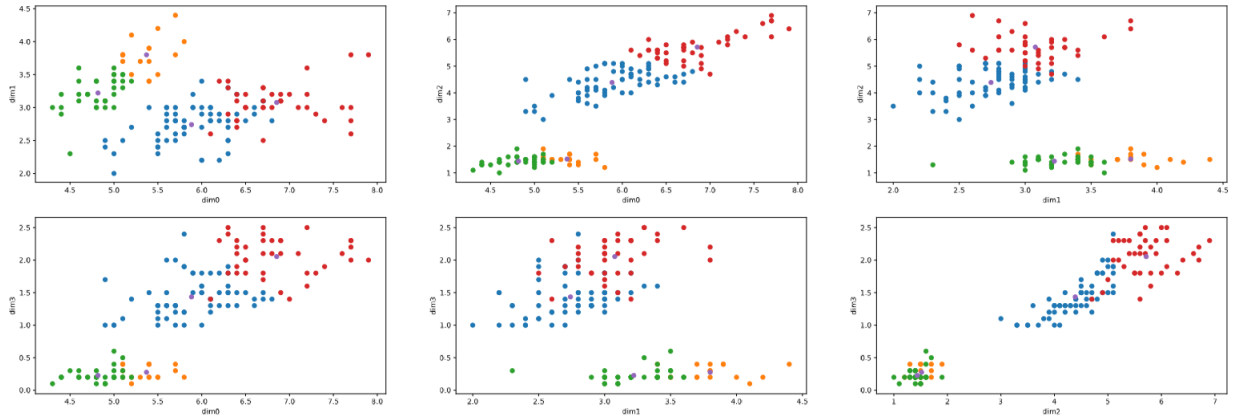
This is the curve of training error and test error of the classifier against k for $l = 1$. The blue line is training error, the orange line is test error.



This is the curve of training error and test error of the classifier against k for $l = 3$. The blue line is training error, the orange line is test error.

All curves show a downward trend as k increases and also fluctuate since the random initialization in the k -means algorithm. And this trend is really like the trend of train error in the 1-NN algorithm as the number of points increase. As the k increases, there are more centers and these centers divide the area into more parts, so the train error and test error will drop.

(g)



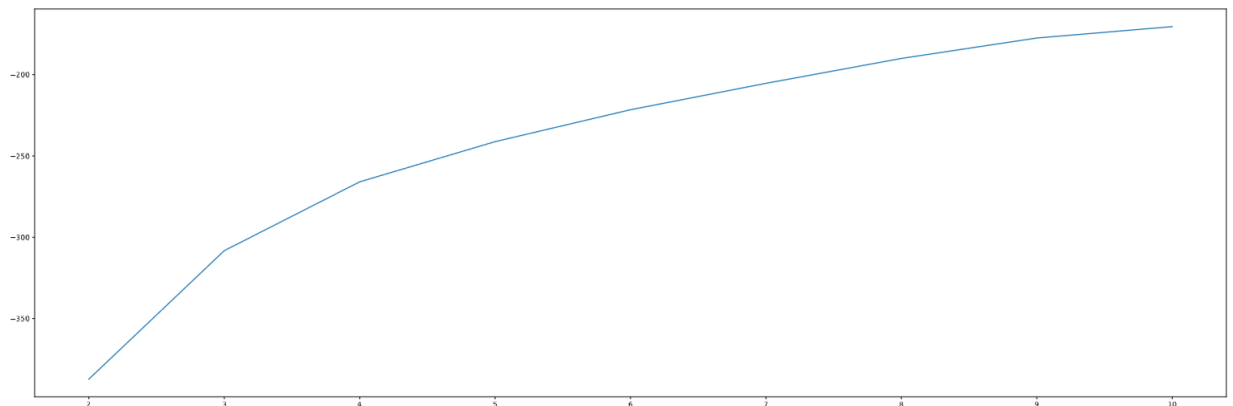
3. E-M and GMMs.

In this problem you will implement the E-M algorithm to learn a mixture of k Gaussians with diagonal covariances, as detailed in lecture. You will be using the same data as in Problem 2.

- (a) Implement the `gmm(X, k)` method. In this method X is a data matrix of shape (n, d) . The positive integer k indicates the number of Gaussian components in the mixture. Your output should be a matrix μ of shape (k, d) where each row corresponds to the mean of one of the Gaussians, a matrix Σ of shape (k, d) matrices where the i -th row corresponds to the diagonal of the covariance matrix of the i -th Gaussians and a k -vector of probability distribution over the k Gaussian components. For initialization, set the weights π to be uniform, the covariances to be diagonal, and the means to be the result of your k -means solution from the previous part after 10 iterations.
- (b) Compute and plot the log-likelihood of the model when trained on the data trained by your algorithm with a uniform `pi` against the value of k ranging from 2 to 10. You can use the method `line_plot(data1, ..., min_k=2, output_file='plot.pdf')` to plot the data.
- (c) Implement the `gmm_predict(x, mu, covars, weights)` method. In this method, x is a $d \times 1$ vector, μ is a matrix of shape (k, d) , the list `covars` is of length k and consists of $d \times d$ covariance matrices and `weights` is a $k \times 1$ vector that is probability distribution indicating the weights of the k Gaussian components. Your method should return a k -vector that is the probability distribution of the datapoint x having been generated by each of the Gaussian components.
- (d) Implement the method `classify_using_gmm(X, Y, k)`. This method takes a data matrix X and label vector Y and positive integer k , and fits a Gaussian mixture model of k components on this data. Let R be the responsibility matrix of this model. Train a logistic model on the data matrix R and labels Y . You can use the method `logistic_regression` from `hw5.utils.py`.
- (e) Train a Gaussian mixture model with 4 components. Plot the data and group them by the closest center. To draw the plot, you can use the method `gaussian_plot_2d_project(X1, ..., output_file='output.pdf', ncol=3)`. This method takes multiple matrices X_1, \dots of size $n_i \times d$ each corresponding to one cluster. It generates $\binom{d}{2}$ plots, one for every pair of dimensions. The output is then saved to the file indicated by `output_file`.

Solution. (*Your solution here.*)

(b)



(e)

