Home exam machine learning fall 2024

Contents

[0.1 Introduction to exam 2](#_Toc180588882)

[1.0 Part one 2](#_Toc180588883)

[1.1 Exercise 1 2](#_Toc180588884)

[1.2 Preprocessing 2](#_Toc180588885)

[1.3 Model selection and reasoning 5](#_Toc180588886)

[1.4 Cross validation and parameter tuning 6](#_Toc180588887)

[1.5 Results and validation 6](#_Toc180588888)

[2.0 Part two 6](#_Toc180588889)

[2.1 What is clustering? 6](#_Toc180588890)

[2.2 K-mean clustering 7](#_Toc180588891)

[2.3 Display of dataset 9](#_Toc180588892)

[2.4 Implementation of the K-means algorithm 9](#_Toc180588893)

[2.5 The models result 10](#_Toc180588894)

[3.0 Conclusion 13](#_Toc180588895)

[4.1 appendix A 13](#_Toc180588896)

[4.2 Appendix B 13](#_Toc180588897)

[5.0 sources 16](#_Toc180588898)

## Introduction to exam

The machine learning exam fall 2024 can be broken down into two parts. **Part one** involves classify whenever molecules like fat or not based on their lipophilicity. The task allows any function/method in the scikit-learn package introduced in the course. **Part two** focuses on implementing a K-nearest neighbors algorithm to classify the dataset frey\_faces.csv. Additionally, there is also a few questions to answer.

# 1.0 Part one

## Exercise 1

**Part One** of this paper presents a solution to a binary classification problem, where molecules are classified based on their lipophilicity. In the following sections, the paper will address several common challenges in machine learning, including data handling, model selection, cross-validation, parameter tuning, and result evaluation.

## Preprocessing

The first step in preprocessing a dataset is to obtain an overview of its structure, which includes checking the matrix size, identifying missing values, and detecting "useless" features. I define useless features as those that do not provide any additional information. For instance, features with the same values across all samples would be considered useless.

In the training set, there are 228 features and over 4,000 samples across two datasets. While there are no empty cells, many features contain a significant number of zero values. In some cases, over 90% of the samples have zero values in certain features. I strongly considered treating at least some of these zero values as missing data. However, lacking domain knowledge specific to this dataset, I ultimately decided against it.

**Removing useless features**

Additionally, there are many useless features that do not provide any additional information and only add complexity to the computational structure of the model(s). There was a total of 16 features removed because of this.

**Correlation matrix of features**

When working with large and complex datasets, it’s easy to get overwhelmed and difficult to understand the relationships between features. Therefore, I decided to create a correlation matrix for each dataset.

A grid with a grid and a grid with a grid and a grid with a grid and a grid with a grid with a grid and a grid with a grid with a grid and a grid with

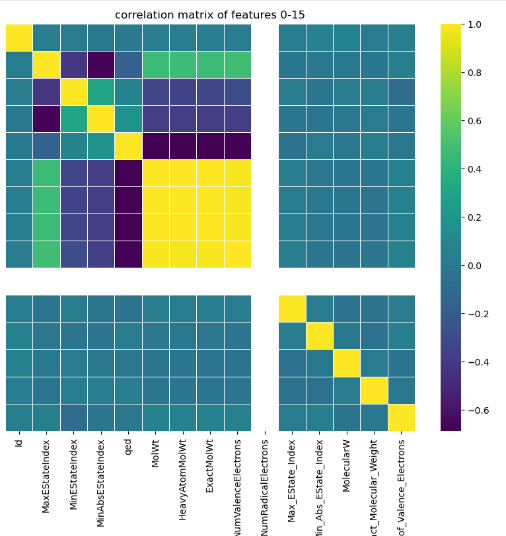
Description automatically generated A grid with a grid and a scale

Description automatically generated with medium confidence

The bar on the right side of the correlation matrix indicates how strong the correlation is between features.

Values closer to one indicates strong, and almost a linear correlation, while a value closer to -1 shows almost no correlation. Both extremes can impact the dataset negatively if not handled appropriately.

When analysing the matrices, a clear difference between the training and test datasets emerges. The white lines highlight features that show no correlation at all, suggesting that they do not provide useful information. The exercise description states: “and some of the features have been made up artificially by some very mean members of the teaching team”. I believe these features are the white lines in the test dataset. In order to remove these features, I zoomed in on the matrix and included feature labels:

A screenshot of a graph

Description automatically generatedA screenshot of a graph

Description automatically generated

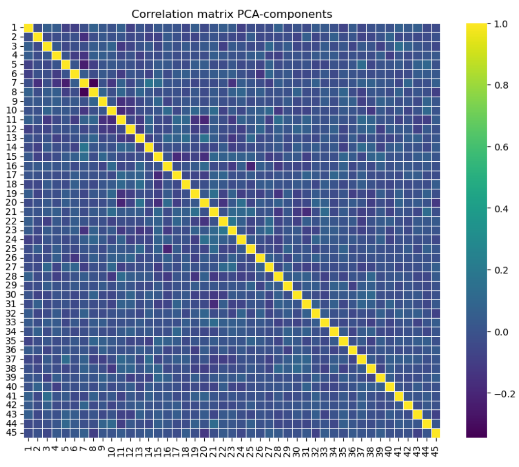
After identifying the features: *['fr\_azo', 'fr\_barbitur', 'fr\_dihydropyridine', 'fr\_phos\_ester', 'fr\_phos\_acid','NumRadicalElectrons']*, as artificially made-up features. The next logically step was to remove them. However, this does not resolve our initial problem of having a highly correlated matrix of features.

**Applying PCA**

Applying Principal Component Analysis (PCA) is common practice in machine learning, when working with highly correlated features. It’s strength in dimension reduction, handling of noise and creation of new uncorrelated features, makes it a powerful tool. PCA improves model performance while simplifying complex datasets.

The first step is to transform the datasets using standard scale. This transformation makes sure that all the features have a mean of zero and a standard deviation of 1. While maintaining the ratio of the original values, this process guarantees all features affecting the calculation the same. This prevents domination due to scale differences.

Afterward the datasets are ready for Principal Component Analysis. When applying the PCA, there is a variable that selects how much of the variance one wish to keep. This will initially be set to 90%, this may be adjusted when trying to optimize the accuracy of the model.

A graph of a number of components

Description automatically generated

We can see that the new features are not correlated with each other. This will hopefully result in the model being able to pick up underlying patterns and predict whether the molecule likes fat or not.

## Model selection and reasoning

Choosing the right model is crucial when solving binary classification. Especially when working with complex datasets such as in this exercise. Since every model introduces in this course is available to use, I have chosen four different models, logistic regression, random forest, k-nearest neighbors and naive bayes classifier. I will consider how they fit the datasets. The primary goal is to maximize accuracy. So, factors such as computational efficiency will not be considered.

**Logistic regression**

Logistic regression **(LR)** is a simple model that pick us linear relationships. The model picks up how each feature affect the outcome. It also predicts the outcome with a certain probability for each sample, which may come in handy. A disadvantage with the model is it’s lack of ability to pick up relationship between features. When working with such complex datasets the model may struggle.

**Random forest**

Random forest **(RF)** is a complex and robust model to solve complex ML problems. The model’s ability to handle non-linearity, makes it able to pick up relationships between different features. Since the forest consists of “k” amount of smaller decision trees, it’s also decent to prevent overfitting.

**k-nearest neighbors**

k-nearest neighbors are a reliable model that does require a statistical distribution to work, it’s great to pick up underlying patterns and relationships between features on higher dimensions. The main problem with this model is its ability to adapt to noisy data and scaling. Which may result in the model struggling to adapt.

**Naive bayes classifier**

The naive bayes classifier is a simple but reliable classifier, it’s ability to make its own threshold may result in it working well with this given dataset. The main problem with these models is their inability to pick up relationships between features. Since it used bayes formula, the model assumes all features are independent to each other.

## Cross validation and parameter tuning

To evaluate the performance of the models before submitting. I used cross validation on the training set. Instead of splitting the training data into a separate training and test set. Cross validation provides a more reliable estimate of how well the models respond to new unseen data. Since it’s over 3000 samples in the training set, cross validation is a suitable choice.

To increase accuracy, there was a need to tweak the parameters of the models. The most time efficient way to do this is to try every combination of parameters one think could improve the model. Therefore, I made a function for each model, that tries all combination of parameters and return the ones with the highest accuracy.

(code provided in appendix A)

|  |  |  |
| --- | --- | --- |
| model name | Default parameters | Tweaked parameters |
| Logistic regression | 76.9% | 77.08% |
| Random forest | 75.4% | 77.05% |
| K-nearest neighbor | 77.3% | 78.4% |
| Naive bayes classifier | 68% | 68% |

As you can see, the tweaked parameters improved the models, but only around 1-2% so the change is minimal.

## Results and validation

Uploading the predictions for the test set did not provide the results expected. Since the models performed in the high 70% one would expect something similar when submitting the test set. The highest score I got was right under 60% with the K-nearest neighbor algorithm with the optimized parameters.

The difference between performance on the training and test dataset, may suggest that the model overfitted in the training process, or that a significant difference between the datasets were not captured by the model. It could also be that the preprocessing of the datasets was not good enough.

# 2.0 Part two

## 2.1 What is clustering?

*Explain what clustering is, and how it is different from classification. Give an example of a problem where clustering might be the appropriate solution.*

Clustering is a machine learning method that groups data together without any labels. It is an unsupervised learning method that focuses on underlying patterns and space in vectors to group together samples. Unlike classification it does not need to be trained beforehand, and its only goal is to group together data.

**Example of a clustering problem**: Clustering could be used to group houses and apartments based on features like size, number of bedrooms, location, and price. Without predefined categories (such as "house" or "apartment"), clustering can automatically find groups of properties that are similar, such as high-end homes or small, affordable apartments, revealing underlying patterns in the housing market

## 2.2 K-mean clustering

*Describe the k-means algorithm. Explain how the cluster centroids are initialized and updated. What is the stopping criterion for the algorithm? Typically, k-means is used on vectors, but how can you use it on 2D image data?*

**K-means algorithm:**

The model’s primary goal is to group data into a pre-selected number of clusters, often notated as **“k”**. Each sample is represented as a vector, where each feature is displayed as a separate dimension. The algorithm creates centroids with some given conditions. It then moves the centroid toward the average position of all the closest samples. Here is a breakdown of how the algorithm manipulates the centroids into clusters of data:

**How centroids are initialized:**

There is primarily two ways to create centroids:

1. **Random**

Centroids are placed randomly within the data space. This method is simple but risky, as randomly chosen centroids may end up too close to each other or too far from the actual data clusters. This could lead to poor clustering results, as certain clusters might overlap or remain underrepresented. However, if the random centroids are placed near the true cluster centers, this approach can work well.

1. **Using samples**

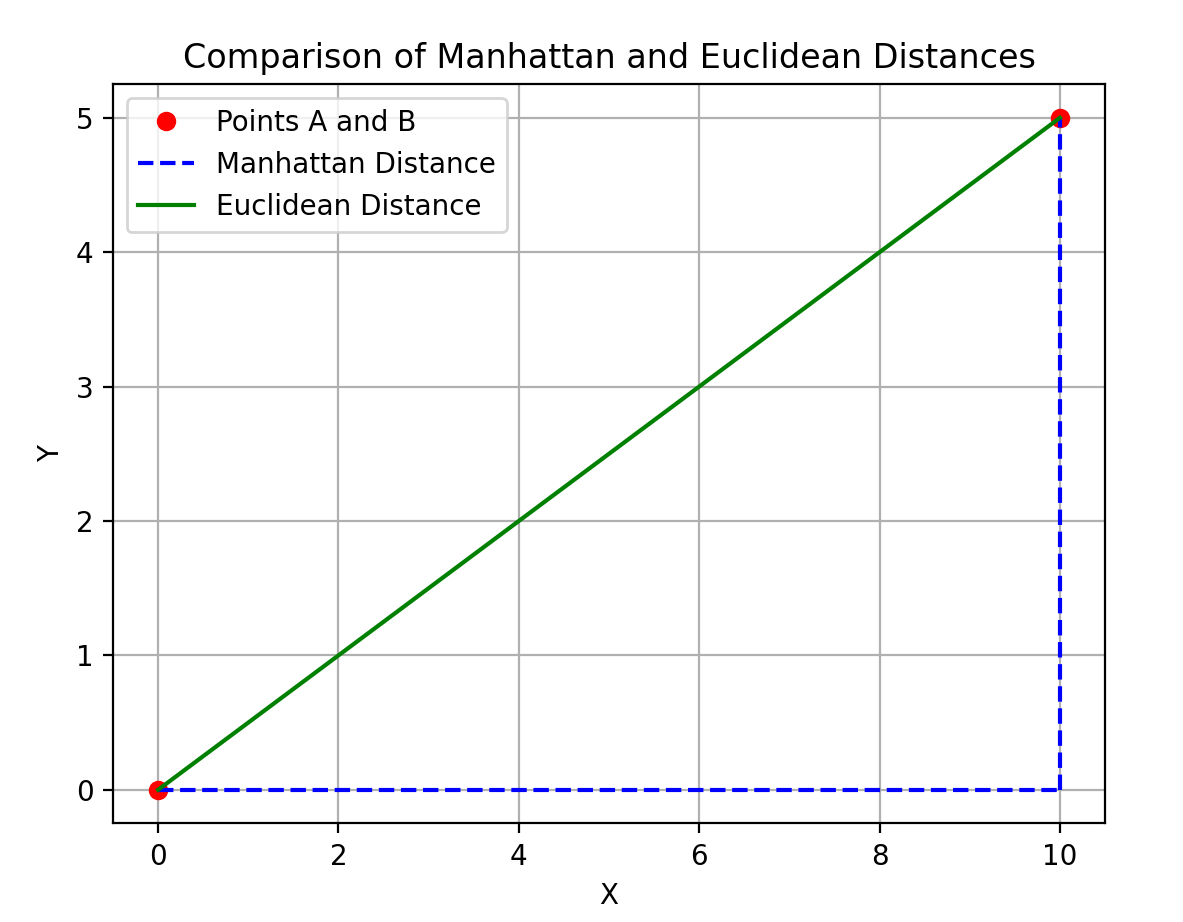
Centroids can also be created by using the vector position of samples in the dataset. This ensures that the centroids are close to the data points we wish to cluster. There is still a chance that we pick samples that is close to each other, therefore it’s important to look at the samples when using samples for centroids. This could be hard to do in high dimensional vector space.

Each method has its own use places depending on the goal of the algorithm and the dataset. Therefore, it is important the developer of model considers which option is the best.

**Updating centroids:**

1. Each vector is assigned to the closest centroid
2. Centroid is moved toward the average position of all the closest centroids.
3. These steps are repeated until a stopping criterion is met.

There are multiple ways to determine the distance between vectors. The most common is Euclidean distance and Manhattan distance. Under is a plot I made to visualize the difference:



Stopping criterions:

1. Max iterations: The model has run for a predefined number of iterations.
2. Minimal change: There is no longer significant change in centroid position from last iteration.

**Using k-means on 2D images:**

By representing each pixel as a feature, we can use K-means algorithm to cluster together images. We can use information such as color or intensity of each feature to make groups of the pictures.

Steps:

1. Flatten the images into a vector of pixels, and give each pixel numerical values determined by their color/intensity
2. Apply k-mean clustering to the vectors
3. Reconstruct the images

## 2.3 Display of dataset

*From the images you see, do you have any intuition on what clusters the k-means algorithm will yield?*

A close-up of a person's face

Description automatically generated

Display of 5 random pictures from the dataset

Given that the angle, lighting, and placement of the faces are consistent across the dataset, I predict that the k-means algorithm will primarily group images based on facial expressions. With relatively few pixels representing each image, capturing finer facial details is challenging. Therefore, the algorithm is likely to focus on more prominent differences, such as variations in facial expression.

## 2.4 Implementation of the K-means algorithm

The k-means algorithm was implemented using the principals in **2.2**, in **summary**:

1. ***Initialization***

The centroids are initially created as random samples within the dataset. I chose this approach because of the dataset. Each sample has 28x20 features (560), so with creating a random centroid, there is a chance the vector would land outside of the data’s range. Leading to poor clustering. Using samples is a safer approach when its impossible to visualize the vector space.

1. ***Distance metric***

In this implementation of the k-means algorithm, the user can choose between Manhattan and Euclidean distance. When testing the program, I did not notice any difference between the methods. Given that the Manhattan distance is computed simpler, I opted for it.

1. ***Stopping criterion***

The model runs either until a maximum number of iterations is reached or until the centroids no longer change significantly between iterations.Specifically, the algorithm stops when the change in centroid positions is smaller than a set tolerance. Due to computational precision issues with very small changes, I set the tolerance to 10-8.

1. ***Data handling***

The dataset is already preprocessed into a 1D array of numerical values. After the clustering process, the pictures are reconstrued using the pyplot import from matplotlib. Chatgpt helped me with the reconstruction.

The full snippet of the code is included in **Appendix B (link her din skibidi).**

## 2.5 The models result

In this implementation, the user has the option to choose the number of clusters (k), Here is the result of different k values:

A collage of different facial expressions

Description automatically generated

K= 3

A collage of different facial expressions

Description automatically generated

K=6

A collage of different facial expressions

Description automatically generated

K=10

*Based on the visualization, what do the individual clusters represent? Does what you observe align with your initial intuition?*

Based on the visualizations, the model effectively clustered pictures of the same person, despite accounting for image flips, facial expressions and different angles. This outcome surprised me, as I initially believed that facial expressions would be the dominating factor. The result suggests that face shape, positing of eyes and facial features are the dominating factors. This also proves that k-means clustering is not only a simple model, but also an effective one.

*What do you think would happen if the faces in the dataset were not perfectly centred in the image but randomly (slightly) shifted to the left or the right? Would you get the same results? why?*

If the pictures were not perfectly centered, I think it would negatively affect the model. Simple algorithms like K-means are sensitive to positioning because each pixel is treated as a feature. When the pixels shift, they would end up being compared with different features. This means prominent features like face shape, eye positioning, and facial details wouldn’t be matched correctly anymore. As a result, the algorithm's ability to detect underlying patterns would significantly weaken, and we would not get the same results.

## 3.0 Conclusion

Ex1:

This exercise has learned me the importance of testing the model on unseen data, to ensure and test the quality of the predictions the model yields.

## 4.1 appendix A

A screen shot of a computer code

Description automatically generated

## 4.2 Appendix B

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

Reconstruction of the images:

A computer screen shot of a program

Description automatically generated

## 5.0 sources