

# Assignment 2

## Supervised Machine Learning Fundamentals

Kyle Bradbury

2026-01-20

### Table of contents

#### Instructions

*Instructions for all assignments can be found [here](#). Note: this assignment falls under collaboration Mode 2: Individual Assignment – Collaboration Permitted. Please refer to the syllabus for additional information. Please be sure to list the names of any students that you worked with on this assignment. Total points in the assignment add up to 90; an additional 10 points are allocated to professionalism and presentation quality.*

#### Learning Objectives:

By successfully completing this assignment you will be able to... - Explain the bias-variance tradeoff of supervised machine learning and the impact of model flexibility on algorithm performance - Perform supervised machine learning training and performance evaluation - Implement a k-nearest neighbors machine learning algorithm from scratch in a style similar to that of popular machine learning tools like `scikit-learn` - Describe how KNN classification works, the method's reliance on distance measurements, and the impact of higher dimensionality on computational speed - Apply regression (linear regression) and classification (KNN) supervised learning techniques to data and evaluate the performance of those methods - Construct simple feature transformations for improving model fit in linear models - Fit a `scikit-learn` supervised learning technique to training data and make predictions using it

## Exercise 1 - Conceptual Questions on Supervised Learning I

[4 points]

For each part below, indicate whether we would generally expect the performance of a flexible statistical learning method to be *better* or *worse* than an inflexible method. Justify your answer.

- 1.1. The sample size  $n$  is extremely large, and the number of predictors  $p$  is small.
- 1.2. The number of predictors  $p$  is extremely large, and the number of observations  $n$  is small.
- 1.3. The relationship between the predictors and response is highly non-linear.
- 1.4. The variance of the error terms, i.e.  $\sigma^2 = \text{Var}(\epsilon)$ , is extremely high.

## Exercise 2 - Conceptual Questions on Supervised Learning II

[6 points]

For each of the following, (i) explain if each scenario is a classification or regression problem AND why, (ii) indicate whether we are most interested in inference or prediction for that problem AND why, and (iii) provide the sample size  $n$  and number of predictors  $p$  indicated for each scenario.

- 2.1. We collect a set of data on the top 500 firms in the US. For each firm we record profit, number of employees, industry and the CEO salary. We are interested in understanding which factors affect CEO salary.
- 2.2. We are considering launching a new product and wish to know whether it will be a success or a failure. We collect data on 20 similar products that were previously launched. For each product we have recorded whether it was a success or failure, price charged for the product, marketing budget, competition price, and ten other variables.
- 2.3. We are interested in predicting the % change in the US dollar in relation to the weekly changes in the world stock markets. Hence we collect weekly data for all of 2012. For each week we record the % change in the dollar, the % change in the US market, the % change in the British market, and the % change in the German market.

### Exercise 3 - Classification using KNN

[6 points]

The table below provides a training dataset containing six observations (a.k.a. samples) ( $n = 6$ ) each with three predictors (a.k.a. features) ( $p = 3$ ), and one qualitative response variable (a.k.a. target).

Table 1. Training dataset with  $n = 6$  observations in  $p = 3$  dimensions with a categorical response,  $y$

Obs.	$x_1$	$x_2$	$x_3$	$y$
<b>1</b>	0	3	0	Red
<b>2</b>	2	0	0	Red
<b>3</b>	0	1	3	Red
<b>4</b>	0	1	2	Blue
<b>5</b>	-1	0	1	Blue
<b>6</b>	1	1	1	Red

We want to use the above training dataset to make a prediction,  $\hat{y}$ , for an unlabeled test data observation where  $x_1 = x_2 = x_3 = 0$  using  $K$ -nearest neighbors. You are given some code below to get you started. *Note: coding is only required for part (a), for (b)-(d) please provide your reasoning based on your answer to part (a).*

**3.1.** Compute the Euclidean distance between each observation and the test point,  $x_1 = x_2 = x_3 = 0$ . Present your answer in a table similar in style to Table 1 with observations 1-6 as the row headers.

**3.2.** What is our prediction,  $\hat{y}$ , when  $K = 1$  for the test point? Why?

**3.3.** What is our prediction,  $\hat{y}$ , when  $K = 3$  for the test point? Why?

**3.4.** If the Bayes decision boundary (the optimal decision boundary) in this problem is highly nonlinear, then would we expect the *best* value of  $K$  to be large or small? Why?

```
import numpy as np

X = np.array([[ 0, 3, 0],
               [ 2, 0, 0],
               [ 0, 1, 3],
               [ 0, 1, 2],
               [-1, 0, 1],
               [ 1, 1, 1]])
y = np.array(['r', 'r', 'r', 'b', 'b', 'r'])
```

## Exercise 4 - Build your own classification algorithm

[18 points]

 Note

[Data for this exercise can be downloaded here](#)

**4.1.** Build a working version of a binary KNN classifier using the skeleton code below. We'll use the `sklearn` convention that a supervised learning algorithm has the methods `fit` which trains your algorithm (for KNN that means storing the data) and `predict` which identifies the  $K$  nearest neighbors and determines the most common class among those  $K$  neighbors. *Note: Most classification algorithms typically also have a method `predict_proba` which outputs the confidence score of each prediction, but we will explore that in a later assignment. Please use `NumPy` to implement euclidean distance function.*

**4.2.** Load the datasets to be evaluated here. Each includes training features ( $\mathbf{X}$ ), and test features ( $\mathbf{y}$ ) for both a low dimensional dataset ( $p = 2$  features/predictors) and a higher dimensional dataset ( $p = 100$  features/predictors). For each of these datasets there are  $n = 1000$  observations of each. They can be found in the data subfolder on github (see link above). Each file is labeled similar to `A2_Q4_X_train_low.csv`, which lets you know whether the dataset is of features,  $X$ , targets,  $y$ ; training or testing; and low or high dimensions.

**4.3.** Train your classifier on first the low dimensional dataset and then the high dimensional dataset with  $k = 5$ . Evaluate the classification performance on the corresponding test data for each of those trained models. Calculate the time it takes each model to make the predictions and the overall accuracy of those predictions for each corresponding set of test data - state each.

**4.4.** Compare your implementation's accuracy and computation time to the scikit learn `KNeighborsClassifier` class. How do the results and speed compare to your implementation? *Hint: your results should be identical to that of the scikit-learn implementation.*

**4.5.** Some supervised learning algorithms are more computationally intensive during training than testing. What are the drawbacks of the prediction process being slow? In what cases in practice might slow testing (inference) be more problematic than slow training?

```
# Skeleton code for part (a) to write your own kNN classifier

class Knn:
    # k-Nearest Neighbor class object for classification training and testing
    def __init__(self):

    def fit(self, x, y):
        # Save the training data to properties of this class
```

```

def predict(self, x, k):
    y_hat = [] # Variable to store the estimated class label for
    # Calculate the distance from each vector in x to the training data

    # Return the estimated targets
    return y_hat

# Metric of overall classification accuracy
# (a more general function, sklearn.metrics.accuracy_score, is also available)
def accuracy(y, y_hat):
    nvalues = len(y)
    accuracy = sum(y == y_hat) / nvalues
    return accuracy

```

## Exercise 5 - Bias-variance tradeoff: exploring the tradeoff with a KNN classifier

[20 points]

This exercise will illustrate the impact of the bias-variance tradeoff on classifier performance by investigating how model flexibility impacts classifier decision boundaries. For this problem, please use Scikit-learn's KNN implementation rather than your own implementation, as you did at the end of the last question.

**5.1.** Create a synthetic dataset (with both features and targets). Use the `make_moons` module with the parameter `noise=0.35` to generate 1000 random samples.

**5.2.** Visualize your data: scatterplot your random samples with each class in a different color.

**5.3.** Create 3 different data subsets by selecting 100 of the 1000 data points at random three times (with replacement). For each of these 100-sample datasets, fit three separate k-Nearest Neighbor classifiers with:  $k = \{1, 25, 50\}$ . This will result in 9 combinations (3 datasets, each with 3 trained classifiers).

**5.4.** For each combination of dataset and trained classifier plot the decision boundary (similar in style to Figure 2.15 from *Introduction to Statistical Learning*). This should form a 3-by-3 grid. Each column should represent a different value of  $k$  and each row should represent a different dataset.

**5.5.** What do you notice about the difference between the decision boundaries in the rows and the columns in your figure? Which decision boundaries appear to best separate the two classes of data with respect to the training data? Which decision boundaries vary the most as the training data change? Which decision boundaries do you anticipate will generalize best to unseen data and why?

**5.6.** Explain the bias-variance tradeoff using the example of the plots you made in this exercise and its implications for training supervised machine learning algorithms.

Notes and tips for plotting decision boundaries (as in part 5.4): - *Resource for plotting decision boundaries with meshgrid and contour:* [https://scikit-learn.org/stable/auto\\_examples/neighbors/plot\\_classification\\_decision\\_boundary\\_with\\_meshgrid.html](https://scikit-learn.org/stable/auto_examples/neighbors/plot_classification_decision_boundary_with_meshgrid.html)

- If you would like to change the colors of the background, and do not like any of the existing cmap available in matplotlib, you can make your own cmap using the 2 sets of rgb values. Sample code (replace r, g, b with respective rgb values):

```
from matplotlib.colors import LinearSegmentedColormap
newcmp = LinearSegmentedColormap.from_list("new", [(r/255, g/255, b/255), (r/255, g/255, b/255)])
```

## Exercise 6 - Bias-variance trade-off II: Quantifying the tradeoff

[18 points]

This exercise explores the impact of the bias-variance tradeoff on classifier performance by looking at the performance on both training and test data.

Here, the value of  $k$  determines how flexible our model is.

**6.1.** Using the function created earlier to generate random samples (using the `make_moons` function setting the `noise` parameter to 0.35), create a new set of 1000 random samples, and call this dataset your test set and the previously created dataset your training set.

**6.2.** Train a kNN classifier on your training set for  $k = 1, 2, \dots, 500$ . Apply each of these trained classifiers to both your training dataset and your test dataset and plot the classification error (fraction of incorrect predictions).

**6.3.** What trend do you see in the results?

**6.4.** What values of  $k$  represent high bias and which represent high variance?

**6.5.** What is the optimal value of  $k$  and why?

**6.6.** In KNN classifiers, the value of  $k$  controls the flexibility of the model - what controls the flexibility of other models?

## Exercise 7 - Linear regression and nonlinear transformations

[18 points]

**i** Note

[Data for this exercise can be downloaded here](#)

Linear regression can be used to model nonlinear relationships when feature variables are properly transformed to represent the nonlinearities in the data folder. In this exercise, you're given training and test data contained in files "A2\_Q7\_train.csv" and "A2\_Q7\_test.csv" in the data. Your goal is to develop a regression algorithm from the training data that performs well on the test data.

*Hint: Use the scikit learn [LinearRegression](#) module.*

**7.1.** Create a scatter plot of your training data.

**7.2.** Estimate a linear regression model ( $y = a_0 + a_1x$ ) for the training data and calculate both the  $R^2$  value and mean square error for the fit of that model for the training data. Also provide the equation representing the estimated model (e.g.  $y = a_0 + a_1x$ , but with the estimated coefficients inserted). Consider this your baseline model against which you will compare other model options. *Evaluating performance on the training data is not a measure of how well this model would generalize to unseen data. We will evaluate performance on the test data once we see our models fit the training data decently well.*

**7.3.** If features can be nonlinearly transformed, a linear model may incorporate those nonlinear feature transformation relationships in the training process. From looking at the scatter plot of the training data, choose a transformation of the predictor variable,  $x$  that may make sense for these data. This will be a multiple regression model of the form  $y = a_0 + a_1z_1 + a_2z_2 + \dots + a_nz_n$ . Here  $z_i$  could be any transformations of  $x$  - perhaps it's  $\frac{1}{x}$ ,  $\log(x)$ ,  $\sin(x)$ ,  $x^k$  (where  $k$  is any power of your choosing). Provide the estimated equation for this multiple regression model (e.g. if you chose your predictors to be  $z_1 = x$  and  $z_2 = \log(x)$ , your model would be of the form  $y = a_0 + a_1x + a_2\log(x)$ ). Also provide the  $R^2$  and mean square error of the fit for the training data.

**7.4.** Visualize the model fit to the training data. Using both of the models you created in parts (b) and (c), plot the original data (as a scatter plot) AND the curves representing your models (each as a separate curve) from (b) and (c).

**7.5.** Now its time to compare your models and evaluate the generalization performance on held out test data. Using the models above from (b) and (c), apply them to the test data and estimate the  $R^2$  and mean square error of the test dataset.

**7.6.** Which models perform better on the training data, and which on the test data? Why?

**7.7.** Imagine that the test data were significantly different from the training dataset. How might this affect the predictive capability of your model? How would the accuracy of generalization performance be impacted? Why?

*To help get you started - here's some code to help you load in the data for this exercise (you'll just need to update the path):*

```

import numpy as np
import pandas as pd

path = './data/a2'
train = pd.read_csv(path + 'A2_Q7_train.csv')
test = pd.read_csv(path + 'A2_Q7_test.csv')

x_train = train.x.values
y_train = train.y.values

x_test = test.x.values
y_test = test.y.values

```

### [OPTIONAL] Bonus Exercise: Designing a performant, low-latency classification system

*Bonus questions can offset missed points in an assignment, but the total score on an assignment cannot exceed 100 points*

[5 points]

For machine learning models, latency can be an important factor depending on the application. There are generally two types of latency to consider with a model: training time and prediction time. For many models, you train the model once, so this could be a one-time event. However, prediction time can be far more important for real-world applications. If you're developing a system for a self-driving car - your predictions need to be made very quickly to be useful so you don't accidentally hit something. Similarly, if you're an online retailer and are trying to make a recommendation for your customer, if it takes 2 minutes for the recommendation to load, the customer will likely have moved on.

Your goal is to design a system that has minimal latency for each prediction while remaining useful. You are able to adjust your KNN model characteristics (changing the value of K, the number of features used, the size of the training data, etc.). Of course, you also are interested in the performance of the model. Walk through each consideration that you factor in, showing plots of the impact varying modeling choices has on your average latency and other key performance metrics. Describe your process for evaluating the tradeoffs and justify your final recommendation for the model design supported by evidence from your analysis. Show and describe your analysis of the various factors that are involved in making this decision and how they vary.

For this problem, use the [Census Income dataset](#) where the goal is to predict whether or not each individual makes greater than \$50k per year. You will need to determine how to best structure the problem and preprocess the data (which have not been cleaned). Describe and

justify the choices you make and be sure to plot some sample of the data to explore your data before you jump into modeling.