Spam Email Classification Through Machine Learning Models

By Emma Allen
UID – 006326040

https://ejallen471.github.io/c111project/

Table of Contents

Introduction 3

Data 3

Performance Metrics 4

- Learning Curve 4
- Confusion Matrix 5
- Receiver Operating Characteristic (ROC) Curve: 5
- Matthews correlation coefficient (MCC): 5
- Cohen's Kappa 5

Modelling Considerations 5

- Logistic Regression 6
- Decision Tree Classification 6
- KNN 6
- SVM 6
- MLP - Sklearn 6

Results 7

- Learning Curve 7
- ROC Curve 9
- MCC: 10
- Cohen's Kappa: 10
- Confusion Matrix 10

Discussion 12

Conclusions 12

- Logistic Regression 13
- Decision Trees 13
- KNN 13
- SVM 13
- MLP - Sklearn 13
- MLP – PyTorch 13

Bibliography 14

Introduction

The first known spam electronic mail was sent on 3rd May 1978 to several hundred users by a marketing manager for digital equipment Corporation (World Economic Forum, 2018). Over the past 40 years, the volume of spam emails has only increased, reaching a point where spam accounted for 48% of all emails sent in 2022. (Statista, 2023).

This project aims to use classify emails as spam through utilising five supervised learning algorithms to conclude which one is the most accurate and precise. The algorithms used are:

1. Logistic Regression
2. Decision Tree
3. K-Nearest Neighbours (KNN)
4. Support Vector Machines (SVM)
5. Multi-Layer Perceptron (MLP) classifier:
    a. Scikit-Learn
    b. PyTorch

Data

The dataset utilised in this project is from the UCI Machine Learning Repository (Hopkins, 1999). Created in 1999, the dataset encompasses 4601 instances, with each instance representing an email. Consisting of 57 continuous features and one binary class label that denotes whether an instance is spam, the dataset is an imbalanced distribution with spam instances accounting for 39.4%. Features of the dataset include word and character frequencies.

The data was processed by adding column names and turning into a pandas data frame. Figure one shows the whole distribution of spam across instances and figure two shows the distribution for a single feature across all instances. This information allows one to determine which features are good differentiators of spam. Notably one finds that the word George and area code 650 are indicators of non-spam.

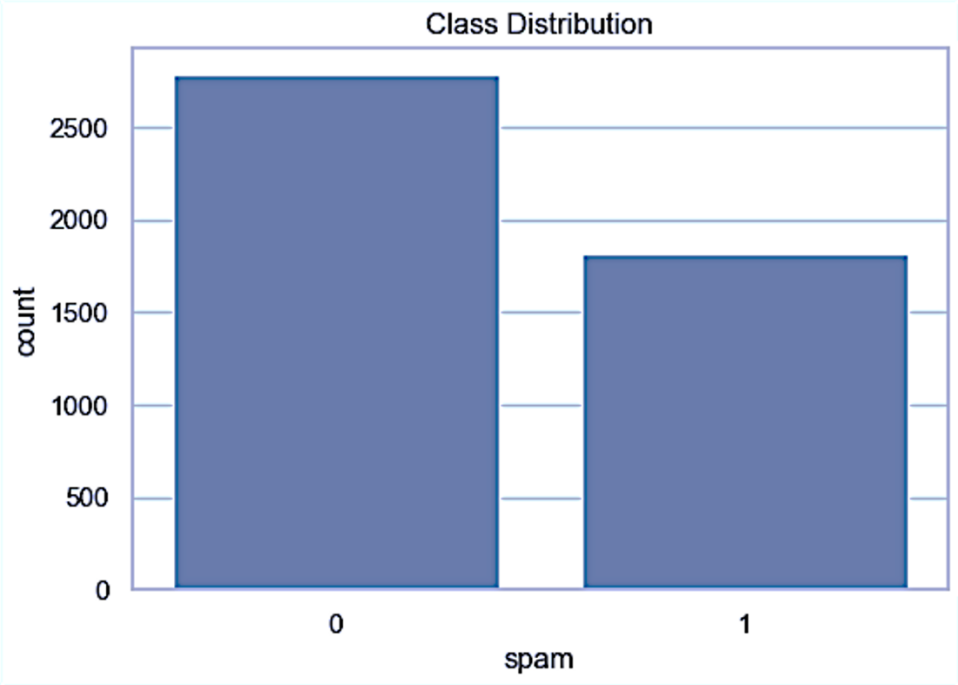

Figure 1 Distribution of spam within the dataset.

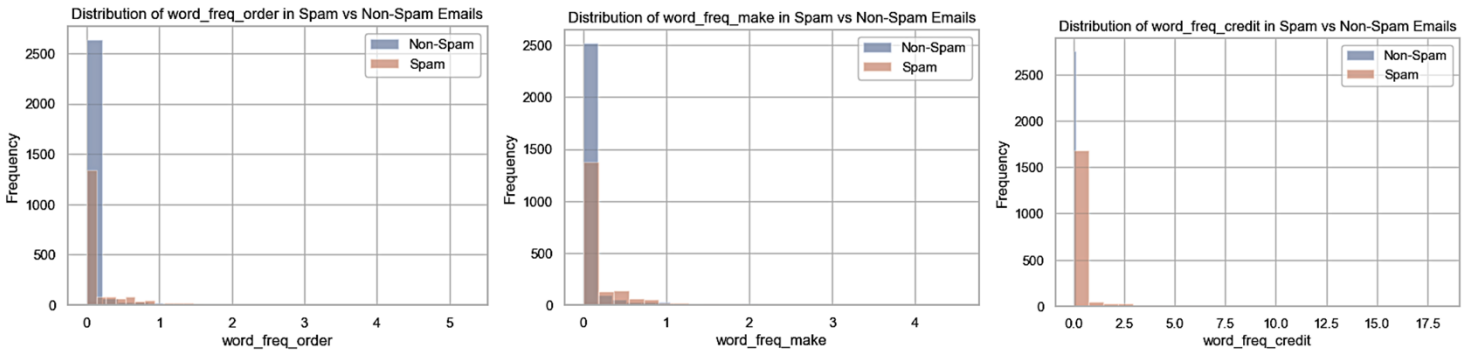

Figure 2 Distribution of Spam across three features.

Performance Metrics

Throughout this project, the definition of accuracy is taken to be to be a measure of the overall correctness of the model across all classes and precision is defined as a measure of the accuracy of the positive predications made by the model (Evidently AI, n.d.). Although the Scikit-Learn package includes an accuracy measure, this measure performs less well with an imbalanced dataset, furthermore due to the PyTorch model the decision was made to forgo this metric. Instead, the following metrics are used.

Learning Curve

The learning curve provides a graphical representation to a model's performance as it is exposed to more training data. This is useful to gauge whether a model has high bias or variance, hence shows whether a model is under or over fitting the data.

Confusion Matrix

The Confusion matrix shows one a visual breakdown of the true positives, true negatives, false positives, and false negatives. A successful algorithm is measured by having minimal false positive and false negatives.

Receiver Operating Characteristic (ROC) Curve:

The ROC curve graphically represents the performance of a binary classification model (Google Machine Learning , n.d.). The ROC curve plots the true positive rate (TPR) against the False Positive Rate (FPR) which are defined as:

$$TPR = \frac{TP}{TP+FN} \qquad FPR = \frac{FP}{TP+FN}$$

The area under the curve (AUC) is a single value that encapsulates the overall performance, ranging from 0 and 1. A higher value indicates better discriminatory power.

Matthews correlation coefficient (MCC):

This metric evaluates the performance of binary classification models by considering the true positives *(TP),* false positives *(FP),* true negatives *(TN)* and false negatives *(FN)* through the formula:

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

A high MCC suggests the model effectively captures true positives while minimising false positives and false negatives. Because it considers all four quadrants of the confusion matrix, it is less sensitive to class imbalance. In these scenarios, the MCC penalizes misclassifications in both minority and majority classes, hence aligning with the project's precision definition.

Cohen's Kappa

It measures the agreement between predicted and actual classifications, through the formula (Data Tab, 2023):

$$Kappa = \frac{Observed\ Agreement - Expected\ Agreement}{1 - Expected\ Agreement}$$

Ranging from -1 to 1 where 1 indicates perfect agreement and -1 signifies perfect disagreement. For an imbalanced dataset, this metric is useful as it evaluates the agreement between model predictions and true classifications while accounting for the possibility of random agreement, aligning with the definition of accuracy for this project.

Modelling Considerations

All models employ k-fold cross-validation to reduce overfitting and ensure each fold has a representative distribution of minority and majority class samples.

Logistic Regression

Given the dataset's imbalance (39.4% spam), class weights are adjusted (0.6 for non-spam, 0.4 for spam). The Newton Conjugate Gradient Optimization Method is chosen as the optimisation algorithm due to its efficiency in moderate-sized datasets with many features and $O(kN^2)$ time complexity (Yue Xie, 2023) where k is the number of iterations required for convergence and N is the number of features.

L2 regularisation is used as the penalty term. This prevents overfitting by indicating an expectation that all features contribute. This ensures a balanced consideration of each feature's impact on classification.

Decision Tree Classification

After experimenting with various values, the max_depth parameter was established at 12, leading to optimal accuracy. This parameter governs the maximum depth of the tree (m), impacting its computational efficiency. This is shown by a time complexity of $O(nplog(p))$ for tree construction and $O(log(m))$ for predictions (SriharshAI, 2022), where n is the number of samples and p is the number of features. This adjustment was particularly significant as, prior to refining the model, execution times were too long.

To prevent overfitting, the ccp_alpha parameter was set to 0.001. This cost-complexity parameter plays a key role in pruning the tree, ensuring a balance between model performance, and avoiding overfitting.

KNN

Five neighbours were chosen, determined through trial and error, ensuring a balance between model complexity and predictive accuracy. This in combination with cross validation attempts to mitigate the curse of dimensionality. (Awan, 2023).

The Manhattan distance metric was adopted for measuring the proximity between instances in the feature space, due to its suitability with non-uniformly scaled features. Furthermore, the algorithm for nearest neighbours was set to ball_tree due to its favourable time complexity and efficiency this dataset.

SVM

The Radial Basis Function (RBF) kernel was chosen because of its ability to handle complex decision boundaries and high dimensions, particularly important for this dataset. The regularisation parameter, C is set at 30 and the gamma parameter, which defines the influence of a single training example was set at 0.0001. Together these prevent overfitting and balance computational efficiency.

MLP - Sklearn

By calculating two-thirds of the input layers, plus the output layer, then testing for optimality, the number of hidden layers was chosen to be 39. L2 regularization (alpha=0.1) is utilised to mitigate overfitting, and a batch size of 32 was chosen to control the number of samples used in each iteration leading to efficient model training. To counteract overfitting, an l2 regularisation parameter and batch size of 32 was utilised.

MLP – PyTorch

A neural network architecture is designed with three hidden layers, each utilising the Rectified Linear Unit (ReLU) activation function to capture complex patterns. The output layer uses a sigmoid activation function, as it is well-suited for binary classification tasks by providing probability-like outputs.

To prevent overfitting and enhance computational efficiency, early stopping is implemented, halting training when the number of epochs with no improvement reaches 35. We picked a binary cross-entropy loss function because it's good at measuring how different the predicted probabilities are from the actual class labels.

Results

Learning Curve

Figure three shows learning curves for each model implemented through sklearn and figure four shows the MLP Classifier (PyTorch) Model. In each case the testing and training curves converge at a high f1 score indicating there is no bias or high variance, hence no model is under or overfitting the data.

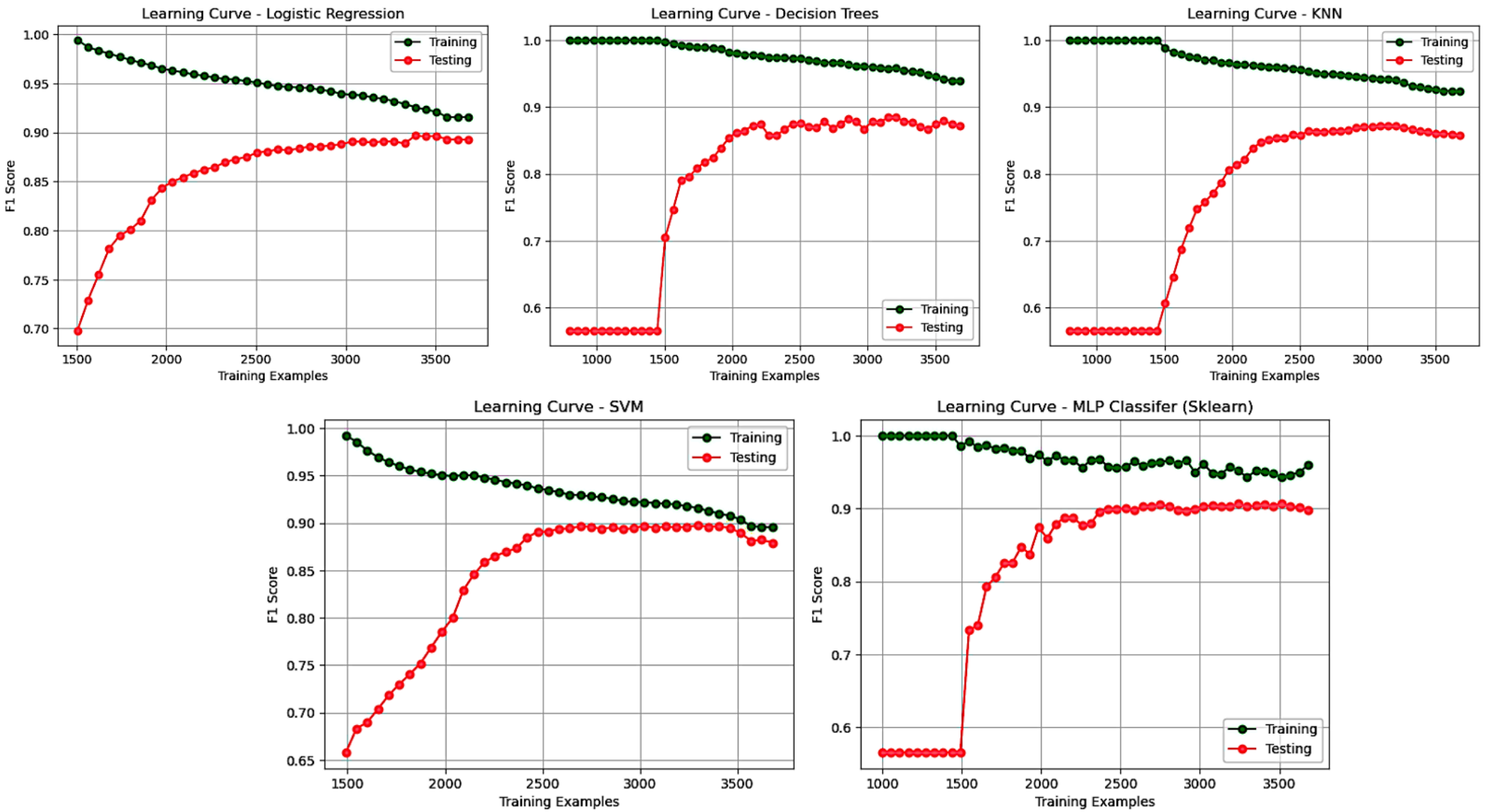

Figure 3 Learning Curves with F1 scoring for all models with sklearn.

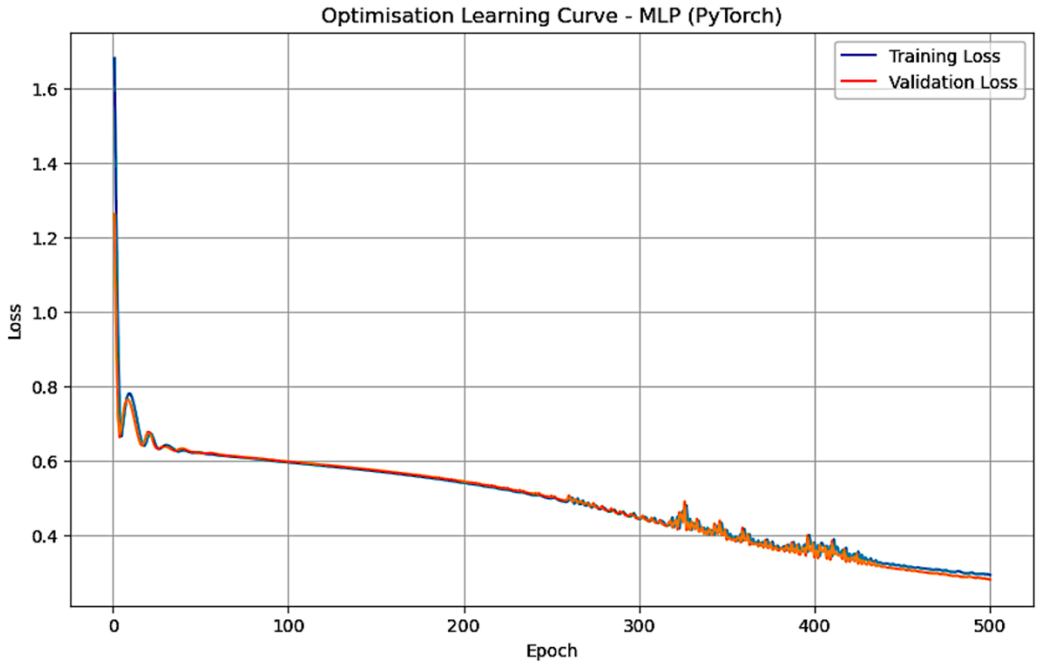

Figure 4 Optimisation Learning Curve for MLP Classifier (PyTorch)

ROC Curve

Figure five shows ROC curves for each algorithm, quantified by the AUC number. Decision trees have the lowest AUC, while the MLP classifier (sklearn) performs the best, though with no clear margin. This result indicates that this model is best in distinguishing between spam and non-spam.

It is worth noting that the AUC metric does not consider the possibility of accidental correctness, therefore across all models is much higher than the MCC and Cohen's kappa.

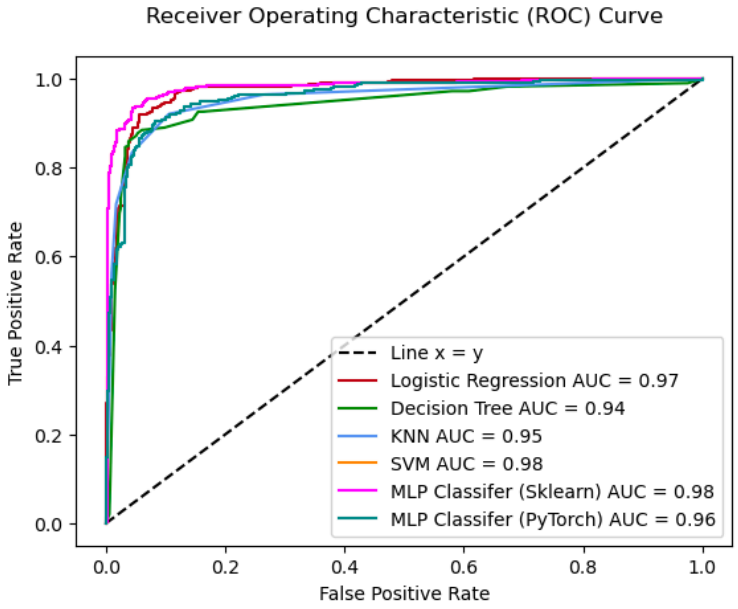

Figure 5 ROC Curve for all models, superimposed with the line y = x.

AUC number rounded to two significant figures.

MCC:

MCC figures range from 0.79333 to 0. 89540. While performing well, KNN shows lower values indicating that it has difficulties in capturing the overall agreement. MLP Classifier (sklearn) demonstrated the highest MCC demonstrating a strong overall agreement and highest precision.

Cohen's Kappa:

MLP Classifier (sklearn) achieved the highest score, hence is the most accurate model. SVM and logistic regression also performed well and KNN shows the weakest performance, indicating difficulties in capturing agreement beyond chance.

Algorithm	Logistic regression	Decision Trees	K-Nearest Neighbours	Support Vector Machines	MLP (Sklearn)	MLP (Pytorch)
AUC	0.97342	0.94015	0.94897	0.97105	0.98377	0.96530
MCC	0.86424	0.83380	0.79333	0.83146	0.89540	0.81611
Cohen's Kappa	0.86422	0.83121	0.78691	0.82902	0.89502	0.81295

Figure 6 Table displaying the AUC number, MCC coefficient and Cohen's Kappa for each model. All rounded to five significant figures.

Confusion Matrix

Figure seven shows that across all divisions, SVM performs best, closely followed by all other models with KNN being the worst. Interestingly all models are worse at predicting true negatives than true positives, this likely is due to the class imbalance of the dataset.

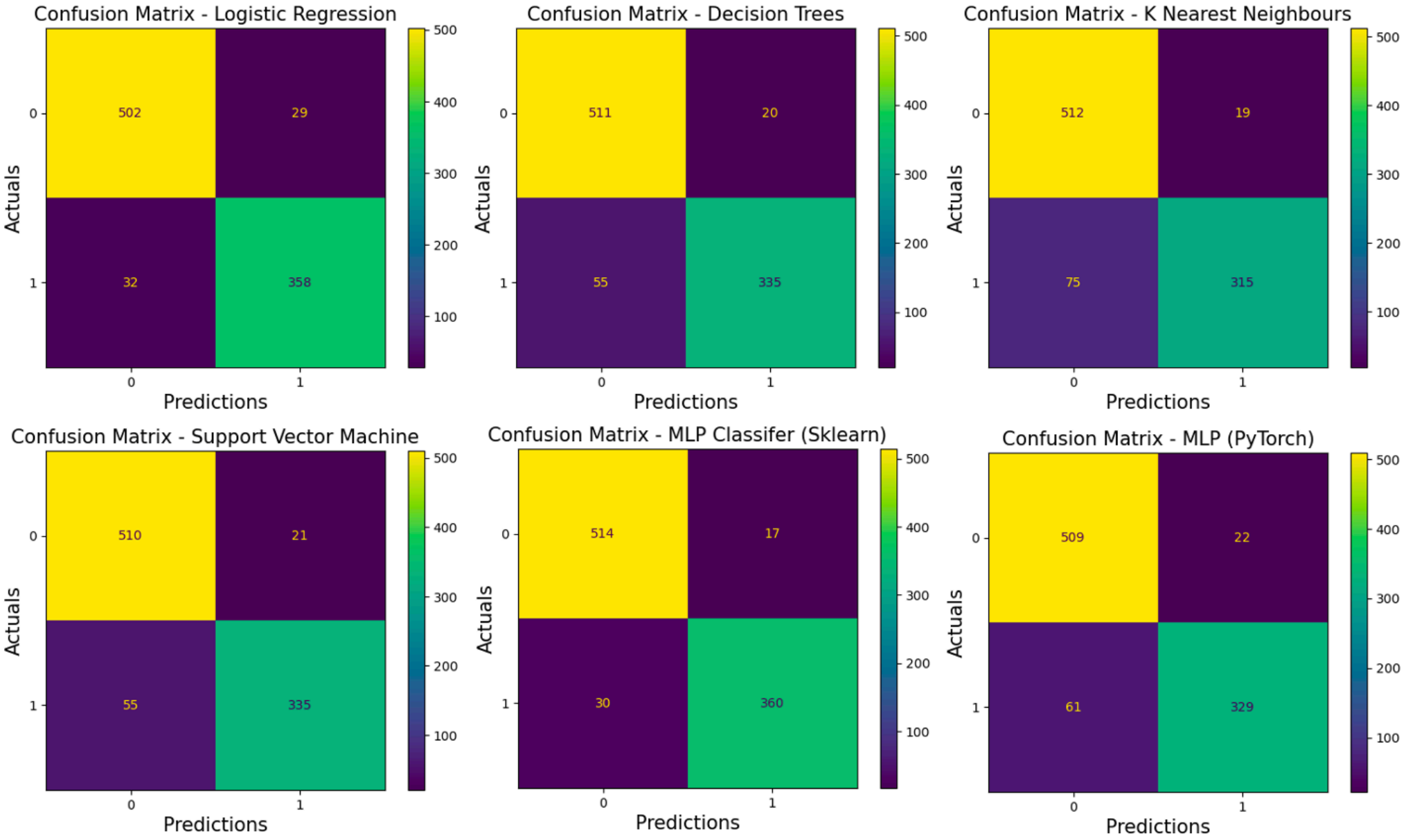

Figure 7 Confusion matrices for all algorithms. The colour scale indicates that yellow is highest and purple is lowest. From top left to bottom right the matrix shows true positive, false positive, false negative and true negatives.

Discussion

Overall KNN displays the weakest performance. This can be attributed to its sensitivity to high-dimensional spaces and the curse of dimensionality, where identifying meaningful relationships becomes challenging. Given the dataset consists of 58 features, this exacerbates the curse of dimensionality, implementing dimensionality reduction techniques could enhance the model's efficacy.

The low MCC and Cohen's Kappa scores can be attributed to its reliance on local decision boundaries, hence it is less effective in capturing global patterns. The fact these are significantly less than the AUC suggests KNN is poor at capturing agreement beyond chance.

Conversely, the MLP Classifier (sklearn) exhibits the most superior performance. The AUC score suggests that the non-linearity inherent in the data is adeptly modelled by the MLP, a feature lacking in decision trees and KNN. These latter models struggled to capture the intricacies of the decision boundary as well, leading to slightly lower scores.

Remarkably, SVM proved highly effective based on the AUC metric, indicating its proficiency in distinguishing spam instances. Although SVM models are generally less effective with imbalanced datasets, introducing class weighting may enhance the performance of this model.

Curiously, the MLP PyTorch performed worse than sklearn this is likely due to their different architectures and specific implementations, such as variations in hidden layer sizes and activation functions.

Interestingly all sklearn models demonstrate high variance and little improvement until a particular number of training examples are reached, typically around 1500 training examples. This could be because these models with their complexity require sufficient volume of data to generalise the varied nature of spam emails from the dataset. Overall, one can be confident that the models are not overfitting the data due to learning curves, cross validation and regularisation techniques employed throughout.

From looking at the learning curve for the PyTorch implementation, Although the graph has no indications of bias or high variance, one expects a negative exponential like shape, which has not occurred here, furthermore this would change on multiple runs of the code. This implies there is an implementation error, perhaps explain why this model performed worse than its sklearn counterpart.

Conclusions

AUC, MCC and Cohen's Kappa indicate a strong and reliable performance across all algorithms. One concludes that MLP classifier (sklearn) is the most accurate and precise for classifying emails as spam. This is closely followed by logistic regression and SVM. KNN performs notably poorer due to the dimensionality of the data. These results were achieved using the spam base dataset. Since this dataset was created in 1999 it is unsuitable to utilise

these models for modern day spam databases, due to changes in spam characteristics and patterns of legitimate emails.
Potential future improvements include integrating the current dataset with a more recent one for broader email classification. Exploring feature engineering on elements like email headers and sender information could enhance the models. Additionally, using feature scaling to emphasise known non-spam indicators, like "George" in this model, but it may not generalise as well to other datasets. Specific model improvements include:

Logistic Regression

Introduce interaction terms between features to capture potential dependencies between them.

Decision Trees

Extend the model into a Random Forest, leveraging an ensemble of decision trees. This would combine predictions from multiple trees, potentially enhancing the model.

KNN

Utilise dimension reduction techniques, such as principal component analysis to transform original features into a lower dimensional space.

SVM

Implement additional measures to address imbalanced datasets, such as class weightings or adjusting the decision threshold.

MLP - Sklearn

Write separate functions for the hidden layers and output layer. For instance, utilising a sigmoid activation function for the output layer as this function exhibits excellent binary classification features.

MLP – PyTorch

Change the architecture of the model, particularly increase the number of hidden layers. Batch normalisation could be implemented to address variability in results in each code run. The variability in results could also be address by changing the learning rate scheduling.

Bibliography

Awan, A. A. (2023). *The Curse of Dimensionality in Machine Learning: Challenges, Impacts and Solutions.* Retrieved from Datacamp: https://www.datacamp.com/blog/curse-of-dimensionality-machine-learning

Data Tab. (2023). *Cohen's Kappa*. Retrieved from Data tab: https://datatab.net/tutorial/cohens-kappa

Evidently AI. (n.d.). *Evidently AI*. Retrieved from Accuracy vs. precision vs. recall in machine learning: what's the difference?: https://www.evidentlyai.com/classification-metrics/accuracy-precision-recall#:~:text=Accuracy%20shows%20how%20often%20a,when%20choosing%20the%20suitable%20metric.

Google Machine Learning . (n.d.). *Classification ROC Curve and AUC*. Retrieved from Google machine learning: https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc#:~:text=An%20ROC%20curve%20(receiver%20operating,True%20Positive%20Rate

Hopkins, M. R. (1999). *Spambase.* Retrieved from UCI Machine Learning Repository. : https://doi.org/10.24432/C53G6X.

SriharshAI. (2022). *What are the Time and Space Complexities of Decision Trees*. Retrieved from https://www.youtube.com/watch?v=P8jE6kYeXhU

Statista. (2023). *Global spam volume as percentage of total e-mail traffic from 2011 to 2022*. Retrieved from Statista: https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

World Economic Forum. (2018, May 4). *40 years on from the first spam email, what have we learned? Here are 5 things you should know about junk mail*. Retrieved from World Economic Forum: https://www.weforum.org/agenda/2018/05/its-40-years-since-the-first-spam-email-was-sent-here-are-6-things-you-didnt/

Wright, C. W. (2019). *A Newton-CG algorithm with complexity guarantees for smooth unconstrained optimization.* Springer-Verlag.

Yue Xie, S. J. (2023). *Complexity of a Projected Newton-CG Method for Optimization with Bounds.* Wisconsin Institute for Discovery at University of Wisconsin-Madison.