MachLearnproj.md 7/19/2022

# Machine Learning - Spam Email Identifier

### **CSE 450 Naive Bayes Classifier By Landon Davis**

Data preprocessing:

This was fairly simple and explained in more detail bellow. The data set was in fairly good shape. I just had to make the features become intergers in order to make it used in a naive bayes classifier model.

Selection, Training, and use of a Machine Learning Model:

While developing this model there where a few things to make it able to classify and do it good enough to where it put an email into a spam or no-spam catorgy. First I was able to take the data that it would train with and cleain it. Making it either have a 1 for spam and a 0 for a real email. This allowed the model to have a catagory system in place.

I was able to train the model using Naive bayes algorithm and I decided to go with a multinomial classifier. This is because the multinomial classifier is used for classification with discrete features. The multinomial distribution normally requires integer feature counts. This is why the features where set to 1 and 0 when cleaning it.

Interpretation of Results:

The best way to score and rate the spam emails to see if the model was correct was through using accracy to measure the performance as the naive baye classifier is best understood this way. The Model was able to train and see what words or phrases accured often in spam emails. Then when given an email it would see if anything that led to a spam email would accure. My model has a 98% accuracy. The more information that it would train with would improve its performance.

#### Communication of Results:

For each image at the bottom there is an array with three numbers a 1 is a spam message and a 0 is a normal message.

Feature 1: You can see the model has a 98% accuracy score when classifing a spam email.

```
[ ] predictions = model.predict(vectorizer.transform(X_test))
    print("Accuracy:", 100 * sum(predictions == Y_test) / len(predictions), '%')
Accuracy: 98.99497487437186 %
```

Feature 2: These are random messages given to the model to see if it would predict correctly and it shows all three are spam emails.

Feature 3: These are random messages given to the model to see if it would predict correctly and it shows all three are normal emails.

MachLearnproj.md 7/19/2022

```
model.predict(vectorizer.transform(
[
    "Thank you, ABC. Can you also share your LinkedIn profile? As you are a good at programming at pyhthon, would be willing to see your personal/college projects.",
    "Hi y'all, We have a Job Openings in the positions of software engineer,
    "Dear ABC, Congratulations! You have been selected as a SOftware Developer at XYZ Company. We were really happy to see your enthusiasm for this vision and mission.

array([0, 0, 0])
```

#### Feature 4: More randomized messages given to model to try.

```
array([1, 0, 1])
```

## **Ethical Implications:**

The project and model where ethical

- There are no ethical implications when organzing emails into spam or not with machine leaning.
- When it comes to the model its accurate in a spam email situation and can be trained to find more. Other then that this model is specifically good for this task or type of one.
- Its a fairly simple but intriguing model and algorithm to use and the understanding behind naive bayes has an important fuction.

### APPENDIX A (PYTHON SCRIPT)

Below is the Google Colab link to the notebook I used during this Project:

https://colab.research.google.com/gist/Landonjdavis36/de8b96fb922336905e6f268a07faf0a6/untitled10.ipynb

MachLearnproj.md 7/19/2022

I would give this project a 2-All requirements were met. I have a working model and well explenation of the process, model, and results. I also have visualizations and code included.