**CSCE 5290: Natural Language Processing**

**Project Proposal – Spam Filtering**

**Increment 1: Documentation**

**Project Description:**

Spam is typically defined as undesired text that is sent or received over social media platforms like Facebook, Twitter, YouTube, e-mail, etc. It is produced by spammers in an effort to divert consumer’s attention from social media marketing and malware distribution, among other purposes. Spam filtering is a mechanism used to filter spam messages or emails to prevent its delivery. The volume of unsolicited email has significantly increased, necessitating the development of more robust and efficient antispam filters. Machine learning algorithms have been used to successfully identify and filter spam emails.

Here, along with the control mechanisms and datasets utilized on spam detection, we also discuss the difficulties in identifying spam.

**Github repository link:** <https://github.com/ShishiraRudrabhatla/spam-filtering-nlp>

**1. Project Title:** Spam Filtering using NLP

**Team Members:** Group # 13

|  |  |  |
| --- | --- | --- |
| **No.** | **Name** | **Student Id** |
| 1 | Shishira Rudrabhatla | 11560633 |
| 2 | Nathisha Marru | 11560642 |
| 3 | Abhishek Rangineni | 11435098 |
| 4 | Venkata Sai Rahul Kumar Katta | 11505841 |

**2. Goals and Objectives:**

**Motivation:**

One of the quickest and most affordable modes of communication is now email.

Spam emails, on the other hand, have dramatically increased over the past several years as a result of the rise in email subscribers. Since spammers are constantly looking for ways to get around existing filters, new filters must be created to stop spam. It is due to this major increase in spam emails that has led to the necessity of this project with an aim to train spam-filtering models better and stay up to date with the latest tricks spammers are coming up with every day and try to filter emails in the most effective ways possible.

**Significance**

It is critical to take extra precautions to safeguard your equipment, especially if it processes sensitive information like user data. This is since clicking on a spam email might put your computer and personal information at risk of being infected with malware. Spam filtering implementation is crucial for every firm as it does not only helps keep junk out of email inboxes, but it also improves the functionality and usefulness of business communications by ensuring that they are only utilized for what they were intended for. Since many email-based attacks attempt to deceive users into clicking on a malicious file, asking them for their credentials, and other information, spam filtering becomes one of the most needed functionalities in such cases.

**Objectives:**

Typically, text classification is the primary methodology used for email screening. There are several alternatives available when determining how to include machine learning into a Python email categorization. The objective is to develop a Python-based spam filtering approach in which relevant spam are first filtered from the training dataset and then used to generate training and testing tables for various data mining algorithms.

**Workflow diagram:** Idea of workflow diagram

**Diagram

Description automatically generated**

**Features:**

The proposed spam filtering system is expected to have the following features once fully implemented:

* Effective performance supported by the advantages and powers in natural language processing.
* Ability to categorize your emails as spam by training the classifier on your own dataset.
* Simplicity in usage.
* Fast performance once the training of the classifier is completed.
* Better model with higher accuracy in filtering spam e-mails.

**Introduction**

Unwanted email campaigns continue to be one of the top concerns, daily harming millions of consumers. Several methods to identify unwanted emails have been developed during the past few years. However, there have not been much work in the area of spam filtering together with sentiment analysis in recent studies. Everyday, scammers are getting more and more cunning, coming up with new ways of getting their spam messages undetected.

This project offers a way to support the idea that since spam is a business communication, its semantics are typically fashioned with a positive meaning. It makes use of sentiment analysis to generate the polarity scores for each message, and then assesses the accuracy of spam filtering classifiers both with and without the polarity scores.

**Background and Related Work**

Techniques for Natural Language Processing (NLP) are gaining popularity. Employing sender information and text content-based NLP has proven to be beneficial for spam filtering techniques. Researchers confirmed that it is feasible to develop a system or an application to use text mining methods and semantic analysis to detect spam in various forms models of language, respectively. This project concentrates on the application of Sentiment Analysis among all NLP methods to further analyze the detected spam messages. This is a distinctive if we contrast this strategy with the conventional short spam detection methods, which pays attention to automated text categorization but ignores sentiment analysis.

A study by Ezpelta et.al. (2016) proves that machine learning algorithms have outperformed all other suggested automatic categorization systems, with detection rates up to 96%. Their study demonstrates that the top 10 results of Bayesian filtering classifiers have been improved, reaching to a 99.21% of accuracy by producing the polarity score of each message using sentiment classifiers, and then comparing spam filtering classifiers with and without the polarity score in terms of accuracy.

Ghiassi et.al. (2022) talks of sentiment analysis and spam filtering as the two prominent uses of text classification in their study on Sentiment analysis and spam filtering using the YAC2 clustering algorithm with transferability. Text classification using traditional machine learning techniques is frequently difficult, non-transferable, and requires supervision. Their study proposes an unsupervised approach to text classification that is rather straightforward and generalizable across problem domains, while offering accuracy on par with or superior to that of existing approaches. It offers an integrated approach for Twitter sentiment analysis and spam filtering of YouTube comments that combines a new clustering algorithm, Yet Another Clustering Algorithm (YAC2), with a domain transferable feature engineering technique.

Whitelaw et.al (2005) in their study on Using appraisal groups for sentiment analysis report that few studies have attempted to leverage fine-grained semantic distinctions in classification features in sentiment analysis, which classifies texts by their "positive" or "negative" orientation. They discover that some forms of assessment seem to be more important than others for categorizing sentiment. However, their study is only limited to sentiment analysis without further input to text classification as whether it is spam or non-spam, serving as one of the huge limitations to the study.

**Dataset and Features Design**

The International Movie Database (IMDb) reviews for 50,000 reviews of films from across the world make up the dataset used for sentiment analysis; it's a binary classification dataset that classifies each review as either positive or negative. Being split at 50%:50%, it has 25,000 training samples and 25,000 test samples.

Starting with the original dataset:

(1) We remove un-important features from the dataset to remain with only the spam and ham (non-spam) columns for filtering analysis;

(2) We then add the discovered classification to the original dataset after using sentiment analysis classifiers;

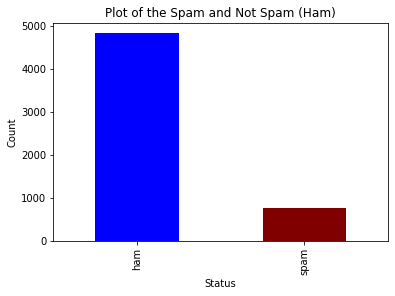
(3) We integrate the results from the two techniques on the original messages to produce the final dataset;

(4) Finally, the dataset's outcomes are then examined.

**Analysis and Implementation**

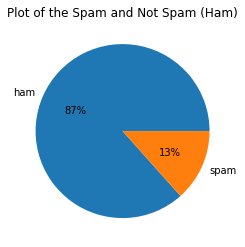
**Spam Filtering**

Having retrieved the dataset for the initial part of the project, spam filtering, exploratory data analysis (EDA) is conducted on the dataset. A visualization of the available spam and ham messages in the dataset is generated for further observations and analysis as can be seen in the figure below:



*Figure 1: Plot of spam and non-spam dataset*

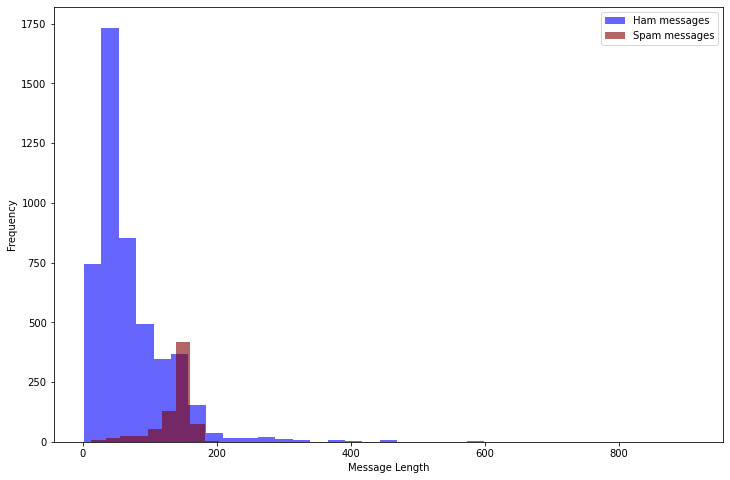
For further visualization, the following is the resulting pie chart from the given dataset:



*Figure 1b: Plot of spam and non-spam dataset*

From the plot, it can be seen that majority of the dataset contains clean messages (ham). 87% of the dataset are the non-spam messages while the remaining 13% are the spam messages. Using this dataset, we can train our model to be able to detect future spam messages.

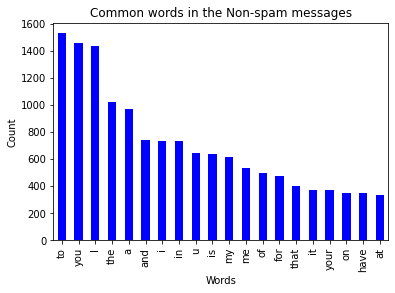
For further analysis on the spam dataset, it was important to compare the length of the messages alongside their ham/spam classification. The analysis conducted resulted in the following plot:



*Figure 2: Plot of message lengths for the spam and ham messages*

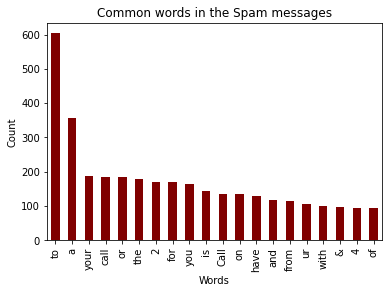
Majority of the messages had a length below 200 characters as can be observed in the above screenshot. Having observed the analysis in comparison to the length of the messages, it was necessary to also compare the frequency of the common words in the dataset.

The following is the plot of the most common words in the dataset for the non-spam messages:



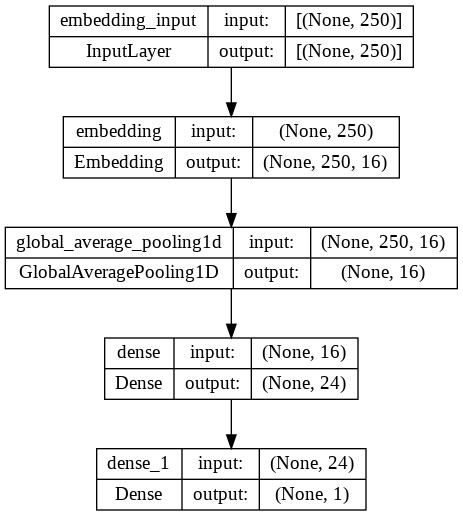
*Figure 3: Plot of most common words in the non-spam messages*

On the other hand, a plot of the common spam words in the dataset is shown below:



*Figure 4: Plot of most common words in the spam messages*

A sequential model was selected for the spam filtering task which, using the graphviz library, can be visualized as follows:

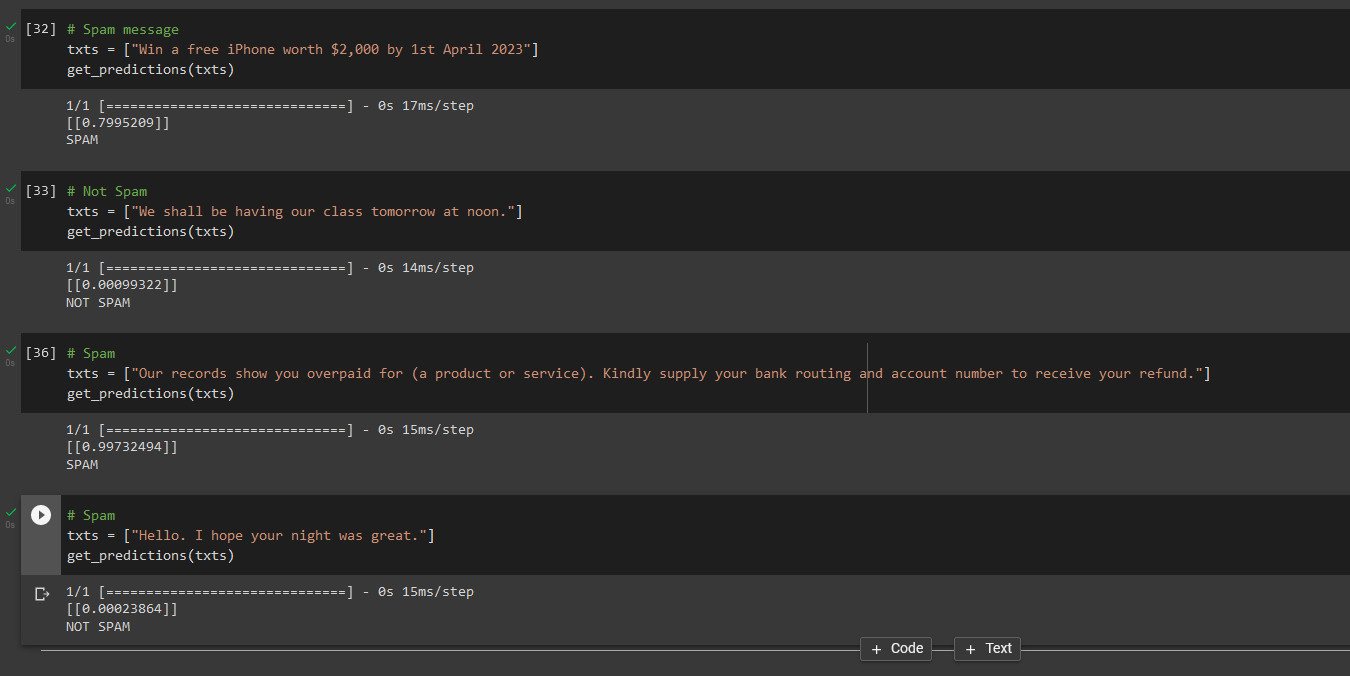


*Figure 5: Graphviz visualization for the sequential model*

Using the available test data, the model was tested and its accuracy calculated. The model’s accuracy was high enough to proceed with the analysis as it was ~98%. It was then saved to be used in the next process for sentiment analysis and other predictions.

**Preliminary results for spam filtering**

The model was used to test sample predictions as can be seen in the following screenshots which tested various message with the potential of being either spam or non-spam:



*Figure 6: Screenshot showing testing of spam/ham messages*

The analysis classifies new incoming messages as follows:

|  |  |
| --- | --- |
| Message | Spam/Not Spam |
| Win a free iPhone worth $2,000 by 1st April 2023 | SPAM |
| We shall be having our class tomorrow at noon. | NOT SPAM |
| Our records show you overpaid for (a product or service). Kindly supply your bank routing and account number to receive your refund. | SPAM |
| Hello. I hope your night was great. | HAM |

*Table 1: Table of Spam/Ham for sample test cases*

**Sentiment Analysis**

For this next part of the project, pytorch library is utilized. Fortunately, it already has certain features installed that will help us work more quickly. For NLP projects, the torch.text library is a fantastic resource as it includes a loader for various popular NLP datasets, including the one we will used for the project, as well as a whole pipeline for data abstraction, data vectorization, data loaders, and data iteration.

To determine how data has to be preprocessed, we will utilize the field method of the data class. The preprocessing will be determined by the arguments we put into that function; we will only change a few parameters and leave the rest at their default values.

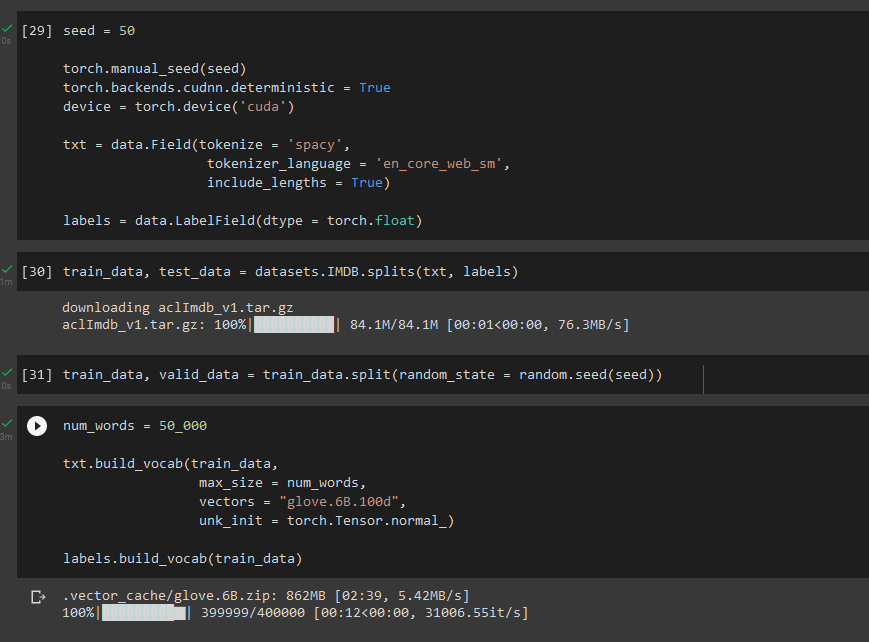
The first parameter, our tokenizer, is spacy, a potent tool for one-line tokenization, which controls how the sentences will be split down or tokenized in NLP standard. Although the default just tokenizes the string based on blank spaces, we advise using this. Additionally, we must instruct the spacy tokenizer on which language model to employ.

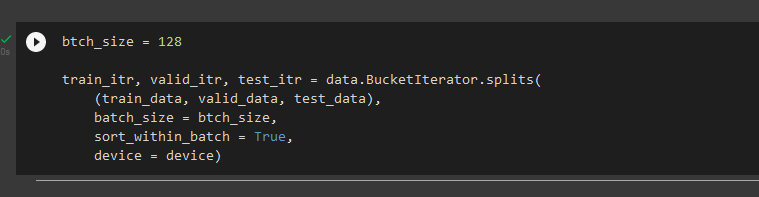
To do Python sentiment analysis, the IMDB dataset is retrieved and divided into train, test, and validation splits. Validation set is further generated from the dataset, which has previously been split into a train and test set. Afterwards, the number of words the model learns is limited to 25000; this will take the 25000 most frequently used terms from the dataset as training data as a result decreasing the model's workload considerably while maintaining accuracy.

Finally, we organize the data we have into a training, testing, and validation batch in order to get it ready to be given to the model in batches of 64 samples at a time.

If a memory problem occurs, its value can be changed.

The following is the source code screenshots responsible for this:





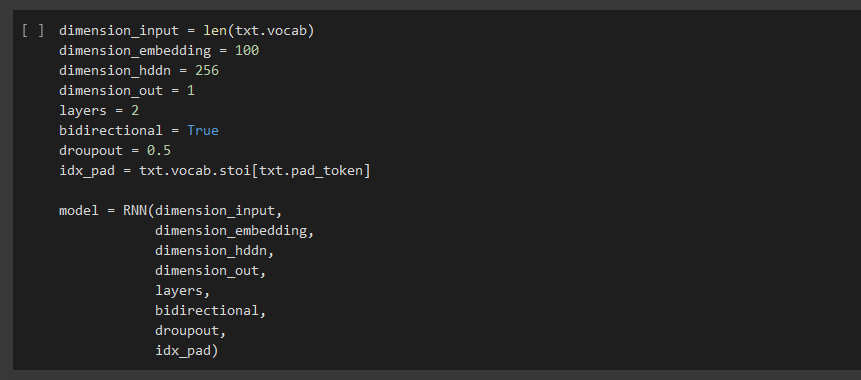
*Figure 7: Screenshots for data preparation and train/test splitting*

Now that the model is ready, its architecture is established. The next stage involves employing a LSTM RNN.

A multi-layer bidirectional RNN will be used. That implies that several RNN layers will be layered on top of one another. The motivation behind having more context than a single directional network is found in bidirectional RNNs. For instance, if a model needs to infer the next word in a phrase that is flowing through it, it would do so based on prior information. However, when two networks run in opposing directions and are piled on top of one another in a bidirectional network, it will also know what comes next. Both the sequence and the direction of the input are the reverse.

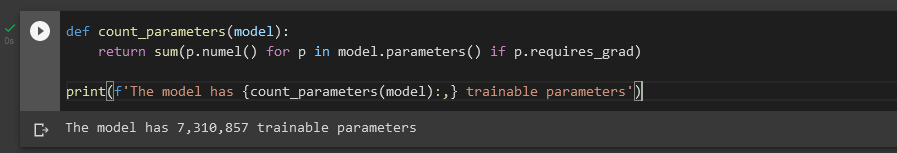
The parameters for the Python sentiment analysis model are then defined, and they are sent to an instance of the model class we just created. The throughput rate, hidden layer, output dimension, number of input parameters, and bidirectionality boolean are all defined. The vocabulary's pad token index that we produced before is also provided.

Below is a screenshot of the source code illustrating this:



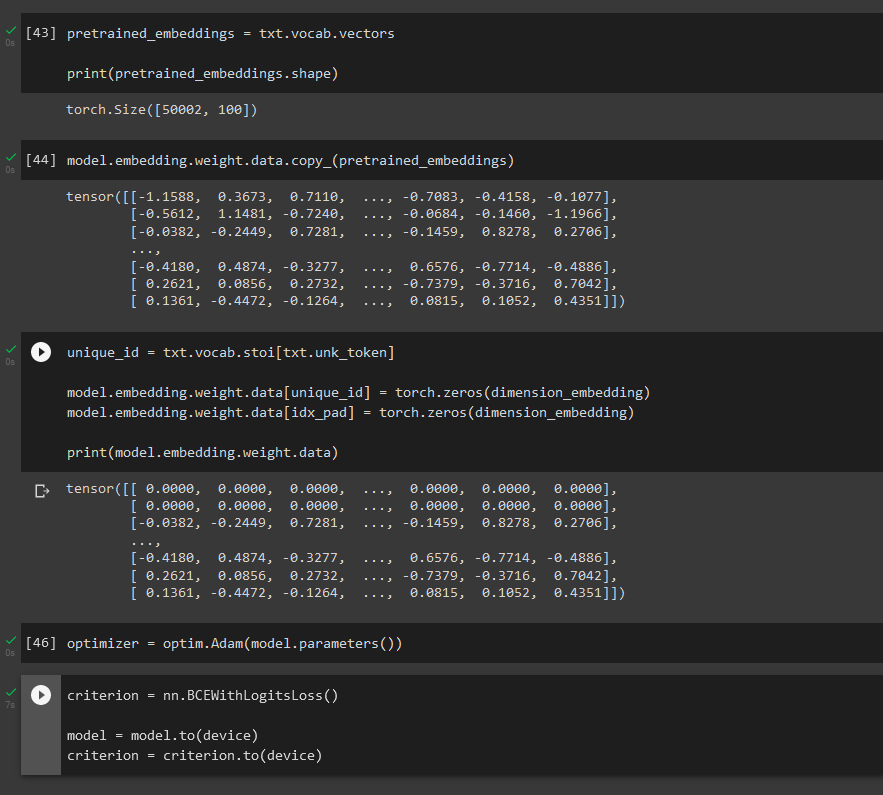
*Figure 8: Screenshot for the parameters for sentiment analysis*

We then print certain model-related information determining how many trainable parameters are included in the model as shown below:



*Figure 9: Screenshot for number of trainable parameters*

The pre-trained embedding weights are then obtained and copied to our model, allowing it to concentrate just on the task at hand—learning the feelings associated with those embeddings—instead of having to learn the embeddings. The original embedding weights are swapped out for pre-trained ones.

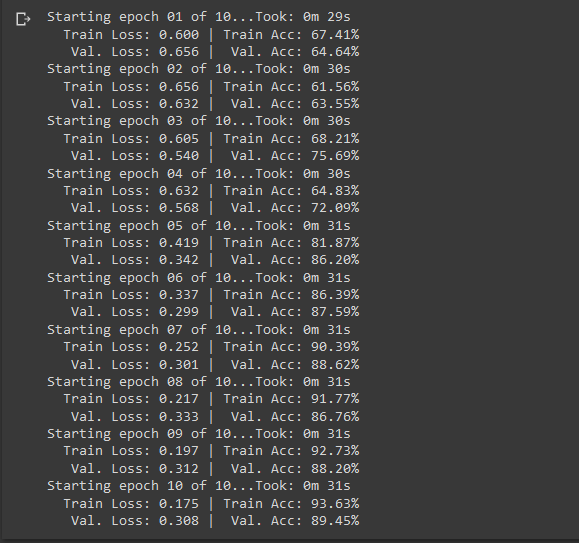


*Figure 10: Screenshot for model operations such as embedding*

The next tasks are now for training and assessing the sentiment analysis model. The binary accuracy function, which we'll use to determine the model's correctness each time, is the first one. We specify the model training and model evaluation function. Here, the procedure is typical. The number of iterations in each epoch is determined by the batch size that we set, and we begin by looping over all of them. The model is given the text, and we obtain the predictions from it. We then calculate the loss for each iteration and propagate that loss backward. The only significant difference between the evaluating function and the training function is that we employ torch instead of backward propagating the loss through the model. No gradient descent is basically what torch.nograd means when assessing.

The training started after setting the number of epochs to 10. In order to comprehend or plot the training curve at a later level, we add the training and validation loss at each stage. The sentiment analysis model in Python with the lowest validation loss is saved. The model's saved checkpoint is then loaded and put it to the test on the earlier-made test set.

We acquired a respectable accuracy score of 89.45% during the dry run of the Python sentiment analysis model as can be seen in the next screenshot:



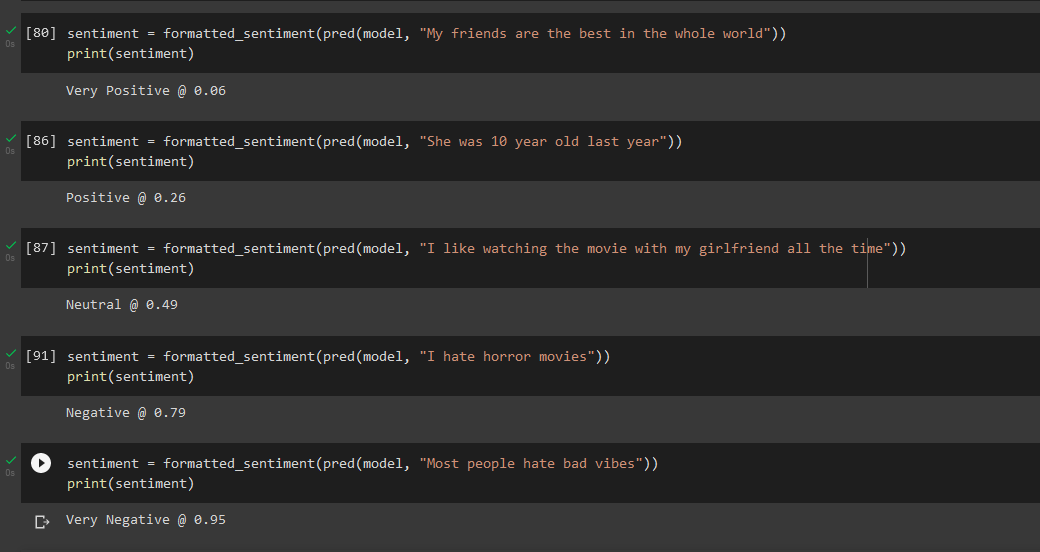
*Figure 11: Screenshot for epoch operations*

**Preliminary results for sentiment analysis**

On our data, we can additionally test the model. We will send it pertinent information for verification as it has been trained to classify movie reviews into very positive, positive, neutral, negative and very negative categories. In order to tokenize the data, we must provide the model, we will import and load Spacy.

Initially, when defining the preprocessing, we utilized the spacy library's built-in torch.text; however, in this case, we are not utilizing batches, and the necessary preprocessing may be handled by the spacy library. For this, we develop a predict sentiment function. Following preprocessing, we turn data into tensors so that it can be sent to the model.

The following are sample results for test texts for sentiment analysis:



*Figure 12: Screenshot for sample sentiment analysis test cases*

As it can be seen, classification is either of the following:

* Very positive
* Positive
* Neutral
* Negative
* Very negative

**Project Management**

Implementation Status Report

* Work Completed

Description: Dataset Collection

Responsibility: Nathisha Marru, Shishira Rudrabhatla

Contribution: Both contributed 50 percent each to the task of dataset collection

Description: Building Model

Responsibility: Venkata Sai Rahul Kumar, Nathisha Marru

Contribution: Model of Spam filtering is built and tested and found accuracy and all teammates contributed to this task as this is major task in project.

Description: Exploratory Data Analysis

Responsibility: Abhishek Rangineni, Shishira Rudrabhatla

Contribution: Exploratory data analysis is key for future tasks, so each contributed 50 percent as their part.

* Work to be Completed

Description: Sentiment Analysis

Responsibility: Nathisha Marru, Shishira Rudrabhatla, Venkata Sai Rahul Kumar

Issues: As suggested we want to add new module so learning it and incorporating is a tough thing.

Description: Combining both Spam filtering and sentiment analysis

Responsibility: Abhishek Rangineni, Venkata Sai Rahul Kumar, Shishira Rudrabhatla

Issues: We have many tasks involving each of them separately but involving both is big task

Description: Model testing and training

Responsibility: Abhishek Rangineni, Venkata Sai Rahul Kumar, Nathisha Marru, Shishira Rudrabhatla,

Issues: As we combined both the spam filtering and sentiment analysis, we need to build new neural network model.

**References/Bibliography**

Ezpeleta, E., Zurutuza, U., & Gómez Hidalgo, J. M. (2016, April). Does sentiment analysis help in bayesian spam filtering?. In *International Conference on Hybrid Artificial Intelligence Systems* (pp. 79-90). Springer, Cham.

Ghiassi, M., Lee, S., & Gaikwad, S. R. (2022). Sentiment analysis and spam filtering using the YAC2 clustering algorithm with transferability. *Computers & Industrial Engineering*, *165*, 107959.

Whitelaw, C., Garg, N., & Argamon, S. (2005, October). Using appraisal groups for sentiment analysis. In *Proceedings of the 14th ACM international conference on Information and knowledge management* (pp. 625-631).

Debnath, K., & Kar, N. (2022, May). Email Spam Detection using Deep Learning Approach. In *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)* (Vol. 1, pp. 37-41). IEEE.

Ismail, S. S., Mansour, R. F., El-Aziz, A., Rasha, M., & Taloba, A. I. (2022). Efficient E-Mail Spam Detection Strategy Using Genetic Decision Tree Processing with NLP Features. *Computational Intelligence and Neuroscience*, *2022*.

<https://www.researchgate.net/publication/220553508_Survey_on_Spam_Filtering_Techniques>

<https://www.researchgate.net/publication/228940659_Using_old_spam_and_ham_samples_to_train_email_filters>

<https://link.springer.com/article/10.1007/s10462-022-10195-4>

<https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset>

<https://www.kaggle.com/datasets/nitishabharathi/email-spam-dataset?select=lingSpam.csv>

<https://www.kaggle.com/datasets/karthickveerakumar/spam-filter>

<https://www.sciencedirect.com/science/article/pii/S2405844018353404#fig5>