Project 1: Scam detection with naïve Bayes

Kevin Yu
Student ID: 1462539
The University of Melbourne

April 16, 2025

1 Supervised model training

The prior probability of **non-malicious class was** 0.7995 (rounded to 4 d.p.), while the **scam class was** 0.2005. This indicates that the dataset is imbalanced, with a higher proportion of non-malicious instances. The distribution aligns well with real-world data, where non-malicious messages significantly outnumber spam.

Table 1 shows the top 10 most "probable" words for each class, based on the conditional probability $P(w \mid c)$. In contract, Table 2 shows the top 10 most "predictive" words for each class, calculated by the ratio, $P(w \mid c)/P(w \mid \neg c)$. Notably, the words in each table differ; although both measure the association of words with a particular class, they serve a slightly different purpose.

For example, most probable words include words such as 'call' ($p = 0.0274$), 'customer' ($p = 0.0092$) and 'reply' ($p = 0.0080$). These words appear frequently in scam messages, which makes them probable; however, intuitively, we expect legitimate messages to frequently contain such words, especially those from customer service. In contrast, the most predictive words include terms such as 'prize' ($p = 88.80$) and 'claim' ($p = 41.21$). These words can appear in legitimate context, however, they are far more likely to be used in scam messages. (How often do you randomly win a prize?)

For non-malicious messages, the most predictive words include slang such as 'lor' ($p = 32.16$), 'wat' ($p = 19.53$) and 'lol' ($p = 17.80$). These casual words are more likely to be used in non-malicious messages, and are not commonly found in scam messages. This serves as a good example of how the model can learn to distinguish between the two classes based on word usage.

Overall, the result is reasonable and it seems feasible to distinguish between scam and non-malicious messages using a multinomial naïve Bayes model. The differences in both frequent and predictive vocabulary across classes suggest the model can effectively learn class-specific language patterns, despite the simplicity of its assumptions.

Scam Class		**Non-malicious Class**	
Word	**Probability**	**Word**	**Probability**
call	0.0274	go	0.0161
free	0.0137	get	0.0143
claim	0.0100	gt	0.0085
customer	0.0092	lt	0.0084
txt	0.0090	call	0.0083
ur	0.0085	ok	0.0078
text	0.0082	come	0.0075
stop	0.0082	ur	0.0075
reply	0.0080	know	0.0075
mobile	0.0078	good	0.0071

Table 1: Top 10 most probable words for each class

Scam Class		Non-malicious Class	
Word	$P(w \mid \textbf{scam})/P(w \mid \textbf{ham})$	**Word**	$P(w \mid \textbf{ham})/P(w \mid \textbf{scam})$
prize	88.80	gt	60.30
tone	57.46	lt	59.73
select	41.79	lor	32.16
claim	41.21	hope	27.57
50	34.82	ok	27.57
paytm	33.08	da	22.40
code	31.34	let	20.10
award	28.73	wat	19.53
won	27.86	oh	18.38
18	26.12	lol	17.80

Table 2: Top 10 most predictive words for each classe based on likelihood ratios

2 Supervised model evaluation

The classifier achieved an **accuracy of** 0.9700, with **precision** = 0.9381, **recall** = 0.9100 and an **F1 score of** 0.9239 (scam as positive class). The model's performance is quite good, indicating that it is effective in distinguishing between scam and non-malicious messages.

The confusion matrix in Figure 1 highlights a high count of true positives and true negatives, supporting the model's effectiveness.

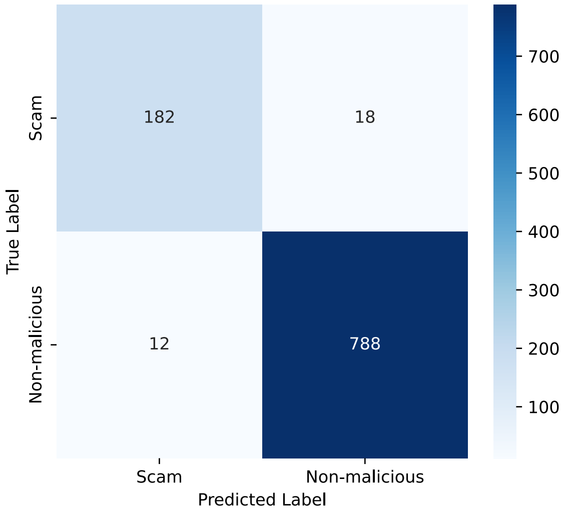

Figure 1: Confusion Matrix for Supervised Model.

Our model encountered 179 **out-of-vocabulary words**, accounting for only 1.6320% of the total. These are likely rare or gibberish words, suggesting the vocabulary covers the dataset well.

Table 3 displays examples of high-confidence scam predictions with a measure of confidence, which is computed as the ratio of the posterior probabilities for each class. It often reference fake rewards from telecom companies and include words like ‘call’, ‘award’ and ‘claim’—strong indicators per Table 2. Due to the naive Bayes’ multiplicative nature, confidence ratios can be very large, reaching up to 10^{17}.

Likewise, for high confidence non-malicious predictions, the messages are often casual, with words like ‘ok’, ‘good’ and ‘wat’. It also includes systemetic transaction messages. While the use of formal language might intuitively align with the scam class, it is important to note that legitimate transactions are typically redacted. For example, the first text in High Confidence Non-Malicious Predictions has reference number, money and time redacted—unlike the scam messages. Additionally, such transations’ raw text uses HTML entity encoding such as `&lt;`(<) and `&gt;`(>) to to enclose redacted content. As shown in Table 2, these tokens are highly predictive of the non-malicious class.

For boundary cases, it often contain neutral vocabulary that does not strongly indicate either class, or mix of words from both classes.

Overall, the **model’s predictions are reasonable** and align with the expected patterns of scam and non-malicious messages.

High Confidence Scam Predictions	
Text	**Confidence Ratio**
Todays Vodafone numbers ending 5347 are selected to receive a Rs.2,00,000 award. If you have a match please call 6299257179 quoting claim code 2041 standard rates apply	1.87×10^{17}
Todays Vodafone numbers ending 3156 are selected to receive a Rs.2,00,000 award. If you have a match please call 7908807538 quoting claim code 9823 standard rates apply	1.40×10^{17}
Todays Voda numbers ending 5226 are selected to receive a ?350 award. If you have a match please call 08712300220 quoting claim code 1131 standard rates apply	1.07×10^{17}

Table 3: High Confidence Scam Predictions

High Confidence Non-Malicious Predictions	
Text	**Confidence Ratio**
NEFT Transaction with reference number <#> for Rs. <DECIMAL> has been credited to the beneficiary account on <#> at <TIME>: <#>	1.18×10^{-17}
no, i *didn’t* mean to post it. I wrote it, and like so many other times i’ve written stuff to you, i let it sit there. It WAS what I was feeling at the time. I was angry...	2.34×10^{-16}
U wake up already? Wat u doing? U picking us up later rite? I’m taking sq825, reaching ard 7 smth 8 like dat. U can check e arrival time. C ya soon...	7.95×10^{-14}

Table 4: High Confidence Non-Malicious Predictions

Boundary Cases (Confidence Ratio ≈ 1)	
Text	**Confidence Ratio**
I've told him that I've returned it. That should I re-order it.	1.00
Glad to see your reply.	1.08
ALRITE SAM ITS NIC JUST CHECKIN THAT THIS IS UR NUMBER-SO IS IT?T.B*	0.90

Table 5: Boundary Cases (Confidence Ratio ≈ 1)

3 Extending the model: Active Learning

For this section, I have chose to implement **Option 2: Active Learning**, where 200 instances of the "unlabelled" data was carefully incorporated to improve the model.

The process began by passing through `sms_unlabelled.csv` to the model trained on the original `sms_supervised_train.csv`. For each message, the model produced a predicted class label along with a confidence score, where the computation is outlined in Section 2 and more detailed in the Jupyter Notebook.

Then, the original supervised data set was split into a training set (80%) and a validation set (20%). I then explored **three selection strategies** for choosing 200 unlabelled instances:

- **Random selection**: serves as a naive baseline, assuming all instances are equally informative.
- **Low-confidence selection**: selects instances near the decision boundary ($R \approx 1$).
- **High-confidence selection**: selects instances where the model is very certain (very high or very low R).

The lowest-confidence strategy was chosen to explore the intuition behind active learning—when model is uncertain, it adjust to gain clarification. These ambiguous instances

Model	Accuracy	Precision	Recall	F1 Score	Error Rate
Random 200	0.9650	0.8837	0.9500	0.9157	0.0350
Low-Confidence 200	0.9750	0.9070	0.9750	0.9398	0.0250
High-Confidence 200	0.9550	0.8605	0.9250	0.8916	0.0450

Table 6: Evaluation metrics for different semi-supervised augmentation strategies.

4 Discussion

Interpret the results and discuss their implications. Highlight any limitations or challenges encountered.

5 Conclusion

Summarize the key findings and contributions of the report. Suggest future work or improvements.

References

1. Author Name, *Title of the Paper/Book*, Publisher, Year.
2. Author Name, "Title of the Article," *Journal Name*, vol. X, no. Y, pp. Z, Year.

Since the dataset is already preprocessed, I'm directly supplying vocabulary=vocabulary to CountVectorizer without calling fit(), to avoid any unintended token filtering (e.g., removing tokens like 'hi') that may occur with the default tokenizer during fitting.