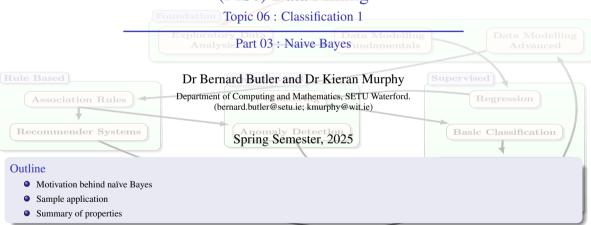
Data Mining (Week 1)

(MSc) Data Mining

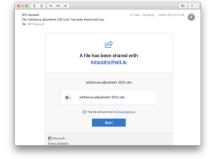


Outline

1. Motivation — Spam Filtering

Spam Filtering

Reality



Simplified Problem

Assume that we have the following set of messages previously classified as spam or ham.

Class
spam
ham
ham
spam
spam
spam

We are interested in classifying the following new message as spam or ham:

Message	Class
"review us now"	?

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam

Word	# in spam	# in ham	Pr(• spam)	$\Pr(\bullet \textbf{ham})$
account				
password				
review				
send				
us				
your				

Class	Count	Probability
spam		
ham		

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam

Word	# in spam	# in ham	Pr(• spam)	$\Pr(\bullet \textbf{ham})$
account				
password				
review				
send				
us				
your				

Class	Count	Probability
spam	4	$\Pr(\text{spam}) = 4/6$
ham	2	$\Pr(\mathbf{ham}) = 2/6$

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam

Word	# in spam	# in ham	Pr(• spam)	Pr(• ham)
account	1	0	1/4	0/2
password				
review				
send				
us				
your				

Class	Count	Probability
spam	4	$\Pr(\text{spam}) = 4/6$
ham	2	$\Pr(\text{ham}) = 2/6$

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam

Word	# in spam	# in ham	Pr(• spam)	Pr(• ham)
account	1	0	1/4	0/2
password	2	1	2/4	1/2
review	1	2	1/4	2/2
send	3	1	3/4	1/2
us	3	1	3/4	1/2
your	3	1	3/4	1/2

Class	Count	Probability
spam	4	$\Pr(\text{spam}) = 4/6$
ham	2	$\Pr(\text{ham}) = 2/6$

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam
_	

Word	# in spam	# in ham	Pr(• spam)	Pr(• ham)
account	1	0	1/4	0/2
password	2	1	2/4	1/2
review	1	2	1/4	2/2
send	3	1	3/4	1/2
us	3	1	3/4	1/2
your	3	1	3/4	1/2

Class	Count	Probability
spam	4	$\Pr(\text{spam}) = 4/6$
ham	2	$\Pr(\text{ham}) = 2/6$

What we have

The probability that a message contains, say the word review, among our message classed as spam, i.e.,

$$\Pr(\text{review}|\text{spam}) = 1/4$$

What we want

The probability that a message is spam given that it contains, say the word review, i.e.,

$$\Pr(\text{spam}|\text{review}) = ?$$

Message	Class
"send us your password"	spam
"send us your review"	ham
"password review"	ham
"review us"	spam
"send your password"	spam
"send us your account"	spam

Word	# in spam	# in ham	Pr(• spam)	Pr(• ham)
account	1	0	1/4	0/2
password	2	1	2/4	1/2
review	1	2	1/4	2/2
send	3	1	3/4	1/2
us	3	1	3/4	1/2
your	3	1	3/4	1/2

prior probabilities

Class	Count	Probability
spam	4	$\Pr(\text{spam}) = 4/6$
ham	2	Pr(ham) = 2/6

What we have

The probability that a message contains, say the word review, among our message classed as spam, i.e.,

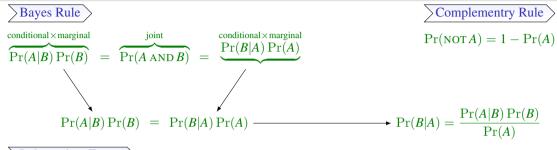
$$Pr(review|spam) = 1/4$$

What we want

The probability that a message is spam given that it contains, say the word review, i.e.,

$$\Pr(\text{spam}|\text{review}) = ?$$

Aside: Probability Laws



Independent Events

If events *A* and *B* are independent, then Pr(A AND B) = Pr(A) Pr(B)

Law of total of probability

Let A be any event. Let $\{B_1, B_2, B_3, \dots, B_n\}$ be a set of events, exactly one of which must occur, then

$$Pr(A) = Pr(A|B_1) Pr(B_1) + Pr(A|B_2) Pr(B_2) + \cdots + Pr(A|B_n) Pr(B_n)$$

Applying the law of total probability, with A = review, and $B_1 = \text{spam}$ and $B_2 = \text{ham}$, then we have

$$\Pr(\text{review}) = \Pr(\text{review}|\text{spam}) \Pr(\text{spam}) + \Pr(\text{review}|\text{ham}) \Pr(\text{ham}) = \frac{1}{4} \cdot \frac{4}{6} + \frac{2}{2} \cdot \frac{2}{6} = \frac{3}{6}$$

Now we can apply Bayes rule, with A = review and B = spam we have

$$\Pr(\text{spam}|\text{review}) = \frac{\Pr(\text{review}|\text{spam})\Pr(\text{spam})}{\Pr(\text{review})} = \frac{\frac{1}{4} \cdot \frac{4}{6}}{\frac{3}{6}} = \frac{1}{3} = 33.3\%$$

And we can apply Bayes rule, with A = review and B = ham to ge

$$\Pr(\text{ham}|\text{review}) = \frac{\Pr(\text{review}|\text{ham})\Pr(\text{ham})}{\Pr(\text{review})} = \frac{\frac{2}{2} \cdot \frac{2}{6}}{\frac{3}{6}} = \frac{2}{3} = 66.7\%$$

Applying the law of total probability, with A = review, and $B_1 = \text{spam}$ and $B_2 = \text{ham}$, then we have

$$\Pr(\text{review}) = \Pr(\text{review}|\text{spam}) \Pr(\text{spam}) + \Pr(\text{review}|\text{ham}) \Pr(\text{ham}) = \frac{1}{4} \cdot \frac{4}{6} + \frac{2}{2} \cdot \frac{2}{6} = \frac{3}{6}$$

Now we can apply Bayes rule, with A = review and B = spam we have

$$\Pr(\text{spam}|\text{review}) = \frac{\Pr(\text{review}|\text{spam})\Pr(\text{spam})}{\Pr(\text{review})} = \frac{\frac{1}{4} \cdot \frac{4}{6}}{\frac{3}{6}} = \frac{1}{3} = 33.3\%$$

And we can apply Bayes rule, with A = review and B = ham to get

$$\Pr(\text{ham}|\text{review}) = \frac{\Pr(\text{review}|\text{ham})\Pr(\text{ham})}{\Pr(\text{review})} = \frac{\frac{2}{2} \cdot \frac{2}{6}}{\frac{3}{6}} = \frac{2}{3} = 66.7\%$$

Applying the law of total probability, with A = review, and $B_1 = \text{spam}$ and $B_2 = \text{ham}$, then we have

$$\Pr(\text{review}) = \Pr(\text{review}|\text{spam}) \Pr(\text{spam}) + \Pr(\text{review}|\text{ham}) \Pr(\text{ham}) = \frac{1}{4} \cdot \frac{4}{6} + \frac{2}{2} \cdot \frac{2}{6} = \frac{3}{6}$$

Now we can apply Bayes rule, with A = review and B = spam we have

$$\Pr(\text{spam}|\text{review}) = \frac{\Pr(\text{review}|\text{spam})\Pr(\text{spam})}{\Pr(\text{review})} = \frac{\frac{1}{4} \cdot \frac{4}{6}}{\frac{3}{6}} = \frac{1}{3} = 33.3\%$$

And we can apply Bayes rule, with A =review and B =ham to get

$$\Pr(\text{ham}|\text{review}) = \frac{\Pr(\text{review}|\text{ham})\Pr(\text{ham})}{\Pr(\text{review})} = \frac{\frac{2}{2} \cdot \frac{2}{6}}{\frac{3}{6}} = \frac{2}{3} = 66.7\%$$

Applying the law of total probability, with A = review, and $B_1 = \text{spam}$ and $B_2 = \text{ham}$, then we have

$$\Pr(\text{review}) = \Pr(\text{review}|\text{spam}) \Pr(\text{spam}) + \Pr(\text{review}|\text{ham}) \Pr(\text{ham}) = \frac{1}{4} \cdot \frac{4}{6} + \frac{2}{2} \cdot \frac{2}{6} = \frac{3}{6}$$

Now we can apply Bayes rule, with A = review and B = spam we have

$$\Pr(\text{spam}|\text{review}) = \frac{\Pr(\text{review}|\text{spam})\Pr(\text{spam})}{\Pr(\text{review})} = \frac{\frac{1}{4} \cdot \frac{4}{6}}{\frac{3}{6}} = \frac{1}{3} = 33.3\%$$

And we can apply Bayes rule, with A =review and B =ham to get

$$\Pr(\text{ham}|\text{review}) = \frac{\Pr(\text{review}|\text{ham})\Pr(\text{ham})}{\Pr(\text{review})} = \frac{\frac{2}{2} \cdot \frac{2}{6}}{\frac{3}{6}} = \frac{2}{3} = 66.7\%$$

• We can now (hopefully) do this for each word in our test message ("review us now"), but what about classifying using multiple words? ... here comes the naïve bit ...

Naïve Bayes assumes that presence of each word are independent events

Recall: independent events means can multiply to get joint probabilities.

We are interested in classifying the messag

review us now

 We don't have data on the word now so only looking at messages containing review and us and no containing account, password. send, or your.

$$\Pr(\{\text{review}, \text{us}\}|\text{spam}) = \underbrace{\left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right)\left(\frac{1}{4}\right)\left(1 - \frac{3}{4}\right)\left(\frac{3}{4}\right)\left(1 - \frac{3}{4}\right)}_{\text{account}} \underbrace{\left(1 - \frac{3}{4}\right)\left(1 - \frac{3}{4}\right)\left(1 - \frac{3}{4}\right)}_{\text{passwerd}} \underbrace{\left(1 - \frac{3}{4}\right)\left(1 - \frac{3}{4}\right)\left(1 - \frac{3}{4}\right)}_{\text{your}} = 0.0044$$

and

$$\Pr(\{\text{review}, \text{us}\}|\text{ham}) = \underbrace{\left(1 - \frac{0}{2}\right) \left(1 - \frac{1}{2}\right) \left(\frac{2}{2}\right) \left(1 - \frac{1}{2}\right) \left(\frac{1}{2}\right) \left(1 - \frac{1}{2}\right)}_{\text{account}} \underbrace{\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2}\right)}_{\text{password}} \underbrace{\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2}\right)}_{\text{your}} = 0.0625$$

• We can now (hopefully) do this for each word in our test message ("review us now"), but what about classifying using multiple words? ... here comes the naïve bit ...

Naïve Bayes assumes that presence of each word are independent events

Recall: independent events means can multiply to get joint probabilities.

• We are interested in classifying the message

review us now

 We don't have data on the word now so only looking at messages containing review and us and not containing account, password. send, or your.

$$\Pr(\{\text{review}, \text{us}\}|\text{spam}) = \underbrace{\left(1 - \frac{1}{4}\right)\left(1 - \frac{2}{4}\right)\left(\frac{1}{4}\right)\left(1 - \frac{3}{4}\right)\left(\frac{3}{4}\right)\left(1 - \frac{3}{4}\right)}_{\text{geopunt}} = 0.0044$$

and

$$\Pr(\{\text{review}, \text{us}\}|\text{ham}) = \underbrace{\left(1 - \frac{0}{2}\right) \underbrace{\left(1 - \frac{1}{2}\right)}_{\text{account}} \underbrace{\left(\frac{2}{2}\right) \underbrace{\left(1 - \frac{1}{2}\right)}_{\text{review}} \underbrace{\left(\frac{1}{2}\right) \underbrace{\left(1 - \frac{1}{2}\right)}_{\text{your}} \underbrace{\left(1 - \frac{1}{2}\right)}_{\text{your}} = 0.0625$$

• We can now (hopefully) do this for each word in our test message ("review us now"), but what about classifying using multiple words? ... here comes the naïve bit ...

Naïve Bayes assumes that presence of each word are independent events

Recall: independent events means can multiply to get joint probabilities.

• We are interested in classifying the message

review us now

 We don't have data on the word now so only looking at messages containing review and us and not containing account, password. send, or your.

$$\Pr(\{\text{review}, \text{us}\}|\text{spam}) = \underbrace{\left(1 - \frac{1}{4}\right) \left(1 - \frac{2}{4}\right) \left(\frac{1}{4}\right) \left(1 - \frac{3}{4}\right) \left(\frac{3}{4}\right) \left(1 - \frac{3}{4}\right)}_{\text{account}} \underbrace{\left(1 - \frac{3}{4}\right) \left(1 - \frac{3}{4}\right) \left(1 - \frac{3}{4}\right)}_{\text{password}} \underbrace{\left(1 - \frac{3}{4}\right) \left(1 - \frac{3}{4}\right) \left(1 - \frac{3}{4}\right)}_{\text{your}} = 0.0044$$

and

$$\Pr(\{\text{review}, \text{us}\}|\text{ham}) = \underbrace{\left(1 - \frac{0}{2}\right) \left(1 - \frac{1}{2}\right) \left(\frac{2}{2}\right) \left(1 - \frac{1}{2}\right) \left(\frac{1}{2}\right) \left(\frac{1}{2}\right) \left(1 - \frac{1}{2}\right)}_{\text{account}} \underbrace{\left(1 - \frac{1}{2}\right) \left(\frac{2}{2}\right) \left(1 - \frac{1}{2}\right) \left(\frac{1}{2}\right) \left(1 - \frac{1}{2}\right)}_{\text{your}} = 0.0625$$

Now we can apply the law of total probability as before

$$\begin{split} \Pr(\{\text{review}, \text{us}\}) = & \Pr(\{\text{review}, \text{us}\}|\text{spam}) \Pr(\text{spam}) + \Pr(\{\text{review}, \text{us}\}|\text{ham}) \Pr(\text{ham}) \\ = & 0.0044 \left(\frac{4}{6}\right) + 0.0625 \left(\frac{2}{6}\right) = 0.0237 \end{split}$$

And finally Bayes rule

$$\Pr(\text{spam}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\text{spam}) \Pr(\text{spam})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0044 \left(\frac{4}{6}\right)}{0.0237} = 0.123$$

and

$$\Pr(\text{ham}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\text{ham})\Pr(\text{ham})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0625\left(\frac{2}{6}\right)}{0.0237} = 0.877$$

Hence, the probability that the message is spam is 12.3%, and ham is 87.7%.

Now we can apply the law of total probability as before

$$\Pr(\{\text{review}, \text{us}\}) = \Pr(\{\text{review}, \text{us}\}|\text{spam}) \Pr(\text{spam}) + \Pr(\{\text{review}, \text{us}\}|\text{ham}) \Pr(\text{ham})$$
$$= 0.0044 \left(\frac{4}{6}\right) + 0.0625 \left(\frac{2}{6}\right) = 0.0237$$

And finally Bayes rule

$$\Pr(\underset{\text{spam}}{\text{spam}}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\underset{\text{spam}}{\text{spam}})\Pr(\underset{\text{spam}}{\text{spam}})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0044\left(\frac{4}{6}\right)}{0.0237} = 0.123$$

and

$$\Pr(\text{ham}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\text{ham})\Pr(\text{ham})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0625\left(\frac{2}{6}\right)}{0.0237} = 0.877$$

Hence, the probability that the message is spam is 12.3%, and ham is 87.7%.

A final comment:

• The classifier picks the class with the largest probability, so in this case

$$\Pr(\underset{\text{spam}}{\text{spam}}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\underset{\text{spam}}{\text{spam}})\Pr(\underset{\text{spam}}{\text{spam}})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0044\left(\frac{4}{6}\right)}{0.0237} = 0.123$$

and

$$\Pr(\text{ham}|\{\text{review}, \text{us}\}) = \frac{\Pr(\{\text{review}, \text{us}\}|\text{ham})\Pr(\text{ham})}{\Pr(\{\text{review}, \text{us}\})} = \frac{0.0625\left(\frac{2}{6}\right)}{0.0237} = 0.877$$

• We can skip the computation of $\Pr(\{\text{review}, \text{us}\})$ involving the law of total probability step since that is a common denominator in above formula, And instead look are relative likelihood

$$\frac{\Pr(\text{spam}|\{\text{review}, \text{us}\})}{\Pr(\text{ham}|\{\text{review}, \text{us}\})} = \frac{\Pr(\{\text{review}, \text{us}\}|\text{spam}) \Pr(\text{spam})}{\Pr(\{\text{review}, \text{us}\}|\text{ham}) \Pr(\text{ham})} \quad \Longrightarrow \begin{cases} > 1 & \text{pick spam} \\ < 1 & \text{pick ham} \end{cases}$$

Outline

2. Application — Trump's Claims

10

Trump's Claims — Dataset

The Washington Post has released a curated list of Donald Trump's false claims while in office. The claim's have been categorised and cross linked. We will see how well a naïve Bayes classifier will do on this dataset.

```
df = pd.read_csv("wapo_trumpclaims_export-012021.csv.gz")
print(df.shape)
df.head(5)
```

(30573, 9)

id location	claim	analys	is pinocchios	category	repeated_ids	repeated_count	date
	"We also got tax cuts, the largest tax cut and	This is Trump's second favorite falsehood, and	4.0	Taxes	31608, 31581, 31305, 31183, 31530, 30920, 3085	296	01/20/2021
	"We just got seventy five million votes. And t	When the counting was finished, Trump had rece	NaN	Election	31609, 31292, 31155, 31016, 31082, 30992, 3156	19	01/20/2021
	"One of the things we're very, very proud of i	Contrary to his boasts, Trump did not achieve	NaN	Miscellaneous	31610, 31598, 31187, 30918, 30374, 29845, 2922	84	01/20/2021
	"Our first lady has been a woman of great grac	In reality, Melania Trump leaves the White Hou	NaN	Miscellaneous	NaN	0	01/20/2021
	"That's why [regulation cuts] we have such goo	Leaving aside Trump's claim about the impact o	NaN	Jobs	NaN	0	01/20/2021

Trump's Claims — Dataset

df.category.value_counts(dropna=False)

Immigration	3225
Foreign policy	3165
Election	3037
Miscellaneous	2767
Coronavirus	2521
Trade	2513
Economy	2475
Russia	1838
Jobs	1732
Health care	1629
Ukraine probe	1377
Environment	1065
Biographical record	963
Taxes	857
Crime	852
NaN	169
Guns	165
Education	151
Terrorism	72
Name: category, dtyp	e:int64

Trump's Claims — Dataset

df.category.value_counts(dropna=**False**)

Immigration	3225
Foreign policy	3165
Election	3037
Miscellaneous	2767
Coronavirus	2521
Trade	2513
Economy	2475
Russia	1838
Jobs	1732
Health care	1629
Ukraine probe	1377
Environment	1065
Biographical record	963
Taxes	857
Crime	852
NaN	169
Guns	165
Education	151
Terrorism	72
Name: category, dtyp	e: int6

General observations ...

- Some classes are relatively rare.
- Some classifications would appear to overlap $Russia \leftrightarrow Election$.
- There are 169 unclassified observations, missing values ... these need to be removed/encoded before model building.
- Total of 30,573 false claims! He was busy between golf sessions ... sorry, I could not resist.

Trump's Claims — Data Preprocessing

We perform our standard train-test split

```
from sklearn.model_selection import train_test_split
X_train, X_test, y_train, y_test = train_test_split(
    df.claim, df.category, test_size=0.2, random_state=42)
```

Next we need to reproduce the word extraction and counts that we did for the simple example earlier:

```
from sklearn.feature_extraction.text import CountVectorizer
count_vectorizer = CountVectorizer()

X_train_counts = count_vectorizer.fit_transform(X_train)
```

```
X_test_counts = count_vectorizer.transform(X_test)
```

Use the train dataset to determine parameters for the operation (fit). Then, apply (transform) to both train and test

Notice the function calls fit_transform on X_train and transform on X_test. The function fit_transform is two separate steps: fit and transform and could be written as

```
count_vectorizer.fit(X_train)
X_train_counts = count_vectorizer.transform(X_train)
```

or

```
X_train_counts = count_vectorizer.fit(X_train).transform(X_train)
```

advisors, adviso

'aironts' 'sirtime' 'sirwaves', 'ajitpaifct' 'ak', 'al', 'alabama', 'aland's', 'alarmed', 'alaska', 'albaghdadi', 'alcindor', 'alcohol', 'alec', 'alert', 'alerted', 'alerting', 'alfred', 'all', 'ali', 'ali

'aid', 'aide', 'aides', 'aides', 'ailment', 'ailments', 'aim', 'aimed', 'aiming', 'ain', 'ainsleyearbardt', 'aint', 'air', 'airborne',

'agenda', 'agent', 'agents', 'ages', 'aggression', 'aggressive', 'aggressively', 'agitated', 'agitators', 'agg

d'. 'alternative'. 'alternatives'. 'although'. 'altogether'. 'aluminum'. 'always'. 'am'. 'amased'. 'amased'. 'amateur'. 'amateurs'. 'amaze'. 'amazed'. 'amazing'. 'amazing'. 'amazon'

analysis' 'analyst' 'analyst' 'analyze' 'analyze' 'analyzing', 'angchist' 'anachist', 'anachist' 'anchor', 'anchor', 'anchor', 'anchor', 'anchor', 'and', 'and', 'and', 'angela', 'angela', 'angela', 'angels',

'alligators', 'allocated', 'allow', 'allowed', 'allowing', 'allows', 'alluding', 'ally', 'allyn', 'almost', 'alone', 'along', 'alongside',

'ambition', 'ambitious', 'amend', 'amendment', 'amer', 'america', 'american', 'americans', 'amicable', 'amid', 'ammunition', 'ampresty', 'amorphous', 'amount', 'amount', 'amount', 'amuck', 'amu', 'amyklobuchar', 'an', 'analogous

'angry', 'anguish', 'anisal', 'anisa

15th', 16', '168', '161', '162', '164', '168', '169', '16th', '17', '171

Trump's Claims — Data Preprocessing

```
How many features?
```

A look at the first 1,000 features ...

ects', 'affh', 'affidavits', 'affirm', 'affirmative',

```
print(count_vectorizer.get_feature_names()[:1000])
```

[100] (000) (000) (005) (006) (006) (006) (006) (007)

As before* we import or model and create an instance of it

```
from sklearn.naive_bayes import MultinomialNB
model = MultinomialNB()
```

Fit our model using the train dataset

```
model.fit(X_train_counts, y_train)
```

Generate predictions using the test dataset

```
y_pred = model.predict(X_test_counts)
```

How well did it do? ... using accuracy score we have

```
from sklearn.metrics import accuracy_score
accuracy_score(y_test, y_pred)
```

```
0.7763525735898701
```

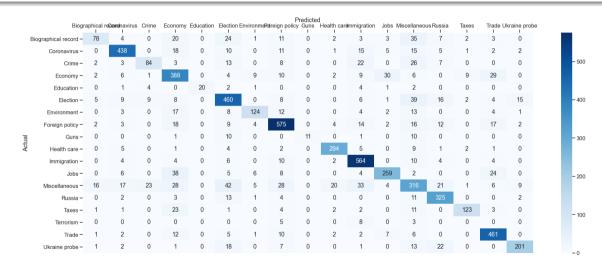
This is not bad ... there are lots of class levels and some overlap between classes.

^{*}This is the beauty of sklearn — consistent interface to all models, pre-/post- processing steps.

Trump's Claims — Model Fit, Prediction and Evaluation

Predicted	Biographical record		Crime	Economy	Education	Election	Environment	Foreign policy	Guns	Health care	Immigration	Jobs	Miscellaneous	Russia	Tax
Actual															
Biographical record	78	4	0	20	0	24	1	11	0	2	3	3	35	7	2
Coronavirus	0	438	0	18	0	10	0	11	0	1	15	5	15	5	1
Crime	2	3	84	3	0	13	0	8	0	0	22	0	26	7	0
Economy	2	6	1	388	0	4	9	10	0	2	9	30	6	0	9
Education	0	1	4	0	20	2	1	0	0	0	4	1	2	0	0
Election	5	9	9	8	0	460	0	8	0	0	6	1	39	16	2
Environment	0	3	0	17	0	8	124	12	0	0	4	2	13	0	0
Foreign policy	2	3	0	18	0	9	4	575	0	4	14	2	16	12	0
Guns	0	0	0	1	0	10	0	0	11	0	1	0	10	0	0
Health care	0	5	0	1	0	4	0	2	0	294	5	0	9	1	2
Immigration	0	4	0	4	0	6	0	10	0	2	564	0	10	4	0
Jobs	0	6	0	38	0	5	6	8	0	0	4	259	2	0	0
Miscellaneous	16	17	23	28	0	42	5	28	0	20	33	4	316	21	1
Russia	0	2	0	3	0	13	1	4	0	0	0	0	11	325	0
Taxes	1	1	0	23	0	1	0	4	0	2	2	0	11	0	123
Terrorism	0	0	0	0	0	0	0	5	0	0	8	0	3	0	0
Trade	1	2	0	12	0	5	1	10	0	2	2	7	6	0	0
Ukraine probe	1	2	0	1	0	18	0	7	0	0	1	0	13	22	0

Trump's Claims — Model Fit, Prediction and Evaluation



• Look at the largest, off main-diagonal entries.

Outline

3. Summary

18

Naïve Bayes Classifier — Review

When to Consider

- Assumption of independence holds
- Categorical features.
- Spam filtering, Sentiment Analysis, and Recommendation Systems (with collaborative filtering).
- Variants exist for numeric (Gaussian-), binary (Bernoulli-) and multi-class (mulinomial-) featured Naïve Bayes.

Advantages

- It is easy and fast to predict class. It also perform well in multi-class prediction.
- When assumption of independence holds, performs better compare to other models like logistic regression and needs less training data.

Disadvantages

- Ignores feature relationships
- If categorical variable has a category (in test data set), which was not observed in training data set, then model will assign a 0 (zero) probability and will be unable to make a prediction. This is often known as "Zero Frequency". To solve this, we can use the smoothing technique. One of the simplest smoothing techniques is Laplace estimation.
- If continuous features, then assumes normality conditions often too restrictive.

Resources

• A Gentle Introduction to Bayes Theorem for Machine Learning

https://machinelearningmastery.com/bayes-theorem-for-machine-learning/

This is well worth a read over a cup of coffee. The author, Jason Brownlee, is worth following.