CS 188: Artificial Intelligence Machine Learning


Instructor: Nicholas Tomlin --- University of California, Berkeley [These slides were created by Dan Klein and Pieter Abbeel for CS188 Intro to AI at UC Berkeley. All CS188 materials are available at http://ai.berkeley.edu.]

## Machine Learning

- Up until now: how use a model to make optimal decisions
- Machine learning: how to acquire a model from data / experience
- Learning parameters (e.g. probabilities)
- Learning structure (e.g. BN graphs)
- Learning hidden concepts (e.g. clustering, neural nets)
- Today: model-based classification with Naive Bayes


## Classification



## Example: Spam Filter

- Input: an email
- Output: spam/ham
- Setup:
- Get a large collection of example emails, each labeled "spam" or "ham"
- Note: someone has to hand label all this data!
- Want to learn to predict labels of new, future emails
- Features: The attributes used to make the ham / spam decision
- Words: FREE!
- Text Patterns: \$dd, CAPS
- Non-text: SenderInContacts, WidelyBroadcast
- ...

Dear Sir.

First, I must solicit your confidence in this transaction, this is by virture of its nature as being utterly confidencial and top secret. ...

TO BE REMOVED FROM FUTURE MAILINGS, SIMPLY REPLY TO THIS MESSAGE AND PUT "REMOVE" IN THE SUBJECT.

99 MILLION EMAIL ADDRESSES FOR ONLY \$99

Ok, Iknow this is blatantly OT but I'm beginning to go insane. Had an old Dell Dimension XPS sitting in the corner and decided to put it to use, I know it was working pre being stuck in the corner, but when I plugged it in, hit the power nothing happened.

## Example: Digit Recognition

- Input: images / pixel grids
- Output: a digit 0-9
- Setup:
- Note: someone has to hand label all this data!
- Want to learn to predict labels of new, future digit images
- Features: The attributes used to make the digit decision
- Pixels: $(6,8)=O N$
- Shape Patterns: NumComponents, AspectRatio, NumLoops
- ...
- Features are increasingly induced rather than crafted


## Other Classification Tasks

- Classification: given inputs $x$, predict labels (classes) y
- Examples:
- Medical diagnosis (input: symptoms, classes: diseases)
- Fraud detection (input: account activity, classes: fraud / no fraud)
- Automatic essay grading (input: document, classes: grades)
- Customer service email routing
- Review sentiment
- Language ID
- ... many more

- Classification is an important commercial technology!

Model-Based Classification


## Model-Based Classification

- Model-based approach
- Build a model (e.g. Bayes' net) where both the output label and input features are random variables
- Instantiate any observed features
- Query for the distribution of the label conditioned on the features
- Challenges
- What structure should the BN have?
- How should we learn its parameters?



## Naïve Bayes for Digits

- Naïve Bayes: Assume all features are independent effects of the label
- Simple digit recognition version:
- One feature (variable) $\mathrm{F}_{\mathrm{ij}}$ for each grid position <i,j>
- Feature values are on / off, based on whether intensity is more or less than 0.5 in underlying image
- Each input maps to a feature vector, e.g.


$$
1 \rightarrow\left\langle F_{0,0}=0 \quad F_{0,1}=0 \quad F_{0,2}=1 \quad F_{0,3}=1 \quad F_{0,4}=0 \ldots F_{15,15}=0\right\rangle
$$

- Here: lots of features, each is binary valued
- Naïve Bayes model: $\quad P\left(Y \mid F_{0,0} \ldots F_{15,15}\right) \propto P(Y) \prod_{i, j} P\left(F_{i, j} \mid Y\right)$
- What do we need to learn?


## General Naïve Bayes

- A general Naive Bayes model:

$$
|\mathrm{Y}| \text { parameters }
$$

$$
P\left(\mathrm{Y}, \mathrm{~F}_{1} \ldots \mathrm{~F}_{n}\right)=P(\mathrm{Y}) \prod_{i} P\left(\mathrm{~F}_{i} \mid \mathrm{Y}\right)
$$



$|Y| x|F|^{n}$ values

$$
\begin{aligned}
& \mathrm{n} \times|\mathrm{F}| \times|\mathrm{Y}| \\
& \text { parameters }
\end{aligned}
$$

- We only have to specify how each feature depends on the class
- Total number of parameters is linear in $n$
- Model is very simplistic, but often works anyway


## Inference for Naïve Bayes

- Goal: compute posterior distribution over label variable $Y$
- Step 1: get joint probability of label and evidence for each label

$$
P\left(Y, f_{1} \ldots f_{n}\right)=\left[\begin{array}{c}
P\left(y_{1}, f_{1} \ldots f_{n}\right) \\
P\left(y_{2}, f_{1} \ldots f_{n}\right) \\
\vdots \\
P\left(y_{k}, f_{1} \ldots f_{n}\right)
\end{array}\right] \quad \begin{array}{|}
P\left(f_{1} \ldots f_{n}\right)
\end{array}
$$

- Step 2: sum to get probability of evidence
- Step 3: normalize by dividing Step 1 by Step 2


$$
P\left(Y \mid f_{1} \ldots f_{n}\right)
$$

## General Naïve Bayes

- What do we need in order to use Naïve Bayes?
- Inference method (we just saw this part)
- Start with a bunch of probabilities: $\mathrm{P}(\mathrm{Y})$ and the $\mathrm{P}\left(\mathrm{F}_{\mathrm{i}} \mid \mathrm{Y}\right)$ tables
- Use standard inference to compute $P\left(Y \mid F_{1} \ldots F_{n}\right)$
- Nothing new here
- Estimates of local conditional probability tables
- $\mathrm{P}(\mathrm{Y})$, the prior over labels
- $P\left(F_{i} \mid Y\right)$ for each feature (evidence variable)
- These probabilities are collectively called the parameters of the model and denoted by $\boldsymbol{\theta}$
- Up until now, we assumed these appeared by magic, but...
- ...they typically come from training data counts: we'll look at this soon


## Example: Conditional Probabilities

$P(Y)$

| 1 | 0.1 |
| :--- | :--- |
| 2 | 0.1 |
| 3 | 0.1 |
| 4 | 0.1 |
| 5 | 0.1 |
| 6 | 0.1 |
| 7 | 0.1 |
| 8 | 0.1 |
| 9 | 0.1 |
| 0 | 0.1 |



## Naïve Bayes for Text

- Bag-of-words Naïve Bayes:
- Features: $\mathrm{W}_{\mathrm{i}}$ is the word at position i
- As before: predict label conditioned on feature variables (spam vs. ham)
- As before: assume features are conditionally independent given label
- New: each $W_{i}$ is identically distributed

Word at position
$i$, not ith word in
the dictionary!

- Generative model: $P\left(Y, W_{1} \ldots W_{n}\right)=P(Y) \prod_{i} P(\underbrace{W_{i} \mid Y})$
- "Tied" distributions and bag-of-words
- Usually, each variable gets its own conditional probability distribution P(F|Y)
- In a bag-of-words model
- Each position is identically distributed
- All positions share the same conditional probs P(W|Y)
- Why make this assumption?
- Called "bag-of-words" because model is insensitive to word order or reordering


## Example: Spam Filtering

- Model: $\quad P\left(Y, W_{1} \ldots W_{n}\right)=P(Y) \prod_{i} P\left(W_{i} \mid Y\right)$
- What are the parameters?


| the $:$ | 0.0210 |
| :--- | :--- |
| to $:$ | 0.0133 |
| of $:$ | 0.0119 |
| $2002:$ | 0.0110 |
| with: | 0.0108 |
| from: | 0.0107 |
| and $:$ | 0.0105 |
| a $:$ | 0.0100 |
| $\ldots$ |  |

- Where do these tables come from?


## Spam Example

| Word | $\mathrm{P}(\mathrm{w} \mid$ spam $)$ | $\mathrm{P}(\mathrm{w} \mid$ ham $)$ | Tot Spam | Tot Ham |
| :--- | ---: | ---: | ---: | ---: |
| (prior $)$ | 0.33333 | 0.66666 | -1.1 | -0.4 |

Training and Testing


## Empirical Risk Minimization

- Empirical risk minimization
- Basic principle of machine learning
- We want the model (classifier, etc) that does best on the true test distribution
- Don't know the true distribution so pick the best model on our actual training set
- Finding "the best" model on the training set is phrased as an optimization problem
- Main worry: overfitting to the training set
- Better with more training data (less sampling variance, training more like test)
- Better if we limit the complexity of our hypotheses (regularization and/or small hypothesis spaces)


## Important Concepts

- Data: labeled instances (e.g. emails marked spam/ham)
- Training set
- Held out set
- Test set
- Features: attribute-value pairs which characterize each $x$
- Experimentation cycle
- Learn parameters (e.g. model probabilities) on training set
- (Tune hyperparameters on held-out set)
- Compute accuracy of test set
- Very important: never "peek" at the test set!
- Evaluation (many metrics possible, e.g. accuracy)
- Accuracy: fraction of instances predicted correctly
- Overfitting and generalization
- Want a classifier which does well on test data
- Overfitting: fitting the training data very closely, but not generalizing well
- We'll investigate overfitting and generalization formally in a few lectures


Generalization and Overfitting


## Overfitting



## Example: Overfitting

$$
\begin{aligned}
& P(\text { features }, C=2) \\
& P(C=2)=0.1 \\
& P(\text { features, } C=3) \\
& P(C=3)=0.1 \\
& P(\text { on } \mid C=2)=0.1 \\
& P(\text { off } \mid C=2)=0.1 \\
& P(\text { on } \mid C=2)=0.01
\end{aligned}
$$



## Example: Overfitting

- Posteriors determined by relative probabilities (odds ratios):

$$
\frac{P(W \mid \text { ham })}{P(W \mid \text { spam })}
$$

```
south-west : inf
nation : inf
morally : inf
nicely : inf
extent : inf
seriously : inf
...
```

$\frac{P(W \mid \text { spam })}{P(W \mid \text { ham })}$

| screens | : inf |
| :--- | :--- |
| minute | : inf |
| guaranteed | : inf |
| $\$ 205.00$ | $:$ |
| delivery | : inf |
| signature | $:$ |
| inf |  |
| $\cdots$ |  |

What went wrong here?


## Generalization and Overfitting

- Relative frequency parameters will overfit the training data!
- Just because we never saw a 3 with pixel $(15,15)$ on during training doesn't mean we won't see it at test time
- Unlikely that every occurrence of "minute" is $100 \%$ spam
- Unlikely that every occurrence of "seriously" is $100 \%$ ham
- What about all the words that don't occur in the training set at all?
- In general, we can't go around giving unseen events zero probability
- As an extreme case, imagine using the entire email as the only feature (e.g. document ID)
- Would get the training data perfect (if deterministic labeling)
- Wouldn't generalize at all
- Just making the bag-of-words assumption gives us some generalization, but isn't enough
- To generalize better: we need to smooth or regularize the estimates


## Parameter Estimation



## Parameter Estimation

- Estimating the distribution of a random variable
- Elicitation: ask a human (why is this hard?)
- Empirically: use training data (learning!)
- E.g.: for each outcome $x$, look at the empirical rate of that value:


$$
P_{\mathrm{ML}}(x)=\frac{\operatorname{count}(x)}{\text { total samples }}
$$



- This is the estimate that maximizes the likelihood of the data

$$
L(x, \theta)=\prod_{i} P_{\theta}\left(x_{i}\right)
$$

## Smoothing



## Maximum Likelihood?

- Relative frequencies are the maximum likelihood estimates

$$
\begin{aligned}
\theta_{M L} & =\underset{\theta}{\arg \max } P(\mathbf{X} \mid \theta) \quad \Rightarrow P_{\mathrm{ML}}(x)=\frac{\operatorname{count}(x)}{\text { total samples }} \\
& =\underset{\theta}{\arg \max _{i} \prod_{\theta} P_{\theta}\left(X_{i}\right)} \quad \text {. }
\end{aligned}
$$

- Another option is to consider the most likely parameter value given the data

$$
\begin{aligned}
\theta_{M A P} & =\underset{\theta}{\arg \max } P(\theta \mid \mathbf{X}) \\
& =\underset{\theta}{\arg \max } P(\mathbf{X} \mid \theta) P(\theta) / P(\mathbf{X}) \quad \square ? ? ? \\
& =\underset{\theta}{\arg \max } P(\mathbf{X} \mid \theta) P(\theta)
\end{aligned}
$$

## Unseen Events



## Laplace Smoothing

- Laplace's estimate:
- Pretend you saw every outcome once more than you actually did


$$
\begin{aligned}
P_{L A P}(x) & =\frac{c(x)+1}{\sum_{x}[c(x)+1]} & & P_{M L}(X)= \\
& =\frac{c(x)+1}{N+|X|} & & P_{L A P}(X)=
\end{aligned}
$$

- Can derive this estimate with Dirichlet priors (see cs281a)


## Laplace Smoothing

- Laplace's estimate (extended):
- Pretend you saw every outcome k extra times

$$
P_{L A P, k}(x)=\frac{c(x)+k}{N+k|X|}
$$

- What's Laplace with $\mathrm{k}=0$ ?
- $k$ is the strength of the prior

$$
P_{L A P, 0}(X)=
$$

$$
P_{L A P, 1}(X)=
$$

- Laplace for conditionals:
- Smooth each condition independently:

$$
P_{L A P, 100}(X)=
$$

$$
P_{L A P, k}(x \mid y)=\frac{c(x, y)+k}{c(y)+k|X|}
$$

## Estimation: Linear Interpolation*

- In practice, Laplace often performs poorly for $\mathrm{P}(\mathrm{X} \mid \mathrm{Y})$ :
- When $|\mathrm{X}|$ is very large
- When |Y| is very large
- Another option: linear interpolation
- Also get the empirical $P(X)$ from the data
- Make sure the estimate of $P(X \mid Y)$ isn't too different from the empirical $P(X)$

$$
P_{L I N}(x \mid y)=\alpha \widehat{P}(x \mid y)+(1.0-\alpha) \widehat{P}(x)
$$

- What if $\alpha$ is 0 ? 1?
- For even better ways to estimate parameters, as well as details of the math, see cs281a, cs288


## Real NB: Smoothing

- For real classification problems, smoothing is critical
- New odds ratios:
$\frac{P(W \mid \text { ham })}{P(W \mid \text { spam })}$

| helvetica | $:$ | 11.4 |
| :--- | :--- | ---: |
| seems | $:$ | 10.8 |
| group | $:$ | 10.2 |
| ago | $:$ | 8.4 |
| areas | $:$ | 8.3 |
| ... |  |  |

$\frac{P(W \mid \text { spam })}{P(W \mid \text { ham })}$

$$
\begin{array}{|ll}
\hline \text { verdana }: 28.8 \\
\text { Credit } & : 28.4 \\
\text { ORDER } & : 27.2 \\
<\text { FONT }> & : 26.9 \\
\text { money } & : 26.5
\end{array}
$$

Do these make more sense?

Tuning

TWEAK-O-MATIC 9000


## Tuning on Held-Out Data

- Now we've got two kinds of unknowns
- Parameters: the probabilities $\mathrm{P}(\mathrm{X} \mid \mathrm{Y}), \mathrm{P}(\mathrm{Y})$
- Hyperparameters: e.g. the amount / type of smoothing to do, $k$, $\alpha$
- What should we learn where?
- Learn parameters from training data
- Tune hyperparameters on different data - Why?
- For each value of the hyperparameters, train and test on the held-out data
- Choose the best value and do a final test on the test data



## Features



## Errors, and What to Do

- Examples of errors

```
Dear GlobalSCAPE Customer,
GlobalSCAPE has partnered with ScanSoft to offer you the
latest version of OmniPage Pro, for just $99.99* - the regular
list price is $499! The most common question we've received
about this offer is - Is this genuine? We would like to assure
you that this offer is authorized by ScanSoft, is genuine and
valid. You can get the . . .
```

```
. . . To receive your $30 Amazon.com promotional certificate,
click through to
    http://www.amazon.com/apparel
and see the prominent link for the $30 offer. All details are
there. We hope you enjoyed receiving this message. However, if
you'd rather not receive future e-mails announcing new store
launches, please click . . .
```


## What to Do About Errors?

- Need more features- words aren't enough!
- Have you emailed the sender before?
- Have 1 K other people just gotten the same email?
- Is the sending information consistent?
- Is the email in ALL CAPS?
- Do inline URLs point where they say they point?
- Does the email address you by (your) name?
- Can add these information sources as new variables in the NB model
- Later this week we'll talk about classifiers which let you easily add arbitrary features more easily, and, later, how to induce new features



## Baselines

- First step: get a baseline
- Baselines are very simple "straw man" procedures
- Help determine how hard the task is
- Help know what a "good" accuracy is
- Weak baseline: most frequent label classifier
- Gives all test instances whatever label was most common in the training set
- E.g. for spam filtering, might label everything as ham
- Accuracy might be very high if the problem is skewed
- E.g. calling everything "ham" gets 66\%, so a classifier that gets $70 \%$ isn't very good...
- For real research, usually use previous work as a (strong) baseline


## Confidences from a Classifier

- The confidence of a probabilistic classifier:
- Posterior probability of the top label

$$
\operatorname{confidence}(x)=\max _{y} P(y \mid x)
$$



- Represents how sure the classifier is of the classification
- Any probabilistic model will have confidences
- No guarantee confidence is correct
- Calibration

- Weak calibration: higher confidences mean higher accuracy
- Strong calibration: confidence predicts accuracy rate
- What's the value of calibration?



## Summary

- Bayes rule lets us do diagnostic queries with causal probabilities
- The naïve Bayes assumption takes all features to be independent given the class label
- We can build classifiers out of a naïve Bayes model using training data
- Smoothing estimates is important in real systems
- Classifier confidences are useful, when you can get them

Linear Classifiers


## Feature Vectors

$$
x
$$

$$
f(x)
$$

$y$

| Hello, |
| :--- |
| Do you want free printr |
| cartriges? Why pay more |
| when you can get them |
| ABSOLUTELY FREE! Just |

$\downarrow\left(\begin{array}{lll}\# \text { free } & : & 2 \\ \text { YOUR_NAME } & : & 0 \\ \text { MISSPELLED } & : & 2 \\ \text { FROM_FRIEND } & : & 0 \\ \cdots & & \end{array}\right)$


SPAM
or
$+$


## Some (Simplified) Biology

- Very loose inspiration: human neurons



## Linear Classifiers

- Inputs are feature values
- Each feature has a weight
- Sum is the activation


$$
\operatorname{activation}_{w}(x)=\sum_{i} w_{i} \cdot f_{i}(x)=w \cdot f(x)
$$

- If the activation is:
- Positive, output +1
- Negative, output -1



## Weights

- Binary case: compare features to a weight vector
- Learning: figure out the weight vector from examples


Decision Rules


## Binary Decision Rule

- In the space of feature vectors
- Examples are points
- Any weight vector is a hyperplane
- One side corresponds to $Y=+1$

- Other corresponds to $Y=-1$

$$
w
$$

| BIAS | $:$ | -3 |
| :--- | :--- | ---: |
| free | $:$ | 4 |
| money | $:$ | 2 |
| $\cdots$ |  |  |

Weight Updates


## Learning: Binary Perceptron

- Start with weights $=0$
- For each training instance:
- Classify with current weights

- If correct (i.e., $\mathrm{y}=\mathrm{y}^{*}$ ), no change!

- If wrong: adjust the weight vector



## Learning: Binary Perceptron

- Start with weights $=0$
- For each training instance:
- Classify with current weights

$$
y= \begin{cases}+1 & \text { if } w \cdot f(x) \geq 0 \\ -1 & \text { if } w \cdot f(x)<0\end{cases}
$$

- If correct (i.e., $\mathrm{y}=\mathrm{y}^{*}$ ), no change!
- If wrong: adjust the weight vector by adding or subtracting the feature vector. Subtract if $y^{*}$ is -1 .

$$
w=w+y^{*} \cdot f
$$

## Examples: Perceptron

- Separable Case



## Multiclass Decision Rule

- If we have multiple classes:
- A weight vector for each class:

$$
w_{y}
$$



- Score (activation) of a class $y$ :

$$
w_{y} \cdot f(x)
$$

- Prediction highest score wins

$$
y=\arg \max _{y} w_{y} \cdot f(x)
$$



## Learning: Multiclass Perceptron

- Start with all weights $=0$
- Pick up training examples one by one
- Predict with current weights

$$
y=\arg \max _{y} w_{y} \cdot f(x)
$$

- If correct, no change!
- If wrong: lower score of wrong answer, raise score of right answer

$$
\begin{aligned}
& w_{y}=w_{y}-f(x) \\
& w_{y^{*}}=w_{y^{*}}+f(x)
\end{aligned}
$$

## Example: Multiclass Perceptron

"win the vote"
"win the election"
"win the game"
$w_{S P O R T S}$

| BIAS | $:$ | 1 |
| :--- | :--- | :--- |
| win | $:$ | 0 |
| game | $:$ | 0 |
| vote | $:$ | 0 |
| the | $:$ | 0 |
| $\cdots$ |  |  |

$w_{\text {POLITICS }}$

$w_{T E C H}$

| BIAS | $:$ | 0 |
| :--- | :--- | :--- |
| win | $:$ | 0 |
| game | $:$ | 0 |
| vote | $:$ | 0 |
| the | $:$ | 0 |
| $\cdots$ |  |  |

## Properties of Perceptrons

- Separability: true if some parameters get the training set perfectly correct
- Convergence: if the training is separable, perceptron will eventually converge (binary case)
- Mistake Bound: the maximum number of mistakes (binary case) related to the margin or degree of separability

$$
\text { mistakes }<\frac{k}{\delta^{2}}
$$

## Separable



Non-Separable


## Problems with the Perceptron

- Noise: if the data isn't separable, weights might thrash
- Averaging weight vectors over time can help (averaged perceptron)
- Mediocre generalization: finds a "barely" separating solution
- Overtraining: test / held-out accuracy usually rises, then falls
- Overtraining is a kind of overfitting



## Improving the Perceptron



## Non-Separable Case: Deterministic Decision



Non-Separable Case: Probabilistic Decision


## How to get probabilistic decisions?

- Perceptron scoring: $z=w \cdot f(x)$
- If $\quad z=w \cdot f(x) \quad$ very positive $\rightarrow$ want probability going to 1
- If $z=w \cdot f(x)$ very negative $\rightarrow$ want probability going to 0
- Sigmoid function

$$
\phi(z)=\frac{1}{1+e^{-z}}
$$



## Best w?

- Maximum likelihood estimation:

$$
\max _{w} l l(w)=\max _{w} \sum_{i} \log P\left(y^{(i)} \mid x^{(i)} ; w\right)
$$

with:

$$
\begin{aligned}
& P\left(y^{(i)}=+1 \mid x^{(i)} ; w\right)=\frac{1}{1+e^{-w \cdot f\left(x^{(i)}\right)}} \\
& P\left(y^{(i)}=-1 \mid x^{(i)} ; w\right)=1-\frac{1}{1+e^{-w \cdot f\left(x^{(i)}\right)}}
\end{aligned}
$$

= Logistic Regression

## Separable Case: Deterministic Decision - Many Options




## Separable Case: Probabilistic Decision - Clear Preference




## Multiclass Logistic Regression

- Recall Perceptron:
- A weight vector for each class: $w_{y}$
- Score (activation) of a class y: $\quad w_{y} \cdot f(x)$
- Prediction highest score wins $\quad y=\arg \underset{y}{\max } w_{y} \cdot f(x)$

- How to make the scores into probabilities?



## Best w?

- Maximum likelihood estimation:

$$
\max _{w} l l(w)=\max _{w} \sum_{i} \log P\left(y^{(i)} \mid x^{(i)} ; w\right)
$$

with:

$$
P\left(y^{(i)} \mid x^{(i)} ; w\right)=\frac{e^{w_{y^{(i)}} \cdot f\left(x^{(i)}\right)}}{\sum_{y} e^{w_{y} \cdot f\left(x^{(i)}\right)}}
$$

## Next Lecture

- Optimization
- i.e., how do we solve:

$$
\max _{w} l l(w)=\max _{w} \sum_{i} \log P\left(y^{(i)} \mid x^{(i)} ; w\right)
$$

