Wei Xu

Binary Classification

(many slides from Greg Durrett and Vivek Srikumar)

Administrivia

- ‣ Homework 1 will be released soon.
	- \rightarrow 2-3 written questions
	- ‣ One programming task:
		- Logistic Regression for Text Classification (Hate Speech)

Outline of the Course

Applications:
MT, IE,
summarization,
dialogue, etc. MT, IE, summarization, dialogue, etc.

ML and structured prediction for NLP

{ Neural Networks semantics

NLP Research

⁴ ACL 2019 conference

 h th

ACL'19 at a Glance

- \blacktriangleright Linear classification fundamentals
- Naive Bayes, maximum likelihood in generative models
- If Three discriminative models: logistic regression, perceptron, SVM \triangleright Different motivations but very similar update rules / inference!

This Lecture

Classification

- \blacktriangleright Datapoint x with label $y \in \{0,1\}$
- \blacktriangleright Embed datapoint in a feature space $f(x) \in \mathbb{R}^n$ but in this lecture $f(x)$ and x are interchangeable
- \blacktriangleright Linear decision rule: $w^\top f(x) + b > 0$ $w^{\top} f(x) > 0$
- $f(x) = [0.5, 1.6, 0.3]$ [0.5, 1.6, 0.3, **1**] ‣ Can delete bias if we augment feature space:

Classification

Linear functions are powerful!

‣ "Kernel trick" does this for "free," but is too expensive to use in NLP applications, training is $O(n^2)$ instead of $O(n \cdot (\text{num} \text{ facts}))$

https://www.quora.com/Why-is-kernelized-SVM-much-slower-than-linear-SVM http://ciml.info/dl/v0_99/ciml-v0_99-ch11.pdf

Classification: Sentiment Analysis

this movie was great! would watch again

that film was awful, I'll never watch again

‣ Surface cues can basically tell you what's going on here: presence or

- absence of certain words (*great*, *awful*)
- Steps to classification:
	- ‣ Turn examples like this into feature vectors
	- ‣ Pick a model / learning algorithm
	- ‣ Train weights on data to get our classifier

Feature Representation

this movie was great! would watch again Positive

- ‣ Convert this example to a vector using *bag-of-words features*
- [contains *the*] [contains *a*] [contains *was*] [contains *movie*] [contains *film*] …position 0 position 1 position 2 position 3 position 4
- 0 1 0 $f(x) = [0 \t 0 \t 1 \t 1 \t 0 \t ...$
	- ‣ Very large vector space (size of vocabulary), sparse features
	- ‣ Requires *indexing* the features (mapping them to axes)

What are features?

‣ Don't have to be just *bag-of-words*

 $f(x) = \begin{pmatrix} \text{count("boring")} \\ \text{count("not boring")} \\ \text{length of document} \\ \text{author of document} \\ \vdots \end{pmatrix}$

I More sophisticated feature mappings possible (tf-idf), as well as lots of other features: character n-grams, parts of speech, lemmas, …

Naive Bayes

Naive Bayes

- \blacktriangleright Data point $x = (x_1, ..., x_n)$, label $y \in \{0, 1\}$
- \blacktriangleright Formulate a probabilistic model that places a distribution *P*(*x, y*)
- $P(y|x)$ \blacktriangleright Compute $P(y|x)$, predict $\arg\!\max_{y} P(y|x)$ to classify $\argmax_y P(y|x)$
- $P(y|x) = \frac{P(y)P(x|y)}{P(x)}$ *P*(*x*) Bayes' Rule

 $P(x_i|y)$

- $\propto P(y)P(x|y)$ constant: irrelevant for finding the max
	- "Naive" assumption: conditional independence

 $\mathrm{argmax}_y P(y|x) = \mathrm{argmax}_y \log P(y|x) = \mathrm{argmax}_y$

 $\overline{\mathsf{H}}$

n

 $= P(y)$

i=1

Why the log?

$\overline{\mathsf{H}}$ *n* $i=1$ $P(x_i|y)$

Q: What could go wrong here?

$$
P(y|x) = \frac{P(y)P(x|y)}{P(x)} = P(y)
$$

 \blacktriangleright Multiplying together lots of probabilities \triangleright Probabilities are numbers between 0 and 1

\blacktriangleright Problem $-$ floating point underflow

\rightarrow Solution: working with probabilities in log space

Why the log?

Maximum Likelihood Estimation

- \blacktriangleright Data points (x_j, y_j) provided (*j* indexes over examples)
- \blacktriangleright Find values of $P(y)$, $P(x_i|y)$ that maximize data likelihood (generative):

Maximum Likelihood Estimation

- ‣ Imagine a coin flip which is heads with probability *p*
- \blacktriangleright Observe (H, H, H, T) and maximize likelihood: \prod

- \sum *m* $j=1$ $\log P(y_j) = 3 \log p + \log(1 - p)$ ‣ Easier: maximize *log* likelihood
- ‣ Maximum likelihood parameters for binomial/ multinomial = read counts off of the data + normalize

m $j=1$ $P(y_j) = p^3(1-p)$

Maximum Likelihood Estimation

- \blacktriangleright Data points (x_j, y_j) provided (*j* indexes over examples)
- \blacktriangleright Find values of $P(y)$, $P(x_i|y)$ that maximize data likelihood (generative):

data points (*j*) features (*i*) $P(x_j_i|y_j)$ $\overline{1}$ ‣ Equivalent to maximizing logarithm of data likelihood: *i*th feature of *j*th example

$$
\sum_{j=1}^{m} \log P(y_j, x_j) = \sum_{j=1}^{m} \left[\log P(y_j) + \sum_{i=1}^{n} \log P(x_{ji} | y_j) \right]
$$

Maximum Likelihood for Naive Bayes

this movie was great! would watch again + *that film was awful, I'll never watch again* I didn't really like that movie dry and a bit distasteful, it misses the mark great potential but ended up being a flop *I liked it well enough for an action flick I expected a great film and left happy* brilliant directing and stunning visuals $P(y|x) \propto$

http://socialmedia-class.org/slides_AU2017/Shimodaira_note07.pdf

Naive Bayes: Learning

 $P(y|x) \propto P(y)$

 \blacktriangleright Learning = estimate the parameters of the model \triangleright Prior probability — P(+) and P(-): \triangleright fraction of + (or -) documents among all documents

 \triangleright Word likelihood — P(word; | +) and P(word; | -): number of documents of + (or -) documents

$\overline{\mathsf{H}}$ *n i*=1 $P(x_i|y)$

-
-
-
- \triangleright number of + (or -) documents word; is observed, divide by the total
	- http://socialmedia-class.org/slides_AU2017/Shimodaira_note07.pdf This is for Bernoulli (binary features) document model!

Zero Probability Problem

and classified in the topic positive?

• What if we have seen no training document with the word "fantastic"

 \triangleright Word likelihood — P(word; | +) and P(word; | -): ‣ frequency of wordi is observed **plus 1**, divide by … ‣ Laplace (add-1) Smoothing

Naive Bayes

‣ Bernoulli document model:

‣ A document is represented by binary features

‣ Feature value be 1 if the corresponding word is represent in the document and 0 if not

 \triangleright Multinominal document model"

- ‣ A document is represented by integer elements
- ‣ Feature value is the frequency of that word in the document
- for more details

‣ See textbook and lecture note by Hiroshi Shimodaira linked below

http://socialmedia-class.org/slides_AU2017/Shimodaira_note07.pdf

Naive Bayes: Summary

‣ Model

$$
P(x, y) = P(y) \prod_{i=1}^{n} P(x_i | y)
$$

P(*x, y*) \blacktriangleright Alternatively: $\log P(y = +|x) - \log P(y = -|x) > 0$ $\Leftrightarrow \log \frac{P(y=+)}{P(y=+)}$ $\frac{P(y = +)}{P(y = -)} + \sum_{i=1}$

‣ Inference

 $\mathrm{argmax}_y \log P(y|x) = \mathrm{argmax}_y$

 \blacktriangleright Learning: maximize $P(x, y)$ by reading counts off the data

Problems with Naive Bayes

the film was beautiful, stunning cinematography and gorgeous sets, but boring

- $P(x_{\text{beautiful}}|+) = 0.1$ $P(x_{\text{stuning}}|+) = 0.1$ $P(x_{\text{gorgeous}}|+) = 0.1$ $P(x_{\text{boring}}|+) = 0.01$ $P(x_{\text{boring}}|-) = 0.1$
-
- Naive Bayes is naive, but another problem is that it's *generative*: spends capacity modeling $P(x,y)$, when what we care about is $P(y|x)$
-

 $P(x_{\text{beautiful}}|-) = 0.01$ $P(x_{\text{stuning}}|-)=0.01$ $P(x_{\text{gorgeous}}|-) = 0.01$

• Correlated features compound: *beautiful* and *gorgeous* are not independent! \triangleright Discriminative models model P(y|x) directly (SVMs, most neural networks, ...)

Generative vs. Discriminative Models

- **Senerative models:** *P*(*x, y*)
	- ‣ Bayes nets / graphical models
	- prediction uses Bayes rule post-hoc
	- ‣ Can sample new instances (*x, y*)
- \blacktriangleright Discriminative models: $P(y|x)$
	- ▶ SVMs, logistic regression, CRFs, most neural networks
	- Model is trained to be good at prediction, but doesn't model x
- \blacktriangleright We'll come back to this distinction throughout this class

• Some of the model capacity goes to explaining the distribution of *x*;

Break!

Logistic Regression

$$
P(y = +|x) = \text{logistic}(w^{\top} x)
$$

$$
P(y = +|x) = \frac{\exp(\sum_{i=1}^{n} v_i)}{1 + \exp(\sum_{i=1}^{n} v_i)}
$$

- P Decision rule: $P(y = +|x|) \geq 0.5 \Leftrightarrow w^{\top} x > 0$
-

 \triangleright To learn weights: maximize discriminative log likelihood of data P(y|x)

$$
\mathcal{L}(x_j, y_j = +) = \log P(y_j = + |x_j)
$$

=
$$
\sum_{i=1}^n w_i x_{ji} - \log \left(1 + \exp \left(\sum_{i=1}^n w_i x_{ji} \right) \right)
$$

sum over features

Logistic Regression

$$
\mathcal{L}(x_j, y_j = +) = \log P(y_j = + |x_j) = \sum_{i=1}^{n} \frac{\partial \mathcal{L}(x_j, y_j)}{\partial w_i} = \frac{x_{ji} - \frac{\partial}{\partial w_i} \log \left(1 + \exp\left(\sum_{i=1}^{n} w_i x_{ji}\right)\right)}{1 + \exp\left(\sum_{i=1}^{n} w_i x_{ji}\right)} \frac{\partial}{\partial w_i}
$$
\n
$$
= x_{ji} - \frac{1}{1 + \exp\left(\sum_{i=1}^{n} w_i x_{ji}\right)}
$$
\n
$$
= x_{ji} - x_{ji} \frac{\exp\left(\sum_{i=1}^{n} w_i x_{ji}\right)}{1 + \exp\left(\sum_{i=1}^{n} w_i x_{ji}\right)}
$$

 $\frac{1}{n} w_i w_j i_j = x_j i (1 - P(y_j = + |x_j))$

- \triangleright Recall that $y_j = 1$ for positive instances, $y_j = 0$ for negative instances.
- \triangleright Gradient of w_i on positive example

If $P(+)$ is close to 1, make very little update

 \blacktriangleright Gradient of w_i on negative examp

-
- Otherwise make *wi* look more like *xji*, which will increase P(+)

If $P(+)$ is close to 0, make very little update Otherwise make *wi* look less like *xji*, which will decrease P(+)

$$
\text{d}e = x_{ji}(-P(y_j = +|x_j))
$$

-
-

$$
e = x_{ji}(y_j - P(y_j = + | x_j))
$$

‣ Can combine these gradients as *^x^j* (*y^j ^P*(*y^j* = 1*|x^j*)) @*L*(*x^j , y^j*)

Logistic Regression

$$
\frac{\partial \mathcal{L}(x_j, y_j)}{\partial w} = x_j(y_j - P(y_j = 1 | x_j))
$$

∂w =

Gradient Decent \blacktriangleright Can combine these gradients as $\frac{\partial \mathcal{L}(x_j, y_j)}{\partial w} = x_j \left(y_j - P(y_j = 1 | x_j) \right)$ log likelihood of data P(y|x) data points (*j*)

\blacktriangleright Training set log-likelihood: $\mathcal{L}(w)$

▶ Gradient vector: $\frac{\partial \mathcal{L}(w)}{\partial w_1} = \left(\frac{\partial \mathcal{L}}{\partial w_1}, \frac{\partial \mathcal{L}}{\partial w_2}, \dots, \frac{\partial \mathcal{L}}{\partial w_n}\right)$

Gradient Decent

\triangleright Gradient decent (or ascent) is an iterative optimization algorithm for finding the minimum (or maximum) of a function.

Learning Rate

³³ Credit: Jeremy Jordan

 \triangleright Regularizing an objective can mean many things, including an L2norm penalty to the weights:

$$
\sum_{j=1}^m \mathcal{L}(x_j, y_j) - \lambda ||w||_2^2 \longrightarrow
$$

- \triangleright Keeping weights small can prevent overfitting
- \triangleright For most of the NLP models we build, explicit regularization isn't necessary
	- ‣ Early stopping
	- ‣ For neural networks: dropout and gradient clipping ‣ Large numbers of sparse features are hard to overfit in a really bad way
	-

Logistic Regression: Summary

‣ Model

‣ Inference

 $\argmax_{y} P(y|x)$ fundamentally same as Naive Bayes $P(y = 1|x) \ge 0.5 \Leftrightarrow w^{\top} x \ge 0$

\blacktriangleright Learning: gradient ascent on the (regularized) discriminative log-likelihood

$$
P(y = +|x) = \frac{\exp(\sum_{i=1}^{n} w_i x_i)}{1 + \exp(\sum_{i=1}^{n} w_i x_i)}
$$

Logistic Regression vs. Naive Bayes

‣ Both are (log) linear models

- \blacktriangleright Logistic regression doesn't assume conditional independence of features ‣ Weights are trained independently ‣ Can handle highly correlated overlapping features
- \triangleright Naive Bayes assume conditional independence of features ‣ Weights are trained jointly

 $w^{\perp}f(x)$

Perceptron/SVM

 \rightarrow Simple error-driven learning approach similar to logistic regression

- \blacktriangleright Decision rule: $w^{\top} x > 0$ \blacktriangleright If incorrect: if positive, if negative, $w \leftarrow w - x$ $w \leftarrow w + x$
- \triangleright Algorithm is very similar to logistic regression
-

Perceptron

‣ Guaranteed to eventually separate the data if the data are separable

Perceptron

History [edit]

Mark I Perceptron machine, the first \Box implementation of the perceptron algorithm. It was connected to a camera with 20×20 cadmium sulfide photocells to make a 400-pixel image. The main visible feature is a patch panel that set different combinations of input features. To the right, arrays of potentiometers that implemented the adaptive weights.^{[2]:213}

original text are shown and corrected.

See also: History of artificial intelligence § Perceptrons and the attack on connectionism, and AI winter § The abandonment of connectionism in 1969

The perceptron algorithm was invented in 1958 at the Cornell Aeronautical Laboratory by Frank Rosenblatt,^[3] funded by the United States Office of Naval Research.^[4]

The perceptron was intended to be a machine, rather than a program, and while its first implementation was in software for the IBM 704, it was subsequently implemented in custom-built hardware as the "Mark 1 perceptron". This machine was designed for image recognition: it had an array of 400 photocells, randomly connected to the "neurons". Weights were encoded in potentiometers, and weight updates during learning were performed by electric motors.^{[2]:193}

In a 1958 press conference organized by the US Navy, Rosenblatt made statements about the perceptron that caused a heated controversy among the fledgling AI community; based on Rosenblatt's statements, The New York Times reported the perceptron to be "the embryo of an electronic computer that [the Navy] expects will be able to walk, talk, see, write, reproduce itself and be conscious of its existence."[4]

Although the perceptron initially seemed promising, it was quickly proved that perceptrons could not be trained to recognise many classes of patterns. This caused the field of neural network research to stagnate for many years, before it was recognised that a feedforward neural network with two or more layers (also called a multilayer perceptron) had greater processing power than perceptrons with one layer (also called a single layer perceptron).

Single layer perceptrons are only capable of learning linearly separable patterns. For a classification task with some step activation function a single node will have a single line dividing the data points forming the patterns. More nodes can create more dividing lines, but those lines must somehow be combined to form more complex classifications. A second layer of perceptrons, or even linear nodes, are sufficient to solve a lot of otherwise non-separable problems.

In 1969 a famous book entitled Perceptrons by Marvin Minsky and Seymour Papert showed that it was impossible for these classes of network to learn an XOR function. It is often believed (incorrectly) that they also conjectured that a similar result would hold for a multi-layer perceptron network. However, this is not true, as both Minsky and Papert already knew that multi-layer perceptrons were capable of producing an XOR function. (See the page on Perceptrons (book) for more information.) Nevertheless, the often-miscited Minsky/Papert text caused a significant decline in interest and funding of neural network research. It took ten more years until neural network research experienced a resurgence in the 1980s. This text was reprinted in 1987 as "Perceptrons - Expanded Edition" where some errors in the

The kernel perceptron algorithm was already introduced in 1964 by Aizerman et al.^[5] Margin bounds guarantees were given for the Perceptron algorithm in the general non-separable case first by Freund and Schapire (1998),^[1] and more recently by Mohri and Rostamizadeh (2013) who extend previous results and give new L1 bounds.^[6]

The perceptron is a simplified model of a biological neuron. While the complexity of biological neuron models is often required to fully understand neural behavior, research suggests a perceptron-like linear model can produce some behavior seen in real neurons.^[7]

 $V \cdot T \cdot E$

Support Vector Machines (extracurricular)

 \blacktriangleright Many separating hyperplanes $-$ is there a best one?

-

-

-

Support Vector Machines (extracurricular)

 \blacktriangleright Many separating hyperplanes $-$ is there a best one?

Minimize s.t. $\|w\|_2^2$ 2 $\forall j \quad w \mid x_j \geq 1 \text{ if } y_j = 1$ $w^{\top} x_j \le -1$ if $y_j = 0$

As a single constraint:

 $\forall j \quad (2y_j - 1)(w^\top x_j) \geq 1$

minimizing norm with fixed margin <=> maximizing margin

Generally no solution (data is generally non-separable) — need slack!

Support Vector Machines (extracurricular)

• Constraint formulation: find *w* via following quadratic program:

N-Slack SVMs (extracurricular)

Minimize
$$
\lambda ||w||_2^2 + \sum_{j=1}^m \xi_j
$$

s.t. $\forall j \ (2y_j - 1)(w^\top x_j) \ge 1 - \xi_j$ $\forall j \ \xi_j \ge 0$

- \blacktriangleright The ζ_i are a "fudge factor" to make all constraints satisfied
- \blacktriangleright Take the gradient of the objective: ∂ ∂w_i $\xi_j = 0$ if $\xi_j = 0$ $\frac{\partial}{\partial x_i}$ ∂w_i
- ‣ Looks like the perceptron! But updates more frequently

$$
\xi_j = (2y_j - 1)x_{ji} \text{ if } \xi_j > 0
$$

= x_{ji} if $y_j = 1$, $-x_{ji}$ if $y_j = 0$

LR, Perceptron, SVM (extracurricular)

Loss

Gradients on Positive Examples

*gradients are for maximizing things, which is why they are flipped

Bo Pang, Lillian Lee, Shivakumar Vaithyanathan (2002)

Sentiment Analysis

this movie was great! would watch again

this movie was not really very enjoyable

 \triangleright Bag-of-words doesn't seem sufficient (discourse structure, negation)

‣ There are some ways around this: extract bigram feature for "*not* X" for all X following the *not*

Sentiment Analysis

▶ Simple feature sets can do pretty well!

Bo Pang, Lillian Lee, Shivakumar Vaithyanathan (2002)

Before neural nets had taken off — results weren't that great

Sentiment Analysis

- $\frac{PQA}{35.3}$
35.3
36.3 Naive Bayes is doing well!
	- Ng and Jordan (2002) NB can be better for small data
- \blacktriangleright Logistic regression: $P(y = 1|x) =$
	- Decision rule: $P(y = 1|x) \ge 0$

Recap

Gradient (unregularized):

$$
1|x) = \frac{\exp(\sum_{i=1}^{n} w_i x_i)}{(1 + \exp(\sum_{i=1}^{n} w_i x_i))}
$$

$$
1|x) \ge 0.5 \Leftrightarrow w^\top x \ge 0
$$

$$
x(y - P(y = 1|x))
$$

- \triangleright Logistic regression, perceptron, and SVM are closely related
- wrong thing"

‣ All gradient updates: "make it look more like the right thing and less like the

Optimization — next time...

Quasi-Newton methods (LBFGS), Adagrad, Adadelta, etc.

gradient update times step size, incorporate estimated curvature information to make the update more effective

• Range of techniques from simple gradient descent (works pretty well) to more complex methods (can work better), e.g., Newton's method,

‣ Most methods boil down to: take a gradient and a step size, apply the

DO YOU HAVE ANY QUESTIONS?

QA Time