Applied Machine Learning

Naive Bayes

Reihaneh Rabbany



Learning objectives

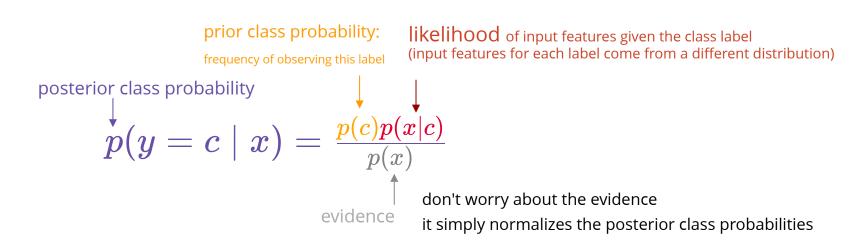
- the assumption of Naive Bayes classifier
- what does learning and prediction steps involve?
- different likelihood functions
- Bayesian parameter learning in Naive Bayes
- practical considerations

Bayes rule for classification

given

- the prior probability of each class
- likelihood of observations given the class

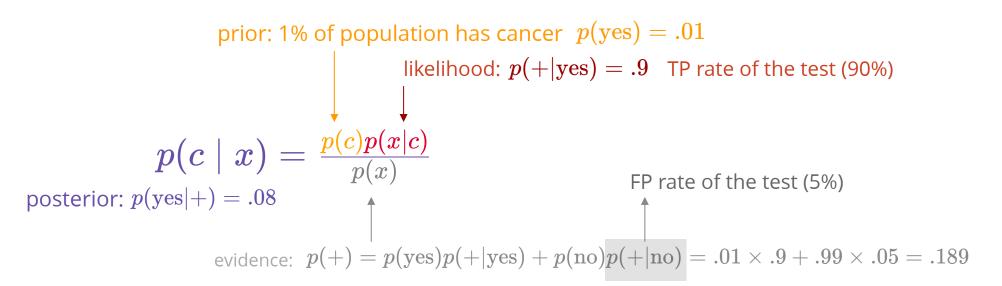
use Bayes rule for classification



Bayes rule for classification

example

```
x \in \{-, +\} input: test results, a single binary feature y \in \{ \text{yes}, \text{no} \} label: patient has cancer
```



Generative classification

training learn the following distributions from the data $\,\mathcal{D} = \{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

prior probability of each class $p(y=c) orall c \in \{1,\ldots,C\}$

likelihood of data for each class p(x|y=c)

prediction

use the Bayes rule to get the posterior class probability

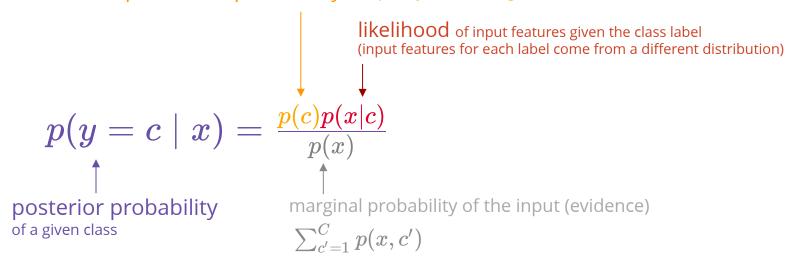
$$p(y = c \mid x) \propto p(c)p(x|c)$$

generative classifier because we are learning the joint data distribution p(x,y)=p(y)p(x|y) we can generate new data from this joint distribution

in a **discriminative classifier** we directly learn p(y|x)

Generative classification

prior class probability: frequency of observing this label



Some generative classifiers:

- Gaussian Discriminant Analysis: the likelihood is multivariate Gaussian
- Naive Bayes: decomposed likelihood _____



Naive Bayes model

assumption about the likelihood $\; p(x|y) = \prod_{d=1}^{\dot{D}} \, p(x_d|y) \;$

when is this assumption correct?

when features are **conditionally independent** given the label $x_i \perp x_i \mid y$

knowing the label, the value of one input feature gives us no information about the other input features

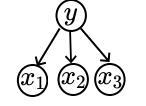
How is the likelihood derived from this independence assumption?

chain rule of probability (true for any distribution)

$$p(x|y) = p(x_1|y)p(x_2|y,x_1)p(x_3|y,x_1,x_2)\dots p(x_D|y,x_1,\dots,x_{D-1})$$

conditional independence assumption

 x_1,x_2 give no extra information, so $p(x_3|y,x_1,x_2)=p(x_3|y)$



number of input features

Naive Bayes: objective

given the training dataset $\mathcal{D} = \{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

a generative classifier maximizes the joint likelihood (or log-likelihood)

$$\begin{split} L(\pi,\theta;\mathcal{D}) &= \prod_{n \in \mathcal{D}} p(x^{(n)},y^{(n)};\pi,\theta) & \pi,\theta \text{ are the model parameters} \\ \ell(\pi,\theta) &= \sum_n \log p(x^{(n)},y^{(n)};\pi,\theta) & p(x,y) &= p(y)p(x|y) \\ &= \sum_n \left[\log p(y^{(n)};\pi) + \log p(x^{(n)}|y^{(n)};\theta)\right] & \\ &= \sum_n \log p(y^{(n)};\pi) + \sum_n \log p(x^{(n)}|y^{(n)};\theta) & \\ &= \sum_n \log p(y^{(n)};\pi) + \sum_n \log \prod_d p(x^{(n)}_d|y^{(n)};\theta_d) & \text{using Naive Bayes assumption here} \\ &= \sum_n \log p(y^{(n)};\pi) + \sum_d \sum_n \log p(x^{(n)}_d|y^{(n)};\theta_d) & p(x|y) &= \prod_{d=1}^D p(x_d|y) \\ &= \sum_n \log p(x|y) &= \sum_{d=1}^D \log p(x_d|y) & \log p(x_d|y) &$$

separate max-likelihood problems for prior and each feature x_d given the label

Prior class probabilities

class probabilities prior to looking at the features

for binary classification, class probability is given by Bernoulli $p(y;\pi)=\pi^y(1-\pi)^{1-y}$

recall the max-likelihood estimate for Bernoulli

$$rg \max_{\pi} \sum_n \log p(y^{(n)};\pi) = rac{1}{N} \sum_n y^{(n)}$$

for multi-class classification, class probability is given by categorical distribution

$$p(y;\pi) = \prod_{c=1}^C \pi_c{}^{\mathbb{I}(y=c)} = \pi_y$$
 note that in this case π is a vector

max-likelihood estimate is again given by empirical frequencies

$$rg \max_{\pi_c} \sum_n \log p(y^{(n)};\pi) = rac{N(y=c)}{N}$$
 frequency of class c in our dataset $\pi^* = [rac{N_1}{N}, \dots, rac{N_C}{N}]$

In both cases we learn the prior simply as the class frequencies in the training data

Naive Bayes: objective

given the training dataset $\mathcal{D} = \{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\}$

a generative classifier maximizes the joint likelihood (or log-likelihood)

$$\begin{split} \ell(\pi,\theta) &= \sum_{n} \log p(x^{(n)},y^{(n)};\pi,\theta) \\ &= \sum_{n} \log p(y^{(n)};\pi) + \log p(x^{(n)}|y^{(n)};\theta) \\ &= \sum_{n} \log p(y^{(n)};\pi) + \sum_{n} \log p(x^{(n)}|y^{(n)};\theta) \\ &= \sum_{n} \log p(y^{(n)};\pi) + \sum_{n} \log \prod_{d} p(x^{(n)}_{d}|y^{(n)};\theta_{d}) \\ &\text{to} \\ &= \sum_{n} \log p(y^{(n)};\pi) + \sum_{d} \sum_{n} \log p(x^{(n)}_{d}|y^{(n)};\theta_{d}) \end{split}$$

so far we know how to maximize this part

Next, how to maximize this part

separate max-likelihood problems for prior and each feature x_d given the label

Likelihood terms

likelihood terms $p(x_d|y; \theta_d)$

- encode our assumption about the *generative process*
- different types of features require different forms of likelihood
 - Bernoulli for binary features
 - Categorical for categorical features
 - Multinomial for "count" features
 - Gaussian is one option for continuous feature
- ullet each feature x_d may use a different likelihood form
- separate maximum conditional likelihood estimate for each feature

$$rg \max_{ heta_d} \sum_{n=1}^N \log p(x_d^{(n)} \mid y^{(n)}; heta_d)$$

Bernoulli Naive Bayes

for a binary **feature** likelihood is Bernoulli

$$\left\{egin{aligned} p(x_d \mid y=0; heta_d) &= ext{Bernoulli}(x_d; heta_{d,0}) \ p(x_d \mid y=1; heta_d) &= ext{Bernoulli}(x_d; heta_{d,1}) \end{aligned}
ight.$$
 one parameter per label

short form: $p(x_d \mid y; \theta_d) = \text{Bernoulli}(x_d; \theta_{d, y})$

max-likelihood estimation is similar to what we saw for the prior

closed form solution of MLE
$$hinspace{0.05cm} hinspace{0.05cm} hinspace{0.05cm}$$

Fatigue 38%

Sore throat 15%

Muscle

Covid-19 classification example

each patient has seven binary features $x \in \{0,1\}^7$ we have a dataset of N=1000 patients, where 200 had covid-19

learning:

learn the prior: $\pi = \frac{N(y=1)}{N} = .2$ Bernoulli $(y;\pi)$

for each symptom d:

Shortness of breath 19% Bernoulli
$$(x_d|y=1; heta_{d,1})$$

Fever 88%

Mucus production 33%

Dry cough 68%

for a new patient x calculate unnormalized posterior

$$\left\{egin{aligned} & ilde{p}(y=0|x) = ext{Bernoulli}(0;\pi) \prod_d ext{Bernoulli}(x_d; heta_{d,0}) \ & ilde{p}(y=1|x) = ext{Bernoulli}(1;\pi) \prod_d ext{Bernoulli}(x_d; heta_{d,1}) \end{aligned}
ight.$$

normalize it
$$\,p(y=1|x)=rac{ ilde{p}(y=1|x)}{ ilde{p}(y=0|x)+ ilde{p}(y=1|x)}$$

Disease diagnosis example

what changes in **multi-class** setting?

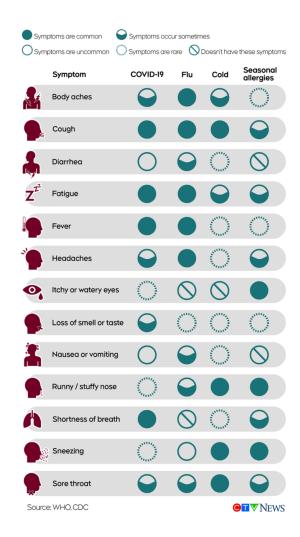
$$p(y;\pi)$$
 learn the prior: $\pi_{m{c}}=rac{N(y=c)}{N}$

for each symptom d:

$$p(x_d|y; heta_d)$$
 learn the conditional likelihood: $y=egin{cases} 0 \ dots \ \end{pmatrix}$ probability of symptom $x_d=1$ given $y=egin{cases} 0 \ dots \ \end{pmatrix}$

how many parameters in our model?

binary classification, binary features 1+2D multi-class classification, binary features C+CD



Document classification

example

e.g., spam filtering

words in our vocabulary

 $x^{(n)} \in \{0,1\}^D$ each document (email) is one instance

 $x_{\scriptscriptstyle J}^{(n)}=1$ if the word d appears in document n

classify the documents based on this bag of words representation

	D = I							
	it	is	puppy	cat	pen	a	this	
it is a puppy	1	1	1	0	0	1	0	
it is a kitten	1	1	0	0	0	1	0	
it is a cat	1	1	0	1	0	1	0	
d this is a pen	0	1	0	0	1	1	1	
it is a matrix	1	1	0	0	0	1	0	

N = 5

that is a dog and this is a per

D - 7

document-term matrix

learning:

MLE for the prior Bernoulli(y; π) (spam frequency in our dataset)

MLE for the likelihood terms Bernoulli(x; $\theta_{d,y}$) (frequency of word (d) in spam/non-spam documents)

prediction:

calculate the posterior $p(y|x) \propto \text{Bernoulli}(y;\pi) \prod_d \text{Bernoulli}(x_d;\theta_{d,u})$

Document classification

example

let's learn the Naive Bayes for the following data the label y=1 if the sentence is about animals

it is a puppy ata it is a kitten it is a cat that is a dog and this is a pen

it is a matrix

 it
 is
 puppy
 cat
 pen
 a
 this

 1
 1
 1
 0
 0
 1
 0

 1
 1
 0
 0
 0
 1
 0

 1
 1
 0
 1
 0
 1
 0

 0
 1
 0
 0
 1
 1
 1

 1
 1
 0
 0
 0
 1
 0

prior parameter: $\pi = \frac{4}{5}$

class conditional parameters: $\, heta_{d,y}$



y = 0	<u>1</u>	<u>1</u>	$\frac{0}{1}$	$\frac{0}{1}$	$\frac{0}{1}$	<u>1</u>	$\frac{0}{1}$ $\theta_{7,0}$?
y = 1	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{4}{4}$	$\frac{1}{4}$ $\theta_{7,1}$?
	d = 1						d=7

we get a new sentence: it is a random sentence

$$x = [1, 1, 0, 0, 0, 1, 0]$$

$$ilde{p}(y=1|x) = rac{4}{5} imes rac{3}{4} imes rac{4}{4} imes rac{3}{4} imes rac{3}{4} imes rac{3}{4} imes rac{3}{4} imes rac{4}{4} imes rac{3}{4} imes rac{3}{4} imes rac{4}{4} imes rac{3}{4} imes .19 \ ilde{p}(y=0|x) = rac{1}{5} imes rac{1}{1} imes n$$

$$p(y=1|x) = \frac{.19}{.2+.19} \approx .49$$

Why Naive Bayes assumption?

Naive Bayes assumption $p(x|y) = \prod_d p(x_d|y)$

what if we did not make this assumption?

consider the **spam filtering example**:

- D can be very large
- with the Naive Bayes assumption: learn the frequency of each word (d) in spam/non-spam documents
- without it: learn the frequency of each possible subset of words in spam/non-spam documents

e.g., for
$$x=[1,1,0,0,0,1,0]$$
 we need to estimate $p(x|y)$

problems

- many combinations of words may not appear in even one document
- we need exponentially more parameters
- even for large datasets, this could lead to overfitting

$(^{\omega} g)$							
	it	is	puppy	cat	pen	a	this
it is a puppy	1	1	1	0	0	1	0
it is a kitten	1	1	0	0	0	1	0
ent it is a cat	1	1	0	1	0	1	0
that is a dog and this is a pen	0	1	0	0	1	1	1
it is a matrix	1	1	0	0	0	1	0

is a puppy	1	1	1	0	0	1	0
is a kitten	1	1	0	0	0	1	0
it is a cat	1	1	0	1	0	1	0
nis is a pen	0	1	0	0	1	1	1
is a matrix	1	1	0	0	0	1	0

Bayesian Naive Bayes

using MLE in Naive Bayes can lead to overfitting

example

let's classify this new sentence:

that dog was my puppy

$$ilde{p}(y=1|x)=rac{4}{5} imesrac{1}{4} imesrac{0}{4} imes\ldots=0$$

$$ilde{p}(y=0|x)=rac{1}{5} imesrac{0}{1} imesrac{0}{1} imes\ldots=0$$

the problem is that the word "is" appears in all instances

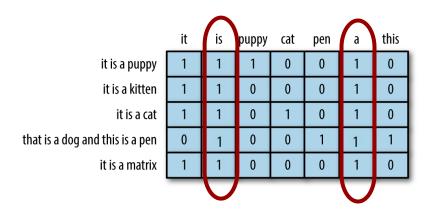
max-likelihood estimate
$$\,\theta_{1,1}=\theta_{1,0}=1\,$$

we can solve this by being Bayesian in parameter learning:

instead of maintaining a point estimates $\pi, \theta_{d,y}$ we maintain distributions $p(\pi), p(\theta_{d,y})$ for $y \in \{0,1\}, d$ start from separate prior for each parameter $p(\pi), p(\theta_{d.u})$

calculate the likelihood
$$\prod_n p(y^{(n)}|\pi)$$

update with observed frequencies in the dataset



Bayesian Naive Bayes

start from separate prior for each parameter $p(\pi) = \text{Beta}(\pi; \alpha^{\pi}, \beta^{\pi})$ $p(\theta_{d,y}) = \text{Beta}(\theta; \alpha^{\theta}, \beta^{\theta})$

calculate the posterior
$$p(\pi|\mathcal{D}) = \mathrm{Beta}(\pi; lpha^\pi + N(y=1), eta^\pi + N(y=0))$$

$$p(heta_{d,ar{u}}|\mathcal{D}) = \mathrm{Beta}(heta_{d,ar{u}}; lpha^\theta + N(y=ar{y}, x_d=1), eta^\theta + N(y=ar{y}, x_d=0))$$

use posterior predictive for a new instance (x) $p(y=1|x,\mathcal{D})=\int_{\theta} p(y=1|\pi)p(\pi|\mathcal{D})\prod_{d}p(x_{d}|\theta_{d,1})p(\theta_{d,1}|\mathcal{D})\mathrm{d}\theta\mathrm{d}\pi$



individual posterior predictives
$$lacksquare$$
 $= \left(\int_{\pi} p(y=1|\pi)p(\pi|\mathcal{D})\mathrm{d}\pi\right)\prod_{d}\left(\int_{\theta_{d,1}} p(x_{d}|\theta_{d,1})p(\theta_{d,1}|\mathcal{D})\mathrm{d}\theta\right)$

for Beta distribution, we simply used the posterior mean (and dropped the integral)

$$ilde{p}(y=1|x,\mathcal{D}) = rac{lpha^\pi + N(y=1)}{lpha^\pi + eta^\pi + N} \prod_d \left(rac{lpha^ heta + N(y=1,x_d=1)}{lpha^ heta + eta^ heta + N(y=1)}
ight)^{x_d} \left(rac{eta^ heta + N(y=1,x_d=0)}{lpha^ heta + eta^ heta + N(y=1)}
ight)^{(1-x_d)}$$
 recall: Laplace smoothing

compare with our previous prediction (using MLE)

$$ilde{p}(y=1|x,\mathcal{D})=rac{N(y=1)}{N}\prod_d\left(rac{N(y=1,x_d=1)}{N(y=1)}
ight)^{x_d}\left(rac{N(y=1,x_d=0)}{N(y=1)}
ight)^{(1-x_d)}$$
 we are simply adding a constant to various frequencies

Bayesian Naive Bayes

example

puppy it is a puppy it is a kitten it is a cat that is a dog and this is a pen it is a matrix

cat

pen

is

let's classify this new sentence using Laplace smoothing:

this dog was my puppy

$$lpha^\pi=eta^\pi=lpha^ heta=eta^ heta=1$$

 $\tilde{p}(y=1|x) = \frac{4+1}{5+2} \times \frac{1+1}{4+2} \times \frac{0+1}{4+2} \times \frac{1+1}{4+2} \times \frac{3+1}{4+2} \times \frac{3+1}{4+2} \times \frac{0+1}{4+2} \times \frac{1+1}{4+2} \approx .00032$

$$ilde{p}(y=0|x) = rac{1+1}{5+2} imes rac{0+1}{1+2} imes rac{0+1}{1+2} imes rac{0+1}{1+2} imes rac{1+1}{1+2} imes rac{1+1}{1+2} imes rac{1+1}{1+2} imes rac{0+1}{1+2} imes rac{0+1}{1+2} pprox .00052$$

$$y = 0$$
 $\frac{1}{1}$ $\frac{1}{1}$ $\frac{0}{1}$ $\frac{0}{1}$ $\frac{0}{1}$ $\frac{1}{1}$ $\frac{0}{1}$

$$\overline{1}$$

$$y=1$$
 $egin{array}{c|ccccc} rac{3}{4} & rac{4}{4} & rac{1}{4} & rac{1}{4} & rac{4}{4} \end{array}$

$$\frac{1}{4}$$

$$d = 1$$

$$d$$
 =

this

$$p(y=0|x) = \frac{.00052}{.00032 + .00052} \approx .62$$

note that if D is large we have to calculate the product of many terms



numerical problems!

Log-Sum-Exp trick

In estimating unnormalized posteriors we could get numerical problems (underflow) when calculating the posterior for new instances, we work with in the **log-domain**:

$$\log ilde{p}(y|x;\pi, heta) = \log p(y;\pi) + \sum_d \log p(x_d|y; heta_d)$$

to get the final probabilities we need to normalize $ilde{\mathcal{p}}$

$$p(y|x;\pi, heta) = rac{ ilde{p}(y|x;\pi, heta)}{\sum_{c=1}^{C} ilde{p}(c|x;\pi, heta)}$$

we can do this **normalization in the log domain** as well:

$$\log p(y|x;\pi, heta) = \log ilde{p}(y|x;\pi, heta) - \log \sum_{c=1}^{C} \exp(\log ilde{p}(c|x;\pi, heta))$$

we could run into very large or small numbers inside the exponential

Log-Sum-Exp trick

we can do this **normalization in the log domain** as well:

$$\log p(y|x;\pi, heta) = \log ilde{p}(y|x;\pi, heta) - \log \sum_{c=1}^{C} \exp(\log ilde{p}(c|x;\pi, heta))$$

observation $\log \sum_c \exp a_c = \log \left(\exp(a_0) (\sum_c \exp(a_c - a_0)) = a_0 + \log \sum_c \exp(a_c - a_0)
ight)$

to make log-sum-exp numerically stable, bring the numbers $\ a_c$ close to zero

for example choose $a_0 \leftarrow \max_c a_c$

Multinomial likelihood

what if we wanted to use word frequencies in document classification?

 $x_d^{(n)}$ is the number of times word d appears in document n

	it	is	puppy	cat	pen	a	this
it is a puppy	1	1	1	0	0	1	0
it is a kitten	1	1	0	0	0	1	0
it is a cat	1	1	0	1	0	1	0
that is a dog and this is a pen	0	2	0	0	1	2	1
it is a matrix	1	1	0	0	0	1	0

Multinomial likelihood

$$p(x|y) = ext{Mult}(x; heta_y) = rac{(\sum_d x_d)!}{\prod_{d=1}^D x_d!} \prod_{d=1}^D heta_{d,y}^{x_d}$$
 probability of word d appearing x_d time

the max-likelihood estimate is again given by the relative frequency

$$heta_{d,c}^{MLE} = rac{\sum_n x_d^{(n)} \mathbb{I}(y^{(n)} = c)}{\sum_n \sum_{d'} x_{d'}^{(n)} \mathbb{I}(y^{(n)} = c)}$$
 counts of word d in all documents labelled count in al

total word count in all documents labelled c

Univariate Gaussian density

Gaussian probability density function (pdf)

$$\mathcal{N}(x;\mu,\sigma^2) = rac{1}{\sqrt{2\pi\sigma^2}} e^{-rac{(x-\mu)^2}{2\sigma^2}}$$

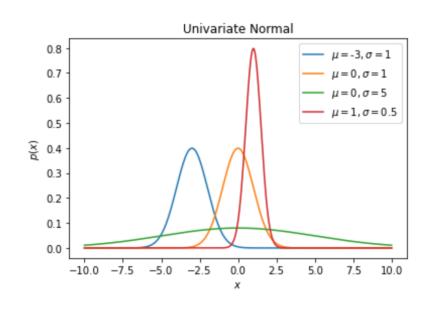
two parameters are μ, σ^2

turn out to be the mean and variance

$$\mathbb{E}[x] = \mu$$

$$\mathbb{E}[(x-\mu)^2] = \sigma^2$$

this is a random variable; we are using the same notation for a random variable and a particular value of that variable



Univariate Gaussian density

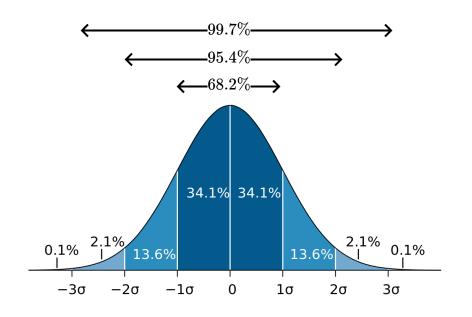
Gaussian probability density function (pdf)

$$\mathcal{N}(x;\mu,\sigma) = rac{1}{\sqrt{2\pi\sigma^2}} e^{-rac{(x-\mu)^2}{2\sigma^2}}$$

given a dataset $\mathcal{D} = \{x^{(1)}, \dots, x^{(N)}\}$

maximum likelihood estimate of μ, σ^2 are empirical mean and variance

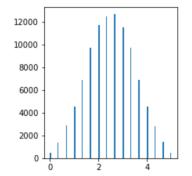
$$\mu^{MLE} = rac{1}{N} \sum_n x^{(n)}$$
 $\sigma^{2^{MLE}} = rac{1}{N} \sum_n (x^{(n)} - \mu^{MLE})^2$



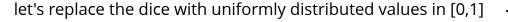
Univariate Gaussian density

two reasons why Gaussian is an important dist.

- maximum entropy dist. with a fixed variance
- central limit theorem

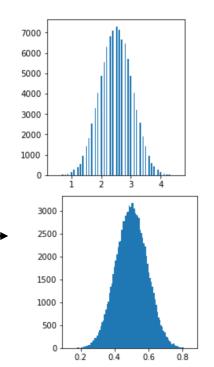


let's throw three dice, repeatedly plot the histogram of the average outcome looks familiar?



the average (and sum) of IID random variables has a Gaussian distribution

justifies use of Gaussian for observations that are mean or sum of some random values



Gaussian Naive Bayes

for continuous features one option is the Gaussian conditional likelihood

$$p(x_d \mid y) = \mathcal{N}(x_d; \mu_{d,y}, \sigma_{d,y}^2) = rac{1}{\sqrt{2\pi\sigma_{d,y}^2}} e^{-rac{(x_d - \mu_{d,y})^2}{2\sigma_{d,y}^2}}$$
 corresponds to what we previously called $heta_{d,y}$

Maximum likelihood estimates:

empirical mean & variance of feature $\,x_d\,$ across instances with label $\,y\,$

$$egin{align} \mu_{d,c} &= rac{1}{N(y=c)} \sum_{n=1}^N x_d^{(n)} \mathbb{I}(y^{(n)} = c) \ & \ \sigma_{d,c}^2 &= rac{1}{N(y=c)} \sum_{n=1}^N \mathbb{I}(y^{(n)} = c) (x_d^{(n)} - \mu_{d,y})^2 \ & \ \end{array}$$

Gaussian Naive Bayes

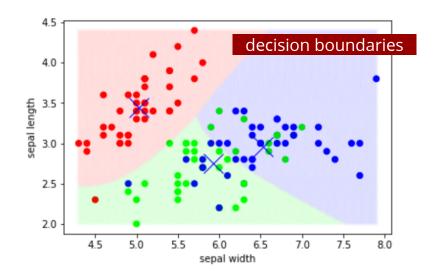
example

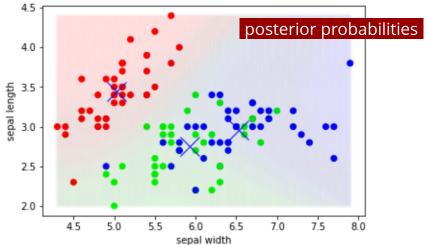
classification on Iris flowers dataset:

- we use categorical class prior (3 classes)
- Gaussian likelihood since the features are continuous (we use D=2 features)

the **decision boundary** found by Gaussian NB three means are identified using X

- ullet note that we have a mean $\,\mu_{d,c}$ and variance $\,\sigma_{d,c}^2$ for each class-feature combination
- in the plot each X is showing the *combined* mean of two features, sepal length and sepal width.





Discreminative vs. generative classification

naive Bayes

learns the **joint** distribution

$$p(y,x) = p(y)p(x \mid y)$$

the max-likelihood estimate of prior and likelihood has closed-form solution

(using empirical frequencies)

makes stronger assumptions

usually works better with smaller datasets

linear decision boundary for Gaussian naive Bayes only **if** the variance is fixed

logistic regression

learns the **conditional** distribution

$$p(y \mid x)$$

no closed-form solution

(use numerical optimization)

weaker assumptions, since it doesn't model the distribution of input (x)

usually works better with larger datasets

linear decision boundary

Summary

- generative classification:
 - learn the class prior and likelihood
 - Bayes rule for conditional class probability
- Naive Bayes
 - assumes conditional independence
 - e.g., word appearances indep. of each other given document type
 - class prior: Bernoulli or Categorical
 - likelihood: Bernoulli, Gaussian, Multinomial...
 - MLE has closed-form, estimated separately for each feature and each label
 - Bayesian Naive Bayes helps with overfitting
 - with frequent or rare feature values