# Classifiers: Naïve Bayes, evaluation 

Tomáš Svoboda and Matěj Hoffmann<br>thanks to Daniel Novák and Filip Železný, Ondřej Drbohlav<br>Vision for Robots and Autonomous Systems, Center for Machine Perception Department of Cybernetics<br>Faculty of Electrical Engineering, Czech Technical University in Prague

May 23, 2022

Example: Digit recognition/classification


- Input: 8-bit image $13 \times 13$, pixel intensities $0-255$. ( 0 means black, 255 means white)
- Output: Digit $0-9$. Decision about the class, classification.
- Features: Pixel intensities

Digit recognition is a very classical example of classification problem. It has been used for decades, and it is used till today, see e.g. MNIST demo at PyTorch

Example: Digit recognition/classification


- Input: 8-bit image $13 \times 13$, pixel intensities $0-255$. ( 0 means black, 255 means white)
- Output: Digit $0-9$. Decision about the class, classification.
- Features: Pixel intensities ...

Decision/classification problem : What cipher is in the (query) image?


Digit recognition is a very classical example of classification problem. It has been used for decades, and it is used till today, see e.g. MNIST demo at PyTorch

## Classification as a special case of statistical decision theory

- Attribute vector $\vec{x}=\left[x_{1}, x_{2}, \ldots\right]^{\top}$ : pixels $1,2, \ldots$
- State set $\mathcal{S}=$ decision set $\mathcal{D}=\{0,1, \ldots 9\}$.
- State $=$ actual class, Decision $=$ recognized class
- Loss function: $I(s, d)= \begin{cases}0, & d=s \\ 1, & d \neq s\end{cases}$


We are using different word - classification instead of decision but the reasoning and methods can be well applied in both. In classification problem we usually treat all mistakes - wrong classificaions - equally painful, contrary to decision problem - remember "What to cook for dinner" problem?

## Classification as a special case of statistical decision theory

- Attribute vector $\vec{x}=\left[x_{1}, x_{2}, \ldots\right]^{\top}$ : pixels $1,2, \ldots$.
- State set $\mathcal{S}=$ decision set $\mathcal{D}=\{0,1, \ldots 9\}$.
- State $=$ actual class, Decision $=$ recognized class
- Loss function: $I(s, d)= \begin{cases}0, & d=s \\ 1, & d \neq s\end{cases}$

Optimal decision strategy:

$$
\delta^{*}(\vec{x})=\arg \min _{d} \sum_{s} \underbrace{I(s, d)}_{0 \text { if } d=s} P(s \mid \vec{x})=\arg \min _{d} \sum_{s \neq d} P(s \mid \vec{x})
$$

Obviously $\sum_{s} P(s \mid \vec{x})=1$, then: $P(d \mid \vec{x})+\sum_{s \neq d} P(s \mid \vec{x})=1$
Inserting into above:

$$
\delta^{*}(\vec{x})=\arg \min _{d}(1-P(d \mid \vec{x}))=\arg \max _{d} P(d \mid \vec{x})
$$

We are using different word - classification instead of decision but the reasoning and methods can be well applied in both. In classification problem we usually treat all mistakes - wrong classificaions - equally painful, contrary to decision problem - remember "What to cook for dinner" problem?

## Optimal (Bayes) Classification

## $\delta^{*}(\quad)=\arg \max _{d} P(d \mid)$

Machine Learnine: Prepare training data , let (an) algorithm learn itself


Training samples: $\left(\vec{x}_{i}, s=0\right)$

Machine Learnine: Prepare training datator cipher1 , let (an) algorithm learn itself


Training samples: $\left(\vec{x}_{i}, s=1\right)$

Machine Learnine: Prepare training daator cipher 2 , let (an) algorithm learn itself


Training samples: $\left(\vec{x}_{i}, s=2\right)$

Bayes classification in practice; $P(s \mid \vec{x})=$ ?

- Usually, we are not given $P(s \mid \vec{x})$
- It has to be estimated from already classified examples - training data
- For discrete $\vec{x}$, training examples $\left(\vec{x}_{1}, s_{1}\right),\left(\vec{x}_{2}, s_{2}\right), \ldots\left(\vec{x}_{l}, s_{l}\right)$
- every ( $\left.\vec{x}_{i}, s\right)$ is drawn independently from $P(\vec{x}, s)$, i.e. sample $i$ does not depend on $1, \cdots, i-1$
- so-called i.i.d (independent, identically distributed) multiset
- Without knowing anything about the distribution, a non-parametric estimate:

$$
P(s \mid \vec{x})=\frac{P(\vec{x}, s)}{P(\vec{x})} \approx \frac{\# \text { examples where } \vec{x}_{i}=\vec{x} \text { and } s_{i}=s}{\# \text { examples where } \vec{x}_{i}=\vec{x}}
$$



## Notes

Why hard? Way too many various $\vec{x}$.
What is the difference between set and multiset?
Reminder about math notation. In literature, vectors are mostly denoted by bold lower case $\mathbf{x}$. In lectures, we use $\vec{x}$ to match notation used on blackboard. It is difficult to write bold with a chalk.

Bayes classification in practice; $P(s \mid \vec{x})=$ ?

- Usually, we are not given $P(s \mid \vec{x})$
- It has to be estimated from already classified examples - training data
- For discrete $\vec{x}$, training examples $\left(\vec{x}_{1}, s_{1}\right),\left(\vec{x}_{2}, s_{2}\right), \ldots\left(\vec{x}_{l}, s_{l}\right)$
- every ( $\left.\vec{x}_{i}, s\right)$ is drawn independently from $P(\vec{x}, s)$, i.e. sample $i$ does not depend on $1, \cdots, i-1$
- so-called i.i.d (independent, identically distributed) multiset
- Without knowing anything about the distribution, a non-parametric estimate:

$$
P(s \mid \vec{x})=\frac{P(\vec{x}, s)}{P(\vec{x})} \approx \frac{\# \text { examples where } \vec{x}_{i}=\vec{x} \text { and } s_{i}=s}{\# \text { examples where } \vec{x}_{i}=\vec{x}}
$$

Hard in practice:

- To reliably estimate $P(s \mid \vec{x})$, the number of examples grows exponentially with the number of elements of $\vec{x}$.
- e.g. with the number of pixels in images
- curse of dimensionality
- denominator often 0


## Notes

Why hard? Way too many various $\vec{x}$.
What is the difference between set and multiset?
Reminder about math notation. In literature, vectors are mostly denoted by bold lower case $\mathbf{x}$. In lectures, we use $\vec{x}$ to match notation used on blackboard. It is difficult to write bold with a chalk.

How many images?


8-bit image $13 \times 13$, pixel intensities $0-255$. ( 0 means black, 255 means white)
A: $169^{256}$
B: $256^{169}$
C: $13^{13}$
D: $169 \times 256$
E : different quantity

## Naïve Bayes classification

- For efficient classification we must thus rely on additional assumptions.
- In the exceptional case of statistical independence between components of $\vec{x}$ for each class $s$ it holds

$$
P(\vec{x} \mid s)=P(x[1] \mid s) \cdot P(x[2] \mid s) \cdot \ldots
$$

- Use simple Bayes law and maximize:

$$
P(s \mid \vec{x})=\frac{P(\vec{x} \mid s) P(s)}{P(\vec{x})}=\frac{P(s)}{P(\vec{x})} P(x[1] \mid s) \cdot P(x[2] \mid s) \cdot \ldots=
$$

- No combinatorial curse in estimating $P(s)$ and $P(x[i] \mid s)$ separately for each $i$ and $s$.
- No need to estimate $P(\vec{x})$. (Why?)
- $P(s)$ may be provided apriori.
- naïve $=$ when used despite statistical dependence


## Notes

Why naïve at all? Consider $N$-dimensional feature space and 8 - bit values. Instead of considering $8^{N}$ combinations (joint prob. distribution), we can consider only $N \times 8$-treating every feature separately.
Think about statistical independence. Example1: person's weight and height. Are they independent? Example2: pixel values in images.

Example: Digit recognition/classification


- Input: 8-bit image $13 \times 13$, pixel intensities $0-255$. ( 0 means black, 255 means white)
- Output: Digit $0-9$. Decision about the class, classification.
- Features: Pixel intensities ...

We can create many more features than just pixel intensities. But first things first.
We are assuming all errors are equally important - minimizing the number of wrong decisions.
Dimension of $\vec{x}$ is $13 \times 13=169$. There are $256^{169}$ possible images. (we already know)

Example: Digit recognition/classification


- Input: 8-bit image $13 \times 13$, pixel intensities $0-255$. ( 0 means black, 255 means white)
- Output: Digit $0-9$. Decision about the class, classification.
- Features: Pixel intensities

Collect data

- $P(\vec{x})$. What is the dimension of $\vec{x}$ ? How many possible images?
- Learn $P(\vec{x} \mid s)$ per each class (digit).
- Classify $s^{*}=\operatorname{argmax}_{s} P(s \mid \vec{x})$.


## Notes

We can create many more features than just pixel intensities. But first things first.
We are assuming all errors are equally important - minimizing the number of wrong decisions.
Dimension of $\vec{x}$ is $13 \times 13=169$. There are $256^{169}$ possible images. (we already know)

From images to $\vec{x}$


## Conditional probabilities, likelihoods



- Apriori digit probabilities $P\left(s_{k}\right)$
- Likelihoods for pixels. $P\left(x_{r, c}=I_{i} \mid s_{k}\right)$


## Notes

A lexical note, especially for Czech speakers. probability as well as likelihood can be translated as pravděpodobnost. I suggest the following mental model than can work for our purposes.

- Probability is related to the future events (unknown outcome). E.g. what is the probability of selecting blue box? What is the probability that a random ZIP Code number begins with 7 ?
- Likelihood refers to past events (known outcome). In my data, how many images of 7 have dark pixel in top right corner? We can think about relative frequency (relativní četnost).


## Conditional likelihoods



For each pixel (position) and possible instensity (image/pixel value) we create such a table.

## Unseen events



Images $13 \times 13$, intensities $0-255,100$ exemplars per each class.


$$
\begin{aligned}
\vdots & =\vdots \\
P\left(x_{0,0}=100 \mid s=7\right) & =0.05 \\
P\left(x_{0,0}=101 \mid s=7\right) & =0 \\
P\left(x_{0,0}=102 \mid s=7\right) & =0.06 \\
\vdots & =\vdots
\end{aligned}
$$

Think about the problem of classifying numerals. Some $P\left(x_{r, c}=I \mid s\right)=0$. What about an example:

$$
\begin{aligned}
\vdots & =\vdots \\
P\left(x_{0,0}=100 \mid s=7\right) & =0.05 \\
P\left(x_{0,0}=101 \mid s=7\right) & =0 \\
P\left(x_{0,0}=102 \mid s=7\right) & =0.06 \\
\vdots & =\vdots
\end{aligned}
$$

A new (not in training) query image with $x_{0,0}=101$. How would you classify?

## Unseen events



Images $13 \times 13$, intensities $0-255,100$ exemplars per each class.


$$
\begin{aligned}
\vdots & =\vdots \\
P\left(x_{0,0}=100 \mid s=7\right) & =0.05 \\
P\left(x_{0,0}=101 \mid s=7\right) & =0 \\
P\left(x_{0,0}=102 \mid s=7\right) & =0.06
\end{aligned}
$$

A new (not in training) query image with $x_{0,0}=101$. How would you classify?

## Notes

Think about the problem of classifying numerals. Some $P\left(x_{r, c}=I \mid s\right)=0$. What about an example:

$$
\begin{aligned}
\vdots & =\vdots \\
P\left(x_{0,0}=100 \mid s=7\right) & =0.05 \\
P\left(x_{0,0}=101 \mid s=7\right) & =0 \\
P\left(x_{0,0}=102 \mid s=7\right) & =0.06 \\
\vdots & =\vdots
\end{aligned}
$$

A new (not in training) query image with $x_{0,0}=101$. How would you classify?

Unseen event, how to decide?

A new (not in training) query image with $x_{0,0}=101$. How would you classify?

$$
P\left(x_{0,0}=101 \mid s_{j}\right)=0, \text { for all classes }
$$

## Laplace smoothing ("additive smoothing")

Think about a particular pixel with intensity $x$

$$
P(x)=\frac{\operatorname{count}(x)}{\text { total samples }}
$$

Problem: $\operatorname{count}(x)=0$

## Laplace smoothing ("additive smoothing")

Think about a particular pixel with intensity $x$

$$
P(x)=\frac{\operatorname{count}(x)}{\text { total samples }}
$$

Problem: $\operatorname{count}(x)=0$
Pretend you see the (any) sample one more time.

$$
P_{\mathrm{LAP}}(x)=\frac{c(x)+1}{\sum_{x}[c(x)+1]}
$$

## Laplace smoothing ("additive smoothing")

Think about a particular pixel with intensity $x$

$$
P(x)=\frac{\operatorname{count}(x)}{\text { total samples }}
$$

Problem: $\operatorname{count}(x)=0$
Pretend you see the (any) sample one more time.

$$
\begin{gathered}
P_{\mathrm{LAP}}(x)=\frac{c(x)+1}{\sum_{x}[c(x)+1]} \\
P_{\mathrm{LAP}}(x)=\frac{c(x)+1}{N+|X|}
\end{gathered}
$$

where $N$ is the number of (total) observations; $|X|$ is the number of possible values $X$ can take (cardinality).

## Laplace smoothing - as a hyperparameter $k$

Pretend you see every sample $k$ extra times:

$$
\begin{gathered}
P_{\mathrm{LAP}}(x)=\frac{c(x)+k}{\sum_{x}[c(x)+k]} \\
P_{\mathrm{LAP}}(x)=\frac{c(x)+k}{N+k|X|}
\end{gathered}
$$

For conditional, smooth each condition independently

$$
P_{\mathrm{LAP}}(x \mid s)=\frac{c(x, s)+k}{c(s)+k|X|}
$$



Hyperparameter would be tuned along with your classifier
For $k=100$ and blue and red, you would get:

- $P_{\text {LAP }}($ red $)=(2+100) /(3+100 * 2)=102 / 203$
- $P_{\text {LAP }}($ blue $)=(1+100) /(3+100 * 2)=101 / 203$

In this case, smoothing ("prior") would dominate over the observations - shifting estimate from empirical to uniform.
In the digit recognition from pixels example: 256 intensity values; $13 \times 13=169$ pixels: Applying Laplace smoothing with $k=1$ to $P(x)$ (prior probability of a particular pixel will take an intensity value $i$ ): $P\left(x_{r, c}=i\right)=$ $(c(x)+1) /(N+256)$
Conditional: relevant for the Naïve Bayes case.

Laplace smoothing - as a hyperparameter $k$
Pretend you see every sample $k$ extra times:

$$
\begin{gathered}
P_{\mathrm{LAP}}(x)=\frac{c(x)+k}{\sum_{x}[c(x)+k]} \\
P_{\mathrm{LAP}}(x)=\frac{c(x)+k}{N+k|X|}
\end{gathered}
$$

For conditional, smooth each condition independently

$$
P_{\mathrm{LAP}}(x \mid s)=\frac{c(x, s)+k}{c(s)+k|X|}
$$



What is $|X|$ equal to?
A: 10
B: 2
C: 256
D: None of the above

Hyperparameter would be tuned along with your classifier
For $k=100$ and blue and red, you would get:

- $P_{\text {LAP }}($ red $)=(2+100) /(3+100 * 2)=102 / 203$
- $P_{\text {LAP }}($ blue $)=(1+100) /(3+100 * 2)=101 / 203$

In this case, smoothing ("prior") would dominate over the observations - shifting estimate from empirical to uniform.
In the digit recognition from pixels example: 256 intensity values; $13 \times 13=169$ pixels: Applying Laplace smoothing with $k=1$ to $P(x)$ (prior probability of a particular pixel will take an intensity value $i$ ): $P\left(x_{r, c}=i\right)=$ $(c(x)+1) /(N+256)$
Conditional: relevant for the Naïve Bayes case.

What is the right degree of polynomial (hyperparameter of a regressor)
Fitting n-degree polynomial to training data


See the tuning_hyper_parameter.m demo. The small values depict sum of square errors on training data.

What is the right degree of polynomial (hyperparameter of a regressor)
Fitting n-degree polynomial to training data


See the tuning_hyper_parameter.m demo. The small values depict sum of square errors on training data.

## Generalization and overfiting

- Data: training, validating, testing . Wanted classifier performs well on what data?
- Overfitting: too close to training, poor on testing.


Training and testing
Data labeled instances.

- Training set
- Held-out (validation) set
- Testing set.

Features : Attribute-value pairs.
Learning cycle:

- Learn parameters (e.g. probabilities) on training set.
- Tune hyperparameters on held-out (validation) set.
- Evaluate performance on testing set.

Training set - biggest part.
$K-$ Nearest Neighbor and Bayes $j^{*}=\operatorname{argmax}_{j} P\left(s_{j} \mid \vec{x}\right)$

Assume data:

- $N$ samples $\vec{x}$ in total.
- $N_{j}$ samples in $s_{j}$ class. Hence, $\sum_{j} N_{j}=N$.

We want classify to $\vec{x}$. We draw a circle (hypher-sphere) centered at $\vec{x}$ containing $K$ points irrespective of class. $V$ is the volume of this sphere. $P\left(s_{j} \mid \vec{x}\right)=$ ?

$$
P\left(s_{j} \mid \vec{x}\right)=\frac{P\left(\vec{x} \mid s_{j}\right) P\left(s_{j}\right)}{P(\vec{x})}
$$


(a)
$k$ - $N N$ for non-parametric density estimation

$$
\begin{aligned}
& P(\vec{x})=\frac{K}{N V} \\
& V=V_{d} R_{k}^{d}(\vec{x})
\end{aligned}
$$

$R_{k}(\vec{x})$ - distance from $\vec{x}$ to its $k$-th nearest neighbour point (radius)

$$
V_{d}=\frac{\pi^{d / 2}}{\Gamma(d / 2+1)}
$$

volume od unit $d$-dimensional sphere,


 $\Gamma$ denotes gamma function. $\quad V_{1}=2, V_{2}=$ $\pi, V_{3}=\frac{4}{3} \pi$


More details, including a computational example, in [?].
A $K-$ NN belongs to non-parametric methods for density estimation, see section 2.5 from [1]. (Figure from [1]) Try yourself, https://scikit-learn.org/stable/modules/density.html\#kernel-density

How to evaluate a classifier? Confusion table
Matching table for test set


Figure from [5]

A result for a one particular classifer and its setting (parameters), one particular testing set.

Precision and Recall, and ...
Consider digit detection (is there a digit?) or SPAM/HAM classification.
Recall :

- How many relevant items are selected?
- Are we missing some items?
- Also called: True positive rate (TPR), sensitivity, hit rate ...


## Precision

- How many selected items are relevant?

selected elements
- Also called: Positive predictive value

False positive rate (FPR)

- Probability of false alarm

By Walber - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=36926283

$$
\begin{gathered}
\mathrm{TPR}=\frac{\mathrm{TP}}{P}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \\
\text { Precision }=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \\
\mathrm{FPR}=\frac{\mathrm{FP}}{N}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}
\end{gathered}
$$

Think about TPR vs FPR graph, what is the best classifier?


Notes

- How do you slide along the curve?
- What is the meaning of the diagonal?
- What would be the shape of the curve for the ideal/worst classifier?
- How would you compare various curve and select the best classifier?
- Think/read about other ways to evaluate/visualise classification results.

$$
P(s \mid \vec{x})=\frac{P(\vec{x} \mid s) P(s)}{P(\vec{x})}=\frac{P(s)}{P(\vec{x})} P(x[1] \mid s) \cdot P(x[2] \mid s) \cdot \ldots
$$

$P(\vec{x})$ not needed, ......

Notes
just try

- $\operatorname{prod}(\operatorname{rand}(1,100))$ and $\operatorname{prod}(r a n d(1,10000))$ in Matlab.
- $\operatorname{prod}(\operatorname{rand}(1,100))==0$ and $\operatorname{prod}(\operatorname{rand}(1,10000))==0$ in Matlab.
or in python console:
- >>> import numpy as np
- >>> np.prod(np.random.rand(100))==0
- >>> np.prod(np.random.rand(1000))==0
- >>> a = np.random.rand(1000)
>>> b = np.random.rand(1000)
>>> np.prod(a)>np.prod(b)
False
>>> np. prod(a)<np.prod(b)
False
>>> np. sum (np. $\log (a))>n p . \operatorname{sum}(n p . \log (b))$
True
Hitting the limit of number representation.
What is the way out?
$P(\vec{x})$ not needed - does not depend on the class.
Laws of logarithms...


## Product of many small numbers

$$
P(s \mid \vec{x})=\frac{P(\vec{x} \mid s) P(s)}{P(\vec{x})}=\frac{P(s)}{P(\vec{x})} P(x[1] \mid s) \cdot P(x[2] \mid s) \cdot \ldots
$$

$P(\vec{x})$ not needed, $\ldots \ldots$

$$
\log (P(x[1] \mid s) P(x[2] \mid s) \cdots)=\log (P(x[1] \mid s))+\log (P(x[2] \mid s))+\cdots
$$

## Notes

just try

- $\operatorname{prod}(\operatorname{rand}(1,100))$ and $\operatorname{prod}(\operatorname{rand}(1,10000))$ in Matlab.
- $\operatorname{prod}(\operatorname{rand}(1,100))==0$ and $\operatorname{prod}(\operatorname{rand}(1,10000))==0$ in Matlab.
or in python console:
- >>> import numpy as np
- >>> np.prod(np.random.rand (100)) $==0$
- >>> np.prod(np.random.rand (1000)) $==0$
- >>> a = np.random.rand(1000)
>>> b = np.random.rand(1000)
>>> np.prod(a)>np.prod(b)
False
>>> np.prod(a)<np.prod(b)
False
>>> np.sum(np. $\log (\mathrm{a}))>\mathrm{np} . \operatorname{sum}(\mathrm{np} . \log (\mathrm{b}))$
True
Hitting the limit of number representation.
What is the way out?
$P(\vec{x})$ not needed - does not depend on the class.
Laws of logarithms...


## References I

Further reading: Chapter 13 and 14 of [4]. Books [1] and [2] are classical textbooks in the field of pattern recognition and machine learning. This lecture has been also inspired by the 21st lecture of CS 188 at http://ai.berkeley.edu (e.g., Laplace smoothing). Many Matlab figures created with the help of [3].
[1] Christopher M. Bishop.
Pattern Recognition and Machine Learning.
Springer Science+Bussiness Media, New York, NY, 2006.
https://www.microsoft.com/en-us/research/uploads/prod/2006/01/
Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf.
[2] Richard O. Duda, Peter E. Hart, and David G. Stork.
Pattern Classification.
John Wiley \& Sons, 2nd edition, 2001.

## References II

[3] Vojtěch Franc and Václav Hlaváč.
Statistical pattern recognition toolbox.
http://cmp.felk.cvut.cz/cmp/software/stprtool/index.html.
[4] Stuart Russell and Peter Norvig.
Artificial Intelligence: A Modern Approach.
Prentice Hall, 3rd edition, 2010.
http://aima.cs.berkeley.edu/.
[5] Tomáš Svoboda, Jan Kybic, and Hlaváč Václav.
Image Processing, Analysis and Machine Vision - A MATLAB Companion.
Thomson, Toronto, Canada, $1^{\text {st }}$ edition, September 2007.
http://visionbook.felk.cvut.cz/.

