Linear Classification

Volker Tresp
Summer 2018
Classification

- Classification is the central task of pattern recognition
- Sensors supply information about an object: to which class do the object belong (dog, cat, ...)?
Linear Classifiers

- Linear classifiers separate classes by a linear hyperplane.
- In high dimensions a linear classifier often can separate the classes.
- Linear classifiers cannot solve the exclusive-or problem.
- In combination with basis functions, kernels or a neural network, linear classifiers can form nonlinear class boundaries.
Hard and Soft (sigmoid) Transfer Functions

- First, the activation function of the neurons in the hidden layer are calculated as the weighted sum of the inputs $x_i$ as
  \[ h(x) = \sum_{j=0}^{M-1} w_j x_j \]
  (note: $x_0 = 1$ is a constant input, so that $w_0$ corresponds to the bias)
- The sigmoid neuron has a soft (sigmoid) transfer function
  \[
  \text{Perceptron} : \quad \hat{y} = \text{sign}(h(x)) \\
  \text{Sigmoidal neuron:} \quad \hat{y} = \text{sig}(h(x))
  \]
Binary Classification Problems

• We will focus first on binary classification where the task is to assign binary class labels $y_i = 1$ and $y_i = 0$ (or $y_i = 1$ and $y_i = -1$)

• We already know the Perceptron. Now we learn about additional approaches

  – I. Generative models for classification
  – II. Logistic regression
  – III. Classification via regression
Two Linearly Separable Classes
Two Classes that Cannot be Separated Linearly
The Classical Example not two Classes that cannot be Separated Linearly: XOR
Separability is not a Goal in Itself. With Overlapping Classes the Goal is the Best Possible Hyperplane
I. Generative Model for Classification

- In a generative model one assumes a probabilistic data generating process (likelihood model). Often generative models are complex and contain unobserved (latent, hidden) variables.

- Here we consider a simple example: how data are generated in a binary classification problem.

- First we have a model how classes are generated $P(y)$. $y = 1$ could stand for a good customer and $y = 0$ could stand for a bad customer.

- Then we have a model how attributes are generated, given the classes $P(x|y)$. This could stand for
  - Income, age, occupation ($x$) given a customer is a good customer ($y = 1$)
  - Income, age, occupation ($x$) given a customer is not a good customer ($y = 0$)

- Using Bayes formula, we then derive $P(y|x)$: the probability that a given customer is a good customer $y = 1$ or bad customer $y = 0$, given that we know the customer’s income, age and occupation.
How is Data Generated?

- We assume that the observed classes $y_i$ are generated with probability

$$P(y_i = 1) = \kappa_1 \quad P(y_i = 0) = \kappa_0 = 1 - \kappa_1$$

with $0 \leq \kappa_1 \leq 1$.

- In a next step, a data point $x_i$ has been generated from $P(x_i|y_i)$

- (Note, that $x_i = (x_{i,1}, \ldots, x_{i,M})^T$, which means that $x_i$ does not contain the bias $x_{i,0}$)

- We now have a complete model: $P(y_i)P(x_i|y_i)$
Bayes’ Theorem

- To classify a data point $x_i$, i.e. to determine the $y_i$, we apply Bayes theorem and get

$$P(y_i|x_i) = \frac{P(x_i|y_i)P(y_i)}{P(x_i)}$$

$$P(x_i) = P(x_i|y_i = 1)P(y_i = 1) + P(x_i|y_i = 0)P(y_i = 0)$$
ML Estimate for Class Probabilities

• Maximum-likelihood estimator for the prior class probabilities are

\[
\hat{P}(y_i = 1) = \hat{\kappa}_1 = \frac{N_1}{N}
\]

and

\[
\hat{P}(y_i = 0) = \hat{\kappa}_0 = \frac{N_0}{N} = 1 - \hat{\kappa}_1
\]

where \( N_1 \) and \( N_0 \) is the number of training data points for class 1, respectively class 0

• Thus the class probabilities simply reflect the class mix
Class-specific Distributions

- To model $P(x_i|y_i)$ one can choose an application-specific distribution.
- A popular choice is a Gaussian distribution

$$P(x_i|y_i = l) = \mathcal{N}(x_i; \mu^{(l)}, \Sigma)$$

with

$$\mathcal{N}(x_i; \mu^{(l)}, \Sigma) = \frac{1}{(2\pi)^{M/2}\sqrt{|\Sigma|}} \exp \left( -\frac{1}{2} (x_i - \mu^{(l)})^T \Sigma^{-1} (x_i - \mu^{(l)}) \right)$$

- Note, that both Gaussian distributions have different modes (centers) but the same covariance matrices. This has been shown to often work well.
Multivariate Normal Distribution
Maximum-likelihood Estimators for Modes and Covariances

• One obtains a maximum likelihood estimators for the modes

\[ \hat{\mu}^{(l)} = \frac{1}{N_l} \sum_{i : y_i = l} x_i \]

• One obtains as unbiased estimators for the covariance matrix

\[ \hat{\Sigma} = \frac{1}{N - M} \sum_{l=0}^{1} \sum_{i : y_i = l} (x_i - \hat{\mu}^{(l)}) (x_i - \hat{\mu}^{(l)})^T \]
Expanding the Quadratic Terms in the Exponent

• Note that

\[-\frac{1}{2} \left( x_i - \mu^{(l)} \right)^T \Sigma^{-1} \left( x_i - \mu^{(l)} \right) \]

\[= -\frac{1}{2} x_i^T \Sigma^{-1} x_i + \mu^{(l)}^T \Sigma^{-1} x_i - \frac{1}{2} \mu^{(l)}^T \Sigma^{-1} \mu^{(l)} \]

• ... and thus, as we need next, for the difference of two quadratic terms (the first terms cancel)...

\[-\frac{1}{2} \left( x_i - \mu^{(0)} \right)^T \Sigma^{-1} \left( x_i - \mu^{(0)} \right) + \frac{1}{2} \left( x_i - \mu^{(1)} \right)^T \Sigma^{-1} \left( x_i - \mu^{(1)} \right) \]

\[= \left( \mu^{(0)} - \mu^{(1)} \right)^T \Sigma^{-1} x_i - \frac{1}{2} \mu^{(0)}^T \Sigma^{-1} \mu^{(0)} + \frac{1}{2} \mu^{(1)}^T \Sigma^{-1} \mu^{(1)} \]
A Posteriori Distribution

- It follows that

\[
P(y_i = 1|x_i) = \frac{P(x_i|y_i = 1)P(y_i = 1)}{P(x_i|y_i = 1)P(y_i = 1) + P(x_i|y_i = 0)P(y_i = 0)}
\]

\[
= \frac{1}{1 + \frac{P(x_i|y_i=0)P(y_i=0)}{P(x_i|y_i=1)P(y_i=1)}}
\]

\[
= \frac{1}{1 + \frac{\kappa_0}{\kappa_1} \exp \left( (\vec{\mu}(0) - \vec{\mu}(1))^T \Sigma^{-1} x_i - \frac{1}{2} \vec{\mu}(0)^T \Sigma^{-1} \vec{\mu}(0) + \frac{1}{2} \vec{\mu}(1)^T \Sigma^{-1} \vec{\mu}(1) \right)}
\]

\[
= \text{sig} \left( w_0 + x_i^T w \right) = \text{sig} \left( w_0 + \sum_j^M x_{i,j} w_j \right)
\]

\[
w = \Sigma^{-1} \left( \vec{\mu}(1) - \vec{\mu}(0) \right)
\]
\[ w_0 = \log \frac{\kappa_1}{\kappa_0} + \frac{1}{2} \bar{\mu}^{(0)} T \Sigma^{-1} \bar{\mu}^{(0)} - \frac{1}{2} \bar{\mu}^{(1)} T \Sigma^{-1} \bar{\mu}^{(1)} \]

- Recall: \( \text{sig}(\text{arg}) = 1/(1 + \exp(-\text{arg})) \)
• This specific generative model leads to linear class boundaries

• But we do not only get class boundaries, we get probabilities

• (Comment: The solution is analogue to Fisher’s linear discriminant analysis (LDA), where one projects the data into a space in which data from the same class have small variance and where the distance between class modes are maximized. In other words, one gets the same results from an optimization criterion without assuming Gaussian distributions)

• Although we have used Bayes formula, the analysis was frequentist. A Bayesian analysis with a prior distribution on the parameters is also possible

• If the two class-specific Gaussians have different covariance matrices ($\Sigma^{(0)}$, $\Sigma^{(1)}$) the approach is still feasible but one would need to estimate two covariance matrices and the decision boundaries are not linear anymore; still, one can simply apply Bayes rule to obtain posterior probabilities
• The generalization to multiple classes is straightforward: simply estimate a different Gaussian for each class (with shared covariances or not) and apply Bayes rule
Special Case: Naive Bayes

- With diagonal covariances matrices, one obtains a Naive-Bayes classifier

\[
P(x_i | y_i = l) = \prod_{j=1}^{M} \mathcal{N}(x_{i,j}; \mu_j^{(l)}, \sigma_j^2)
\]

- The naive Bayes classifier has considerably fewer parameters but completely ignores class-specific correlations between features; this is sometimes considered to be naive

- Even more naive:

\[
P(x_i | y_i = l) = \prod_{j=1}^{M} \mathcal{N}(x_{i,j}; \mu_j^{(l)}, 1)
\]

and then

\[
w = \vec{\mu}^{(1)} - \vec{\mu}^{(0)}
\]

\[
w_0 = \log \kappa_1 / \kappa_0 + \frac{1}{2} \vec{\mu}^{(0)T} \vec{\mu}^{(0)} - \frac{1}{2} \vec{\mu}^{(1)T} \vec{\mu}^{(1)}
\]
Special Case: Bernoulli Naive Bayes

- Naive Bayes classifiers are popular in text analysis with often more than 10000 features (key words). For example, the classes might be SPAM and no-SPAM and the features are keywords in the texts.

- Instead of a Gaussian distribution, a Bernoulli distribution is employed.

- \( P(\text{word}_j = 1|\text{SPAM}) = \gamma_{j,s} \) is the probability of observing word \( \text{word}_j \) in the document for SPAM documents.

- \( P(\text{word}_j = 0|\text{SPAM}) = 1 - \gamma_{j,s} \) is the probability of not observing word \( \text{word}_j \) in the document for SPAM documents.

- \( P(\text{word}_j = 1|\text{no-SPAM}) = \gamma_{j,n} \) is the probability of observing word \( \text{word}_j \) in the document for non-SPAM documents.

- \( P(\text{word}_j = 0|\text{no-SPAM}) = 1 - \gamma_{j,n} \) is the probability of not observing word \( \text{word}_j \) in the document for non-SPAM documents.
Then

\[ P(\text{SPAM}|\text{doc}) = \]

\[ \frac{\kappa_s \prod_j \gamma_{j,s}^{\text{word}_j} (1 - \gamma_{j,s})^{1-\text{word}_j}}{\kappa_s \prod_j \gamma_{j,s}^{\text{word}_j} (1 - \gamma_{j,s})^{1-\text{word}_j} + \kappa_n \prod_j \gamma_{j,n}^{\text{word}_j} (1 - \gamma_{j,n})^{1-\text{word}_j}} \]

Simple ML estimates are \( \gamma_{j,s} = \frac{N_{j,s}}{N_s} \) and \( \gamma_{j,n} = \frac{N_{j,n}}{N_n} \)

(\( N_s \) is the number of SPAM documents in the training set, \( N_{j,s} \) is the number of SPAM documents in the training set where \( \text{word}_j \) is present)

(\( N_n \) is the number of no-SPAM documents in the training set, \( N_{j,n} \) is the number of no-SPAM documents in the training set where \( \text{word}_j \) is present)
II. Logistic Regression

• The generative model motivates

\[ P(y_i = 1|x_i) = \text{sig} \left( x_i^T w \right) \]

(now we include the bias \( x_i^T = (x_{i,0} = i, 1, x_{i,1}, \ldots, x_{i,M-1})^T \)). \text{sig}() as defined before (logistic funktion).

• One now optimizes the likelihood of the conditional model

\[ L(w) = \prod_{i=1}^{N} \text{sig} \left( x_i^T w \right)^{y_i} \left( 1 - \text{sig} \left( x_i^T w \right) \right)^{1-y_i} \]
Log-Likelihood

- Log-likelihood function

\[
l = \sum_{i=1}^{N} y_i \log \left( \frac{1}{1 + \exp(-x_i^T w)} \right) + (1 - y_i) \log \left( \frac{1}{1 + \exp(x_i^T w)} \right)
\]

\[
l = - \sum_{i=1}^{N} y_i \log(1 + \exp(-x_i^T w)) + (1 - y_i) \log(1 + \exp(x_i^T w))
\]
Adaption

- The derivatives of the log-likelihood with respect to the parameters

\[
\frac{\partial l}{\partial w} = \sum_{i=1}^{N} y_i x_i \exp(-x_i^T w) \left( \frac{1}{1 + \exp(-x_i^T w)} \right) - (1 - y_i) x_i \exp(x_i^T w) \left( \frac{1}{1 + \exp(x_i^T w)} \right)
\]

\[
= \sum_{i=1}^{N} y_i x_i (1 - \text{sig}(x_i^T w)) - (1 - y_i) x_i \text{sig}(x_i^T w)
\]

\[
= \sum_{i=1}^{N} (y_i - \text{sig}(x_i^T w)) x_i
\]

- A gradient-based optimization of the parameters to maximize the log-likelihood

\[w \leftarrow w + \eta \frac{\partial l}{\partial w}\]

- Typically one uses a Newton-Raphson optimization procedure
Logistic Regression as a Generalized Linear Models (GLM)

- Consider a Bernoulli distribution with $P(y = 1) = \theta$ and $P(y = 0) = 1 - \theta$, with $0 \leq \theta \leq 1$

- In the theory of the exponential family of distributions, one sets $\theta = \text{sig}(\eta)$. Now we get valid probabilities for any $\eta \in \mathbb{R}$!

- $\eta$ is called the natural parameter and $\text{Sig}(\cdot)$ the inverse parameter mapping for the Bernoulli distribution.

- This is convenient if we make $\eta$ a linear function of the inputs and one obtains a Generalized Linear Model (GLM)

$$P(y_i = 1|x_i, w) = \text{sig}(x_i^T w)$$

- Thus logistic regression is the GLM for the Bernoulli likelihood model.
Application to Neural Networks and other Systems

- Logistic regression essentially defines a new cost function
- It can be applied as well to neural networks
  \[ P(y_i = 1 | x_i, w) = \text{sig}(\text{NN}(x_i)) \]
  or systems of basis functions or kernel systems
Multiple Classes and Softmax

- Consider a multinomial distribution with \( P(y = c) = \theta_c \), with \( \theta_c \geq 0 \) and \( \sum_{c=1}^{C} \theta_c = 1 \). \( c \) is the class index and \( C \) is the number of classes.

- We reparameterize (exponential family of distributions)

\[
\theta_c = \frac{\exp(\eta_c)}{\sum_{c'=1}^{C} \exp(\eta_{c'})}
\]

- The \( \eta_c \) are unconstrained; softmax notation: \( \theta_c = \text{softmax}_c(\tilde{\eta}) \)

- In GLM, we set \( \eta_c = x^T w_c \) and

\[
P(y = c|x) = \frac{\exp(x^T w_c)}{\sum_{c'=1}^{C} \exp(x^T w_{c'})}
\]

- The negative log-likelihood (cross entropy) becomes

\[
-l = - \sum_{i=1}^{N} \left( \sum_{c=1}^{C} y_{i,c} x_i^T w_c - \log \sum_{c=1}^{C} \exp(x_i^T w_c) \right)
\]
• The gradient becomes

\[- \frac{\partial l}{\partial w_{j,c}} = - \sum_i \left( y_{i,c} x_{i,j} - \frac{x_{i,j} \exp(x_i^T w_c)}{\sum_{c=1}^{C} \exp(x_i^T w_c)} \right)\]

and SGD becomes

\[w_{j,c} \leftarrow w_{j,c} + \eta x_{i,j} (y_{i,c} - \text{softmax}_c(x_i^T w_c))\]

• Compare: for the Bernoulli model with $C$ binary classes, we got

\[w_{j,c} \leftarrow w_{j,c} + \eta x_{i,j} \left( y_{i,c} - \text{sig} \left( x_i^T w_c \right) \right)\]
III. Classification via Regression

- Linear Regression:

\[ f(x_i, w) = w_0 + \sum_{j=1}^{M-1} w_j x_{i,j} \]

\[ = x_i^T w \]

- We define as target \( y_i = 1 \) if the pattern \( x_i \) belongs to class 1 and \( y_i = 0 \) (or \( y_i = -1 \)) if pattern \( x_i \) belongs to class 0.

- We calculate weights \( w_{LS} = (X^TX)^{-1}X^Ty \) as LS solution, exactly as in linear regression.

- For a new pattern \( x \) we calculate \( f(x) = x^T w_{LS} \) and assign the pattern to class 1 if \( f(x) > 1/2 \) (or \( f(x) > 0 \)) ; otherwise we assign the pattern to class 0.
Bias

- Asymptotically, a LS-solution converges to the posterior class probabilities, although a linear function is typically not able to represent $P(c = 1|x)$. The resulting class boundary can still be sensible.

- One can expect good class boundaries in high dimensions and/or in combination with basis functions, kernels, and neural networks; in high dimensions sometimes consistency can be achieved. In essence it is necessary that the linear model can model the expected probability $P(c = 1|x)$.
Classification via Regression with Linear Functions
Classification via Regression with Radial Basis Functions

Klasse 0

Klasse 1

y

1

0.5

x
Performance

- Although the approach might seem simplistic, the performance can be excellent (in particular in high dimensions and/or in combination with basis functions, kernels and neural networks). The calculation of the optimal parameters can be very fast!
Logistic Regression in Medical Statistics
Logistic Regression in Medical Statistics

- Logistic regression has become one of the most important tools in medicine to analyse the outcome of treatments.

- $y = 1$ means that the patient has the disease. $x_1 = 1$ might represent the fact that the patient was exposed (e.g., by a genetic variant) and $x_1 = 0$ might mean that the patient was not exposed. The other inputs are often typical confounders (age, sex, ...); in other applications, $x_1 = 1$ means that the patient received the treatment, and $x_1 = 0$ means that the patient did not receive the treatment.

- Logistic regression then permits the prediction of the outcome for any patient.

- Of course, of great interest is if $w_1$ is significantly positive (i.e., the exposure was harmful).
Log-Odds

- The odds is defined as

\[
\text{odds}(x_i) = \frac{P(y_i = 1|x_i)}{P(y_i = 0|x_i)}
\]

- For logistic regression, the log odds is

\[
\log \frac{P(y_i = 1|x_i)}{P(y_i = 0|x_i)} = \log \frac{1}{1 + \exp(-x_i^T w)} = x_i^T w
\]

- Thus the log odds of the outcome is \( h = x_i^T w \)
Log Odds Ratio

• Thus the log odds of getting the disease, when the patient does not get the treatment is

$$w_0 + 0 + \sum_{j=2}^{N} x_{i,j}$$

Thus the log odds of getting the disease, when the patient gets treatment is

$$w_0 + w_1 + \sum_{j=2}^{N} x_{i,j}$$

• The difference between both is the log odds ratio where the odds ratio is

$$OR = \frac{Odds(x_{x_1=1})}{Odds(x_{x_1=0})}$$

• The log odds ratio evaluates the effect of the treatment and is identical to $w_1$:

$$\log(OR) = \log Odds(x_{x_1=1}) - \log Odds(x_{x_1=0}) = w_1$$
• If $w_1 \approx 0$, then the exposure does not have an effect. The odds ratio is commonly used in case-control studies!
Appendix: Information Theory
Entropy and Cross Entropy

• In information theory, the **entropy** is defined as

\[
H(P) = - \sum_x P(X = x) \log P(X = x)
\]

It represents the (minimum) number of bits to encode data generated from \(P(X)\).

• The **cross entropy** between a true distribution \(P\) and an approximative distribution \(Q\) is defined as

\[
H(P, Q) = - \sum_x P(X = x) \log Q(X = x)
\]

It represents the minimum number of bits if the encoding uses \(Q(X)\) whereas the true distribution is \(P(X)\).
KL-Divergence

The cross-entropy cannot be smaller than the entropy: $H(P, Q) \geq H(P)$. The difference between the cross entropy and the entropy is a distance measure, the relative entropy or KL divergence (Kullback-Leibler divergence)

$$D(P\|Q) = H(P, Q) - H(P)$$

where

$$D(P\|Q) = \sum_x P(X = x) \log \frac{P(X = x)}{Q(X = x)}$$
Cross-entropy Cost Function

- Consider that you fit a multivariate Gaussian to data

- We apply the cross entropy and assume that \( P(X) \) is represented by the data and \( Q(X) \) represents the model and we get

\[
H(P, Q) = - \sum_{i} \log Q(x_i)
\]

Thus the cross entropy is identical to the negative log-likelihood (we can also start with KL-divergence, since \( H(P) \) is only data dependent)
Cross-entropy Cost Function for Prediction (Conditional Models)

- We consider the true $P(Y|X)$ and the model $Q(Y|X)$.

- The cross entropy of interest is

  $$H(P, Q) = -\int \int P(Y|X) \log Q(Y|X) P(X) dX dY$$

  $$= -\int \int P(X, Y) \log Q(Y|X) dX dY$$

- We approximate $P(X, Y)$ by the observed data and get

  $$H(P, Q) = -\sum_i \log Q(y_i|x_i)$$

  which again is the negative log likelihood.
Relationship between Random Variables

• Whereas in the definition of entropy, cross entropy and KL divergence we were interested in the relationships between different distributions defined on the same random variables, another goal is to quantify relationships between two different random variables $X$ and $Y$ when $P(X, Y)$ is given.

• **Conditional Entropy**: $H(Y|X) = \sum_x \sum_y P(x, y)P(y|x)$. In information theory, the conditional entropy (or equivocation) quantifies the amount of information needed to describe the outcome of a random variable $Y$ given that the value of another random variable $X$ is known.
Mutual Information

- **Mutual Information**: \( I(X; Y) = H(Y) - H(Y|X) \); Intuitively, mutual information measures the information that \( X \) and \( Y \) share: It measures how much knowing one of these variables reduces uncertainty about the other. It is defined as:

\[
I(X; Y) = \sum_{y \in Y} \sum_{x \in X} p(x, y) \log \left( \frac{p(x, y)}{p(x)p(y)} \right)
\]

Mutual information is one quantity used to determine if two random variables are dependent or independent. For example it might be used if an input \( X \) is predictive for an output \( Y \), in particular if both quantities are discrete.