01-03-2022 - 26-04-2022, EVERY TUESDAY FROM 18-20h

MACHINE LEARNING SPRING SCHOOL

THE BASICS OF ML 4 SOCIAL GOOD

FROM CORRELAID #LC-MUENCHEN



One note

I will add slides for Cross Validation and Classification for more than two classes tomorrow.



This module is comprised of two parts

- -The first week can be used to study this presentation and try to tackle the problem of classifying trees on your own.
- Hence this is an invitation to explore some of the possibilities for yourself or with the others from the course.
- –After the first week, you will get a notebook from me which you can compare with your own approaches taken in the first week.
- In our session we will discuss some of the findings you made.

I want to encourage you to explore the data and make findings by yourselves and in a group or team like real Data Scientists at a company or research institution would do.



Ask yourselves the following questions

- –What is the difference between a Data Scientist, Data Engineer, Machine Learning Specialist and how do you think do they approach a problem?
- -What does LEARNING in Machine Learning even mean?
- -If you were an entrepreneur, would you see Machine Learning as a tool to build a product or as a product in itself?
- -Would you trust a car's autopilot so much that you would dispose of the car's pedals and steering wheel?
- –What do you think are common misconceptions when talking about Machine Learning and specifically so called Artifical Intelligence?



Data Engineer

Profile

- Assessing the data infrastructure.
- Assessing already existing pipelines.
- Automating the process to collect, centralize and pre engineer the data such that Data Scientists can work with it.
- Guaranteeing consistent quality of the data, by implementing validations, tests

Proficiencies

- Knowledgeable in everything data base management systems.
- Myriad of possible pipeline solutions, even automated data base management (creation, updating, dropping) systems are more and more introduced.
- General understanding of "useful" data and their (relational) structure in an IT ecosystem.

My experience has shown that companies introducing Machine Learning models have the data, but in most cases do not know what to do with it. Hence, there is no useful infrastructure present to develop useful Machine Learning on.

Data Scientist

Profile

- Assessing the (possibly existing) inherent structure of the data or parts of it.
- By experience or intuition in the applied to field or past work knows what to look for to get useful results.
- Is able to implement and use Machine Learning Models, furthermore does know their limitations.

Proficiencies

- The more diverse the background knowledge of a team of Data Scientists the better (a social scientist differently analyses problems compared to a physicist).
- Knowledge of applied Machine Learning Models in the form of programming and mathematical theory.
- Has the ability to feature engineer useful
 information into the existing data

Usually Data Scientists do some of the work of a Data Engineer and Machine Learning Specialist too, especially useful feature engineering is something all profiles share.

Machine Learning Specialist

Profile

- Deep and intricate understanding of the theory behind models.
- Mathematical understanding of modelling and the learning process of the models.
- Can ask and (try to answer) theoretical questions how to improve models under certain assumptions.

Proficiencies

- Theoretical tools to approach Machine Learning questions and problems.
- Proficiency in statistics and optimization.
- Ability to implement proof of concept versions of theory, e.g. implementing a Support Vector Machine w/o using for example scikit-learn (NO easy task, doing it correctly).

Although Data Scientists need some of a Specialists's tools, "you do not have to be a mathematician to apply a linear regression or Support Vector Machine and understand what it does".

The Process



Learn A Thing Company wants to help Sarah save water in her everyday life.

Sarah like everyone else creates data







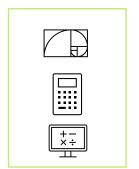


Data Engineer Petra collects and preprocesses the data, e.g. by talking to Data scientist Peter

Data Scientist Peter tries to find a logic in the data Sarah creates and tailor her experience at Learn A
Thing Company to be a happier customer



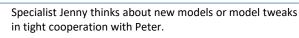






Machine Learning helped Sarah to find wasteful water usage by analyzing data that indirectly depends on water usage







General Introduction to Modelling

Or, what are we even doing?



What are you going to learn?

- To help you to learn and understand on your own, I want to give you a more general view on some of the more common models used in Data Science.
- We will take the role of someone who is a mix of a Data Scientist and a Machine Learning Specialist.
- The theory presented here should help you with working on the actual problem you already know from the last sessions.



Supervised and Unsupervised Learning

Supervised Learning

We are given pairs of Variables (X, Y)

consisting of a Feature or Input Vector X and a Label or Output Vector Y. In most cases it holds:

$$X \in \mathbb{R}^d$$
.

Then we can make two distinctions:

- 1. If it holds that: $Y \in \mathbb{R}$ we talk about regression.
- 2. If it holds that: $Y \in \{1, ..., K\}$ we talk about classification.

In practice, the dimension of the Input d is (very) large. Although this can lead to the so-called Curse of Dimensionality – meaning massive optimization problems with increasing dimension and hence problems finding solutions to a given problem – there are models accounting for this.

Unsupervised Learning

We are only given the Input Vector X without an observed label Y.

Here, the task is to find a structure in X which is not generated by random "noise".

Theoretically this means to do inference on the probability distribution of X.

Examples for unsupervised problems are:

- 1. Reduction of the complexity of data.
- 2. Reduction of the problem's dimension.
- 3. "Clustering" data, although not necessarily classifying them.



From Data To Algorithm 1/2

We want to find a (deterministic) function

$$f^*: \mathcal{X} \to \mathcal{Y}, X \mapsto f^*(X) = Y,$$

where $X \in \mathcal{X} \subset \mathbb{R}^d, Y \in \mathcal{Y} \subset \mathbb{R}$ for regression and $\mathcal{Y} \subset \{1, \dots, K\}$ for classification.

In reality, we are given n pairs of data (X_i, Y_i) , i = 1, ... n. Before we connect these observations with above function we have to consider the following technicality.

Throughout the remainder we assume that the pairs (X_i, Y_i) are identical and stochastically independent.

- 1. Independence means that for two arbitrary observations (X_i, Y_i) , (X_j, Y_j) they do not influence each other. (For example, time series from economic variables are highly dependent without further transformations.)
- 2. Identical means that they all follow the same probability distribution. Meaning that they all follow the same structure. There exist models for the cases where one assumes or does not assume such a distribution.



From Data To Algorithm 2/2

The problem we face is that we do not know the true function f^{st} .

Although, we can limit the "space" of possible functions, which we call a *model assumption*, e.g. by assuming that the dependance between X and Y is linear.

Given this model assumption and the data given in the form of the n pairs (X_i,Y_i) , we can define an approximating function \hat{f}_n which depends on our data and maps an Input Vector X onto an Output Y:

$$\hat{f}_n(X_1, Y_1, \dots X_n, Y_n | X) = Y.$$

Machine Learning is concerned with finding useful model assumptions (recall that you could predict anything from everything or nothing at all) and useful optimization methods to approximate with \hat{f}_n the true dependence f^* . Thus, in the following, we will introduce different approximations for different model assumptions which we can call algorithms or machine learning models.



Regression

By now you may have already guessed that the tree dataset leads to a classification problem. Nevertheles, regression is as import as classification and should not come short.

We will introduce three different regression models, but have to start with a short introduction to the overall problem.

Assume we have a true dependence of Y on X given by $Y = f^*(X)$. Where X is a d dimensional vector and Y is a real number. In its most simple form we assume a linear dependence, thus:

$$Y = f^*(X) = \sum_{j=1}^{a} \beta_j X_j + \epsilon$$

Here, $\beta_j \in \mathbb{R}$ are the real coefficients giving the weight of a feature with regards to the Output Y. Furthermore, the $\epsilon \in \mathbb{R}$ is a noise or error term. These can be most generally understood as errors introduced by measuring or collecting our data. Now, we can introduce n such observations to get:

$$Y_i = \sum_{j=1}^d \beta_{ij} X_{ij} + \epsilon_i$$



Regression

This again can be written in matrix notation as: $Y = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = \begin{pmatrix} X_{11} & X_{12} & \dots & X_{1d} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \dots & X_{nd} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} + \begin{pmatrix} \epsilon_1 \\ \vdots \\ \epsilon_d \end{pmatrix} = X\beta + \epsilon.$

In most classes and textbooks the most understood case where the error term ϵ is a Gaussian with mean 0 and bounded variance is presented.

In statistics or machine learning you want to find the weights β and there is rich theory how to approximate f^* by using $\hat{f}_n(X) = X\beta + \epsilon$. Here approximation is literally visible as we have to account for the error term.

Many of you already know that there is a direct estimator for the weights under the assumption that the error is a Gaussian, given as:

$$\hat{\beta} = \left(X^t X\right)^{-1} X^t Y.$$

Here X^t is the transpose of a matrix and X^{-1} its inverse. So why do I introduce you to this?

Regression is prone to the curse of dimensionality. Recall that this means that the dimension d of our inputpace is very big. Furthermore, if we have more parameters than observations in our model (n << d) the general question would be how useful our estimations are.



Curse of Dimensionality

Unfortunately this is not the whole picture of this curse. In addition (and some of you may already know) matrix inversion is computationally very expensive. Although modern machines are more sophisticated, there are lower bounds on the runtime algorithms for matrix inversion can achieve.

Plainly speaking: even for a simple model as linear regression we face the problem that we may not be able to solve our problem with the "standard" approaches you may have learned at school or university.

Before we introduce the following two models which were developed in statistics but found their way into the machine learning canon, we have to think of one more technicality.

Matrix inversion is unfeasible if the matrix' dimensions are very big and most of the values are not zero (thus we have measurements of X which are not zero). Two questions arise:

- 1. If most of the values in this very big matrix are zero, can we achieve some runtime optimization?
- 2. Even if most of the values are not zero, are really all features $X_{j1},...,X_{jd},j=1,...,n$ of our observations relevant? These two questions lead in the past to the so-called Ridge and Lasso regression models.

One note: this is just one shortcoming of linear regression applied in reality, hence there are many more methods developed for different kinds of problems that arise. For example, a search for generalized least squares would be a good starting point for further information when the error term behaves in a more complex way.



Short Recap

Recall the empirical error from Berhard's talk, given by¹:

$$\mathcal{R}\left(\hat{f}_{n}\right) = \frac{1}{n} \sum_{i=1}^{n} \left(y_{i} - \hat{f}_{n}\left(x_{i}\right)\right)^{2}.$$

This can be rewritten as:

$$\mathcal{R}\left(\hat{f}_n\right) = \frac{1}{n} \sum_{i=1}^n \left(\beta_i x_i + \epsilon_i - \hat{\beta}_i x_i\right)^2 = \frac{1}{n} \sum_{i=1}^n \left(\left(\beta_i - \hat{\beta}_i\right) x_i + \epsilon_i\right) = \mathcal{R}\left(\hat{\beta}_n\right).$$

Thus, we combined the error measure of a least squares with a model assumption of a linear regression. Our problem is finding a solution to:

$$\min_{\hat{\beta}_n \in \mathbb{R}^n} \mathcal{R}\left(\hat{\beta}_n\right).$$

The mathematical optimal² solution to this so called Ordinary Least Squares (OLS) problem is: $\hat{\beta}_n = (X^t X)^{-1} X^t Y$.

Ridge and Lasso (1/2)

As mentioned earlier, OLS is prone to the curse of dimensionality. There are two ways to account for the problem of "too much information". They are called Ridge and Lasso estimators. In both cases the model assumption does not change (hence we still assume a linear model). The change is given by the loss or error functions. For the Ridge estimator it is given as:

$$\min_{\hat{\beta}_n \in \mathbb{R}^n} \mathcal{R}\left(\hat{\beta}_n\right) = \frac{1}{n} \sum_{i=1}^n \left(y_i - \hat{\beta}_{in} x_i\right)^2 + \lambda \sum_{i=1}^d \hat{\beta}_{in}^2.$$

The minimizing estimator (thus the solution) for the weight vector $\hat{\beta}_n$ is given as:

$$\hat{\beta}_n = \left(X^t X + \lambda I_n\right)^{-1} X^t Y.$$



Ridge and Lasso (2/2)

For the Lasso estimator the empirical loss loses the squares in the second part of the sum and reduces to:

$$\min_{\hat{\beta}_n \in \mathbb{R}^n} \mathcal{R}\left(\hat{\beta}_n\right) = \frac{1}{n} \sum_{i=1}^n \left(y_i - \hat{\beta}_{in} x_i\right)^2 + \lambda \sum_{i=1}^d |\hat{\beta}_{in}|.$$

Although there exists a closed form solution (hence a plain formula as for the other cases) we will not go into detail on it.

This is a good point to introduce you to another concept of ML, namely so called hyper paramters.



Hyper Parameters

You may have already noticed the parameter λ . Notice, that lambda is not part of the model assumption but the empirical loss or error. This implies that we can neither estimate nor learn the parameter given data. We could call this parameter exogenous or in Machine Learing speak a hyper parameter. ¹

There are ways to find optimal² hyper parameters, which leads to yet another important concept, called cross validation and validation data sets.³

For Ridge and Lasso, λ is called a penalty term. Without going into detail:

the greater the value of λ the more weight parameters in the linear model are set to zero. This implies that the matrices in the linear models are "sparse" hence there are fewer weight parameters for which to solve. This in turn reduces runtime of the algorithms immensly. 4



Classification – Introduction (1/3)

Recall that in contrast to regression, classifiaction is tasked with the problem to make inference between pairs of data (X_i, Y_i) i = 1, ..., n, where

 $Y_i \in \{1, \dots, K\}$. Unfortunately, this complicates the mathematical theory of modelling and finding solutions to the problem. In general, discrete (when values can not be plotted as a line, as known from functions in school) problems are harder to handle than continuous (values can be plotted as a line, as known from functions in school) problems.

This means that we will have to take a "higher-level" approach to classification in the remainder.



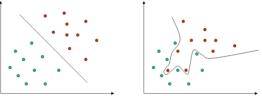
Classification – Introduction (2/3)

There are several technical approaches one can take to introduce classification problems. One that fits our purpose are decision regions. You can understand a decision region as:

A way to separate points in a space (not necessarily in three dimensions) such that you can find planes separating different data points from each other. Each "sub-space" is then identified with one of the classes $Y_i \in \{1, ..., K\}$.

In two dimensions such a "plane" would be a line which separates "clouds of

points".





Classification – Introduction (3/3)

Above picture shows a crucial difference one can make. Whereas in the first picture the two decision regions (class 1 red, class 2 green) are separated by a straight line, i.e. a linear function, the decision regions in the second picture are separated by an (arbitrary) looking function in two dimensions.

We have to keep this difference in mind when working on classification problems. Nevertheless, there are the so called Support Vector Machines which techincally are a linear model but are highly flexible when working with non "linear separable" data. Thus, we want to focus on a few standard and linear Machine Learning algorithms for calssification.



Linear and Quadratic Discriminant Analysis (1/2)

Two of the most basic models for linear classification are Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).

We have to introduce the concept of conditional probabilities to understand classification.

Assume the question: How probable is it, that my data belongs to a certain class $k=1,\ldots,K$ given the data I collected? Mathematically this can be written as (where $\mathbb P$ assigns probabilities): $\mathbb P\left(Y_i=k|X_i=x\right)$.

Now, of course we want to find the most probable class $k=1,\ldots,K$ our data belongs to. This implies the problem we have to solve:

$$\max_{k \in \{1, \dots, K\}} \mathbb{P} \left(Y_i = k | X_i = x \right).$$



Linear and Quadratic Discriminant Analysis (2/2)

There are two cases. The first being that we assume a probability distribution which our aforementioned \mathbb{P} follows. And the second being that we can or will not assume a distribution for \mathbb{P} .

LDA and QDA belong to the former. In both cases one assumes that the data is distributed according to a Gaussian (Normal distribution). This implies that they have a (multidimensional) means and (multidimensional) covariance matrices.

In the case of LDA we assume that classes have different means but identical covariance matrices between classes. In the case of QDA we assume that classes have different means and different covariance matrices. LDA has linear separated decision regions and QDA has quadratically separated decision regions.¹



Logistic Regression (1/4) – Abstract Introduction

Although the name suggests otherwise, logistic regression is an approach to solve classification problems. In contrast to LDA and QDA logistic regression does not necessitate a probability distribution assumption for P

which was a Gaussian in LDA and QDA. The logic behind Logistic Regression is to find decision functions for each of the possible classes. Then, after the training procudere, a new datapoint X is plugged into each decision function and is assigned to the class for which the decision function has the greatest value. Thus, while LDA and QDA find classes by litterally finding regions in space to separate the data into classes, Logistic Regression uses functions to rank the probability for a new data point belonging to a certain class.



Logistic Regression (2/4)

There are versions of LR which use linear decision functions and non-linear decision functions. Technically they are not that much of a difference so we will focus on the linear version. In the linear case we assume that it holds¹:

For each k = 1, ..., K there exists a weight vector $\beta^{*(k)}$ such that²:

$$\log\left(\frac{\mathbb{P}(Y=k|X=x)}{\mathbb{P}(Y=K|X=x)}\right) = x^t \beta^{*(k)}.$$

Under this assumption we can calculate probabilities for the classes directly: $\exp(x^t \beta^{*(k)})$

$$\mathbb{P}(Y = k | X = x) = \frac{\exp(x^t \beta^{*(k)})}{1 + \sum_{j=1}^{K-1} \exp(x^t \beta^{*(k)})}, k = 1, \dots, K - 1,$$

$$\mathbb{P}(Y = k | X = x) = \frac{1}{1 + \sum_{j=1}^{K-1} \exp(x^t \beta^{*(k)})}.$$



Logistic Regression (3/4)

You might have already noticed that we do not know the true weights $\beta^{*(k)}$

for each class. Hence, we have to estimate them given our data. At this point ML is introduced. Estimation of these parameters is not possible in a closed form, implying that we can not calculate the probabilities in a closed form to get a ranking of possible classes for a new data point X.

Nevertheless, using the logic from OLS, Ridge and Lasso we can define an error or loss function¹ for estimators $\hat{\beta}^{(k)}$ for the true weights $\beta^{*(k)}, k = 1, ..., K$.

Then the weights are optimized² such that this error is minimized and we get our decision functions in the form of³: $(x^t \hat{\beta}^{(k)}, k = 1,...,K-1)$

 $\delta_k(x) = \begin{cases} x^t \hat{\beta}^{(k)}, & k = 1, \dots, K - 1 \\ 0, & k = K. \end{cases}$



Logistic Regression (4/4)

The last step would be to plug in the new data point X into all decision functions $\begin{pmatrix} X^t \hat{\beta}^{(k)} & k-1 & K-1 \end{pmatrix}$

 $\delta_k(X) = \begin{cases} X^t \hat{\beta}^{(k)}, & k = 1, \dots, K - 1 \\ 0, & k = K \end{cases}$

and chose the class for X given by the rule:

$$Y = \max_{k \in \{1, \dots, K\}} \delta_k(X).$$

As you can see there is a lot of (ommitted) machinery behind one of the simpler classification algorithms. I encourge you to read on about LR, especially how the estimators for the weights $\hat{\beta}^{(k)}$ are calculated.1



k-Nearest-Neighbors (kNN)

There is another easy to understand but often useful classification algorithm. k-Nearest-Neighbors¹ does not assume any probability distribution as it does some simple geometry.

The idea is quite simple:

for every new data point X calculate its distance² from every data point given by the training data already collected. Then assign the class to X which has the most counts across the k neighbors with the least distance to X. This is called a majority vote. For example, if k = 3 you would calculate the distance from X

to all points of the training set, take the 3 closest to X and count the occurences of possible classes. Hence if two neighbors are of class 1 and one neighbor is of class 2 you would assign class 1 to X.



k-Nearest-Neighbors (kNN) - Implementation

Of course it would be interesting to programm every presented model and their optimization algorithms (which we ommitted, frankly). The problem with this is the sheer amount of work you would have to do to implement something like a feasible usable Logistic Regression. Thus, in reality everyone uses open source¹ libraries to solve their ML or Data Science problems.

But and we would like you to try it:

kNN is a really simple algorithm which you could and should try to implement for the forest data set.²



Support Vector Machines – SVM (1/2)

Support Vector Machines are the most advanced¹ models we want to take a look at. They are highly flexible and have (under certain circumstances) good runtimes.

Firstly, they are highly flexible because they allow not only for linear decision boundaries but more or less arbitrary ones.² This implies that the decision regions can be rather arbitrary which again implies highly flexible classification possibilities.



Support Vector Machines – SVM (2/2)

Secondly, they are highly flexible because they allow for errors in their training process. This is due to the fact that their decision regions are not only one line but three, in fact. This "street" is always visualized in presentations of SVM results as three parallel lines.

At last, they can be reformulated as a convexe optimization problem. The theory behind these problems is a highly advanced mathematical field. Thus there exist optimal and fast solutions in many cases.

