

Mathematical Notes

Contents

I	Machine Learning	3
1	Supervised Learning	4
1.1	Linear Regression	4
1.2	Optimization Techniques	9
1.2.1	Normal Equation	9
1.2.2	Gradient Descent	10
1.3	Logistic Regression	11
1.3.1	Normal Equation	14
1.3.2	Gradient Descent	15
1.3.3	Softmax Regression	16
1.4	Generalized Linear Model	16
1.5	Errors	16
1.5.1	Point-Wise, Overall, In-Sample & Out-Of-Sample Error	16
1.5.2	Bias & Variance	17
1.6	Evaluation	19
1.7	Regularization	22
1.7.1	Ridge Regression (L2 Regularization)	22
1.7.2	Lasso Regression (L1 Regularization)	24
1.7.3	Elastic Net	24
1.7.4	Early Stopping	25
1.8	Classification Error Metrics	25
1.9	Support Vector Machine	27
1.10	Applied Machine Learning	34
	Appendices	38
A	Constrained Optimization	39
A.1	Equality Constrained Optimization	39
A.2	Equality & Inequality Constrained Optimization	40
B	Kernels	41
C	Convolution	43

Part I

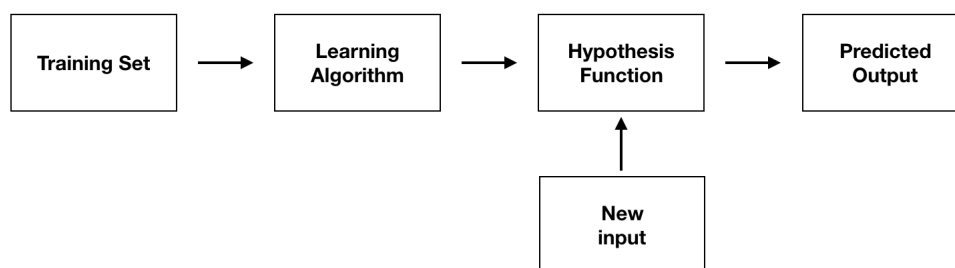
Machine Learning

Chapter 1

Supervised Learning

Supervised learning is one of the four basic categories of machine learning, and it consists of a family of models and techniques that we will introduce in this chapter. First let's start with a formal definition of supervised learning.

Definition 1.1 (Supervised Learning). ***Supervised learning** is the machine learning task of learning a function that maps an input to an output based on examples of “input - output” pairs called a “training set”.*



Some more specific notation that we will be using throughout supervised learning:

- Input variables, or attributes, or features: x .
- The i^{th} feature: x_i .
- The j^{th} training example: $x^{(j)}$.
- The i^{th} feature of the j^{th} training example: $x_i^{(j)}$.
- Output variables, or targets, or classes, or labels: y .
- The i^{th} target: $y^{(i)}$.
- Total number of training examples: m .
- Total number of features: n .

Now let's dive in the models and techniques of supervised learning, starting with one of the most basic ones called “linear regression”.

1.1 Linear Regression

Definition 1.2 (Linear Regression). ***Linear regression** is a linear approach to modelling the relationship between a dependent variable (target) and one or more independent variables (features).*

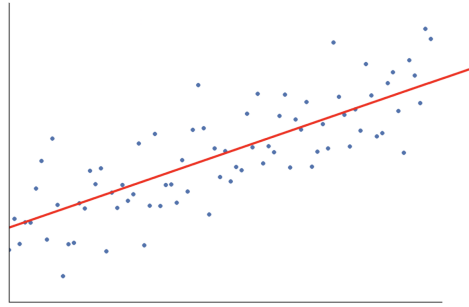
Definition 1.3 (Simple / Multiple Linear Regression). *When there is only one independent variable (feature) then the model is called **simple linear regression**. For more than one independent variables (features) the process is called **multiple linear regression**.*

Definition 1.4 (Univariate / Multivariate Linear Regression). *When only one dependent variable (target) is predicted then the model is called **univariate linear regression**. For more than one correlated, dependent variables (targets) being predicted, the process is called **multivariate linear regression**.*

In linear regression the hypothesis function h is a linear combinations of the features:

$$h(x) = w_0 + w_1x_1 + \dots + w_nx_n$$

where w_0 is called “bias” or “intercept” and the rest w_i ’s are called “weights”. We usually refer to weights and bias as the “parameters” of the regression (or the model) and they are the ones that we try to determine through the training examples by using a learning algorithm. Once we find them then h is ready to predict new inputs with unknown outcomes.



It is a usual procedure to define $x_0 = 1$, so the linear regression hypothesis function can be rewritten as:

$$h(x) = w_0x_0 + w_1x_1 + \dots + w_nx_n = \sum_{i=0}^n w_ix_i$$

Moreover by defining the feature vector \mathbf{x} and parameter vector \mathbf{w} as:

$$\mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad \mathbf{w} = \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_n \end{bmatrix}$$

we can rewrite the linear regression the hypothesis function in the very simple form of:

$$h(x) = \mathbf{w}^\top \mathbf{x}$$

(Notice that linear regression does not “allow” any polynomial terms of second or higher degree, thus the naming. However, what if our data is more complex than a straight line? Surprisingly, we can use a linear model to fit nonlinear data. The way to do this is to add powers of each feature as new features, and then move on with linear regression. This technique is called “polynomial regression”).

Now that we have a hypothesis function, we need a rule in order to be able to find the parameters \mathbf{w} . This rule can be obtained through the probabilistic interpretation of linear regression.

More precisely, after having obtained the parameters \mathbf{w} , the hypothesis will fit the data in the best possible way but, since as we said we are dealing with probabilistic systems, we will still have some errors ϵ . In other words, for each training example the following formula will apply:

$$y^{(i)} = h(x^{(i)}) + \epsilon^{(i)} = \mathbf{w}^\top \mathbf{x}^{(i)} + \epsilon^{(i)}$$

where $\mathbf{x}^{(i)}$ is the corresponding training example feature vector:

$$\mathbf{x}^{(i)} = \begin{bmatrix} x_0^{(i)} \\ x_1^{(i)} \\ \vdots \\ x_n^{(i)} \end{bmatrix}$$

At this point we will make one assumption which needs to be valid in order for the linear regression to be valid. Namely, we assume that **the errors $\epsilon^{(i)}$ are independent and identically distributed following a normal distribution with mean 0 and variance σ^2 :**

$$\epsilon^{(i)} \sim N(0, \sigma^2)$$

which means that the probability distribution of the errors is given by:

$$P(\epsilon^{(i)}) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(\epsilon^{(i)})^2}{2\sigma^2}\right)$$

From the assumption of the errors follows:

$$\begin{aligned} y^{(i)} &= \mathbf{w}^\top \mathbf{x}^{(i)} + \epsilon^{(i)} \Rightarrow \\ \epsilon^{(i)} &= y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)} \end{aligned}$$

By substituting the error back to the probability:

$$\begin{aligned} P(\epsilon^{(i)}) &= \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-\frac{(\epsilon^{(i)})^2}{2\sigma^2}\right) \Rightarrow \\ P(y^{(i)}|\mathbf{x}^{(i)}; \mathbf{w}) &= \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2}\right) \end{aligned}$$

In other words we get that the conditional distribution of $y^{(i)}$ given $\mathbf{x}^{(i)}$ and \mathbf{w} is a normal distribution with mean $\mathbf{w}^\top \mathbf{x}^{(i)}$ and variance σ^2 :

$$y^{(i)} \sim N(\mathbf{w}^\top \mathbf{x}^{(i)}, \sigma^2)$$

Given the probability distribution of $y^{(i)}$ as a function of the parameters, we can now use the principle of maximum likelihood that we developed in parametric inference chapter, in order to find the rule that will give us the best parameters \mathbf{w} .

For the likelihood we get:

$$\mathcal{L}(\mathbf{w}|y) = P(y^{(1)}, y^{(2)}, \dots, y^{(m)} | \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(m)}; \mathbf{w}) = \prod_{i=1}^m P(y^{(i)} | \mathbf{x}^{(i)}; \mathbf{w})$$

where we used the fact that $\epsilon^{(i)}$ are independent. By substituting the probability:

$$\mathcal{L}(\mathbf{w}|y) = \prod_{i=1}^m \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2}\right)$$

Subsequently for the log-likelihood:

$$\begin{aligned}
l(\mathbf{w}|y) &= \ln \mathcal{L}(\mathbf{w}|y) \\
&= \ln \left[\prod_{i=1}^m \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2}\right) \right] \\
&= \sum_{i=1}^m \ln \left[\frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp\left(-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2}\right) \right] \\
&= \sum_{i=1}^m \ln \left[\frac{1}{\sqrt{2\pi\sigma^2}} \right] + \sum_{i=1}^m \ln \left[\exp\left(-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2}\right) \right] \\
&= \sum_{i=1}^m \ln \left[\frac{1}{\sqrt{2\pi\sigma^2}} \right] + \sum_{i=1}^m \left[-\frac{(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}{2\sigma^2} \right]
\end{aligned}$$

According to the principle of maximum likelihood, the best parameters can be found by maximizing the log-likelihood. The first term of the log-likelihood is just a constant term so it does not contribute at all to the maximization, and the same holds for the denominator of the second term. Hence:

$$\begin{aligned}
\mathbf{w} &= \arg \max_{\mathbf{w}} [l(\mathbf{w}|y)] \\
&= \arg \max_{\mathbf{w}} \left[\sum_{i=1}^m -(y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2 \right] \\
&= \arg \max_{\mathbf{w}} \left[-\sum_{i=1}^m (y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2 \right] \\
&= \arg \min_{\mathbf{w}} \left[\sum_{i=1}^m (y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2 \right]
\end{aligned}$$

At this point we can formally define the following function.

Definition 1.5 (Mean Squared Error Loss Function). *Mean squared error loss function (MSE)* $J(\mathbf{w})$ is defined as:

$$J(\mathbf{w}) = \frac{1}{2m} \sum_{i=1}^m (y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2$$

Hence, the principle of maximum likelihood translates to finding the parameters \mathbf{w} that minimize the MSE loss function. The intuition behind the minimization of the MSE loss function is straight forward since what we are actually doing is minimizing the square of the errors between the prediction and the actual outcome (square because only the magnitude of the error is important and not the sign). By minimizing as much as possible the errors we will eventually get the best line that fits the data.

As a final note, we can group together all training examples in one matrix and all training labels in one vector as follows:

$$X = \begin{bmatrix} (\mathbf{x}^{(1)})^\top \\ (\mathbf{x}^{(2)})^\top \\ \vdots \\ (\mathbf{x}^{(m)})^\top \end{bmatrix} = \begin{bmatrix} x_0^{(1)} & x_1^{(1)} & \dots & x_n^{(1)} \\ x_0^{(2)} & x_1^{(2)} & \dots & x_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{(m)} & x_1^{(m)} & \dots & x_n^{(m)} \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \vdots \\ y^{(m)} \end{bmatrix}$$

By doing so then we can write the MSE loss function in the simple form of:

$$J(\mathbf{w}) = \frac{1}{2m} (\mathbf{X}\mathbf{w} - \mathbf{y})^2 = \frac{1}{2m} (\mathbf{X}\mathbf{w} - \mathbf{y})^\top (\mathbf{X}\mathbf{w} - \mathbf{y})$$

Beside the MSE loss function that is derived directly through the principal of maximum likelihood, in machine learning is quite common to use some variations of MSE depending on the problem. Here we will introduce the most basic of them.

Definition 1.6 (Root Mean Squared Error Loss Function). *Root mean squared error loss function (RMSE) $J(\mathbf{w})$ is defined as:*

$$J(\mathbf{w}) = \sqrt{MSE} = \sqrt{\frac{1}{2m} \sum_{i=1}^m (y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})^2}$$

RMSE is a frequently used measure of the differences between values predicted by a model and the values observed, and it is simply the square root of the average of squared errors. The effect of each error on RMSE is proportional to the size of the squared error, thus larger errors have a disproportionately large effect on RMSE. Consequently, RMSE is sensitive to outliers.

RMSE is always non-negative, and a value of 0 (almost never achieved in practice) would indicate a perfect fit to the data. In general, a lower RMSE is better than a higher one. However, comparisons across different types of data would be invalid because the measure is dependent on the scale of the numbers used.

RMSE is probably the most easily interpreted statistic, since it has the same units as the data. In other words RMSE is the average distance of a data point from the fitted line, measured along a vertical line.

The RMSE is directly interpretable in terms of measurement units, and so is a better measure of goodness of fit than a correlation coefficient. One can compare the RMSE to observed variation in measurements of a typical point. The two should be similar for a reasonable fit.

Definition 1.7 (Mean Bias Error). *Mean bias error loss function (MBE) $J(\mathbf{w})$ is defined as:*

$$J(\mathbf{w}) = \frac{1}{2m} \sum_{i=1}^m (y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)})$$

MBE captures the average bias in the prediction and is usually not used as a measure of the model error as high individual errors in prediction can also produce a low MBE. MBE is primarily used to estimate the average bias in the model and to decide if any steps need to be taken to correct the model bias. MBE can convey useful information, but should be interpreted cautiously because positive and negative errors will cancel out.

Definition 1.8 (Mean Absolute Error). *Mean absolute error loss function (MAE) $J(\mathbf{w})$ is defined as:*

$$J(\mathbf{w}) = \frac{1}{2m} \sum_{i=1}^m |y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)}|$$

MAE measures the average magnitude of the errors in a set of predictions, without considering their direction. It's the average over the test sample of the absolute differences between prediction and actual observation where all individual differences have equal weight. If the absolute value is not taken (the signs of the errors are not removed), the average error becomes the MBE.

Definition 1.9 (Mean Absolute Percentage Error). *Mean absolute percentage error loss function (MAPE) $J(\mathbf{w})$ is defined as:*

$$J(\mathbf{w}) = \frac{1}{2m} \sum_{i=1}^m \left| \frac{y^{(i)} - \mathbf{w}^\top \mathbf{x}^{(i)}}{y^{(i)}} \right|$$

MAPE (also known as mean absolute percentage deviation (MAPD)) is the mean of the absolute percentage errors of forecasts. Error is defined as actual or observed value minus the forecasted value. Percentage errors are summed without regard to sign to compute MAPE. This measure is easy to understand because it provides the error in terms of percentages. Also, because absolute percentage errors are used, the problem of positive and negative errors canceling each other out is avoided. Consequently, MAPE has managerial appeal and is a measure commonly used in forecasting. The smaller the MAPE the better the forecast.

1.2 Optimization Techniques

Given the MSE loss function (or any other loss function), the goal of machine learning is to optimize it (usually minimize it) in order to obtain the best parameters that fit the data. Optimizing loss functions is one of the biggest parts of machine learning and we can do so with the so called “optimization techniques”.

Definition 1.10 (Optimization Techniques). *Optimization techniques are techniques used for finding the optimum solution or unconstrained maxima or minima of continuous and differentiable functions. These are analytical methods and make use of differential calculus in locating the optimal solution.*

1.2.1 Normal Equation

Probably the most straight forward optimization technique is the so called “normal equation”. Since we are looking a minimum for $J(\mathbf{w})$ the natural thing to do, is to simply calculate the derivative with respect to the parameter vector and then set it to zero (as we did when we introduced the principle of maximum likelihood).

It is more handy to use the vector form of MSE loss function, so for the derivative we get:

$$\begin{aligned}\nabla_{\mathbf{w}} J(\mathbf{w}) &= \frac{1}{2m} \nabla_{\mathbf{w}} \left[(\mathbf{X}\mathbf{w} - \mathbf{y})^\top (\mathbf{X}\mathbf{w} - \mathbf{y}) \right] \\ &= \frac{1}{2m} \nabla_{\mathbf{w}} \left[\left((\mathbf{X}\mathbf{w})^\top - \mathbf{y}^\top \right) (\mathbf{X}\mathbf{w} - \mathbf{y}) \right] \\ &= \frac{1}{2m} \nabla_{\mathbf{w}} \left[(\mathbf{X}\mathbf{w})^\top (\mathbf{X}\mathbf{w}) - (\mathbf{X}\mathbf{w})^\top \mathbf{y} - \mathbf{y}^\top (\mathbf{X}\mathbf{w}) + \mathbf{y}^\top \mathbf{y} \right] \\ &= \frac{1}{2m} \nabla_{\mathbf{w}} \left[(\mathbf{X}\mathbf{w})^\top (\mathbf{X}\mathbf{w}) - 2(\mathbf{X}\mathbf{w})^\top \mathbf{y} + \mathbf{y}^\top \mathbf{y} \right] \\ &= \frac{1}{2m} \nabla_{\mathbf{w}} \left[\mathbf{w}^\top \mathbf{X}^\top \mathbf{X} \mathbf{w} - 2\mathbf{w}^\top \mathbf{X}^\top \mathbf{y} + \mathbf{y}^\top \mathbf{y} \right] \\ &= \frac{1}{2m} \left[2\mathbf{X}^\top \mathbf{X} \mathbf{w} - 2\mathbf{X}^\top \mathbf{y} \right] \\ &= \frac{1}{m} \left[\mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} \right]\end{aligned}$$

By setting the derivative to 0 we obtain:

$$\begin{aligned}\nabla_{\mathbf{w}} J(\mathbf{w}) &= 0 \Rightarrow \\ \frac{1}{m} \left[\mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} \right] &= 0 \Rightarrow \\ \mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} &= 0 \Rightarrow \\ \mathbf{X}^\top \mathbf{X} \mathbf{w} &= \mathbf{X}^\top \mathbf{y} \Rightarrow \\ \underbrace{(\mathbf{X}^\top \mathbf{X})^{-1} (\mathbf{X}^\top \mathbf{X})}_I \mathbf{w} &= (\mathbf{X}^\top \mathbf{X})^{-1} \mathbf{X}^\top \mathbf{y} \Rightarrow \\ \mathbf{w} &= (\mathbf{X}^\top \mathbf{X})^{-1} \mathbf{X}^\top \mathbf{y}\end{aligned}$$

This final expression is called “Normal Equation”, and it is an exact analytical solution that gives the parameter vector.

Despite the fact that normal equation gives an exact analytical result, computing the seemingly harmless inverse of an $((n+1) \times m) \times ((n+1) \times m) = (n+1) \times (n+1)$ matrix is, with today’s most efficient computer science algorithm, of cubic time complexity (in other words, if you double the number of

features, you multiply the computation time by roughly 2^3). This means that as the dimensions of X increase (mainly the number of features), the amount of operations required to compute the final result increases in a cubic trend. If X was rather small, then using the normal equation would be feasible.

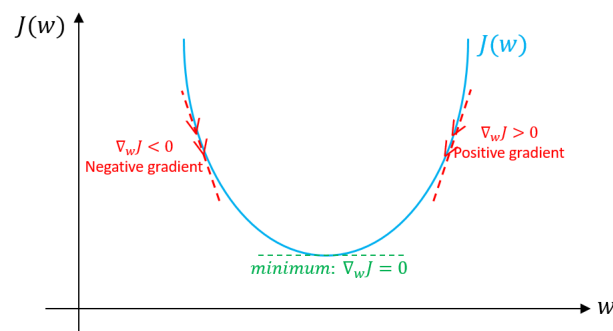
In practise, for the vast majority of any industrial application with large datasets, the normal equation would take extremely, sometimes nonsensically, long. This is the reason why normal equation is almost never used. Now let's move on to the most standard optimization technique used today called "gradient descent".

1.2.2 Gradient Descent

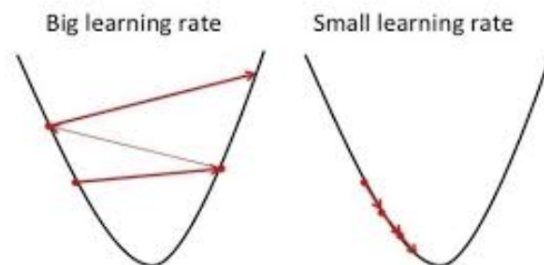
Gradient descent, and all its improvements and alternatives, is the most used optimization technique in machine learning and deep learning. It is a generic optimization algorithm capable of finding optimal solutions to a wide range of problems. The general idea of gradient descent is to tweak parameters iteratively in order to minimize a cost function by starting with some random initial values for the parameters and calculating the value of the loss function based on them, and finally updating them based on the following relation:

$$\mathbf{w} := \mathbf{w} - \alpha \nabla_{\mathbf{w}} J(\mathbf{w})$$

Since the derivative is positive when J is upwards slopping and negative when it is downwards slopping, the minus sign makes sure that we always update the parameters towards the direction that minimizes J . Once the minimum is reached then J is at a global optimum so the derivative is 0 and further updates are not possible. At this stage the gradient descent is over and the best parameters have been found.



The hyperparameter α is called "learning rate" and defines how big or small steps we take after each iteration of gradient descent. If α is too large, we might fail to find the minimum due to oscillations around it. If α is too small then gradient descent might take too much time to reach the minimum of J . Tuning learning rate in a "right" value is a topic by itself and it is quite have researched today.



Of course, not all cost functions look like nice, regular bowls. There may be holes, ridges, plateaus, and all sorts of irregular terrains, making convergence to the minimum difficult. In general gradient descent works best with convex functions, where if you pick any two points on the curve of a convex function, the line segment joining them never crosses the curve. This implies that there are no local minima, just

one global minimum. They are also continuous functions with slopes that never changes abruptly. Hence in convex functions gradient descent is guaranteed to approach arbitrarily close the global minimum (if you wait long enough and if the learning rate is not too high).

Coming back to our case, let's find the update rule specifically for linear regression. Fortunately, the MSE cost function for a Linear Regression model happens to be a convex function. The only thing missing is the derivative of MSE loss function J . However in the previous chapter with normal equation we showed that:

$$\nabla_{\mathbf{w}} J(\mathbf{w}) = \frac{1}{m} (X^\top X \mathbf{w} - X^\top \mathbf{y}) = \frac{1}{m} X^\top (X \mathbf{w} - \mathbf{y})$$

Hence the update rule reads:

$$\mathbf{w} := \mathbf{w} - \frac{\alpha}{m} X^\top (X \mathbf{w} - \mathbf{y})$$

As we already mentioned there are many improvements and modified algorithms based on gradient descent philosophy. We are going to cover a lot of them in these notes. For now, let's start with 3 basics versions of gradient descent.

- **Batch Gradient Descent**

Batch gradient descent is actually the one we just saw. As we see in gradient descent, the whole training set X is used in order to make just one update of the parameters. We usually refer to the whole training set as the “batch”. For that reason, the usual terminology for what we have seen so far is “batch gradient descent”, meaning that the whole batch is used to update the parameter.

- **Mini-Batch Gradient Descent**

In “mini-batch gradient descent” we divide the whole dataset to b subsets of $\frac{m}{b}$ training examples each, called “mini-batches”, and we update the parameters using each of the mini-batches in each iteration.

- **Stochastic Gradient Descent**

In “stochastic gradient descent” we only use one training example per time to update the parameters. In every iteration we pick the training example randomly hence the naming.

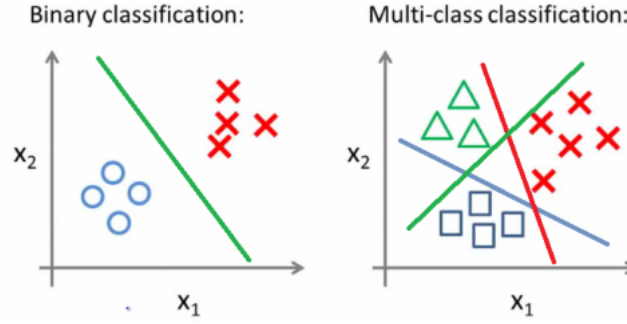
One of the main problems of batch gradient descent is that as the number of training examples grows the dimensions of X grows and using the whole training set for every iteration becomes computationally expensive. Both mini-batch and stochastic gradient descent deal with this problem.

In a way, mini-batch gradient descent tries to strike a balance between the goodness of batch gradient descent and speed of stochastic gradient descent. In general, batch gradient descent works just fine so we don't need the alternative techniques we just introduced. However in more complicated models, such as deep learning models, these techniques can be really useful. For this reason we will examine again these techniques in more details in the chapter of deep learning.

1.3 Logistic Regression

Definition 1.11 (Logistic Regression). ***Logistic regression** (or classification) is a statistical model that is used for the classification of a discrete dependent variable (target).*

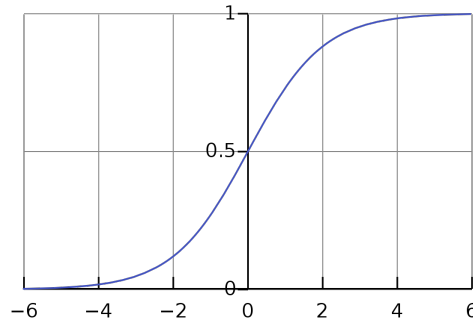
Definition 1.12 (Binary / Multiclass Classification). ***Binary** classification is the problem of classifying instances into one of two classes. Classifying instances into three or more classes is called **multiclass** or (multinomial) classification.*



For now we will focus on binary classification. Since the output is binary and can take only the values 0 or 1, the hypothesis function of the linear regression is not a valid approximator for logistic regression since it produces a continuous set of outputs. So our first step is to find a suitable hypothesis function h for logistic regression. The hypothesis function that we actually use in logistic regression is the sigmoid function and it is given by:

$$h(\mathbf{x}) = \frac{1}{1 + \exp(-\mathbf{w}^\top \mathbf{x})}$$

(From now on, in order to save space, we will write $h(\mathbf{x})$ instead of the actual expression for the sigmoid function).



Hence, in logistic regression, the hypothesis function computes a weighted sum of the input features (plus a bias term), but instead of outputting the result directly like the linear regression hypothesis function does, it outputs the logistic (sigmoid function) of this result. Notice that $h(\mathbf{x}) < 0.5$ when $\mathbf{w}^\top \mathbf{x} < 0$, and $h(\mathbf{x}) \geq 0.5$ when $\mathbf{w}^\top \mathbf{x} \geq 0$, so a logistic regression model predicts 1 if $\mathbf{w}^\top \mathbf{x}$ is positive and 0 if it is negative. (The argument of the sigmoid function is often called “logit”).

It is worth mentioning that one can alter the threshold of 0.5 to any value between 0 and 1. This is quite usual in logistic regression models when obtaining the correct class is more important than a possible misclassification.

Now let's try to give a meaning to the hypothesis function. As we can see the sigmoid function produces results in the interval $[0, 1]$. It is quite close to what we need, but not exactly so, since we do not need all the values between 0 and 1. For this reason we will interpret the hypothesis function of logistic regression as a probability measure of the target to belong to class 1. The closer to 0 the hypothesis function, the more unlikely for the target to belong in class 1 (hence it belongs to class 0) and the closer to 1 the more likely to belong to the class 1. Hence, by defining a threshold (say at 0.5) the idea is that for $h(\mathbf{x}) < 0.5$ the algorithm will predict 0 and for $h(\mathbf{x}) \geq 0.5$ the algorithm will predict 1. Based on this intuition, we can write:

$$h(\mathbf{x}) = P(y = 1 | \mathbf{x}; \mathbf{w})$$

Of course since the output must be either 0 or 1 we get:

$$\begin{aligned} P(y = 0|\mathbf{x}; \mathbf{w}) + P(y = 1|\mathbf{x}; \mathbf{w}) &= 1 \Rightarrow \\ P(y = 0|\mathbf{x}; \mathbf{w}) &= 1 - P(y = 1|\mathbf{x}; \mathbf{w}) \Rightarrow \\ P(y = 0|\mathbf{x}; \mathbf{w}) &= 1 - h(\mathbf{x}) \end{aligned}$$

We can combine these two probabilities in one in the following way:

$$P(y|\mathbf{x}; \mathbf{w}) = h(\mathbf{x})^y \cdot (1 - h(\mathbf{x}))^{(1-y)}$$

So in logistic regression the output follows a Bernoulli distribution with parameter $h(\mathbf{x})$. Now that we have a probability distribution, similarly to the linear regression, we can use the principle of the maximum likelihood in order to obtain the best parameters that maximize the likelihood. Thus, we will obtain the loss function for the logistic regression case.

By making again the assumption that we are dealing with independent and identically distributed random variables, for the likelihood is:

$$\mathcal{L}(\mathbf{w}|y) = P(y^{(1)}, y^{(2)}, \dots, y^{(m)} | \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(m)}; \mathbf{w}) = \prod_{i=1}^m P(y^{(i)} | \mathbf{x}^{(i)}; \mathbf{w})$$

By substituting the probability:

$$\mathcal{L}(\mathbf{w}|y) = \prod_{i=1}^m h(\mathbf{x}^{(i)})^{y^{(i)}} \cdot (1 - h(\mathbf{x}^{(i)}))^{(1-y^{(i)})}$$

Subsequently for the log-likelihood:

$$\begin{aligned} l(\mathbf{w}|y) &= \ln \mathcal{L}(\mathbf{w}|y) \\ &= \ln \left[\prod_{i=1}^m h(\mathbf{x}^{(i)})^{y^{(i)}} \cdot (1 - h(\mathbf{x}^{(i)}))^{(1-y^{(i)})} \right] \\ &= \sum_{i=1}^m \ln \left[h(\mathbf{x}^{(i)})^{y^{(i)}} \cdot (1 - h(\mathbf{x}^{(i)}))^{(1-y^{(i)})} \right] \\ &= \sum_{i=1}^m \left[\ln \left(h(\mathbf{x}^{(i)})^{y^{(i)}} \right) + \ln \left((1 - h(\mathbf{x}^{(i)}))^{(1-y^{(i)})} \right) \right] \\ &= \sum_{i=1}^m \left[y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right] \end{aligned}$$

Once again, according to the principle of maximum likelihood, the best parameters can be found by maximizing the log-likelihood. Hence:

$$\begin{aligned} \mathbf{w} &= \arg \max_{\mathbf{w}} [l(\mathbf{w}|y)] \\ &= \arg \max_{\mathbf{w}} \left[\sum_{i=1}^m \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right) \right] \\ &= \arg \min_{\mathbf{w}} \left[- \sum_{i=1}^m \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right) \right] \end{aligned}$$

At this point we can formally define the following function.

Definition 1.13 (Cross Entropy Loss Function). ***Cross entropy loss function** (also called log loss)*

is defined as:

$$J(\mathbf{w}) = -\frac{1}{m} \sum_{i=1}^m \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right)$$

The cross entropy is the loss function of the logistic regression in the similar way where MSE loss function is the loss function for linear regression. The name “cross entropy” comes from the definition of cross entropy which is the average amount of information needed to identify an event between two probability distributions p and q over the same underlying set of events

Notice that the only possible values of $y^{(i)}$ is 0 or 1. This means that in any case, one of the terms $y^{(i)}$ or $(1 - y^{(i)})$ in J will vanish and the other one will be equal to 1. So in the end the only thing that is actually part of the loss is the logarithm of the hypothesis function, which given that the hypothesis function is a sigmoid function which is always between 0 and 1, the logarithm is always negative. With the overall negative sign the loss turns positive and this is what we want to minimize.

We are not going to write a vectorized form for the cross entropy loss function for two reasons. First of all, not all matrices have a logarithm and those matrices that do have a logarithm may have more than one logarithm. So one has to be careful when uses the vectorized form of logistic regression because it carries logarithms of matrices. Secondly, derivatives of logarithms of non square matrices sometimes are not defined. Since we need to calculate the derivative of J we might get problems. For this reason we will use the non vectorized form for the calculations, however we will express the final result in a vectorized form.

As in the linear case, the principle of maximum likelihood leads to the minimization of the cross entropy loss function in order to obtain the best parameters. We will examine the same techniques that we developed for the gradient descent in the linear case, i.e normal equation and gradient descent.

1.3.1 Normal Equation

As we already mentioned, since we want to minimize a function the straight forward way of doing that is to calculate the derivative and then set it to 0. However, in the case of logistic regression the normal equation does not apply since there is no closed analytical solution of $\nabla_{\mathbf{w}} J(\mathbf{w}) = 0$. The only way for solving the optimization problem is through gradient descent.

1.3.2 Gradient Descent

Gradient descent works fine in logistic regression. First, let's calculate the derivative of $J(\mathbf{w})$ for logistic regression:

$$\begin{aligned}
\nabla_{\mathbf{w}} J(\mathbf{w}) &= -\frac{1}{m} \nabla_{\mathbf{w}} \left[\sum_{i=1}^m \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right) \right] \\
&= -\frac{1}{m} \sum_{i=1}^m \left(y^{(i)} \cdot \nabla_{\mathbf{w}} \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \nabla_{\mathbf{w}} \ln(1 - h(\mathbf{x}^{(i)})) \right) \\
&= -\frac{1}{m} \sum_{i=1}^m \left(y^{(i)} \cdot \frac{\nabla_{\mathbf{w}} h(\mathbf{x}^{(i)})}{h(\mathbf{x}^{(i)})} - (1 - y^{(i)}) \cdot \frac{\nabla_{\mathbf{w}} h(\mathbf{x}^{(i)})}{1 - h(\mathbf{x}^{(i)})} \right) \\
&= -\frac{1}{m} \sum_{i=1}^m \left(\frac{y^{(i)}}{h(\mathbf{x}^{(i)})} - \frac{1 - y^{(i)}}{1 - h(\mathbf{x}^{(i)})} \right) \cdot \nabla_{\mathbf{w}} h(\mathbf{x}^{(i)}) \\
&= -\frac{1}{m} \sum_{i=1}^m \left(\frac{y^{(i)} \cdot (1 - h(\mathbf{x}^{(i)})) - (1 - y^{(i)}) \cdot h(\mathbf{x}^{(i)})}{h(\mathbf{x}^{(i)}) \cdot (1 - h(\mathbf{x}^{(i)}))} \right) \cdot \nabla_{\mathbf{w}} \left[\frac{1}{1 + \exp(-\mathbf{w}^\top \mathbf{x}^{(i)})} \right] \\
&= -\frac{1}{m} \sum_{i=1}^m \left(\frac{y^{(i)} - y^{(i)} \cdot h(\mathbf{x}^{(i)}) - h(\mathbf{x}^{(i)}) + y^{(i)} \cdot h(\mathbf{x}^{(i)})}{h(\mathbf{x}^{(i)}) \cdot (1 - h(\mathbf{x}^{(i)}))} \right) \cdot \left(\frac{-1}{(1 + \exp(-\mathbf{w}^\top \mathbf{x}^{(i)}))^2} \cdot \exp(-\mathbf{w}^\top \mathbf{x}^{(i)}) \cdot (-\mathbf{x}^{(i)}) \right) \\
&= -\frac{1}{m} \sum_{i=1}^m \left(\frac{y^{(i)} - h(\mathbf{x}^{(i)})}{h(\mathbf{x}^{(i)}) \cdot (1 - h(\mathbf{x}^{(i)}))} \right) \cdot \left(h(\mathbf{x}^{(i)})^2 \cdot \frac{1 - h(\mathbf{x}^{(i)})}{h(\mathbf{x}^{(i)})} \cdot \mathbf{x}^{(i)} \right) \\
&= \frac{1}{m} \sum_{i=1}^m \frac{h(\mathbf{x}^{(i)}) - y^{(i)}}{h(\mathbf{x}^{(i)}) \cdot (1 - h(\mathbf{x}^{(i)}))} \cdot h(\mathbf{x}^{(i)}) \cdot (1 - h(\mathbf{x}^{(i)})) \cdot \mathbf{x}^{(i)} \\
&= \frac{1}{m} \sum_{i=1}^m (h(\mathbf{x}^{(i)}) - y^{(i)}) \cdot \mathbf{x}^{(i)}
\end{aligned}$$

Hence the update rule reads:

$$\mathbf{w} := \mathbf{w} - \frac{\alpha}{m} \sum_{i=1}^m \left(\frac{1}{1 + \exp(-\mathbf{w}^\top \mathbf{x}^{(i)})} - y^{(i)} \right) \cdot \mathbf{x}^{(i)}$$

Or in vectorized form:

$$\mathbf{w} := \mathbf{w} - \frac{\alpha}{m} X^\top \left(\frac{1}{1 + \exp(-X\mathbf{w})} - \mathbf{y} \right)$$

At this point, notice that gradient descent can be generalized into one model for both linear and logistic regression since the update rule for both of them can be written in one coherent way as:

$$\mathbf{w} := \mathbf{w} - \frac{\alpha}{m} X^\top (h(X) - \mathbf{y})$$

where one has to use either MSE loss function or cross entropy loss function depending on the regression problem.

1.3.3 Softmax Regression

1.4 Generalized Linear Model

As we showed, in linear regression the target follows a normal distribution while in logistic regression the target follows a Bernoulli distribution. We can generalize both regressions in one coherent model called “generalized linear model” in which the target is allowed to follow a broad family of probability distributions.

Definition 1.14 (Generalized Linear Model). ***Generalized linear model (GLM)** is a model that allows the dependent variable to follow an exponential family of probability distributions of the form:*

$$P(y|\eta) = b(y) \cdot \exp(\eta^\top T(y) - a(\eta))$$

By picking specific values for b , η , T and a we end up with different distributions (including linear and logistic regression). Then we simply assume independence and apply the principle of maximum likelihood to obtain a loss function, in order to minimize it and find the best parameters.

1.5 Errors

Since h is an estimator of f , the theory we developed in the chapter of parametric inference for estimators also holds for h . In other words, for the hypothesis function, which acts as an estimator for f , we can define quantities such as MSE, sampling deviation, bias and variance. We can then use these quantities in order to evaluate how well a machine learning model performs. Let us see now the definitions of these quantities adjusted for the case of machine learning where the estimator is h .

1.5.1 Point-Wise, Overall, In-Sample & Out-Of-Sample Error

Starting from the corresponding MSE, in machine learning case we define the following quantities:

Definition 1.15 (Point-Wise Error). *We define the **point-wise error** e as a function of the real target function f and the hypothesis function h at point x :*

$$e = e(f(x), h(x))$$

For example, for linear regression we could use $e(f(x), h(x)) = (f(x) - h(x))^2$ while for logistic regression $e(f(x), h(x)) = [f(x) \neq h(x)]$. Given point-wise error we can generalize to overall error.

Definition 1.16 (Overall Error). *We define the **overall error** E as the average over all point-wise errors $e(f(x), h(x))$ at every point x .*

We distinguish between two kind of overall errors: the in-sample error and the out-of-sample error.

Definition 1.17 (In-Sample Error). *We define the **in-sample error** E_{in} as the average of point-wise errors of the dataset that the model was trained:*

$$E_{in} = \frac{1}{m} \sum_{i=1}^m e(f(x^{(i)}), h(x^{(i)}))$$

In other words in-sample error shows how well the model performs on the data used to build it.

Definition 1.18 (Out-Of-Sample Error). *We define the **out-of-sample error** E_{out} as the expected value of point-wise errors of new data:*

$$E_{out} = E_x[e(f(x), h(x))]$$

In other word out-of-sample error show how well the model generalizes to predictions for data it has not seen before. It makes sense that in order for h to work well out of sample, so it can predict, it must be $E_{out} \approx 0$.

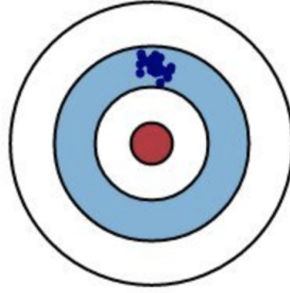
1.5.2 Bias & Variance

Back in parametric inference chapter, we introduced the bias B of an estimator $\hat{\theta}$, as the difference between the expected value of the estimator and the actual true parameter we want to estimate, $B = E[\hat{\theta}_n] - \theta$. Coming to our case where our estimator is $\hat{\theta} = h(x)$ and the true parameter is the target function $\theta = f(x)$, for the bias we get:

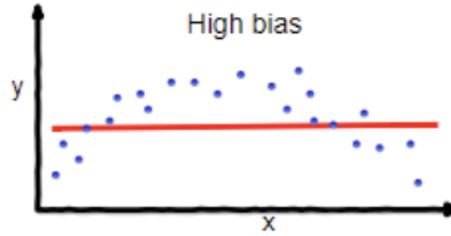
Definition 1.19 (Bias). *We define the **bias** B of the hypothesis function h as the quantity:*

$$B = E[h(x)] - f(x)$$

The bias error is an error from erroneous assumptions in the learning algorithm. When we are dealing with high bias, formally we can say that the hypothesis set $H = \{h\}$ was not big enough in order to contain function that can approximate well the target function f . So our best approximation for f is still a bad one that cannot fit the data well.



High bias can cause an algorithm to miss the relevant relations between features and target outputs and fail to capture the underlying structure of the dataset. We call this a case of **underfitting**, since the model fails to fit the given dataset well.



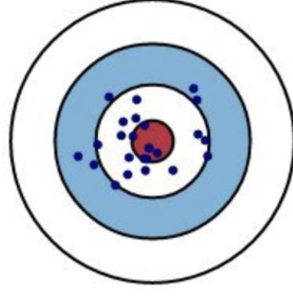
Underfitting is one of the two main problems that a machine learning model can have and it leads to a high in-sample error E_{in} which subsequently leads to a high out-of-sample error E_{out} . Hence even that the problem is coming from the in-sample error it leads to not being able to generalize for out-of-sample data.

In parametric inference chapter, we also defined the variance of an estimator $\hat{\theta}_n$ as the expected value of the square difference of the estimator from the expected value of the estimator: $Var = E[(\hat{\theta}_n - E[\hat{\theta}_n])^2]$. Coming back to machine learning for the variance we get:

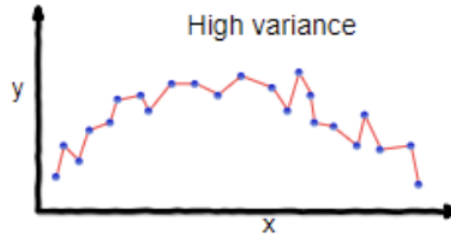
Definition 1.20 (Variance). *We define the **variance** B of the hypothesis function h as the quantity:*

$$Var = E_x[(h(x) - E_x[h(x)])^2]$$

The variance is an error from sensitivity to small fluctuations in the training set.



When we are dealing with high variance, informally we can say that the hypothesis set $H = \{h\}$ is very big so in order to compensate the spread of dataset the model finds a function that fits the particular data very well but fails to generalize to new data. We call this a case of **overfitting**, since the model fails to generalize to new data.

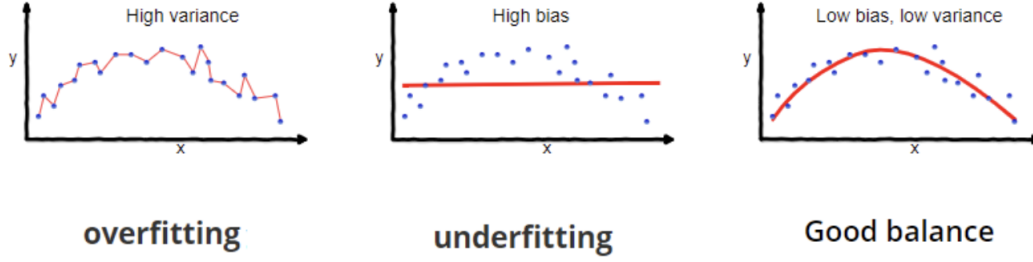


Overfitting leads to a very low in-sample $E_{in} \approx 0$, since it does a very good job on fitting the given data. However it fails to generalize, hence to predict new data, which leads to a very high out-of-sample error E_{out} .

Back in parametric inference we also showed that the mean squared error can be decomposed to bias and variance, and of course the same holds in our case since for the out of sample error of linear regression we can show:

$$\begin{aligned}
 E_{out} &= E_x [e(f(x), h(x))] \\
 &= E_x \left[\left(f(x) - h(x) \right)^2 \right] \\
 &= E_x \left[\left(f(x) - h(x) + E_x[h(x)] - E_x[h(x)] \right)^2 \right] \\
 &= E_x \left[\left(\left(f(x) - E_x[h(x)] \right) + \left(E_x[h(x)] - h(x) \right) \right)^2 \right] \\
 &= E_x \left[\left(f(x) - E_x[h(x)] \right)^2 + 2 \left(f(x) - E_x[h(x)] \right) \left(E_x[h(x)] - h(x) \right) + \left(E_x[h(x)] - h(x) \right)^2 \right] \\
 &= E_x \left[\left(f(x) - E_x[h(x)] \right)^2 \right] + E_x \left[2 \left(f(x) - E_x[h(x)] \right) \left(E_x[h(x)] - h(x) \right) \right] + E_x \left[\left(E_x[h(x)] - h(x) \right)^2 \right] \\
 &= \left(f(x) - E_x[h(x)] \right)^2 + 2 \left(f(x) - E_x[h(x)] \right) \left(E_x \left[E_x[h(x)] - h(x) \right] \right) + E_x \left[\left(E_x[h(x)] - h(x) \right)^2 \right] \\
 &= \left(f(x) - E_x[h(x)] \right)^2 + 2 \left(f(x) - E_x[h(x)] \right) \left(E_x[h(x)] - E_x[h(x)] \right) + E_x \left[\left(E_x[h(x)] - h(x) \right)^2 \right] \\
 &= \left(f(x) - E_x[h(x)] \right)^2 + E_x \left[\left(E_x[h(x)] - h(x) \right)^2 \right] \\
 &= B^2 + Var
 \end{aligned}$$

Hence, the out-of-sample error is actually a combination of bias and variance. So in order to have a model that generalizes well, we have to keep both of them low. However, since they are of opposite nature, the more we reduce bias the more variance increases and vice versa. This is the so called **bias-variance trade off**. The goal in machine learning is to balance this trade off so the model fits the data well and doesn't fail to generalize.



In this graph we see that in the case of high bias (underfitting) we have restricted our model to linear predictors, however the data do not follow a linear trend, hence the hypothesis set is too small and the model cannot find a good curve to fit the data. On the other hand, in the case of high variance (overfitting) the hypothesis set is so big allowing complex predictors so the model managed to find a high degree polynomial that fit the data really good, however it will fail to generalize since it depends a lot on the initial values of the data and it is sensitive to fluctuations of them. Finally in the last graph we have a good balance of bias and variance and the model found a good curve.

One has to keep in mind that increasing a model's complexity will typically increase its variance and reduce its bias. Conversely, reducing a model's complexity increases its bias and reduces its variance. This is why it is called a "trade-off".

1.6 Evaluation

Evaluation is about how good a model generalizes to new data. After applying the learning algorithm to the data and having obtained a hypothesis h , the machine learning model is ready to make new predictions. However before that, we have to evaluate the model by analysing the errors that we just introduced.

The starting part is the in-sample and out-of-sample errors that we defined previously:

$$E_{in} = \frac{1}{m} \sum_{i=1}^m e(f(x^{(i)}), h(x^{(i)})) \quad \text{and} \quad E_{out} = E_x[e(f(x), h(x))]$$

In general, for the error function e we use the corresponding loss function J that we used to train the model (although some times we can use variations of it), since it is a function of the target and hypothesis functions as e , and it is a really good measure of error:

$$E_{in} = \frac{1}{m} \sum_{i=1}^m J^{(i)}(f(x^{(i)}), h(x^{(i)})) \quad \text{and} \quad E_{out} = E_x[J(f(x), h(x))]$$

where here the notation $J^{(i)}$ means the error coming from the i^{th} training example. Hence, now E_{in} is calculated with the data that we trained the model, so it's a very good measure of how well the model performs in the data that it was trained on. The problem comes from E_{out} since we don't know how to compute this expected value. Unsurprising we will perform the usual trick of substituting the expected value with the average so:

$$E_{in} = \frac{1}{m} \sum_{i=1}^m J^{(i)}(f(x^{(i)}), h(x^{(i)})) \quad \text{and} \quad E_{out} = \frac{1}{m} \sum_{i=1}^m J^{(i)}(f(x^{(i)}), h(x^{(i)}))$$

Of course since we estimate the expected value with an average that brings an error to the estimation of the out-of-sample error. However for our purposes we assume that this error is neglectful, and from now on we will treat the estimated out-of-sample error as the actual out-of-sample error. In general we have to keep in mind though that out-of-sample error carries an error.

The question that arises is what data are we going to use for E_{out} . Using the same data that we trained the model is a really bad idea since, first of all, we will simply get $E_{out} = E_{in}$ and secondly the model

already knows the correct answers of the data since we used them to train it, and the evaluation will be biased.

In order to overcome this problem, we split the dataset (before training the model) into two parts: training set and evaluation set. Then we use the first to train the model and obtain E_{in} and the latter to evaluate its performance and obtain E_{out} . Since the model is trained with the train set, it has never seen the evaluation set so the estimation of the out-of-sample error with the evaluation set will be unbiased.

One of the things to consider is the proportions of splitting the dataset into training set and evaluation set. This again is an area of heavy research, but in general in machine learning we usually split them either in a proportion of “70% - 30%” or more often of “80% - 20%” depending on the amount of data. (In all cases the largest proportion goes for training the model). In other areas of machine learning like deep learning where we usually have a very large amount of data we use splitting rules of “99% - 1%”. But we will address this issue in details in deep learning chapter.

Hence, before training we split the dataset as:

- Training Dataset: $\{x_{\text{train}}^{(i)}, y_{\text{train}}^{(i)}\}, \quad i = 1, 2, \dots, m_{\text{train}} \quad (70\% \text{ or } 80\% \text{ of initial dataset}).$
- Test Dataset: $\{x_{\text{eval}}^{(i)}, y_{\text{eval}}^{(i)}\}, \quad i = 1, 2, \dots, m_{\text{eval}} \quad (30\% \text{ or } 20\% \text{ of initial dataset}).$

And subsequently the errors become:

$$E_{in} = \frac{1}{m_{\text{train}}} \sum_{i=1}^{m_{\text{train}}} J^{(i)}(f(x^{(i)}), h(x^{(i)})) \quad \text{and} \quad E_{out} = \frac{1}{m_{\text{eval}}} \sum_{i=1}^{m_{\text{eval}}} J^{(i)}(f(x^{(i)}), h(x^{(i)}))$$

From now on we will be referring to the first expression as $J_{\text{train}} = E_{in}$ and to the second one as $J_{\text{eval}} = E_{out}$.

So for example for linear regression we would have:

$$J_{\text{train}} = \frac{1}{2m_{\text{train}}} \sum_{i=1}^{m_{\text{train}}} (y^{(i)} - \mathbf{w}^T \mathbf{x}^{(i)})^2 \quad \text{and} \quad J_{\text{eval}} = \frac{1}{2m_{\text{eval}}} \sum_{i=1}^{m_{\text{eval}}} (y^{(i)} - \mathbf{w}^T \mathbf{x}^{(i)})^2$$

While for logistic regression we would have:

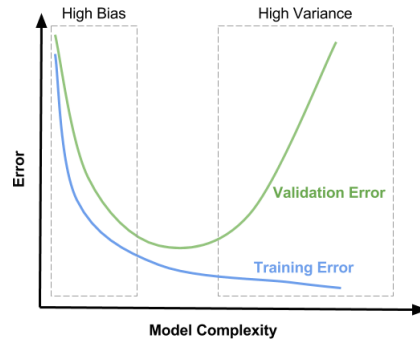
$$J_{\text{train}} = -\frac{1}{m_{\text{train}}} \sum_{i=1}^{m_{\text{train}}} \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right)$$

and:

$$J_{\text{eval}} = -\frac{1}{m_{\text{eval}}} \sum_{i=1}^{m_{\text{eval}}} \left(y^{(i)} \cdot \ln h(\mathbf{x}^{(i)}) + (1 - y^{(i)}) \cdot \ln(1 - h(\mathbf{x}^{(i)})) \right)$$

Now that we have J_{train} and J_{eval} we know how well the models performs in and out of sample. However we can also use them in order to find if the model suffers from underfitting or overfitting. There are two ways that we can do so.

The first way, is by gradually increasing the complexity of the model (higher polynomial degrees so bigger hypothesis set), training the model for each complexity level and calculate both J_{train} and J_{eval} for each model. Then by plotting out the different values for different levels of complexity we usually end up with the following graph:



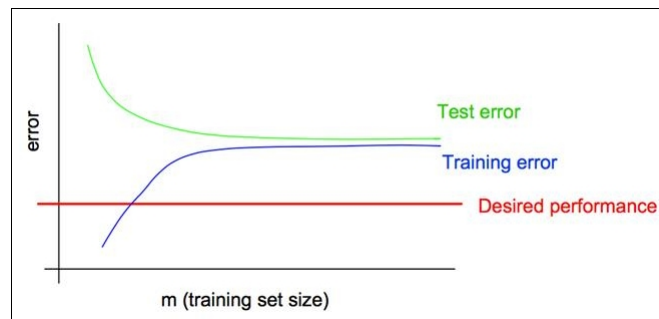
In the high bias area both J_{train} and J_{eval} are high. This means that the model does not fit the training data well hence it fails to generalize. This is the case of underfitting. In the high variance area, J_{train} is low but J_{eval} is high. This means that the model fits the training data well but fails to generalize to unseen data. This is the case of overfitting. Hence by using the graph we can diagnose both cases!

The second way to diagnose the problem of the model, is through the so called “learning curves”.

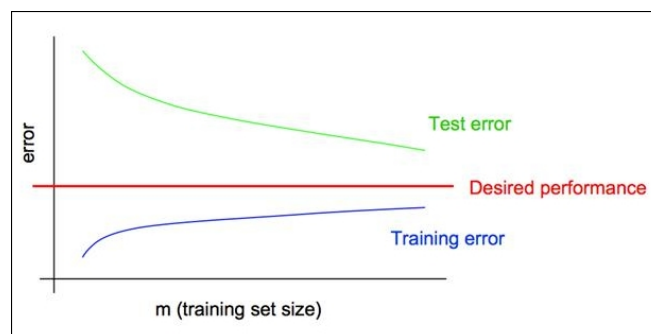
Definition 1.21 (Learning Curve). A **learning curve** is a graphical representation of how an increase in learning comes from greater experience; or how the more someone performs a task, the better they get at it.

Informally, a learning curve is the relation between error (as expressed in loss function) and training examples m . By plotting this relation for both J_{train} and J_{eval} we end up with two learning curves and by their relative position we can diagnose if our model suffers from high bias or high variance.

More specifically, when the learning curves of J_{train} and J_{eval} do not have a large gap between them as m increases we are usually dealing with a case of high bias and underfitting.



On the other hand when there is a large gap between the two curves we are dealing with the case of high variance and overfitting.



Once we detect the problem then we have to make some changes in order to fix them! Here are some of the techniques that we follow:

- For high bias (underfitting):
 - Increase model complexity.
 - Increase number of features.
- For high variance (overfitting):
 - Decrease model complexity.
 - Decrease number of features.
 - Find more training examples.
 - Regularization (next section).

1.7 Regularization

As we saw in the previous section, when we allow a very broad hypothesis set with many higher order terms the model might find a hypothesis function h that gives a 0 in-sample error but fails to generalize. This is due to high variance, i.e large dependence on the very specific dataset used for training, and we call this a case of overfitting. A way to deal with overfitting is a collection of techniques that undergo with the name “regularization”.

Definition 1.22 (Regularization). *Regularization is the process of adding information in order to solve an ill-posed problem and to prevent overfitting.*

There are many different regularization techniques. We will begin with four main ones called “Ridge Regression” (or “L2 Regularization”), “Lasso Regression” (or “L1 Regularization”), “Elastic Net”, and “Early Stopping”.

1.7.1 Ridge Regression (L2 Regularization)

The reason of overfitting is that the parameters \mathbf{w} are free to get any value. With regularization we penalize the parameters by imposing an extra constraint on \mathbf{w} of the form:

$$\mathbf{w}^\top \mathbf{w} \leq C$$

where C is a constant defined by us and it controls the effect of regularization. It is called “L2 regularization” because the quantity $\mathbf{w}^\top \mathbf{w}$ is actually the squared L2 norm of the vector \mathbf{w} :

$$\|\mathbf{w}\|_2^2 = \mathbf{w}^\top \mathbf{w}$$

Hence now the optimization problem becomes to minimize the loss function $J(\mathbf{w})$ subject to the above mentioned constraint. According to (Appendix A) in order to do so we define the Lagrangian:

$$\mathcal{L}(\mathbf{w}) = J(\mathbf{w}) + \frac{\lambda}{2m} \mathbf{w}^\top \mathbf{w}$$

where λ is the Lagrange multiplier, and then we solve the equation:

$$\nabla_{\mathbf{w}} \mathcal{L}(\mathbf{w}) = 0$$

For example, for linear regression where $J(\mathbf{w})$ is the MSE loss function, the Lagrangian reads:

$$\mathcal{L}(\mathbf{w}) = J(\mathbf{w}) + \frac{\lambda}{2m} \mathbf{w}^\top \mathbf{w} = \frac{1}{2m} (\mathbf{X}\mathbf{w} - \mathbf{y})^\top (\mathbf{X}\mathbf{w} - \mathbf{y}) + \frac{\lambda}{2m} \mathbf{w}^\top \mathbf{w}$$

At this point we can redefine this Lagrangian as a new loss function of the form:

$$J(\mathbf{w}) = \frac{1}{2m} \left[(\mathbf{X}\mathbf{w} - \mathbf{y})^\top (\mathbf{X}\mathbf{w} - \mathbf{y}) + \lambda \mathbf{w}^\top \mathbf{w} \right]$$

and then the problem is to minimize this loss function which is actually a regression problem. The corresponding regression is called “Ridge regression” (or “Tikhonov regularization”), where the only difference with linear regression is that we have to add the extra term in the loss function to reduce overfitting.

The coefficient λ is the one that controls the regularization effect on the regression. In one extreme where $\lambda = 0$ the regularization term vanishes, and the loss function ends up to the mean squared error loss function, hence the ridge regression turns to linear regression. In the other extreme where $\lambda \rightarrow \infty$ then the regularization term penalizes all parameters in an extreme way, so the ridge regression, in order to minimize the loss, is forced to set all the parameters to 0. In the end we end up with $\mathbf{w}^\top \mathbf{x} = 0$. For all intermediate values of λ we get different levels of regularization. It is actually our job to tune the model to the right λ that does the job.

Now that we have a loss function, we treat the problem in the similar way as we did before. For example, in the linear case of ridge regression we can solve the normal equation in the same way we solved it before:

$$\begin{aligned}
J(\mathbf{w}) &= \frac{1}{2m} \left[(\mathbf{X}\mathbf{w} - \mathbf{y})^\top (\mathbf{X}\mathbf{w} - \mathbf{y}) + \lambda \mathbf{w}^\top \mathbf{w} \right] \\
&= \frac{1}{2m} \left[\left((\mathbf{X}\mathbf{w})^\top - \mathbf{y}^\top \right) (\mathbf{X}\mathbf{w} - \mathbf{y}) + \lambda \mathbf{w}^\top \mathbf{w} \right] \\
&= \frac{1}{2m} \left[(\mathbf{X}\mathbf{w})^\top (\mathbf{X}\mathbf{w}) - (\mathbf{X}\mathbf{w})^\top \mathbf{y} - \mathbf{y}^\top (\mathbf{X}\mathbf{w}) + \mathbf{y}^\top \mathbf{y} + \lambda \mathbf{w}^\top \mathbf{w} \right] \\
&= \frac{1}{2m} \left[(\mathbf{X}\mathbf{w})^\top (\mathbf{X}\mathbf{w}) - 2(\mathbf{X}\mathbf{w})^\top \mathbf{y} + \mathbf{y}^\top \mathbf{y} + \lambda \mathbf{w}^\top \mathbf{w} \right] \\
&= \frac{1}{2m} \left[\mathbf{w}^\top \mathbf{X}^\top \mathbf{X} \mathbf{w} - 2\mathbf{w}^\top \mathbf{X}^\top \mathbf{y} + \mathbf{y}^\top \mathbf{y} + \lambda \mathbf{w}^\top \mathbf{w} \right]
\end{aligned}$$

By setting the derivative to 0 we obtain:

$$\begin{aligned}
\nabla_{\mathbf{w}} J(\mathbf{w}) &= 0 \Rightarrow \\
\frac{1}{2m} \nabla_{\mathbf{w}} \left[\mathbf{w}^\top \mathbf{X}^\top \mathbf{X} \mathbf{w} - 2\mathbf{w}^\top \mathbf{X}^\top \mathbf{y} + \mathbf{y}^\top \mathbf{y} + \lambda \mathbf{w}^\top \mathbf{w} \right] \\
\frac{1}{2m} \left[2\mathbf{X}^\top \mathbf{X} \mathbf{w} - 2\mathbf{X}^\top \mathbf{y} + 2\lambda \mathbf{w} \right] &= 0 \Rightarrow \\
\frac{1}{m} \left[\mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} + \lambda \mathbf{w} \right] &= 0 \Rightarrow \\
\mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} + \lambda \mathbf{w} &= 0 \Rightarrow \\
(\mathbf{X}^\top \mathbf{X} + \lambda \mathbf{I}) \mathbf{w} &= \mathbf{X}^\top \mathbf{y} \Rightarrow \\
\underbrace{(\mathbf{X}^\top \mathbf{X} + \lambda \mathbf{I})^{-1} (\mathbf{X}^\top \mathbf{X} + \lambda \mathbf{I})}_{\mathbf{I}} \mathbf{w} &= (\mathbf{X}^\top \mathbf{X} + \lambda \mathbf{I})^{-1} \mathbf{X}^\top \mathbf{y} \Rightarrow \\
\mathbf{w} &= (\mathbf{X}^\top \mathbf{X} + \lambda \mathbf{I})^{-1} \mathbf{X}^\top \mathbf{y}
\end{aligned}$$

The only difference with the normal equation of linear regression is the extra term $\lambda \mathbf{I}$ coming from regularization.

Gradient descent also works for ridge regression. For the derivative of J :

$$\nabla_{\mathbf{w}} J(\mathbf{w}) = \frac{1}{m} \left(\mathbf{X}^\top \mathbf{X} \mathbf{w} - \mathbf{X}^\top \mathbf{y} + \lambda \mathbf{w} \right) = \frac{1}{m} \mathbf{X}^\top \left((\mathbf{X} + \lambda \mathbf{I}) \mathbf{w} - \mathbf{y} \right)$$

Hence the update rule reads:

$$\mathbf{w} := \mathbf{w} - \frac{\alpha}{m} X^\top \left((X + \lambda I) \mathbf{w} - \mathbf{y} \right)$$

Of course, L2 regularization can be applied also for the case of logistic regression. More specifically, for cross entropy loss function of logistic regression the Lagrangian reads:

$$\mathcal{L}(\mathbf{w}) = J(\mathbf{w}) + \frac{\lambda}{2m} \mathbf{w}^\top \mathbf{w} = -\frac{1}{m} \left(\mathbf{y}^\top \cdot \ln h(X) + (I - \mathbf{y})^\top \cdot \ln(I - h(X)) \right) + \frac{\lambda}{2m} \mathbf{w}^\top \mathbf{w}$$

Similarly to the linear case, we redefine this Lagrangian as a new loss function of the form:

$$J(\mathbf{w}) = -\frac{1}{m} \left[\mathbf{y}^\top \cdot \ln h(X) + (I - \mathbf{y})^\top \cdot \ln(I - h(X)) - \frac{\lambda}{2} \mathbf{w}^\top \mathbf{w} \right]$$

As we said back in logistic regression, normal equation does not apply here since there is no closed analytical solution, however gradient descent still applies where the rule simply reads:

$$\mathbf{w} := \left(1 - \frac{\alpha \lambda}{m} \right) \mathbf{w} - \frac{\alpha}{m} X^\top \left(\frac{1}{1 + \exp(-X\mathbf{w})} - \mathbf{y} \right)$$

In both cases solving ridge regression will give us as a result a solution that slightly underfits the data, compared to linear or logistic regression. This underfitting will produce higher bias hence, due to bias-variance trade off, a reduced variance which will lead to the reduction of overfitting.

1.7.2 Lasso Regression (L1 Regularization)

In ridge regression we used the L2 norm of the vector \mathbf{w} . Another way of regularization is to use L1 norm which is:

$$\|\mathbf{w}\|_1 \leq C$$

By repeating the same way of analysis as in ridge regression, we can define the following loss function for linear regression:

$$J(\mathbf{w}) = \frac{1}{2m} \left[(X\mathbf{w} - \mathbf{y})^\top (X\mathbf{w} - \mathbf{y}) + \lambda \|\mathbf{w}\|_1 \right]$$

and for logistic regression:

$$J(\mathbf{w}) = -\frac{1}{m} \left[\mathbf{y}^\top \cdot \ln h(X) + (I - \mathbf{y})^\top \cdot \ln(I - h(X)) - \frac{\lambda}{2} \|\mathbf{w}\|_1 \right]$$

The corresponding regression is called “Least Absolute Shrinkage and Selection Operator Regression”, usually simply called “Lasso regression”. An important characteristic of Lasso regression is that it tends to eliminate the weights of the least important features (i.e set them to zero). In other words, Lasso regression automatically performs feature selection and outputs a sparse model (i.e with few nonzero feature weights).

As before, we can use normal equation and gradient descent to solve Lasso regression.

1.7.3 Elastic Net

Elastic net is a middle ground between Ridge Regression and Lasso Regression. The regularization term is a simple mix of both Ridge and Lasso’s regularization terms, and you can control the mix ratio between them with a parameter r .

The elastic net loss function for linear regression reads:

$$J(\mathbf{w}) = \frac{1}{2m} \left[(X\mathbf{w} - \mathbf{y})^\top (X\mathbf{w} - \mathbf{y}) + r\lambda \|\mathbf{w}\|_1 + (1 - r)\lambda \mathbf{w}^\top \mathbf{w} \right]$$

and for logistic regression:

$$J(\mathbf{w}) = -\frac{1}{m} \left[\mathbf{y}^\top \cdot \ln h(X) + (I - \mathbf{y})^\top \cdot \ln(I - h(X)) - r\frac{\lambda}{2} \|\mathbf{w}\|_1 - (1 - r)\frac{\lambda}{2} \mathbf{w}^\top \mathbf{w} \right]$$

When $r = 0$, Elastic Net is equivalent to Ridge Regression, and when $r = 1$, it is equivalent to Lasso Regression.

Since Elastic Net summarizes both Ridge and Lasso Regression, it is a good point to analyse, when one should use plain Linear (or Logistic) Regression (without any regularization), Ridge, Lasso, or Elastic Net? It is almost always preferable to have at least a little bit of regularization, so generally plain Linear Regression should be avoided. Ridge is a good default, but if one suspects that only a few features are useful, they should prefer Lasso or Elastic Net because they tend to reduce the useless features' weights down to zero, as we have discussed. In general, Elastic Net is preferred over Lasso because Lasso may behave erratically when the number of features is greater than the number of training instances or when several features are strongly correlated.

1.7.4 Early Stopping

A very different way to regularize iterative learning algorithms such as Gradient Descent is to stop training as soon as the validation error reaches a minimum. This is called “early stopping”. In general as the algorithm learns, its prediction error on the training set goes down, along with its prediction error on the validation set. After a while though, the validation error stops decreasing and starts to go back up. This indicates that the model has started to overfit the training data. Early stopping just stops training as soon as the validation error reaches the minimum. It is such a simple and efficient regularization technique that Geoffrey Hinton called it a “beautiful free lunch”.

1.8 Classification Error Metrics

In classification problems where both input and output can be either 0 or 1, we can follow a different approach of error evaluation based on exact matches and mismatches between prediction and actual result. The usual case, since we are dealing with a binary output, is to define either 0 or 1 as the positive class and the remaining as the negative one. Which one is which depends on the nature of the problem. For now we will stick with the case where 0 represents the negative class and 1 the positive one.

Given that both the actual class and the predicted class can be either positive or negative we end up with 4 different, distinct situations. Let us define them formally.

Definition 1.23 (True Positive). ***True positive (TP)** also called **hit**, is the case where the model predicts a positive result when the actual outcome is indeed positive.*

Definition 1.24 (True Negative). ***True negative (TN)** also called **correct rejection**, is the case where the model predicts a negative result when the actual outcome is indeed negative.*

Definition 1.25 (False Positive). ***False positive (FP)** also called **false alarm** or **type I error**, is the case where the model predicts a positive result when the actual outcome is negative.*

Definition 1.26 (False Negative). ***False negative (FN)** also called **miss** or **type II error**, is the case where the model predicts a negative result when the actual outcome is positive.*

Once the model is trained, we test it on the evaluation set and we measure the number of occurrences of each category. Then we gather them all together to the so called “confusion matrix”.

Definition 1.27 (Confusion Matrix). ***Confusion matrix** is a table that reports the number of true positives TP, true negatives TN, false positives FP and false negatives FN of a model.*

	Predicted 0	Predicted 1
Actual 0	TN	FP
Actual 1	FN	TP

Once we have constructed the confusion matrix we can define the following error metrics:

Definition 1.28 (Accuracy). **Accuracy** (ACC) is the rate that shows overall how often the model was correct:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

Definition 1.29 (Error Rate). **Error rate** (ERR) also called **misclassification**, is the rate that shows overall how often the model was incorrect:

$$ERR = \frac{FP + FN}{TP + TN + FP + FN}$$

It is of course: $ACC + ERR = 1$

Definition 1.30 (True Positive Rate). **True positive rate** (TPR) also called **sensitivity** or **recall** or **hit rate**, is the rate that shows how often the model predicts positive when the actual outcome is indeed positive:

$$TPR = \frac{TP}{TP + FN}$$

Definition 1.31 (False Negative Rate). **False negative rate** (FNR) also called **miss rate**, is the rate that shows how often the model predicts negative when the actual outcome is positive:

$$FNR = \frac{FN}{TP + FN}$$

It is of course: $TPR + FNR = 1$

Definition 1.32 (True Negative Rate). **True negative rate** (TNR) also called **specificity** or **selectivity**, is the rate that shows how often the model predicts negative when the actual outcome is indeed negative:

$$TNR = \frac{TN}{TN + FP}$$

Definition 1.33 (False Positive Rate). **False positive rate** (FPR) also called **fall-out rate**, is the rate that shows how often the model predicts positive when the actual outcome is negative:

$$FPR = \frac{FP}{TN + FP}$$

It is of course: $TNR + FPR = 1$

Definition 1.34 (Positive Predicted Value). **Positive predicted value** (PPV) also called **precision**, is the rate that shows how often the model is correct when it predicts positive:

$$PPV = \frac{TP}{TP + FP}$$

Definition 1.35 (False Discovery Rate). **False discovery rate** (FDR) is the rate that shows how often the model is wrong when it predicts positive:

$$FDR = \frac{FP}{TP + FP}$$

It is of course: $PPV + FDR = 1$

Definition 1.36 (Negative Predicted Value). *Negative predicted value (NPV) is the rate that shows how often the model is correct when it predicts negative:*

$$NPV = \frac{TN}{TN + FN}$$

Definition 1.37 (False Omission Rate). *False omission rate (FOR) is the rate that shows how often the model is wrong when it predicts negative:*

$$FOR = \frac{FN}{TN + FN}$$

It is of course: $NPV + FOR = 1$

Definition 1.38 (F_β Score). F_β **score** (FOR) is defined as the harmonic mean of positive predicted value PPV (aka precision) and true positive rate (aka recall) each weighted based on value of β :

$$F_\beta = \frac{(1 + \beta^2) \cdot PPV \cdot TPR}{\beta^2 \cdot PPV + TPR} = \frac{(1 + \beta^2) \cdot \text{precision} \cdot \text{recall}}{\beta^2 \cdot \text{precision} + \text{recall}} = \frac{(1 + \beta^2) \cdot TP}{(1 + \beta^2) \cdot TP + \beta^2 \cdot FN + FP}$$

The coefficient β is chosen such that recall is considered β times as important as precision. The most commonly used value for β is 1, corresponding to the F_1 where precision and recall are weighted equally:

$$F_1 = \frac{2 \cdot PPV \cdot TPR}{PPV + TPR} = \frac{2 \cdot \text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} = \frac{2 \cdot TP}{2 \cdot TP + FN + FP}$$

Two other commonly used values for β are 2 and 0.5, corresponding to the F_2 where weighs recall higher than precision (by placing more emphasis on false negatives) and the $F_{0.5}$ measure, which weighs recall lower than precision (by attenuating the influence of false negatives).

Definition 1.39 (Null Error Rate). *Null error rate is the rate that shows how often a model would be wrong if it always predicts the most frequent type of outcome (either positive or negative depending on the dataset).*

Definition 1.40 (Cohen's Kappa). *Cohen's kappa is the rate that shows how much better a model performs compared to a hypothetical model that would pick a category completely randomly.*

1.9 Support Vector Machine

Support vector machine (SVM) is another, more advanced supervised learning algorithm. It applies mainly in classification problems however there is also another model called support vector regression that applies the same ideas in regression problems. Here we will explore only SVM.

To tell the SVM story, we'll need to first talk about margins and the idea of separating data with a large "gap". Next, we'll talk about the optimal margin classifier, which will lead us into a digression on Lagrange duality. We'll also see kernels, which give a way to apply SVM's efficiently in very high dimensional (such as infinite dimensional) feature spaces, and finally, we'll close off the story with the SMO algorithm, which gives an efficient implementation of SVM's.

Consider logistic regression, where the probability $P(y = 1|\mathbf{x}; \mathbf{w})$ is modelled by:

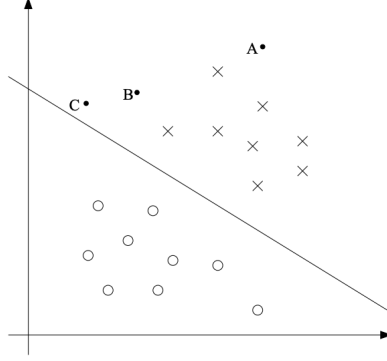
$$h(\mathbf{w}^\top \mathbf{x}) = \frac{1}{1 + \exp(-\mathbf{w}^\top \mathbf{x})}$$

We would then predict 1 on an input \mathbf{x} if and only if $h(\mathbf{w}^\top \mathbf{x}) \geq 0.5$ or equivalently, if and only if $\mathbf{w}^\top \mathbf{x} \geq 0$. Consider a positive training example ($y = 1$). The larger $\mathbf{w}^\top \mathbf{x}$ is, the larger also is $h(\mathbf{w}^\top \mathbf{x})$ a.k.a the larger $P(y = 1|\mathbf{x}; \mathbf{w})$ is, and thus also the higher our degree of confidence that the label is 1. Thus, informally we can think of our prediction as being a very confident one that $y = 1$ if $\mathbf{w}^\top \mathbf{x} \gg 0$.

Similarly, we think of logistic regression as making a very confident prediction of $y = 0$, if $\mathbf{w}^\top \mathbf{x} \ll 0$. Given a training set, again informally it seems that we'd have found a good fit to the training data if we

can find \mathbf{w} so that $\mathbf{w}^\top \mathbf{x}^{(i)} \gg 0$ whenever $y^{(i)} = 1$ and $\mathbf{w}^\top \mathbf{x}^{(i)} \ll 0$ whenever $y^{(i)} = 0$, since this would reflect a very confident (and correct) set of classifications for all the training examples. This seems to be a nice goal to aim for, and we'll soon formalize this idea using the notion of functional margins.

For a different type of intuition, consider the following figure, in which the symbol "X" represent positive training examples, the symbol "O" denote negative training examples, a decision boundary (this is the line given by the equation $\mathbf{w}^\top \mathbf{x} = 0$ is also called the separating hyperplane) is also shown, and three points have also been labelled "A", "B" and "C".



Notice that the point "A" is very far from the decision boundary. If we are asked to make a prediction for the value of y at "A", it seems we should be quite confident that $y = 1$ there. Conversely, the point "C" is very close to the decision boundary, and while it's on the side of the decision boundary on which we would predict $y = 1$, it seems likely that just a small change to the decision boundary could easily have caused our prediction to be $y = 0$. Hence, we're much more confident about our prediction at "A" than at "C". The point "B" lies in-between these two cases, and more broadly, we see that if a point is far from the separating hyperplane, then we may be significantly more confident in our predictions. Again, informally we think it'd be nice if, given a training set, we manage to find a decision boundary that allows us to make all correct and confident (meaning far from the decision boundary) predictions on the training examples. We'll formalize this later using the notion of geometric margins.

To make our discussion of SVM's easier, we'll first need to introduce a new notation for talking about classification. We will be considering a linear classifier for a binary classification problem with labels y and features x . From now, we'll use $y \in \{-1, 1\}$ (instead of $\{0, 1\}$) to denote the class labels. Also, we will separate the w_0 component from \mathbf{w} and from now on we will be denoting it b , and we will write our classifier as:

$$h_{\mathbf{w},b}(\mathbf{x}) = g(\mathbf{w}^\top \mathbf{x} + b)$$

This \mathbf{w}, b notation allows us to explicitly treat the intercept term b separately from the other parameters. (We also drop the convention we had previously of letting $x_0 = 1$ be an extra coordinate in the input feature vector.) Note also that, from our definition of g above, our classifier will directly predict either 1 or -1 without first going through the intermediate step of estimating the probability of y being 1 (which was what logistic regression did).

Definition 1.41 (Functional Margin Of A Training Example). *Given a training example $(\mathbf{x}^{(i)}, y^{(i)})$ we define the **functional margin** of (\mathbf{w}, b) with respect to the training example as:*

$$\hat{\gamma}^{(i)} = y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b)$$

Note that if $y^{(i)} = 1$, then for the functional margin to be large (i.e., for our prediction to be confident and correct), we need $\mathbf{w}^\top \mathbf{x}^{(i)} + b$ to be a large positive number. Conversely, if $y^{(i)} = -1$, then for the functional margin to be large (i.e., for our prediction to be confident and correct), we need $\mathbf{w}^\top \mathbf{x}^{(i)} + b$ to be a large negative number. Moreover, if $\mathbf{w}^\top \mathbf{x}^{(i)} + b \neq 0$, then our prediction on this example is correct. Hence, a large functional margin represents a confident and a correct prediction.

For a linear classifier with the choice of g given above, there's one property of the functional margin that makes it not a very good measure of confidence, however. Given our choice of g , we note that if we replace \mathbf{w} with $2\mathbf{w}$ and b with $2b$, then since $g(\mathbf{w}^\top \mathbf{x} + b) = g(2\mathbf{w}^\top \mathbf{x} + 2b)$ this would not change $h_{\mathbf{w},b}(\mathbf{x})$

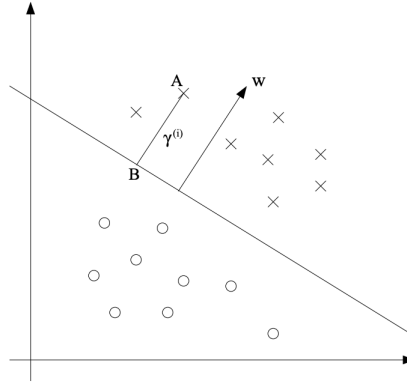
at all meaning that g , and hence also $h_{\mathbf{w},b}(\mathbf{x})$, depends only on the sign, but not on the magnitude, of $\mathbf{w}^\top \mathbf{x} + b$. However, replacing the scaling by a factor also results in multiplying our functional margin by the same factor. Thus, it seems that by exploiting our freedom to scale \mathbf{w} and b , we can make the functional margin arbitrarily large without really changing anything meaningful. Intuitively, it might therefore make sense to impose some sort of normalization condition.

Given a training set we also define the functional margin of (\mathbf{w}, b) with respect to the set as follows.

Definition 1.42 (Functional Margin Of A Set). *Given a training set $\{x^{(i)}, y^{(i)}\}$ we define the **functional margin** of (\mathbf{w}, b) with respect to the training set as:*

$$\hat{\gamma} = \min \hat{\gamma}^{(i)}$$

Next, let's talk about geometric margins. Consider the picture below:



The decision boundary corresponding to (\mathbf{w}, b) is shown, along with the vector \mathbf{w} . Note that \mathbf{w} is orthogonal to the separating hyperplane. Consider the point at A , which represents the input $\mathbf{x}^{(i)}$ label $y^{(i)} = 1$. Its distance to the decision boundary, $\gamma^{(i)}$ is given by the line segment AB .

How can we find the value of $\gamma^{(i)}$? Well, $\frac{\mathbf{w}}{\|\mathbf{w}\|}$ is a unit-length vector pointing in the same direction as \mathbf{w} . Since A represents $\mathbf{x}^{(i)}$ we therefore find that the point B is given by $\mathbf{x}^{(i)} - \gamma^{(i)} \frac{\mathbf{w}}{\|\mathbf{w}\|}$. But this point lies on the decision boundary, and all points on the decision boundary satisfy the equation $\mathbf{w}^\top \mathbf{x} + b = 0$. Hence:

$$\mathbf{w}^\top \left(\mathbf{x}^{(i)} - \gamma^{(i)} \frac{\mathbf{w}}{\|\mathbf{w}\|} \right) + b = 0$$

Solving for $\gamma^{(i)}$ yields:

$$\gamma^{(i)} = \frac{\mathbf{w}^\top \mathbf{x}^{(i)} + b}{\|\mathbf{w}\|} = \left(\frac{\mathbf{w}}{\|\mathbf{w}\|} \right)^\top \mathbf{x}^{(i)} + \frac{b}{\|\mathbf{w}\|}$$

This was worked out for the case of a positive training example at A in the figure, where being on the positive side of the decision boundary is good.

We are now ready to properly define the geometrical margin.

Definition 1.43 (Geometrical Margin Of A Training Example). *Given a training example $(x^{(i)}, y^{(i)})$ we define the **geometrical margin** of (\mathbf{w}, b) with respect to the training example as:*

$$\gamma^{(i)} = y^{(i)} \left(\left(\frac{\mathbf{w}}{\|\mathbf{w}\|} \right)^\top \mathbf{x}^{(i)} + \frac{b}{\|\mathbf{w}\|} \right)$$

Note that if $\|\mathbf{w}\| = 1$, then the functional margin equals the geometric margin. This thus gives us a way of relating these two different notions of margin. Also, the geometric margin is invariant to rescaling of the parameters. This will in fact come in handy later. Specifically, because of this invariance to the scaling of the parameters, when trying to fit \mathbf{w} and b to training data, we can impose an arbitrary scaling constraint on \mathbf{w} without changing anything important.

Finally, given a training set we also define the geometric margin of (\mathbf{w}, b) with respect to the set to be the smallest of the geometric margins on the individual training examples:

Definition 1.44 (Geometrical Margin Of A Set). *Given a training set $\{x^{(i)}, y^{(i)}\}$ we define the **geometrical margin** of (\mathbf{w}, b) with respect to the training set as:*

$$\gamma = \min \gamma^{(i)}$$

Given a training set, it seems from our previous discussion that a natural desideratum is to try to find a decision boundary that maximizes the (geometric) margin, since this would reflect a very confident set of predictions on the training set and a good “fit” to the training data. Specifically, this will result in a classifier that separates the positive and the negative training examples with a “gap” (geometric margin).

For now, we will assume that we are given a training set that is linearly separable, i.e that it is possible to separate the positive and negative examples using some separating hyperplane. How we we find the one that achieves the maximum geometric margin? We can pose the following optimization problem:

$$\max_{\gamma, \mathbf{w}, b} \gamma$$

subject to:

$$y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b) \geq \gamma, \quad i = 1, 2, \dots, m \quad \text{and} \quad \|\mathbf{w}\| = 1$$

In other words, we want to maximize γ , subject to each training example having functional margin at least γ . The $\|\mathbf{w}\| = 1$ constraint moreover ensures that the functional margin equals to the geometric margin, so we are also guaranteed that all the geometric margins are at least γ . Thus, solving this problem will result in parameters with the largest possible geometric margin with respect to the training set.

If we could solve the optimization problem above, we’d be done. But the $\|\mathbf{w}\| = 1$ constraint is a nasty (non-convex) one, and this problem certainly isn’t in any format that we can plug into standard optimization software to solve. So, lets try transforming the problem into a nicer one. Consider:

$$\max_{\gamma, \mathbf{w}, b} \frac{\hat{\gamma}}{\|\mathbf{w}\|}$$

subject to:

$$y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b) \geq \hat{\gamma}, \quad i = 1, 2, \dots, m$$

Here, we’re going to maximize $\frac{\hat{\gamma}}{\|\mathbf{w}\|}$ subject to the functional margins all being at least $\hat{\gamma}$. Since the geometric and functional margins are related by $\gamma = \frac{\hat{\gamma}}{\|\mathbf{w}\|}$ this will give us the answer we want. Moreover, we’ve gotten rid of the constraint $\|\mathbf{w}\| = 1$ that we didn’t like. The downside is that we now have a nasty (again, non-convex) objective $\frac{\hat{\gamma}}{\|\mathbf{w}\|}$ function, and, we still don’t have any off-the-shelf software that can solve this form of an optimization problem.

Lets keep going. Recall our earlier discussion that we can add an arbitrary scaling constraint on \mathbf{w} and b without changing anything. This is the key idea we’ll use now. We will introduce the scaling constraint that the functional margin of \mathbf{w} and b with respect to the training set must be 1:

$$\hat{\gamma} = 1$$

Since multiplying \mathbf{w} and b by some constant results in the functional margin being multiplied by that same constant, this is indeed a scaling constraint, and can be satisfied by rescaling \mathbf{w} and b . Plugging this into our problem above, and noting that maximizing $\frac{\hat{\gamma}}{\|\mathbf{w}\|} = \frac{1}{\|\mathbf{w}\|}$ is the same thing as minimizing $\|\mathbf{w}\|^2$, we now have the following optimization problem:

$$\min_{\gamma, \mathbf{w}, b} \frac{1}{2} \|\mathbf{w}\|^2$$

subject to:

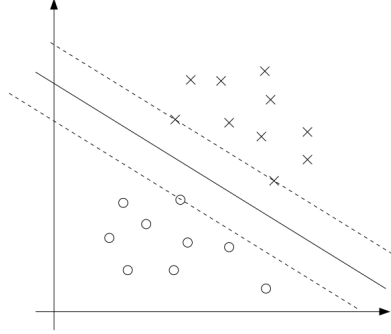
$$y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b) \geq 1, \quad i = 1, 2, \dots, m$$

We can rewrite the constraints as:

$$g_i(\mathbf{w}) = -y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b) + 1 \leq 0, \quad i = 1, 2, \dots, m$$

According to (Appendix A) we are dealing with an inequality constrained optimization problem (with no equality part) so we will use the KKT multipliers in order to solve it.

Notice that that all KKT conditions are satisfied, since we do not have any equality constraints (hence $\mu_i = 0, \forall i$), and we have $\lambda_i > 0$ only for the training examples that have functional margin exactly equal to one, i.e the ones corresponding to constraints that hold with equality $g_i(\mathbf{w}) = 0$. Consider the figure below, in which a maximum margin separating hyperplane is shown by the solid line.



The points with the smallest margins are exactly the ones closest to the decision boundary. Here these are the three points: one negative and two positive examples, that lie on the dashed lines parallel to the decision boundary. Thus, only three of the λ_i (the ones corresponding to these three training examples) will be non-zero at the optimal solution to our optimization problem. These three points are called “support vectors”. The fact that the number of support vectors can be much smaller than the size the training set will be useful later.

Moving on by applying what we developed in (Appendix A) the Lagrangian of the inequality constrained optimization problem reads:

$$\mathcal{L}(\mathbf{w}, b, \lambda_i) = \frac{1}{2} \|\mathbf{w}\|^2 - \sum_i \lambda_i \left(y^{(i)}(\mathbf{w}^\top \mathbf{x}^{(i)} + b) - 1 \right)$$

Note that there are only λ_i but no μ_i Lagrange multipliers, since the problem has only inequality constraints.

Now we move on trying to solve this optimization problem. Once again, according to (Appendix A) the necessary conditions for optimization of \mathcal{L} turn to:

$$\nabla_{\mathbf{w}} \mathcal{L}(\mathbf{w}, b, \lambda_i) = 0 \quad \text{and} \quad \frac{\partial \mathcal{L}(\mathbf{w}, b, \lambda_i)}{\partial b} = 0 \quad \text{and} \quad \frac{\partial \mathcal{L}(\mathbf{w}, b, \lambda_i)}{\partial \lambda_i} = 0$$

Starting with the first one, quite straightforward we obtain:

$$\nabla_{\mathbf{w}} \mathcal{L}(\mathbf{w}, b, \lambda_i) = \mathbf{w} - \sum_i \lambda_i y^{(i)} \mathbf{x}^{(i)} = 0$$

which implies:

$$\mathbf{w} = \sum_i \lambda_i y^{(i)} \mathbf{x}^{(i)}$$

As for the derivative with respect to b , we obtain:

$$\frac{\partial \mathcal{L}(\mathbf{w}, b, \lambda_i)}{\partial b} = \sum_i \lambda_i y^{(i)} = 0$$

By manipulating the initial Lagrangian and by substituting the results from the two first derivatives we end up to:

$$\begin{aligned} \mathcal{L}(\mathbf{w}, b, \lambda_i) &= \frac{1}{2} \|\mathbf{w}\|^2 - \sum_i \lambda_i \left(y^{(i)} (\mathbf{w}^\top \mathbf{x}^{(i)} + b) - 1 \right) \\ &= \frac{1}{2} \|\mathbf{w}\|^2 - \sum_i \lambda_i y^{(i)} \mathbf{w}^\top \mathbf{x}^{(i)} - b \sum_i \lambda_i y^{(i)} + \sum_i \lambda_i \\ &= \frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} - \sum_i \lambda_i y^{(i)} \left(\sum_j \lambda_j y^{(j)} \left(\mathbf{x}^{(j)} \right)^\top \right) \mathbf{x}^{(i)} + \sum_i \lambda_i \\ &= \frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} - \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} + \sum_i \lambda_i \\ &= \sum_i \lambda_i - \frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} \end{aligned}$$

Hence now the Lagrangian reads:

$$\mathcal{L}(\lambda_i) = \sum_i \lambda_i - \frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)}$$

where the dependencies on the parameters \mathbf{w} and b are gone and the Lagrangian is just a function of the KKT multipliers. So we ended up with the so called “dual optimization problem” which is:

$$\max_{\lambda_i} \left(\sum_i \lambda_i - \frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} \right)$$

subject to:

$$\lambda_i \geq 0, \quad i = 1, 2, \dots, m \quad \text{and} \quad \sum_i \lambda_i y^{(i)} = 0$$

where as per usual we can turn the maximization to minimization by multiplying the Lagrangian with a minus sign so we end up with:

$$\min_{\lambda_i} \left(\frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} \left(\mathbf{x}^{(i)} \right)^\top \mathbf{x}^{(j)} - \sum_i \lambda_i \right)$$

subject to:

$$\lambda_i \geq 0, \quad i = 1, 2, \dots, m \quad \text{and} \quad \sum_i \lambda_i y^{(i)} = 0$$

As usual we can rewrite everything in form of matrices. By introducing the matrix Q and the KKT multipliers vector $\boldsymbol{\lambda}$:

$$Q = \begin{bmatrix} y^{(1)} y^{(1)} \left(\mathbf{x}^{(1)} \right)^\top \mathbf{x}^{(1)} & \dots & y^{(1)} y^{(m)} \left(\mathbf{x}^{(1)} \right)^\top \mathbf{x}^{(m)} \\ y^{(2)} y^{(2)} \left(\mathbf{x}^{(2)} \right)^\top \mathbf{x}^{(2)} & \dots & y^{(2)} y^{(m)} \left(\mathbf{x}^{(2)} \right)^\top \mathbf{x}^{(m)} \\ \vdots & \vdots & \ddots \\ y^{(m)} y^{(1)} \left(\mathbf{x}^{(m)} \right)^\top \mathbf{x}^{(1)} & \dots & y^{(m)} y^{(m)} \left(\mathbf{x}^{(m)} \right)^\top \mathbf{x}^{(m)} \end{bmatrix}, \quad \boldsymbol{\lambda} = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix}$$

we can rewrite the dual optimization problem as:

$$\max_{\boldsymbol{\lambda}} \left(\frac{1}{2} \boldsymbol{\lambda}^T Q \boldsymbol{\lambda} - \boldsymbol{\lambda} \right)$$

subject to:

$$\boldsymbol{\lambda} \geq 0 \quad \text{and} \quad \mathbf{y}^T \boldsymbol{\lambda} = 0$$

This final dual optimization problem is usually solved numerically through quadratic programming (as for example we use gradient descent for loss functions optimization problems). Once we solve it we obtain the KKT multipliers vector $\boldsymbol{\lambda}$ and subsequently all the individual KKT multipliers λ_i from its components. We also notice that almost all λ_i 's are 0 except from a few ones where $\lambda_i > 0$ coming from the support vectors. By making use of the KKT multipliers we find the parameter \mathbf{w} as:

$$\mathbf{w} = \sum_i \lambda_i y^{(i)} \mathbf{x}^{(i)}$$

We once again notice that the only terms that survive are the ones with $\lambda_i > 0$ coming from the support vectors. All the other points do not contribute at all to the model.

Once we have \mathbf{w} we can compute b from the fact that for support vectors their distance from the plane is equal to 1, i.e:

$$y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) = 1$$

hence:

$$b = \frac{1}{y^{(i)}} - \mathbf{w}^T \mathbf{x}^{(i)}$$

for any i that is a support vector. This last equation should produce the same parameter b for all support vectors. This is a good way to check that the models works fine.

By having found both \mathbf{w} and b , we have found the separator $\mathbf{w}^T \mathbf{x} + b$ and we are in the position to predict to which class a new point belongs. Since $\mathbf{w}^T \mathbf{x} + b$ is going to be either negative (if the point lies below the plane) or positive (if the point lies above the plane) we finally have for the prediction:

$$h(\mathbf{x}) = \text{sign}(\mathbf{w}^T \mathbf{x} + b)$$

This model of classification is called “hard margin support vector machine”.

Everything we have said so far assumed that the data is linearly separable. However the generalization of SVM to non-linear separable is easy. Without getting into details two of the ways we can achieve this are the following.

- **Non-Linear Transformations & Kernels:** By switching from a space X where the data are not linear separable to a space Z where the data are linear separable through a transformation Φ :

$$(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n) \xrightarrow{\Phi} (\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_n)$$

Accordingly the dual optimization problem would change to:

$$\min_{\lambda_i} \left(\frac{1}{2} \sum_i \sum_j \lambda_i \lambda_j y^{(i)} y^{(j)} (\mathbf{z}^{(i)})^T \mathbf{z}^{(j)} - \sum_i \lambda_i \right)$$

subject to:

$$\lambda_i \geq 0, \quad i = 1, 2, \dots, m \quad \text{and} \quad \sum_i \lambda_i y^{(i)} = 0$$

and then we would follow the same procedure as before in order to obtain a solution.

The biggest caveat of this method is the inner product $(\mathbf{z}^{(i)})^T \mathbf{z}^{(j)}$ that needs to be computed in Z space and it's computationally expensive. One way to overcome this problem is by using the trick

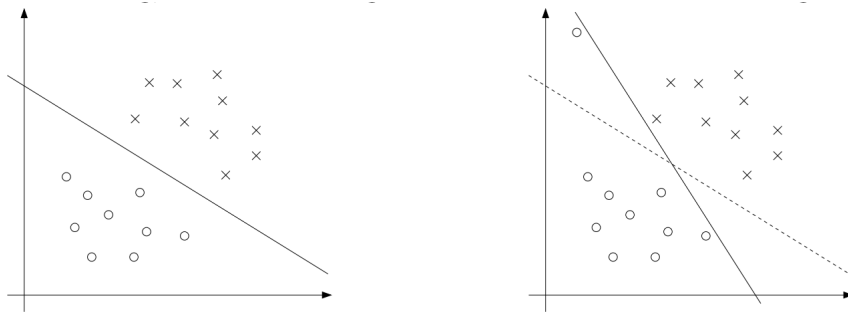
of kernels ((Appendix B) in which we substitute the inner product with a kernel:

$$\left(\mathbf{z}^{(i)}\right)^{\top} \mathbf{z}^{(j)} = K(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$$

Given the freedom of choosing a kernel the model turns quite flexible.

- **L1 Regularization & Soft Margin SVM:** While mapping data to a high dimensional feature space via Φ does generally increase the likelihood that the data is separable, we can't guarantee that it always will be so. Also, in some cases it is not clear that finding a separating hyperplane is exactly what we'd want to do, since that might be susceptible to outliers.

To make the algorithm work for non-linearly separable datasets as well as be less sensitive to outliers, we can simply impose the technique of L1 Regularization that we mentioned in the previous chapter. That way our model is more open to errors and it allows some wrongly labeled data.



In this case the final model is called “soft margin support vector machine” (in contrast with the SVM we developed in the beginning called “hard margin support vector machine”), due to the fact that it allows the margin to be violated by outliers.

1.10 Extra: Applied Machine Learning

In this section we will cover the applied side of machine learning.

This checklist can guide you through your Machine Learning projects. There are eight main steps:

1. Frame the problem and look at the big picture:

- Define the objective in business terms.
- How will your solution be used?
- What are the current solutions/workarounds (if any)?
- How should you frame this problem (supervised/unsupervised, online/offline, etc)?
- How should performance be measured?
- Is the performance measure aligned with the business objective?
- What would be the minimum performance needed to reach the business objective?
- What are comparable problems? Can you reuse experience or tools?
- Is human expertise available?
- How would you solve the problem manually?
- List the assumptions you (or others) have made so far.
- Verify assumptions if possible.

2. Get the data:

- List the data you need and how much you need.
- Find and document where you can get that data.

- Check how much space it will take.
- Check legal obligations, and get authorization if necessary.
- Get access authorizations.
- Create a workspace (with enough storage space).
- Get the data.
- Convert the data to a format you can easily manipulate (without changing the data itself).
- Ensure sensitive information is deleted or protected (e.g. anonymized).
- Check the size and type of data (time series, sample, geographical, etc).
- Sample a test set, put it aside, and never look at it.
- Automate as much as possible so you can easily get fresh data.

3. Explore the data:

- Make sure you data are not insufficient, of poor quality, or non representative.
- Create a copy of the data for exploration (sampling it down to a manageable size if necessary).
- Create a Jupyter notebook to keep a record of your data exploration.
- Study each attribute and its characteristics:
 - Name.
 - Type (categorical, int/float, bounded/unbounded, text, structured, etc).
 - Percentage of missing values.
 - Noisiness and type of noise (stochastic, outliers, rounding errors, etc).
 - Usefulness for the task,
 - Type of distribution (Gaussian, uniform, logarithmic, etc).
- For supervised learning tasks, identify the target attribute(s).
- Visualize the data.
- Study the correlations between attributes.
- Study how you would solve the problem manually.
- Identify the promising transformations you may want to apply.
- Identify extra data that would be useful.
- Document what you have learned.
- Try to get insights from a field expert for these steps.

4. Prepare the data:

- Work on copies of the data (keep the original dataset intact).
- Write functions for all data transformations you apply, for the following reasons:
 - So you can easily prepare the data the next time you get a fresh dataset.
 - So you can apply these transformations in future projects.
 - To clean and prepare the test set.
 - To clean and prepare new data instances once your solution is live.
 - To make it easy to treat your preparation choices as hyperparameters.
- Clean the data:
 - Fix or remove outliers.
 - Fill in missing values (e.g., with zero, mean, median,etc) or drop their rows (or columns).
- Feature selection/engineering:
 - Drop the attributes that provide no useful information for the task.
 - Drop variables that have a very high percentage of missing values.
 - Drop variables that have a very low variation (i.e not too much information).
 - Drop variables that have very low correlation with the target.

- Find variables that are highly correlated with each other (i.e same behaviour), and keep the ones that have higher correlation with the target (drop the other ones).
- Use Principal Component Analysis if you don't care about physical meaning of variables and to eliminate multicollinearity issues.
- Select best features based on a metric (eg model accuracy). Either start with one variable and add more (forward selection), or start with all variables and eliminate (backward elimination or recursive feature elimination).
- Discretize continuous features.
- Decompose features (e.g categorical, date/time, etc).
- Add promising transformations of features.
- Aggregate features into promising new features.
- Feature scaling: Standardize or normalize features.

5. Shortlist promising models:

- If the data is huge, you may want to sample smaller training sets so you can train many different models in a reasonable time (be aware that this penalizes complex models such as large neural nets or Random Forests).
- Once again, try to automate these steps as much as possible.
- Train many quick-and-dirty models from different categories using standard parameters.
- Measure and compare their performance.
- For each model, use K-fold cross-validation and compute the mean and standard deviation of the performance measure on the K folds.
- Analyze the most significant variables for each algorithm.
- Analyze the types of errors the models make. What data would a human have used to avoid these errors?
- Shortlist the top three to five most promising models, preferring models that make different types of errors.

6. Fine-Tune the system:

- You will want to use as much data as possible for this step, especially as you move toward the end of fine-tuning.
- As always, automate what you can.
- Fine-tune the hyperparameters using cross-validation:
- Try ensemble methods. Combining your best models will often produce better performance than running them individually.
- Once you are confident about your final model, measure its performance on the test set to estimate the generalization error.
- Don't tweak your model after measuring the generalization error: you would just start overfitting the test set.

7. Present your solution:

- Document what you have done.
- Create a nice presentation.
- Make sure you highlight the big picture first.
- Explain why your solution achieves the business objective.
- Don't forget to present interesting points you noticed along the way.
- Describe what worked and what did not.
- List your assumptions and your system's limitations.
- Ensure your key findings are communicated through beautiful visualizations or easy-to-remember statements.

8. **Launch:**

- Get your solution ready for production.
- Write monitoring code to check your system's live performance at regular intervals and trigger alerts when it drops.
- Beware of slow degradation: models tend to “rot” as data evolves.
- Measuring performance may require a human pipeline.
- Also monitor your inputs' quality.
- Retrain your models on a regular basis on fresh data (automate as much as possible).

Appendices

Appendix A

Constrained Optimization

Constrained optimization is the problem of finding a minimum (or maximum) of a function $f(x)$ called the “objective function”, subject to a number of constraints of the following types:

- $h_i(x) = 0$, $i = 1, 2, \dots$ called “equality constraints”
- $g_i(x) \leq 0$, $i = 1, 2, \dots$ called “inequality constraints”

Let’s start first with the equality constraints and then we will add inequality constraints.

A.1 Equality Constrained Optimization

The formulation of the optimization problem is to optimize $f(x)$ subject to $h_i(x) = 0$, $i = 1, 2, \dots$. Let’s assume for simplicity only one constraint $h_1(x) = h(x) = 0$. The idea here is that the point that $f(x)$ touches $h(x)$ is the point that $f(x)$ is minimum (or maximum) while the constraint is also valid. At that point $f(x)$ is parallel to $h(x)$ and the tangents $\nabla_{\mathbf{w}}f(x)$ and $\nabla_{\mathbf{w}}h(x)$ which are perpendicular to $f(x)$ and $h(x)$ respectively, are also parallel to each other. Hence, since $\nabla_{\mathbf{w}}f(x)$ and $\nabla_{\mathbf{w}}h(x)$ are parallel this translates to:

$$\nabla_{\mathbf{w}}f(x) = \mu \nabla_{\mathbf{w}}h(x)$$

which is the condition for the $f(x)$ to be minimum (or maximum) while $h(x) = 0$.

Without loss of generality the condition for many constraints reads:

$$\nabla_{\mathbf{w}}f(x) = \sum_i \mu_i \nabla_{\mathbf{w}}h_i(x)$$

or by bringing everything in one side:

$$\nabla_{\mathbf{w}}f(x) - \sum_i \mu_i \nabla_{\mathbf{w}}h_i(x) = 0$$

$$\nabla_{\mathbf{w}}(f(x) - \sum_i \mu_i h_i(x)) = 0$$

At this point we define the “Lagrangian” as follows:

$$\mathcal{L}(x, \mu_i) = f(x) + \sum_i \mu_i h_i(x)$$

where μ_i are called “Lagrange multipliers”. Subsequently the necessary conditions for optimization of \mathcal{L} turns to:

$$\nabla_{\mathbf{w}}\mathcal{L} = 0 \quad \text{and} \quad \frac{\partial \mathcal{L}}{\partial \mu_i} = 0$$

The solution of this system of equations minimizes (or maximizes) $f(x)$ subject to $h_i(x) = 0$, $\forall i$.

A.2 Equality & Inequality Constrained Optimization

Now on top of equality constraints we also have inequality constraints. The formulation of the optimization problem is to optimize $f(x)$ subject to $h_i(x) = 0$, $i = 1, 2, \dots$ and $g_i(x) \leq 0$, $i = 1, 2, \dots$. Following a similar way of thinking as before, although a bit more technical, we can show (but we won't) that if the following four conditions, called "Karush - Kuhn - Taler conditions" (KKT), hold:

- $h_i(x) = 0$, $\forall i$
- $g_i(x) \leq 0$, $\forall i$
- $\lambda_i \leq 0$, $\forall i$
- $\lambda_i g_i(x) = 0$, $\forall i$

then there exist constants μ_i and λ_i called "KKT multipliers" such that:

$$\nabla_{\mathbf{w}} f(x) = \sum_i \mu_i \nabla_{\mathbf{w}} h_i(x) + \sum_i \lambda_i \nabla_{\mathbf{w}} g_i(x)$$

By following the same philosophy as for the equality constrained optimization we define the "Lagrangian" as follows:

$$\mathcal{L}(x, \mu_i, \lambda_i) = f(x) + \sum_i \mu_i h_i(x) + \sum_i \lambda_i g_i(x)$$

and the necessary conditions for optimization of \mathcal{L} turn to:

$$\nabla_{\mathbf{w}} \mathcal{L} = 0 \quad \text{and} \quad \frac{\partial \mathcal{L}}{\partial \mu_i} = 0 \quad \text{and} \quad \frac{\partial \mathcal{L}}{\partial \lambda_i} = 0$$

This final form of the optimization problem is usually called the "dual optimization problem".

This is the most general case of constrained optimization. If there are no equality constraints $h_i(x)$ then we simply have a theory for inequality constrained optimization. If there are no inequality constraints $g_i(x)$ then the whole theory turns to the equality constrained optimization problem we developed previously and the KKT multipliers turn to Lagrangian multipliers. Finally, if there are no equality constraints $h_i(x)$ neither inequality constraints $g_i(x)$ the theory is just a usual optimization problem where we just find the solution where the derivative of $f(x)$ is zero.

Appendix B

Kernels

Definition B.1 (Kernel). *Let \bar{x} and \bar{x}' be two vectors of space X and Φ a non-linear transformation. We define \bar{z} and \bar{z}' as the transformed vectors $\Phi(\bar{x})$ and $\Phi(\bar{x}')$:*

$$\bar{x} \in X \xrightarrow{\Phi} \bar{z} = \Phi(\bar{x}) \in Z$$

$$\bar{x}' \in X \xrightarrow{\Phi} \bar{z}' = \Phi(\bar{x}') \in Z$$

We define the **kernel** of space Z as the function that is equal to the inner product of the transformation vectors:

$$K(\bar{x}, \bar{x}') = \bar{z}^T \bar{z}'$$

Let's for example assume the following non-linear transformation:

$$\bar{x} = (x_1, x_2) \xrightarrow{\Phi} \bar{z} = \Phi(\bar{x}) = (1, x_1^2, x_2^2, \sqrt{2}x_1, \sqrt{2}x_2, \sqrt{2}x_1x_2)$$

$$\bar{x}' = (x'_1, x'_2) \xrightarrow{\Phi} \bar{z}' = \Phi(\bar{x}') = (1, x_1'^2, x_2'^2, \sqrt{2}x'_1, \sqrt{2}x'_2, \sqrt{2}x'_1x'_2)$$

Then for the inner product:

$$\bar{z}^T \bar{z}' = 1 + x_1^2 x_1'^2 + x_2^2 x_2'^2 + 2x_1 x_1' + 2x_2 x_2' + 2x_1 x_2 x_1' x_2'$$

However we can get to the same result by simply defining a Kernel of the form:

$$\begin{aligned} K(\bar{x}, \bar{x}') &= (1 + \bar{x}\bar{x}')^2 \\ &= (1 + x_1 x_1' + x_2 x_2')^2 \\ &= 1 + x_1^2 x_1'^2 + x_2^2 x_2'^2 + 2x_1 x_1' + 2x_2 x_2' + 2x_1 x_2 x_1' x_2' \end{aligned}$$

Hence by knowing the Kernel of a space Z of some non-linear transformation Φ we can compute inner products without the need of transforming vectors from X to Z .

The kernel trick is to use this idea in the opposite direction. Namely, to assume that a function $K(\bar{x}, \bar{x}')$ is the kernel of some space Z for some non-linear transformation Φ and to compute inner products without even knowing the transformation.

The question that arises is how do we know that some function $K(\bar{x}, \bar{x}')$ is actually the kernel of a space Z . There are three approaches to this problem:

1. By construction (as we did in the example above).
2. By Mercer's condition that states that $K(\bar{x}, \bar{x}')$ is a valid kernel for some space Z if

$$\int K(\bar{x}, \bar{x}') g(\bar{x}) g(\bar{x}') d\bar{x} d\bar{x}' \geq 0 \quad \forall \text{ square integrable functions } g(\bar{x})$$

3. Sometimes we don't care if $K(\bar{x}, \bar{x}')$ is a valid kernel for some space Z as long as it does the job.

Appendix C

Convolution

Definition C.1 (Convolution). *Convolution is a mathematical operation on two functions f and g that produces a third function expressing how the shape of one is modified by the other. The term convolution refers to both the result function and to the process of computing it. It is defined as the integral of the product of the two functions after one is reversed and shifted.*

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t - \tau)d\tau$$