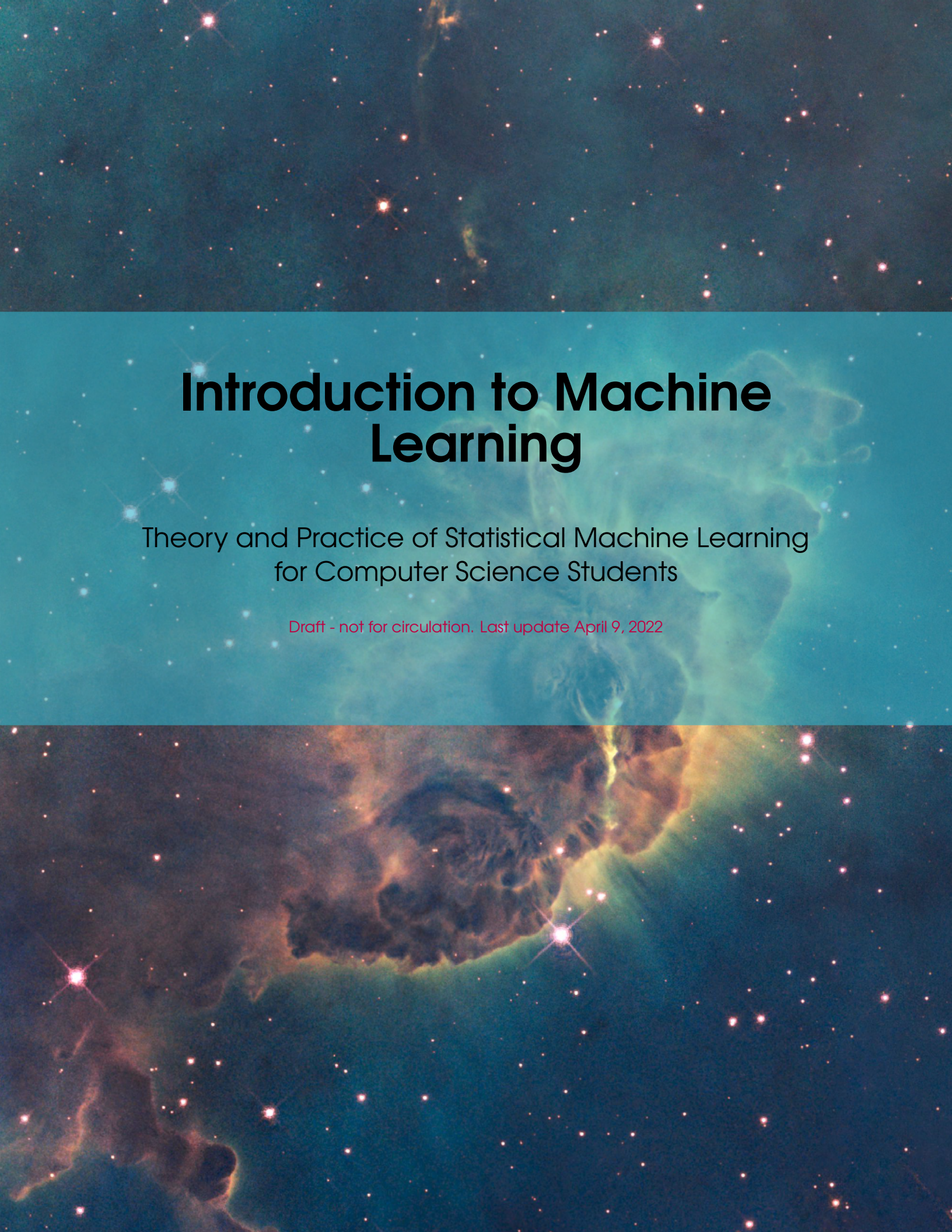


Introduction to Machine Learning

Theory and Practice of Statistical Machine Learning
for Computer Science Students

Draft - not for circulation. Last update April 9, 2022

INTRODUCTION TO MACHINE LEARNING

Matan Gavish and Gilad Green

Contents

1. Estimation Theory

"All models are wrong, but some are useful" — George E.P. Box, in *Science and Statistics*, 1976

In the study and practice of machine learning we try and define models in attempt to explain different observed phenomena, and into which we pour our understanding of the problem. These models, sometimes incorporating a probabilistic aspect, often depend on unknown parameters, whose values are to be inferred from given data.

Suppose for example we would like to know the current time. We do not have a means of telling the time ourselves, and so we ask people around us. We asked an individual and were told that the time is 13:15. Since people tend to approximate the time, it is possible that the true time is not 13:15 as told but rather 13:13. To get a better accurate assessment of the true time we decide to ask multiple individuals and record their answers. We organize the answers as *observations* denoted by $x_1,\ldots,x_m$, for m the number of individuals asked. Intuitively, we can now *estimate/approximate* the true time by averaging over the observations $\frac{1}{m}\sum x_i$.

It is helpful to consider the observations $x_1,\ldots,x_m$ as the *realization* of the *random variables* $X_1,\ldots,X_m$. These are called a *repeated sample* or simply a *sample*. By doing so, we emphasis the probabilistic nature of the problem and can devise a simplified probabilistic model for it. This model, will capture the essence of the problem by incorporating our prior knowledge and assumptions on the manner in which the observations behave (i.e. the underlying probability distribution).

Given a sample $x_1,\ldots,x_m$ for which we assume some underlying probability distribution $\mathcal{P}$ we say that $x_1,\ldots,x_m$ are *identically distributed* if they are all the realizations of random variables over the same probability distribution function, i.e. $X_1,\ldots,X_m \sim \mathcal{P}$. We further say that $x_1,\ldots,x_m$ are independent identically distributed (i.i.d) if they are all the realizations of random variables which are independent random variables and identically distributed. We denote this as $X_1,\ldots,X_m \overset{i.i.d}{\sim} \mathcal{P}$ for $X_1 = x_1,\ldots,X_m = x_m$ the realizations of $X_1,\ldots,X_m$. To simplify notation we often write $x_1,\ldots,x_m \overset{i.i.d}{\sim} \mathcal{P}$ (even though $x_1,\ldots,x_m$ are not random variables) in the sense that the corresponding random variables are i.i.d.

Probability versus Statistics

Throughout this chapter, and the rest of this book, we will be using concepts from both probability theory and from statistics. Though both are related fields of mathematics dealing with analyzing the chances of events happening, there are some key fundamental differences in the manner in which they address the matter.

The field of probability is first and foremost a theoretical study, asking the outcome of mathematical definitions. It deals with *predicting* how likely are events to occur in a given setup. Statistics on the other hand, is primarily an applied study, that attempts to explain observed phenomena in the real world. It involves the *analysis of past* events.

In the context of the time estimation problem above

- If we are to think as a probabilist, we would notice the answers take a wide continuous range of values. We would then *assume* they follow some distribution, say Gaussian, and ask what is the probability of predicting a specific time.
- If we are to think as a statistician, though noticing the answers take a wide continuous range of values, we would be concerned with the question of "how do we assure these observations follow a Gaussian distribution?". We would then use these past observations to decide if they are indeed consistent with the Gaussian distribution assumption.

We will use both fields to tackle the different learning problems we will face.

1.1 Estimation of Distribution Parameters

Often the underlying probability distribution $\mathcal{P}$ is characterized by some set of parameters $\boldsymbol{\theta} \in \Theta$. $\boldsymbol{\theta}$ denotes a vector of parameters and Θ the set with all possible values for the paramerers. For example, a Poisson distribution $Poisson(\lambda)$ is characterized by the parameter λ, so $\boldsymbol{\theta} := \{\lambda\}$ and $\Theta := \mathbb{N}_0$. In the case of a Normal distribution $\mathcal{N}(\mu, \sigma^2)$, it is characterized by μ, σ^2, so $\boldsymbol{\theta} := \{\mu, \sigma^2\}$ and $\Theta := \mathbb{R} \times \mathbb{R}_+$.

In the case of (parametric) estimation theory, we assume some underlying probability distribution $\mathcal{P}(\boldsymbol{\theta})$ characterized by the parameters $\boldsymbol{\theta}$. Then, given a sample $x_1, \ldots, x_m$, drawn according to $\mathcal{P}(\boldsymbol{\theta})$ and for which we *do not* know the true value of $\boldsymbol{\theta}$, we wish to choose $\boldsymbol{\theta}^*$ "best" expressing the true value of $\boldsymbol{\theta}$. We formulate this problem by defining a decision function (or decision rule) $\delta_m : \mathbb{F}^m \to \Theta$ mapping the observations to the parameter space. For simplicity we shall omit the index and write $\delta(x_1, \ldots, x_m)$. Since we can devise many different decision functions, the problem of choosing $\boldsymbol{\theta}^* \in \Theta$ becomes a problem of choosing the *optimal* decision function δ from the set Δ:

$$\Delta := \{\delta(x_1, \ldots, x_m) : \mathbb{F}^m \to \Theta\} \tag{1.1}$$

where the notion of what does an optimal decision function means will be covered later. In the context of machine learning we refer to this set Δ by the term *hypothesis class* and each function in it as an *hypothesis*.

Definition 1.1.1 Let $\delta \in \Delta$ be a decision function. Then $\delta(X_1, \ldots, X_m)$ is called a point statistical estimator of a parameter $\boldsymbol{\theta}$, or simply an estimator.

Let us return to the example above of determining the current time. Given the answers of m different individuals $x_1, \ldots, x_m$ we stated that we could simply average the answers and approximate the true time as $\frac{1}{m}\sum x_i$. In fact, the function $f : \mathbb{R}^m \to \mathbb{R}$ defined by $f(x_1, \ldots, x_m) = \frac{1}{m}\sum x_i$ *is* a decision rule, and when using it over the random variables $X_1, \ldots, X_m$ (whose realizations are $x_1, \ldots, x_m$) we in fact defined an estimator.

1.1.1 Estimation of Univariate Gaussian Parameter

Recall the probability density function of the normal distribution.

Definition 1.1.2 — (Univariate) Normal Distribution. A random variable x has a ***normal distribution*** with expectation μ and variance σ^2 if it has a PDF of the form:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp^{-\frac{1}{2\sigma^2}(x-\mu)^2}$$

In this case we write: $x \sim \mathcal{N}(\mu, \sigma^2)$

Consider the problem of estimating the expected value μ and variance σ^2 for a given sample drawn, i.i.d from a normal distribution characterized by μ, σ^2: $x_1, \ldots, x_m \overset{i.i.d}{\sim} \mathcal{N}\left(\mu, \sigma^2\right)$. To do so we should define decision rules that take the m observations and output an estimation of the expected value and variance. We define the estimators:

- ***Sample mean***: an estimator for the population mean

$$\hat{\mu}_X := \frac{1}{m}\sum_{i=1}^{m} x_i \tag{1.2}$$

- ***Sample variance***: an estimator for the population variance

$$\hat{\sigma}_X^2 := \frac{1}{m-1}\sum_{i=1}^{m}(x_i - \hat{\mu}_X)^2 \tag{1.3}$$

where the $\hat{}$ (hat) notation expressed that $\hat{\mu}_X, \hat{\sigma}_X^2$ are estimators of the true parameters μ, σ^2. Whenever context is clear, we will omit the subscript X.

R Note that the sample variance is somewhat different from the variance of the x_i's where we divide by $m-1$ rather than by m. The factor by which we divide (m or $m-1$) is determined by what is known as the number of *degrees of freedom*. Though beyond the scope of this book, an estimator's number of degrees of freedom is the number of independent observations used for estimation minus the number of parameters used for the estimation. In the case of the sample variance estimator (1.3) we provide m samples but use one parameter (being the estimator of the sample mean). Thus, we divide by $m-1$. The difference between the two options will be discussed shortly under bias of estimators (Definition 1.1.6).

1.1.2 Properties of Estimators

From the definition of the sample variance (1.3) we understand that we have a great deal of freedom when designing different estimators. Indeed, we might also consider the following functions are estimators of the sample variance:

$$\hat{\sigma} := \frac{1}{m}\sum(x_i - \hat{\mu}), \quad \hat{\sigma} := \frac{1}{m}\sum|x_i - \hat{\mu}|, \quad \hat{\sigma} := \frac{1}{m-1}\sum|x_i - \hat{\mu}|$$

Therefore, the question is how to choose the "right"/"best" estimator, what does it actually mean to be the "right"/"best" estimator, and does this decision depend on the given problem? Consider for example the following scenario. Suppose $x_1, \ldots, x_m \overset{i.i.d}{\sim} \mathcal{N}(\mu, 1)$ and the two following estimators for the expectation:

$$\hat{\mu}_1(x_1, \ldots, x_m) = \tfrac{1}{m}\sum x_i, \qquad \hat{\mu}_2(x_1, \ldots, x_m) = 1$$

Clearly, choosing $\hat{\mu}_2$ does not seem like a smart decision as for any true value of the distribution's expectation $\mu \neq 1$ our estimation will probably be wrong. However, if the true value is indeed $\mu = 1$ then the sample mean estimator $\hat{\mu}_1$ will be out-performed by $\hat{\mu}_2$.

And so, to try and answer the questions above we need to devise ways to evaluate estimators. To do so we define two types of objects:

- Properties of estimators - these will be desired properties that an estimator might fulfill, and that will help us choose an estimator.
- A loss function - A measure to compare between the estimated values obtained by the estimator and the true value of the parameters.

Then, using these objects we can define in what sense is one estimator better than another. Usually this will be done in the form of finding an estimator that minimizes some loss function out of the set of estimators fulfilling some property.

Throughout this book we will encounter different examples where we will switch from using one estimator with another depending on what we are trying to achieve.

1.1.2.1 Loss Functions

Definition 1.1.3 A *loss function* is a function that maps an event onto a real number: $L : \Omega \to \mathbb{R}$

Intuitively, a loss function represents the *cost* associated with the event. In the context of decision theory such an event will be the estimation outputted by an estimator and we will often want to find the estimator minimizing this cost. Here are a few examples for different loss functions that we will encounter throughout the book:

- The ℓ_{0-1} loss function defined as: $L(\hat{\theta},\theta) := \mathbb{1}_{\hat{\theta}=\theta}$.
- The ℓ_ε loss function defined as: $L_\varepsilon(\hat{\theta},\theta) := \mathbb{1}_{||\hat{\theta}-\theta||\leq\varepsilon}$ for some predetermined norm and $\varepsilon \geq 0$.
- The absolute-value (ℓ_1) loss function defined as: $L(\hat{\theta},\theta) := \left|\hat{\theta}-\theta\right|$.
- The quadratic or squared-error (ℓ_2) loss function defined as: $L(\hat{\theta},\theta) := \left(\hat{\theta}-\theta\right)^2$.

For different scenarios different loss functions are used. For example, in the case of the estimating the current time, perhaps estimating the exact time is less important than being close to it. If that is the case, we might prefer using the absolute-value or squared-error loss functions. Or perhaps we are not concerned with how far is our estimation as long as it is within a certain deviance from the actual time. In such case we might prefer using the ℓ_ε loss function.

Another term associated with the notion of loss functions is the *risk function* of a decision rule.

Definition 1.1.4 Let X be a set of observations and $\delta(X)$ a decision rule for parameter $\boldsymbol{\theta}$. The risk function of δ and $\boldsymbol{\theta}$ with respect to a loss function L is defined as the expected loss:

$$\mathcal{R}(\boldsymbol{\theta},\delta) := \mathbb{E}_X\left[L(\theta,\delta(X))\right]$$

One such risk function, which we will see in chapter 2, is the Mean Squared Error (MSE) risk function. This is the risk function with respect to the squared-error loss function $\mathcal{R}(\boldsymbol{\theta},\hat{\boldsymbol{\theta}}) := \mathbb{E}_X[(\boldsymbol{\theta}-\hat{\boldsymbol{\theta}}(X))^2]$.

1.1.2.2 Bias, Variance & Consistency

Unbiasedness

One of the most desirable properties of an estimator is to be unbiased. That is, that on average our estimation equals to the true parameter estimated. Formally,

Definition 1.1.5 Let $\delta(x_1,\ldots,x_m)$ be an estimator for a parameter θ. The difference $d = \delta(x_1,\ldots,x_m) - \theta$ is called the *error* of the estimator δ.

Definition 1.1.6 Let $\delta(x_1,\ldots,x_m)$ be an estimator for a parameter θ. The quantity

$$Bias_\theta\left[\delta(x_1,\ldots,x_m)\right] := \mathbb{E}_{x_1,\ldots,x_m|\theta}\left[d\right] = \mathbb{E}_{x_1,\ldots,x_m|\theta}\left[\delta(x_1,\ldots,x_m)-\theta\right]$$

for $x_1,\ldots,x_m|\theta$ denoting the probability of sample $x_1\ldots,x_m$ from $\mathcal{P}(\theta)$, is called the *bias* (or systematic error) of the estimator δ.

Definition 1.1.7 Let $\delta(x_1,\ldots,x_m)$ be an estimator for a parameter θ. δ is said to be *unbiased* if

$$\forall\theta\in\Theta \quad Bias_\theta\left[\delta(x_1,\ldots,x_m)\right]=0 \text{ or equivelantly } \forall\theta\in\Theta \quad \mathbb{E}_{x_1\ldots,x_m|\theta}\left[\delta(x_1,\ldots,x_m)\right]=\theta$$

Let us revisit the previously defined sample mean (1.2) and sample variance (1.3) estimators and show that these are both unbiased estimators. Beginning with the sample mean estimator then

$$\mathbb{E}(\hat{\mu})=\mathbb{E}\left(\frac{1}{m}\sum_{i=1}^{m}x_i\right)=\frac{1}{m}\sum_{i=1}^{m}\mathbb{E}(x_i)=\mathbb{E}(X)\frac{1}{m}\sum_{i=1}^{m}1=\mathbb{E}(X)=\mu \tag{1.4}$$

where we used the linearity property of the expectation and that the samples are i.i.d. Similarly we can show that the sample variance is unbiased:

$$\begin{aligned}\mathbb{E}\left(\hat{\sigma}^2\right) &= \frac{1}{m-1}\sum_{i=1}^{m}\mathbb{E}\left((x_i-\hat{\mu})^2\right)\\ &= \frac{1}{m-1}\sum_{i=1}^{m}\mathbb{E}\left(x_i^2-2x_i\frac{1}{m}\sum_{j=1}^{m}x_j+\frac{1}{m^2}\sum_{k,j=1}^{m}x_kx_j\right)\end{aligned}$$

The X_i's are i.i.d which implies that $\mathbb{E}(x_i)=\mathbb{E}(X)$ and $\mathbb{E}\left(x_i^2\right)=\mathbb{E}\left(X^2\right)$ for every i, as well as that $\mathbb{E}(x_kx_j)=\mathbb{E}^2(X)=\mu_X^2$ for every $k\neq j$. Substituting into the above sums we obtain that:

$$\mathbb{E}\left(\hat{\sigma}^2\right)=\mathbb{E}\left(X^2\right)-\mathbb{E}^2(X)=Var(X)=\sigma^2$$

In a similar manner we can show that the estimator of sample variance where we divide by m instead of $m-1$ is a *biased* estimator. Ex.2

Variance

Another useful property of an estimator, that provides us with an indication of how well is the estimator performing, is its variance. Since an estimator is a function of (a set of) random variables, it itself is a random variable. Therefore, the variance of an estimator is simply the variance of a random variable, where the probability space is defined over the events of obtaining a given set of samples.

Definition 1.1.8 Let $\delta(x_1,\ldots,x_m)$ be an estimator for a parameter θ. The *variance* of δ is defined as

$$Var(\delta):=\mathbb{E}_{x_1,\ldots,x_m|\theta}\left[\left(\delta(x_1,\ldots,x_m)-\mathbb{E}_{x_1,\ldots,x_m|\theta}\left[\delta(x_1,\ldots,x_m)\right]\right)^2\right]$$

where expectation is taken over the even of sampling $x_1,\ldots,x_m$ from $\mathcal{P}(\theta)$.

Let us compute the variance of the sample mean estimator (1.2). Let $x_1,\ldots,x_m$ be a set of independent random variables with identical variance σ^2. As the sample mean estimator is the mean of m random variables we could simply:

$$\begin{aligned}Var(\hat{\mu}) &= Var\left(\frac{1}{m}\sum x_i\right)\\ &= \frac{1}{m^2}Var\left(\sum x_i\right)\\ &\overset{(*)}{=} \frac{1}{m^2}\sum Var(x_i)\\ &\overset{(**)}{=} \frac{1}{m^2}\cdot m\cdot\sigma^2\\ &= \frac{\sigma^2}{m}\end{aligned}$$

where we used the assumption that the samples are independent $(*)$ and with identical variance $(**)$.

Consistency

Going back to the task of determining a given time where we defined our estimator as the sample mean, it seems intuitive that the more individuals asked the more accurate (i.e closer to the true value) our estimation should be. Let us formulate this as a property an estimator might fulfill.

Definition 1.1.9 A sequence $\{Z_n\}$ of random variables is said to *converge in probability* to a random variable Z if for any $\varepsilon > 0$

$$\lim_{n\to\infty} \mathbb{P}(|Z_n - Z| > \varepsilon) = 0$$

and is denoted by $Z_n \xrightarrow{p} Z$.

Definition 1.1.10 An estimator $\theta_n(x_1,\ldots,x_n)$ of parameter θ is said to be *consistent* if it converges in probability to the true value of θ:

$$\forall \varepsilon > 0 \ \lim_{n\to\infty} \mathbb{P}(|\theta_n - \theta| > \varepsilon) = 0$$

Let us understand these definitions as it is to be applied for an estimator. Since an estimator is a function of the random variables $x_1,\ldots,x_m \sim \mathcal{P}$ it is itself a random variable. Consider a set of estimators (random variables) $\{\hat{\theta}_n\}_{n=1}^{\mathbb{N}}$, each calculated over the first n samples. In addition, denote θ the constant random variable valuing as the true parameter estimated. Therefore, $\theta_n \xrightarrow{p} \theta$ means that as we increase the sample size n the probability of our estimation deviating from the true parameter by more than a fixed amount ε tends to zero. It can be shown that the sample mean has the property of being a consistent estimator.

In this section we have discussed the first and second moments of an estimator (first moment in the form of an estimator's bias). Being a random variable, we can also discuss the distribution of a random variable, as seen shortly in Lab 01 - Data Simulation and Sampling.

1.1.3 The Maximum Likelihood Estimator

And so, we can now define a criteria by which we define what does it mean for an estimator to be "optimal". For example, for a set of estimators Δ, we can decide that the optimal estimator is one that is *unbiased* and that achieves the minimal variance out of all estimators in Δ. This approach is known as the Minimum Variance Unbiased (MVU). This is a logical decision. Unbiased estimators are right "on average" and having a small as possible variance means we are often not far from this average. Notice also that by this definition there could be more than a single "optimal" estimator in Δ.

Another approach is to look for the *Maximum Likelihood Estimator*. This approach suggests choosing the estimator under which the observed data was *most likely*. Suppose we obtained the observations $x_1,\ldots,x_m \overset{i.i.d}{\sim} \mathcal{P}(\boldsymbol{\theta})$. For the probability distribution function $\mathcal{P}$ we define the likelihood function.

Definition 1.1.11 — Likelihood. Let X be a random variable following some probability distribution $\mathcal{P}$ with a density function f that depends on a parameter $\boldsymbol{\theta} \in \Theta$. The *likelihood* function is

$$\mathcal{L}(\boldsymbol{\theta}|x) := f_{\boldsymbol{\theta}}(x)$$

for x the realization of X.

For example, consider the case of the univariate Gaussian distibution seen above (1.1.2). Then, for $\boldsymbol{\theta} = \{\mu, \sigma^2\}$

the likelihood function of $\mathcal{P} = \mathcal{N}(\mu, \sigma^2)$ is:

$$\mathcal{L}(\boldsymbol{\theta}|x_i) = f_{\boldsymbol{\theta}}(x_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x_i-\mu)^2}{2\sigma^2}\right), \quad i \in [m] \tag{1.5}$$

where, for the sample $x_1, \ldots, x_m$ where the samples are drawn i.i.d the likelihood is:

$$\begin{array}{rcl} \mathcal{L}(\boldsymbol{\theta}|x_1,\ldots,x_m) & = & f_{\boldsymbol{\theta}}(x_1,\ldots,x_m) \\ & = & \prod_{i=1}^{m} f_{\boldsymbol{\theta}}(x_i) \\ & = & \frac{1}{\left(2\pi\sigma^2\right)^{m/2}} \exp\left(-\frac{1}{2\sigma^2}\sum(x_i-\mu)^2\right) \end{array} \tag{1.6}$$

Using the likelihood function derived for the univariate Gaussian distribution we can now provide each $\boldsymbol{\theta}$ with a quantity (the likelihood) of how likely is it to have generated the observed data.

■ **Example 1.1** Let $x_1, x_2, x_3, x_4 \overset{i.i.d}{\sim} \mathcal{N}(\mu, \sigma^2)$ where $x_1 = -1, x_2 = 0, x_3 = 0, x_4 = 1$ and $\sigma^2 = 1$. Let us calculate the likelihood for:

- $\mu = 0$:

$$\begin{array}{rcl} \mathcal{L}(\mu=0,\sigma^2=1|x_1,x_2,x_3,x_4) & = & \frac{1}{(2\pi)^2}\exp(-\frac{1}{2}\sum_{i=1}^{4}x_i^2) \\ & = & \frac{1}{4\pi^2}\exp(-\frac{2}{2}) \\ & \approx & 0.00931 \end{array}$$

- $\mu = 1$:

$$\begin{array}{rcl} \mathcal{L}(\mu=1,\sigma^2=1|x_1,x_2,x_3,x_4) & = & \frac{1}{(2\pi)^2}\exp(-\frac{1}{2}\sum_{i=1}^{4}(x_i-1)^2) \\ & = & \frac{1}{4\pi^2}\exp(-\frac{2^2+1+1}{2}) \\ & \approx & 0.00126 \end{array}$$

■

And so, given the likelihood function we define the Maximum Likelihood Estimator (MLE) as $\boldsymbol{\theta} \in \Theta$ that maximizes the likelihood function. Formally:

Definition 1.1.12 Let $\mathcal{L}$ be the likelihood function of some probability distribution $\mathcal{P}$ characterized by $\boldsymbol{\theta} \in \Theta$. Let $X \sim \mathcal{P}(\boldsymbol{\theta})$ be a random variable and x its realization. The *Maximum Likelihood Estimator* (MLE) for $\boldsymbol{\theta}$ is

$$\hat{\boldsymbol{\theta}}^{MLE} := \underset{\boldsymbol{\theta}\in\Theta}{\operatorname{argmax}}\ \mathcal{L}(\boldsymbol{\theta}|x)$$

Let us derive the MLE for the expectation of a univariate Gaussian distribution when σ^2 is known. Let $x_1, \ldots, x_m \overset{i.i.d}{\sim} \mathcal{N}(\mu, \sigma^2)$. So:

$$\hat{\mu}^{MLE} = \underset{\mu\in\mathbb{R}}{\operatorname{argmax}}\ \mathcal{L}(\mu|x_1,\ldots,x_m,\sigma^2)$$

Since the logarithm function is a monotonous increasing transformation the maximizer of the likelihood

function is also the maximizer of the *log-likelihood*. Thus:

$$\begin{aligned}\hat{\mu}^{MLE} &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ \mathcal{L}(\mu|x_1,\ldots,x_m,\sigma^2)\\ &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ \log\mathcal{L}(\mu|x_1,\ldots,x_m,\sigma^2)\\ &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ \log\left(\prod_{i=1}^{m}\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x_i-\mu)^2}{2\sigma^2}\right)\right)\\ &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ \log\left(\frac{1}{(2\pi\sigma^2)^{m/2}}\exp\left(-\frac{1}{2\sigma^2}\sum(x_i-\mu)^2\right)\right)\\ &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ \log\left(\exp\left(-\frac{1}{2\sigma^2}\sum(x_i-\mu)^2\right)\right)\\ &= \underset{\mu\in\mathbb{R}}{\text{argmax}}\ -\sum_{i=1}^{m}(x_i-\mu)^2\end{aligned} \tag{1.7}$$

And so, to find the maximizer, we calculate the derivative with respect to μ and equate to zero:

$$\begin{gathered}\frac{\partial}{\partial\mu}\left(-\sum_{i=1}^{m}(x_i-\mu)^2\right) = -\sum_{i=1}^{m}\frac{\partial(x_i-\mu)^2}{\partial\mu} = \sum_{i=1}^{m}2(x_i-\mu) = 0\\ \Downarrow\\ \hat{\mu}^{MLE} = \frac{1}{m}\sum_{i=1}^{m}x_i\end{gathered} \tag{1.8}$$

Notice that when we previously used the sample mean estimator (1.2) we have therefore actually used the maximum likelihood estimator for the expectation. Similarly, we can derive that the sample variance defined above is the MLE of the variance.

1.1.3.1 Beyond Maximum Likelihood - A Bayesian Approach

Suppose we are facing the task of estimating average human height. We observe $x_1,\ldots,x_m$ a set of i.i.d samples reflecting the heights of m individuals. In order to estimate the average human height $\hat{\theta}$, we must first specify a principle by which we select an estimator.

In the section above we defined the likelihood function $\mathcal{L}(\boldsymbol{\theta}|x)$ and the strategy of selecting the estimator that maximizes the likelihood function - the MLE. Let us assume that $x|\boldsymbol{\theta}$ follows a normal distribution. If our sample is $x_1 = 2m, x_2 = 2.03m, x_3 = 1.95m, x_4 = 2.1m, x_5 = 1.65m$ then the MLE is the sample mean: $\hat{\theta}^{MLE} = 1.94m$. This however seems to be an odd estimation. Even without looking at our observations it seems logical that over the general population the average human height should probably be lower than 1.9m and perhaps higher than 1.5m. This seems logical as we have some additional knowledge (a prior belief) on the problem. Therefore, the question is how could we include this additional knowledge in our estimation?

Let us go back to the likelihood function. We defined it as the PDF of an observation x under a probability distribution characterized by $\boldsymbol{\theta}$. We interpret $\mathcal{L}(\boldsymbol{\theta}|x)$ as "how likely is $\boldsymbol{\theta}$ "given" the observation x". The term "given" is itself interpreted as "while fixing the observation x" and not in the sense of probability theory. We could however further *assume* that both X and $\boldsymbol{\theta}$ are random variables which have some *joint probability distribution* function $f_{X,\Theta}(x,\boldsymbol{\theta})$. By doing so we can derive a new criteria for selecting an estimator. Under such assumption of a joint probability distribution $f_{X,\Theta}(x,\boldsymbol{\theta})$ the expression $x|\boldsymbol{\theta}$ can be understood through the conditional distribution:

$$f_{X|\Theta=\boldsymbol{\theta}}(x) = \frac{f_{X,\Theta}(x,\boldsymbol{\theta})}{f_{\Theta}(\boldsymbol{\theta})} \tag{1.9}$$

Same as before, we can choose the MLE as $\hat{\boldsymbol{\theta}}^{MLE}$ that maximizes $f_{X|\Theta=\boldsymbol{\theta}}(x)$. Now, by applying Bayes' theorem of conditional distributions we can express the conditional $\Theta|X$ as:

$$\overbrace{f_{\Theta|X=x}(\boldsymbol{\theta})}^{posterior} = \frac{\overbrace{f_{X|\Theta=\boldsymbol{\theta}}(x)}^{likelihood}\cdot\overbrace{f_{\Theta}(\boldsymbol{\theta})}^{prior}}{\underbrace{f_X(x)}_{evidence}} \tag{1.10}$$

where $f_{X|\Theta=\boldsymbol{\theta}}(x)$ is the likelihood function, $f_\Theta(\boldsymbol{\theta})$ is the marginal distribution of Θ and $f_X(x)$ the marginal distribution of X functioning as a normalization factor. The marginal f_Θ reflects our *belief* regarding the true value of $\boldsymbol{\theta}$ *before* (i.e *prior*) observing the data. Therefore, the *A-Posteriori* distribution $f_{\Theta|X=x}$, i.e the conditional of $\boldsymbol{\theta}$ *after* observing the data, is the weighting of the likelihood function by our prior belief and the evidence of the data.

By using the A-Posteriori distribution, we can derive the Maximum A-Posteriori estimator (MAP):

$$\hat{\boldsymbol{\theta}}^{MAP} := \underset{\boldsymbol{\theta}\in\Theta}{\operatorname{argmax}}\, f_{\Theta|X=x}(\boldsymbol{\theta}) = \underset{\boldsymbol{\theta}\in\Theta}{\operatorname{argmax}}\, \frac{f_{X|\Theta=\boldsymbol{\theta}}(x)\cdot f_\Theta(\boldsymbol{\theta})}{f_X(x)} = \underset{\boldsymbol{\theta}\in\Theta}{\operatorname{argmax}}\, f_{X|\Theta=\boldsymbol{\theta}}(x)\cdot f_\Theta(\boldsymbol{\theta}) \tag{1.11}$$

Namely, the estimator that while takes into account both what is observed (the likelihood) and the prior belief.

Returning to the task of estimating human heights, let us further assume that the average human height follows a normal distribution centered around 1.7m with a variance of 0.01m. Therefore we assume that:

$$\theta \sim \mathcal{N}(1.7, 0.01) \quad (1)$$
$$x_i|\theta \overset{i.i.d}{\sim} \mathcal{N}(\theta, \sigma^2)\ \forall i \quad (2)$$

where we set σ^2 as $(\hat{\sigma}^2)^{MLE} \approx 0.17$. Under these assumptions and the sample above $x_1 = 2m, x_2 = 2.03m, x_3 = 1.95m, x_4 = 2.1m, x_5 = 1.65m$ we can now evaluate different values of θ:

- For $\theta = 1.94$ (the likelihood maximizer) we find that:

$$\log\left(f_{X|\theta=1.94,\sigma^2=0.17}(x_1,\ldots,x_5)\cdot f_\Theta(1.94)\right) = \log\left(f_\Theta(1.94)\cdot\prod_i f_{\theta=1.94,\sigma^2=0.17}(x_i)\right) = 1.264$$

- For $\theta = 1.7$ (the prior's expectation) we find that:

$$\log\left(f_{X|\theta=1.7,\sigma^2=0.17}(x_1,\ldots,x_5)\cdot f_\Theta(1.94)\right) = \log\left(f_\Theta(1.7)\cdot\prod_i f_{\theta=1.7,\sigma^2=0.17}(x_i)\right) = 1.442$$

Thus, under this prior we see that the MLE does not achieve the maximal posterior probability.

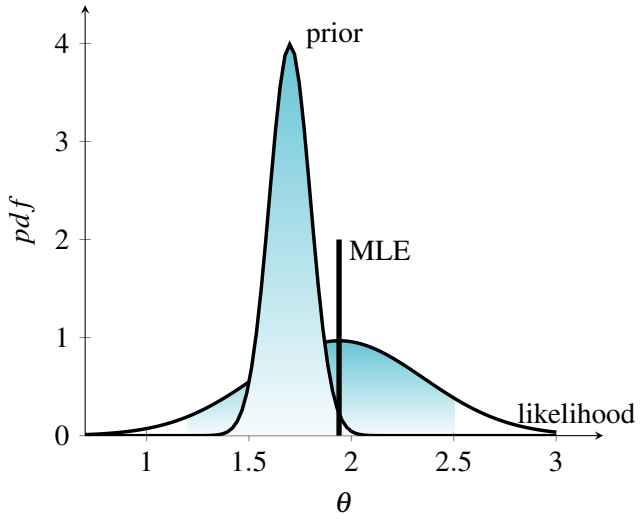


Figure 1.1: *Likelihood and prior distributions for human heights example*

R In general, the field of statistical learning splits between these two approaches: frequentistic methods which aim to express and maximize the likelihood function, and Bayesian methods which assume some prior distribution and derive estimators that use both the likelihood and the prior (one of these estimators is the MAP estimator seen above). It can be shown that when we correctly assume a prior distribution the Bayesian estimators are superior to the MLE. The challenge however with the Bayesian methods lies precisely in how to obtain such (estimation of ?) prior. Though this book focuses on frequentistic methods, we shortly discuss some Bayesian methods in section 3.5.

1.1.4 Measures of Concentration For Estimation Tasks

Occasionally, providing an estimation for some parameter of interest is not sufficient, and we are further interested in providing some bounds describing how "good"/"close" is our estimation to the true value. Consider for example the following scenario. Suppose we have a coin for which we want to estimate its bias, that is with what probability p flipping the coin will result with "Heads" being up and with probability $1-p$ "Tails" being up. Formally, we can think (i.e. model) a single coin flip as a Bernoulli random variable X which takes the value of 1 for "Heads" or 0 for "Tails".

We shall denote the probability distribution of X by $\mathcal{D}_p$ such that:

$$\mathcal{D}_p(X) = \begin{cases} p & X = 1 \\ 1-p & X = 0 \end{cases}, \quad p \in [0,1] \tag{1.12}$$

To estimate the value of p we take a sequence of m tosses of the coin $X_1, \ldots, X_m \overset{i.i.d}{\sim} Ber(p)$ and denote the results of the tosses (i.e. the samples) by $S = \{x_1, \ldots, x_m\}$ where x_i refers to the result of the random variable X_i. Lastly, we denote the probability distribution of the m coin tosses by $\mathcal{D}_p^m$ and therefore the probability of obtaining a specific sample S by $\mathcal{D}_p^m(S)$. To simplify notation we will omit the writing of p and write $\mathcal{D}^m(S)$.

Now, given such sample we would like to devise a *learning algorithm*, $\mathcal{A}$ to estimate/predict the true value of p. So, a coin prediction learning algorithm is a procedure which takes as input a sample $S = \{x_1, \ldots, x_m\}$, drawn according to $\mathcal{D}^m$, and outputs estimation of p. This estimation is denoted by $\mathcal{A}(S)$ or $\hat{p}(S)$ or simply $\hat{p}$. A straightforward strategy (i.e. algorithm) is to estimate p simply by calculating the empirical proportion of heads (ones):

$$\hat{p}(S) = \frac{1}{m}\sum x_i \tag{1.13}$$

It can be shown that this estimator is the MLE of the problem. Notice, that as we have shown earlier, the empirical mean in an unbiased estimator for the expectation (1.4). Namely, if we sample many set of samples $S_i = \left\{x_1^{(i)}, \ldots, x_m^{(i)}\right\}$, for each run our algorithm and output $\hat{p}_i$, then calculate the expected value over the p_is, then the result is p. Formally, $\mathbb{E}_S[\hat{p}(S)] = p$. This clearly seems like a desirable properly for our algorithm. However, since we seldomly have many different sets of samples and as a given sample S is finite, we do not expect our estimation of $\hat{p}$ to be exact. Instead we acknowledge that the algorithm might yield a $\hat{p}$ which satisfies that $|\hat{p} - p| \leq \varepsilon$, for some $\varepsilon \in (0,1)$ which is called the *accuracy* parameter. That is, our algorithm might not return exactly p, but it returns a result $\hat{p}$ which is "close enough".

Even then, unless p equals 1 or 0, there is always *some* chance that the drawn sample would be highly non-representative. We might for example, though unlikely, end up with a sample of all "Heads" or "Tails" regardless to the true value of p. So it is impossible to obtain a guarantee that $|\hat{p} - p| \leq \varepsilon$ holds with absolute certainty. Hence, we introduce a *confidence* parameter $\delta \in (0,1)$, and require that the event $\{S : |\hat{p} - p| > \varepsilon\}$ occurs with a probability of at most δ. In other words, we require our algorithm to be such that the probability of flipping the coin m times and obtaining a sequence S that causes it to produce an inaccurate estimation, $\hat{p}(S)$ ('inaccurate' meaning $|\hat{p} - p| > \varepsilon$) is smaller or equal to δ.

Intuitively, the larger the number of flips, the more information we have about the coin and the better chance

we have to satisfy the accuracy and confidence requirements. Since the accuracy and confidence parameters ε and δ are fixed, there should be some finite number of flips $m_{\mathcal{A}}$ (which depends on ε, δ and $\mathcal{A}$) such that for any sample of size $m \geq m_{\mathcal{A}}$ our algorithm satisfies the above accuracy and confidence requirements. The function that given ε, δ returns $m_{\mathcal{A}}$ such that that accuracy and confidence requirements are met is called the *sample complexity* function.

Measure Concentration Using Markov's Inequality

And so, we would like to ask "How good is our learning algorithm"? We already know that on average our learning algorithm will output the correct answer. In addition, as the empirical mean is a consistent estimator we know that the estimation will become more accurate as the number of samples m increases. What we do not know is how many samples do we need and can we somehow bound the probability of being inaccurate (i.e. the confidence) by some function depending on the number of samples. To do so we begin with using the most basic measure of concentration by applying Markov's inequality.

Notice that $|\hat{p} - p|$ is a non-negative random variable. Therefore, by fixing some accuracy level $\varepsilon \in (0,1)$ we can bound from above the probability of $\hat{p}$ deviating from p by more than ε:

$$\mathcal{D}^m \left[|\hat{p} - p| \geq \varepsilon \right] \leq \frac{\mathbb{E}\left[|\hat{p} - p| \right]}{\varepsilon}$$

where the expectation can be bounded from above by:

$$\begin{array}{rcccl} \mathbb{E}^2\left[|\hat{p} - p| \right] & \leq & \mathbb{E}\left[|\hat{p} - p|^2 \right] & = & \mathbb{E}\left[(\hat{p} - p)^2 \right] \\ & = & \mathbb{E}\left[(\hat{p} - \mathbb{E}[\hat{p}])^2 \right] & = & Var(\hat{p}) \\ & = & Var\left(\frac{1}{m} \sum x_i \right) & = & \frac{1}{m^2} Var\left(\sum x_i \right) \\ & = & \frac{p(1-p)}{m} & \leq & \frac{1}{4m} \\ & & \Downarrow & & \\ & & \mathbb{E}\left[|\hat{p} - p| \right] \leq \frac{1}{\sqrt{4m}} & & \end{array}$$

where we used the definition of variance $Var(A) = \mathbb{E}\left[A^2\right] - \mathbb{E}^2[A]$. Put together:

$$\mathcal{D}^m \left[|\hat{p} - p| \geq \varepsilon \right] \leq \frac{\mathbb{E}\left[|\hat{p} - p| \right]}{\varepsilon} \leq \frac{1}{\sqrt{4m\varepsilon^2}}$$

Thus we have obtained a bound on the confidence, for a given accuracy, as a function of the number of samples. We can now express the above as follows. If we select m to be $m \geq \left\lceil \frac{1}{4\varepsilon^2} \cdot \frac{1}{\delta^2} \right\rceil$ then the right-hand side is smaller or equals to δ. So, for any $\varepsilon, \delta \in (0,1)$, if we sample $m_{\mathcal{A}}(\varepsilon, \delta) \geq \left\lceil \frac{1}{4\varepsilon^2} \cdot \frac{1}{\delta^2} \right\rceil$ samples then this learning algorithm achieves:

$$\mathcal{D}_p^m \left[|\hat{p}(S) - p| \geq \varepsilon \right] \leq \delta$$

Namely, the algorithm is accurate enough (as specified by ε) with a high enough confidence (as specified by $1 - \delta$).

Measure Concentration Using Chebyshev's Inequality

We can improve the upper bound seen in (1.1.4) (i.e find a sample complexity function that will need less samples) by using Chebyshev's inequality.

Theorem 1.1.1 — Chebyshev's Inequality. Let X be a random variable with a finite mean $\mathbb{E}[X]$ and

variance $Var(X)$. Then, for every $\varepsilon > 0$:

$$\mathbb{P}[|X - \mathbb{E}[X]| \geq \varepsilon] \leq \frac{Var(X)}{\varepsilon^2}$$

Proof. Consider the random variable $Y = (X - \mathbb{E}[X])^2$. This is a non-negative random variable and as such we can apply Markov's inequality over it. We obtain that $\mathbb{P}\left[(X - \mathbb{E}[X])^2 \geq \varepsilon^2\right] \leq \frac{Var(X)}{\varepsilon^2}$. To conclude the proof, observe that $\mathbb{P}[|X - \mathbb{E}[X]| \geq \varepsilon] = \mathbb{P}\left[(X - \mathbb{E}[X])^2 \geq \varepsilon^2\right]$. ■

So, given a sample $x_1, \ldots, x_m \overset{i.i.d}{\sim} Ber(p)$ we can now bound the deviance of our estimator $\hat{p}$ from its expected value as follows:

$$\begin{array}{lllll} \mathbb{P}[|\hat{p} - \mathbb{E}[\hat{p}]| \geq \varepsilon] & \overset{unbiased}{=} & \mathbb{P}[|\hat{p} - p| \geq \varepsilon] & \overset{Chebyshev}{\leq} & \frac{Var(\hat{p})}{\varepsilon^2} \\ & = & \frac{1}{\varepsilon^2} Var\left(\frac{1}{m}\sum x_i\right) & \overset{i.i.d}{=} & \frac{1}{\varepsilon^2 \cdot m^2}\sum Var(x_i) \\ & = & \frac{p(1-p)}{m\varepsilon^2} & & \end{array}$$

For which, since the variance of a Bernoulli random variable is $p(1-p) \leq 1/4$, we can simply conclude that $\mathbb{P}[|\hat{p} - \mathbb{E}[\hat{p}]| \geq \varepsilon] \leq \frac{1}{4m\varepsilon^2}$. The bound obtained using Chebyshev's inequality tends to zero as $\frac{1}{m}$ while the one obtained from Markov's inequality tends to zero as $\frac{1}{\sqrt{m}}$. By solving for m $\delta = \frac{1}{4m\varepsilon^2}$ then we derive a tighter bound for the sample complexity $m_{\mathcal{A}}(\varepsilon, \delta) \leq \left\lceil \frac{1}{4\delta\varepsilon^2} \right\rceil$.

Measure Concentration Using Hoeffding's Inequality

A natural question which arises is whether the obtained bound is optimal (tight). Indeed, we can further improve the bound by exploiting the fact that our random variable not only has a finite variance, but it is also bounded between 0 and 1. For this end we use Hoeffding's inequality for the average of independent and bounded random variables.

Theorem 1.1.2 — Hoeffding's inequality. Let $X_1, \ldots X_m$ be independent and bounded random variables with $a_i \leq X_i \leq b_i$. Let $\overline{X} = \frac{1}{m}\sum_{i=1}^m X_i$. Then,

$$\mathbb{P}\left[\left|\overline{X} - \mathbb{E}\left[\overline{X}\right]\right| \geq \varepsilon\right] \leq 2\exp\left(\frac{-2m^2\varepsilon^2}{\sum_{i=1}^m (b_i - a_i)^2}\right)$$

Corollary 1.1.3 Let $X_1, \ldots X_m$ be a sequence of m i.i.d random variables, each with an expectation value $\mathbb{E}[X]$ and all of which are bounded: $a \leq X_i \leq b$. Denote $\overline{X} = \frac{1}{m}\sum_{i=1}^m X_i$ then:

$$\mathbb{P}\left[\left|\overline{X} - \mathbb{E}[X]\right| \geq \varepsilon\right] \leq 2\exp\left(\frac{-2m\varepsilon^2}{(b-a)^2}\right)$$

Proof. Notice that as $X_1, \ldots, X_m$ all share the same expectation and bounds then

$$\mathbb{E}\left[\overline{X}\right] = \frac{1}{m}\sum_{i=1}^m \mathbb{E}[X] = \mathbb{E}[X], \quad \sum_{i=1}^m (b_i - a_i)^2 = m \cdot (b-a)^2$$

By placing these expressions in Lemma 1.1.2 we conclude the inequality. ■

By applying Hoeffding's inequality to the case of the coin prediction problem, then for a sample of size m, we obtain that $\mathcal{D}_p^m[|\hat{p} - p| \geq \varepsilon] \leq 2\exp\left(-2m\varepsilon^2\right)$. Therefore, if using Hoeffding's inequality we are able to

get a bound which converges exponentially in m. By taking $m \geq \left\lceil \frac{1}{2\varepsilon^2} \cdot \log(\frac{2}{\delta}) \right\rceil$ samples we obtain that this probability is bound above by δ as required.

1.2 Multivariate Distributions

Up to now, we only dealt with random variables taking a single value. However, we often face a situation where an observation consists of multiple properties. As different properties may (or may not) influence one another we wish to define how the set of properties jointly behaves.

■ **Example 1.2** Consider the question of describing human weight and height. It is possible to model (i.e. describe how the data behaves) each of these properties independently using some distribution. Suppose $w_1,\ldots,w_m$ are the weights (in kilograms) of m individuals and $h_1\ldots,h_m$ are the heights (in centimeters) of the same individuals. Let us assume that the weights and heights each follow some normal distribution:

$$w_1,\ldots,w_m \overset{i.i.d}{\sim} \mathcal{N}(75,3)$$
$$h_1,\ldots,h_m \overset{i.i.d}{\sim} \mathcal{N}(170,5)$$

However, we know that the properties of weight and height are linked. There exists (in the data) a connection between the two such that, in general, the taller an individual is the higher the weight. As such, we would prefer to model the data using a *join distribution* that describes the pairs of weights and heights $(w_1,h_1),\ldots,(w_m,h_m)$.
■

Definition 1.2.1 — Joint distribution. Given random variables $X_1,\ldots,X_d$, that are defined on a probability space, the joint probability distribution for $X_1,\ldots,X_d$ is a probability distribution that gives the probability that each of $X_1,\ldots,X_d$ falls in any particular range (for continuous RVs) or discrete set (for discrete RVs) of values specified for that variable.

Definition 1.2.2 — Joint PDF of a random vector. Two random variables X_1 and X_2 are ***jointly continuous*** if there exists a non-negative function $f_{X_1,X_2}:\mathbb{R}^2\to\mathbb{R}$, such that, for any set $A\in\mathbb{R}^2$, it holds that

$$\mathcal{D}((x_1,x_2)\in A)=\int_A f_{X_1,X_2}(x_1,x_2)\,dx_1dx_2$$

The function f_{X_1,X_2} is called the ***joint probability density function (JPDF)*** of X_1 and X_2. Often, if the context is clear, one omits the subscripts of f and simply writes $f(x_1,x_2)$.

Definition 1.2.3 — Random vector. A (column) ***random vector***: $X \coloneqq (X_1,\ldots,X_d)^\top$, is a finite collection of random variables, denoted $X_1,\ldots,X_d$, defined on a common probability space $(\Omega,\mathcal{D})$.

Returning to the task of describing a distribution of human weights and heights we can now denote the observations using random vectors $\mathbf{x}_1,\ldots,\mathbf{x}_m\in\mathbb{R}^d$ for $d=2$. We could then consider how does a specific feature manifest in the sample. For the i'th property $\mathbf{x}_1(i),\ldots,\mathbf{x}_m(i)$ are the realizations random variables $X_1^{(i)},\ldots,X_m^{(i)}$. Another form of writing $\mathbf{x}_1(i),\ldots,\mathbf{x}_m(i)$ is by using two indices, the first standing for the sample's index and the second for the property $x_{1,i},\ldots,x_{m,i}$.

When dealing with more than a single random variable we can ask how do the different variables jointly vary. For two jointly distributed real-valued random variables X,Y with finite second moments, the covariance between X and Y as $cov(X,Y)=\mathbb{E}[X-\mathbb{E}[X]]\,\mathbb{E}[Y-\mathbb{E}[Y]]$. The covariance between a random variable and itself is $cov(X,X)=\mathbb{E}[X-\mathbb{E}[X]]^2=Var(X)$. We arrange the covariances between d different random variables in the form of a *covariance matrix*

Definition 1.2.4 — Covariance Matrix. Let $X := (X_1, \ldots, X_d)^\top$ be a random vector. The *Covariance Matrix* Σ is the $d \times d$ matrix whose (i,j) entry is the covariance $\Sigma_{ij} := \sigma(X_i, X_j)$:

$$\Sigma := \begin{pmatrix} \mathbb{E}[(X_1 - \mathbb{E}[X_1])(X_1 - \mathbb{E}[X_1])] & \ldots & \mathbb{E}[(X_1 - \mathbb{E}[X_1])(X_d - \mathbb{E}[X_d])] \\ \vdots & \ddots & \vdots \\ \mathbb{E}[(X_d - \mathbb{E}[X_d])(X_1 - \mathbb{E}[X_1])] & \ldots & \mathbb{E}[(X_d - \mathbb{E}[X_d])(X_d - \mathbb{E}[X_d])] \end{pmatrix}$$

- In matrix notation we can express the covariance matrix as:

$$\Sigma := \mathbb{E}\left[(X - \mathbb{E}[X])(X - \mathbb{E}[X])^\top\right]$$

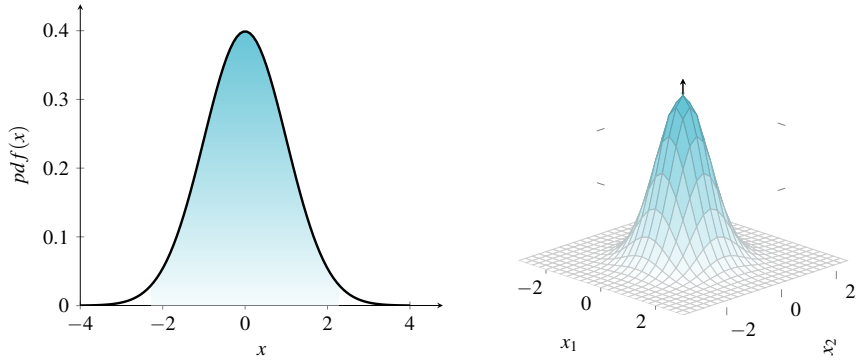
- The diagonal elements of Σ are $\sigma(X_i, X_i) \equiv \sigma^2_{X_i} \equiv Var(X_i)$. *Sigma* is a symmetric positive semi-definite matrix.

Now, using the notion of random vectors, joint distributions and covariance matrix we can define *multivariate normal distributions*.

Definition 1.2.5 A random vector $X := (X_1, \ldots, X_d)^\top$ has a *multivariate normal distribution* with expectation μ and covariance matrix (see definition below) Σ if it has a joint PDF of the form:

$$f(X) = \frac{1}{\sqrt{(2\pi)^d |\Sigma|}} \exp\left\{-\frac{1}{2}(X-\mu)^\top \Sigma^{-1} (X-\mu)\right\}$$

In this case we write: $X \sim \mathcal{N}(\mu, \Sigma)$



(a) *Univariate Gaussian* $\mathcal{N}(0,1)$ ***(b)*** *Bivariate Gaussian* $\mathcal{N}(0, I_2)$

Figure 1.2: *Visualization of Uni- and Bivariate standard normal distributions*

Observe that Definition 1.2.5 is a generalization of Definition 1.1.2, i.e. when $d = 1$ both definitions are same. In the case of modeling human weight and height suppose the covariance between the properties is 0.2. We then denote the bi-variate normal distribution and the samples drawn from it by:

$$\mathbf{x}_1, \ldots, \mathbf{x}_m \overset{i.i.d}{\sim} \mathcal{N}\left(\begin{bmatrix} 75 \\ 170 \end{bmatrix}, \begin{bmatrix} 3 & 0.2 \\ 0.2 & 5 \end{bmatrix}\right)$$

Sometimes, we are interested only in how a subset of the variates distributes, without the influence of the rest. For example what is the distribution of human height only. To do so, we would like to look at the *marginal distribution* of that subset.

Definition 1.2.6 The *marginal distribution* of a subset of coordinates of random variables with a joint probability distribution, is the probability distribution of the variables in the set:

$$f(\mathbf{x}) = \int_{\mathbf{y}} f(\mathbf{x},\mathbf{y})\, d\mathbf{y}$$

where the $\mathbf{y}$ integration is over all the random variables not in $\mathbf{x}$.

Let us find the marginal distribution of a bi-variate Gaussian. Let $\mathbf{x} \sim \mathcal{N}(\mu,\Sigma)$ where $\mathbf{x} \in \mathbb{R}^2$ and

$$\mu = (\mu_1,\mu_2)^\top, \quad \Sigma = \begin{bmatrix} \sigma_1^2 & 0 \\ 0 & \sigma_2^2 \end{bmatrix}$$

To find the PDF of the marginal distribution of (w.l.o.g) x_1, Observe that we can write the PDF as follows:

$$\begin{aligned} f(\mathbf{x}) &= \frac{1}{\sqrt{(2\pi)^2|\Sigma|}} \exp\left(-\frac{1}{2}(\mathbf{x}-\mu)^\top \Sigma^{-1}(\mathbf{x}-\mu)\right) \\ &= \frac{1}{\sqrt{(2\pi)^2\sigma_1^2\sigma_2^2}} \exp\left(-\frac{1}{2}\begin{bmatrix} x_1-\mu_1 & x_2-\mu_2 \end{bmatrix}\begin{bmatrix} \sigma_1^{-2} & 0 \\ 0 & \sigma_2^{-2} \end{bmatrix}\begin{bmatrix} x_1-\mu_1 \\ x_2-\mu_2 \end{bmatrix}\right) \\ &= \frac{1}{\sqrt{(2\pi)^2\sigma_1^2\sigma_2^2}} \exp\left(-\frac{1}{2}\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2 - \frac{1}{2}\left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right) \\ &= \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{1}{2}\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2\right) \cdot \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{1}{2}\left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right) \end{aligned}$$

Using the definition of the marginal distribution:

$$\begin{aligned} f(x_1) &= \int_{-\infty}^{\infty} f(x_1,x_2)\, dx_2 \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{1}{2}\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2\right) \cdot \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{1}{2}\left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right) dx_2 \\ &= \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{1}{2}\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2\right) \cdot \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{1}{2}\left(\frac{x_2-\mu_2}{\sigma_2}\right)^2\right) dx_2 \end{aligned}$$

Notice that now we integrate a function of a uni-variate Gaussian for all values $x_2 \in (-\infty,+\infty)$. Therefore this integral equals to 1 and we are left with:

$$f(x_1) = \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{1}{2}\left(\frac{x_1-\mu_1}{\sigma_1}\right)^2\right)$$

Which by definition 1.1.2 is a univariate Gaussian of the form $x_1 \sim \mathcal{N}(\mu_1,\sigma_1^2)$. Notice that this result is to be expected. The covariance between the two properties is zero, namely they are uncoordinated and as such they do not influence each others distribution.

1.2.1 Estimators of Multivariate Gaussian Distribution

Just as we were interested in estimating parameters in the univariate case so we are in the multivariate case. The sample mean estimator of a multivariate distribution is simply the univariate estimator in each of the coordinates:

$$\hat{\mu} := \begin{bmatrix} \vdots \\ \hat{\mu}_j \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \frac{1}{m}\sum_i x_{i,j} \\ \vdots \end{bmatrix} \tag{1.14}$$

To define an estimator for the covariance matrix we must first define an estimator for the sample covariance between two random variables. The unbiased estimator of the *sample covariance* of the i'th and j'th random

variables is given by:

$$\hat{\sigma}(X_i, X_j) = \frac{1}{m-1}\sum_{k=1}^{m}(x_{k,i} - \hat{\mu}_i)(x_{k,j} - \hat{\mu}_j) \tag{1.15}$$

where $\hat{\mu}_i$ is the sample mean of the random variable X_i.
In particular, notice that for the case where $i = j$ we are left with the unbiased estimator previously seen. We can now define the sample covariance matrix $\hat{\Sigma}$:

Definition 1.2.7 — Sample Covariance Matrix. Let $X = (X_1, \ldots, X_d)^\top$ be a d-dimensional random vector. Let $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^d$ be m i.i.d samples realizing X.. The ***sample covariance matrix*** is a square d-by-d matrix $\hat{\Sigma}$ such that $\hat{\Sigma}_{i,j} = \hat{\sigma}(X_i, X_j) \quad i, j = 1, \ldots, d$.

In matrix notation, for $\mathbf{X} \in \mathbb{R}^{m \times d}$ the matrix whose rows are the samples $\mathbf{x}_1, \ldots, \mathbf{x}_m$, the (biased) estimator for the sample covariance matrix is given by:

$$\hat{\Sigma} \coloneqq \frac{1}{m}\sum_{i=1}^{m}(\mathbf{x}_i - \hat{\mu})(\mathbf{x}_i - \hat{\mu})^\top = \frac{1}{m}\widetilde{\mathbf{X}}^\top\widetilde{\mathbf{X}}$$

for $\widetilde{\mathbf{X}}$ being the centered matrix: $\widetilde{\mathbf{X}}_{\cdot,i} \coloneqq \mathbf{X}_{\cdot,i} - \hat{\mu}$. The unbiased estimator is given by:

$$\hat{\Sigma} \coloneqq \frac{1}{m-1}\sum_{i=1}^{m}(\mathbf{x}_i - \hat{\mu})(\mathbf{x}_i - \hat{\mu})^\top = \frac{1}{m-1}\widetilde{\mathbf{X}}^\top\widetilde{\mathbf{X}}$$

■ **Example 1.3** Let $\mathbf{X} = \begin{pmatrix} 150 & 45 \\ 170 & 74 \\ 184 & 79 \end{pmatrix}$ be samples of height and weight of 3 different individuals. To calculate the sample covariance matrix we begin with centering the data. That is, subtract the empirical mean from each sample. The sample mean is: $\hat{\mu} = (168, 66)^\top$, so:

$$\mathbf{X}_{centered} = \mathbf{X} - \begin{pmatrix} 168 & 66 \\ 168 & 66 \\ 168 & 66 \end{pmatrix} = \begin{pmatrix} 150 & 45 \\ 170 & 74 \\ 184 & 79 \end{pmatrix} - \begin{pmatrix} 168 & 66 \\ 168 & 66 \\ 168 & 66 \end{pmatrix} = \begin{pmatrix} -18 & -21 \\ 2 & 8 \\ 16 & 13 \end{pmatrix}$$

Now, following the definition of the sample covariance matrix:

$$\hat{\Sigma} = \frac{1}{3-1}\mathbf{X}_{centered}^\top\mathbf{X}_{centered} = \begin{pmatrix} 292 & 301 \\ 301 & 337 \end{pmatrix}$$

■

1.3 Summary, Labs & Exercises

Exercises

Theoretical Questions

1. Let $x_1, x_2, \ldots \overset{i.i.d}{\sim} \mathcal{P}$ be a sample of infinity size drawn from some probability distribution function $\mathcal{P}$ with finite expectation and variance. Show that the sample mean estimator $\hat{\mu}_n = \frac{1}{n}\sum x_i$ calculated over the first n samples is a consistent estimator.

2. Consider the estimator of sample variance with *unknown* sample mean defined as $\hat{\sigma}^2 = \frac{1}{m}\sum(x_i - \hat{\mu})^2$, for $\hat{\mu}$ the sample mean estimator. Show that this is a biased estimator and find its systematic error.

3. Consider the estimator of sample variance with *known* sample mean defined as $\hat{\sigma}^2 := \frac{1}{m}\sum(x_i-\mu)^2$. Show that this is an unbiased estimator. Explain why the estimator in the question above is biased while the current estimator is unbiased.

4. Consider the estimator of sample variance with *unknown* sample mean defined as $\hat{\sigma}^2 = \frac{1}{m-1}\sum(x_i-\hat{\mu})^2$, for $\hat{\mu}$ the sample mean estimator. Show that this is an unbiased estimator.

5. Let $x_1,\ldots,x_m \overset{i.i.d}{\sim} \mathcal{N}\left(\mu,\sigma^2\right)$. Derive the MLE for the variance σ^2 and show that it is in fact the estimator seen in question Ex.2.

6. Let $\mathbf{x}_1,\ldots,\mathbf{x}_m \overset{i.i.d}{\sim} \mathcal{N}(\mu,\Sigma)$ be m observations sampled i.i.d from a multivariate Gaussian with expectation of $\mu \in \mathbb{R}^d$ and a covariance matrix $\Sigma \in \mathbb{R}^{d\times d}$. Derive the likelihood function of $\mathcal{N}(\mu,\Sigma)$. Hint: follow the approach used to derive the likelihood function for the univariate case (1.6).

7. Prove that multivariate Gaussian distributions are closed under affine transformations. That is, for $\mathbf{x} \sim \mathcal{N}(\mu,\Sigma)$, $\mu \in \mathbb{R}^d$, $\Sigma \in \mathbb{R}^{d\times d}$ and fixed $A \in \mathbb{R}^{m\times d}, b \in \mathbb{R}^m$ then $A\mathbf{x}+b$ follows a multivariate Gaussian distribution. What is the expectation and covariance matrix?

8. Let $X \sim \mathcal{N}(\mu,\Sigma)$ be a multivarite Gaussian distribution with $\mu \in \mathbb{R}^d$ and $\Sigma \in \mathbb{R}^{d\times d}$. Denote $X = [X_1|X_2]^\top$ some partitioning of the coordinates of X. Prove that the conditional distribution $X_1|X_2$ is also a multivariate Gaussian and find its expectation and covariance matrix.

9. Let $X \sim \mathcal{N}(\mu,\Sigma)$ be a multivarite Gaussian distribution with $\mu \in \mathbb{R}^d$ and $\Sigma \in \mathbb{R}^{d\times d}$. Denote $X = [X_1|X_2]^\top$ some partitioning of the coordinates of X. Prove that the marginal distribution X_1 is also a multivariate Gaussian and find its expectation and covariance matrix.

Practical Questions

Clone the IML.HUJI GitHub repository and setup a working python environment as explained on GitHub page.

1. Implement the `fit, pdf` and `log_likelihood` functions in class `UnivariateGaussian`, file `learners.GaussianEstimators.py`. Follow the details specified in class and function documentation.
   (a) Using `numpy.random.normal` draw 1000 samples $x_1,\ldots,x_{100} \overset{i.i.d}{\sim} \mathcal{N}(10,1)$ and fit a univariate Gaussian. What are the estimations of the expectation and variance?

   (b) Over previously drawn samples, fit a series of models of increasing samples size: 10, 20,...,100, 110,...1000. Plot the absolute distance between the estimated- and true value of the expectation, as a function of the sample size. What estimator property are we able to conclude for the sample mean estimator?

   (c) Compute the PDF of the previously drawn samples using the model fitted above (over all samples) and plot the empirical PDF distribution.

   (d) Over a sample $S = \{1,5,2,3,8,-4,-2,5,1,10,-10,4,5,2,7,1,1,3,2,-1,-3,1,-4,1,2,1\}$ which of the following models is more likely to have generated these samples: $\mathcal{N}(1,1)$ or $\mathcal{N}(10,1)$?

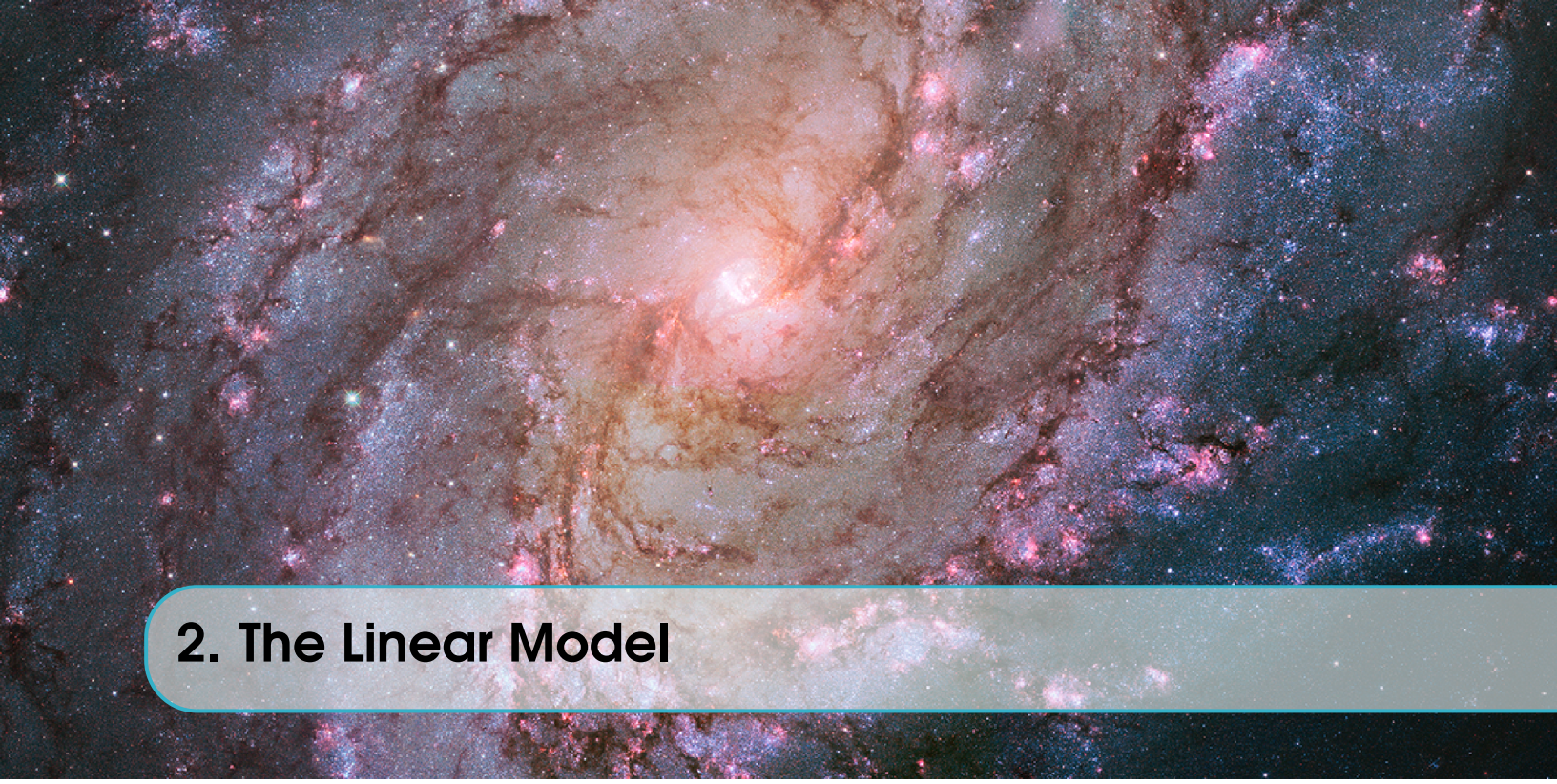
2. Implement the `fit, pdf` and `log_likelihood` functions in class `MultivariateGaussian`, file `learners.GaussianEstimators.py`. Follow the details specified in class and function documentation.

(a) Using `numpy.random.multivariate_normal` draw 1000 samples $\mathbf{x}_1, \ldots, \mathbf{x}_{1000} \overset{i.i.d}{\sim} \mathcal{N}(\mu, \Sigma)$

$$\mu = \begin{bmatrix} 0 \\ 0 \\ 4 \\ 0 \end{bmatrix}, \quad \Sigma = \begin{bmatrix} 1 & 0.2 & 0 & 0.5 \\ 0.2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0.5 & 0 & 0 & 1 \end{bmatrix}$$

Fit a multivariate Gaussian and evaluate the estimated expectation and covariance matrix with respect to the true parameters.

(b) Using the samples drawn in the question above calculate the log-likelihood for models with expectation $\mu = [f_1, 0, f_3, 0]^\top$ and the true covariance matrix defined above, where f_1, f_3 get values returned from `np.linspace(-10, 10, 200)`. Plot a heatmap of $f1$ values as rows, f_3 values as columns and color coded by the calculated log likelihood. What can be learned from the plot? What configuration of (f_1, f_3) values achieved maximal likelihood?



2. The Linear Model

2.1 Batch Supervised Regression Models

Machine learning models can be designed to accomplish many different tasks. We'll start with a very common task: *batch supervised regression on the domain* $\mathbb{R}^d$. To understand what the words "batch", "supervised", "regression" and "on the domain $\mathbb{R}^d$" mean in the context of machine learning, here is an example.

Imagine we work for an online store and would like to predict the "customer lifetime value", that is, the total future net revenue that an online customer will provide to the store. To do so, we choose different customer properties that we think might be relevant such as age, income, total spending in the website, average monthly visits, etc. Suppose that we choose d different properties. The vector space defined over all possible values of these d properties (commonly called *d features*) is our *sample domain*. We denote it by $\mathcal{X}$. In our example, $\mathcal{X} := \mathbb{R}^d$, where d the number of features we will use. The set containing all the possible values for the quantity we want to predict is called the *response set* and denoted $\mathcal{Y}$. In our example, this set contains all possible customers' lifetime value, so that we can use $\mathcal{Y} = \mathbb{R}$.

A machine learning problem where we are given a *sample* $x \in \mathcal{X}$, and would like to predict a *label* $y \in \mathcal{Y}$ associated with it, is called a *prediction problem*. When our prediction for the label of a new sample $x \in \mathcal{X}$ is to be based on past observations of pairs $(x, y) \in \mathcal{X} \times \mathcal{Y}$, we say that the learning problem *supervised*. When the sample domain is the Euclidean space $\mathcal{X} = \mathbb{R}^d$, we can say that each sample is a features vector with d features. When the label set is the real line $\mathcal{Y} = \mathbb{R}$, we say that the prediction problem is a *regression problem*. So we now know what the phrase "supervised regression prediction learning problem on the domain $\mathbb{R}^d$" means.

How can we predict customer lifetime value? It makes sense to start by collecting all the d features we chose for m customers, for who we already know the lifetime value. This way, we can hope to detect patterns that relate the d features of a customer $x \in \mathbb{R}^d$ to their lifetime value $y \in \mathbb{R}$. This set of m *observations*, of the form $S = \{(x_i, y_i)\}_{i=1}^m$ will be our *training sample* or *training dataset*. We denote it by S. We would like to use our training dataset to find a way to predict, as accurately as possible, the lifetime values of any new customer using solely their feature vector. This setup, where we are given a training set of m labeled samples, and would

like to use them in order to create a prediction rule that can predict the label of any new sample $\mathbf{x} \in \mathcal{X}$ we may encounter, is called *batch supervised learning*.

A *prediction model* is a way to represent a functional relation that maps a sample $x \in \mathcal{X}$ to a response $\in \mathcal{Y}$. So, we will *assume* that there exists some function $f : \mathcal{X} \to \mathcal{Y}$ that captures the relation we are interested in for each sample $x \in \mathcal{X}$ and its response $y \in \mathcal{Y}$. This function f is unknown to us and we would like to find it. It may be deterministic or it may contain a random component.

For simplicity, let us begin by assuming that the functional relation between $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ is *deterministic*. So we assume that there exists a function $f : \mathcal{X} \to \mathcal{Y}$ such that, each sample we observe, now or in the future, is of the form (x, y) with $y = f(x)$. In particular for our training set $y_i = f(x_i)$ for every training sample $i = 1, \ldots, m$. Our goal is to *learn* f from a training sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, so we can estimate or predict the value $f(x)$ for a new value x. A sample we haven't seen in our training set – a new sample – is sometimes called a *test* sample. Using the training sample, which we denote by S, we will create a function that we hope is as similar as possible to the unknown function f. This function is the *prediction rule* or *decision rule* and we denote it by $\hat{f}$ or h_S. (The notation h_S emphasizes that our prediction rule very much depends on the training sample S).

For reasons we discuss later (section 4.2), whenever we try to model a functional relation f, we restrict ourselves to functions f in a specified family of functions. Such a family is referred to as a *hypothesis class*. While we can build regression models over any domain $\mathcal{X}$, the simplest domain to consider is the Euclidean space $\mathbb{R}^d$ where each point x is a feature vector with d real numbers. In this chapter (and in most of this book) we consider the case $\mathcal{X} := \mathbb{R}^d$.

2.1.1 The Linear Regression Model

Let us assume that the relation $\mathcal{X} \to \mathcal{Y}$ is *linear*. This is perhaps the simplest relation we can describe. Formally, we define the *linear model*, or the *linear hypothesis class*, as the set of linear functions from the domain set to the response set:

$$\mathcal{H}_{reg} := \left\{ h(x_1, \ldots, x_d) = w_0 + \sum_{i=1}^{d} x_i w_i \;\middle|\; w_0, w_1, \ldots, w_d \in \mathbb{R} \right\}. \tag{2.1}$$

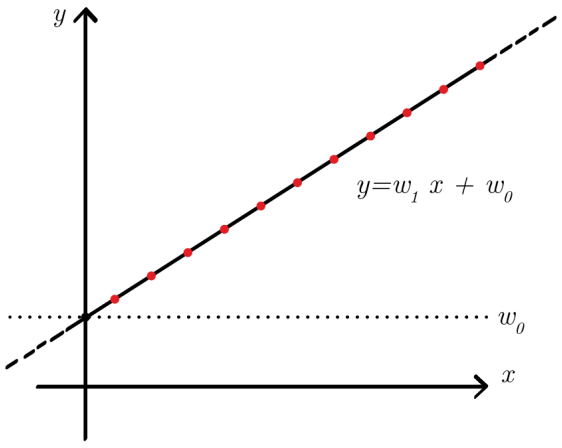


Figure 2.1: *Illustration of a linear regression model with $\mathcal{X} = \mathbb{R}$ and $\mathcal{Y} = \mathbb{R}$. Red dots are samples. The solid curve is the learned prediction rule $\hat{f}$.*

2.1.2 Linear Regression

Let us assume that the relation $\mathcal{X} \to \mathcal{Y}$ is *linear*. This is perhaps the simplest relation we can describe. Formally, we define the *linear model*, or the *linear hypothesis class*, as the set of linear functions from the domain set to the response set:

$$\mathcal{H}_{reg} := \left\{ h(x_1,\ldots,x_d) = w_0 + \sum_{i=1}^{d} x_i w_i \;\middle|\; w_0, w_1, \ldots, w_d \in \mathbb{R} \right\} \tag{2.2}$$

In statistics, learning f from a training sample is known as *linear regression*[1]. Each function $h \in \mathcal{H}_{reg}$ is characterized by the *weights* (also known as regression coefficients) $w_1,\ldots,w_d$ representing the d features and an *intercept* w_0. To simplify the notation, for a given sample $\mathbf{x} = (x_1,\ldots,x_d)^\top \in \mathbb{R}^d$ we add a zero-th coordinate with the value of 1, and define $\mathbf{x} = (1,x_1,\ldots,x_d)^\top \in \mathbb{R}^{d+1}$. Using this notation each function in the linear hypothesis class can be written in the form $h(\mathbf{x}) := \langle \mathbf{x}, \mathbf{w} \rangle = \mathbf{x}^\top \mathbf{w}$. For the remainder of this chapter, we will assume that the intercept is already incorporated into the weights vectors, so we can define linear hypothesis class equivalently as

$$\mathcal{H}_{reg} := \left\{ h_{\mathbf{w}}(\mathbf{x}) = \mathbf{x}^\top \mathbf{w} \mid \mathbf{w} \in \mathbb{R}^{d+1} \right\} \tag{2.3}$$

Note that by convention, the first coordinate of $\mathbf{w}$ is the intercept w_0.So, given a training set S, we are looking for a vector $\mathbf{w} \in \mathbb{R}^{d+1}$ such that $y_i = \mathbf{x}_i^\top \mathbf{w}$ for all $i \in [m]$.

The regression matrix

Let us arrange the training data $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ in matrix form. We define the *response vector* as the column vector $\mathbf{y} \in \mathbb{R}^m$ and the *regression matrix* (or *design matrix*) $\mathbf{X} \in \mathbb{R}^{m \times (d+1)}$ as follows.

$$\mathbf{X} = \begin{bmatrix} — & \mathbf{x}_1 & — \\ — & \mathbf{x}_2 & — \\ & \vdots & \\ — & \mathbf{x}_m & — \end{bmatrix} \qquad \mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}$$

Note that m rows of $\mathbf{X}$ represent our m training samples and the $d+1$ columns of $\mathbf{X}$ represent the intercept and d features. In this notation, we are looking for a vector $\mathbf{w} \in \mathbb{R}^{d+1}$ that satisfies a system of m linear equations in the variable $\mathbf{w}$,

$$\mathbf{X}\mathbf{w} = \mathbf{y} \tag{2.4}$$

At this point, we will assume that $m \geq d+1$, namely, that we have *enough training samples* so that the linear system (2.4) is *not under-determined*. In practical terms, this means that we have at least as many training samples as we have features. In our online store example, this means that we must collect data on $m \geq d+1$ customers before we start training our regression model, where d is the number of features we collect on each customer (e.g. age, income, total spending, number of monthly visits to the website, etc).

2.1.3 Designing A Learning Algorithm

2.1.3.1 Realizablity

Recall that to derive the problem of finding $\mathbf{w} \in \mathbb{R}^{d+1}$ that satisfies (2.4) we have restricted ourselves to describing functional relations $\mathcal{X} \xrightarrow{f} \mathcal{Y}$ such that $f \in \mathcal{H}_{reg}$. The case where there exists a solution for (2.4) is called the *Realizable* case. Let $\hat{\mathbf{w}}$ be a solution for (2.4), then the prediction rule we choose is $\hat{f}(\mathbf{x}) = \mathbf{x}^\top \hat{\mathbf{w}}$.

The case where there is no $f \in \mathcal{H}_{reg}$ that satisfies the system of equations (i.e there is no solution for the system) is called the *Non-Realizable* case. In this case, since we decided to choose a prediction rule in

[1] The name "regression" refers to a statistical phenomenon known as "regression to the mean".

$\mathcal{H}_{reg}$, we must settle for finding $\hat{f} \in \mathcal{H}_{reg}$ which is *"most fitting"* for our purposes.

Our learning algorithm for linear regression must address both the realizable and non-realizable cases. In the realizable case, to find the rule f, all we need to do is solve the linear system (2.4) for $\mathbf{w}$. But what will we do in the non-realizable case, where $f \notin \mathcal{H}_{reg}$? How should we choose the prediction rule $\hat{f}$?

2.1.3.2 Empirical Risk Minimization

As we have seen in the previous chapter (subsubsection 1.1.2.1), one way to choose $\hat{f} \in \mathcal{H}_{reg}$ in the non-realizable case is to assign each $f \in \mathcal{H}_{reg}$ with some measure of quality, through the use of some *loss function*. This function will provide a measure of quality for the hypothesis by comparing between the true- and predicted values:

$$\sum_{i=1}^{m} L\left(f(\mathbf{x}_i), \hat{f}(\mathbf{x}_i)\right), \quad i = 1, \ldots, m$$

Two commonly used loss functions for regression problems are the *Absolute Value Loss* and *Squared Loss* functions.

$$L\left(y, \hat{f}(\mathbf{x})\right) := \left|y - \hat{f}(\mathbf{x})\right|, \quad L\left(y, \hat{f}(\mathbf{x})\right) := \left(y - \hat{f}(\mathbf{x})\right)^2$$

We focus on the linear regression setup when using the square loss function. As we are concerned for the performance of an estimator $\hat{f}$ on a new data point $\mathbf{x}$, we hope to minimize the *risk* (i.e. expected loss, 1.1.4) embodied in choosing $\hat{f}$ as our estimator, with respect to the squared loss:

$$\mathcal{R}\left(f, \hat{f}\right) := \mathbb{E}_{\mathbf{x}}\left[L\left(f(\mathbf{x}), \hat{f}(\mathbf{x})\right)\right] = \mathbb{E}_{\mathbf{x}}\left[\left(f(\mathbf{x}), \hat{f}(\mathbf{x})\right)^2\right]$$

where the expectation is taken over the selection of the test sample $\mathbf{x}$. However, as we do not have access to the underlying distribution and only have the training set, we will evaluate this risk *empirically*, that is, over *the training data*. And so, using the sample mean as an estimator of the expectation, the *empirical risk* embodied in choosing $\hat{f}$ (with respect to the squared loss) is

$$\frac{1}{m}\sum_{i=1}^{m}\left(y_i - \hat{f}(\mathbf{x}_i)\right)^2$$

In the case of the square loss, the empirical risk of the linear function $\hat{f}(\mathbf{x}_i) = \mathbf{x}_i^\top \hat{\mathbf{w}}$ is given by:

$$\frac{1}{m}\sum_{i=1}^{m}\left(y_i - \mathbf{x}_i^\top \hat{\mathbf{w}}\right)^2 = \frac{1}{m}||\mathbf{y} - \mathbf{X}\hat{\mathbf{w}}||^2 = \frac{1}{m}\left(\mathbf{y} - \mathbf{X}\hat{\mathbf{w}}\right)^\top \left(\mathbf{y} - \mathbf{X}\hat{\mathbf{w}}\right) \tag{2.5}$$

We will then pick the estimator which *minimizes* the empirical risk. This strategy for choosing $\hat{f}$ is known as *Empirical Risk Minimization* (ERM). Since we are in search of the minimizer we often omit the constant value of $\frac{1}{m}$.

2.1.3.3 Least Squares Optimization Problem

Minimizing the empirical risk of (2.5) means minimizing the sum of squares of the deviations of the responses from a linear function. In other words, we choose the linear function in $\mathcal{H}_{reg}$ that is closest to the responses in terms of the squared error distance. The deviation $y_i - \mathbf{x}_i^\top \mathbf{w}$ is called the i-th *residual* and the total empirical risk in our case is called *Residual Sum of Squares* (or *RSS*):

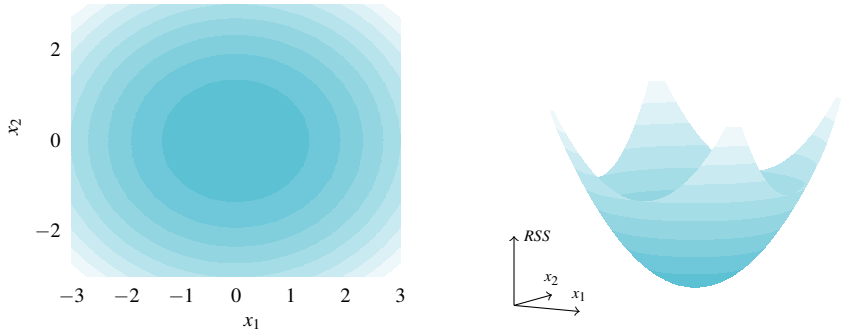
$$RSS_{\mathbf{X},\mathbf{y}}(\mathbf{w}) := ||\mathbf{y} - \mathbf{X}\mathbf{w}||^2$$

To simplify notation we often write $RSS(\mathbf{w})$ keeping the dependence on $\mathbf{X}, \mathbf{y}$ implicit. So to learn the linear function by empirical Risk minimization we want to find

$$\underset{\mathbf{w}\in\mathbb{R}^d}{\operatorname{argmin}}\ RSS(\mathbf{w}) = \underset{\mathbf{w}\in\mathbb{R}^d}{\operatorname{argmin}}\ ||\mathbf{y} - \mathbf{X}\mathbf{w}||^2 \tag{2.6}$$

It is important to notice that the optimization problem (2.15) addresses both the realizable and non-realizable cases:

- In the realizable case, as $\mathbf{y} \in Im(\mathbf{X})$ we know there exists at least one solution $\widehat{\mathbf{w}}$ such that $\mathbf{X}\widehat{\mathbf{w}} = \mathbf{y}$. Such a solution will achieve a value of zero. As the RSS function is bounded below by zero, such a solution is therefore a minimizer of the RSS.
- In the non-realizable case, as $\mathbf{y} \notin Im(\mathbf{X})$ there is no solution $\widehat{\mathbf{w}}$ such that $\mathbf{X}\widehat{\mathbf{w}} = \mathbf{y}$. Therefore, no vector $\widehat{\mathbf{w}}$ will achieve a value of zero for the RSS objective. Instead, we decide to find a vector that is "good enough" in the sense of minimizing the squared loss.



(a) *Contour lines of the RSS function*

(b) *3D visualization of the paraboloid defined by the RSS*

Figure 2.2: *Visualization of RSS function*

A *necessary* condition for $\mathbf{w}$ to be a minimizer of the function $||\mathbf{y} - \mathbf{X}\mathbf{w}||^2$ is that all its partial derivative vanish at $\mathbf{w}$. Recalling the definition of the inner product, this condition can be written as:

$$\frac{\partial}{\partial w_j} RSS(\mathbf{w}) = -2\sum_{i=1}^{m} (\mathbf{x}_i)_j \cdot (y_i - \mathbf{x}_i\mathbf{w}) = 0 \tag{2.7}$$

for all $j = 0, \ldots, d$, where $(\mathbf{x}_i)_j$ is the j-th entry of $\mathbf{x}_i$. It is the $x_{j,i}$ element of the matrix $\mathbf{X}$. Notice that this constructs a system of $d+1$ linear equations in $\mathbf{w}$. We can organize (2.7) as such to get the form below. Recall that we have already derived this function in .11.

$$\nabla RSS(\mathbf{w}) = -2\mathbf{X}^\top (\mathbf{y} - \mathbf{X}\mathbf{w}) = 0 \tag{2.8}$$

2.1.3.4 The Normal Equations

So a minimizer of (2.15) must also be a solution for the following linear system, known as the **Normal Equations**:

$$\mathbf{X}^\top (\mathbf{y} - \mathbf{X}\mathbf{w}) = 0 \quad \Longleftrightarrow \quad \mathbf{X}^\top \mathbf{y} = \mathbf{X}^\top \mathbf{X}\mathbf{w} \tag{2.9}$$

Geometric Interpretation

Let us derive a geometric interpretation of linear regression and gain a better understanding what the solution to (2.9) might be like. We usually think of $\mathbf{X} \in \mathbb{R}^{m \times (d+1)}$ as a matrix that consists of m rows, one for each training sample. Instead, we can equivalently think of $\mathbf{X}$ as a matrix that consists of $d+1$ columns, one for each feature (and the intercept). Define

$$\mathbf{X} := \begin{bmatrix} | & & | \\ \varphi_0 & \cdots & \varphi_d \\ | & & | \end{bmatrix}$$

and recall that the vector space spanned by the columns of $\mathbf{X}$ is:

$$span(\varphi_0,\ldots,\varphi_d) = Im(\mathbf{X}) \subset \mathbb{R}^m$$

Since we assume $m \geq d+1$, $Im(\mathbf{X})$ is a linear subspace of $\mathbb{R}^m$. If we have many more samples than features, $m \gg d+1$, then $Im(\mathbf{X})$ is just a small subspace of $\mathbb{R}^m$. If we have the minimal number of samples possible, $m = d+1$, and the vectors $\varphi_0,\ldots,\varphi_d$ form an independent set, then the subspace fills the entire space: $Im(\mathbf{X}) = \mathbb{R}^m$.

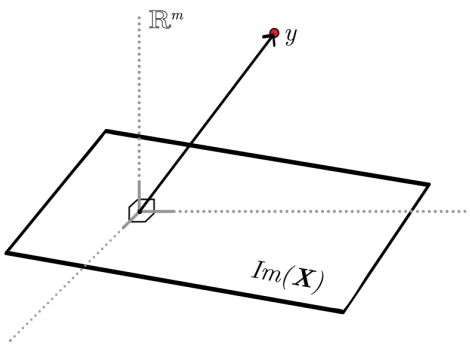
Now, consider the response vector $\mathbf{y} \in \mathbb{R}^m$:

- If $\mathbf{y} \in Im(\mathbf{X})$ then by definition $\mathbf{y}$ is a linear combination of $\varphi_0,\ldots,\varphi_d$ and there exists a vector $\mathbf{w} \in \mathbb{R}^{d+1}$ such that $\mathbf{X}\mathbf{w} = \mathbf{y}$. This is the realizable case. We can now differentiate between two sub-cases:
  - If $\varphi_0,\ldots,\varphi_d$ are linearly independent, then $\mathbf{y}$ can be expressed as a *unique* linear combination of the columns of $\mathbf{X}$. In this case the linear system (2.9) has a unique solution.
  - If however $\varphi_0,\ldots,\varphi_d$ are in fact linearly dependent, then there are infinitely many ways to express $\mathbf{y}$ as a linear combination of the columns of $\mathbf{X}$. Any one of these ways is a valid solution for (2.9).
- If $\mathbf{y} \notin Im(\mathbf{X})$ then $\mathbf{y}$ is not a linear combination of $\varphi_0,\ldots,\varphi_d$. As such there is no vector $\mathbf{w} \in \mathbb{R}^{d+1}$ that satisfies $\mathbf{X}\mathbf{w} = \mathbf{y}$. This is the non-realizable case. In this case we decided to choose the vector $\mathbf{w}$ for which $RSS(\mathbf{w}) = ||\mathbf{X}\hat{\mathbf{w}} - \mathbf{y}||$ is minimal.

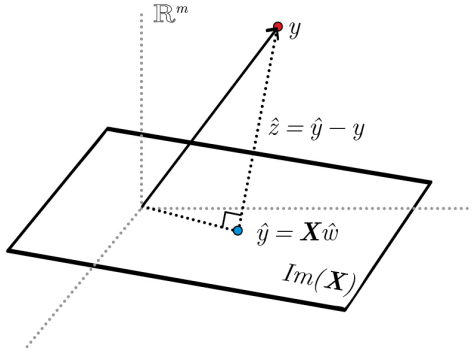
Now we are able to understand what is "normal" about the normal equations (2.9). Observe that the equations (2.7), from which we have derived the normal equations, can be equivalently written as

$$\langle \varphi_j, \mathbf{y} - \mathbf{X}\mathbf{w} \rangle = 0 \quad j = 0,\ldots,d \tag{2.10}$$

We conclude that $\mathbf{w}$ is a solution to the normal equations if and only if $\mathbf{y} - \mathbf{X}\mathbf{w}$ is perpendicular to $\varphi_0,\ldots,\varphi_d$. Since these vectors span the subspace $Im(\mathbf{X})$, another way to write this is $\mathbf{y} - \mathbf{X}\mathbf{w} \in Im(\mathbf{X})^{\perp}$.



(a) *In the non-realizable case, the response vector* $\mathbf{y}$ *lies outside* $Im(\mathbf{X})$*, the subspace spanned by the columns of* $\mathbf{X}$*. In this case there is no solution for the system* $\mathbf{X}\mathbf{w} = \mathbf{y}$*.*



(b) *If* $\hat{\mathbf{w}}$ *is a solution to the normal equations, then* $\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}}$ *is an orthogonal projection of the response vector* $\mathbf{y}$ *onto* $Im(\mathbf{X})$*. The difference* $\hat{\mathbf{z}} = \mathbf{y} - \hat{\mathbf{y}}$ *is therefore perpendicular (normal) to* $Im(\mathbf{X})$*.*

Figure 2.3: Geometric interpretation of linear regression

Let $\hat{\mathbf{w}}$ be a solution to the normal equations and define $\hat{\mathbf{y}} \coloneqq \mathbf{X}\hat{\mathbf{w}}$. Note that $\hat{\mathbf{y}}$, the vector where the i-th entry is

the prediction on the i-th training sample $\mathbf{x}_i$, is $\hat{\mathbf{y}} \in Im(\mathbf{X})$. In this notation, when solving the normal equations, namely when seeking to minimize the RSS, we minimize $||\mathbf{y}-\hat{\mathbf{y}}||^2$. Define the *residual vector* $\hat{\mathbf{z}} := \mathbf{y}-\hat{\mathbf{y}}$. Note that from (2.10) we get that $\hat{\mathbf{z}} \in Im(\mathbf{X})^{\perp}$. In other words, if $\hat{\mathbf{w}}$ is a solution to the normal equations then $\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}}$ is the *orthogonal projection* of $\mathbf{y}$ on $Im(\mathbf{X})$ and $\hat{\mathbf{z}} = \mathbf{y}-\hat{\mathbf{y}}$ is a *normal* (a perpendicular vector) to $Im(\mathbf{X})$. Hence the name the "normal equations".

Solving The Normal Equations

As we have seen, from a geometric perspective, if $m \geq d+1$, solving the normal equations means finding a vector $\hat{\mathbf{w}}$ such that $\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}}$ is the orthogonal projection of $\mathbf{y}$ on $Im(\mathbf{X})$. We can deduce from this two important facts about the existence and uniqueness of a solution to the normal equations:

- **Existence:** As a linear system, the normal equations can have either (i) no solutions, (ii) a unique solution, or (iii) an infinite number of solutions that constitute an affine subspace. From the geometric interpretation we see that (i) is impossible. Indeed it can be shown that the normal equations must have at least one solution, so that they have a unique solution or an infinite number of solutions.
- **Uniqueness:**
  - If the columns of $\mathbf{X}$ form a linearly independent set (equivalently, if $dim(Ker(\mathbf{X})) = 0$) then the projection $\hat{\mathbf{y}}$ can be described uniquely as a linear combination of the columns $\varphi_0, \ldots, \varphi_d$, namely, there exists a unique $\hat{\mathbf{w}}$ such that $\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}}$. This vector of coefficients $\hat{w}$ is a unique solution to the normal equations.
  - If the columns of $\mathbf{X}$ contain linear dependencies (equivalently, if $dim(Ker(\mathbf{X})) > 0$) then the projection $\hat{\mathbf{y}}$ can be described as infinitely many linear combinations of the columns $\varphi_0, \ldots, \varphi_d$. Any such linear combination will suffice and we simply need to find *one* vector $\hat{w}$ such that $\hat{y} = \mathbf{X}\hat{\mathbf{w}}$.

Case 1: Linearly Independent Feature Vectors

If the features are linearly independent then the kernel of $\mathbf{X}$ is trivial ($dim(Ker(\mathbf{X})) = 0$). Now, consider the square and symmetric matrix $\mathbf{X}^\top\mathbf{X}$. As $Ker(\mathbf{X}) = Ker(\mathbf{X}^\top\mathbf{X})$, then $\mathbf{X}^\top\mathbf{X}$ too has a trivial kernel. This means that $\mathbf{X}^\top\mathbf{X}$ is invertible and that a vector $\mathbf{w}$ satisfies $\mathbf{X}^\top\mathbf{y} = \mathbf{X}^\top\mathbf{X}\mathbf{w}$ if and only if $\mathbf{w} = \left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\mathbf{y}$. So in this case the unique solution to the normal equations is Ex.1

$$\hat{\mathbf{w}} := \left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\mathbf{y} \tag{2.11}$$

Lastly, as the RSS function is a convex function (.20) we conclude that the unique solution $\hat{\mathbf{w}}$ is a minimizer of the function.

Notice when deriving a geometric interpretation of the normal equations (Figure 2.3) we argued that the minimizer will orthogonally project $\mathbf{y}$ onto the subspace spanned by the columns of $\mathbf{X}$. Looking at $\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}} = \mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\mathbf{y}$ we indeed find that $\mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top$ is an orthogonal projection matrix onto the column space of $\mathbf{X}$. Ex.2

■ **Example 2.1** Let us find the estimator $\hat{\mathbf{w}}$ for the following scenario. Suppose we are interested in estimating the running times in a 100 meters long race, besed on an athlete's height and weight. We gathered the details of the 4 top ranking athletes in the 2016 Rio Olympics:

Athlete	Weight (kg)	Height (cm)	Running Time (sec)
Usain Bolt	94	195	9.81
Justin Gatlin	79	185	9.89
Andre de Grasse	70	176	9.91
Yohan Blake	80	180	9.93

So the features are the *weight, height* and the response is *running time*. To fit a linear regression model to the data we begin with arranging it in a matrix and adding the intercept:

$$\mathbf{X} := \begin{bmatrix} 1 & 94 & 195 \\ 1 & 79 & 185 \\ 1 & 70 & 176 \\ 1 & 80 & 180 \end{bmatrix}, \quad \mathbf{y} := \begin{bmatrix} 9.81 \\ 9.89 \\ 9.91 \\ 9.93 \end{bmatrix}$$

As we have proven above, the estimator is given by the closed form of $\hat{\mathbf{w}} := \left[\mathbf{X}^\top \mathbf{X}\right]^{-1} \mathbf{X}^\top \mathbf{y}$. Over given data we obtain that $\hat{\mathbf{w}} \approx (11.38, 0.003, -0.009)^\top$ (up to rounding up numbers).

Next, let us use this estimator to estimate the running times of a new sample $\mathbf{x} = (1, 74, 176)^\top$:

$$\hat{y} = \mathbf{x}^\top \hat{\mathbf{w}} = \left\langle \begin{bmatrix} 1 \\ 74 \\ 176 \end{bmatrix}, \begin{bmatrix} 11.38 \\ 0.003 \\ -0.009 \end{bmatrix} \right\rangle = 10.018$$

■

Case 2: Linearly Dependent Feature Vectors

Next, let us consider the case of features that are linearly dependent. In this case the columns of $\mathbf{X}$ are linearly dependent and $dim\left(Ker\left(\mathbf{X}\right)\right) > 0$. Therefore, there are infinitely many was to express the projection $\hat{\mathbf{y}}$ as a linear combination of the columns of $\mathbf{X}$. Since we need some way, it would be convenient if we could find a solution $\hat{\mathbf{w}}$ that is close to the origin in $\mathbb{R}^{d+1}$ (rather than a solution with very large norm, say). One way to do that is by using the SVD of $\mathbf{X}$.

Definition 2.1.1 Let $\mathbf{X} \in \mathbb{R}^{m \times (d+1)}$ and let $\mathbf{X} = U\Sigma V^\top$ be its SVD. The **Moore-Penrose pseudoinverse** of $\mathbf{X}$ is $\mathbf{X}^\dagger = V\Sigma^\dagger U^\top$ where $\Sigma^\dagger$ is a $(d+1) \times m$ diagonal matrix defined by:

$$\Sigma^\dagger_{i,i} = \begin{cases} 1/\Sigma_{i,i} & \Sigma_{i,i} \neq 0 \\ 0 & \Sigma_{i,i} = 0 \end{cases}$$

This is a generalization of the inverse matrix and indeed when the matrix $\mathbf{X}$ is invertible then then $\mathbf{X}^\dagger = \mathbf{X}^{-1}$. Using the definition above, let us find a minimizer of (2.15).

Claim 2.1.1 Let $\mathbf{X}, \mathbf{y}$ be a regression problem where $m \geq d+1$. If $dim(Ker(\mathbf{X})) \neq 0$ then $\hat{\mathbf{w}} = \mathbf{X}^\dagger \mathbf{y}$ is a minimizer of the RSS (2.15).

Proof. Denote the rank of $\mathbf{X}$ by r for which, since the kernel of $\mathbf{X}$ is non-trivial, $r\,[1, d+1)$. Let $X = U\Sigma V^\top$ be the SVD of $\mathbf{X}$ and $\sigma_1 \geq \ldots \geq \sigma_r > 0$. Recall the columns of U and V provide orthonormal bases for the four fundamental subspaces:

$$\begin{array}{llcl} U_{\mathcal{R}} \in \mathbb{R}^{m \times r} & \mathcal{R}\left(\mathbf{X}\right) & = & span\left\{\mathbf{u}_1, \ldots, \mathbf{u}_r\right\} \\ V_{\mathcal{R}} \in \mathbb{R}^{(d+1) \times r} & \mathcal{R}\left(\mathbf{X}^\top\right) & = & span\left\{\mathbf{v}_1, \ldots, \mathbf{v}_r\right\} \\ U_{\mathcal{N}} \in \mathbb{R}^{m \times (m-r)} & \mathcal{N}\left(\mathbf{X}^\top\right) & = & span\left\{\mathbf{u}_{r+1}, \ldots, \mathbf{u}_m\right\} \\ V_{\mathcal{N}} \in \mathbb{R}^{(d+1) \times (d+1-r)} & \mathcal{N}\left(\mathbf{X}\right) & = & span\left\{\mathbf{v}_{r+1}, \ldots, \mathbf{v}_{d+1}\right\} \end{array}$$

Denote $\mathcal{S} \in \mathbb{R}^{r \times r}$ the diagonal matrix with the r positive singular values on its main diagonal: $\mathcal{S} := diag\left(\sigma_1, \ldots, \sigma_r\right)$. Using these notations, recall the compact SVD form of $\mathbf{X}$ (3). So

$$\mathbf{X} := U\Sigma V^\top = \begin{bmatrix} U_{\mathcal{R}} & U_{\mathcal{N}} \end{bmatrix} \begin{bmatrix} \mathcal{S} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} V_{\mathcal{R}}^\top \\ V_{\mathcal{N}}^\top \end{bmatrix} = U_{\mathcal{R}} \mathcal{S} V_{\mathcal{R}}^\top = \widetilde{U}\widetilde{\Sigma}\widetilde{V}^\top$$

Now we solve the normal equations for $\mathbf{w}$, substituting $\mathbf{X}$ with its compact SVD form:

$$\begin{aligned}\mathbf{X}^\top\mathbf{y} &= \mathbf{X}^\top\mathbf{X}\mathbf{w}\\ \widetilde{V}\widetilde{\Sigma}^\top\widetilde{U}^\top\mathbf{y} &= \widetilde{V}\widetilde{\Sigma}^\top\widetilde{U}^\top\widetilde{U}\widetilde{\Sigma}\widetilde{V}^\top\mathbf{w}\\ \widetilde{\Sigma}\widetilde{U}^\top\mathbf{y} &= \widetilde{\Sigma}^2\widetilde{V}^\top\mathbf{w}\end{aligned}$$

Since $\widetilde{\Sigma}\in\mathbb{R}^{r\times r}$ of full rank then $\widetilde{\Sigma}^{-1}$ exists and therefore:

$$\mathbf{w} = \widetilde{V}\widetilde{\Sigma}^{-1}\widetilde{U}^\top\mathbf{y}$$

Lastly, using the Moore-Perose pseudoinverse definition we "expand" the compact SVD form and conclude that:

$$\begin{aligned}\hat{\mathbf{w}} &= \widetilde{V}\widetilde{\Sigma}^{-}1\widetilde{U}^\top\mathbf{y}\\ &= V\Sigma^\dagger U^\top\mathbf{y}\\ &= \mathbf{X}^\dagger\mathbf{y}\end{aligned}$$

■

An important property of the pseudoinvers is that for a linear system of equations $A\mathbf{x}=\mathbf{b}$ with an infinite number of solutions, then $A^\dagger\mathbf{b}$ is a solution with minimal ℓ_2 norm, namely

$$A^\dagger\mathbf{b} = \text{argmin}\left\{||\mathbf{x}||_2 \;\middle|\; A\mathbf{x}=\mathbf{b}\right\} \tag{2.12}$$

and therefore $\hat{\mathbf{w}} := X^\dagger\mathbf{y}$ is the solution closest to the origin with respect ot the Euclidean norm.

It can be shown that when dealing with a matrix of linearly independent columns ($dim\,(Ker\,(\mathbf{X}))=0$) then the previously found solution $\hat{\mathbf{w}}=\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\mathbf{y}$ equals to $\mathbf{X}^\dagger\mathbf{y}$. We conclude that the formula $\mathbf{X}^\dagger\mathbf{y}$ *always* gives us a solution to the normal equations: the unique solution if the solution is unique, and the solution with minimal ℓ_2 norm if not. Ex.4

Lastly, recall that when deriving a geometric intuition for what a minimizer of the normal equations should achieve, we realized that it would provide an orthogonal projection of $\mathbf{y}$ onto $Im\,(\mathbf{X})$. Indeed, in the non-singular form of solution then:

$$\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}} = \overbrace{\mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top}^{P_\mathbf{X}}\mathbf{y}$$

where $P_\mathbf{X}$ being square and symmetric is a projection matrix onto the range of $\mathbf{X}$:

$$P_\mathbf{X}^2 = \left(\mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\right)\left(\mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\right) = \mathbf{X}\left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top = P_\mathbf{X}$$

In the general case for $\hat{\mathbf{w}}=\mathbf{X}^\dagger\mathbf{y}$ then:

$$\begin{aligned}\hat{\mathbf{y}} &= \mathbf{X}\hat{\mathbf{w}} = \mathbf{X}\mathbf{X}^\dagger\mathbf{y} = U\Sigma V^\top V\Sigma^\dagger U^\top\mathbf{y} = U\Sigma\Sigma^\dagger U\mathbf{y}\\ &= U\left[\begin{array}{c|c} I_r & 0\\ \hline 0 & 0\end{array}\right]U^\top\mathbf{y} = U_\mathcal{R}U_\mathcal{R}^\top\mathbf{y} = \textstyle\sum_{i=1}^r \mathbf{u}_i\mathbf{u}_i^\top\mathbf{y}\end{aligned}$$

for $rank(\mathbf{X})=r$, providing an orthogonal projection matrix onto the range of $\mathbf{X}$.

R In this chapter we have only delt with the case where $m\geq d+1$, namely that we are more samples than features, and were therefore able to find solutions to the linear system. If however $m<d+1$ we do not have enough data to learn a map $\mathcal{X}\xrightarrow{f}\mathcal{Y}$. Our hypothesis class is a $d+1$ dimensional linear subspace, so to learn we require at least $d+1$ samples. In general, the larger d, the more complicated the more complex our hypothesis class and therefore the more samples we will need in order to learn it. This intuition will be further formulated in **??**.

2.1.4 Numerical Implementation Considerations

So far we have designed the learning algorithm. Now we want to *implement* it, namely, write efficient code that implements the algorithm that we have designed. The field of *numerical linear algebra* assists in addressing this challenge as the implementation of every machine learning algorithm is eventually reduced to performing linear algebra computations (e.g. matrix-vector or matrix-matrix products, matrix inverses and matrix decompositions). In the case of linear regression, as we have seen, to write software that trains a linear regression model, we need to be able to calculate a matrix SVD.

In your basic linear algebra courses you worked with mathematical objects over real and complex vector spaces. Likely, you did not stop to wonder how to compute (say) the inverse of a matrix on a computer. This is not as simple as it may sound. Computers do not calculate over $\mathbb{R}$, they use bits and more specifically floating-point arithmetics with finite precision. There is an entire field in the intersection of mathematics and computer science, known as numerical linear algebra, that studies the accuracy and complexity of algorithms for computing linear algebraic quantities and matrix decompositions. As a machine learning expert, you must be as knowledgable as possible regarding the numerical implementation of your learning algorithms. You should care *deeply* about how your algorithms are implemented and when they break numerically.

Let's see a simple example for a numerical consideration in our case of linear regression. (We will discover that the SVD is even more useful than we thought.) Recall that if $dim(Ker(\mathbf{X})) = 0$, and equivalently if $\mathbf{X}^\top\mathbf{X}$ is not singular (invertible) then we have a simple formula for training our linear regression model. But what happens if $\mathbf{X}^\top\mathbf{X}$ is "almost singular"?

Sometimes $\mathbf{X}^\top\mathbf{X}$ is formally invertible but *close to singular*. This happens if columns of $\mathbf{X}$ are almost co-linear or if one column of $\mathbf{X}$ is almost spanned by other columns. When this happens, if we are not careful we will run into numerical trouble. For example:

- Suppose we use the formula $\hat{\mathbf{w}} = \left[\mathbf{X}^\top\mathbf{X}\right]^{-1}\mathbf{X}^\top\mathbf{y}$ and try to compute $[\mathbf{X}^\top\mathbf{X}]^{-1}$ using (say) Gauss elimination, we'll find that Gauss elimination may yield wildly incorrect results.
- Suppose we use the pseudoinverse formula and compute $\mathbf{X}^\dagger$. When $\mathbf{X}^\top\mathbf{X}$ is close to singular, we'll discover that the smallest singular values σ_i of $\mathbf{X}$ are very very small; when we try to compute $1/\sigma_i$ for the pseudoinverse with floating-point arithmetics, $1/\sigma_i$ will not be precise.

There is a simple practical solution for this problem: we choose a "numerical precision threshold" $\varepsilon > 0$ in advance. We can choose, say, $\varepsilon := 10^{-8}$. We then change the definition of the pseudoinverse slightly and define

$$\Sigma^{\dagger,\varepsilon}_{i,i} = \begin{cases} 1/\sigma_i & \sigma_i > \varepsilon \\ 0 & \sigma_i \leq \varepsilon \end{cases}.$$

This ensures that even if the columns of $\mathbf{X}$ are close to being linearly dependent our implementation will be numerically stable.

2.1.5 A Statistical Model - Adding Noise

So far we assumed that the response y was a deterministic function of the sample $\mathbf{x}$, and that there was some deterministic function $f : \mathcal{X} \to \mathcal{Y}$ that underlies the relation $\mathcal{X} \to \mathcal{Y}$. This is an unrealistic assumption - in reality, measurements always contain randomness. In our online store example, we may consider that the revenue y measured for a customer is the sum of a deterministic component $\mathbf{x}^\top\mathbf{w}$ (where $\mathbf{x}$ is the customer's feature vector) and some random component z. This means that our dataset will not look like Figure 2.1 even if it is well described by the linear model. Instead is more likely to look like Figure 2.4.

To address this problem we describe a probabilistic model of the data. Let us assume, as before, that the relation $\mathcal{X} \to \mathcal{Y}$ linear, but with an additional factor capturing randomness in the relation. Suppose now that there exists a function $f : \mathcal{X} \to \mathcal{Y}$ such that the response for sample $\mathbf{x}$ is $y = f(\mathbf{x}) + \varepsilon$ where ε is some random variable. We assume that the noise ε in a sample is identically distributed and independent of the noise in any

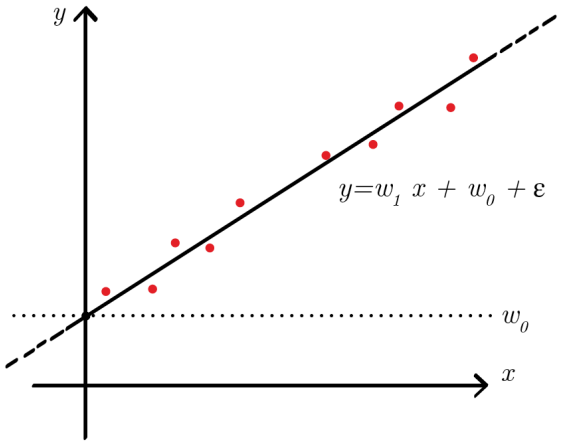


Figure 2.4: *Illustration of a linear regression model where training data is noisy*

other sample. In particular, our training sample S is

$$\left(x_i\,,\,f\left(\mathbf{x}_i\right)+\varepsilon_i\right) \qquad i=1,\ldots,m$$

with $\varepsilon_1,\ldots\varepsilon_m$ being i.i.d: independent and identically distributed. Let us adapt the learning algorithm we designed for the deterministic case to the probabilistic (noisy) case. Let us choose the linear hypothesis class $\mathcal{H}_{reg}$ as before, so that our learning algorithm will output a linear prediction rule. We also assume that we have enough training data to learn, namely that $m \geq d+1$. We assume that there is a vector $\mathbf{w} \in \mathbb{R}^{d+1}$ such that for every sample vector $\mathbf{x}_i$ in our data follows the model:

$$y_i = \mathbf{x}_i^\top \mathbf{w} + \varepsilon_i$$

Denoting the noise vector $\boldsymbol{\varepsilon} := (\varepsilon_1,\ldots,\varepsilon_m)^\top$ we have in matrix notation

$$\mathbf{y} = \mathbf{X}\mathbf{w} + \boldsymbol{\varepsilon}$$

Note that the vector $\mathbf{y}$ will typically not be in $Im(\mathbf{X})$, so that system $\mathbf{y} = \mathbf{X}\mathbf{w}$ has no solutions. As before, using the square loss function, and learning by the empirical risk minimization principal then:

$$\hat{\mathbf{w}} := \underset{\mathbf{w}\in\mathbb{R}^{d+1}}{\operatorname{argmin}} \; ||\mathbf{y}-\mathbf{X}\mathbf{w}||^2$$

This means that our learning algorithm remains the same. We learn by solving the normal equation. As mentioned, $\mathbf{y} \notin Im(\mathbf{X})$ since the noise "pushed" $\mathbf{y}$ out of $Im(\mathbf{X})$. As we have seen, solving the normal equations is equivalent to projecting $\mathbf{y}$ back onto $Im(\mathbf{X})$, so our algorithms effectively attempts to remove the noise and recover the original prediction rule f.

2.1.5.1 An Alternative Approach: Maximum Likelihood

Above we derived an algorithm for learning the linear model using the principle of empirical risk minimization for the square loss. We developed it under the noiseless assumption, but discovered that the algorithm can be used even under noise. Now, let us consider a completely different principle to learning the linear model. Suppose that there is noise, and assume further that the noise is Gaussian $\varepsilon_i \overset{i.i.d}{\sim} \mathcal{N}(0,\sigma^2)$. This means that the i-th observation is independently distributed $y_i \sim \mathcal{N}(\mathbf{x}_i^\top \mathbf{w}, \sigma^2)$. In vector notation, we are assuming that the responses in our training sample follow a multivariate Gaussian distribution:

$$\mathbf{y} \sim \mathcal{N}\left(\mathbf{X}\mathbf{w}, \sigma^2 I_m\right) \tag{2.13}$$

Now, suppose we *knew* the weight vector $\mathbf{w}$, we could then ask the following question: Given a fixed design matrix $\mathbf{X}$ and a known coefficients vector $\mathbf{w}$, what is the probability of observing the response vector $\mathbf{y}$? As each sample is independent to the others, the probability density is the product of the Gaussian densities of each sample

$$p(\mathbf{y}|\mathbf{w}) = \prod_{i=1}^{m} \mathcal{N}\left(y_i|\mathbf{x}_i^\top \mathbf{w}, \sigma^2\right) = \prod_{i=1}^{m} \left[\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(\mathbf{x}_i^\top \mathbf{x} - y)^2}{2\sigma^2}\right)\right] \tag{2.14}$$

This is a question in probability: We know $\mathbf{w}$ and ask for the chance to observe $\mathbf{y}$? However, when we design a learning algorithm, we are actually interested in the reverse question. We have the training sample, including the response vector $\mathbf{y}$. We are interested in a way to choose a linear prediction rule in $\mathcal{H}_{reg}$ and, equivalently, a vector $\mathbf{w}$. We can ask: what is the most "likely" value of $\mathbf{w}$ given the response vector that we observed. This is the Maximum Likelihood approach (subsection 1.1.3) where we choose $\mathbf{w}$ for which the probability density of getting the observed $\mathbf{y}$ is maximal.

As we assumed Gaussian noise, we could express the likelihood function (**??**) of $\mathbf{w}$ using the density function of the Gaussian distribution (1.2.5).

$$\begin{aligned}
\mathcal{L}(\mathbf{w}|X,\mathbf{y}) &= \prod_{i=1}^{m} \mathcal{N}\left(y_i|\mathbf{x}_i^\top \mathbf{w}, \sigma^2\right) \\
&= \prod_{i=1}^{m} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\left(\mathbf{x}_i^\top \mathbf{w} - y_i\right)^2}{2\sigma^2}\right) \\
&= \frac{1}{\left(2\pi\sigma^2\right)^{m/2}} \prod_{i=1}^{m} \exp\left(-\frac{\left(\mathbf{x}_i^\top \mathbf{w} - y_i\right)^2}{2\sigma^2}\right) \\
&= \frac{1}{\left(2\pi\sigma^2\right)^{m/2}} \exp\left(-\frac{1}{2\sigma^2} \sum_{i=1}^{m} \left(\mathbf{x}_i^\top \mathbf{w} - y_i\right)^2\right)
\end{aligned}$$

Now we can use the likelihood function to derive the MLE for our linear regression model (2.13):

$$\begin{aligned}
\hat{\mathbf{w}}^{MLE} &= \underset{\mathbf{w}}{\operatorname{argmax}}\ \mathcal{L}(\mathbf{w}|\mathbf{y}) \\
&= \underset{\mathbf{w}}{\operatorname{argmax}}\ \log \mathcal{L}(\mathbf{w}|\mathbf{y}) \\
&= \underset{\mathbf{w}}{\operatorname{argmax}}\ \exp\left(-\frac{1}{2\sigma^2} \sum_{i=1}^{m} \left(\mathbf{x}_i^\top \mathbf{w} - y_i\right)^2\right) \\
&= \underset{\mathbf{w}}{\operatorname{argmin}}\ \sum_{i=1}^{m} \left(\mathbf{x}_i^\top \mathbf{w} - y_i\right)^2
\end{aligned}$$

We therefore conclude that the maximum likelihood estimator (assuming i.i.d Gaussian noise) gives an *identical* learning algorithm to the one developed using "least squares", namely, using the principle of empirical risk minimization for the square loss.

2.1.6 Categorical Variables

The learning algorithm we have developed can be used whenever $\mathcal{X} = \mathbb{R}^d$ (namely, samples are Euclidean feature vectors) and $\mathcal{Y} = \mathbb{R}$. An issue that often comes up is the following: some of the features we wish to use are numeric (for example, speed in km/h or age in years) while others take values in some discreet set (for example, car manufacturer or house color). To use our model, we must convert all features to numerical values - even those which are non-numeric and take values in a discreet set. In statistics, such features are called *categorical features* or *categorical variables*. As a preliminary step to using the learning algorithm we have developed, which assumes numeric features, we must encode the values of a categorical variable as numerical values.

The set of all possible values that a certain categorical feature can take are called the *levels* of that categirical feature. For example, suppose we look at a training set, where we have some categorical variable describing car color taking values in $\{white, black, red, green\}$. To encode this feature as a numerical feature, we might consider the following idea: we encode each of the levels as some numerical value, and replace the value *white* by 0, *black* by 1, *red* by 2 and *green* by 3. Now, we use this numerical feature vector, obtained using

this encoding, and fit a linear model. This feature will have a linear coefficient and will participate linearly in the linear prediction. However, how should we interpret a coefficient of say 2? Does it mean that as we move from value 0 (white) to value 1 (black) the expected change in the response will increase in 2? What if instead of the mapping above we would have replaced the value *white* by 0, *black* by -1, *red* by 1 and *green* by 3. What would the obtained coefficient mean at this point?

Therefore, when the levels of a categorical variable do not have a natural ordering (colors, for example, do not have a natural order), we cannot simply map each category to a numeric value under the same feature vector. Instead, a categorical variable of k levels turns into $k-1$ binary numeric feature vectors. Each but one of the levels corresponds to one of these new binary numeric features. In our example, we will replace the "color" with three numeric features x_{white}, x_{black} and x_{red}. Then, for a sample where color is *red*, we will have $(x_{white}, x_{black}, x_{red}) = (0,0,1)$ and for a sample where color is *green* (the one level that does not correspond to a new feature), we will have $(x_{white}, x_{black}, x_{red}) = (0,0,0)$. Notice that the feature vectors that we add to the training regression matrix $\mathbf{X}$ are mutually orthogonal. This has advantages statistically and also from a numeric computation perspective. We see that encoding of a categorical feature with k levels into $k-1$ numeric features is defined by a map. This map is known as a *contrast* in the statistical literature.

Two very important considerations to take into account when working with contrasts are: (i) what happens when a test sample contains a level of the categorical variable we have not seen in the training set? (It might be wise to include a level "other" to handle this case). (ii) If the number of levels k is high, we won't want to add $k-1$ new feature vectors to the regression matrix. We might keep the most frequently occurring levels (as seen in the training set), and map all other levels to a new level we may call "other", in order to keep the number of levels in the contrast as small as possible.

Finally, what do we do when the levels have a natural order? A categorical variable whose levels have a natural order is known *ordered categorical variable.* Some examples are: position rank (junior, senior, etc); experience level (no experience, some experience, a lot of experience, master); survey items opinion items such as "I agree with this statement" (do not agree, neutral, agree somewhat, agree, strongly agree), and so on. For ordered categorical variables, it makes sense to use a more sophisticated contrast than the simple binary contrast described above - perhaps a contrast that will capture the order between the levels.

2.2 Coefficient of Determination - R^2

When fitting a linear regression model we search for $\mathbf{w} \in \mathbb{R}^{d+1}$ which minimizes the RSS

$$\underset{\mathbf{w}\in\mathbb{R}^d}{\operatorname{argmin}} \operatorname{RSS}(\mathbf{w}) = \underset{\mathbf{w}\in\mathbb{R}^d}{\operatorname{argmin}} ||\mathbf{y} - \mathbf{X}\mathbf{w}||^2 \tag{2.15}$$

Notice however, that for a given model $\mathbf{w}$ and a sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, the quantity $\operatorname{RSS}(\mathbf{w})$ is not very informative as it has an arbitrary range, determined by the scaling of the data. As such, we cannot tell if an RSS of, say, $10,000$ represents a successful fit to the training data. If the scaling of the data is in 0.1 this is an enormous error, but if the scaling of the data is in the millions then this error is not too bad. We would therefore like to derive some quantity with an intuitively meaningful range of values, which is insensitive to the scaling of the data.

The R-squared (R^2) provides a measure of the goodness of fit of a model. It measures how good are the model predictions in approximating the real data and is defined as the fraction of variance of $\mathbf{y}$ explained by the model

$$R^2 := 1 - \frac{\text{Unexplained Variation}}{\text{Total Variation}} \tag{2.16}$$

The unexplained variation is the sum of the squared errors (SSE), while the total variation is total sum of squares (SST)

$$\text{SSE} := \sum (y_i - \hat{y}_i)^2, \quad \text{SST} := \sum (y_i - \bar{y})^2 \tag{2.17}$$

It holds that SSE $\leq$ SST and thus $R^2 \in [0,1]$, providing an intuitive measure of how good is the fit. If $R^2 = 1$ it means that the amount of unexplained variation in y is zero, namely a perfect fit. If $R^2 = 0$ it means our model does not explain any of the observed variation in y.

2.2.1 Connection With Correlation Coefficient

An interesting observation regarding the R^2 is its connection to the Pearson correlation coefficient. The Pearson correlation coefficient is defined as follows:

$$\rho_{A,B} \coloneqq \frac{cov(A,B)}{\sigma_A \sigma_B} \tag{2.18}$$

This measure, denoted also as r, captures the strength and direction of the *linear* relation between the two random variables A and B. Its values range between $[-1,1]$ where a value of 1 indicates a perfect linear relation between A and B, a value of 0 indicates no linear relation between A and B, and a value of -1 indicates a perfect linear anti-relation between A and B (i.e. $A = -B$).

It holds, that in the case of a linear LS regression with an intercept and a *single* variate then $R^2 = \rho^2_{y,x}$. In the multivariate case then $R^2 = \rho^2_{y,\hat{y}}$.

2.3 Polynomial fitting

Next, we would like to address the question of what type of functions we can learn using the linear regression model. Could we, for example, use the tools developed above, to learn the function $p(x)$ seen in Figure 2.5? And then, given some new value of x predict the value of $p(x)$?

Clearly this function is not a linear function. However, if we look closely at this polynomial $y = x^3 - 3x^2 + \frac{1}{2}x + 2$ and think of it not as a function of x but rather as a function of the coefficients of the polynomial, we realize that this is indeed a linear function. This function simply does not take the original values of x but instead some transformation of the original values: $x \mapsto \left(1, x, x^2, x^3\right)^\top$.

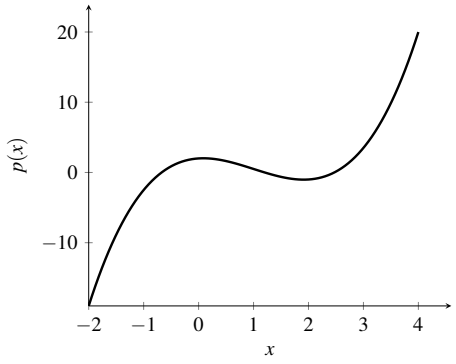


Figure 2.5: *A univariate polynomial* $p(x) = x^3 - 3x^2 + \frac{1}{2}x + 2$

To formulate the above understanding let $\psi_1, \ldots, \psi_k : \mathbb{R}^d \to \mathbb{R}$ be a set of functions such that each ψ_j receives a sample $\mathbf{x} \in \mathbb{R}^d$ and outputs a single value - namely, each ψ_j computes a single feature. Now, using these functions, that are referred to as *basis functions*, we can describe a relation that is *linear* in the parameters $\mathbf{w}$ but could be non-linear in the original input data:

$$y = \sum_{j=1}^{k} \psi_j(\mathbf{x}) \cdot w_j = \boldsymbol{\psi}(\mathbf{x})^\top \mathbf{w}, \qquad \boldsymbol{\psi}(\mathbf{x}) \coloneqq (\psi_1(\mathbf{x}), \ldots, \psi_k(\mathbf{x}))^\top \tag{2.19}$$

For the specific case of (univariate) polynomial fitting we would like to describe a polynomial relation between $\mathcal{X} = \mathbb{R}$ and $\mathcal{Y} = \mathbb{R}$ of degree at most $k \in \mathbb{N}$, but linear in the coefficients. The hypothesis class fitting this relation is:

$$\mathcal{H}^k_{poly} = \left\{ x \mapsto p_{\mathbf{w}}(x) \,|\, \mathbf{w} \in \mathbb{R}^{k+1} \right\} \tag{2.20}$$

where $p_{\mathbf{w}}(x) = \sum_{i=0}^{k} w_i x^i$. Thus, the set of basis functions is $\psi_j(x) = x^j$ for any $j \in \{0,\ldots,k\}$. As before, given a training sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ we would like to choose a coefficients vector $\mathbf{w}$, best describing the coefficients of the polynomial. To do so we solve, as before, the LS problem:

$$\hat{\mathbf{w}} := \underset{\mathbf{w}\in\mathbb{R}^{k+1}}{\operatorname{argmin}} \frac{1}{m} \sum \left(y_i - p_{\mathbf{w}}(x_i)\right)^2 = \underset{\mathbf{w}\in\mathbb{R}^{k+1}}{\operatorname{argmin}} \frac{1}{m} \sum \left(y_i - \psi(\mathbf{x})^\top \mathbf{w}\right)^2 \tag{2.21}$$

Notice that the design matrix $\mathbf{X}$, defined over the transformation $\psi(\mathbf{x})$, is the Vandermonde matrix:

$$\mathbf{X} := \begin{bmatrix} — & h(x_1) & — \\ — & h(x_2) & — \\ & \vdots & \\ — & h(x_m) & — \end{bmatrix} = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^k \\ 1 & x_2 & x_2^2 & \cdots & x_2^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^k \end{bmatrix}$$

Since we assume that the x_i's are different from one another, the design matrix $\mathbf{X}$ is of full rank. This means that solving this linear (in $\mathbf{w}$) system of equations can be done as we have seen for the non-singular case above. After finding $\hat{\mathbf{w}}$, we can predict the value of the unknown function p at a new point x using the value $p_{\hat{\mathbf{w}}}(x)$.

R Here we discuss polynomial fitting where $\mathcal{X} = \mathbb{R}$. With very little adaptation, we could also allow the input data to be $\mathcal{X} = \mathbb{R}^d$, $d > 1$. In such cases the defined polynomial could include terms of multiplication of two (or more) features. We will encounter such an example in **??**.

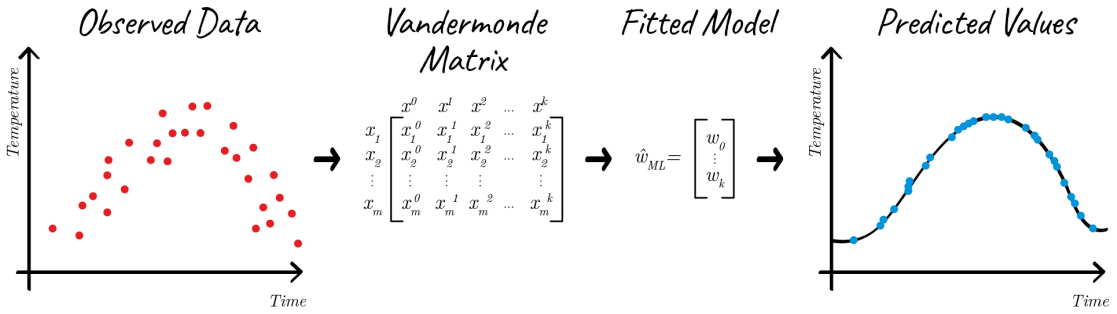


Figure 2.6: Scheme of Polynomial Fitting

2.4 Bias and Variance

In the sections above we have seen that given a regression problem $\mathbf{X}, \mathbf{y}$, where $\mathbf{y} = \mathbf{X}\mathbf{w} + \varepsilon$, $\varepsilon \sim \mathcal{N}\left(0, \sigma^2 I_m\right)$, the estimator $\hat{\mathbf{w}} \in \mathbb{R}^d$ minimizing $||\mathbf{y} - \mathbf{X}\hat{\mathbf{w}}||$ is given by $\hat{\mathbf{w}} := \mathbf{X}^\dagger \mathbf{y}$. It is important to notice that as $\mathbf{y}$ is a

random variable, the LS estimator is too a random variable. Therefore, let us look at different properties of this estimator, specifically the *bias* (1.1.6) and *variance* (1.1.8):

$$Bias\left(\hat{\theta}\right) = \mathbb{E}\left[\hat{\theta}\right] - \theta, \quad Var\left(\hat{\theta}\right) = \mathbb{E}\left[\left(\hat{\theta} - \mathbb{E}\left[\hat{\theta}\right]\right)^2\right]$$

Both these properties involve calculating the expectation of $\hat{\theta}$, but over what is the expectation calculated? An estimator is a decision function over a sample, used to estimate some parameter. Therefore, the expectation is over the selection of the samples:

$$Bias\left(\hat{\theta}\right) = \mathbb{E}_S\left[\hat{\theta}\right] - \theta, \quad Var\left(\hat{\theta}\right) = \mathbb{E}_S\left[\left(\hat{\theta} - \mathbb{E}_S\left[\hat{\theta}\right]\right)^2\right]$$

for $S \overset{i.i.d}{\sim} (\mathcal{X} \times \mathcal{Y})^m$. As we are not assuming any probability distribution over $\mathcal{X}$ this is equivalent to calculating the expectation over the sampling of $\varepsilon \sim \mathcal{N}\left(0, \sigma^2 I_m\right)$ and obtaining $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ where $y_i = \mathbf{x}_i^\top \mathbf{w} + \varepsilon_i$. And so, going back to the LS estimator, it can be shown that this is an *unbiased* estimator with variance of $\sigma^2 \left[\mathbf{X}^\top \mathbf{X}\right]^{-1}$.

To understand how bias and variance help quantify the quality of our estimation, let us revisit polynomial fitting. Consider for example the polynomial

$$Y = X^4 - 2X^3 - 0.5X^2 + 1 + \varepsilon \quad \varepsilon \sim \mathcal{N}(0, 2) \tag{2.22}$$

and let $x_1, \ldots, x_m$ be a set of samples where $x_i \in [-2, 2]$. For these observations let us create 10 different datasets, generated according to the model above. For each dataset we use $x_1, \ldots, x_m$ and generate the response value $y_1, \ldots, y_m$ with the addition of the noise. Figure Figure 2.7 shows the different datasets generated by the model above and the fitted polynomial of degree 1. Black, red and blue points represent the true model, the observed data-points (with the sample noise) and the fitted model over the observed data-points. Notice how the different datasets yield different predicted models. This is the randomness of the prediction, driven by the randomness of the trainset. Over these datasets we can now ask, for each value of x, what is the average prediction and its variance:

- In green is the average prediction of y for a given x across all datasets. The difference between the green and black lines capture the concept of the bias.
- In grey is the area of $\mathbb{E}[\hat{y}] \pm 2 \cdot Var(\hat{y})$ for a given x, also known as the confidence interval. The wider this area is, the more out prediction of $\hat{y}$ varies for different samples. This area captures the concept of the variance.

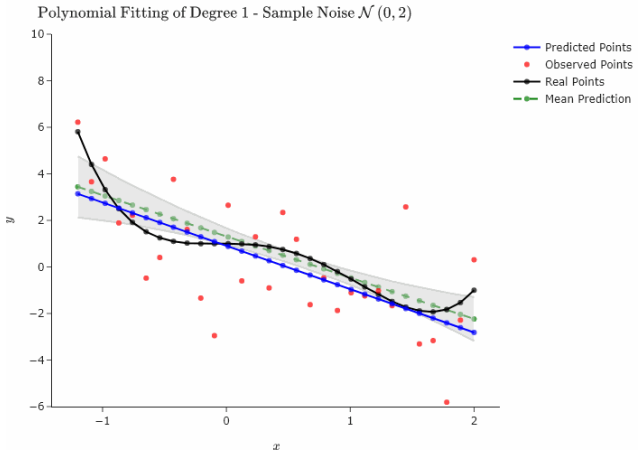


Figure 2.7: ***Polynomial Fitting:*** *Fitted polynomial of degree* 1 *over different datasets differing only in values of added sample noise.* *Chapter 2 Examples - Source Code*

Two phenomena are visible. The first is that the average distance of the fitted model (in green) and the true model (in black) is large. This means that our hypothesis class doesn't have sufficient expressive power to learn the true model. As such, we conclude that the *bias* of our estimator is high. The second is that the fitted models over different datasets do not differ by much. As such, we conclude that the *variance* of our estimator is low.

Next, consider the same setup as before but with the fitting of a polynomial of degree 8 (Figure 2.8). This time the different between the average prediction at each x and the true value of x is lower, while the differences between the fitted models (as indicated by the confidence intervals) is much higher. So the **bias** is low and the **variance** is high. As we enable more "flexible" (i.e. complex) models we are able to fit a model better to our given sample. However, as seen in Figure 2.8, if the model is too complex we might actually be fitting a model to the noise, rather than the actual true signal.

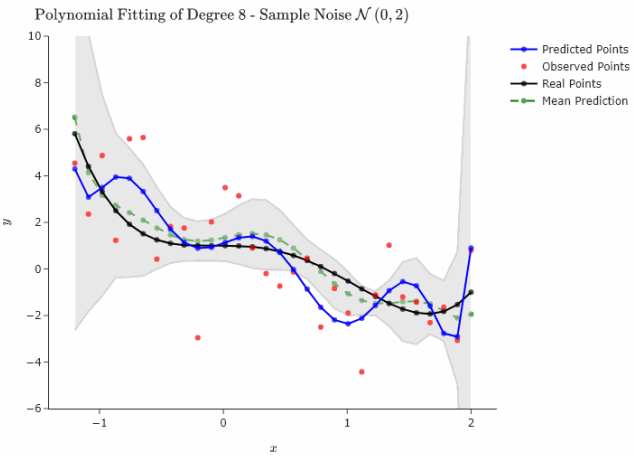


Figure 2.8: ***Polynomial Fitting:*** *Fitted polynomial of degree* 8 *over different datasets differing only in values of added sample noise. Chapter 2 Examples - Source Code*

R It is important to note that what is seen in the figures are not the bias and variance of $\widehat{\mathbf{w}}^{LS}$ themselves but how these manifest over the shown datasets.

Interestingly, these two properties of bias and variance are linked. Let $\hat{\mathbf{y}} = \hat{\mathbf{y}}(S)$ denote the estimator of $\mathbf{y}$ when using $\widehat{\mathbf{w}}^{LS}$, and $\mathbf{y}^*$ the true $\mathbf{y}$ values. When solving the regression problem we wanted to minimize the mean square error between $\widehat{\mathbf{y}}$ and $\mathbf{y}^*$. What would be the expected MSE value?

Denote $\overline{\mathbf{y}} = \mathbb{E}[\hat{\mathbf{y}}]$ so:

$$\begin{aligned}
\mathbb{E}\left[(\hat{\mathbf{y}}-\mathbf{y}^*)^2\right] &= \mathbb{E}\left[(\hat{\mathbf{y}}-\overline{\mathbf{y}}+\overline{\mathbf{y}}-\mathbf{y}^*)^2\right] \\
&= \mathbb{E}\left[(\hat{\mathbf{y}}-\overline{\mathbf{y}})^2\right] + 2(\hat{\mathbf{y}}-\overline{\mathbf{y}})\,\mathbb{E}[\hat{\mathbf{y}}-\overline{\mathbf{y}}] + (\overline{\mathbf{y}}-\mathbf{y}^*)^2 \\
&= \mathbb{E}\left[(\hat{\mathbf{y}}-\overline{\mathbf{y}})^2\right] + (\overline{\mathbf{y}}-\mathbf{y}^*)^2 \\
&= Var(\hat{\mathbf{y}}) + Bias^2(\hat{\mathbf{y}})^2
\end{aligned} \tag{2.23}$$

Namely, we could *decompose* the generalization error (expected square loss between prediction and true value) into a variance component and a (squared) bias component.

$$MSE(\hat{\mathbf{y}}) = Var(\hat{\mathbf{y}}) + Bias^2(\hat{\mathbf{y}}) \tag{2.24}$$

This means, that whenever we devise some estimator over our training data, the generalization error is influenced by both these factors. This is called the *Bias-Variance Trade-off*.

2.5 Summary and Exercises

Exercises

Theoretical Questions

1. Let $\mathbf{A}$ be some matrix. Show that $Ker(\mathbf{A}) = Ker\left(\mathbf{A}^\top \mathbf{A}\right)$.
2. Let $\mathbf{X}$ be a design matrix with independent columns. Prove that $\mathbf{X}^\top \left[\mathbf{X}^\top \mathbf{X}\right]^{-1} \mathbf{X}^\top$ is an orthogonal projection matrix onto the column space of $\mathbf{X}$.
3. Let $\mathbf{A}$ be an invertible matrix. Show that $\mathbf{A}^\dagger = \mathbf{A}^{-1}$.
4. Let $\mathbf{X}, \mathbf{y}$ be a linear regression problem where the columns of $\mathbf{X}$ are linearly independent. Show that $\left[\mathbf{X}^\top \mathbf{X}\right]^{-1} \mathbf{X}^\top = {\mathbf{X}^\dagger}^\top \mathbf{y}$.
5. Let $\mathbf{X}, \mathbf{y}$ be a regression problem such that $\mathbf{y} = \mathbf{X}\mathbf{w} + \varepsilon,\ \varepsilon \sim \mathcal{N}\left(0, \sigma^2 I_m\right)$ and $\hat{\mathbf{w}} := \mathbf{X}^\dagger \mathbf{y}$ the LS estimator. Show that $\hat{\mathbf{w}}$ is an unbiased estimator.
6. Let $\mathbf{X}, \mathbf{y}$ be a regression problem such that $\mathbf{y} = \mathbf{X}\mathbf{w} + \varepsilon,\ \varepsilon \sim \mathcal{N}\left(0, \sigma^2 I_m\right)$ and $\hat{\mathbf{w}} := \mathbf{X}^\dagger \mathbf{y}$ the LS estimator. Prove that the variance of $\hat{\mathbf{w}}$ is $\sigma^2 \left[\mathbf{X}^\top \mathbf{X}\right]^{-1}$.

Practical Questions

Fitting A Linear Regression Model

In this part you will fit a linear regression model to the House Sales dataset.

1. Implement the `mean_square_error` function in the `metrics.loss_functions.py` file as described in the function documentation.

2. Implement the `LinearRegression` class in the `learners.regressors.linear_regression.py` file as described in the documentation. When implementing the `_loss` function be sure to call the `mean_square_error` function previously implemented.

3. Implement the `load_data` function in the `house_sales_prediction.py` and call the function. The function receives the path to the house sales dataset and returns a design matrix and response vector after performing any necessary preprocessing:
   - Addressing missing/invalid values for different features.
   - Treating categorical features.
   - Adding additional features that might be beneficial for predicting the price of the house.
   - Remove irrelevant features.

   Elaborate on the data exploration and decision making process that lead to the final preprocessing code.

4. Implement the `split_train_test` function in the `utils.utils.py` file as described in the function documentation. Call the function in the `house_sales_prediction.py` file, splitting the loaded dataset into a train set (75%) and test set (25%).

5. After splitting the dataset, fit a linear regression model (using your implementation of the `LinearRegression` class) over increasing percentages of the *train set* and evaluate performance over the *test set*. Do so in the following manner:
   - Iterate for every value $p = 10\%, 11\%, \ldots, 100\%$ of the train set samples.
   - Sample p of the train set, fit a model over these samples and evaluate performance over the test set.
   - Repeat the procedure of sampling, fitting and evaluating 10 times for every value of p.

   Plot the average loss, as well as a confidence interval of $\text{mean}(loss) \pm 2 \cdot \text{std}(loss)$, as a function of $p\%$. Explain the results seen in the plot.

6. Repeat the procedure of splitting the train- and test-sets and of fitting the model for different sample sizes (i.e questions 4,5) multiple times. Plot the average of loss averages as well as the confidence interval as a function of $p\%$. Explain what is the difference between the current evaluation approach and the previous.

Performing Polynomial Fitting

In this part you will perform polynomial fitting to the Daily Temperature of Major Cities dataset.

1. Implement the `PolynomialFitting` class in the `learners.regressors.polynomial_fitting.py` file as specified in class documentation. Avoid repeating code from the `LinearRegression` class.

2. Implement the `load_data` function in the `city_tempretaure_prediction.py` file.
   - When loading the dataset remember to deal with invalid data.
   - Use the `parse_dates` argument of the `pandas.read_csv` to set the type of the `'Date'` column.
   - Add a `'DayOfYear'` column based on the `'Date'` column. This column will be the feature to be used for the polynomial fitting.

3. Subset the dataset to contain samples only from your own country. Investigate how the average daily temperature (`'Temp'` column) change as a function of the `'DayOfYear'`.
   - Scatter plot this relation, and color code the data points by the different years. What polynomial degree might be suitable for this data?
   - Group the samples by `'Month'` and plot a bar plot showing for each month the standard deviation of the daily temperatures. Suppose you fit a polynomial model (with the correct degree) over data sampled uniformly at random from this dataset, and then use it to predict temperatures from random days across the year. Based on this plot, do you expect a model to succeed equally over all months or are there times of the year where it will perform better than on others?

4. Subset the dataset to contain samples from 4 countries, your own, a second in the same hemisphere, and two others in the opposite hemisphere. Group the samples according to `'Country'` and `'Month'` and calculate the average and standard deviation of the temperature. Plot a line plot of the average monthly temperature, with error bars (using the standard deviation) color coded by the country. Based on this graph, do all countries share a similar pattern? For which other countries is the model fitted for your own country likely to work well and for which not?

5. Over the subset containing observations only from your own country perform the following:
   - Randomly split the dataset into a training set (75%) and test set (25%).
   - For every value $k \in [1,10]$, fit a polynomial model of degree k using the training set.
   - Record the loss of the model over the test set, rounded to 2 decimal places.

   Print the test error recorded for each value of k. In addition plot a bar plot showing the test error recorded for each value of k. Based on these which value of k best fits the data? In the case of multiple values of k achieving the same loss select the simplest model of them. Are there any other values that could be considered?

6. Fit a model over the entire subset of records from your own country (i.e do not split for a train- and test set) using the k chosen above. Plot a bar plot showing the model's error over each of the other countries. Explain your results based on this plot and the results seen in question 3.

3. Classification

3.1 Classification Overview

In the previous chapter we discussed learning a regression problem where the response is a continuous value $\mathcal{Y} = \mathbb{R}$. When the response set $\mathcal{Y}$ is a finite set, this is a **classification** problem. We distinguish between classification problems where $|\mathcal{Y}| = 2$ (such as $\mathcal{Y} = \{\pm 1\}$ or $\mathcal{Y} = \{0,1\}$) and multi-classification problems where $\mathcal{Y} = \{1,\ldots,k\}$. In the binary classification problem (or just "classification"), we provide a "yes"/"no" prediction. In a multi-class classification, we predict one of $k > 2$ classes. For most, we restrict out discussion only to binary classification problems, though all methods below can be generalized to k classes. Also, we will only deal with the Euclidean sample space $\mathcal{X} = \mathbb{R}^d$, namely, each sample has d **features**. Therefore out setup is as follows:

$$\mathcal{X} := \mathbb{R}^d, \mathcal{Y} := \{\pm 1\}$$

Classification Problems Examples

- Predict whether a patient will develop a certain medical condition, or not.
- Predict whether a user will like a new product, or not.
- Determine if a given network traffic pattern is one of a cyber attack or not.
- Determine whether an art work is an original or forged.
- Determine whether a given email is spam or not.
- Detect fraud on credit card transactions.
- Predict whether a loan applicant will default on the loan.
- (Multi-class) What are the objects seen in a given picture.

■ **Example 3.1** Seen in Figure 3.1 are samples of the "South Africa Heart Disease" dataset. Given the parameters of blood pressure, smoking, family history, etc., could we predict who has/will have coronary heart disease (chd)? Notice that some of the features are numerical (e.g. tabacco, ldl, etc.) while some are categorical (e.g famhist). ■

Visualizing The Feature Space

When given a learning problem it is important to try and get intuition into "what the data looks like". In the case of a training sample for binary classification, we can plot the different axes and color by the label

	sbp	tobacco	ldl	adiposity	famhist	typea	obesity	alcohol	age	chd
0	160	12.00	5.73	23.11	Present	49	25.30	97.20	52	1
1	144	0.01	4.41	28.61	Absent	55	28.87	2.06	63	1
2	118	0.08	3.48	32.28	Present	52	29.14	3.81	46	0
3	170	7.50	6.41	38.03	Present	51	31.99	24.26	58	1
4	134	13.60	3.50	27.78	Present	60	25.99	57.34	49	1
...	...	...	...	...	...	...	...	...	...	...
457	214	0.40	5.98	31.72	Absent	64	28.45	0.00	58	0
458	182	4.20	4.41	32.10	Absent	52	28.61	18.72	52	1
459	108	3.00	1.59	15.23	Absent	40	20.09	26.64	55	0
460	118	5.40	11.61	30.79	Absent	64	27.35	23.97	40	0
461	132	0.00	4.82	33.41	Present	62	14.70	0.00	46	1

Figure 3.1: Example classification dataset: *South African Heart Data from Elements of Statistical Learning*

(Figure 3.2). This task is more difficult for data of higher dimensions, but attempting to imagine it in such cases will help understand what models might fit better to the specific task.

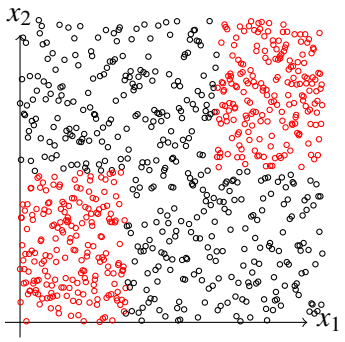


Figure 3.2: Classification training sample in $\mathbb{R}^2$***:*** *Where samples are positioned in space according to the values of their features and color coded by their label.*

3.1.1 Type-I and Type-II Errors

When we discussed regression problems we decided to measure the performance of a given hypothesis using the square loss (and mentioned that we could also use the absolute loss). In the case of classification our hypothesis outputs a label $\{\pm 1\}$ which we want to compare with the true labels also in $\{\pm 1\}$. It therefore makes less sense to measure "how far" is the prediction from the true value (as we do using the squared loss). Instead we would like to measure if we were correct or not. A very straight forward way to evaluate the performance of a classification predictor is to simply count the number of correctly classified samples. That is, given a prediction rule $h : \mathcal{X} \to \{\pm 1\}$ and a labeled sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, the *misclassification* loss of h on this sample is:

$$L_S(h) := \sum_{i=1}^{m} \mathbb{1}_{y_i \neq h(\mathbf{x}_i)} = |\{i | y_i \neq h(\mathbf{x}_i)\}| \tag{3.1}$$

Can there be any problems or issues with the misclassification loss? After all, it just counts the number of times h was wrong - the number of times h misclassified a sample. In practice, there are two kinds of errors the

classifier can make, and making each kind of error might have very different implications, or costs. Therefore, simply counting the total number of errors may not be a useful performance measure.

■ **Example 3.2 — Credit Decisions.** Suppose we are building a classifier that predicts whether a bank customer seeking a loan is credit-worthy and will return a given loan or not. We choose the labels such that -1 means "not credit worth - deny loan", and 1 means "credit worthy - approve loan". Denote y_i the true label and $\widehat{y_i}$ the classifier-predicted label of sample i. The two errors this classifier might make have very different consequences:

- If $y_i = -1$ and $\hat{y}_i = 1$, the classifier predicted that a non-credit-worthy customer will return the loan. If we act on this prediction, and the customer defaults on the loan, the bank loses all the loan sum.
- On the other hand, if $y_i = 1$ and $\hat{y}_i = -1$, the classifier predicted that a credit-worthy customer, which would have paid the interest and returned the loan in full, is not credit-worthy and should be denied the loan. If we act on this recommendation, the bank loses the interest it would have earned on the loan.

Which of the two errors is more serious? Which of the two errors cost more for the bank? If we could choose which error should we avoid "at all costs" and which error could we "allow to happen", what would we choose? ■

■ **Example 3.3 — Drug safety.** Let us look at a more extreme example to help illustrate this point. We are creating a classifier to predicts whether a certain drug **is safe** to use for a particular person, or **unsafe/** deadly/ dangerous to use. We choose the labels such that -1 means "unsafe drug - do not use" and 1 means "safe drug - ok to use". Similar to before our errors are:

- If $y_i = -1$ and $\hat{y}_i = 1$, the classifier recommends to give a drug which is actually potentially deadly.
- If $y_i = 1$ and $\hat{y}_i = -1$, the classifier recommends that the patient should avoid a drug which is actually safe to use.

■

Therefore, we see that depending on the context of the classification problem, the two kinds of errors can have very different costs. We name the first error, the one we would like to avoid at all costs, the *Type-I error* and the second error as *Type-II error*. By choosing what label is "negative" and what label is "positive" we essentially defined what error is the Type-I error. As such, given a classification problem we try to choose the "negative" and "positive" labels such that the error we are more concern of (and therefore would like to avoid more) is the Type-I Error. That is, the error of misclassifying a negative sample by predicting it as a positive sample.

Returning to the drug safety example 3.3, we can assign the following meaning to the labels: $y = -1$ (negative) means the new drug is safe to use and $y = 1$ (positive) means the new drug is dangerous. In this case the Type-I error means that we decided not to offer a safe drug. If however we reverse the meaning such that $y = -1$ (negative) means the drug is dangerous and $y = 1$ (positive) means the new drug is safe, then the Type-I error means that we have decided to offer a dangerous drug. In this case this assignment of labels is the more serious of the two kinds of errors we can make.

For the classification problem of "is this email spam or not" how would you choose the labels? What are the two errors a spam detector can make? which one is the one we really want to avoid? So, which of the labels "spam email" and "not spam, valid email" would you label "negative" and which is "positive"?

3.1.2 Measurements of performance

With the decision on "positive" and "negative" labels, we define four basic terms: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative(FN). These terms refer to the prediction made for a sample with respect to its true label. So suppose a sample's true label is $y = -1$ (negative). If a classifier predicts:

- $\hat{y} = -1$ we term this as true negative.

- $\hat{y} = 1$ we term this as false positive.

Now, suppose a sample's true label is $y = 1$ (positive) then if a classifier predicts:

- $\hat{y} = -1$ we term this as false negative.
- $\hat{y} = 1$ we term as true positive.

Therefore, the false negative and false positive cases are the misclassification errors. False positive is what we referred to as Type-I error and false negative is what we called Type-II error. These four options are shown in **??**.

Using these four basic groups we can devise more domain-specific measurements. Denote by P the number of positive samples and N the number of negative samples then:

- The *Error Rate* is the number of misclassification out of all predictions: $(FP+FN)/(P+N)$.
- The *Accuracy* is the number of correct classification out of all predictions: $(TP+TN)/(P+N) = 1-ErrorRate$.
- The *Recall/ Sensitivity/ True-Positive-Rate (TPR)* is the number of truthfully positive predictions out of all positive samples: TP/P.
- The *False-Positive-Rate (FPR)* is the number of of falsely positive predictions out of all negative samples: FP/N.

There are many more measurements that can be defined from the four basic ones presented with different fields using different measurements. In Computer Science we often encounter the TPR and FPR for reasons described below.

3.1.3 Decision Boundaries

Let h be a binary classification rule in $\mathbb{R}^d$. (Suppose, for example, that we used a training sample to select h from some hypothesis class $\mathcal{H}$). We can feed any point $\mathbf{x} \in \mathbb{R}^d$ into h and get one of two classes. This means that we can view $\mathbb{R}^d$ as disjoint union of two sets:

$$\mathbb{R}^d = \{\mathbf{x}|h(\mathbf{x}) = 1\} \biguplus \{\mathbf{x}|h(\mathbf{x}) = 0\}$$

These sets can be very simple (two half-spaces) or very complicated. The boundary between these two sets is called the *decision boundary*: a test sample on one side of the boundary will be classified to one class by h, and a test sample on the other side of the boundary will be classified to the other class.

Different classifies, derived from different hypothesis classes, will generate different decision boundaries (Figure 3.3). Observing these over different data scenarios is helpful to understand is modeled by the different classifiers. It can also help get a qualitative assessment of the bias and variance of the classifiers.

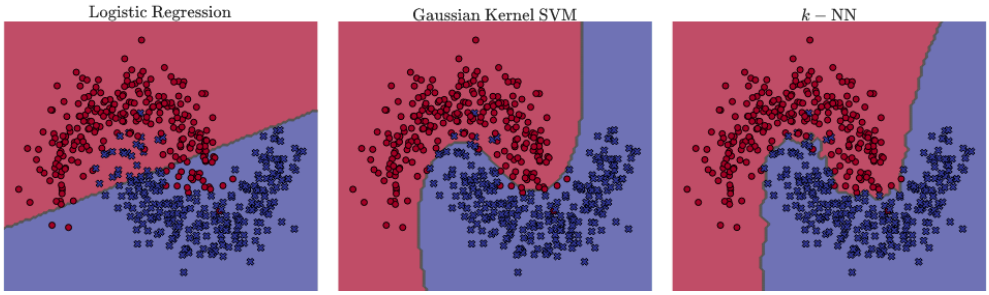


Figure 3.3: Decision Boundaries *of classifiers fitted over moons dataset. Chapter 3 Examples - Source Code*

3.1.4 Studying A New Classifier

For the rest of this chapter we will discuss different sorts of classifiers. As there are numerous types of classifiers, each for tailored for specific data scenarios, it is important to understand how to read about a new classifier. Therefore, when going over the classifiers below keep in mind the following guiding questions:

- How does it model the classification problem? and what are the assumptions made on the data?
- What is the hypothesis class defined? and how does the decision boundary looks like?
- What is the learning principle we use? and how does the algorithm match the learning principle?
- How can the learning principle can be implemented computationally? What is the time complexity of the algorithm and are there any considerations of numeric stability?
- What is done in the training step? and how, given a trained model, to predict for new samples?
- Is the model interpretable? Are we provided with estimations of class probabilities?
- Are we facing a single model or rather a family of models with some parameters for choosing specific models from this family? How do these parameters affect the bias-variance tradeoff?
- When will we decide to use this learning algorithm? What are its advantages and disadvantages?

3.2 Half-Space Classifier

Similar to linear regression, one of the simplest families of classifiers is that of linear classifiers. In these, we are interested in separating a given dataset into two classes using a linear separator function, as seen in Figure 3.4. It will be convenient to work with the class labels of $\mathcal{Y} := \{\pm 1\}$.

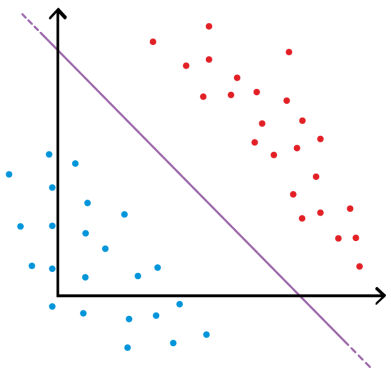


Figure 3.4: Half-space Classification Illustration: *For a domain-set $\mathcal{X} \in \mathbb{R}^2$ the two classes, coded as red and blue colors, are linearly separable .*

Similar to the definition used in linear regression (2.3), the family of linear functions can be described as the set of functions of the form $\mathbf{x} \mapsto \mathbf{x}^\top \mathbf{w} + b,\ \mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$. The linearity refers to the functions being linear in the parameters $\mathbf{w}$. Unlike in the regression setup, here we are interested in a mapping to a discrete response value.

To define a linear separator we begin with defining a hyperplane. For $\mathbf{w} \in \mathbb{R}^d$ and $b \in \mathbb{R}$, the *hyperplane* $(\mathbf{w}, b)$ is the set of points $\{\mathbf{x} | \langle \mathbf{w}, \mathbf{x} \rangle + b = 0\}$. Using a hyperplane we can then state if a given point is "below" or "above" it, and thus separate $\mathbb{R}^d$ into two groups (i.e classes). To understand *how* does a hyperplane perform such separation, consider the transformation that it does to $\mathbf{v} \in \mathbb{R}^d$. Let $(\mathbf{w}, b)$ be a hyperplane where w.l.o.g let $b = 0$. Recall that the orthogonal projection of $\mathbf{v}$ onto $\mathbf{w}$ is given by $\langle \mathbf{v}, \hat{\mathbf{w}} \rangle \hat{\mathbf{w}}$ for $\hat{\mathbf{w}} := \mathbf{w} / ||\mathbf{w}||$. Equivalently, this can be written as $\hat{\mathbf{w}}\hat{\mathbf{w}}^\top \mathbf{v}$ where $\hat{\mathbf{w}}\hat{\mathbf{w}}^\top$ is the orthogonal projection matrix onto the (one-dimensional) subspace spanned by $\hat{\mathbf{w}}$, and $\hat{\mathbf{w}}^\top \mathbf{v}$ is the *coordinate* of $\mathbf{x}$ *in* (i.e. once embedded) the subspace. Once we have embedded $\mathbf{v}$ in this subspace, we can now ask where is its embedding relative to the hyperplane. Notice that

for points on the hyperplane itself, it holds that their embedding $\mathbf{v}^\top \mathbf{w}$ equals to zero. We define the *positive-* and *negative half-spaces* of $(\mathbf{w}, b)$ as the sets of points

$$HS_+ := \{\mathbf{x} | \langle \mathbf{w}, \mathbf{x} \rangle + b > 0\}, \qquad HS_- := \{\mathbf{x} | \langle \mathbf{w}, \mathbf{x} \rangle + b < 0\} \tag{3.2}$$

where together with the hyperplane it holds that $\mathbb{R}^d = HS_+ \uplus \{\mathbf{x} | \mathbf{x}^\top \mathbf{w} = 0\} \uplus HS_-$. Following the same reasoning as above, we now see that the embedding of points $\mathbf{v} \in HS_+$, given by $\mathbf{v}^\top \mathbf{w}$ will be positive and the embedding of points $\mathbf{v} \in HS_-$, given by $\mathbf{v}^\top \mathbf{w}$ will be negative. Using an equivalent way to define the halfspaces

$$HS_+ := \{\mathbf{x} | \text{sign}(\langle \mathbf{w}, \mathbf{x} \rangle + b) > 0\}, \qquad HS_- := \{\mathbf{x} | \text{sign}(\langle \mathbf{w}, \mathbf{x} \rangle + b) < 0\} \tag{3.3}$$

we can define the hypothesis class of half-spaces in $\mathbb{R}^d$.

$$\mathcal{H}_{half} := \left\{ h_{\mathbf{w},b}(\mathbf{x}) := \text{sign}\left(\mathbf{x}^\top \mathbf{w} + b\right) \mid \mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R} \right\} \tag{3.4}$$

The case where $b = 0$ is called the *homogeneous* case, as the hyperplane is a linear subspace going through the origin. When $b \neq 0$ the hyperplane does not go through the origin and is called the non-homogeneous case.

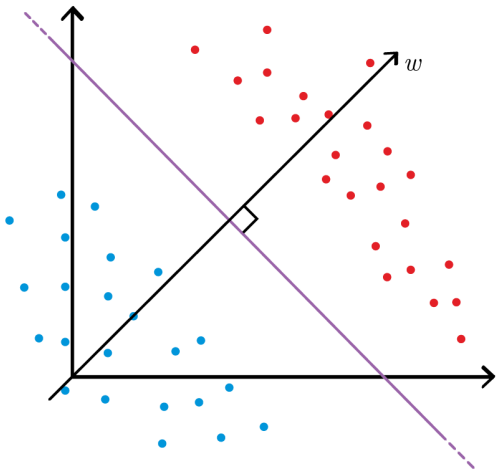


Figure 3.5: *Corresponding Hyperplane to* $\mathbf{w}^\perp$

R Notice, that by definition the hyperplane $\{\mathbf{x} | \mathbf{x}^\top \mathbf{w} = 0\}$ is the set of points perpendicular to $\mathbf{w}$, that is $\mathbf{w}^\perp = \{\mathbf{x} | \mathbf{x}^\top \mathbf{w}\}$. As such, each vector $\mathbf{w} \in \mathbb{R}^d$ defines a hyperplane $\mathbf{w}^\perp$ that divides $\mathbb{R}^d$ into two half-spaces.

Given a sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, we would like to find an hypothesis $h_{\mathbf{w},b} \in \mathcal{H}_{half}$ such that all data points in S that are labeled 1 are on the one side of the hyper-plane and all those labeled -1 are on the other side. To find such an hypothesis we must first make the assumption that the dataset is *linearly separable*. That is, there exists a hyper-plane such that samples of opposing labels are on opposite sides. Mathematically, we assume that

$$\exists \mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R} \quad s.t \quad \forall i \in [m] \quad y_i \cdot \text{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b) = 1$$

or equivalently since the inner product will be negative for all samples with $y_i < 0$ and positive for all samples with $y_i > 0$:

$$\exists \mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R} \quad s.t \quad \forall i \in [m] \quad y_i \cdot (\langle \mathbf{x}, \mathbf{w} \rangle + b) > 0 \tag{3.5}$$

Note, that assuming that a given training set is linearly separable is a *realizability assumption*. Namely, the labels are generated by a function in our hypothesis class $\mathcal{H}_{half}$. For simplicity, let us consider the homogeneous case where $b = 0$, since in the non-homoneneous case we can always shift the data by some fixed vector such that the separating hyperplane goes through the origin. So the hypothesis class of linear separators is of the form:

$$\mathcal{H}_{half} := \left\{ h_{\mathbf{w}}(\mathbf{x}) = \text{sign}\left(\mathbf{x}^\top \mathbf{w}\right) \;\middle|\; \mathbf{w} \in \mathbb{R}^d \right\} \tag{3.6}$$

3.2.1 Learning Linearly Separable Data Via ERM

To train a model over the defined hypothesis class of homogenous half-spaces ($\mathbf{w} \in \mathbb{R}^d, b = 0$) observe the following: for any hypothesis $h_{\mathbf{w}} \in \mathcal{H}_{half}$, the misclassified training samples are exactly those where $y_i \cdot sign\left(\mathbf{x}^\top \mathbf{w}\right) = -1$ or equivalently $y_i \cdot \mathbf{x}^\top \mathbf{w} < 0$. So defining the loss of a given hypothesis over S is:

$$L_S(h_{\mathbf{w}}) := \sum_{i=1}^{m} \mathbb{1}_{y_i \cdot \mathbf{x}^\top \mathbf{w} < 0} \tag{3.7}$$

Since we are assuming realizability (i.e. that S is linearly separable), we would like to find $h_{\mathbf{w}} \in \mathcal{H}_{half}$ that perfectly separates the training set. Such an hypothesis will be one that achieves $L_S(h_{\mathbf{w}}) = 0$. In other words, we are applying the ERM principle and seeking for any separating hyperplane $\mathbf{w}^\perp$, corresponding to an hypothesis $h_{\mathbf{w}}$ that minimizes the empirical risk $L_S(h_{\mathbf{w}})$.

So the next task is finding a compulationally efficient algorithm to find the desired hypothesis. As we are applying the ERM principle we would like to efficiently compute

$$\hat{\mathbf{w}} := \underset{\mathbf{w} \in \mathbb{R}^d}{\text{argmin}}\; L_S(h_{\mathbf{w}}) \tag{3.8}$$

where since assuming realizability, we know there exists a vector $\mathbf{w}^* \in \mathbb{R}^d$ such that $y_i \langle \mathbf{x}_i, \mathbf{w}^* \rangle > 0 \quad i = 1, \ldots, m$ (3.5). Notice, that if we define $\bar{\mathbf{w}} = \frac{\mathbf{w}^*}{\gamma}$ for $\gamma = \min_i (y_i \langle \mathbf{x}, \mathbf{w}^* \rangle)$ we have that

$$y_i \langle \mathbf{x}_i, \bar{\mathbf{w}} \rangle = \frac{1}{\gamma} y_i \langle \mathbf{x}_i, \mathbf{w}^* \rangle \geq 1 \quad i = 1, \ldots, m \tag{3.9}$$

Thus, it is enough to search for a vector $\hat{\mathbf{w}}$ that satisfies

$$y_i \cdot \text{sign}\left(\mathbf{x}^\top \hat{\mathbf{w}}\right) \geq 1 \quad \forall i = 1, \ldots, m \tag{3.10}$$

Convex Optimization

In (3.10) we therefore understand that the problem of finding a linear separator is in fact a problem of finding a vector that satisfies m linear constraints. As these constraints are all convex constraints this is an exaple of what is known as a *convex optimization problem*. Specifically it is a case of a linear program.

Definition 3.2.1 An *optimization problem* over $\mathbb{R}^d$ has the general form:

$$\begin{array}{ll} \text{minimize} & f_0(\mathbf{x}) \\ \text{subject to} & f_i(\mathbf{x}) \leq b_i \quad i = 1, \ldots, n \end{array}$$

where $\mathbf{x}$ is the optimization variable, $f_0 : \mathbb{R}^d \to \mathbb{R}$ is the objective function and $f_i : \mathbb{R}^d \to \mathbb{R}$ are the constraint functions. It is implicitly implied that the optimization problem happens over $\text{dom}(f_0) \subset \mathbb{R}^d$, the domain of f_0.

Then, naturally, a convex optimization problem is an optimization problem as above in which $f_0, f_1, \ldots, f_n$ are all convex functions. When these functions are all linear, this is a linear programming problem

In general, optimization problems are hard to solve computationally. We take special interest in *convex optimization* problems since they have a unique solution, and that solution can be found in computationally tractable ways. A great deal is known about *convex optimization algorithms*, which are iterative numerical algorithms that converge to the solution of a convex optimization problem. There are general solvers, which will solve a convex problem in the general form above, and there are specialized solvers for specific types, or families, of convex optimization problems. A specialized solver is typically preferred, as it leverages some particular structure of the problem to solve it more efficiently, using less space, etc.

Why is convex optimization interesting for machine learning? In supervised learning, we would like to choose a hypothesis $h \in \mathcal{H}$ from our selected hypothesis class, based on some learning principle (such as ERM). Many learning principles are formulated as optimization problems, namely, the h chosen by the learning algorithm is given as the minimizer of some quantity. So implementation of the learning algorithm needs to solve an optimization problem.

Sometimes, our hypothesis class is equivalent to a Euclidean space. When this happens, our learning principle reduces to solving an optimization problem, namely, the hypothesis we choose $h \in \mathcal{H}$ is found as a minimum over $\mathbb{R}^d$ or a subset of $\mathbb{R}^d$ of some objective function, usually a loss function. When this objective is convex, we can use convex optimization algorithms to implement our learning algorithm efficiently.

3.2.2 Solving ERM for Half-Spaces

Returning to the problem of the half-spaces classifier, we have seen that a hyperplane $\mathbf{w}^{\perp}$ minimizing the empirical risk is in fact a solution to the following linear program:

$$\begin{array}{ll} \text{minimize} & 0 \\ \text{subject to} & y_i \cdot \langle \mathbf{x}, \mathbf{w} \rangle \geq 1 \quad i = 1, \ldots, m \end{array} \tag{3.11}$$

Such an optimization problem, where a trivial objective, it is a *feasibility* problem. That is, we are looking for any vector which satisfies the constraints. To solve this we can apply some generic solver for linear programs.

3.2.2.1 The Perceptron Algorithm

Another way for finding a separating hyperplane using the ERM principle is by using the Perceptron algorithm, suggested by Frank Rosenblatt in 1958. This is an iterative algorithm that constructs a series of vectors $\mathbf{w}^{(0)}, \mathbf{w}^{(1)}, \ldots$, where each vector is derived from the vector preceeding it. At each iteration t we search for a sample i which is misclassified by $w^{(t)}$. Then, we update $\mathbf{w}^{(t)}$ by moving it in the direction of thhe misclassified sample $\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} + y_i \mathbf{x}_i$.

Algorithm 1 Batch-Perceptron

procedure PERCEPTRON($S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$)
  $\mathbf{w}^{(1)} \leftarrow 0$ ▷ Initialize parameters
  for $t = 1, 2, \ldots$ **do**
    if $\exists i \; s.t. \; y_i \left\langle \mathbf{w}^{(t)}, \mathbf{x}_i \right\rangle \leq 0$ **then** ▷ If there exists a misclassified sample
      $\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} + y_i \mathbf{x}_i$
    else
      return $\mathbf{w}^{(t)}$
    end if
  end for
end procedure

Our goal when using the Perceptron algorithm is to find a vector $\mathbf{w}$ such that $y_i \cdot \mathbf{x}_i^{\top} \mathbf{w} > 0 \quad i = 1, \ldots, m$.

Notice that as

$$y_i\langle \mathbf{w}^{(t+1)}, \mathbf{x}_i\rangle = y_i\langle \mathbf{w}^{(t)} + y_i\mathbf{x}_i, \mathbf{x}_i\rangle = y_i\langle \mathbf{w}^{(t)}, \mathbf{x}_i\rangle + ||\mathbf{x}_i||^2$$

the update rule of the Perceptron iteratively adjusts the hyperplane to be "more correct" on the i'th sample. It can be shown that in the realizable case the algorithm is guaranteed to terminate, returning a solution that correctly classifies all the samples.

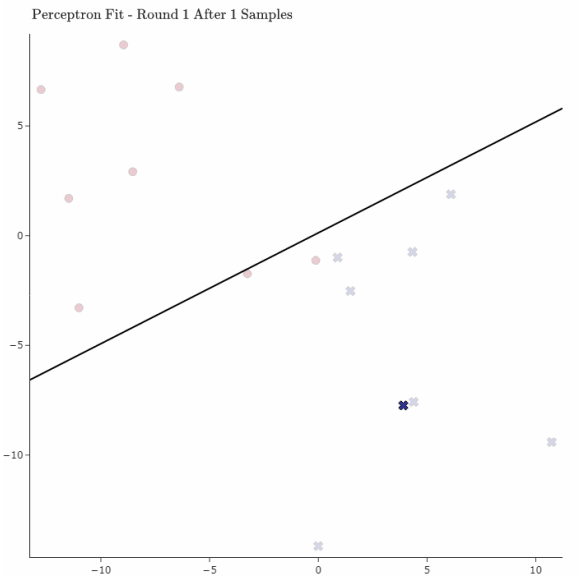


Figure 3.6: ***Perceptron Fitting:*** *Fit a separating hyperplane using Perceptron algorithm. Chapter 3 Examples - Source Code*

R The Perceptron algorithm is in fact a simple case of the more general algorithm of Subgradient Descent covered in **??**.

3.2.3 Learner ID Card

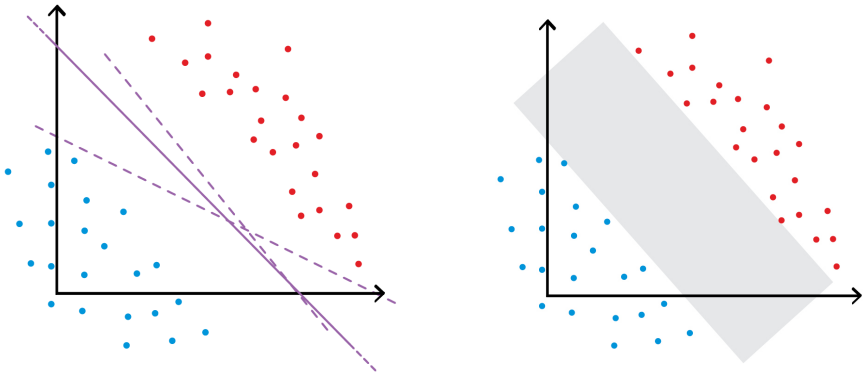
- **Hypothesis class:** the class of linear separators (3.6)
- **Learning principle used for training:** ERM for misclassification loss
- **Computational implementation:** Linear programming or Perceptron
- **Interpretability:** We do not have any specific insight into why a solution was chosen besides it simply satisfying the conditions.
- **Family of models:** No.
- **Storing fitted model:** Fitted model is the vector $\mathbf{w}$ perpendicular to the hyperplane defining the half-space. To store the model we simply store the d coefficients of the vector. In the case of non-homogeneous halfspace we also store the intercept coordinate
- **Prediction of new sample:** $\hat{y}_{new} := \text{sign}\left(\mathbf{x}_{new}^\top \mathbf{w} + b\right)$
- **When to use:** Since realizability assumption rarely holds this classifier is only used as a simple baseline

3.3 Support Vector Machines (SVM)

When using the half-space classifier seen above, we encounter two problems:

- Solution Uniqueness: When we are searching for a separating half-space the solution is not unique. That is, there could be more than a single vector satisfying the constraints of (3.11) and achieving the minimal empirical loss (of zero when assuming realizability or any other positive number if not). As such we are faced with the problem of which one to choose. Figure 3.7 illustrates the existance of multiple separating hyper-planes.

- Realizability: A more severe problem rises when we chose to work with the ERM learning principle for selecting the hypothesis, but the data is not linearly separable (non-realizible case). In this case the optimization problem described in 3.11 is computationally hard.



(a) *Algorithm selected hyper-plane (solid line) and additional optional separating hyperplanes (dashed lines)*

(b) *All hyper-planes linearly separating the data*

Figure 3.7: *Illustration of the existance of multiple separating hyper-planes*

Returning to the hypothesis class of non-homogeneous separating half-spaces $\mathcal{H}_{half}$ (3.4), we would like to describe a different learning principle that will be able to cope with both problems above: finds a unique hyperplane and that can be implemented computationally efficiently even when data is not linearly separable (i.e with polynomial running time given the input).

3.3.1 Maximum Margin Learning Principle

This learning principle is the one of maximum margin.

Definition 3.3.1 Let $(\mathbf{w}, b) \in \mathbb{R}^d \times \mathbb{R}$ be a hyperplane and $u \in \mathbb{R}^d$. Define the distance between $(\mathbf{w}, b)$ and u by:

$$d\left((\mathbf{w}, b), u\right) := \min_{v:\langle v,w\rangle+b=0} ||u - v||$$

(namely, the Euclidean distance between u and the closest point on the hyperplane)

Definition 3.3.2 Let $(\mathbf{w}, b) \in \mathbb{R}^d \times \mathbb{R}$ be a hyperplane and $S = u_1, \ldots, u_m \in \mathbb{R}^d$ a set of points. The *margin* of $(\mathbf{w}, b)$ and S is the smallest distance between the hyperplane and any point:

$$M\left((\mathbf{w}, b), S\right) := \min_{i \in [m]} d\left((\mathbf{w}, b), u_i\right)$$

The margin of a given hyperplane with respect to S is therefore the minimal distance between the hyperplane and a sample in S. It seems logical that a hyperplane with a larger margin is more likely to still satisfy all

separability constraints even if S is slightly different.

So, the new learning principle is: choose $h_{\mathbf{w},b} \in \mathcal{H}_{half}$ that has the *largest margin* with respect to our training data S. Figure 3.8 illustrates the margins of two different potential hyperplanes. Based on these, we would prefer selecting the hyper-plane that is in the center of the grey area. The vectors closest to the hyperplane determine the margin. They are called *support vectors* and hence this learner's name.

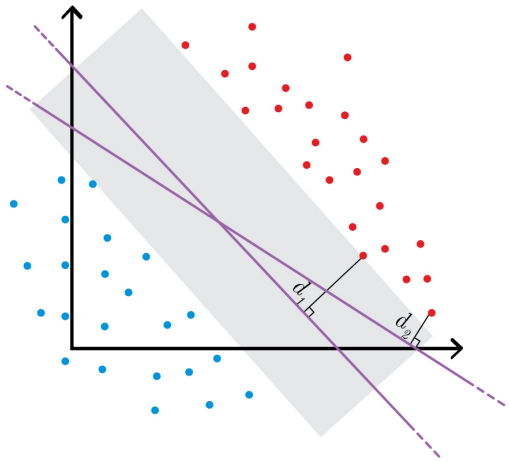


Figure 3.8: *Margin of specified hyper-planes*

3.3.2 Hard-SVM

Let us start with the *realizable case*. To implement our learning principle of maximal margin, we need to search, among all the separating hyperplanes of S, for the hyperplane with maximum margin. Namely, the hypothesis $h_{\mathbf{w},b} \in \mathcal{H}_{half}$ our learner will choose is the solution to the following optimization problem:

$$\begin{array}{ll} \text{maximize} & M\left((\mathbf{w},b),S\right) \\ \text{subject to} & y_i \cdot (\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0 \quad i = 1,\ldots,m \end{array} \tag{3.12}$$

The optimization variables are $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$. Comparing with the linear program of half-spaces (3.11) we see that the constraints are kept, which ensure the hyperplane chosen separates the training sample, but instead of a trivial objective, we seek to maximize the margin.

3.3.2.1 Solving Hard-SVM

So is the Hard-SVM a convex optimization problem? Recall, that by our optimization problem (3.12), we are searching of a separating hyperplane that maximizes the margin from all points. As for any $c > 0$ it holds that $(\mathbf{w},b) = (c\mathbf{w},cb)$ we can w.l.o.g constraint ourselves to $||\mathbf{w}|| = 1$. This way, each hyperlane has a unique vector $\mathbf{w}$ that corresponds to it.

In order to calculate the margin $M\left((\mathbf{w},b),S\right)$ we first must define what does it mean to measure a distance between a point in space and a set of point. For the purpose of the SVM classifier we define the distance as follows. Let $\mathbf{x} \in \mathbb{R}^d$ and $B \subseteq \mathbb{R}^d$. The distance from $\mathbf{x}$ to B: is $\inf_{\mathbf{v} \in B} ||\mathbf{x} - \mathbf{v}||$.

Lemma 3.3.1 Let $(\mathbf{w},b) \in \mathbb{R}^d \times \mathbb{R}$ be a hyperplane where $||w|| = 1$ and $\mathbf{x} \in \mathbb{R}^d$ then the distance between $\mathbf{x}$ and the hyperplane $(\mathbf{w},b)$ is $|\langle \mathbf{x}, \mathbf{w} \rangle + b|$.

* We saw that adding a 1 coordinate to the feature vector allows us to express the bias term. Therefore, for brevity, we would neglect it and only consider $|\langle \mathbf{x}, \mathbf{w} \rangle|$ instead of $|\langle \mathbf{x}, \mathbf{w} \rangle + b|$.

Proof. Since we define the distance between $\mathbf{x}$ and the hyperplane as the minimal distance between $\mathbf{x}$ and a vector in the hyperplane we are in fact looking that the orthogonal projection of $\mathbf{x}$ onto the heyperplane.

Similar to the way we have dealt with the intercept term in linear regression, let us assume that $\mathbf{x}, \mathbf{w} \in \mathbb{R}^{d+1}$, $x_0 = 1$ and w_0 represents the intercept. Let $P = \mathbf{w}\mathbf{w}^\top$ be the projection matrix onto span$(\mathbf{w})$ and consider the matrix $(I - P)$. Firstly, this is a projection matrix as

$$(I-P)^2 = I^2 - 2P + P^2 = I - 2P + P = I - P$$

Secondly, it holds that $Im\,(I-P)$ is the hyperplane defined by $(\mathbf{w}, b)$. Let $\mathbf{u} \in \mathbb{R}^d$ then :

$$\begin{aligned} \langle (I-P)\,\mathbf{u}, \mathbf{w} \rangle &= \langle \mathbf{u} - P\mathbf{u}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle - \langle P\mathbf{u}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle - \left\langle \mathbf{u}, P^\top \mathbf{w} \right\rangle \\ &= \langle \mathbf{u}, \mathbf{w} \rangle - \left\langle \mathbf{u}, \mathbf{w}\mathbf{w}^\top \mathbf{w} \right\rangle = \langle \mathbf{u}, \mathbf{w} \rangle - \langle \mathbf{u}, \mathbf{w} \rangle = 0 \end{aligned}$$

Thus $(I-P)$ is an orthogonal projection matrix onto the hyperplane $(\mathbf{w}, b)$ and $(I-P)\mathbf{x}$ is the orthogonal projection of $\mathbf{x}$ onto $(\mathbf{w}, b)$. Therefore, the distance between $\mathbf{x}$ and the hyperplane is given by:

$$||\mathbf{x} - (I-P)\mathbf{x}|| = ||\mathbf{x} - \mathbf{x} + P\mathbf{x}|| = \left|\left|\mathbf{w}\mathbf{w}^\top \mathbf{x}\right|\right| = ||\langle \mathbf{x}, \mathbf{w} \rangle \cdot \mathbf{w}|| = |\langle \mathbf{x}, \mathbf{w} \rangle| \cdot ||\mathbf{w}|| = |\langle \mathbf{x}, \mathbf{w} \rangle|$$

■

So, as the margin between a given hyperplane $(\mathbf{w}, b)$ and a set of points S is the minimal distance between the hyperplane and any point in the set, we derive that our optimization problem is in fact of the form:

$$\begin{array}{ll} \underset{(\mathbf{w},b):||\mathbf{w}||=1}{\text{argmax}} & \min_{i \in [m]} |\langle \mathbf{w}, \mathbf{x}_i \rangle + b| \\ \text{subject to} & y_i \cdot (\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0 \quad i = 1, \ldots, m \end{array} \tag{3.13}$$

While the constraints enforce $\mathbf{w}$ to define a separating hyperplane, the objective will make us choose a separating hyperplane with the maximal margin. We further simplify the optimization problem. Consider a *feasible* solution $\mathbf{w}$ to the problem (i.e. that satisfies all constraints). It holds that $|\langle \mathbf{x}_i, \mathbf{w} \rangle + b| = y_i\,(\langle \mathbf{x}_i, \mathbf{w} \rangle + b)$. Hence, we can rewrite (3.13) as:

$$\begin{array}{ll} \underset{(\mathbf{w},b):||\mathbf{w}||=1}{\text{argmax}} & \min_{i \in [m]} y_i\,(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) \\ \text{subject to} & y_i \cdot (\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0 \quad i = 1, \ldots, m \end{array} \tag{3.14}$$

Notice that the constraints are now redundant. If $\mathbf{w}$ is infeasible then $\min_i y_i \left(\mathbf{x}_i^\top \mathbf{w} + b\right) < 0$, achieving a lower objective than any feasible solution. Therefore, we can re-write the problem as:

$$\underset{(\mathbf{w},b):||\mathbf{w}||=1}{\text{argmax}} \quad \min_{i \in [m]} y_i\,(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) \tag{3.15}$$

And lastly, we notice that we can represent (3.15) as a norm minimization problem instead of margin maximization problem:

Claim 3.3.2 Consider the following optimization problem:

$$\underset{(\mathbf{w},b)}{\text{argmin}} \; ||\mathbf{w}||^2 \qquad \text{subject to} \quad y_i\,(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) \geq 1 \quad i = 1, \ldots, m \tag{3.16}$$

If $(\mathbf{w}^*, b^*)$ is an optimal solution to (3.16) then $\left(\hat{\mathbf{w}}, \hat{b}\right)$ is an optimal solution to (3.15), where $\hat{\mathbf{w}} = \frac{\mathbf{w}^*}{||\mathbf{w}^*||}$, $\hat{b} = \frac{b^*}{||\mathbf{w}^*||}$.

Proof. Let $(\mathbf{w}, b)$ be a feasible solution to (3.15) and denote the margin achieved by $(\mathbf{w}, b)$ by γ then:

$$y_i\left(\langle \mathbf{x}_i, \mathbf{w}\rangle + b\right) \geq \gamma \quad i = 1, \ldots, m$$

Since $\gamma = \min_i y_i\left(\langle \mathbf{x}_i, \mathbf{w}\rangle + b\right)$ it holds that:

$$y_i\left(\left\langle \mathbf{x}_i, \frac{\mathbf{w}}{\gamma}\right\rangle + \frac{b}{\gamma}\right) \geq 1 \quad i = 1, \ldots, m$$

meaning that $(\frac{\mathbf{w}}{\gamma}, \frac{b}{\gamma})$ is a feasible solution to (3.16). Let $(\mathbf{w}^*, b^*)$ be an optimal solution for (3.16). As such, it achieves the minimal norm out of all feasible solutions and specifically it means that:

$$||\mathbf{w}^*|| \leq \left|\left|\frac{\mathbf{w}}{\gamma}\right|\right| = \frac{1}{\gamma}||\mathbf{w}|| = \frac{1}{\gamma}$$

where the last equality is due to $(\mathbf{w}, b)$ being a feasible solution to (3.15) and therefore $\mathbf{w}$ a unit vector. Consider $(\hat{\mathbf{w}}, \hat{b})$ achieved from $(\mathbf{w}^*, b^*)$. It follows that for all $i \in [m]$:

$$y_i\left(\langle \mathbf{x}_i, \hat{\mathbf{w}}\rangle + \hat{b}\right) = y_i\left(\left\langle \mathbf{x}_i, \frac{\mathbf{w}^*}{||\mathbf{w}^*||}\right\rangle + \frac{b^*}{||\mathbf{w}^*||}\right) = \frac{1}{||\mathbf{w}^*||} y_i\left(\langle \mathbf{x}_i, \mathbf{w}^*\rangle + b^*\right) \geq \frac{1}{||\mathbf{w}^*||} \geq \gamma$$

with $\hat{\mathbf{w}}$ being a unit vector. Thus, $(\hat{\mathbf{w}}, \hat{b})$ achieves a higher or equal objective to (3.15) from any feasible solution, concluding optimality. ■

This means in fact that maximizing the margin is equivalent to minimizing the size of the hyperplane.

Definition 3.3.3 An optimization problem is called a *Quadratic Program* (QP) if it can be written in the following form:

$$\begin{array}{ll} \underset{\mathbf{w}\in\mathbb{R}^n}{min} & \frac{1}{2}\mathbf{w}^\top Q\mathbf{w} + \mathbf{a}^\top \mathbf{w} \\ \text{such that} & A\mathbf{w} \leq \mathbf{d} \end{array}$$

where $Q \in \mathbb{R}^{n\times n}, A \in \mathbb{R}^{m\times n}, \mathbf{a} \in \mathbb{R}^n, \mathbf{d} \in \mathbb{R}^m$ are fixed vectors and matrices.

The optimization problem written in (3.16) is a Quadratic Program (QP) for which there exist efficient solvers. By using them to solve problem (3.16) we can obtain an optimal solution for the Hard-SVM optimization problem.

But so how is it that minimizing $||\mathbf{w}||^2$ is equivalent to maximizing the margin? Let us denote the width of the total margin (i.e. the sum of margin from both sides) by l, and let x_+ and x_- be the positive- and negative support vectors . To calculate the value of l we will project the vector $x_+ - x_-$ onto the normalized normal $\mathbf{w}$:

$$\begin{aligned} l &= \left\langle x_+ - x_-, \frac{\mathbf{w}}{||\mathbf{w}||}\right\rangle \\ &= \left(\langle x_+, \mathbf{w}\rangle - \langle x_-, \mathbf{w}\rangle\right)||\mathbf{w}|| \\ &= \left(1 - b - (-1 - b)\right)/||\mathbf{w}|| \\ &= 2/||\mathbf{w}|| \end{aligned}$$

where support vectors satisfy $y_i\left(\langle \mathbf{w}, \mathbf{x}_i\rangle + b\right)$ and that for positive samples $y_i = 1$ and negative samples $y_i = -1$. This shows how minimizing $||\mathbf{w}||$ maximizes l.

3.3.3 Soft-SVM

The basic assumption of Hard-SVM is that the training sample is *linearly separable*, that is, that the realizability assumption holds. If that is not the case then the optimization problem has no solutions as for any candidate $(\mathbf{w}, b)$ at least one of the constraints $y_i \cdot \left(\mathbf{x}_i^\top \mathbf{w} + b\right) \geq 1$ cannot be satisfied.

However, what if the training sample is *almost* linearly separable? That is, what if most of the samples are linearly separable with only a few violating the constraints by "not too much"? Recall that if $y_i \cdot \left(\mathbf{x}_i^\top \mathbf{w} + b\right) < 0$ then sample $\mathbf{x}_i$ is on the "wrong side" of the hyperplane. This means that:

$$\exists \xi_i > 0 \quad s.t. \quad y_i \cdot \left(\mathbf{x}_i^\top \mathbf{w} + b\right) \geq 1 - \xi_i$$

Therefore, sample $\mathbf{x}_i$ is on the "wrong" side of the *margin* by an amount proportional to ξ_i (Figure 3.9). To allow training samples to violate the constraints "a little", we modify the optimization problem to:

$$\begin{array}{ll} \text{minimize} & ||\mathbf{w}||^2 \\ \text{subject to} & \begin{cases} y_i \cdot \left(\mathbf{x}_i^\top \mathbf{w} + b\right) \geq 1 - \xi_i & i = 1, \ldots, m \\ \xi_i \geq 0 \quad \wedge \quad \frac{1}{m} \sum_{i=1}^m \xi_i \leq C \end{cases} \end{array} \tag{3.17}$$

where $C > 0$ is a constant we specify. The variables $\xi_1, \ldots, \xi_m$ are new auxiliary variables we introduce (sometimes known as slack variables). Notice that the larger we choose C to be, the more violations of margin we allow. On the one hand, we want to allow "noisy" samples to violate the margin, so the hyperplane will ignore them. On the other hand, if we allow too many violations, we lose touch with the training sample and its structure. This is exactly the bias-variance trade-off: the larger C, the more freedom the learner has to "chase after the training sample".

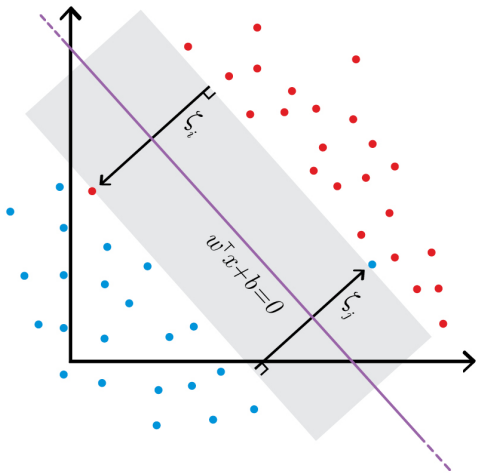


Figure 3.9: *Slack variables of data-points that are on the "wrong" side of the hyper-plane.*

Instead of specifying C directly, we often prefer working with a slightly different optimization problem, where instead of constraining the value of $\frac{1}{m}\sum \xi_i$ we jointly minimize the norm of $\mathbf{w}$ (related to the margin) and the average of ξ_i (corresponding margin violations).

$$\begin{array}{ll} \underset{\mathbf{w}, b, \{\xi_i\}}{\text{minimize}} & \lambda \, ||\mathbf{w}||^2 + \frac{1}{m} \sum_{i=1}^m \xi_i \\ \text{subject to} & y_i \cdot \left(\mathbf{x}_i^\top \mathbf{w} + b\right) \geq 1 - \xi_i, \; \xi_i \geq 0 \quad i = 1, \ldots, m \\ & \lambda \geq 0 \end{array} \tag{3.18}$$

To simplify the above optimization problem let use define the *hinge* loss function:

$$\ell^{hinge}(a) := \max\{0, 1-a\}, \; a \in \mathbb{R} \tag{3.19}$$

Claim 3.3.3 Given a training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ and hyperplane $(\mathbf{w}, b)$, the Soft-SVM optimization problem (**??**) is equivalent to

$$\underset{\mathbf{w},b}{\operatorname{argmin}} \left(\lambda \|\mathbf{w}\|^2 + L_S^{hinge}((\mathbf{w}, b)) \right)$$

where $L_S^{hinge}((\mathbf{w}, b)) := \frac{1}{m} \sum \ell^{hinge}\left(y_i \cdot \mathbf{x}_i^\top \mathbf{w}\right)$

Proof. Given a specific hyperplane $(\mathbf{w}, b)$ consider the minimization over $\xi_1, \ldots, \xi_m$. Since we defined the auxiliary variables to be nonnegative, the optimal assignment of ξ_i is

$$\xi_i := \begin{cases} 0 & y_i\left(\mathbf{x}_i^\top \mathbf{w} + b\right) \\ 1 - y_i\left(\langle \mathbf{x}_i, \mathbf{w} \rangle + b\right) > 1 & otherwise \end{cases}$$

Thus $\xi_i = \ell^{hinge}\left(y_i\left(\mathbf{x}_i^\top \mathbf{w} + b\right)\right)$ ■

The hyper-parameter λ controls the trade-off between the norm of $\mathbf{w}$ and the violations of margin.

- The larger λ, the less sensitive the solution will be to the term $\frac{1}{m}\sum_{i=1}^m \xi_i$, and will allow more violations.
- The smaller λ, the more sensitive and will allow less violations.

Therefore when we consider the parameter λ in (3.18) (or equivalently C in (3.17)), we are in fact considering different learners within a *family of learners*, where each member of the family is specified by a specific value of λ (or C). These different family members can be placed somewhere along the hypothesis complexity axis. Thus, changing the value of λ (or C) moves us along the bias-variance tradeoff. λ is known as a *regularization parameter*. This topic is covered in **??**.

3.3.4 Learner ID Card

- **Hypothesis class:** the class of non-homogeneous linear separators (3.4)
- **Learning principle used for training:** Maximal margin
- **Computational implementation:** Quadratic Program
- **Interpretability:** Retrieved solution does not provide meaningful insights regarding predictions
- **Family of models:** The Soft-SVM learner provides us with a set of models, indexed by the regularization parameter $\lambda \in [0, \infty)$
- **Storing fitted model:** Fitted model is the vector $\mathbf{w}$ perpendicular to the hyperplane defining the half-space as well as the intercept coordinate
- **Prediction of new sample:** $\hat{y}_{new} := \text{sign}\left(\mathbf{x}_{new}^\top \mathbf{w} + b\right)$
- **When to use:** By itself this learner should be used as a simple baseline. However, after embedding the data in some high-dimensional space (kernelization) this becomes a powerful learner (**??**)

3.4 Logistic Regression

3.4.1 A Probabilistic Model For Noisy Labels

Let us revisit the model of linear regression. Recall that when assuming Gaussian errors (2.1.5) we modeled the relation between the domain and response spaces as $\mathbf{y} = \mathbf{X}\mathbf{w} + \varepsilon$ for $\varepsilon \sim \mathcal{N}\left(0, \sigma^2 I_m\right)$. Notice that as ε is a random variable, $\mathbf{y}$ too is a random variable distributing as a multi-variate Gaussian:

$$\mathbf{y} \sim \mathcal{N}\left(\mathbf{X}\mathbf{w}, \sigma^2 I_m\right) \tag{3.20}$$

Focusing on a single pair $(\mathbf{x}_i, y_i)$, we can think of the above as the *conditional probability* of y_i given $\mathbf{x}_i$:

$$p(y_i|\mathbf{x}_i, \mathbf{w}) = \mathcal{N}\left(y_i|\phi_{\mathbf{w}}(\mathbf{x}_i), \sigma^2\right) \quad \text{where} \quad \phi_{\mathbf{w}}(\mathbf{x}) = \mathbf{x}^\top \mathbf{w} \tag{3.21}$$

where the notation of $\mathcal{N}(y_i|\mathbf{x}_i, \mathbf{w})$ means the probability of observing the response y_i for the feature vector of $\mathbf{x}_i$ and coefficients vector $\mathbf{w}$. We also condition on $\mathbf{w}$ (though not a random variable) to explicitly state the dependence on the model parameters. In other words, we assumed that each sample $(\mathbf{x}, y)$ is such that the *expected value* of the label y is linear in $\mathbf{x}$. As we are dealing with a regression model and $y_i \in \mathbb{R}$, the support of the random variable $y_i|\mathbf{x}_i, \mathbf{w}$ is $\mathbb{R}$.

Let us adapt the model above to fit for classification problems. We would like to assume that y_i distributes *Bernoulli* with the probability $p(\mathbf{x}_i)$ of y_i being 1 depending on the specific feature vector $\mathbf{x}_i$.

$$p(y_i|\mathbf{x}_i) = Ber(y_i|p(\mathbf{x}_i)) \tag{3.22}$$

How shall $p(\mathbf{x}_i)$ relate with $\mathbf{x}_i$? Unlike the linear regression model, we cannot assume a linear function $\phi_{\mathbf{w}}(\mathbf{x}) = \mathbf{x}^\top \mathbf{w}$ as $\phi_{\mathbf{w}} \in \mathbb{R}$ while $p(\mathbf{x}_i)$ is restricted to $[0,1]$. Instead, we would like to choose some *link* function $\phi_{\mathbf{w}} : \mathbb{R} \to [0,1]$ that is monotone increasing and maps $(-\infty, \infty)$ bijectively to $(0,1)$. Define the relation to be:

$$p(y_i|\mathbf{x}_i, \mathbf{w}) = Ber(y_i|\phi_{\mathbf{w}}(\mathbf{x}_i)), \quad \phi_{\mathbf{w}} := \sigma\left(\mathbf{x}^\top \mathbf{w}\right) \tag{3.23}$$

where σ is the *sigmoid* function, also known as the *logistic* function:

$$\sigma(\mathbf{a}) := \frac{e^{\mathbf{a}}}{e^{\mathbf{a}} + 1} \tag{3.24}$$

This function is indeed monotone increasing and maps $(-\infty, \infty)$ bijectively to $(0,1)$:

- As $\mathbf{x}^\top \mathbf{w} \to -\infty$ then $\sigma\left(\mathbf{x}^\top \mathbf{w}\right) \to 0$. This means that it is "very unlikely" that the label is 1: $p(y_i = 1|\mathbf{x}_i, \mathbf{w}) \to 0$.
- As $\mathbf{x}^\top \mathbf{w} \to \infty$ then $\sigma\left(\mathbf{x}^\top \mathbf{w}\right) \to 1$. This means that it is "very likely" that the label is 1: $p(y_i = 1|\mathbf{x}_i, \mathbf{w}) \to 1$.

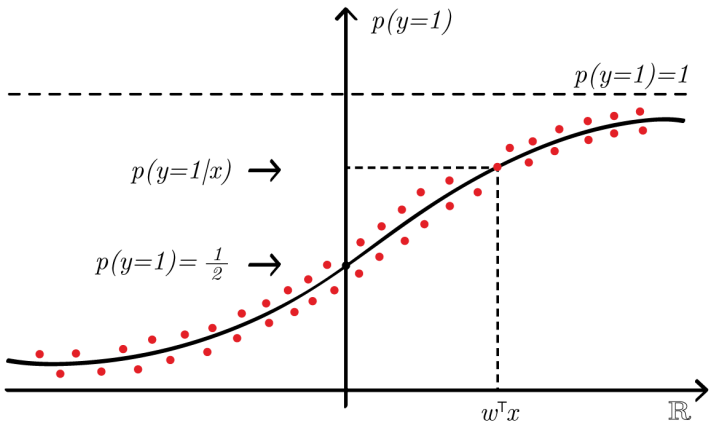


Figure 3.10: Illustration of fitted logit function *for values corresponding to* $\mathbf{x}^\top \mathbf{w}$.

R In (3.23) we modeled the logistic regression model for binary classification problems. Notice that the Bernoulli distribution can be seen as a private case of the Multinomial distribution $Multinomial(p_1, \ldots, p_K)$, $\sum_p i = 1, 0 \leq p_i \leq 1$. We can expand the above logistic regression model to fit multi-classification problems by extending the sigmoidal function to what is known as the softmax function $\sigma(\mathbf{a}) = e^{\mathbf{a}_i} / \sum_{j=1}^{K} e^{\mathbf{a}_j}$

3.4.1.1 The Hypothesis Class

So we would like to define the hypothesis class of logistic regression as:

$$\mathcal{H}_{logistic} := \left\{ h_{\mathbf{w}}(\mathbf{x}) = \sigma\left(\mathbf{x}^\top \mathbf{w}\right) | \mathbf{w} \in \mathbb{R}^{d+1} \right\} \tag{3.25}$$

where $\mathbf{w} \in \mathbb{R}^{d+1}$ since we incorporate the intercept variable into $\mathbf{w}$ (and a zeroth coordinate of 1 to $\mathbf{x}$) similar to the way we did in the linear regression hypothesis class. Notice that the hypotheses are defined $h_{\mathbf{w}} : \mathbb{R}^{d+1} \to [0,1]$ and not $h_{\mathbf{w}} : \mathbb{R}^{d+1} \to \{0,1\}$ as required for classification problems. Since $\{0,1\} \subset [0,1]$, we can use the training sample to select a function in $\mathcal{H}_{logistic}$. This means we will be able to train a model, but how will we predict over new samples? Suppose our learner chose some $h_{\mathbf{w}} \in \mathcal{H}_{logistic}$. As we think of $h_{\mathbf{w}}(\mathbf{x})$ as an estimate of the probability that the label corresponding to $\mathbf{x}$ is 1, we can use it for classification. If $h_{\mathbf{w}}(\mathbf{x})$ is low the label is likely to be 0. If $h_{\mathbf{w}}(\mathbf{x})$ is high, the label is likely to be 1. Choosing some *cutoff* value $\alpha \in [0,1]$, our class prediction will be: $\hat{y} := \mathbb{1}_{h_{\mathbf{w}}(\mathbf{x}) > \alpha}$. To choose a fitting value for α we can calculate the Type-I and Type-II errors (subsection 3.1.1) of the classifier and plot its ROC curve (3.4.4)

3.4.1.2 Learning Via Maximum Likelihood

Once we have defined the logistic regression model (3.23) and hypothesis class (3.25), we would like to come up with a learner. To do so we will use the *maximum likelihood principle*. Recall, that by the maximum likelihood principle, we estimate the parameters (the desired hypothesis) as those that have the highest probability, given the data.

Let $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ be our sample of independent observations, assuming that $\mathbf{y}_i \sim Ber(\phi_{\mathbf{w}}(\mathbf{x}))$ where ϕ is the logistic function. Therefore, the likelihood of $\mathbf{w} \in \mathbb{R}^{d+1}$ is:

$$\begin{aligned}
\mathcal{L}(\mathbf{w}|\mathbf{X},\mathbf{y}) &= \mathbb{P}(y_1,\ldots,y_m|\mathbf{X},\mathbf{w}) \\
&= \prod \mathbb{P}(y_i|\mathbf{x}_i,\mathbf{w}) \\
&= \prod_{i:y_i=1} \mathbb{P}(y_i|\mathbf{x}_i,\mathbf{w}) \cdot \prod_{i:y_i=0} \mathbb{P}(y_i|\mathbf{x}_i,\mathbf{w}) \\
&= \prod_{i:y_i=1} p_i(\mathbf{w}) \cdot \prod_{i:y_i=0} (1-p_i(\mathbf{w})) \\
&= \prod p_i(\mathbf{w})^{y_i} (1-p_i(\mathbf{w}))^{1-y_i}
\end{aligned} \tag{3.26}$$

where $p_i(\mathbf{w}) = \phi_{\mathbf{w}}(\mathbf{x}_i)$. Since the log function is monotone increasing we can maximize the log-likelihood $\ell(\mathbf{w}) := \log \mathcal{L}(\mathbf{w})$ instead:

$$\begin{aligned}
\ell(\mathbf{w}|\mathbf{X},\mathbf{y}) &= \sum_{i=1}^m \left[y_i \log\left(p_i(\mathbf{w})\right) + (1-y_i)\log\left(1-p_i(\mathbf{w})\right) \right] \\
&= \sum_{i=1}^m \left[y_i \log\left(\frac{e^{\mathbf{x}_i^\top \mathbf{w}}}{1+e^{\mathbf{x}_i^\top \mathbf{w}}}\right) + (1-y_i)\log\left(\frac{1}{1+e^{\mathbf{x}_i^\top \mathbf{w}}}\right) \right] \\
&= \sum_{i=1}^m \left[y_i \cdot \mathbf{x}_i^\top \mathbf{w} - \log\left(1+e^{\mathbf{x}_i^\top \mathbf{w}}\right) \right]
\end{aligned} \tag{3.27}$$

And therefore, choosing the function $h \in \mathcal{H}_{logistic}$ by applying the maximum likelihood principle means that:

$$\hat{\mathbf{w}} := \underset{\mathbf{w} \in \mathbb{R}^{d+1}}{\operatorname{argmax}} \sum_{i=1}^m \left[y_i \cdot \mathbf{w}^\top \mathbf{x}_i - \log\left(1+e^{\mathbf{w}^\top \mathbf{x}_i}\right) \right] \tag{3.28}$$

R Instead of deriving the learner using the maximum likelihood principle, we could derive it using the ERM principle with the following loss function: $\ell(h_{\mathbf{w}}) := \log\left(1+\exp\left(-y\langle \mathbf{w}, \mathbf{x}\rangle\right)\right)$. We would have reached the same optimization expression.

3.4.2 Computational Implementation

Now that we have defined the hypothesis class and an optimization problem to find the desired hypothesis, the next step is finding an efficient algorithm to solve it. By working with the logistic function, the resulting log-likelihood expression is **concave** function of the optimization variable $\mathbf{w}$. This means, that instead of solving the maximization problem (3.28) we can solve the minimization of minus the log-likelihood, which is convex. As such, there are general algorithms for finding the minima of such functions.

While there is no closed form for the maximizer $\hat{\mathbf{w}}$, as logistic regression is a very useful learner, there is a custom iterative algorithm that usually converges quickly to $\hat{\mathbf{w}}$. This algorithm is based on the second-order descent method of **Newton-Raphson** iterations, broadly discussed at **??**.

3.4.3 Interpretability

One important properly of the logistic regression learner is interpretability both in the sense of which features were important for the model and why was a certain prediction given. When working with $\mathcal{X} = \mathbb{R}^d$, we gather many feature, and might think that some of them are important for prediction while others less. Similar to linear regression, we are able to ask "which features were important" for the model by simply investigating the entries of the fitted coefficients vector $\mathbf{w}$. Features corresponding to coefficients of values close to zero have a small impact on prediction and therefore these features are less important for the model. Features corresponding to coefficients of values far from zero have a large impact on prediction and are therefore important for the model.

Then, for a given sample $\mathbf{x}$, by looking at entries corresponding to important features we can understand why the model predicted $\hat{y}$. If in entries of $\mathbf{x}$ corresponding important features there are large (positive or negative) values, they will have much influence the outcome. If these values are of same sign as of the coefficients then the expression $\mathbf{x}^\top \mathbf{w}$ will be larger, increasing the likelihood of the prediction being 1. If these values are of opposite signs to the coefficients then the expression $\mathbf{x}^\top \mathbf{w}$ will become smaller, decreasing the likelihood of the prediction being 1.

3.4.4 Predictions Over New Samples & The ROC Curve

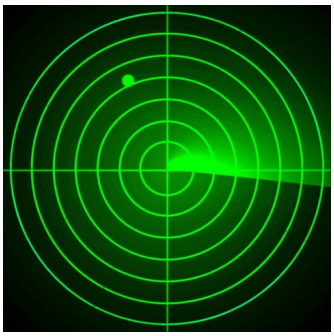
As we will encounter later in this chapter, in many classification scenarios we face the following question: Suppose we trained some classifier $h \in \mathcal{H}$ and derive classifications by the following rule: for some cutoff value $\alpha \in [0,1]$

$$\hat{y} := \begin{cases} 1 & h(\mathbf{x}) > \alpha \\ 0 & h(\mathbf{x}) \leq \alpha \end{cases}$$

How do we choose α? There is an important *tradeoff* in the selection of α. If we set α to be very high we are mainly going to predict 0. By doing so we are *less* likely to have false-positives (which is the error we try to avoid at all cost), for which we are pleased. However, at the same time, we are *also* more likely to have false-negatives. So by setting α too high we might have low a FPR but "miss" (misclassify) most of the positive samples. On the other extreme, if we set α to be very low we are mainly going to predict 1. So we will be *more* likely to have false-positives, but at the same time will be *less* likely to have false-negatives. So if we set α too low, we might have a high FPR but "catch" (correctly classify) most of the positive samples. Therefore, we see that changing $\alpha \in [0,1]$ governs some trade-off between the chances of making a Type-I error (false-positives) and correctly classifying positive samples.

This trade-off was first studied during World War II, when radar was invented. The designer of the radar had to choose when to put a green dot on the radar, indicating a target detected there. Sometime radar waves would bounce off back from clouds or birds, and the designer had to choose a *threshold* α. If the radar pulse returning is stronger than α, the radar screen would show a green dot. If weaker than α, no dot. Now, if α is set too low (say $\alpha = 0.1$), the screen would be full of a thousand green dots - since any bird or cloud (with, say, $h(\mathbf{x} = 0.2)$) would be classified as *positive*, a target. So that the radar will be full of false positives, false targets, and will be useless. On the other hand, if α is set too high (say $\alpha = 0.9$) then enemy airplanes (with,

say, $h(\mathbf{x} = 0.8)$) will not appear on the screen, since they will be classified by mistake as birds, and the radar again would be useless.



The radar engineers developed a way to visualize this tradeoff, which is still used today in machine learning. After training some linear model (choosing some hypothesis $h \in \mathcal{H}$) we make a grid of values of $\alpha \in [0,1]$. For each value of α we create a classifier by thresholding h at α, and calculate the number of Type-I and Type-II errors the classifier makes over a test sample that was not used for training. We plot a parametric curve of TPR (true positive rate) against FPR (false positive rate) when α is the parameter. This curve is called the *Receiver Operating Characteristic (ROC)* curve. It is continuous, increasing and goes from $(0,0)$ in the FPR-TPR plane (for $\alpha = 0$ we classify everything as negative, so no false positives and not true positives) to $(1,1)$ (for $\alpha = 1$ we classify everything as positive, so false positive rate is 1 - we make every possible Type-I error - and also true positive rate is 1 - we "catch" all the positive samples).

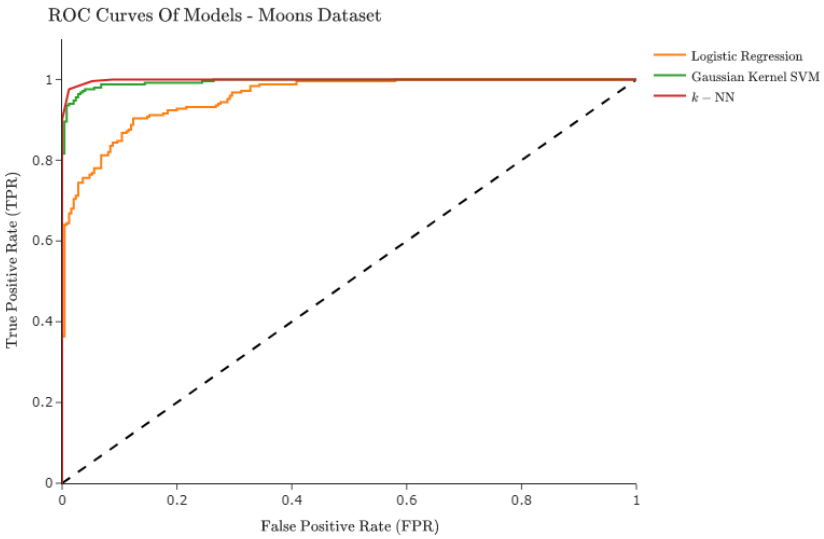


Figure 3.11: ROC Curve *of classifiers fitted over moons dataset.* *Chapter 3 Examples - Source Code*

If the ROC curve is a linear line from $(0,0)$ to $(1,1)$, the classifier is just a random guess. If a classifier has an ROC curve that is close to this linear line, it's a poor classifier. Now convince yourself that if the ROC curve rises sharply from $(0,0)$, for example makes a "jump" to $(FPR = 0.1, TPR = 0.9)$, it's a good classifier - we are able to correctly detect 0.9 of the positive samples at the price of 0.1 false positive rate.

Plotting the ROC curve of a classifier has a few different uses:

- **Tuning α:** It allows us to see the tradeoff, provided by the classifier, between Type-I errors and correct detection of positive samples, so we can choose the tuning of α we would like to work with for the

actual prediction.

- **AUC - Area Under Curve:** A performance measure for the tradeoff itself. This performance measure evaluates the prediction rule h we chose without having to decide on α - it measures the quality of the **tradeoff** provided by h, a tradeoff from which we must choose a specific point in order to actually classify new samples. AUC is simply the *definite integral* of the ROC curve on the segment $[0,1]$ - the area under the AUC curve. As mentioned above, AUC around $1/2$ means that h is poor - more specifically, that the *tradeoff* provided by h is poor. AUC is bounded from above by 1, so an AUC close to 1 means h offers an excellent trade-off, and in this case we expect to be able to find a cutoff α that gives a classifier with very few false-positives and very high detection rate (true positive rate).
- **Comparing candidate rules:** Suppose we have a couple of candidate rules h_1, h_2 (or more). For example, maybe we trained some classifier on the same training sample with different features, or maybe we trained two different types of classifiers over the same data, and we are wondering which one to use. Now we have a problem - we can't turn h_i into an actual classification rule without choosing a cutoff α_i, but would like to compare h_1 to h_2 without committing to a cutoff - to compare the tradeoff offered by h_1 to that offered by h_2. It is very useful here to plot the two ROC curves of h_1 and h_2 on a single axis - and visually compare the tradeoffs they offer.

3.4.5 Multiclass Logistic Regression

To be added

3.4.6 Learner ID Card

- **Hypothesis class:** The composite of the sigmoidal function over the linear functions (3.25)
- **Learning principle used for training:** Maximum likelihood
- **Computational implementation:** Specialized iterative method based on Netwon-Raphson iterations, or a general convex solver. When using a general convex solver we must pay attention to the effective rank of the regression matrix, similar to linear regression. Near-singular regression matrices will lead to numerical instabilities
- **Interpretability:** Given a fitted model we can interprate which features drive the classification as well as understand why a given sample was predicted as it was
- **Family of models:** As seen in **??** it is possible to add regularization terms to control the bias-variance properties of the fitted model
- **Storing fitted model:** Store the regression coefficients vector $\mathbf{w}$
- **Prediction of new sample:** To perform predictions we must specify a thresholding parameter $\alpha \in (0,1)$. Once we chose a value of α then prediction is performed by $\hat{y}_{new} := \mathbb{1}_{\sigma(\mathbf{x}_{new}^\top \mathbf{w}+b)\geq\alpha}$
- **When to use:** The logistic regression learner, especially when adding regularization terms, is a powerful learner. It is always good to try it, especially when classes are more or less balanced.

For the logistic regression learner we have adapted the hypothesis class of linear regression by composing it with the sigmoid function:

$$\mathcal{H}_{logistic} := \left\{ \mathbf{x} \mapsto \sigma\left(\mathbf{x}^\top \mathbf{w}\right) \;\middle|\; \mathbf{w} \in \mathbb{R}^d \right\}$$

Then, we have derived an optimization problem using the maximum likelihood principle (3.28). To computationally implement the learner there are specialized iterative methods based on Newton-Raphson iterations, or general convex solvers. It is important to note that just like linear regression we must pay attention to the effective rank of the regression matrix. Near-singular matrices will cause numerical problems.

Given trained model, we have to specify a threshold parameter α, which will provide some good tradeoff between the FPR and TPR. Once we have specified α prediction of a new sample is given by $\hat{y} := \mathbb{1}_{sigm(\mathbf{x}_{new}^\top \mathbf{w})\geq\alpha}$.

3.5 Bayes Classifiers

When deriving the logistic regression model, we assumed a probability distribution over the response set $\mathcal{Y}$ and treated the observations as deterministic values influencing the distribution of the response. We could however *assume* that both the response set and the domain set follow some *joint probability distribution* $\mathcal{F}$ over $\mathcal{X} \times \mathcal{Y}$. Under such assumption we are now able to look at the data from two different perspectives. Given the sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, we could first consider $\mathbf{x}_1, \dots, \mathbf{x}_m$ as fixed and learn $y_i|\mathbf{x}_i$. That is, the distribution of the response given the observation. This is the perspective used in the logistic regression, as well as the linear regression, model. For the second perspective we consider $y_1, \dots, y_m$ as fixed and ask how do the observations depend on the responses $\mathbf{x}_i|y_i$.

$$\overbrace{f_{Y|X=\mathbf{x}}(y) \cdot f_X(\mathbf{x})}^{\text{Perspective I}} = \overbrace{f_{X,Y}(\mathbf{x}, y)}^{\substack{\text{Joint Probability} \\ \text{Distribution}}} = \overbrace{f_{X|Y=y}(\mathbf{x}) \cdot f_Y(y)}^{\text{Perspective II}} \tag{3.29}$$

■ **Example 3.4** Consider the classification task of separating images of cats and dogs. Let the domain space be RBG images of 1024-by-1024 pixels and the response set be $\mathcal{Y} := \{\text{cat}, \text{dog}\}$. Further assume there exists some joint probability distribution $\mathcal{F}$ over $\mathcal{X} \times \mathcal{Y}$. Considering the first perspective where we wish to learn the conditional distribution $y_i|\mathbf{x}_i$. By doing so we try to discriminate a given picture being either of cat or of dog. That is, we simply try to understand how to differentiate between these two possibilities. If however we consider the second perspective, we wish to learn the conditional distribution of $\mathbf{x}_i|y_i$. This probability distribution describes what sort of observations might be seen for a given response. That is, what do pictures of cats or of dogs look like. ■

Besides providing insights into the manner in which different samples behave - how do cat pictures look? how do dog pictures look? - what benefit do we get from considering this second perspective? How can it be used for predicting the response of a given sample? To answer this question we use the Bayes' Law of conditional probability. Given a joint probability distribution function $f_{X,Y}$ over the observation $\mathbf{x}$ and response y we can express the conditional distribution $y|\mathbf{x}$ using the conditional distribution $\mathbf{x}|y$:

$$f_{Y|X=\mathbf{x}}(y) = \frac{f_{X|Y=y}(\mathbf{x}) \cdot f_Y(y)}{f_X(\mathbf{x})}$$

From this relation we are able to derive the Bayes Optimal classifier.

3.5.1 Maximum Aposteriori Estimation

Definition 3.5.1 Let $f_{\mathcal{D}}$ be a joint probability distribution function over $\mathcal{D} := \mathcal{X} \times \mathcal{Y}$. The *Bayes Optimal Classifier* is defined as

$$h^{Bayes}(\mathbf{x}) := \underset{y \in \mathcal{Y}}{\text{argmax}}\ f_{Y|X=\mathbf{x}}(y)$$

That is, we predict the response that (given the observation) achieves the highest probability. Since we are searching for a maximizer, we can use Bayes' Law to express the Bayes Optimal classifier as

$$h^{Bayes}(\mathbf{x}) := \underset{y \in \mathcal{Y}}{\text{argmax}}\ f_{Y|X=\mathbf{x}}(y) = \underset{y \in \mathcal{Y}}{\text{argmax}}\ \frac{f_{X|Y=y}(\mathbf{x}) f_Y(y)}{f_X(\mathbf{x})} \overset{(*)}{=} \underset{y \in \mathcal{Y}}{\text{argmax}}\ f_{X|Y=y}(\mathbf{x}) f_Y(y)$$

where $(*)$ is because given $\mathbf{x}$, $f_X(\mathbf{x})$ is constant over the different values of y. Notice that we have already seen this sort of algorithm (in the context of regression) when mentioning Bayesian statistics (subsubsection 1.1.3.1). The conditional $f_{X|y=y}$ is the *likelihood function* whose maximizer is the maximum likelihood estimator. It assesses the probability of observing $\mathbf{x}$ given that the response was y. The marginal distribution $f_Y(y)$ is the *prior* distribution and it assesses the *a-priori* probability (i.e belief) of receiving a sample with such a response. Therefore, the Bayes Optimal classifier weights the MLE according to the different class probabilities. The

conditional distribution $f_{Y|X=x}$ is called the *a-posteriori* distribution - the probability of the response *after* (i.e give) observing $\mathbf{x}$. This estimator is called the *Maximum A-Posteriori Estimator* (MAP) and is often denoted as $\hat{y}^{MAP}$.

What is left to explain where does the "Optimal" in "Bayes Optimal" comes from. For that, let us consider the misclassification loss function. It therefore holds that the Bayes Optimal classifier achieves the minimal misclassification risk out of all possible classifiers.

Theorem 3.5.1 Let $f_{X,Y}$ be a joint probability distribution function over $\mathcal{X} \times \mathcal{Y}$ for $\mathcal{Y} = [K]$, $K \in \mathbb{N}$. The Bayes optimal classifier is the optimal classifier with respect to the misclassification error. Namely that for any hypothesis $h : \mathcal{X} \to \mathcal{Y}$ it holds that $L_{\mathcal{D}}(h^{Bayes}) \leq L_{\mathcal{D}}(h)$.

Proof. Let $h : \mathcal{X} \to \mathcal{Y}$ be some hypothesis. The generalization error of h with respect to the misclassification loss is given by

$$\begin{array}{rcllcl} L_{\mathcal{D}}(h) & = & \mathbb{E}_{\mathbf{x},y}\left[h(\mathbf{x}) \neq y\right] & = & \int_{\mathbf{x},y} f_{X,Y}(\mathbf{x},y) \cdot \mathbb{1}_{h(\mathbf{x})\neq y} d(\mathbf{x},y) \\ & = & \int_{\mathbf{x}} f_X(\mathbf{x}) \sum_y f_{Y|X=\mathbf{x}}(y) \cdot \mathbb{1}_{h(\mathbf{x})\neq y} d\mathbf{x} & = & \int_{\mathbf{x}} f_X(\mathbf{x}) \left(1 - f_{Y|X=\mathbf{x}}(y) \cdot \mathbb{1}_{h(\mathbf{x})=y}\right) d\mathbf{x} \\ & = & \int_{\mathbf{x}} f_X(\mathbf{x}) \left(1 - f_{Y|X=\mathbf{x}}(h(\mathbf{x}))\right) d\mathbf{x} & & \end{array}$$

Since the Bayes classifier is defined to return the class maximizing the posterior then $f_{Y|X=\mathbf{x}}(h(\mathbf{x})) \leq f_{Y|X=\mathbf{x}}(h^{Bayes}(\mathbf{x}))$ and therefore:

$$\begin{aligned} L_{\mathcal{D}}(h) &= \int_{\mathbf{x}} f_X(\mathbf{x}) \left(1 - f_{Y|X=\mathbf{x}}(h(\mathbf{x}))\right) d\mathbf{x} \\ &\geq \int_{\mathbf{x}} f_X(\mathbf{x}) \left(1 - f_{Y|X=\mathbf{x}}(h^{Bayes}(\mathbf{x}))\right) d\mathbf{x} \\ &= \mathop{\mathbb{E}}_{(\mathbf{x},y)\sim\mathcal{D}} \left[h^{Bayes}(\mathbf{x}) \neq y\right] \\ &= L_{\mathcal{D}}\left(h^{Bayes}\right) \end{aligned}$$

Thus, $L_{\mathcal{D}}(h^{Bayes}) \leq L_{\mathcal{D}}(h)$ and we conclude the optimality of the Bayes classifier. ■

It is important to note that in reality *we do not know the underlying distribution* $\mathcal{D}$, to whom all we have is a mere window in the form of the dataset. Therefore, we *cannot program* an algorithm that would find the maximizer of the posterior distribution. As such, we must think of the Bayes optimal classifier as an *Oracle* - a "black box" entity capable of solving the problem of finding the maximizer of the posterior.

If however implementing the Bayes optimal classifier is not feasible is it of any practical use? Though we do not know $\mathcal{D}$ we might still have some prior insights into the manner by which the data behaves. For example we might have some prior knowledge regarding the prevalence of different labels or we might assume that for different responses different feature values are more likely to be observed. We can incorporate these insights into the derived model. Then, if these assumptions hold, we might be able to provide a realization of the Bayes optimal classifier. Below are two examples for such realizations.

3.5.2 Linear Discriminant Analysis

The Linear Discriminant Analysis (LDA) algorithm is a realization of the Bayes Optimal classifier. In this model we assume that samples of different labels have different Gaussian distributions.

Definition 3.5.2 Let $\Omega = \{1, \ldots, K\}$ for $K \in \mathbb{N}$ be a sample space. A random variable $X : \Omega \to [0,1]$ follows a *Multinomial* distribution with parameter $\pi \in [0,1]^K, \sum \pi_i = 1$ if $\mathbb{P}(X = j) = \pi_j$, $j \in [K]$. We denote $X \sim \text{Mult}(\pi)$.

Explicitly, the LDA model assumes the following generative model:

1. Each sample "selects" a label y_i according to a multinomial distribution with K classes.
2. Then, the sample itself is drawn from the conditional probability of $X|Y$ where X denotes the random variable of sampling some samples $X = \mathbf{x}$ and Y denotes the random variable of $Y = y$, $y \in [K]$. The distribution used to model $X|Y$ is a Gaussian distribution where each label is characterized by a different mean vector $\{\mu_k \in \mathbb{R}^d\}_{k=1}^K$ but the same covariance matrix $\Sigma \in \mathbb{R}^{d\times d}$.

Namely, for any $i \in 1,\ldots,m$ we assume that:

$$\begin{aligned} y_i &\sim \text{Mult}(\pi) \\ \mathbf{x}_i|y_i &\sim \mathcal{N}(\mu_{y_i}, \Sigma) \end{aligned} \tag{3.30}$$

Under these assumptions, predicting the class of a new sample is done by simply using the Bayes Law over the Bayes Optimal classifier to get:

$$\hat{y}(\mathbf{x}) \coloneqq \underset{y}{\text{argmax}}\ \mathbb{P}(y|\mathbf{x}) = \underset{y}{\text{argmax}}\ \frac{\mathbb{P}(\mathbf{x}|y)\,\mathbb{P}(y)}{\mathbb{P}(x)}$$

Claim 3.5.2 Let $f_{X,Y}$ be the pdf of $\mathcal{D}$ a joint distribution over $\mathcal{X}\times\mathcal{Y}$ and suppose

$$y \sim \text{Mult}(\pi), \quad y|\mathbf{x} \sim \mathcal{N}(\mu_k, \Sigma)$$

for $\pi \in [0,1]^K$, $\sum \pi_k = 1$. Then the Bayes Optimal classifier is given by:

$$\hat{y}(\mathbf{x}) \coloneqq \underset{k}{\text{argmax}}\ a_k^\top \mathbf{x} + b_k, \quad a_k \coloneqq \Sigma^{-1}\mu_k,\ b_k \coloneqq \log(\pi_k) - \tfrac{1}{2}\mu_k\Sigma^{-1}\mu_k$$

Proof. To prove the claim we begin with expressing $f_{Y|X}(k)$ using Bayes Law:

$$f_{Y|X=\mathbf{x}}(k) = \frac{f_{X|Y=k}(\mathbf{x})\cdot f_Y(k)}{f_X(\mathbf{x})} = \frac{f_{X|Y=k}(\mathbf{x})\cdot f_Y(k)}{\sum_{k'} f_{X|Y=k'}(\mathbf{x})\cdot f_Y(k')} = \frac{\pi_k\cdot\mathcal{N}(\mathbf{x}|\mu_k,\Sigma)}{\sum_{k'}\pi_{k'}\cdot\mathcal{N}(\mathbf{x}|\mu_{k'},\Sigma)}$$

Notice, that since we wish to maximize the posterior distribution $f_{Y|X}$ for a *given* sample $\mathbf{x}$, we can ignore the evidence $f_X(\mathbf{x})$. Then, by the pdf of the multivatiate Gaussian (**??**) then:

$$\begin{aligned} \text{argmax}_k f_{Y|X=\mathbf{x}}(k) &= \text{argmax}_k \frac{f_{X|Y=k}(\mathbf{x})\cdot f_Y(k)}{f_X(\mathbf{x})} \\ &= \text{argmax}_k \pi_k\cdot\mathcal{N}(\mathbf{x}|\mu_k,\Sigma) \\ &= \text{argmax}_k \pi_k\cdot\tfrac{1}{Z}\exp\left(-\tfrac{1}{2}(\mathbf{x}-\mu_k)^\top\Sigma^{-1}(\mathbf{x}-\mu_k)\right) \\ &= \text{argmax}_k \log(\pi_k) - \tfrac{1}{2}\mathbf{x}^\top\Sigma^{-1}\mathbf{x} + \mathbf{x}^\top\Sigma^{-1}\mu_k - \tfrac{1}{2}\mu_k\Sigma^{-1}\mu_k \\ &= \text{argmax}_k \log(\pi_k) + \mathbf{x}^\top\Sigma^{-1}\mu_k - \tfrac{1}{2}\mu_k\Sigma^{-1}\mu_k \end{aligned}$$

for $Z \coloneqq \sqrt{(2\pi)^d|\Sigma|}$ the Gaussians' normalization factor. Denote $a_k \coloneqq \Sigma^{-1}\mu_k, b_k \coloneqq \log(\pi_k) - \frac{1}{2}\mu_k\Sigma^{-1}\mu_k$ and we conclude that $\hat{y}(\mathbf{x}) = \text{argmax}_k\ a_k^\top\mathbf{x} + b_k$. ■

Notice, that we were able to remove $\mathbf{x}^\top\Sigma^{-1}\mathbf{x}$ since we assumed that the classes are generated from Gaussians with the *same* covariance matrix, and therefore the expression did not depend on any specific class k. The claim above, besides showing that under the LDA assumptions we are dealing with a Bayes classifier, also tells us something about the classifier learned. Looking at the expression derived from the assumptions, we see that the classification is in fact done by some *linear separator/discriminant*.

It can be shown, by taking the $\log -likelihood$ ratio between the likelihood for being classified for a class divided the likelihood for being classified for the other class, that the decision boundary between the classes is linear, similar to Figure 3.12.

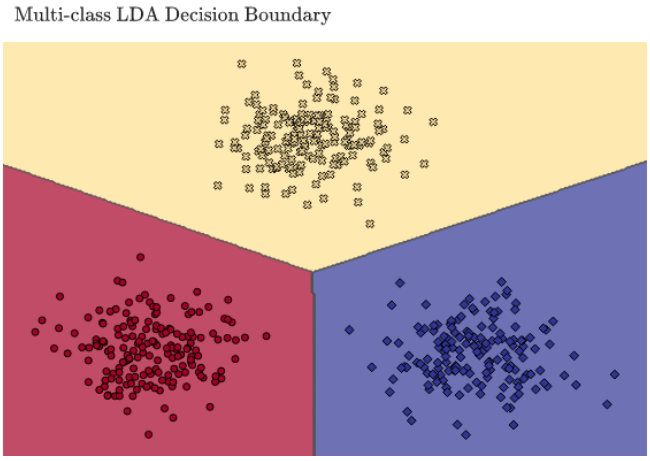


Figure 3.12: LDA Decision Boundaries *for a multiclass setup of three Gaussians. Chapter 3 Examples - Source Code*

Learning A LDA Classifier

So, in order to predict using an LDA classifier we need to know the class probabilities π, the Gaussian centers $\{\mu_i\}$ and the covariance matrixmeans Σ. To do so we derive the maximum likelihood estimators. Let us generalize the binary LDA model (i.e. of classification) to a multiclassification LDA model.
Then, the LDA model assumptions are:

$$\begin{aligned} y &\sim \text{Mult}(\pi) \\ x|y=k &\sim \mathcal{N}(\mu_k, \Sigma) \end{aligned} \tag{3.31}$$

Given a training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ then the likelihood is given by:

$$\begin{aligned} \mathcal{L}(\Theta|\mathbf{X},\mathbf{y}) &= f_{X,Y|\Theta}\left(\{(\mathbf{x}_i,y_i)\}_{i=1}^m\right) \\ &\overset{iid}{=} \prod_{i=1}^m f_{X,Y|\Theta}(\mathbf{x}_i,y_i) \\ &= \prod_{i=1}^m f_{X|Y=y_i}(\mathbf{x}_i)\cdot f_{Y|\Theta}(y_i) \\ &= \prod_{i=1}^m \mathcal{N}(\mathbf{x}_i|\mu_{y_i},\Sigma)\cdot \text{Mult}(y_i|\pi) \end{aligned}$$

Since the log transformation is monotonous increasing finding the maximizer of the likelihood is equivalent to finding the maximizer of the log-likelihood.

$$\begin{aligned} \ell(\Theta|\mathbf{X},\mathbf{y}) &= \log\left(\textstyle\prod_i \mathcal{N}(\mathbf{x}_i|\mu_{y_i},\Sigma)\cdot \text{Mult}(y_i|\pi)\right) \\ &= \textstyle\sum_i \log\left(\mathcal{N}(\mathbf{x}_i|\mu_{y_i},\Sigma)\right) + \log\left(\text{Mult}(y_i|\pi)\right) \\ &= \textstyle\sum_i \log\left(\frac{1}{\sqrt{(2\pi)^d|\Sigma|}}\exp\left(-\frac{1}{2}(\mathbf{x}_i-\mu_{y_i})^\top\Sigma^{-1}(\mathbf{x}_i-\mu_{y_i})\right)\right) + \log(\pi_{y_i}) \\ &= \textstyle\sum_i \log(\pi_{y_i}) - \frac{d}{2}\log(2\pi) - \frac{1}{2}\log|\Sigma| - \frac{1}{2}(\mathbf{x}_i-\mu_{y_i})^\top\Sigma^{-1}(\mathbf{x}_i-\mu_{y_i}) \\ &= \textstyle\sum_k\left[n_k\cdot\log(\pi_k) - \frac{1}{2}\sum_i(\mathbf{x}_i-\mu_k)^\top\Sigma^{-1}(\mathbf{x}_i-\mu_k)\right] - \frac{md}{2}\log(2\pi) - \frac{m}{2}\log|\Sigma| \end{aligned}$$

for $n_k = \sum_i \mathbb{1}_{y_i=k}$. To find the maximizers we derive with respect to the different parameters $\{\pi_k\}, \{\mu_k\}, \Sigma$ and equate to zero. However, before doing so recall the constraint on π: $\pi \in [0,1]^K$, $\sum_k \pi_k = 1$. To solve the optimization problem with the constraint we use the Lagrange Multipliers method. Since the constraint is $\sum_k \pi_k = 1 \iff \sum_k \pi_k - 1 = 0$, we define the function $g(\pi) = \sum_k \pi_k - 1$ and the Lagrangian

$$\mathcal{L} = \ell(\Theta|\mathbf{X}, \mathbf{y}) - \lambda g(\pi)$$

Now, we derive with respect to each of the parameters including λ. Beginning with the class probabilities then:

$$\frac{\partial \mathcal{L}}{\partial \pi_k} = \frac{\partial}{\partial \pi_k} \ell(\Theta|\mathbf{X}, \mathbf{y}) - \lambda \frac{\partial}{\partial \pi_k} g(\pi) = \frac{n_k}{\pi_k} - \lambda = 0 \quad \Rightarrow \quad \pi_k = \frac{n_k}{\lambda} \tag{3.32}$$

To find the value of λ we replace π in the constraint with the expression found in (3.32).

$$1 = \sum_k \pi_k = \sum_k \frac{n_k}{\lambda} \quad \iff \quad \lambda = m$$

and therefore, the MLE of the class probabilities are $\hat{\pi}_k^{MLE} = \frac{n_k}{m}$. To find the MLE of the Gaussian parameters notice that the log-likelihood above is identical to the one derived of a single Gaussian while considering only samples sharing the same label. As such

$$\hat{\mu}_k^{MLE} = \frac{1}{n_k} \sum_i \mathbb{1}_{y_i=k} \mathbf{x}_i, \qquad \hat{\Sigma}^{MLE} = \frac{1}{m} \sum_i \left(\mathbf{x}_i - \hat{\mu}_{y_i}^{MLE}\right) \left(\mathbf{x}_i - \hat{\mu}_{y_i}^{MLE}\right)^\top \tag{3.33}$$

Looking closely at the expressions derived we in fact realize that the MLE predicts the values proportional to what is found in the training set.

R This estimator described in 3.33 is known as the *pooled covariance* where we take into account that different samples originate from different Gaussians and therefore should use the sample mean estimator of their own Gaussian. This is a *biased* pooled covariance estimator. The unbiased estimator is given by replacing the $\frac{1}{m}$ factor with $\frac{1}{m-K}$, where K is the number of classes.

3.5.3 Quadratic Discriminant Analysis

In the LDA algorithm we assumed the data is generated from a set of Gaussians, differing in their mean but sharing the same covariance matrix (3.30). The Quadratic Discriminant Analysis algorithm allows different covariance matrices. That is, for any $i \in 1, \ldots, m$ we assume that:

$$\begin{aligned} y_i &\sim \text{Mult}(\pi) \\ \mathbf{x}_i | y_i &\sim \mathcal{N}(\mu_{y_i}, \Sigma_{y_i}) \end{aligned} \tag{3.34}$$

By enabling different covariance matrices the quadratic expression (in $\mathbf{x}$) of $\mathbb{P}(y = k|\mathbf{x})$ does not cancel out. This in turn causes the decision boundaries between classes to be quadratic rather than linear. In both Figure 3.12 and Figure 3.13 the same data was used to fit either the LDA or the QDA models. We can see that while the decision boundaries of the LDA fit (Figure 3.12) are linear, in the case of QDA (Figure 3.13) we get curved (quadratic) boundaries.

Learning A QDA Classifier

Fitting a QDA classifier is very similar to the process of fitting a LDA classifier. The difference is in the estimation of the covariance matrices. In this case we fit a different covariance matrix for each class based on the samples of the class:

$$\hat{\Sigma}_k^{MLE} := \frac{1}{m_k} \sum_{i:y_i=k} \left(\mathbf{x}_i - \hat{\mu}_k^{MLE}\right) \left(\mathbf{x}_i - \hat{\mu}_k^{MLE}\right)^\top \tag{3.35}$$

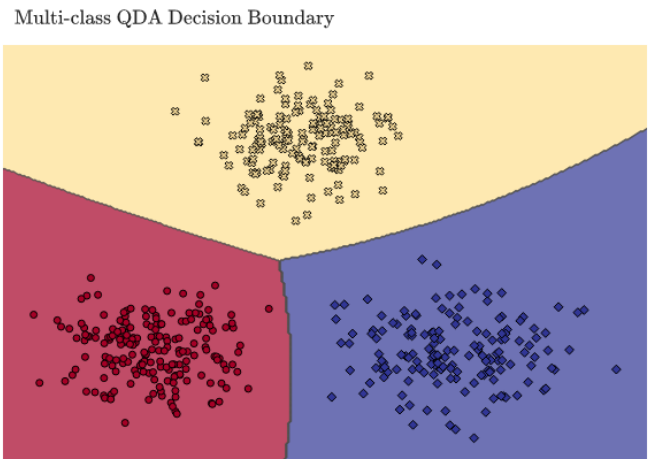


Figure 3.13: QDA Decision Boundaries *for a multiclass setup of three Gaussians. Chapter 3 Examples - Source Code*

3.6 Nearest Neighbors

Nearest Neighbors classifiers are a popular, simple and effective learner in which we predict a sample's response based on a set of "nearest" training samples. This classifier is **not** based on the paradigm of a hypothesis class and learning principle. It is a *model free* learner and has no training stage. Instead, when given a training set, we store it in some manner. Then, when we are given a new sample to predict its response we "simply" find the subset of training samples nearest to the new sample, with respect to some measure of distance, and make a prediction based on the responses of those neighbor samples.

R This family of leaners are part of a wider *graph-based approach* for learning. In this approach we first define some graph structure over the samples - forming the nodes of the graph. Then, using the constructed graph we perform training and prediction. The different learners differ in how to define edges in the graph; are they weighted or not? how to transition between nodes; and how is this structure used for training and prediction. Another graphed-based approach that will be seen later is of Spectral Clustering **??**.

3.6.1 Prediction Using k-NN

Let us begin with the simplest form of k-NN. The first step is to determine two hyper-parameters required by the algorithm: an integer k (the number of neighbors to use) and a distance function $\rho : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}_+$. We can decide for example to use the square Euclidean norm $\rho(\mathbf{x}_1, \mathbf{x}_2) := ||\mathbf{x}_1 - \mathbf{x}_2||^2$ or a weighted square norm giving different importance levels to different features $\rho(\mathbf{x}_1, \mathbf{x}_2) := \sum \omega_i((\mathbf{x}_1)_j - (\mathbf{x}_2)_j)^2$.

Then, given a training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ the prediction is done as follows:

3.6.2 Selecting Value of k Hyper-Parameter

A very important aspect in k-NN is the chosen value of k. Though methods for determining the "right" k will be discussed in future chapters, let us dwell on a few cases:

- $k = 1$**:** The test point is given the label of the single nearest neighbor in the training set. Such classifier has a very low bias but very high variances.
- $k = m$**:** The classifier predicts a single label for any given test sample, regardless to its values. It will predict the majority vote of the training set labels. In this case the bias is very high and the variance is zero.

Algorithm 2 k-NN

procedure k-NN(k, ρ, S,$\mathbf{x}'$)▷ Where k, ρ are the pre-determined hyper-parameters, S the training set and $\mathbf{x}'$ the sample to predict for

Compute distance from $\mathbf{x}'$ with respect to ρ: $\forall \mathbf{x} \in S \quad d_{\mathbf{x}} := \rho(\mathbf{x}', \mathbf{x})$.

Denote $\pi = (\pi_1, \ldots, \pi_m)$ the permutation of $(1, \ldots, m)$ such that $d_{\mathbf{x}_{\pi_1}} \leq \ldots \leq d_{\mathbf{x}_{\pi_m}}$

Select k nearest samples $\mathbf{x}_{\pi_1}, \ldots, \mathbf{x}_{\pi_k}$ and predict by majority vote:

$$\hat{y} := \underset{y \in \{0,1\}}{\operatorname{argmax}} \sum_{i=1}^{k} \mathbb{1}_{y_{\pi_i} = y}$$

return $\hat{y}$

end procedure

As we change k we change the bias-variance tradeoff, with larger values of k creating simpler models while smaller values of k creating more complex models (Figure 3.14).

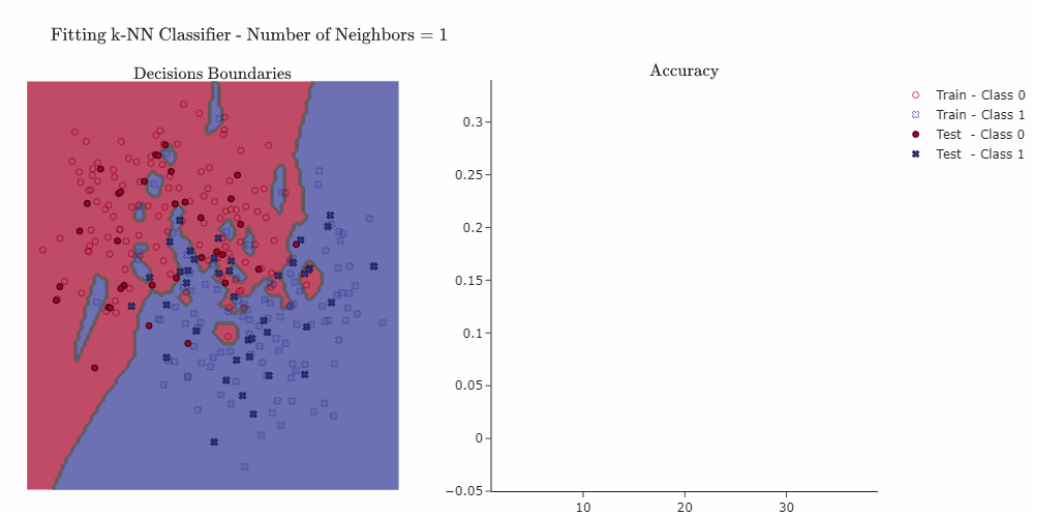


Figure 3.14: ***Decision Boundaries of k-NN:*** *Fitting model over dataset for different values of k.* *Chapter 3 Examples - Source Code*

3.6.3 Computational Implementation

Implementing a k-nearest-neighbors classifier is very easy on small datasets, but becomes computationally challenging (either in terms of execution time or in terms of space) when d and/or m are large. There are generally three types of implementation approaches:

- **Brute force implementation:** We keep the entire training sample S in storage during the entire prediction process. For each new test sample $\mathbf{x} \in \mathbb{R}^d$ we calculate $\rho(\mathbf{x}, \mathbf{x}_i)$ $i \in [m]$ and partially sort to find the k smallest distances.
  Suppose ρ is the Euclidean distance. What are the computational costs of prediction? As the sample space is $\mathbb{R}^d$ computing the distance between two points is $\mathcal{O}(d)$. Doing so for all points in the dataset is $\mathcal{O}(dm)$. Next we want to retrieve the k nearest train samples. If $k \ll m$ we can retrieve k times the

sample of minimal distance (without repeating previously selected samples) in a time complexity of $\mathcal{O}(km)$. However, if $k \approx ....$ then it is more computationally efficient to sort all distances and then select the k minimal. Lastly, summation over selected samples is done in $\mathcal{O}(k)$. All together the time complexity of such approach is $\mathcal{O}(dm+km)$. In terms of space complexity we must store distances of all training samples and thus $\mathcal{O}(m)$.

- **Exact nearest neighbors search with preprocessed data structure:** Depending on the selection of ρ, we could pre-process the training sample and construct a special data structure. After doing so in the training step, we can use this data structure to quickly locate the k nearest neighbors of a given test sample. In the case of ρ being the Euclidean distance we could you an algorithm such as *kd-tree*.

- **Fast randomized nearest neighbors search:** Beyond the scope of this course.

3.6.4 Learner ID Card

- **Hypothesis class:** This is a "model free" learner and therefore has no hypothesis class
- **Learning principle used for training:** There is no training phase for this learner
- **Computational implementation:** Different strategies for calculating the nearest neighbors. Simplest method is by brute force nearest neighbor search
- **Interpretability:** We do not know why s given sample was predicted as it was. We can only explain near what other training samples it is
- **Family of models:** Indexed according to the hyper-parameter k
- **Storing fitted model:** Must store the entire training sample or some preprocessed data structure
- **Prediction of new sample:** Find the k samples in the training set closest (with respect to the used metric) to the given sample. Predict based on the majority vote of these samples
- **When to use:** When implementation is computationally feasible try this model.

3.7 Decision Trees

Decision Trees are classification and regression methods by which we partition the sample space into disjoint parts. Then, given such a partition, the response of our classification (or regression) is computed based on the training samples in the partition of the observation in question. These methods are very intuitive and yet capture many interesting aspects of learning. We will discuss some of these aspects in details in the following chapter.

To this day, one of the more powerful classification and regression algorithms is what is called: Classification And Regression Trees (CART) Random Forest. It uses the power of committee decisions over the basic decision trees to achieve very good performances. Some of the aspects of this algorithm will be discussed in later chapters.

3.7.1 Axis-Parallel Partitioning of $\mathbb{R}^d$

Earlier in this chapter we have discussed two classifiers that use piecewise-constant prediction rules: half-spaces and SVM. For both, the hypothesis class consisted of half-spaces where prediction was determined by position of sample with respect to the hyper-plane. For decision trees we will describe a more complicated piecewise-constant prediction rule (more complex hypotheses). Let us consider a rule that partitions the sample space $\mathbb{R}^d$ into **axis-parallel boxes, or "hyper-rectangles"** where each box is associated with labels 1 or -1. The learner's task would be to use the training sample to "chop" the samples space $\mathcal{X}$ int a disjoint union of axis-parallel boxes, and to assign a class prediction to each box.
To make out hypothesis $\mathcal{H}_{CT}$ class smaller and simpler, we will focus on disjoint unions of boxes that are obtained by iteratively splitting an existing box into two smaller boxes along one of the axes:

- We start with the whole sample space $\mathbb{R}^d$.

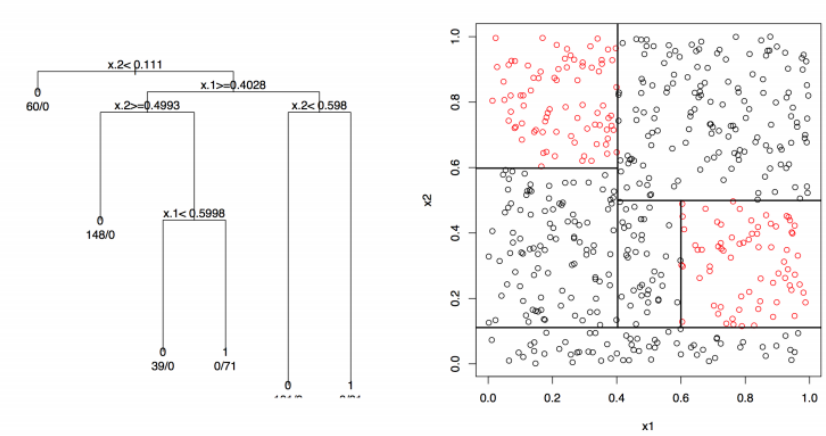


Figure 3.15: *Decision tree and induced partitioning of* $\mathbb{R}^2$ *sample space*

- By selecting some coordinate $i_1 \in [d]$ and some value $t_1 \in \mathbb{R}$ we split R^d into two axis-parallel "boxes" (half-spaces). We obtain:

$$B_1^+ = \left\{ \mathbf{x} \in \mathbb{R}^d | \mathbf{x}_{i_1} > t_1 \right\}, \quad B_1^- = \left\{ \mathbf{x} \in \mathbb{R}^d | \mathbf{x}_{i_1} \leq t_i \right\}$$

- Next, by focusing of some previously split "box" B_j^s for $s \in \{-,+\}$, we can again select some coordinate $i_{j+1} \in [d]$ and some splitting value $t_{j+1} \in \mathbb{R}^d$ to obtain B_{j+1}^-, B_{j+1}^+. Notice that B_{j+1}^- and B_{j+1}^+ are disjoint, and if following this procedure then by induction they are also disjoint from any other obtained box.

Note that the partitions obtained this way are special - most partitions of $\mathbb{R}^d$ into axis-aligned boxes are not Tree Partitions. Namely, cannot be constructed by such a top-down iterative chopping procedure.

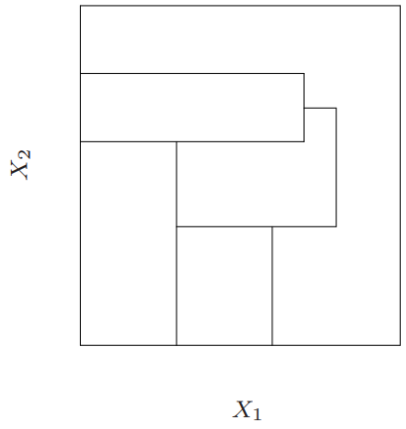


Figure 3.16: *Partitioning* $\mathbb{R}^2$ *into axis-aligned boxes not describing a tree partition*

3.7.2 Classification & Regression Trees

The hypothesis class $\mathcal{H}_{CT}$ we will consider consists of piecewise-constant functions, that assign a class prediction (1 or 0) to each box in a Tree Partition. Unless we restrict it somehow, the class contains all piecewise-constant functions supported on all Tree Partitions of $\mathbb{R}^d$ (to any number of boxes). Formally, for a

Tree Partition $\mathbb{R}^d = \biguplus_{j=1}^{N} B_j$ of $\mathbb{R}^d$ into N boxes, and label assignments $c_j \in \{0,1\}$ ($j = 1,\ldots,N$) assigning label c_j to box B_j, the hypothesis $h \in \mathcal{H}_{CT}$ is a function $h : \mathbb{R}^d \to \{0,1\}$ defined by

$$h(\mathbf{x}) \coloneqq \sum_{j=1}^{N} c_j \mathbb{1}_{\mathbf{x}\in B_j}$$

■ **Example 3.5** Consider the following scenario: suppose someone comes into a hispital emergency room. The first step of triage is to determine - fast - whether they are in a life-threatening medical emergency, or else they can wait in line and receive treatment in a little while. The triage uses a sequence of yes/no questions, such as: Is the patient conscious yes/no?

- If not conscious: classify as **emergency**
- If patient is conscious: is the patient's pulse < 40 beats per minute?
  - If yes (pulse < 40): classify as textbfemergency
  - If no, (pulse ≥ 40): is the patient's pulse > 130 beats per minute?
    - If yes (pulse > 130): is the patient's systolic blood pressure < 80 mmHg?
      - If yes classify as **emergency**
      - If not, is the patient's systolic blood pressure > 140 mmHg? If yes, classify as **emergency**. Otherwise, classify as **no emergency**
    - If not classify as **no emergency**

This is a decision tree that uses three features: conscious (a binary categorical feature), pulse (a numerical feature) and blood pressure (also a numerical feature). See if you can we write a diagram for this decision tree in the shape of a tree, where every node is a question, and every leaf is a decision / classification. The root of the tree is the first question ("conscious yes/no?"). Now observe that every function in our Classification Trees hypothesis class $\mathcal{H}_{CT}$ is equivalent to a decision tree. In the notations of the generic example above, the first question is: "$x_{i_1} > t_1$-yes/no?". If yes, we ask the second question "$x_{i_{2,1}} > t_{2,1}$ - yes/no?". If not, we ask the second question: "$x_{i_{2,2}} > t_{2,2}$ - yes/no?". And so on, until there are no more splits and we have reached a box over which the function in $\mathcal{H}_{CT}$ is constant. If the constant value is 1, we classify / predict class 1. If the constant value is 0, we predict class 0. This is why our hypothesis class is called - classification trees ■

3.7.3 Growing a Classification Tree

Having defined our hypothesis class, the next question is what learning principle to use. That is, how shall be select $h_s \in \mathcal{H}_{CT}$ based on the training sample S. Suppose we have already obtained a Tree Partition of $\mathbb{R}^d$ is some manner, that consists of N disjoint boxes $\mathbb{R}^d = \biguplus_{j=1}^{N} B_j$. Let $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^{m}$ be our taining set and denote the predicted label assigned to box B_j by $\hat{y}(B_j) \in \{0,1\}$. As such, the number of misclassification errors that are incurred by the training sample that fall inside B_j is

$$\sum_{\mathbf{x}_i \in B_j} \mathbb{1}\left[y_i \neq \hat{y}(B_j)\right]$$

Let us begin learning by applying the ERM principle. Denote the fraction of misclassified samples with label $y \in \{0,1\}$ in some box B by:

$$\ell_S(B,y) \coloneqq \frac{1}{|B|} \sum_{\mathbf{x}_i \in B} \mathbb{1}\left[y_i \neq y\right]$$

The label that will minimize the empirical risk for those training samples in box B is the **majority vote** over the labels. So, for any sample falling in box B we would predict

$$\hat{y}_S(B) \coloneqq \operatorname*{argmin}_{y\in\{0,1\}} \ell_S(B,y)$$

Applying over the entire Tree Partition, minimizing the empirical risk is achieved by labeling box B_j with $\hat{y}_S(B_j)$, $j \in [N]$. Therefore, for a given training set S, every Tree Partition corresponds with a unique label

assignment, and as such, a unique classification tree $h \in \mathcal{H}_{CT}$ that minimizes the empirical risk. It seems therefore, that finding the desired ERM tree is done by solving

$$h^* := \underset{h \in \mathcal{H}_{CT}}{\operatorname{argmin}} \; L_S(h)$$

where $L_S(h)$ is the misclassification error of h over S. Looking back at the described procedure is it therefore possible to describe which tree would minimize the empirical risk and therefore be selected (for any training set S)? Consider the tree where the number of leaves is $|S|$ and each sample is in a box containing only itself. Following the prediction rule we devised, such a tree would achieve $L_S(h) = 0$. Though we achieved the lowest possible empirical risk, this tree will fail to generalize to new samples. To cope with this problem we should limit the number of levels in the classification tree (equivalent for limiting number of leaves). Denote $\mathcal{H}^k_{CT}$ the hypothesis class of all tree partitions with at most k levels. Now, we will choose k and then using the ERM principle return

$$h^* := \underset{h \in \mathcal{H}^k_{CT}}{\operatorname{argmin}} \; L_S(h) \tag{3.36}$$

Selecting A Value For k:

Note that by adding the hyper-parameter k we now have *a family of hypothesis classes*, one for each value of k. The value of k controls the size of the hypothesis class and therefore controls the bias-variance tradeoff (Figure 3.17):

- For small values of k, the hypothesis class is smaller, containing trees of smaller sizes. Therefore the ERM learner will have a **higher** bias as it can only select simple Tree Partitions. It will also have a **lower** variance: as the boxes are very large, the labels assigned to each box are based on a majority vote of typically many training samples. Therefore changing a few training samples will barely change the selected hypothesis.
- For large values of k, the hypothesis class is much more complex, with more "specialized" trees in it. Therefore the ERM learner will have a **lower** bias and **higher** variance.

Later in the course we will introduce a few methods for selecting the value of k.

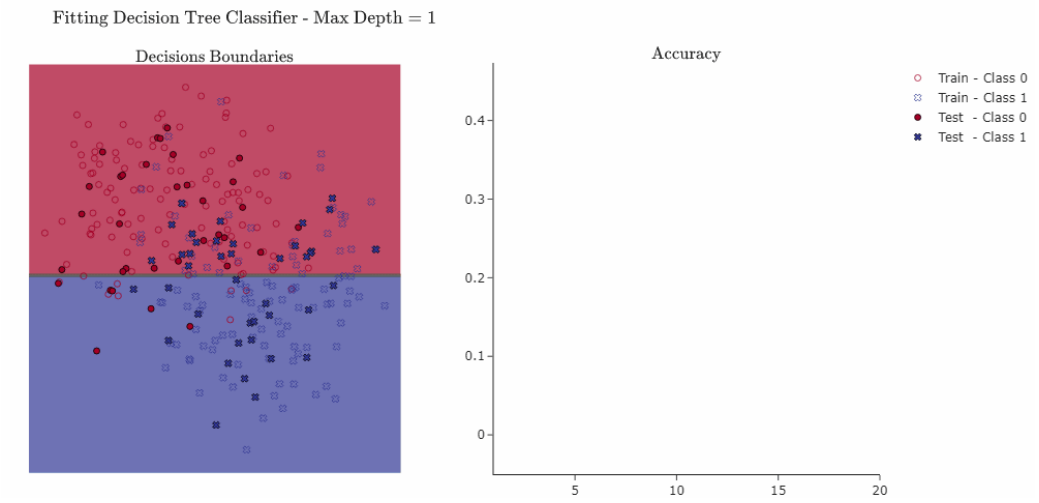


Figure 3.17: ***Decision Boundaries of Decision Trees:*** *Fitting model over dataset for different values of max depth k.* *Chapter 3 Examples - Source Code*

3.7.4 CART Heuristic For Growing Trees

The next challenge is how to find the minimizer of (3.36) computationally? So far, all the ERM learners we encountered were **computationally tractable**:

- The linear regression optimization problem was based on ERM. We were able to find aclosed form expression for the minimizer.
- The Half-space classifier was based on ERM and lead to a simple convex optimization problem.

In contrast to those examples the search space over $\mathcal{H}^k_{CT}$ is exponentially large and has no Euclidean or other structure to be used. Finding an ERM solution would mean to use brute-force search, which is infeasible. In fact, it has been proven that implementing ERM on $\mathcal{H}^k_{CT}$ is an NP-Hard problem with respect to the training sample size[1] .

This is our first encounter with the bitter truth that though the ERM principle is nice, it is often impossible to implement efficiently, especially when the hypothesis class has no Euclidean structure. Therefore, we must resort to defining and using **heuristics**: an approach to solving the optimization problem that does not guaranteed to be optimal, but is still sufficient for finding a solution. While the definition of decision trees, the hypothesis class and prediction assignment to boxes in a tree partition are all canonical, there are several different heuristic approaches to the way we "grow a decision tree', namely to the way we choose an hypothesis in practice.

One common approach, coming out of the statistical learning community, is called **Classification and Regression Trees** (CART). This heuristic cinsists of two stages: **growing** the tree, resulting in a tree that is a little too large, and then **pruning** it to bring it down to the most effective size.

Suppose we have chosen k to be the maximal tree depth. The heuristic of growing a full decision tree with at most k levels will proceed top-down, starting from $\mathbb{R}^d$ and progressively chopping each box into two boxes. A given box is **not chopped** if either:

- The maximum number of levels k has been reached.
- The box has reached a pre-determined minimal number of training samples. At the very least we would not split a box if it consists of only a single training sample.

Chopping is done by finding the **best** coordinate, at the **best** value to chop, and whenever you chop given each half-box the **best** class assignment, in the sense of minimizing misclassification error over the training sample. Formally, the pseudocode of the CART heuristic is seen in Algorithm 3.

Time Complexity Analysis

Before we introduced the CART heuristic we described that solving the ERM principle over this hypothesis class is NP-Complete and therefore cannot be done in polynomial time. Let us see that the CAR heuristic can indeed be computed efficiently.

The algorithm iteratively splits boxes into two by finding a coordinate $i \in [d]$ and a value $t \in \mathbb{R}$. It scans all d coordinates and for each scans all possible values of t. Notice, that even though $t \in \mathbb{R}$ we do not need to try all values and it suffices to check only the values in the i'th coordinate of the training sample: $\{\mathbf{x}_i | \mathbf{x} \in S\}$. As we have m samples we only need to evaluate for at most m values, giving each step a time complexity of $\mathcal{O}(md)$.

The next question is how many steps will the algorithm perform? We know that the algorithm will terminate after growing a tree with at most k levels. Such a tree will have at most $2^k - 1$ nodes and leaves. Though this seems exponentinal in the given input (notice that the hyper-parameter k is also part of the input) we can upper bound this value. As we do not allow empty boxes (and in fact any box with less than some minimal number

[1] By reduction from "three dimensional matching", see Hyafil and Rovest, "Constructing Optimal Binary Decision Trees is NP-Complete", Information Processing Letters 5(1), 1976

Algorithm 3 CART - For Growing Classification Tree

procedure CART($S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, k, m_{min})
  $Tree - Partition \leftarrow \emptyset$
  $Boxes \leftarrow \left\{\mathbb{R}^d\right\}$ ▷ Entire sample space as initial box
  while $Boxes \neq \emptyset$ **do**
    $B \leftarrow \text{pop}\,(Boxes)$
    if $|B| \leq m_{min}$ or depth at B reached k **then**
      $Tree - Partition \leftarrow Tree - Partition \cup \{B\}$
      continue
    end if
    for all feature $i \in [d]$ **do** ▷ Scan all features
      for all threshold value $t \in \mathbb{R}$ **do** ▷ Scan thresholds for features
        Split B along coordinate i at value t:

$$B_{i,t}^+ := \left\{\mathbf{x} \in \mathbb{R}^d | \mathbf{x}_i > t\right\}, \quad B_{i,t}^- := \left\{\mathbf{x} \in \mathbb{R}^d | \mathbf{x}_i \leq t\right\}$$

        Let $\hat{y}(B_{i,t}^{\pm})$ denote the class assignment for boxes $B_{i,t}^{\pm}$.
        Let $\ell_S(B_{i,t}^{\pm}, \hat{y}(B_{i,t}^{\pm}))$ denote the empirical risk incurred by $\hat{y}(B_{i,t}^{\pm})$.
        Define $g_i(t) := \ell_S(B_{i,t}^+, \hat{y}(B_{i,t}^+)) + \ell_S(B_{i,t}^-, \hat{y}(B_{i,t}^-))$
      end for
      Set the **best** splitting point: $t_i \leftarrow \text{argmin}_{t \in \mathbb{R}}\, g_i(t)$
    end for
    Select **best** feature to split by: $i^* \leftarrow \text{argmin}_{i \in [d]}\, g_i(t_i)$
    $Boxes \leftarrow Boxes \cup \left\{B_{i^*,t_{i^*}}^+, B_{i^*,t_{i^*}}^-\right\}$ ▷ Split box by best feature and threshold
  end while
  return $Boxes$
end procedure

of samples) the number of nodes (including leaves) in the tree is at most m. We therefore conclude that the time complexity of the CART heuristic is $\mathcal{O}\left(m^2 d\right)$

Pruning a Decision Tree

Pruning a tree means cutting off unnecessary branches. The tree obtained when we are done with the "growing" stage of CART may be too large. A tree too large means some of the boxes are too small, so we are not in an optimal point on the bias-variance tradeoff. It could help reduce the generalization error to merge some of the boxes together, so that the majority votes to determine the box label assignment would be based on larger sets of training samples. Merging two boxes is equivalent, from the decision tree perspective, to merging to leaves together and removing the node between them. Hence, "pruning". We will complete the CART heuristic when we discuss regularization (**??**).

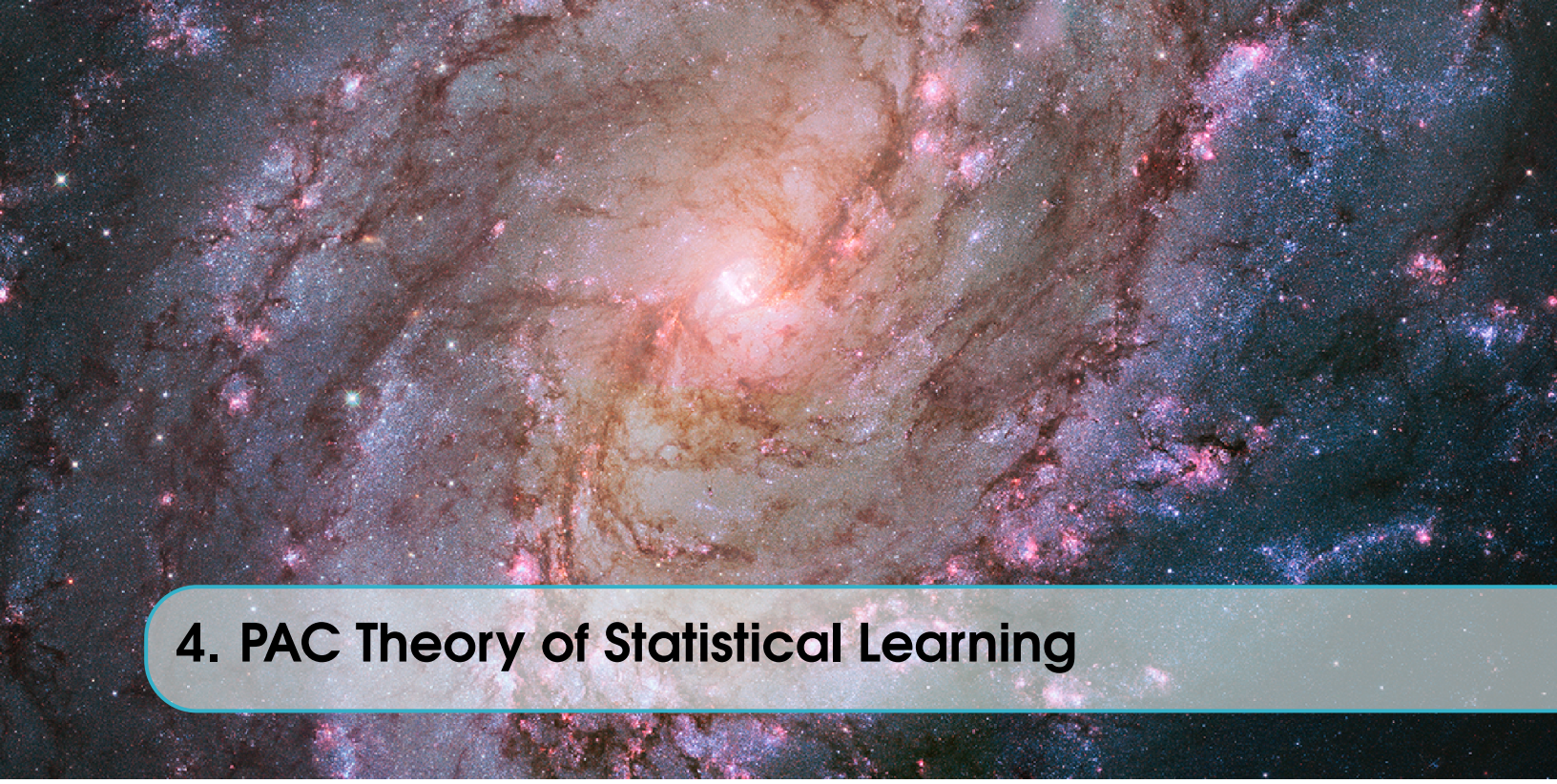
3.7.5 Interpretability

One of the great advantages of a classification tree is that it is very interpretable. To understand which features where important in the classification process, we just look at the nodes (the splits) and see which features the classification tree algorithm chose to split on. A feature that never appeared in any split has not been useful for classification of the training sample. A feature that appears once or more (remember that the algorithm can choose to split on some feature again and again in different areas of R^d) has been useful. To understand why a

new sample was classified the way it was classified, we just follow the tree from top to bottom, and see how each answer to each question went.

3.7.6 Learner ID Card

- **Hypothesis class:** The piecewise-constant functions induced by Tree Partitions (axis-aligned rectangles) of depth at most k: $\mathcal{H}_{CT}^{k}$
- **Learning principle used for training:** ERM
- **Computational implementation:** Implementation of ERM is NP-Hard. Therefore we use heuristics such as the top-down greedy heuristic of CART
- **Interpretability:** A very interpretable learner. Simply reading the tree structure
- **Family of models:** Indexed by k the maximal tree depth
- **Storing fitted model:** To store this model we must store for each node the split information: the coordinate i by which to split and the threshold value t. In addition we need to store the label assignment at the leafs of the tree
- **Prediction of new sample:** Navigate top-down along the tree until reaching a leaf
- **When to use:** This classifier is used as a simple baseline or to get a highly interpretable rule that is easy to explain and plot. Otherwise, classification trees are used to construct "random forests" which are covered in 5.3.4



4. PAC Theory of Statistical Learning

4.1 A Theoretical framework for learning

The basic questions in machine learning are: Which tasks are learnable? How do we learn learnable tasks? How many training samples do we need in order to learn them? In this chapter we develop the ***PAC theory of learnability***, which provides us, within its definitions and assumptions, a complete answer to these questions, for ***batch supervised learning***.

A Data-generation Model

The two basic assumptions in the PAC framework are:

- There exists a (deterministic) function f which is the correct classifier, i.e., for every $\mathbf{x}$ there is a single correct label, given by $y = f(\mathbf{x})$. We shall refer to this case as the ***PAC Model***.

- All samples, either in the training set or in any future test set are independent and identically distributed (i.i.d) random variables, i.e., they are sampled independently using a distribution $\mathcal{D}$ over the sample space $\mathcal{X}$. In particular, this means that the probability, $\mathbb{P}(S)$, of drawing the sequence $\mathbf{x}_1, \ldots, \mathbf{x}_m$ (which equals, due to the previous assumption, the probability of getting the sequence $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ with $y_i = f(\mathbf{x}_i)$) is given by $\mathbb{P}(S) = \prod_{i=1}^m \mathcal{D}(\mathbf{x}_i)$.

R Later on, in section 4.4, we shall relax these assumptions and consider a more general case which we will call the ***Agnostic PAC model*** and in which the *same* $\mathbf{x}$ may appear with *different* labels, meaning that the labels themselves will be random, at least to some extent, and therefore also the probability density will be defined over $\mathcal{X} \times \mathcal{Y}$.

Let us compare the assumptions of the PAC model to the linear regression model covered in chapter 2. In both cases we have received a set of examples $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathcal{X}$. In the case of linear regression we implicitly assumed all the $\mathbf{x}_i$'s had equal importance, for example, in their contribution to the global error. Now, the $\mathbf{x}_i$'s are *i.i.d* sampled according to $\mathcal{D}$, i.e., they have different probabilities to appear and therefore may have different weights in the loss function. Another difference is that in the case of the linear model we started with

the assumption $y_i = f(\mathbf{x}_i)$ where f was deterministic and linear. Here, we do assume f to be deterministic, but otherwise it may take the form of any possible function from $\mathcal{X}$ to $\mathcal{Y}$.

In the linear model we eventually relaxed the deterministic assumption and considered y to be a random function of $\mathbf{x}$ of the form: $y_i = f(\mathbf{x}_i) + z_i$. An analogous generalization will take place also here, once we consider the more general, agnostic, case. Finally we note that, although this chapter will focus on *classifiers*, many principles we will encounter will hold also for linear regression problems.

Generalization Error for Classifiers

For a classification task, we define the ***Generalization Error*** of a hypothesis h as the probability to obtain an $\mathbf{x}$ for which $h(\mathbf{x})$ is different than the correct label $f(\mathbf{x})$:

$$L_{\mathcal{D},f}(h) \equiv \mathbb{P}_{\mathbf{x}\sim\mathcal{D}}[h(\mathbf{x}) \neq f(\mathbf{x})] \equiv \mathcal{D}(\{\mathbf{x} \in \mathcal{X} : h(\mathbf{x}) \neq f(\mathbf{x})\}) \tag{4.1}$$

where $\mathcal{D}$ and f are unknowns. The generalization error is also called the ***Risk***, or the ***True Error***. Note, one should be critical about an error measure that counts the total number of misclassification errors of a classifier. Recall the distinction we make between the Type-I and Type-II errors, where often the one is worse than the other. For now however, we only consider the generalization error with respect to the misclassification error and therefore do not distinguish between the two types of errors.

The Fundamental Theorem of Statistical Learning

So our task is to design a learning algorithm (a learner), $\mathcal{A}$. The algorithm will receive a training sample of size m $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ and outputs a prediction rule (a hypothesis) $h : \mathcal{X} \to \mathcal{Y}$. For classification problems, for example, $\mathcal{Y} = \{\pm 1\}$, but the framework we develop has a much broader applicability.

We assume that the data points, both in training set and in the test set, are generated by sampling independently $\mathcal{X}$ using a distribution $\mathcal{D}$, which is unknown to us. The labels y are fixed: given a particular $\mathbf{x}$ there exists some deterministic function f such that $y = f(\mathbf{x})$, where f is unknown to us and the training set is our only view to what f does.

Finally, the performance of any candidate rule $h : \mathcal{X} \to \mathcal{Y}$ that our learner may produce, will be evaluated by how well it will perform on future, unseen samples. This is done using the expected misclassification rate $L_{\mathcal{D},f}(h) \equiv \mathbb{P}_{\mathbf{x}\sim\mathcal{D}}[h(\mathbf{x}) \neq f(\mathbf{x})]$. The next sections will be devoted for a detailed understanding of the following important definitions:

Definition 4.1.1 A hypothesis class, $\mathcal{H}$, is a ***PAC Learnable hypothesis class*** if there exist a learning algorithm $\mathcal{A}$ and a function $m_{\mathcal{H},\mathcal{A}} : (0,1)^2 \to \mathbb{N}$ with the following property:

- For every $\varepsilon, \delta \in (0,1)$
- For every distribution $\mathcal{D}$ over $\mathcal{X}$
- For every labeling function $f : \mathcal{X} \to \{\pm 1\}$ that such that there exists $h^* \in \mathcal{H}$ which satisfies $L_{\mathcal{D},f}(h^*) = 0$

when running the learning algorithm $\mathcal{A}$ on $m \geq m_{\mathcal{H},\mathcal{A}}(\varepsilon, \delta)$ *i.i.d* samples generated by $\mathcal{D}$ and labeled by f, the algorithm returns a hypothesis $h_S = \mathcal{A}(S)$ such that, with probability of at least $1 - \delta$ (over the choice of the training samples), we have $L_{\mathcal{D},f}(h_S) \leq \varepsilon$.

$$\mathcal{D}^m\left(S \middle| L_{\mathcal{D},f}(h_S) \leq \varepsilon\right) \geq 1 - \delta$$

Denote the minimal sample size required for the above conditions to hold with respect to ε, δ and with respect to any algorithm, by $m_{\mathcal{H}}(\varepsilon, \delta) = \min_{\mathcal{A}} m_{\mathcal{H},\mathcal{A}}(\varepsilon, \delta)$. The function $m_{\mathcal{H}} : (0,1)^2 \to \mathbb{N}$ is called the ***Sample Complexity*** of the PAC learnable hypothesis class $\mathcal{H}$.

Definition 4.1.2 Let $\mathcal{H} \subseteq \{\pm 1\}^{\mathcal{X}}$ be a hypothesis class. For a subset $C \subset \mathcal{X}$ let $\mathcal{H}_C$ be the restriction of $\mathcal{H}$ to C, namely, $\mathcal{H}_C = \{h_C : h \in \mathcal{H}\}$, where for $h : \mathcal{X} \to \mathcal{Y}$, $h_C : C \to \mathcal{Y}$ is the function such that $h_C(\mathbf{x}) = h(\mathbf{x})$ for every $\mathbf{x} \in C$. Define the ***VC-dimension*** of $\mathcal{H}$ by:

$$VCdim(\mathcal{H}) = \max\left\{|C| \;\middle|\; C \subset \mathcal{X} \text{ and } |\mathcal{H}_C| = 2^{|C|}\right\}$$

By choosing PAC learnability as our interpretation of what learnability means, definitions Definition 4.1.1 and Definition 4.1.2 provide a *well defined necessary and sufficient condition* for when learning is possible and the minimal training sample size needed in order to learn. This framework also provides a "universal" learner that successfully learns given a sufficiently large training set. In short, we have a full theory of batch learning - a full theory of when it is possible to generalize from a training sample to new samples, and how to do it. This result is sometimes known as "***The Fundamental Theorem of Statistical Learning***" and states that:

- A hypothesis class $\mathcal{H}$ is PAC-learnable *if and only if* $VCDim(\mathcal{H})$ is finite.
- The sample complexity of a hypothesis class with a finite VC-dimension is given approximately by

$$m_{\mathcal{H}}(\varepsilon, \delta) \sim \frac{VCDim(\mathcal{H}) + \log(1/\delta)}{\varepsilon}$$

- The ERM rule achieves this minimum, namely, when learning is possible, ERM learns with a minimial number of examples.

The first step in gaining a detailed understanding of PAC-learnability, VC-dimension and the fundamental theorem, will be to present a different perspective of the above framework.

4.1.1 Learning As A Game - First Attempt

The framework in section 4.1 can be thought of as a *game* between us and Nature, with a random payoff. The game proceeds as follows. First, the number of training samples m is determined in advanced as a game parameter.

We perform the first step and choose some learner $\mathcal{A}$ that trains on m examples. This is our strategy. Then Nature makes the second step and chooses a distribution $\mathcal{D}$ and a labeling function f. This is Nature's strategy. Importantly, Nature knows the strategy we chose when she chooses her strategy. To calculate the game's payoff, an $i.i.d$ sample S of size m is drawn according to the distribution $\mathcal{D}$ and labeled according to the function f, both of which were chosen by Nature. This set is then fed into the learner $\mathcal{A}$ that we chose to obtain the prediction rule $h_S = \mathcal{A}(S)$. The notation h_S emphasizes that the prediction rule we learn, h_S, strongly depends on the random sample S. The payoff is $L_{\mathcal{D},f}(h_S)$.

Our goal in the game is to end up with an $L_{\mathcal{D},f}(h_S)$ which is as small as possible while Nature is an adversary that wants $L_{\mathcal{D},f}$ to be as large as possible. Note that the payoff is random as it depends on the sample S that was drawn. If we are unlucky, and the sample S is "bad", namely, does not represent $\mathcal{D}$ very well then the rule h_S our learner produces might not generalize well and the random loss (for that draw of S) will be high.

Under such setting, what is the best strategy for us? How to best design the learner $\mathcal{A}$? Remember that Nature will know what we chose, and can try to be "cruel", namely, to choose $\mathcal{D}$ and f that our learner did not prepare well for. Also, there is always a chance that we will draw a "bad" sample S, which will mislead us in choosing a rule h_S that will not generalize well. So, is there a way to defend ourselves against "cruel" strategies $\mathcal{D}, f$ that Nature might play, and against unlucky draws of a training sample S? Is there anything at all that can be said in this generality about the problem of learning (i.e., the problem of generalizing from training samples to new samples)?

Definition 4.1.3 ***The Learning Game*** (first version):

- A sample size m is fixed.
- We choose a strategy (a learner) $\mathcal{A}$. That is, a function that matches every sample S to a prediction rule $h_S : \mathcal{X} \to \mathcal{Y}$.
- Nature knows our strategy and, after us, chooses a strategy that consists of a probability distribution $\mathcal{D}$ over $\mathcal{X}$, and a label function $f : \mathcal{X} \to \mathcal{Y}$.
- A sample S of size m is drawn according to $\mathcal{D}$ and is labeled according to f.
- The sample S is fed into $\mathcal{A}$ to produce a prediction rule $h_S = \mathcal{A}(S)$.
- The payoff is $L_{\mathcal{D},f}(h_S)$, namely, the expected fraction of misclassification errors h_S will make on future data drawn *i.i.d* according to $\mathcal{D}$ and labeled according to f. The payoff is *random* since S is random and therefore h_S is random.
- Nature does her best to win. So we will look for learners $\mathcal{A}$ for which we can *ensure* that the loss $L_{\mathcal{D},f}(h_S)$ ever exceeds a certain value, *for any* strategy $\mathcal{D}, f$ that Nature might play.

4.1.2 Probably Correct & Approximately Correct Learners

The generalization loss, $L_{\mathcal{D},f}(h_S)$, is random since it depends on the randomly-drawn training sample, S. Therefore, in general, one should talk about the *probability* that a learner has a certain loss. In particular, saying that $L_{\mathcal{D},f}(h_S)$ *never* exceeds a certain value, actually means that (for the specific f, $\mathcal{D}$ and $\mathcal{A}$) the probability of drawing a training sample S that, for which, $\mathcal{A}$ produces a rule with a loss smaller than a certain value, is 1. This brings us to the following definition:

Definition 4.1.4 Let $\varepsilon \in (0,1)$. We say that a learner $\mathcal{A}$ is ***Approximately Correct*** with an ***accuracy*** ε, if we are certain (with probability 1) that for any training sample, S, drawn using $\mathcal{D}$, $\mathcal{A}$ will output a prediction rule, h_S, with a loss smaller or equal to ε:

$$\mathcal{D}\left(S|\, L_{\mathcal{D},f}(h_S) \leq \varepsilon\right) = 1$$

Is there an accuracy parameter, $\varepsilon \in (0,1)$, for which we can find an approximately correct learner? Unfortunately, the answer to this question is no. For any ε, Nature always has a strategy that can make sure that there is a non-zero probability, even if very small, to get a "pathological" training sample S that does not represent $\mathcal{D}$ at all. The resulting rule h_S can be wrong on most of $\mathcal{X}$, which would cause a loss arbitrarily close to 1, higher than any specified ε. We shall prove this assertion by giving an example of one such strategy that Nature can use.

■ **Example 4.1** Let $\varepsilon \in (0,1)$ and consider any two points $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$. Let us denote by S' a training sample that happened to have only $\mathbf{x}'$'s in it (in particular, S' does not contain $\mathbf{x}$): $S' = (\mathbf{x}_1, y_1), ..(\mathbf{x}_m, y_m)$ with $\mathbf{x}_i = \mathbf{x}'$ and $y_i = f(\mathbf{x}')$ for $i = 1..m$. Although such a sample might be rare, it can not be excluded and therefore, our algorithm, $\mathcal{A}$, should specify what label its output rule, $h_{S'}$ should predict on other points beside $\mathbf{x}'$, and in particular on $\mathbf{x}$, in case it receives S' as an input. Assume, without a loss of generality, that we choose $h_{S'}(\mathbf{x}) = +1$, that is, if the training sample is S' then $\mathcal{A}$ will predict $+1$ on $\mathbf{x}$.

Nature's strategy comprises of two parts. First, it reduces $\mathcal{X}$ to a 2-point space by choosing $\mathcal{D}$ that vanishes everywhere except on $\mathbf{x}$ and $\mathbf{x}'$. More specifically, it chooses $\mathcal{D}$ with $\mathcal{D}(\mathbf{x}) = \gamma$, $\mathcal{D}(\mathbf{x}') = 1 - \gamma$, where γ is a number satisfying $0 < \varepsilon < \gamma < 1$. Second, Nature chooses a labeling function f with $f(\mathbf{x}) = -1 = -h_{S'}(\mathbf{x})$. The probability of obtaining S' is not zero since it is given by $(1-\gamma)^m > 0$. Therefore, to show that Nature's strategy prevents $\mathcal{A}$ from being approximately correct with an accuracy ε, all we need to show is that the loss in the case of obtaining the set S', is larger than ε. Indeed:

$$L_{\mathcal{D},f}(h_{S'}) = \mathcal{D}(\mathbf{x})\mathbb{1}_{f(\mathbf{x})\neq h_{S'}(\mathbf{x})} + \mathcal{D}\left(\mathbf{x}'\right)\mathbb{1}_{f(\mathbf{x}')\neq h_{S'}(\mathbf{x}')}$$

where $\mathbb{1}_{a\neq b}$ is 1 if $a \neq b$ and 0 otherwise. Both terms on the right are non-negative and therefore:

$$L_{\mathcal{D},f}(h_{S'}) \geq \mathcal{D}(\mathbf{x})\mathbb{1}_{f(\mathbf{x})\neq h_{S'}(\mathbf{x})} = \gamma\mathbb{1}_{-1=-1} = \gamma > \varepsilon$$

So, for any fixed $\varepsilon \in (0,1)$, for any strategy $\mathcal{A}$ we might play, Nature has a strategy $\mathcal{D}, f$, such that there is a non-zero probability over the choice of training samples of length m, that we will have $L_{\mathcal{D},f}(h_S) > \varepsilon$. As ε was arbitrary, that means that Nature can, with a non-vanishing probability, cause the game to end with a loss arbitrarily close to 1. ∎

In the above example, even if very small, with probability $(1-\gamma)^m$ we get a "bad" training sample, S, that does not represent $\mathcal{D}$ good enough, and does not allow us to generalize. We therefore conclude, that given any accuracy parameter $\varepsilon \in (0,1)$, no learner $\mathcal{A}$ can guarantee, that with probability 1, the loss will not exceed ε. Nature can always find a strategy for which $L_{\mathcal{D},f}(h_S) > \varepsilon$ will have a non-zero probability to occur.

So the possibility of bad samples means that we should not aspire for an *absolute* certainty in achieving a limited loss. We will accept the fact that on such bad training samples, the learner $\mathcal{A}$ might fail completely (i.e., produce h_S with a potentially high loss). We will therefore, only require a *limited* certainty, that we will call *confidence*, for having a limited loss. This means that we will demand that the probability of drawing a bad sample will not exceed a certain threshold, $\delta \in (0,1)$. This parameter too will be specified prior to the beginning of the game, together with ε.

Since we no longer demand absolute confidence in having a limited loss, perhaps we can instead require absolute accuracy (zero loss), but with a limited confidence? That is, perhaps we can require that at least for those good training samples (the ones that will have a probability of at least $1-\delta$ to appear) the loss will vanish?

Definition 4.1.5 Let $\delta \in (0,1)$. We say that a learner, $\mathcal{A}$, is ***Probably Correct*** with a ***confidence*** δ, if the probability to obtain a training sample, S, for which $\mathcal{A}$ will output a prediction rule, h_S, with a perfect accuracy (zero loss), is larger or equal to $1-\delta$:

$$\mathcal{D}^m\left(S|\, L_{\mathcal{D},f}(h_S) = 0\right) \geq 1-\delta$$

Note that in definition 4.1.4 we required prefect confidence $\delta = 0$ (i.e., with probability 1) to have a certain accuracy ($0 < \varepsilon < 1$), while in definition 4.1.5 we require a certain confidence $0 < \delta < 1$ to have a prefect accuracy $\varepsilon = 0$. In addition, although it is named "confidence", δ actually means *lack of confidence* since the larger it is, the less sure we can be that our loss is limited.

Is there a confidence parameter $\delta \in (0,1)$, for which we can find a probably correct learner? Here too, the answer is no. For any δ, Nature always has a strategy that with probability larger than $1-\delta$ will cause the rule to have a non-vanishing loss: $L_{\mathcal{D},f}(h_S) > 0$.

Recall that zero loss means that, with probability 1 with respect to $\mathcal{D}$, the predicted label is always correct. Nature can play a $\mathcal{D}$ that gives a finite but tiny probability to a certain $\mathbf{x} \in \mathcal{X}$. Then, with high probability, the training sample will not include $\mathbf{x}$, and therefore, whatever label the learner assigns to $\mathbf{x}$, it will be a guess and therefore might be incorrect, causing a finite loss. Again, we shall prove this assertion through an example of such a strategy that Nature may adopt.

■ **Example 4.2** Let $\delta \in (0,1)$ and consider any two points $\mathbf{x}, \mathbf{x}' \in \mathcal{X}$. Similar to 4.1, we consider the training sample $S' = (\mathbf{x}_1, y_1), ..(\mathbf{x}_m, y_m)$ with $\mathbf{x}_i = \mathbf{x}'$ and $y_i = f(\mathbf{x}')$ for $i = 1..m$, and assume that once this sample is fed into our algorithm, it will predict $h_{S'}(\mathbf{x}) = +1$.

As before, Nature's strategy is to chooses a labeling function f with $f(\mathbf{x}) = -1 = -h_{S'}(\mathbf{x})$ and a distribution, $\mathcal{D}$, with $\mathcal{D}(\mathbf{x}) = \gamma, \mathcal{D}(\mathbf{x}') = 1-\gamma$. This time however, γ is chosen such that $\delta < (1-\gamma)^m$. This means that when m is large, the probability of getting $\mathbf{x}$, namely, γ, is chosen to be very small. Therefore, in th present case S' is a typical sample, in the sense that its probability to appear, $(1-\gamma)^m$ is larger than δ.

The same calculation as in example 4.1 yields $L_{\mathcal{D},f}(h_{S'}) \geq \gamma$ and since $\gamma > 0$ that would mean a non-zero loss. Since the probability of obtaining S' is larger than δ, the probability of ending up with a non-zero loss is also larger than δ. In other words, our learner $\mathcal{A}$ is not a probably correct one. ∎

We conclude that for any confidence parameter $\delta \in (0,1)$, no learner $\mathcal{A}$ can guarantee, that with probability of at least $1-\delta$, the loss will vanish: Nature can always find a strategy for which $L_{\mathcal{D},f}(h_S) > 0$ will have a probability large than δ to occur. Even a "typical" training sample may miss small areas in $\mathcal{X}$. On these areas the resulting h_S might be wrong.

Examples 4.1 and 4.2 teach us that no matter what learner we construct, we can never have an absolute confidence that our loss will be limited, neither we can have a limited-confidence that we can obtain an absolute accuracy. What we *might* be able is to have *some* confidence that our loss will not exceed *some* threshold. This brings us to the following definition.

Definition 4.1.6 Let $\delta, \varepsilon \in (0,1)$. We say that a learner, $\mathcal{A}$, is ***Probably Approximately Correct*** with a confidence δ and an accuracy ε if and only if the probability of obtaining a training sample S, for which $\mathcal{A}$ will output a prediction rule, h_S, with a loss that does not exceeds ε, is larger or equal to $1-\delta$:

$$\mathcal{D}^m\left(S | L_{\mathcal{D},f}(h_S) \leq \varepsilon\right) \geq 1-\delta$$

It is important to understand the difference between the *accuracy* ε and the *confidence* δ.

- Recall that we first draw the training sample S at random. Then, the learning algorithm runs on this random sample and its prediction is therefore random. If S is by chance "weird" (not representing $\mathcal{D}$ well), the rule h_S produced will be "wrong", namely, it will not generalize well. The number δ is the probability of failure due to a "weird" sample S.
- After the learner outputs a rule h_S, it is then tested on a new sample. The new sample is also random. $L_{\mathcal{D},f}(h_S)$ is the expected fraction of errors h_S will make, i.e., its accuracy, over such data. The number ε refers to that accuracy.

4.1.3 Learning As A Game - Second Attempt

Since we can only hope to build a *Probably Approximately* correct learner, we will update the game definition. The sample size m will no longer be fixed. Instead, the accuracy ε and confidence δ, which our learner is required to achieve, are specified as game parameters. We get to decide on m as part of our strategy. Note that there is a subtle nuance in notation now. When we write $\mathcal{A}$ for the learner, we actually mean a *sequence* of learners - one for each sample size m. It would be better to write $\mathcal{A}_m : (\mathcal{X} \times \mathcal{Y})^m \to \mathcal{Y}^{\mathcal{X}}$. However, to keep the notation simple we will continue writing $\mathcal{A}$, and understand that there is in fact a dependence also on m.

Definition 4.1.7 ***The Learning Game*** (second version):
Fix the desired accuracy and confidence parameters $\varepsilon, \delta \in (0,1)$ and then:

- We choose a sample size m and a learner $\mathcal{A}$, both of which may depend on (ε, δ).
- Nature knows our strategy, and, after us, chooses a strategy that consists of a probability distribution $\mathcal{D}$ over $\mathcal{X}$, and a label function $f : \mathcal{X} \to \mathcal{Y}$. Nature's strategy may too depend on the specified (ε, δ) and also on our choice of m and $\mathcal{A}$.
- A sample S of size m is drawn according to $\mathcal{D}$ and is labeled according to f.
- The sample S is fed into $\mathcal{A}$ to produce a prediction rule h_S.
- The payoff is $L_{\mathcal{D},f}(h_S)$. It is random since S is random and therefore h_S is random.
- Nature does her best to win. So we will look for learners $\mathcal{A}$ for which there is a probability of at least $1-\delta$ that the loss $L_{\mathcal{D},f}(h_S)$ will not exceed ε, no matter what strategy $\mathcal{D}, f$ Nature might play.
- To determine if we were successful in the game, we play the game many many times. Each time

both us and Nature play the same strategies. Each time however, the training samples drawn are different. calculate the probability, over the random draws of training samples S, of the event $\left\{S \sim \mathcal{D}^m \,\middle|\, L_{\mathcal{D},f}(h_S) \leq \varepsilon\right\}$. If this probability is found to be larger than $1-\delta$, that is, if the learner $\mathcal{A}$ we chose was Probably Approximately correct with accuracy ε and confidence δ - against Nature's best strategy - we say that *we have been successful (with regards to the parameters ε, δ).*

The game perspective, although phrased differently, is equivalent to the more standard description of our learning challenge, which is the following: The learner doesn't know $\mathcal{D}$ and f. The learner receives an accuracy parameter ε and a confidence parameter δ. It then asks for training data, S, containing $m(\varepsilon,\delta)$ examples (that is, the number of examples can depend on the value of ε and δ, but it can not depend on the unknown $\mathcal{D}$ or f). Finally, the learner should output a hypothesis h_S, that depends only on ε, δ and the training sample S drawn, such that with probability of at least $1-\delta$ it holds that $L_{\mathcal{D},f}(h_S) \leq \varepsilon$. That is, the learner should be Probably Approximately correct, with the specified accuracy ε and confidence δ.

Since we can now choose the sample size m and since data costs time and money, we want m to be as small as possible though we should expect a certain trade-off between ε, δ and our choice of m.

4.2 No Free Lunch and Hypothesis Classes

It turns out that, unfortunately, we cannot, in general, be successful against Nature even in the second version of our game. With no restrictions placed on the choice of $\mathcal{D}$ or f, we can not be confident-enough that we can find an accurate-enough h_S. This is true no matter how large is our sample size m.

In examples 4.1 and 4.2 above, Nature used $\mathcal{D}$ that vanishes everywhere in the sample space $\mathcal{X}$ except for two points. In particular, Nature's strategies were enough to prevent us from constructing a learner that enjoys confidence $\delta = 0$ or accuracy $\varepsilon = 0$ for any $\mathcal{X}$ with two or more points. In the following example, Nature's strategy can be applied only if $\mathcal{X}$ has an infinite number of points (though it is enough to have a countable infinite amount of them).

■ **Example 4.3** Suppose that $|\mathcal{X}| = \infty$ and follow the steps of the second version of the game for some $\delta \in (0,1)$ and some $0 < \varepsilon < \frac{1}{2}$.

- We fix m.
- We now decide what label to predict on a point that does not appear in the training sample, S. We could, for example, decide that whenever a point, say, $\mathbf{x}_4$, does not appear in S but $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ do appear, all with the label +1, then we take $h_S(\mathbf{x}_4) = 1$ but if these 3 points, all show up with the label -1, then we take $h_S(\mathbf{x}_4) = -1$. That would mean that the value we choose for $h_S(\mathbf{x}_4)$ would depend on S. However, we will restrict ourselves to choosing the *same* value, $h_S(\mathbf{x}_4)$, whenever S does not contain $\mathbf{x}_4$, independently of which specific S it is. In other words, we choose a function, $g(\mathbf{x})$, and if a point $\mathbf{x} \in \mathcal{X}$ is *not* observed in S, then at this point, the rule, $h_S(\mathbf{x})$ that $\mathcal{A}$ outputs, will satisfy $h_S(\mathbf{x}) = g(\mathbf{x})$, independently of the specific S we got.
- Nature knows m, so it picks some finite set $C \subset \mathcal{X}$ with $|C| > 2m$, and chooses $\mathcal{D}$ to vanish outside C while being uniform over it: for any $\mathbf{x} \in C$, $\mathcal{D}(\mathbf{x}) = \frac{1}{|C|} < \frac{1}{2m}$.
- Nature also knows $g(\mathbf{x})$, so as a labeling function f, Nature plays a sinister move and chooses $f(\mathbf{x}) = -g(\mathbf{x})$ for all $\mathbf{x} \in \mathcal{X}$, namely, just the opposite of what h_s will predict on unseen points.
- Now, let S be a training sample. Let $supp(S) \subset C$ denote the set of different points $\mathbf{x} \in \mathcal{X}$, that appears in S. Recall that the same $\mathbf{x}$ may appear in S several times and therefore the $|supp(S)|$ can take any value between 1 and m. Since $|supp(S)| \leq m$ and since $\mathcal{D}$ is uniform over C, we have $\mathcal{D}(\{\mathbf{x} \in \mathcal{X} \setminus supp(S)\}) \geq 1/2$. In other words, the probability that a new test point drawn according to $\mathcal{D}$ was not seen in S is at least $1/2$.
- Now, as the game requires, we feed the sample S into $\mathcal{A}$ and obtain $h_S = \mathcal{A}(S)$. What is the loss? Regardless of what h_S predicts on points seen in S, a test point has probability $\geq 1/2$ to be in the unseen part $\mathcal{X} \setminus supp(S)$. Thus, with probability of at least $1/2$, the rule h_S will predict $h_S(\mathbf{x}) = g(\mathbf{x})$ and will

be wrong, since $f(\mathbf{x}) = -g(\mathbf{x})$. Therefore, $L_{\mathcal{D},f}(h_S) \geq 1/2$.

- But this happens for *every* training sample S. So, Nature's strategy ensures that with probability 1 (over the choice of training samples according to $\mathcal{D}$), the game results in a loss $L_{\mathcal{D},f}(h_S) \geq 1/2$.
- So, we can not find a learner $\mathcal{A}$ that will be Probably Approximately correct (for any δ and for $\varepsilon < \frac{1}{2}$) regardless of Nature's strategy $\mathcal{D}, f$. Asking for a larger training sample won't help - if we increase m, Nature will just choose a larger set C and a distribution $\mathcal{D}$ which is uniform over that larger C.

■

What went wrong? Nature could choose *any* labeling function, f, that she wanted, and we tried to learn (to generalize/predict) f from a sample that was too small compared to the number of possible functions Nature could choose from. We find that we just cannot design a Probably Approximately correct learner if the set of possible labeling functions is "too large".

This is known as ***"No Free Lunch" Theorem***[1]: without assuming anything in advance on the label function, f, learning is impossible. Equivalently, if the set of possible labeling function f is too large, then Nature can play a function that we can't learn. Even if we take a larger sample, Nature, in turn, chooses a more complicated f. So if no limitations are placed on Nature's choice of label function, learning is impossible. Example 4.3 demonstrated the essence of the No Free Lunch Theorem, but was not a proof of it, since we restricted ourselves to $g(\mathbf{x})$ that was independent of S. That restriction made life easier for Nature since it enabled her to choose $f(\mathbf{x}) = -g(\mathbf{x})$ as a label function that maximized the error of our learner. In reality, we could choose different $g_S(\mathbf{x})$'s for each of the different S's that did not contain $\mathbf{x}$, thus limiting Nature's ability to maximize the loss. In any case, example 4.3 gives the crucial bits of intuition which we will need later on.

As mentioned above, there are several theorems that can be called a "No Free Lunch" - basically any theorem that shows that without some prior knowledge on the labeling function, that is, when there are too many possibilities for f, learning it is impossible. Below is an actual, formal, No Free Lunch theorem. Its proof, which uses the notion of Agnostic PAC that we will encounter a bit later, can be found in the book "Understanding Machine Learning" (Theorem 5.1, and exercise 3 in section 5.5 in that book).

Theorem 4.2.1 — No Free Lunch. Let $\mathcal{X}$ be a sample domain, $|\mathcal{X}| = \infty$. For every $0 < \varepsilon < 1/2$, there exists $\delta > 0$ such that, for every algorithm $\mathcal{A}$, there exists a distribution $\mathcal{D}$ over $\mathcal{X}$ and a function $f : \mathcal{X} \to \mathcal{Y}$ for which, when running $\mathcal{A}$ over a sample S of any finite size, drawn *i.i.d* from $\mathcal{D}$, then with probability of at least δ, the output of $\mathcal{A}$, h_S, has a loss larger than ε: $L_{\mathcal{D},f}(h_S) \geq \varepsilon$.

Note that $L_{\mathcal{D},f} = 1/2$ is the loss that one gets from a completely *random guess* of labels. Thus, the condition $\varepsilon < 1/2$ in the above theorem implies that without prior assumptions on f we can not guarantee a prediction which will have a lesser loss than a random guess.

Needing Hypothesis Classes

The No Free Lunch principle implies that to be able to learn, the learner *must* receive enough prior knowledge about the function f. In other words, we should assume that the target f comes from some *hypothesis class*, $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$, or at least that it resembles closely some functions in that class. The class of functions $\mathcal{H}$ should not be too broad or else the problem we encountered in example 4.3 might reappear.

Realizability Assumption

Suppose that a hypothesis class $\mathcal{H}$ is specified for our game, meaning that we restrict the choice of rules that our algorithm can predict to a certain family of functions. The ***realizable case*** is when Nature must play a function $f \in \mathcal{H}$. Actually, we don't care if Nature plays a function f that is not in $\mathcal{H}$ as long as there is a function h^* in $\mathcal{H}$ which is identical to f on all points over which $\mathcal{D}$ does not vanish so that we will never see examples where $f(\mathbf{x}) \neq h(\mathbf{x})$, neither in the training nor in the test samples. So the formal mathematical ***Realizability Assumption*** is this: Nature plays a function f such that there exists $h^* \in \mathcal{H}$ with $L_{\mathcal{D},f}(h^*) = 0$.

[1] There are in fact several "No Free Lunch" theorems revolving around the same idea

The learner is given $\mathcal{H}$ before the learning starts and will only output $h_S \in \mathcal{H}$. In other words, for a training sample of size m the learner (learning algorithm) is a map $\mathcal{A} : (\mathcal{X} \times \mathcal{Y})^m \to \mathcal{H}$ such that $\mathcal{A} : S \mapsto h \in \mathcal{H}$. As before, we will continue to abuse notation and write $\mathcal{A}$ instead of $\mathcal{A}_m$, and when we say "the learning algorithm $\mathcal{A}$" we will sometimes mean "a sequence of learners $\{\mathcal{A}_m\}_{m=1}^{\infty}$, one for each possible sample size".

Theorem 4.2.1 told us that if $|\mathcal{X}| = \infty$ then $\mathcal{H} = \mathcal{Y}^{\mathcal{X}}$ is too large to learn. This brings us to ask the following questions:

- What are the "small enough" hypothesis classes $\mathcal{H}$ for which we *can* find a Probably Approximately correct learner? And what are the "too large" hypothesis classes $\mathcal{H}$ for which we *cannot*?
- Assume we have a "small enough" $\mathcal{H}$, in the sense that for every ε, δ we have at least one strategy, $(m, \mathcal{A})$, such that $\mathcal{A}$ is Probably Approximately correct, with accuracy ε and confidence δ, no matter how Nature plays. This means that for every ε, δ there is a *minimal number of training samples*, which we will denote by $m_{\mathcal{H}}(\varepsilon, \delta)$, for which there exists at least one algorithm with the required accuracy and confidence. Can we find this minimal function $m_{\mathcal{H}}(\varepsilon, \delta)$? Is there a relation between the "size" of the hypothesis class $\mathcal{H}$ and $m_{\mathcal{H}}(\varepsilon, \delta)$?
- Assume we have a "small enough" $\mathcal{H}$. Can we find a concrete learner $\mathcal{A}$ that always succeeds in learning functions from $\mathcal{H}$? If yes, how many training samples m does $\mathcal{A}$ need to always succeed in learning a function from $\mathcal{H}$ (always be Probably Approximately correct, no matter how Nature plays)?
- Can we find the *most training-data efficient* learner, namely a learner that can succeed with the minimal number of samples $m_{\mathcal{H}}(\varepsilon, \delta)$ mentioned above?

4.2.1 Learning As A Game - Third Version

To reach a final version of our learning game, we now include the hypothesis class to it.

Definition 4.2.1 ***The Learning Game (third version)***: Fix desired accuracy $\varepsilon \in (0,1)$ and confidence $\delta \in (0,1)$. Fix a hypothesis class $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$.

- We choose a sample size m and a learner $\mathcal{A} : (\mathcal{X}, \mathcal{Y})^m \to \mathcal{H}$. Both m and $\mathcal{A}$ can depend on (ε, δ).
- Nature knows our strategy and, after us, chooses strategy that consists of a probability distribution $\mathcal{D}$ over $\mathcal{X}$, and a label function *from the hypothesis class*, $f \in \mathcal{H}$. That is, Nature's strategy depends not only on ε, δ, m and $\mathcal{A}$ but also on the hypothesis class, $\mathcal{H}$. (This rule of the game is somewhat stricter than necessary since, as mentioned above, we could allow Nature to choose a function $f \notin \mathcal{H}$ as long as there exists $h^* \in \mathcal{H}$ with $L_{\mathcal{D},f}(h^*) = 0$).
- A sample S of size m is drawn according to $\mathcal{D}$ and is labeled according to f
- The sample S is fed into $\mathcal{A}$ to produce a prediction rule $h_S = \mathcal{A}(S)$. Note that $h_S \in \mathcal{H}$.
- The payoff is $L_{\mathcal{D},f}(h_S)$. It is random since S is random and therefore h_S is random.
- Nature does her best to win. So we will look for learners $\mathcal{A}$ for which there is a probability of at least $1-\delta$ that the loss $L_{\mathcal{D},f}(h_S)$ will not exceed ε, no matter what strategy $\mathcal{D}, f$ Nature might play.
- To determine if we were successful in the game, we play the game many many times (both us and Nature play the same strategies, just the training samples drawn are different). We count and calculate the probability, over the random draws of training samples S, of the event $\{S \sim \mathcal{D}^m \,|\, L_{\mathcal{D},f}(h_S) \leq \varepsilon\}$. If this probability is found to be larger than $1-\delta$, that is, if the learner $\mathcal{A}$ we chose was Probably Approximately correct with accuracy ε and confidence δ - against Nature's best strategy - we say that *we have been successful (with regards to the parameters ε, δ and hypothesis class $\mathcal{H}$).*

4.2.2 Example: Threshold Functions

We saw above that if $|\mathcal{X}| = \infty$ and $\mathcal{H}$ is the class of all functions from $\mathcal{X}$ to $\mathcal{Y}$, namely $\mathcal{H} = \mathcal{Y}^{\mathcal{X}}$, we can't be successful in the third version of the learning game. On the other hand, we know that if we take a very small $\mathcal{H}$, for example, one that contains only a single function, learning is possible and is in fact trivial. So we know that when the hypothesis class is "small enough", it *is* possible to be successful in the third version of the

learning game even when the sample space is infinite, which is the reason why learning is possible. What is left to find out is how broad $\mathcal{H}$ can be chosen while maintaining the possibility to learn.

In the following example we will have an infinite (in fact uncountably infinite) sample space, and a very simple hypothesis class. We will see that we can be successful in the third version of the game, for any ε, δ. Consider the domain $\mathcal{X} = \mathbb{R}$, i.e., there is only one feature. We still consider a classification problem but use the label set $\mathcal{Y} = \{0, 1\}$ instead of $\{\pm 1\}$, in order to be able to use the standard definition of Threshold Functions.

Definition 4.2.2 — Threshold Functions Hypothesis Class. The set of function:

$$\mathcal{H}_{th} = \{x \mapsto h_\theta(x) : \theta \in \mathbb{R}\}$$

where $h_\theta(x) = \mathbb{1}_{x>\theta}$ and $h_\infty(x) = 0, h_{-\infty}(x) = 1$ for all $x \in \mathbb{R}$, is called the Hypothesis Class of ***Threshold Functions*** over $\mathbb{R}$.

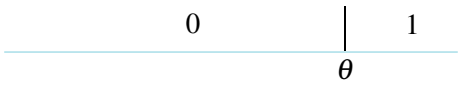


Figure 4.1: *An example of a threshold function*

For the hypothesis class $\mathcal{H}_{th}$ our learning game takes the following form. Functions in $\mathcal{H}_{th}$ classify points on the real line as 0 up to a certain threshold point. Beyond that threshold, they classify all points as 1. Nature chooses one of these functions, that is, it chooses a threshold θ (which is unknown to us) and a distribution $\mathcal{D}$ over the real line. We receive a training sample S of labeled points, and would like to successfully predict the label of future samples. Our job is therefore to determine, as accurately as possible, the unknown cutoff θ.

Now that we were given a hypothesis class, $\mathcal{H}_{th}$, we should specify our strategy, which consists of the number of samples m we need and a learning algorithm $\mathcal{A}$ that will process a training sample and produce a decision rule. As before let $S = \{(x_i, y_i)\}_{i=1}^m$ be the training set. As we will see, our choice of learner will not depend on ε or δ but our choice of m will certainly depend on them.

Learning Algorithm for Threshold Functions

The training data may take the form shown in Figure 4.2 below, but not the form shown in Figure 4.3, which is forbidden because it does not obey the Realizability Assumption (the assumption that Nature chooses $h \in \mathcal{H}$).

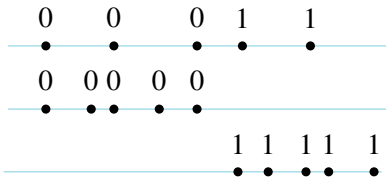


Figure 4.2: *Valid training data for $\mathcal{H}_{th}$*

One possible algorithm, which follows the ERM principle, is the following:

Figure 4.3: *Invalid training data for $\mathcal{H}_{th}$ - violates the Realizability Assumption*

Algorithm 4 Find Threshold Function

Return hypothesis $h_{\theta_{alg}}(x)$ where

- If $y_i = 1$ for all $i = 1,\ldots,m$, then $\theta_{alg} = -\infty$, (the rule classifying all points as 1)
- If $y_i = 0$ for all $i = 1,\ldots,m$, then $\theta_{alg} = +\infty$, (the rule classifying all points as 0)
- In all other cases $\theta_{alg} = \max_i \{x_i : \ y_i = 0\}$

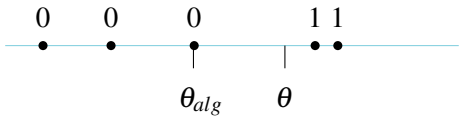


Figure 4.4: *Algorithm for predicting threshold functions*

Number of Samples

Given $\varepsilon, \delta \in (0,1)$ we would like to know what is the sample size, m, that guarantees that, with probability at least $1-\delta$, the true error is at most ε.

Claim 4.2.2 Let $\varepsilon, \delta \in (0,1)$. If $m \geq \frac{\log(1/\delta)}{\varepsilon}$ then for any distribution $\mathcal{D}$ over the real line and any choice of threshold function $f_\theta \in \mathcal{H}_{th}$, with probability of at least $1-\delta$ (over the choice of training sample S of size m), the loss $L_{\mathcal{D},f_\theta}(h_{\theta_{alg}})$ of Algorithm 4 for learning threshold functions is at most ε:

$$\mathcal{D}^m \left\{ S | L_{\mathcal{D},f_\theta}\left(h_{\theta_{alg}}\right) \leq \varepsilon \right\} \geq 1-\delta$$

Proof. Let $\mathcal{D}$ be a probability distribution over $\mathbb{R}$. Let $f_\theta \in \mathcal{H}_{th}$ be the true label function $f_\theta \in \mathcal{H}_{th}$. From the properties of the algorithm it follows that:

$$\theta_{alg} \leq \theta$$

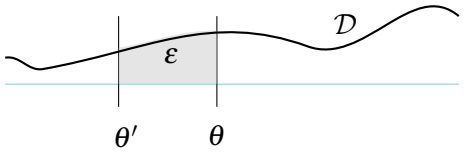
The prediction rule produced by the algorithm will be correct for test samples with $x \leq \theta_{alg}$ or with $x > \theta$ and incorrect for $\theta_{alg} < x \leq \theta$. Thus, the true error is given by

$$L_{\mathcal{D},f_\theta}(h_{\theta_{alg}}) = \mathcal{D}(x : \theta_{alg} < x \leq \theta)$$

If $\mathcal{D}(x : -\infty < x \leq \theta) < \varepsilon$ then $\mathcal{D}(x : \theta_{alg} < x \leq \theta) < \varepsilon$ and therefore the true error is *always* (that is, with probability 1, regardless of S or m) smaller than ε which is what we needed to prove. If $\mathcal{D}(x : -\infty < x \leq \theta) \geq \varepsilon$ then there exists θ' such that $\mathcal{D}(x : \theta' < x \leq \theta) = \varepsilon$.
If there is a point $(x_i, y_i) \in S$ with $\theta' < x_i \leq \theta$ then $y_i = 0$ (because $x_i \leq \theta$) and therefore $\theta' \leq \theta_{alg} \leq \theta$. Thus,

$$L_{\mathcal{D},f_\theta}(h_{\theta_{alg}}) = \mathcal{D}(\{x : \theta_{alg} < x \leq \theta\}) \leq \mathcal{D}(\{x : \theta' < x \leq \theta\}) = \varepsilon$$

The probability of *not* getting such sample in the train set is $(1-\varepsilon)^m$ and therefore the probability of having a true error which is larger than ε is not larger than $(1-\varepsilon)^m$. Now, using $m \geq \frac{\log(1/\delta)}{\varepsilon}$ and $1-\varepsilon < e^{-\varepsilon}$ (which holds for $\varepsilon > 0$), we have $(1-\varepsilon)^m < e^{-m\varepsilon} < \delta$. ■



Threshold Functions - Conclusion

We saw that, for $\mathcal{X} = \mathbb{R}, \mathcal{Y} = \{0,1\}$ and $\mathcal{H} = \mathcal{H}_{th}$, we have a strategy (a choice of sample size $m = m_{\mathcal{H}_{th}}(\varepsilon, \delta)$ and a learning algorithm $\mathcal{A}$) that is *always successful against Nature*, for any values ε, δ specified.

Recall that for $\mathcal{X} = \mathbb{R}$, $\mathcal{Y} = \{0,1\}$ and $\mathcal{H} = \{h |\ h : \mathbb{R} \to \mathbb{R}\}$ there were values of ε, δ for which we *could not be successful* regardless of how we played. In fact, we could not be successful for any $\varepsilon < 1/2$. So whether we can be successful for any ε and δ seems to be a property of the hypothesis class we choose. This leads us to the famous definition of a ***Probably Approximately Correct (PAC)*** learnable hypothesis class.

4.3 PAC Learning

Definition 4.3.1 A hypothesis class, $\mathcal{H}$, is ***PAC Learnable*** if there exists a learning algorithm $\mathcal{A}$ and a function $m_{\mathcal{H},\mathcal{A}} : (0,1)^2 \to \mathbb{N}$ with the following property that:

- For every $\varepsilon, \delta \in (0,1)$
- For every distribution $\mathcal{D}$ over $\mathcal{X}$
- For every labeling function $f : \mathcal{X} \to \{\pm 1\}$ such that there exists $h^* \in \mathcal{H}$ that satisfies $L_{\mathcal{D},f}(h^*) = 0$

when running the learning algorithm $\mathcal{A}$ on $m \geq m_{\mathcal{H},\mathcal{A}}(\varepsilon, \delta)$ *i.i.d* samples generated by $\mathcal{D}$ and labeled by f, the algorithm returns a hypothesis $h_S = \mathcal{A}(S)$ such that, with probability of at least $1 - \delta$ (over the choice of the training samples), we have $L_{\mathcal{D},f}(h_S) \leq \varepsilon$:

$$\mathcal{D}^m \left(\left\{ S \middle| L_{\mathcal{D},f}(h_S) \leq \varepsilon \right\} \right) \geq 1 - \delta$$

Denote the minimal sample size required for the above definition to hold with respect to ε, δ and with respect to any algorithm, by

$$m_{\mathcal{H}}(\varepsilon, \delta) = \min_{\mathcal{A}} m_{\mathcal{H},\mathcal{A}}(\varepsilon, \delta)$$

The function $m_{\mathcal{H}} : (0,1)^2 \to \mathbb{N}$ is called the ***Sample Complexity*** of the PAC learnable hypothesis class $\mathcal{H}$.

R Note that PAC learnability is only one possible definition of learning that can account for the fundamental limitations on accuracy and confidence. We could, for example, settle for a specific, "good enough", values of δ and ε, instead of requiring that the above condition holds for *any* $\varepsilon, \delta \in (0,1)$. Such *weak learners* will be discussed in later chapters.

4.3.1 PAC Learnability of Finite Hypothesis Classes

To better understand when a hypothesis class is PAC learnable, let us first consider the case where $\mathcal{H}$ is a *finite* hypothesis class. Though finite, this hypothesis class is still very large. For example, consider $\mathcal{H}$ as the set all the functions from $\mathcal{X}$ to $\mathcal{Y}$ that can be implemented using a Python program of length at most b, for b fixed and large. Or, take $\mathcal{H}$ to be all the functions from $\mathcal{X}$ to $\mathcal{Y}$ where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are finite.

One might expect that there would not be much to say in this generality, without specific details of $\mathcal{X}$ and $\mathcal{H}$. Surprisingly, it turns out that there is a simple type of learner, called **Empirical Risk Minimization**, that is always successful on finite hypothesis classes and in fact on many other hypothesis classes that we will encounter later. The idea behind these powerful learners is very natural: try to be as correct as possible on the training data. In other words, find the function h in $\mathcal{H}$ that gives the correct label to the maximal number of points in the training sample, S.

Definition 4.3.2 For $h \in \mathcal{H}$ and $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ we define the ***empirical risk*** by

$$L_S(h) = \frac{1}{m} |\{i : h(\mathbf{x}_i) \neq y_i\}| .$$

A rule, h, with $y_i = h(\mathbf{x}_i)$ for $i = 1, \ldots, m$, that is, with $L_S(h) = 0$, is called ***Consistent*** with the training sample, S.

Definition 4.3.3 An algorithm that, for each S, predicts a rule that minimizes the empirical risk $L_S(h)$, is called an ***Empirical Risk Minimization (ERM)*** learner and is denoted by $ERM_{\mathcal{H}}$. That is,

$$ERM_{\mathcal{H}} : S \mapsto \underset{h \in \mathcal{H}}{\operatorname{argmin}}\, L_S(h)$$

Notice that since $L_S(h) \geq 0$ and we are minimizing over a finite class, a minimum exists. For each given S, the minimum may be obtained by more than one h in $\mathcal{H}$, in which case $ERM_{\mathcal{H}}$ actually refers to a *set of algorithms*, each of which returns one of the minimizers. *Under the realizability assumption* we know that the lower bound $L_S(f) = 0$ is achievable. In other words, under our assumption that $f \in \mathcal{H}$, an ERM learner will always return a consistent rule. Hence, in the realizable case, the terms "consistent rule" or "ERM rule" are synonyms.

Learning Finite Classes

Theorem 4.3.1 Let $\varepsilon, \delta \in (0,1)$, $|\mathcal{H}| < \infty$, $m \geq \frac{\log(|\mathcal{H}|/\delta)}{\varepsilon}$ and let h_S^{ERM} be the prediction rule of an $ERM_{\mathcal{H}}$ learner. Then for every $f \in \mathcal{H}$ and every $\mathcal{D}$, with probability of at least $1-\delta$ (over the choice of S of size m), $L_{\mathcal{D},f}(h_S^{ERM}) \leq \varepsilon$.

Proof. Let $\varepsilon \in (0,1)$, $\mathcal{D}$ a probability distribution over $\mathcal{X}$ and a labeling function f. By specifying $\varepsilon, \mathcal{D}$ and f we implicitly define define a subset of $\mathcal{H}$, which we will denote as $\mathcal{H}_B$ ("B" for "bad"), containing all the "bad" h's. That is, all hypothesis that do not approximate f well:

$$\mathcal{H}_B = \left\{ h \in \mathcal{H} \,\middle|\, L_{\mathcal{D},f}(h) > \varepsilon \right\}$$

By definition

$$\left\{ S \,\middle|\, L_{\mathcal{D},f}\left(h_S^{ERM}\right) > \varepsilon \right\} = \left\{ S \,\middle|\, h_S^{ERM} \in \mathcal{H}_B \right\}$$

and therefore, to prove theorem 4.3.1, we have to show that

$$\mathcal{D}^m \left(\left\{ S \,\middle|\, h_S^{ERM} \in \mathcal{H}_B \right\} \right) < \delta$$

.

Any sample S defines a subset of $\mathcal{H}$, which we will denote as $\mathcal{H}_C^S$ ("C" for "consistent"), containing all h's that are consistent with f on S:

$$\mathcal{H}_c^S = \{h :\ L_S(h) = 0\} = \{h :\ h(\mathbf{x}_i) = f(\mathbf{x}_i),\ i = 1 \ldots, m\}$$

Any sample S, also defines an intersection set $\mathcal{H}_{BC}^S = \mathcal{H}_B \cap \mathcal{H}_C^S$ which contains all h's that are consistent *and* bad (Figure 4.5).
Our algorithm is an ERM learner, $h_S^{ERM} \in \mathcal{H}_C^S$. Therefore all the samples S, in the set $\left\{S : h_S^{ERM} \in \mathcal{H}_B\right\}$ are such that the intersection set, $\mathcal{H}_{BC}^S$, is not empty since it contains at least one function, namely, h_S^{ERM}. Thus,

$$\left\{S \middle| h_S^{ERM} \in \mathcal{H}_B\right\} \subseteq \left\{S \middle| \mathcal{H}_{BC}^S \neq \varnothing\right\}$$

As such it is sufficient to prove that:

$$\mathcal{D}^m\left(\left\{S : \mathcal{H}_{BC}^S \neq \varnothing\right\}\right) < \delta$$

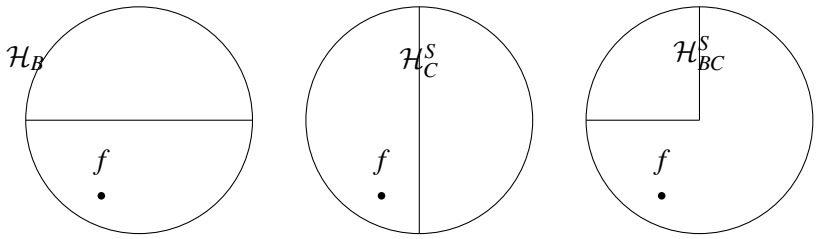


Figure 4.5: *The Bad ($\mathcal{H}_B$) and S-Consistent ($\mathcal{H}_C^S$) subsets of $\mathcal{H}$ and their intersection set ($\mathcal{H}_{BC}^S$)*

Note that

$$\left\{S \middle| \mathcal{H}_{BC}^S \neq \varnothing\right\} = \bigcup_{h\in\mathcal{H}} \left\{S \middle| h \in \mathcal{H}_{BC}^S\right\} = \bigcup_{h\in\mathcal{H}_B} \left\{S \middle| h \in \mathcal{H}_C^S\right\}$$

The first equality is simply a way of saying that instead of checking each S to see if its related intersection set, $\mathcal{H}_{BC}^S$, is non-empty, and then adding it to the above set, we can check each h in $\mathcal{H}$ to see if it appears in any of the $\mathcal{H}_{BC}^S$'s, and each time it does, we add the S that defined that particular $\mathcal{H}_{BC}^S$ to the set. The second equality results from the definition $\mathcal{H}_{BC}^S = \mathcal{H}_B \cap \mathcal{H}_C^S$. We are therefore left with proving that:

$$\mathcal{D}^m\left(\bigcup_{h\in\mathcal{H}_B} \left\{S \middle| h \in \mathcal{H}_C^S\right\}\right) < \delta$$

Using the union bound we get that

$$\mathcal{D}^m\left(\bigcup_{h\in\mathcal{H}_B} \left\{S \middle| h \in \mathcal{H}_C^S\right\}\right) \leq \sum_{h\in\mathcal{H}_B} \mathcal{D}^m\left(\left\{S \middle| h \in \mathcal{H}_C^S\right\}\right)$$

Given a hypothesis h, $\mathcal{D}^m\left(\left\{S|h \in \mathcal{H}_C^S\right\}\right)$ is the probability to pull a sample over which h is perfectly correct (has the right labels for all $\mathbf{x}_i$'s). Since the samples are drawn independently, this probability equals the probability that h will be correct for each $\mathbf{x}_i$ separately. The probability that h will be *incorrect* for a random $\mathbf{x}$ is exactly $L_{\mathcal{D},f}(h)$ and therefore the probability to be correct for m such $\mathbf{x}$'s is $\left(1 - L_{\mathcal{D},f}(h)\right)^m$. We therefore have, for any h,

$$\mathcal{D}^m\left(\left\{S \middle| h \in \mathcal{H}_C^S\right\}\right) = \left(1 - L_{\mathcal{D},f}(h)\right)^m$$

and in particular, if $h \in \mathcal{H}_B$ then $L_{\mathcal{D},f}(h) > \varepsilon$ which means that

$$\mathcal{D}^m\left(\left\{S \middle| L_S(h) = 0\right\}\right) < (1-\varepsilon)^m \quad \forall h \in \mathcal{H}_B$$

Thus we obtain

$$\mathcal{D}^m\left(\bigcup_{h\in\mathcal{H}_B} \left\{S \middle| h \in \mathcal{H}_C^S\right\}\right) \leq \sum_{h\in\mathcal{H}_B} (1-\varepsilon)^m < |\mathcal{H}_B| \cdot (1-\varepsilon)^m \leq |\mathcal{H}| \cdot (1-\varepsilon)^m$$

Finally, using $1-\varepsilon \leq e^{-\varepsilon}$ we conclude:

$$\mathcal{D}^m\left(\left\{S\middle|L_{\mathcal{D},f}(ERM_{\mathcal{H}}(S))>\varepsilon\right\}\right)<|\mathcal{H}|\,e^{-\varepsilon\cdot m}$$

If specifying $m \geq \frac{\log(|\mathcal{H}|/\delta)}{\varepsilon}$, the right-hand side would be smaller δ which concludes the proof. ■

Theorem 4.3.1 means that, by definitions 4.3.1 and 4.1.6 any *finite* hypothesis class $\mathcal{H}$ is PAC-learnable with a sample complexity not larger than $\log(|\mathcal{H}|/\delta)/\varepsilon$. Moreover, for any m greater or equal to that lower bound, any $ERM_{\mathcal{H}}$ learner is a PAC learner.

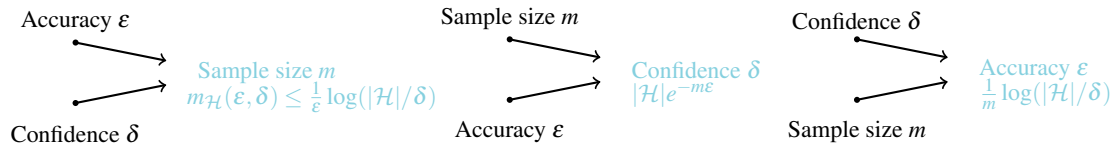


Figure 4.6: *Relation between m, ε and δ*

We have therefore shown that any finite hypothesis class $\mathcal{H}$ is PAC learnable using any ERM learning algorithm, and has a sample complexity $m_{\mathcal{H}}(\varepsilon,\delta) \leq \log(|\mathcal{H}|/\delta)/\varepsilon$. In practical terms, this means that whenever we are given $\varepsilon,\delta \in (0,1)$, a finite hypothesis class $\mathcal{H}$, and a sample of size of at least $\log(|\mathcal{H}|/\delta)/\varepsilon$, we can simply scan $\mathcal{H}$ to find a hypothesis that labels the points in S correctly. With probability of at least $1-\delta$ the generalization error of that hypothesis will not exceed ε.

Several natural questions may now come to mind:

- Is the bound $m_{\mathcal{H}}(\varepsilon,\delta) \leq \frac{\log(|\mathcal{H}|/\delta)}{\varepsilon}$ tight? In other words, can the ERM learner, or an other learner, be Probably Approximately correct (with accuracy ε and confidence δ) using fewer than $\frac{\log(|\mathcal{H}|/\delta)}{\varepsilon}$ samples?
- What happens when noise is present so the y's are not deterministically determined by x?
- What happens when our hypothesis class is infinite?

Consider the last question. As we have seen, the class of threshold functions over $\mathbb{R}$, $\mathcal{H}_{th}$, in spite of being infinite, *is* PAC learnable, with sample complexity $m_{\mathcal{H}_{th}}(\varepsilon,\delta) \leq \frac{\log(1/\delta)}{\varepsilon}$, which is obtained by using an $ERM_{\mathcal{H}_{th}}$ learning rule (recall that the rule output by our algorithm was consistent on any sample). So $\mathcal{H}_{th}$ appears to be simple to learn, even simpler, in terms of the sample complexity, than a finite class. While $\mathcal{Y}^{\mathcal{X}}$ is too complex to learn. Can we explain why? What we need in order to answer the above questions systematically is some sort of a *complexity measure* with which we can order classes by their difficulty along the complexity axis shown in the figure below.

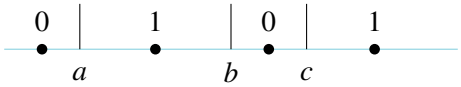
harder classes $\longrightarrow$

$\mathcal{H}_{th}$ *finite class* $\mathcal{Y}^{\mathcal{X}}$

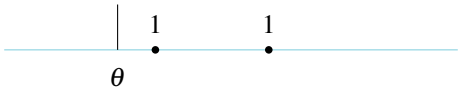
For example, consider the ***Two-Intervals*** hypothesis class, defined by

$$\mathcal{X}=\mathbb{R},\quad \mathcal{H}=\left\{h_{a,b,c}:a<b<c\in\mathbb{R}\right\},\quad h_{a,b,c}=\mathbb{1}_{x\in[a,b]\vee x\geq c}$$

Suppose we would like to learn with the threshold function class, $\mathcal{H}_{th}$, the following sample:

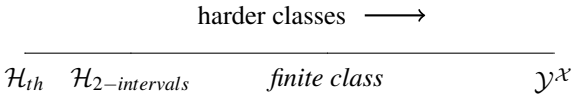


A possible answer would be:



However, samples where $x_1 < x_2$ and $y_1 = 1, y_2 = 0,$, as in the figures below, can not be learned (consistently) by $\mathcal{H}_{th}$, although it can be learned with the 2-intervals class:

Indeed, we somehow feel that the 2-Interval class has a larger complexity than that of $\mathcal{H}_{th}$ but smaller than that of finite classes.



4.3.2 VC Dimension

The VC-Dimension is a*measure of complexity* of hypothesis classes. It is called a *combinatorial* measure because it relies on a certain way of counting the possibilities available in the hypothesis class to label points in $\mathcal{X}$. This measure provides a *precise* test for whether or not a hypothesis class is simple enough to learn in the sense of PAC learnability. It also enables the calculation of clear bounds on the sample complexity of a simple hypothesis class $\mathcal{H}$.

Suppose we receive a training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ and were able to fully explain the labels using a hypothesis from a class $\mathcal{H}$, namely, to find a function $h \in \mathcal{H}$ with empirical risk $L_S(h) = 0$. Suppose now, only to see what will happen, we deliberately corrupt our sample S by changing 'by hand' certain labels, and denote the corrupted sample by S'.
Suppose that we *also* succeed in explaining S' using a different hypothesis from the same class $\mathcal{H}$, namely, find another function $h' \in \mathcal{H}$ with $L_{S'}(h') = 0$. If we are able to do that, no matter what labels we choose to corrupt and regardless of the sample size, it means that something isn't right. How can we hope to generalize based on a training sample S if, regardless of the labels in S, we can find $h \in \mathcal{H}$ with $L_S(h) = 0$?

Definition 4.3.4 — Restriction. Let $C \subseteq \mathcal{X}$ be a subset of the sample space, $\mathcal{X}$, and let $h \in \mathcal{H}$ be a hypothesis. The function $h_C : C \to \mathcal{Y}$, defined as: $\forall \mathbf{x} \in C$, $h_C(\mathbf{x}) = h(\mathbf{x})$, is called the ***restriction*** of h to C. The set $\mathcal{H}_C = \{h_C \,|\, h \in \mathcal{H}\}$ of the restrictions of the h's in $\mathcal{H}$ is called the restriction of $\mathcal{H}$ to C.

R Since $\mathcal{Y} = \{\pm 1\}$, we can represent each h_C by the vector $(h(x_1), \ldots, h(x_{|C|})) \in \{\pm 1\}^{|C|}$. The number of possible such vectors is $2^{|C|}$, therefore $|\mathcal{H}_C| \leq 2^{|C|}$.

To further clarify the above point, consider the following important observation. Suppose that $\mathcal{H}$ contains *all* the possible functions over a set $C \subset \mathcal{X}$ of size m, that is, $\mathcal{H}_C = \mathcal{Y}^C$, then there is no Probably Approximately Correct learner that uses $m/2$ or fewer training samples. To understand why, recall example 4.3 that demonstrated the argument behind the No Free Lunch theorem. To play our game against Nature, we choose a learner $\mathcal{A}$ and ask for a training sample size of $m/2$ or less. For points $\mathbf{x} \in \mathcal{X}$ not seen in the training set, we choose to predict $g(\mathbf{x})$, where $g : \mathcal{X} \to \mathcal{Y}$. We only have to make sure that $g(\mathbf{x})$ is such that the resulting h_S will belong to $\mathcal{H}$.

As in example 4.3, Nature plays a distribution $\mathcal{D}$ that is uniform over C and zero elsewhere, and a labeling function f such that $f_C(\mathbf{x}) = -g_C(\mathbf{x})$, that is, $f(\mathbf{x}) = -g(\mathbf{x})$ for any $\mathbf{x} \in C$ (Since $\mathcal{D}$ vanishes outside of C, Nature doesn't really care how her f is defined outside C). Nature can *always* choose such f, since $\mathcal{H}_C = \mathcal{Y}^C$ so in particular $-g_C(\mathbf{x}) \in \mathcal{H}_C$, which means that there is at least one $h \in \mathcal{H}$ with $h_C(\mathbf{x}) = -g_C(\mathbf{x})$. Again, as in example 4.3, our learner fails since the loss will be $1/2$ or more - regardless of the training sample (as long as it is of size $m/2$ or smaller).
As in example 4.3, the argument presented here is not a full proof since we restricted our choice of algorithm only to such that chooses the *same* label $g(\mathbf{x})$, for *all* S's in which $\mathbf{x}$ does not appear. However, the intuition that our argument implies is correct: As long as $\mathcal{H}$ contains *any* set C of size $2m$ with the property that $\mathcal{H}_C = \mathcal{Y}^C$, then we cannot learn with a training sample of size m. It follows that the *maximal size* of such a set C in $\mathcal{H}$ is a *critical quantity*: (i) it gives us a lower bound on $m_{\mathcal{H}}$, the minimal sample size needed, and (ii) if the maximal size is ∞, namely, if for any $m \in \mathbb{N}$, $\mathcal{X}$ contains such as set C with $|C| > m$, $\mathcal{H}$ is not PAC-learnable.

Definition 4.3.5 — Shattering. Let $C = \{\mathbf{x}_1, \ldots, \mathbf{x}_{|C|}\} \subset \mathcal{X}$, $\mathcal{Y} = \{\pm 1\}$ and $\mathcal{H}_C$ be the restriction of $\mathcal{H}$ to C. We say that $\mathcal{H}$ ***shatters*** C if $|\mathcal{H}_C| = 2^{|C|}$, which is equivalent to saying that $\mathcal{H}_C = \mathcal{Y}^C$.

Definition 4.3.6 — VC-dimension. The ***VC-dimension*** of the hypothesis class $\mathcal{H}$ is defined as

$$VCdim(\mathcal{H}) = \max\{|C| \ : \ \mathcal{H} \ \text{ shatters } \ C\}$$

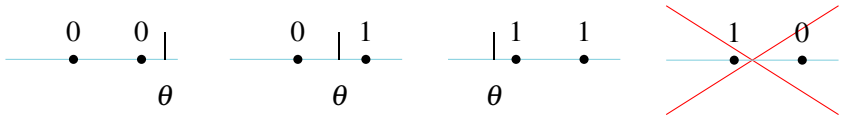
that is, the VC dimension is the maximal size of a set $C \subset \mathcal{X}$ such that $\mathcal{H}_C = \mathcal{Y}^C$.

According to the above definition, in order to show that $VCdim(\mathcal{H}) = d$ we need to show that:

1. There *exists* a set C of size d which is shattered by $\mathcal{H}$.
2. for *any* set C of size greater than d, C is not shattered by $\mathcal{H}$.

■ **Example 4.4 — Threshold class.** Consider the hypothesis class of thereshold function $\mathcal{H}_{th}$. The set $\{0\}$ is shattered by $\mathcal{H}_{th}$ since $x = 0$ can receive both the label 0 and 1, depending on the location of the threshold θ.

In contrast to the above, no two points, x_1 and x_2 can be shattered because if $x_1 < x_2$ then $y_1 \leq y_2$ and therefore the pair of labels $y_1 = 1, y_2 = 0$ is forbidden.



■

■ **Example 4.5 — One-Interval hypothesis class.** Consider the *One-Interval hypothesis class* over $\mathcal{X} = \mathbb{R}$ defined as

$$\mathcal{H} = \left\{ h_{a,b} : a < b \in \mathbb{R} \right\}, \quad h_{a,b}(x) = \mathbb{1}_{x \in [a,b]}$$

Now, take for example the two points $\{0,1\}$. We can place the interval over both, over any one of them, or outside $[0,1]$. Therefore, $\{0,1\}$ is shattered. However, any three points cannot be shattered. Let $x_1 < x_2 < x_3$, then no single interval can cover x_1 and x_3 without containing also x_2 and therefore the labeling $y_1 = 1, y_2 = 0, y_3 = 1$ is forbidden. ■

4.3.3 The Fundamental Theorem of Statistical Learning

In the previous sections, we worked hard to understand two fundamental definitions: PAC-Learnability (and sample complexity) of a hypothesis class, and VC-dimension of a hypothesis class.

Along the way, we saw some connections between these two definitions:

- We saw that a finite hypothesis class is PAC-learnable (using the ERM learners) with sample complexity

$$m_{\mathcal{H}}(\varepsilon, \delta) \leq \frac{\log(|\mathcal{H}|) + \log(1/\delta)}{\varepsilon}$$

  and also that in this case $VCdim(\mathcal{H}) \leq \log_2(|\mathcal{H}|)$. These results indicate that there might be a general relation, valid for other hypothesis classes as well, between an *upper bound* on $m_{\mathcal{H}}$ and $VCdim(\mathcal{H})$.
- We saw, using the same argument that led us to the No Free Lunch theorem, that $VCdim(\mathcal{H})$ also gives a *lower bound* on the sample complexity $m_{\mathcal{H}}$ of a hypothesis class $\mathcal{H}$, and that if $VCdim(\mathcal{H})$ is infinite, that class is not PAC-Learnable.

The surprising, wonderful, truth is that VC-dimension gives a complete characterization of PAC-learnability and sample complexity of a hypothesis class, and gives a decisive answer to all the questions we posed at various stages along the way (such as which classes are PAC-learnable, with what sample complexity, and with what algorithm, and is there an algorithm that uses the minimal possible sample size.) These facts result from the ***The Fundamental Theorem of Statistical Learning*** which states the following:

- The PAC-learnability of a hypothesis class is characterized by its *VC dimension*, a combinatorial property that denotes the maximal size of a sample that can be shattered by the class.
- A hypothesis class is PAC-learnable *if and only if* its VC-dimension is finite.
- When $VCdim(\mathcal{H})$ is finite, $\mathcal{H}$ has a finite sample complexity which is, up to multiplicative constants, given by

$$m_H(\varepsilon, \delta) \sim \frac{VCdim(\mathcal{H}) + \log(1/\delta)}{\varepsilon}$$

- The ERM learning rule is a generic (near) optimal learner, in the sense that when a hypothesis class is PAC-learnable, an ERM learner using

$$m(\varepsilon, \delta) \sim \frac{VCdim(\mathcal{H}) \log(1/\varepsilon) + \log(1/\delta)}{\varepsilon}$$

  is a Probably Approximately correct learner with accuracy ε and confidence δ.

Theorem 4.3.2 — The Fundamental Theorem of Statistical Learning. Let $\mathcal{H}$ be a hypothesis class of binary classifiers with VC-dimension $d \leq \infty$. Then, $\mathcal{H}$ is PAC-learnable if and only if $d < \infty$. In this case: there are absolute constants C_1, C_2 (that is, they are independent of d, ε and δ) such that the sample complexity of $\mathcal{H}$ satisfies

$$C_1 \frac{d + \log(1/\delta)}{\varepsilon} \leq m_{\mathcal{H}}(\varepsilon, \delta) \leq C_2 \frac{d \log(1/\varepsilon) + \log(1/\delta)}{\varepsilon}$$

Furthermore, the upper bound on sample complexity is achieved by the ERM learner.

As we saw, the intuition behind the lower bound was based on how the VC-dimension $VCdim(\mathcal{H})$ was related to the *minimal* number of training samples needed to PAC-learn the hypothesis class $\mathcal{H}$.

To understand the upper bound, we need to understand how is it that the ERM learner is a *generic learning algorithm* that is able to PAC-learn $\mathcal{H}$ with a training sample size related to the VC-dimension $VCdim(\mathcal{H})$.

Before discussing the upper bound, we shall extend our theoretic framework to make it much more flexible and realistic.

4.4 Agnostic PAC

The theoretical framework we developed so far has several serious limitations when it comes to real-world learning problems.

- *It doesn't model noisy labels*: We have no model for measuring errors in labels. In practice, sometimes even though the label for some $x \in \mathcal{X}$ should have been for example 1, it can be measured as -1 due to measurement mistake, noise, etc. We want the learning framework to allow for the fact that we may, with low probability, observe the point $x \in \mathcal{X}$ twice, and get two different labels.
- *The realizability assumption is unrealistic*: The hypothesis class is, after all, only an intelligent guess, and it is unrealistic to assume that the true label function will belong to it.
- *Limited to misclassification loss*: In the previous sections we measured the performance of a classifier using the misclassification loss (the 0-1 loss). We would like to be able to measure performance using any loss function.

To address these limitations we introduce the ***Agnostic PAC*** framework. In addition to address these limitations we can also prove that the the fundamental theorem of statistical learning holds in the Agnostic PAC framework as well.

4.4.1 Introducing the Joint Probability Distribution Over $\mathcal{X} \times \mathcal{Y}$

In the PAC framework, $\mathcal{D}$ is a probability distribution over the sample space $\mathcal{X}$ and the labels are determined deterministically using the label function f. In the new, more general framework, $\mathcal{D}$ will be a probability distribution over $\mathcal{X} \times \mathcal{Y}$.

This means that when we draw a new random example $(\mathbf{x}, y)$ - whether for the training sample S or as a test sample - there is randomness in *both* $\mathbf{x}$ and y which are now *dependent* random quantities.

We can factor $\mathcal{D}$ in two ways, conditioning on $\mathbf{x}$ or on y, both are useful for our understanding. Let (X,Y) be a random variable taking valued in $\mathcal{X} \times \mathcal{Y}$ whose distribution is $\mathcal{D}$.

- $\mathbb{P}(X = \mathbf{x}, Y = y) = \mathbb{P}(X = \mathbf{x})\mathbb{P}(Y = y | X = \mathbf{x})$. From this perspective, this is a direct generalization of our previous framework, where $\mathbf{x}$ was random and $y = f(\mathbf{x})$. Indeed, we draw $\mathbf{x}$ from the marginal distribution with probability $\mathbb{P}(X = \mathbf{x})$ - as we did in the previous framework. We then choose a corresponding label according to the conditional probability $\mathbb{P}(Y = y | X = \mathbf{x})$.
  Since the marginal random variable Y describing the label is a Bernoulli random variable, one can think of it as a result of a coin flip of a biased coin, with a probability $p(\mathbf{x})$ to obtain +1, where the function $p : \mathcal{X} \to [0,1]$ is defined by $\mathbb{P}(Y = +1 | X = \mathbf{x}) = p(\mathbf{x})$. If $p(\mathbf{x}) = 0$ or $p(\mathbf{x}) = 1$ for some $\mathbf{x}$, the label is deterministic and we are back to the label function f. But for other values of $p(\mathbf{x})$, whereas before the label depended deterministically on $\mathbf{x}$, now it is random. This models *measurement noise* - the fact that there may be noise in the labels and that the distribution of the noise may change from one $\mathbf{x}$ to another. This attitude is similar to that of the Logistic Regression classifier, although in that case we did not pay attention to the distribution on $\mathbf{x}$ - instead, we assumed the samples are given and tried to estimate the conditional probability $\mathbb{P}(Y = +1 | X = \mathbf{x}) = p(\mathbf{x})$.

- $\mathbb{P}(X=\mathbf{x},Y=y)=\mathbb{P}(Y=y)\mathbb{P}(X=\mathbf{x}|Y=y)$. From this perspective, we first draw the label according to a "coin flip" - a Bernoulli random variable. Then, each label has its own distribution for the samples $\mathbf{x}$. We draw the sample $\mathbf{x}$ from $\mathbb{P}(X=\mathbf{x}|Y=+1)$ or from $\mathbb{P}(X=\mathbf{x}|Y=-1)$, according to the label y we obtained. This is a similar approach to the one used in the LDA classifier.

When $\mathcal{D}$ was a distribution over $\mathcal{X}$ alone, we defined the misclassification loss, (4.1), as the probability of obtaining an $\mathbf{x}$ whose *correct* label, $f(\mathbf{x})$, differs from the predicted one, $h(x)$. Now, with $\mathcal{D}$ as a distribution over $\mathcal{X}\times\mathcal{Y}$, we generalize simply by defining the loss as the probability of obtaining an $\mathbf{x}$ whose *measured* label, y, will differ from the predicted one, $h(\mathbf{x})$:

$$L_{\mathcal{D}}(h)=\mathbb{P}_{(\mathbf{x},y)\sim\mathcal{D}}\{h(\mathbf{x})\neq y\}=\mathcal{D}\{(\mathbf{x},y)\,|\,h(\mathbf{x})\neq y\} \tag{4.2}$$

4.4.2 Relaxing Realizability Assumption

Recall that in the case of deterministic labeling, under the realizability assumption, we could reach zero generalization error:

$$\min_{h\in\mathcal{H}} L_{\mathcal{D},f}(h)=L_{\mathcal{D},f}(f)=0$$

However, according to (4.2), in order to calculate the loss, we now have to compare a deterministic values, $h(\mathbf{x})$, to a random one, the measured y, and therefore we can no longer expect zero loss. In other words, we no longer have a "ground truth" labeling function f, at least not one accessible by measurement. The closest thing we have to f is the conditional probability $\mathbb{P}(Y=y|X=\mathbf{x})$).

So the realizability assumption is no longer practical in the sense that we no longer expect to be able to reach 0 generalization loss. Even if a certain underlying true-label function does exist, and no matter how close our predicted rule, $h(\mathbf{x})$, resembles it, we may end up with a non-negligible loss due to the noise. This means we have to change also the definition of *accuracy*: we would like the learning algorithm to output a rule which has generalization loss at most ε *above the minimal possible loss* $\min_{h\in\mathcal{H}} L_{\mathcal{D}}(h)$. We now proceed to identify such a lower bound for the loss.

Definition 4.4.1 Let $\mathcal{D}$ be a probability distribution over $\mathcal{X}\times\mathcal{Y}$. We define the ***Bayes Optimal Classifier*** by

$$f_{\mathcal{D}}(\mathbf{x})=\begin{cases}1 & \mathbb{P}(y=1|\mathbf{x})\geq 1/2\\ 0 & otherwise\end{cases}$$

Note that although $f_{\mathcal{D}}:\mathcal{X}\to\mathcal{Y}$ is a hypothesis, it depends on $\mathcal{D}$, which according to the rules of the game, we don't know. So $f_{\mathcal{D}}$ is what is known as an ***Oracle Quantity***: if we had an oracle telling us $\mathcal{D}$, then we could classify with $f_{\mathcal{D}}$. Oracle quantities, like this one, are used to compare the loss of any other rule to the loss of the *best possible* rule.

Definition 4.4.2 Let $\varepsilon>0$. We say that a rule $h\in\mathcal{H}$ is ***Approximately Correct*** with ***accuracy*** ε with respect to the distribution $\mathcal{D}$ on $\mathcal{X}\times\mathcal{Y}$ if $L_{\mathcal{D}}(h)$ is as most ε away from the best possible loss achievable by *any* hypothesis in $\mathcal{H}$:

$$L_{\mathcal{D}}(h)\leq\min_{h'\in\mathcal{H}} L_{\mathcal{D}}(h')+\varepsilon$$

Notice once more that in our previous framework, under the realizability assumption, the minimal loss was simply 0 since we *assumed* the existence of some $h'\in\mathcal{H}$ with $L_{\mathcal{D}}(h')=0$. Thus, we let go of the realizability assumption: we no longer assume that there exists a "correct" labeling function and in particular no longer assume that Nature plays a labeling function in the chosen hypothesis class $\mathcal{H}$. Nature's strategy consists only of choosing the joint distribution $\mathcal{D}$ over $\mathcal{X}\times\mathcal{Y}$.

4.4.3 General Loss Function

The last extension of the framework developed in the previous sections is to allow the use of a general loss function.

Definition 4.4.3 A ***Loss Function*** is a function $\ell : \mathcal{H} \times Z \to [0,\infty)$, where $Z = \mathcal{X} \times \mathcal{Y}$.

R Instead of writing $\ell(h,z)$, we shall often write $\ell(h,(\mathbf{x},y))$ or $\ell(h(\mathbf{x}),y)$.

We already used the most common example of a classification loss function - the misclassification loss, also known as the *0-1 loss*:

$$\ell_{0,1}(h,(\mathbf{x},y)) := \begin{cases} 1 & h(\mathbf{x}) \neq y \\ 0 & h(\mathbf{x}) = y \end{cases}$$

The definition, (4.2), of the generalization loss we have been using, $L_{\mathcal{D}}(h)$, can be rewritten in terms of $\ell_{0,1}$ as:

$$L_{\mathcal{D}}(h) = \mathbb{E}_{\mathcal{D}}[\ell_{0,1}(h,(\mathbf{x},y))]$$

where $\mathbb{E}_{\mathcal{D}}[\cdot]$ denotes the expected value according to $(\mathbf{x},y) \sim \mathcal{D}$.
Written in its new form, the above definition can be naturally extended to include any loss function:

Definition 4.4.4 — Generalization Loss. Given a distribution $\mathcal{D}$ over $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$, a hypothesis $h : \mathcal{X} \to \mathcal{Y}$ and a general loss function $\ell : \mathcal{H} \times \mathcal{Z} \to [0,\infty)$, we define the Generalization Loss, $L_{\mathcal{D}}(h)$, of a Hypothesis h induced by ℓ with respect to $\mathcal{D}$, as the expected value (according to $z \sim \mathcal{D}$) of ℓ:

$$L_{\mathcal{D}}(h) = \mathbb{E}_{\mathcal{D}}[\ell(h,z)]$$

Since definition 4.4.2 did not refer explicitly to the choice of a loss function, we shall keep it as our definition of an approximately correct learner and of the accuracy ε, also in the case of a general (not necessarily 0-1) loss function.

4.4.4 Agnostic-PAC Learnability

The new, more general framework we develop is called ***Agnostic-PAC***.

Definition 4.4.5 Let $\varepsilon, \delta \in (0,1)$. We say that a learner, $\mathcal{A}$, is ***Agnostic Probably Approximately Correct*** (Agnostic-PAC) with a confidence δ and an accuracy ε, ***with respect to*** a loss function ℓ, hypothesis class $\mathcal{H}$ and a distribution $\mathcal{D}$ on $\mathcal{X} \times \mathcal{Y}$, if the probability of obtaining a training sample, S, for which $\mathcal{A}$ will output a prediction rule, $h_S \in \mathcal{H}$, with a loss, $L_{\mathcal{D}}(h_S)$, of at most ε away from the best possible loss achievable by *any* hypothesis in $\mathcal{H}$, is larger or equal to $1-\delta$:

$$\mathcal{D}^m\left(\left\{S \middle| L_{\mathcal{D}}(h_S) \leq \min_{h' \in \mathcal{H}} L_{\mathcal{D}}(h') + \varepsilon\right\}\right) \geq 1-\delta$$

Definition 4.4.6 — Agnostic PAC Learnability. A hypothesis class $\mathcal{H}$ is Agnostic-PAC learnable with respect to loss $\ell : \mathcal{H} \times (\mathcal{X} \times \mathcal{Y}) \to [0,\infty)$ if there exists a function $\tilde{m}_{\mathcal{H}} : (0,1)^2 \to \mathbb{N}$ and a learning algorithm $\mathcal{A} : (\mathcal{X} \times \mathcal{Y})^m \to \mathcal{H}$ with the following property:

- For any $\varepsilon, \delta \in (0,1)$
- For any distribution $\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$

when running the learning algorithm $\mathcal{A}$ on $m \geq \tilde{m}_{\mathcal{H}}(\varepsilon,\delta)$ *i.i.d* samples degenerated by $\mathcal{D}$, the algorithm

returns a hypothesis $h_S = \mathcal{A}(S)$ such that, with probability of at least $1-\delta$:

$$\mathcal{D}^m\left(\left\{S \,\middle|\, L_{\mathcal{D}}(h_S) \leq \min_{h' \in \mathcal{H}} L_{\mathcal{D}}(h) + \varepsilon\right\}\right) \geq 1-\delta$$

It can be shown that an Agnostic-PAC learner with $\mathcal{A}$ is a PAC learner (see Ex.5). Using Agnostic-PAC learnability , let us write the "learning game" in the Agnostic PAC framework. Let $\varepsilon, \delta \in (0,1)$ be the desired accuracy and confidence levels, let $\mathcal{H}$ be a hypothesis class $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$ and a loss function ℓ. We play a game against Nature, with random payoff.

- We choose a sample size m and a learner $\mathcal{A} : (\mathcal{X}, \mathcal{Y})^m \to \mathcal{H}$ where m and $\mathcal{A}$ can depend on ε, δ.
- Nature knows our strategy, and, after us, chooses a strategy that consists of a probability distribution $\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$. This strategy can depend on $\varepsilon, \delta, \mathcal{H}$ and also on our strategy, m and $\mathcal{A}$.
- A sample $S \in (\mathcal{X} \times \mathcal{Y})^m$ of size m is drawn according to $\mathcal{D}$.
- The sample S is fed into $\mathcal{A}$ to produce a prediction rule $h_S = \mathcal{A}(S)$. Note that $h_S \in \mathcal{H}$.
- The payoff is $L_{\mathcal{D}}(h_S) = \mathbb{E}_{(\mathbf{x},y)\sim\mathcal{D}}[\ell(h,(\mathbf{x},y))]$. It is random since S is random and therefore h_S is random.
- Nature does her best to win so we look for learners $\mathcal{A}$ that have a **guaranteed maximal loss** $L_{\mathcal{D}}(h)$ **for any** strategy $\mathcal{D}, f$ that Nature might play.
- To determine if we were successful in the game, we play the game many many times (both us and Nature play the same strategies, just the training samples drawn are different). We count and calculate the probability, over the random draws of training samples S, of the event $\{S \sim \mathcal{D}^m \,|\, L_{\mathcal{D}}(h_S) \leq \min_{h' \in \mathcal{H}} L_{\mathcal{D}}(h') + \varepsilon\}$. If this probability is found to be larger than $1-\delta$, that is, if the learner $\mathcal{A}$ we chose was Probably Approximately correct with accuracy ε and confidence δ - against Nature's best strategy - *we say that we've been successful (with regards to the parameters ε, δ) and the hypothesis class $\mathcal{H}$.*

Note that in order to calculate the probability of the event $\{S \sim \mathcal{D}^m \,|\, L_{\mathcal{D}}(h_S) \leq \min_{h' \in \mathcal{H}} L_{\mathcal{D}}(h') + \varepsilon\}$ we have to assume a knowledge of the "Oracle quantity" $\min_{h' \in \mathcal{H}} L_{\mathcal{D}}(h')$ - the best possible loss of any rule in $\mathcal{H}$.

One may ask whether the Agnostic PAC learnability, allowing, for example, more choices for the distribution $\mathcal{D}$, imply PAC-learnability. Not only the answer to this question is positive, but perhaps surprisingly, the inverse claim is also true. In other words, moving to the more general framework of Agnostic-PAC did not change anything, as expressed by the following theorem:

Theorem 4.4.1 Let $\mathcal{X}$ be a sample space and $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$ a hypothesis class. Then $\mathcal{H}$ is PAC-Learnable if and only if it is Agnostic-PAC learnable.

4.5 The Fundamental Theorem of Statistical Learning

Recall that in the realizable case, an ERM learner was defined as any $h \in \mathcal{H}$ consistent with the training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ which in turn implied that it minimized the empirical risk. In the current more general case (where the notion of consistency is no more relevant - even the training set does not have to be consistent with itself since the same point may appear with different labels) we redefine ERM as *any* minimizer of the empirical risk.

Definition 4.5.1 — Empirical Risk and ERM Learner in the Agnostic-PAC framework. Let $h : \mathcal{X} \to \mathcal{Y}$ be a prediction rule. We define the ***empirical risk*** of h with respect to the loss function ℓ and

the sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ by

$$L_S(h) = \frac{1}{m}\sum_{i=1}^{m} \ell(h, z_i), \quad z_i = (\mathbf{x}_i, y_i)$$

An ***ERM Learning Algorithm***, $\mathcal{A}_{ERM}$, in the Agnostic-PAC framework is defined as an algorithm that outputs a hypothesis that minimizes the empirical risk:

$$\mathcal{A}_{ERM} : S \mapsto h, \quad h \in \left\{ \operatorname*{argmin}_{h \in \mathcal{H}} L_S(h) \right\}$$

Notice that as before the ERM rule may not be unique. There can be many hypotheses in $\mathcal{H}$ that achieve the minimum $\min_{h\in\mathcal{H}} L_S(h)$.
ERM learners are successful and logical due to the Weak Law of Large Numbers (WLLN) which states that if X_i are a series of $i.i.d$ random variables and $\mu = \mathbb{E}(X_i)$, then

$$\lim_{m\to\infty} \frac{1}{m}\sum_{i=1}^{m} X_i = \mu$$

where the convergence is *in probability*. Namely, for any $\delta > 0$

$$\lim_{m\to\infty} \mathbb{P}\left\{ \left| \frac{1}{m}\sum_{i=1}^{m} X_i - \mu \right| > \delta \right\} = 0$$

which is equivalent to require that for any $\varepsilon, \delta > 0$ there is $m_0 \in \mathbb{N}$ such that for $m > m_0$,

$$\mathbb{P}\left\{ \left| \frac{1}{m}\sum_{i=1}^{m} X_i - \mu \right| > \delta \right\} < \varepsilon.$$

Observe now that for any h we have

- $\mathbb{E}_{\mathcal{D}}[L_S(h)] = L_{\mathcal{D}}(h)$
- By WLLN, when S is $i.i.d$ sample of size m, $\lim_{m\to\infty} L_S(h) = L_{\mathcal{D}}(h)$, in probability
- Therefore for any $\delta > 0$ there is $m_0 \in \mathbb{N}$ such that for $m > m_0$,

$$\mathbb{P}\left\{ \left| L_S(h) - L_{\mathcal{D}}(h) \right| > \delta \right\} < \varepsilon\,.$$

- But does this mean that $\operatorname{argmin}_{h\in\mathcal{H}} L_S(h)$ is close to $\operatorname{argmin}_{h\in\mathcal{H}} L_{\mathcal{D}}(h)$?

Although this is a good start, does this imply that $\operatorname{argmin}_{h\in\mathcal{H}} L_S(h)$ is close to $\operatorname{argmin}_{h\in\mathcal{H}} L_{\mathcal{D}}(h)$?

4.5.1 The Fundamental Theorem

Let us reformulate the Fundamental Theorem using Agnostic-PAC learnability and the generalized notion of ERM we just defined.

Theorem 4.5.1 — The Fundamental Theorem of Statistical. Let $\mathcal{H}$ be a hypothesis class of binary classifiers with VC-dimension $d \le \infty$. Then, $\mathcal{H}$ is **Agnostic-PAC learnable** if and only if $d < \infty$. In this case:

1. There are absolute constants C_1, C_2 such that the sample complexity of $\mathcal{H}$ satisfies

$$C_1 \frac{d + \log(1/\delta)}{\varepsilon^2} \le m_{\mathcal{H}}(\varepsilon, \delta) \le C_2 \frac{d + \log(1/\delta)}{\varepsilon^2}$$

2. Furthermore, the upper bound on sample complexity is achieved by the ERM learner.

Note that the "price" we pay for Agnostic PAC learning is that the sample complexity is proportional to $1/\varepsilon^2$ and not to $1/\varepsilon$ as in the PAC Fundamental theorem.

We conclude this chapter with partially going into the proof of the above theorem (4.5.1), and doing so for the qualitative rather than the quantitative part of the theorem. This will help to understand as to how is it that the VC-dimension characterizes learnability, namely, why is that $\mathcal{H}$ **is Agnostic-PAC learnable if and only if** $VCdim(\mathcal{H}) < \infty$. The first part of the theorem is that learning $\mathcal{H}$ is possible if and only if $\mathcal{H}$ is of finite VC-dimension. If it is not of finite VC-dimension then it is impossible to create an Agnostic-PAC learner $\mathcal{A}$ for $\mathcal{H}$ (with accuracy ε and confidence δ) by **any** learning algorithm and using **any** number of training samples.

We have already gained some intuition when discussing the No-Free Lunch theorem (4.2.1). We saw an informal argument that, if there exists $C \subset \mathcal{X}$ that is **shattered** by $\mathcal{H}$, then no learning algorithm can be a Probably Approximately correct learner if it is based on less than $|C|/2$ samples. Now, the statement $VCdim(\mathcal{H}) = \infty$ just means that there are subsets of $\mathcal{X}$ of arbitrary size that are shattered by $\mathcal{H}$ and therefore, no finite sample size will do.

The second part of Lemma 4.5.1, states that if $\mathcal{H}$ is a hypothesis class with $VCdim(\mathcal{H}) = d < \infty$ then $\mathcal{H}$ is Agnostic-PAC learnable as defined in Definition 4.4.4, using any ERM learner. To prove this we will need to define the Uniform Convergence property of hypothesis classes.

4.5.2 Uniform Convergence property

An ERM learner chooses a rule $ERM_{\mathcal{H}}(S)$ which minimizes $L_S(h)$ for the sample S at hand. We hope that the rule $h_S \in ERM_{\mathcal{H}}(S)$, which has minimal empirical risk, will generalize well. Formally, we have to prove that

$$\mathcal{D}^m \left\{ S \in (\mathcal{X} \times \mathcal{Y})^m \,\middle|\, |L_{\mathcal{D}}(h_S) - L_S(h_S)| \leq \varepsilon \right\} \geq 1 - \delta$$

This can only happen if S is a "special" sample - one for which for any $h \in \mathcal{H}$ the empirical risk $L_S(h)$ is pretty close to the generalization loss $L_{\mathcal{D}}(h)$. This is hard to prove. Note that for any $h \in \mathcal{H}$ we have $\mathbb{E}[L_S(h)] = L_{\mathcal{D}}(h)$, so, as we have seen above, by the weak law of large numbers, $L_S(h)$ converges to $L_{\mathcal{D}}(h)$ in probability as the sample size $m \to \infty$. This means that

$$\forall \mathcal{D}\ \forall h \in \mathcal{H}\ \forall \varepsilon, \delta \in (0,1) \quad \exists m_0 \in \mathbb{N} \quad \text{such that} \quad \mathbb{P}\{|L_S(h) - L_{\mathcal{D}}(h)| < \varepsilon\} > 1 - \delta$$

However m_0 depends on both $\mathcal{D}$ and h. We want m_0 that is **uniform** in the distributions $\mathcal{D}$ and the hypotheses $h \in \mathcal{H}$.

Definition 4.5.2 — Uniform Convergence of Function Sequences. A sequence of functions $f_n : X \to \mathbb{R}$ converges uniformly to $f : X \to \mathbb{R}$ if and only if

$$\forall \varepsilon > 0 \quad \exists m_0 \in \mathbb{N} \quad \text{such that} \quad \forall x \in X \ |f_n(x) - f(x)| < \varepsilon$$

Indeed, what we want is to ensure that $L_S(h)$ converges to $L_{\mathcal{D}}(h)$ **uniformly in** $\mathcal{D}$ **and in** $h \in \mathcal{H}$. This leads to the following definition.

Definition 4.5.3 — ε-representative. A training sample S is called ε-representative for $\mathcal{D}, \mathcal{H}, \ell$ if and only if

$$\forall h \in \mathcal{H} \quad |L_S(h) - L_{\mathcal{D}}(h)| < \varepsilon$$

This condition will ensure that minimizing $L_S(h)$ over $h \in \mathcal{H}$ will be close to minimizing $L_D(h)$ over $h \in \mathcal{H}$, which is approximately what we would like to achieve. Specifically, we can show that if we have an ε-representative training set S, then $ERM_{\mathcal{H}}(S)$ will "almost" achieve $\min_{h \in \mathcal{H}} L_{\mathcal{D}}(h)$.

Lemma 4.5.2 Let S be an $\varepsilon/2$-representative sample for $\mathcal{D}, \mathcal{H}, \ell$. Let h_S be any output of $ERM_{\mathcal{H}}(S)$, namely,$h_S \in \operatorname{argmin}_{h\in\mathcal{H}} L_S(h)$. Then

$$L_{\mathcal{D}}(h_S) \leq \min_{h\in\mathcal{H}} L_{\mathcal{D}}(h) + \varepsilon$$

Definition 4.5.4 — Uniform Convergence Property. A hypothesis class $\mathcal{H}$ is said to have the **uniform convergence property** if and only if there exists a function $m_{\mathcal{H}}^{UC} : (0,1)^2 \to \mathbb{N}$ such that for every $\varepsilon, \delta \in (0,1)$ and every distribution $\mathcal{D}$ on $\mathcal{X} \times \mathcal{Y}$

$$\mathcal{D}^m\left(\{S \in (\mathcal{X}\times\mathcal{Y})^m \,|\, S \text{ is } \varepsilon\text{-representative}\}\right) \geq 1-\delta$$

It can then be shown that if a hypothesis class has the uniform convergence property with function $m_{\mathcal{H}}^{UC}$ then $\mathcal{H}$ is Agnostic-PAC learnable with sample complexity $m_{\mathcal{H}}(\varepsilon,\delta) \leq m^{UC}(\varepsilon/2,\delta)$.

Finite VC-Dimension Implies Uniform Convergence Property

So to show Part Two of the fundamental theorem (that ERM is a universal learner), it is enough to show that if $VCdim(\mathcal{H}) < \infty$ then $\mathcal{H}$ has the uniform convergence property. This means showing that for large enough m, that does not depend on $\mathcal{D}$, an $i.i.d$ sample is ε-representative with probability at least $1-\delta$, and that this hold for any possible $\mathcal{D}$.
To achieve uniformity across both $\mathcal{D}$ and $h \in \mathcal{H}$ we define the following functionn $F_m^{\mathcal{D}} : (\mathcal{X}\times\mathcal{Y})^m \to \mathbb{R}$ by

$$F_m^{\mathcal{D}}(S) = \sup_{h\in\mathcal{H}} \left| L_{\mathcal{D}}(h) - L_S(h) \right| \tag{4.3}$$

$F_m^{\mathcal{D}}$ maps a training sample of size m, to a real number measuring its "worse possible confusion" - the maximal difference, over $\mathcal{H}$, between an empirical risk of a hypothesis h and the generalization error of that h. Observe that $F_m^{\mathcal{D}}$ is a function of the random sample S, so it is a random variable, whose distribution depends on the distributions $\mathcal{D}^m$ of training sets of length m.

In essence, we would like to show that with high probability, $F_m^{\mathcal{D}}$ is small. Formally, we would like to show that for every $\varepsilon, \delta \in (0,1)$ there exists $m_{\mathcal{H}}^{UC}(\varepsilon,\delta) \in \mathbb{N}$ such that for every distribution $\mathcal{D}$:

$$\mathcal{D}^m\left\{F_m^{\mathcal{D}}(S) > \varepsilon\right\} < \delta$$

The Case Of Finite $\mathcal{H}$

To understand the key argument, let us first consider the easier case of finite $\mathcal{H}$ and see how Agnostic-PAC learnability can be proven.

Claim 4.5.3 Let $\varepsilon, \delta \in (0,1)$ then there exists $m_0 \in \mathbb{N}$ such that for any $m > m_0$ it holds that

$$\forall \mathcal{D} \text{ over } \mathcal{X}\times\mathcal{Y} \quad \mathcal{D}^m\left\{F_m^{\mathcal{D}}(S) > \varepsilon\right\} \leq \delta$$

Proof. Directly by definition then

$$\begin{aligned}
\mathcal{D}^m\left\{F_m^{\mathcal{D}}(S) > \varepsilon\right\} &\overset{def.}{=} \mathcal{D}^m\left\{S \,\middle|\, \exists h \in \mathcal{H}, |L_S(h) - L_{\mathcal{D}}(h)| > \varepsilon\right\} \\
&\overset{union\ bound}{\leq} \sum_{h\in\mathcal{H}} \mathcal{D}^m\left\{S \,\middle|\, |L_S(h) - L_{\mathcal{D}}(h)| > \varepsilon\right\} \\
&\leq |\mathcal{H}| \cdot \max_{h\in\mathcal{H}} \mathcal{D}^m\left\{S \,\middle|\, |L_S(h) - L_{\mathcal{D}}(h)| > \varepsilon\right\}
\end{aligned}$$

We thus need to bound $\mathcal{D}^m\left\{S\left|\,|L_S(h)-L_{\mathcal{D}}(h)|>\varepsilon\right.\right\}$ uniformly in $\mathcal{D}$ and h. By the weak law of large numbers (WLLN), since $L_S(h)$ is an empirical mean of $i.i.d$ random variables with expected value $L_{\mathcal{D}}(h)$, we know that

$$\forall\varepsilon>0\quad \mathcal{D}^m\left\{\left|L_S(h)-L_{\mathcal{D}}(h)\right|>\varepsilon\right\}\overset{m\to\infty}{\longrightarrow}0$$

This is not sufficient as we want the bound to not depend on $\mathcal{D},h$. What we need is a known as a **concentration of measure** inequality: a way to bounds the distance between the empirical mean and the expected value. Indeed, recall Hoeffding's Inequality: Let $\theta_1,\dots\theta_m$ be a sequence of $i.i.d$ random variables and assume that for all i, $\mathbb{E}[\theta_i]=\mu$ and $\mathbb{P}\{a\le\theta_i\le b\}=1$. Then:

$$\forall\varepsilon>0\quad \mathbb{P}\left\{\left|\frac{1}{m}\sum_{i=1}^{m}\theta_i-\mu\right|>\varepsilon\right\}\le 2\exp\left(-2\frac{m\varepsilon^2}{(b-a)^2}\right)$$

Therefore, let us define $\theta_i=\ell(h,(\mathbf{x}_i,y_i))$. Observe that $L_{\mathcal{D}}(h)=\mathbb{E}[\theta_i]$, where the expectation is with respect to $\mathcal{D}$, and that $L_S(h)=\frac{1}{m}\sum_{i=1}^{m}\theta_i$. As such we get that

$$\begin{gathered}\mathcal{D}^m\left\{S\left|\,|L_S(h)-L_{\mathcal{D}}(h)|>\varepsilon\right.\right\}\le 2\exp\left(-2m\varepsilon^2\right)\\ \Downarrow\\ |\mathcal{H}|\cdot\max_{h\in\mathcal{H}}\mathcal{D}^m\left\{S\left|\,|L_S(h)-L_{\mathcal{D}}(h)|>\varepsilon\right.\right\}\le 2|\mathcal{H}|\exp\left(-2m\varepsilon^2\right)\end{gathered}$$

By choosing that $m\ge\frac{\log(2|\mathcal{H}|/\delta)}{2\varepsilon^2}$ we get that:

$$\mathcal{D}^m\left\{F_m^{\mathcal{D}}(S)>\varepsilon\right\}\le 2|\mathcal{H}|\exp\left(-2m\varepsilon^2\right)\le\delta$$

■

The Case Of Infinite $\mathcal{H}$

Unfortunately, we are not apply to apply the union bound over an inifinite number of hypotheses. Instead, recall that for every finite $C\subseteq\mathcal{X}$, we write $\mathcal{H}_C$ for the hypotheses in $\mathcal{H}$, all restricted to C. The key to the proof is to understand **how fast** can the restriction $\mathcal{H}_C$ grow with $|C|$. If $|C|\le VCdim(\mathcal{H})$ it could be that $\mathcal{H}$ shatters $|C|$ and therefore it could be that $|\mathcal{H}_C|=2^{|C|}$. However, if $|C|>VCdim(\mathcal{H})$ it can't be - by definition - that $|\mathcal{H}_C|=2^{|C|}$. So the question is how large can $|\mathcal{H}_C|$ be.

Definition 4.5.5 For a hypothesis class $\mathcal{H}$ Define $\tau\mathcal{H}(m)$ by

$$\tau_{\mathcal{H}}(m)=\max\left\{|\mathcal{H}_C|\,\middle|\,C\subset\mathcal{X},|C|=m\right\}$$

This definition is a combinatorial property of $\mathcal{H}$: the maximal number of functions that can be obtained by restricting $\mathcal{H}$ to any subset of size m. The larger and more complicated $\mathcal{H}$, the larger we can expect $\tau_{\mathcal{H}}(m)$ to be. In other words, $\tau_{\mathcal{H}}(m)$ measures how fast - at most - $\mathcal{H}_C$ can grow with $|C|$. For example, we saw that if $VCdim(\mathcal{H})=\infty$, then $\tau_{\mathcal{H}}(m)=2^m$, namely, $\mathcal{H}_C$ can grow exponentially in $|C|$.

Definition 4.5.6 Let $\mathcal{H}\subset\mathcal{Y}^{\mathcal{X}}$. Suppose there exist $m_0\in\mathbb{N}$, $b>0$ and $\beta>0$ such that: for all

$$\forall m>m_0\quad \tau_{\mathcal{H}}(m)\le b\cdot m^{\beta}$$

Then we say that $\mathcal{H}_C$ grows **polynomially** in $|C|$.

So the proof that a finite VC-dimension implies the uniform convergence is based on two parts:

1. If $|\mathcal{H}_C|$ grows polynomially in $|C|$, then $\mathcal{H}$ has the uniform convergence property. Hence it Agnostic-PAC learnable using the ERM rule.
2. If $VCdim(\mathcal{H})<\infty$, then $|\mathcal{H}_C|$ grows polynomially in $|C|$.

Claim 4.5.4 Let $\mathcal{H}$ be a hypothesis class such that $|\mathcal{H}_C|$ grows polynomially in $|C|$ then $\mathcal{H}$ has the uniform convergence property.

Proof. Recall that we would like to show that

$$\mathcal{D}^m\left(\left\{F_m^{\mathcal{D}}(S) > \varepsilon\right\}\right) < \delta$$

uniformly in $\mathcal{D}$. Since $F_m^{\mathcal{D}}$ is a non-negative random variable, we consider Markov's inequality. We would like to define a sequence of numbers α_m that will depend on $\mathcal{H}$ but *not* on the distribution $\mathcal{D}$, for which it holds that that

$$\mathbb{E}_{\mathcal{D}^m}\left[F_m^{\mathcal{D}}(S)\right] \leq \alpha_m \tag{4.4}$$

By doing so we will bound $\mathbb{E}_{\mathcal{D}^m}[F_m^{\mathcal{D}}(S)]$ uniformly across $\mathcal{D}$. If we are successful in doing so then

$$\mathbb{P}_{\mathcal{D}^m}\left\{\sup_{h\in\mathcal{H}}\left|L_{\mathcal{D}}(h) - L_S(h)\right| > \varepsilon\right\} = \mathbb{P}_{\mathcal{D}^m}\left\{F_m^{\mathcal{D}}(S) > \varepsilon\right\} \leq \frac{\mathbb{E}_{\mathcal{D}^m}[F_m^{\mathcal{D}}(S)]}{\varepsilon} \leq \frac{\alpha_m}{\varepsilon}.$$

Which means that with probability at least $1-\alpha_m/\varepsilon$, a training set of length m is ε-representative. Therefore, we managed to achieve uniformity across both $h \in \mathcal{H}$ (by using $F_m^{\mathcal{D}}$, a supremum over h) and over $\mathcal{D}$ (by bounding the expected value of $F_m^{\mathcal{D}}$ independently of $\mathcal{D}$).

Note, that is we are able to find such as sequence α_m that decreases to 0, then for any ε, δ we can set m_0 to be such that for all $m > m_0$, $\alpha_m/\varepsilon < \delta$. This would imply that $\mathcal{H}$ has the uniform convergence property. To find such a sequence α_m we use the following lemma

Lemma 4.5.5 Let $F_m^{\mathcal{D}}$ be as in (4.3). Then independently of $\mathcal{D}$

$$\mathbb{E}_{\mathcal{D}^m}\left[F_m^{\mathcal{D}}(S)\right] \leq \mathcal{O}\left(\frac{\sqrt{\log(\tau_{\mathcal{H}}(2m))}}{\sqrt{2m}}\right) + o(m)$$

Since we assumed that $|\mathcal{H}_C|$ grows polynomially in $|C|$, we have for all $m > m_0$ (for some m_0) that $\tau_{\mathcal{H}}(m) \leq b \cdot m^{\beta}$ for some $b, \beta > 0$. Hence,

$$\mathbb{E}_{\mathcal{D}^m}[F_m^{\mathcal{D}}(S)] \leq O\left(\frac{\sqrt{\beta \cdot \log(2m)}}{\sqrt{2m}}\right) + o(m) \searrow 0$$

and therefore if $|\mathcal{H}_C|$ grows polynomially in $|C|$ then $\mathcal{H}$ has the uniform convergence property. ■

Claim 4.5.6 Let $\mathcal{H}$ be a hypothesis class with a finite VC-dimension. Then $|\mathcal{H}_C|$ grows polynomially in $|C|$

Proof. By definition, if $m \leq VCdim(\mathcal{H})$ then there exists a set $C \subset \mathcal{X}$, of size m, which is shattered by $\mathcal{H}$. This means that if $m \leq VCdim(\mathcal{H})$ then $\tau_{\mathcal{H}}(m) = 2^m$. It can be shown, see Ex.7, that if $m > VCdim(\mathcal{H})$ then $\tau_{\mathcal{H}}(m) \leq (em/d)^d$. Therefore, while $\tau_{\mathcal{H}}(m)$ grows exponentially in m for $m \leq VCdim(\mathcal{H})$, it only grows **polynomially** in m for $m > VCdim(\mathcal{H})$. ■

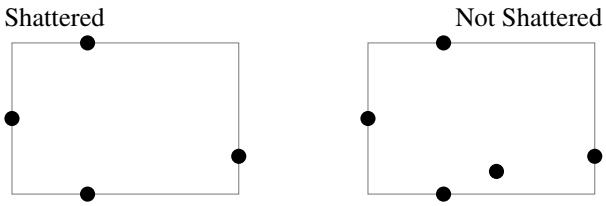
So, that was a taste of the proof of the second part of the fundamental theorem. We proved everything formally, except Lemma 2. This lemma is indeed deep and meaningful: it bounds the expected value of the "worse possible deviation" between empirical risk and generalization error, $\sup_{h\in\mathcal{H}}\left|L_{\mathcal{D}}(h) - L_S(h)\right|$, over a random choice of training sample, uniformly in $\mathcal{D}$. The bound uses $\tau_{\mathcal{H}}(m)$, which bounds how fast the size of a restriction $\mathcal{H}_C$ can grow with $|C|$.

4.6 Summary and Exercises

1. The ***Axis-aligned rectangles*** hypothesis class over the sample space $\mathcal{X} = \mathbb{R}^2$ is defined as:

$$\mathcal{H} = \left\{ h_{(a_1,a_2,b_1,b_2)} : a_1 < a_2 \wedge b_1 < b_2 \right\} \quad h_{(a_1,a_2,b_1,b_2)}(x_1,x_2) = \mathbb{1}_{x_1 \in [a_1,a_2] \wedge x_2 \in [b_1,b_2]}$$

   Note that every function in this hypothesis class defines a finite rectangle aligned with the x and y axes $\mathbb{R}^2$. Show that no set of 5 points can be shattered by the Axis-aligned rectangles class while any 4 points located on 4 different edges (away from the corners) of any given rectangle can:



   Hint: note that the 3 points (x_k, y_k), (x_i, y_i), and $(x_{k'}, y_{k'})$ can not be shattered if $x_k \leq x_i \leq x_{k'}$ and $y_k \leq y_i \leq y_{k'}$.
2. Consider the case of a finite hypothesis class.
   - Show that the VC dimension of a finite $\mathcal{H}$ is at most $\log_2(|\mathcal{H}|)$.
   - Show that, over the same sample space, $\mathcal{X}$, VC dimensions can take any value between 1 and $\log_2(|\mathcal{H}|)$ even for hypothesis classes of the same size: Given $n \in \mathbb{N}$, find a sample space, $\mathcal{X}$, and a hypothesis class, $\mathcal{H}^{(n)}$ with $VCdim(\mathcal{H}^{(n)}) = \log_2(|\mathcal{H}^{(n)}|) = n$. Then, for each $k = 1..n-1$ construct a hypothesis class, $\mathcal{H}^{(k)}$, with $|\mathcal{H}^{(k)}| = |\mathcal{H}^{(n)}|$ but with $VCdim(\mathcal{H}^{(k)}) = k$.
3. Let $\mathcal{X} = \mathbb{R}^d$. The ***hypothesis class*** of half-spaces through the origin is defined as

$$\mathcal{H} = \left\{ \mathbf{x} \mapsto sign(\mathbf{x}^\top \mathbf{w}) : \mathbf{w} \in \mathbb{R}^d \right\}$$

   - Show that $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ is shattered by $\mathcal{H}$.
   - Show that any $d+1$ points cannot be shattered (consider the standard basis vectors).
   - What is $VCdim(\mathcal{H})$?
4. Let $|\mathcal{X}| = \infty$. Let $\mathcal{H} \subset \{\pm 1\}^{\mathcal{X}}$ with VCdim($\mathcal{H}$)<∞. Let $\mathcal{H}'$ be the complement hypothesis class, namely, $\mathcal{H}' \equiv \{\pm 1\}^{\mathcal{X}} \setminus \mathcal{H}$. Let $C \subset \mathcal{X}$, $|C| < \infty$, be *any* finite subset of $\mathcal{X}$. Show that $\mathcal{H}'$ shatters C.
5. Let $\mathcal{X}$ be a sample space, $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$ a hypothesis class, and let ℓ_{0-1} be the $0-1$ loss function. Let $\varepsilon, \delta \in (0,1)$. Assume that $h \in \mathcal{H}$ is an Agnostic Probably Approximately correct learner with accuracy ε and confidence δ, with respect to ℓ_{0-1}, $\mathcal{H}$. Show that $\mathcal{A}$ is a Probably Approximately Correct learner (with accuracy ε and confidence δ).
6. Prove Lemma 4.5.2: for S an $\varepsilon/2$-representative sample for $\mathcal{D}, \mathcal{H}, \ell$ any ERM ourput h_S satisfies that

$$L_{\mathcal{D}}(h_S) \leq \min_{h \in \mathcal{H}} L_{\mathcal{D}}(h) + \varepsilon$$

7. Let $\mathcal{H}$ be some hypothesis class of functions $\mathcal{X} \to \{\pm 1\}$ with finite VC-dimension. If $m > VCdim(\mathcal{H})$ then $\tau_{\mathcal{H}}(m) \leq (em/d)^d$.
8. Let $\tilde{\mathcal{D}}$ be a distribution on $\mathcal{X}$ alone, and let $f : \mathcal{X} \to \mathcal{Y}$ be a labeling function, $\mathcal{Y} = \{\pm 1\}$. Construct an equivalent joint distribution $\mathcal{D}(\mathbf{x}, y)$ on $\mathcal{X} \times \mathcal{Y}$, assuming no-noise. Verify the answer by calculating the distribution for the pair $(\mathbf{x}, f(\mathbf{x}))$ and for the pair $(\mathbf{x}, -f(\mathbf{x}))$.
9. Consider again $\tilde{\mathcal{D}}(\mathbf{x})$ and $\mathcal{D}(\mathbf{x}, y)$ defined in Ex.8. Verify that Equation 4.1 gives, for $\tilde{\mathcal{D}}(\mathbf{x})$, the same misclassification loss as Equation 4.2 gives, for $\mathcal{D}(\mathbf{x}, y)$.

5. Ensemble Methods

In previous chapters we discussed different classification algorithms, each of which implements a different learning principle for choosing the learning rule $h_s \in \mathcal{H}$. In this chapter we will not cover new learning algorithms per se, but rather consider several general "meta-algorithms" for the creation of *ensembles* of classifiers. These collection of classifier can be applied to any existing learning algorithm and improve its performance. We will learn about the three B's: *Bootstrapping*, *Bagging* and *Boosting* and understand how they give us better control over the *Bias-Variance Trade-off*. These powerful techniques are broadly used and applicable for many difficult problems even outside the context of the meta-algorithms presented in this chapter

5.1 Bias-Variance Trade-off

Throughout the book we have stated informally that the "larger" or "more complicated" our chosen hypothesis class, typically our learner will have lower **bias** and higher **variance**. We said informally that bias is part of the generalization error that is incurred by the "best" hypothesis in $\mathcal{H}$. If we think of an unknown labeling function f chosen by nature, then bias measures how well the unknown labeling function f can be decried by the "closest" hypothesis in $\mathcal{H}$. Intuitively, the larger $\mathcal{H}$, the more expressive power it has to describe more complicated functions f - hence a lower bias. We also said informally that variance is the part of the generalization error that is incurred by the fact that the training sample is random, hence our chosen rule h_s is also random. The larger $\mathcal{H}$ will be, the more freedom our learning algorithm has to "chase" random fluctuations in the training sample, which do not represent the underlying labeling we are trying to learn.

R The variance part can be further broken down into two parts - one part comes from randomness in the choice of training samples while another part comes from the measurement noise or noise in the labels. For simplicity we will represent the variance as a single component.

As such, the bias-variance **tradeoff** is that: the more complicated the model, the smaller the bias and the larger the variance. Informally, the generalization error is some combination of the two. In cases where we can

tune the model complexity (that is, the size/complexity of the hypothesis class) we would like to look for the "sweet spot" of a model that has "just the right amount of complexity".

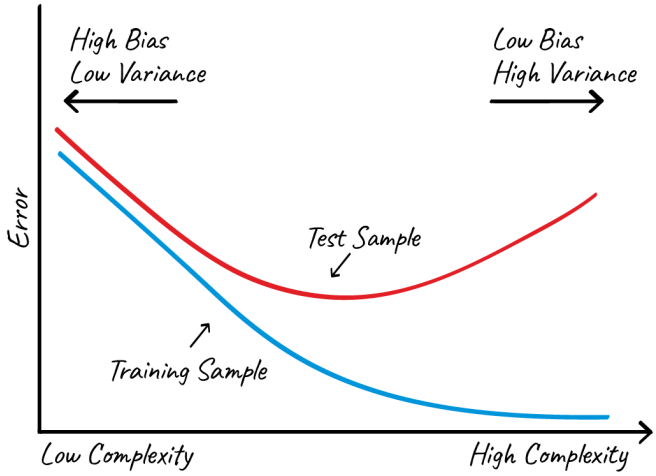


Figure 5.1: The bias-variance tradeoff: *Train- vs. test errors as function of complexity of h*

The methods describe below allow us to escape the tradeoff in some sense. They enable the reduction of the bias or variance of a learner without substantially increasing the other.

5.1.1 Generalization Error Decomposition

We have already encountered the generalization error decomposition when discussing linear regression problems. There we have shown how we can decompose the MSE into the bias and variance components (2.23). Next, let us revisit the decomposition but for some general loss function. Let $h^* = \text{argmin}_{h \in \mathcal{H}} L_{\mathcal{D}}(h)$ and $h_S = \mathcal{A}(S)$ be the output of a learning algorithm, then we can decompose the generalization error of the hypothesis returned by the learner as follows:

$$L_{\mathcal{D}}(h_S) = \underbrace{L_{\mathcal{D}}(h^*)}_{\varepsilon_{approximation}} + \underbrace{L_{\mathcal{D}}(h_S) - L_{\mathcal{D}}(h^*)}_{\varepsilon_{estimation}} \tag{5.1}$$

- The **approximation error** is $L_{\mathcal{D}}(h^*)$. Namely, the error of the hypothesis $h \in \mathcal{H}$ achieving the lowest generalization error. This term does not depend at all on our training sample and its size m. It depends only on the selection of $\mathcal{H}$. As we expand the hypothesis class to become richer we might find a better hypothesis for explaining the data. This error is what we already know as the **bias** error, induced by restricting the hypothesis class.
- The **estimation error** is $L_{\mathcal{D}}(h_S) - L_{\mathcal{D}}(h^*)$. Namely, it is the difference between the generalization error achieved by the selected hypothesis and the best hypothesis in $\mathcal{H}$. This term depends on the training set and its size. This error is what we already know as the **variance** error.

5.2 Ensemble/Committee Methods

> "A collective wisdom of many is likely more accurate than any one." — Aristotle, in *Politics*, circa 300BC

Before exploring specific ensemble methods, let us analyze some mathematical properties of a committee based decision. This will provide insights into how committee based methods manage to improve generalization. Consider a committee of T members, which has to make a "yes"/"no" decision. Each member casts a

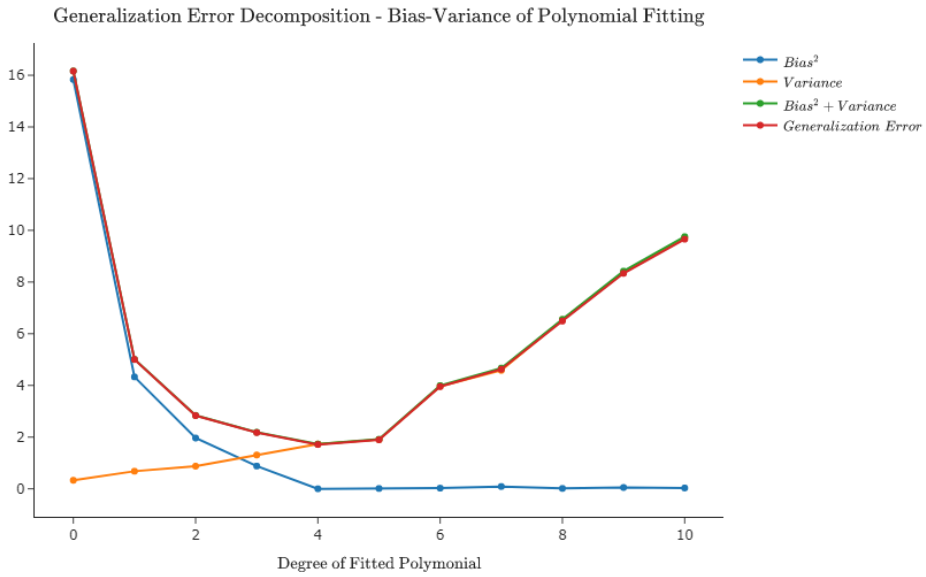


Figure 5.2: Bias-Variance Tradeoff Graph: *for polynomial fitting of true polynomial degree* 4. *Chapter 5 Examples - Source Code*

vote, which with probability p_i being correct and probability $1-p_i$ being wrong. Let us further assume for simplicity that all members are "equally wise", so that p is the same for all members. After all members vote, the committee's decision is simply the majority vote. For this setup we can ask questions such as:

- What is the probability of the committee deciding the right decision?
- What would a typical decision be? and how consistent is it?
- How does the number of members in the committee influence the measures above?
- If committee members are not independent from one another, and influence each other's decisions, how does it influence the measures above?

We begin answering these questions theoretically starting with the probability of a committee deciding the right decision.

Lemma 5.2.1 Let $X_1,\ldots,X_T \overset{i.i.d}{\sim} Ber(p)$ taking values in $\{\pm 1\}$ and denote $X=\sum X_i$. The probability of the committee making the correct decision is $\mathbb{P}(X>0)$.

Proof. As the committee decides by a majority vote then the probability of the committee deciding right is the same as the probability of having more members deciding right than members deciding wrong:

$$\mathbb{P}(\text{Committee decides right}) = \mathbb{P}(|\text{Decided right}| > |\text{Decided wrong}|)$$

W.o.l.g, suppose the true answer is $+1$. As each random variable takes a value in $\{\pm\}$ we could express the collective vote as $X = sign(\sum X_i)$. If the committee decided right, then there are more members that voted right and $\sum X_i > 0$ which means that $X=1$. On the other hand, if the committee decided wrong, then more members voted wrong and $\sum X_i <= 0$ which means that $X=-1$. So, we conclude that:

$$\mathbb{P}(\text{Committee decides right}) = \mathbb{P}(X>0)$$

■

Lemma 5.2.2 Let $X_1,\ldots,X_T \overset{i.i.d}{\sim} Ber(p)$ taking values in $\{\pm 1\}$ with $p > 0.5$ and denote $X = \sum X_i$. The probability of the committee deciding correctly is bounded below by $1-\exp\left(-\frac{T}{2p}\left(p-\frac{1}{2}\right)^2\right)$.

Proof. W.l.o.g let us assume that the correct answer is $+1$ and denote $X = \sum_{i=1}^{T} X_i$. We are therefore interested in bounding $\mathbb{P}(X > 0)$ from below. We will achieve this by bounding $\mathbb{P}(X \leq 0)$ from above. Notice that for any $a > 0$ it holds that:

$$\mathbb{P}(X \leq 0) = \mathbb{P}(-aX \geq 0) = \mathbb{P}\left(e^{-aX} \geq e^0\right)$$

Now, using Markov's inequality

$$\mathbb{P}(X \leq 0) \leq \mathbb{E}\left[e^{-aX}\right] = \mathbb{E}\left[e^{-a\sum_i X_i}\right] \overset{iid}{=} \mathbb{E}\left[e^{-aX_1}\right]^T$$

Notice that as $X_1 \sim Ber(p)$ over $\{\pm 1\}$ it holds that:

$$\mathbb{E}\left[e^{-aX_1}\right] = pe^{-a} + (1-p)e^{a} = e^{a}\left(1-p+pe^{-2a}\right) \leq e^{a-p+pe^{-2a}}$$

where the last inequality is because $1+x \leq e^x$. Next, we use the inequality $x\ln(x) \geq \frac{x^2}{2} - \frac{1}{2} \quad x \in (0,1)$. For a selection of $a = \frac{1}{2}ln(2p)$ which is positive for $p > 0.5$ we get that:

$$\begin{array}{rcllcl}
\mathbb{P}(X \leq 0) & \leq & \mathbb{E}\left[e^{-aX_1}\right]^T & & \leq & \exp\left(T\left(a-p+pe^{-2a}\right)\right) \\
& = & \exp\left(T\left(\frac{1}{2}ln(2p)-p+\frac{1}{2}\right)\right) & & = & \exp\left(Tp\left(-\frac{1}{2p}ln\left(\frac{1}{2p}\right)-1+\frac{1}{2p}\right)\right) \\
& \leq & \exp\left(Tp\left(\frac{1}{2}-\frac{1}{2(2p)^2}-1+\frac{1}{2p}\right)\right) & & = & \exp\left(-\frac{Tp}{2}\left(\frac{1}{4p^2}-\frac{1}{p}+1\right)\right) \\
& = & \exp\left(-\frac{Tp}{2}\left(\frac{1}{2p}-1\right)^2\right) & & = & \exp\left(-\frac{T}{2p}\left(p-\frac{1}{2}\right)^2\right)
\end{array}$$

Finally, we conclude that:

$$\mathbb{P}(X > 0) = 1 - \mathbb{P}(X \leq 0) \geq 1 - \exp\left(-\frac{T}{2p}\left(p-\frac{1}{2}\right)^2\right)$$

■

Therefore, it turns out that if each member is typically right ($p > 0.5$) then the probability that the committee is right is higher than any individual member. In addition, the probability of the committee being wrong decays with a rate of $\mathcal{O}\left(e^{-T}\right)$. Relating this to our learning scheme, it means that the confidence $1-\delta$ in our prediction increases exponentially as T increases.

Based on (5.2.1) and (5.2.2) we can now simulate different scenarios for different values of T and p and see how committees behave. Figure 5.3 shows the theoretical bound achieved above and the empirical results for committees if increasing size and for different values of p. We can see that:

- The larger the committee size T the higher the probability of the committee being correct.
- The larger the probability of each committee member of being correct p, the fewer committee members are needed for the committee to be correct with probability of 1.

We also see that empirical results agree with the theoretical lower bound devised above.

5.2.1 Uncorrelated Predictors

Next, let us calculate what is a typical decision ($\mathbb{E}(X)$) and how consistent is it ($Var(X)$)? Let $X_1,\ldots,X_T \overset{iid}{\sim} Ber(p)$ taking values of $\{\pm 1\}$ with $p > 0.5$. What is the expectation and variance of $X = \frac{1}{T}\sum_{i=1}^{T} X_i$?

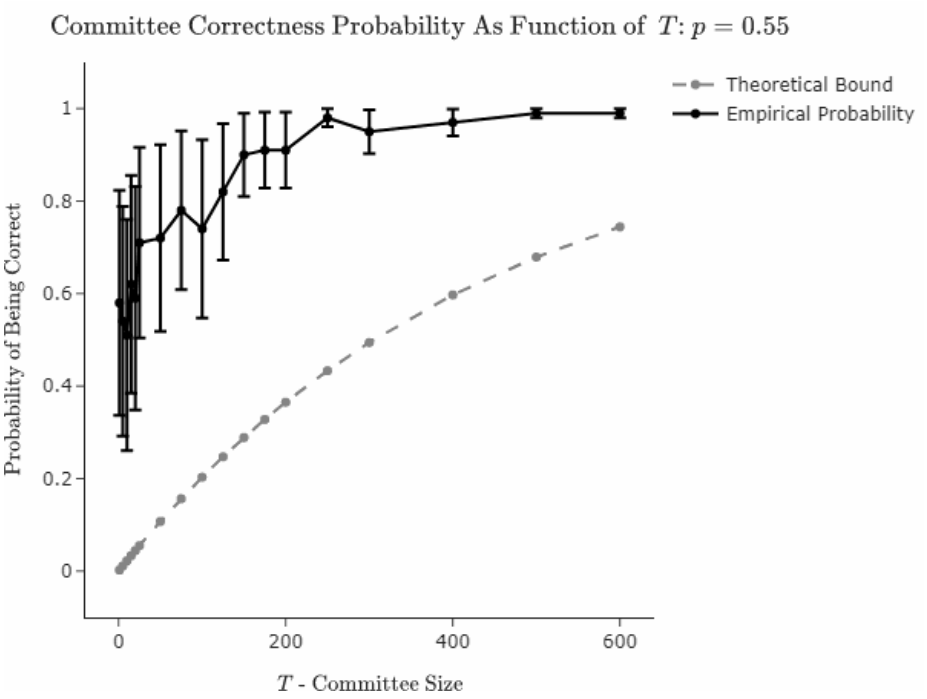


Figure 5.3: Committee Decision - Correctness Probability: *Theoretical bounds and empirical results as function of T, p.* *Chapter 5 Examples - Source Code*

We begin with calculating the expectation and variance of each committee member:

$$\begin{aligned}\mathbb{E}[X_i] &= 1\cdot\mathbb{P}(X_i=1)+(-1)\cdot\mathbb{P}(X_i=-1)\\ &= 2p-1\end{aligned}$$

$$\begin{aligned}Var(X_i) &= \mathbb{E}\left[(X_i-\mathbb{E}[X_i])^2\right]\\ &= p(1-(2p-1))^2+(1-p)(-1-(2p-1))^2\\ &= 4p(1-p)^2+4p^2(1-p)\\ &= 4p(1-p)\end{aligned}$$

Then, for X:

$$\begin{aligned}\mathbb{E}[X] &= \tfrac{1}{T}\textstyle\sum_i \mathbb{E}[X_i] = 2p-1\\ Var(X) &= \tfrac{1}{T^2}Var\left(\textstyle\sum_i X_i\right) \overset{iid}{=} \tfrac{1}{T^2}\textstyle\sum_i Var(X_i) = \tfrac{4}{T}p(1-p)\end{aligned}$$

Therefore, when using a committee of independent members the expectation of decision remains the same while decreasing the variance at a rate of $\mathcal{O}\left(\frac{1}{T}\right)$. In other word, we are able to keep the same accuracy while increasing the confidence.

5.2.2 Correlated Predictors

In practice, however, committee members rarely vote independently. So let us assume that each two members are correlated with equal correlation $\rho \in [0,1]$.

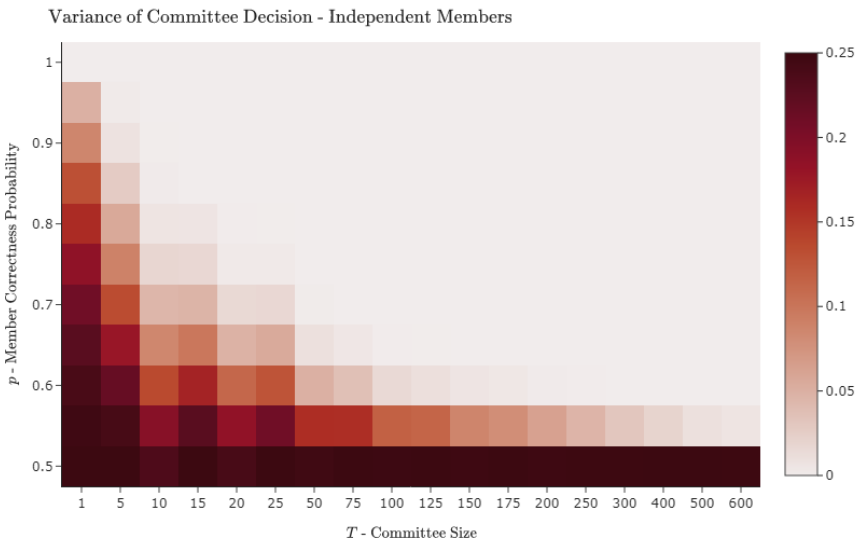


Figure 5.4: Variance of Committee Decision: *with independent members, as function of T, p.*
Chapter 5 Examples - Source Code

Lemma 5.2.3 Let $X_1, \ldots, X_T$ be a set of identically-distributed real-valued random variables such that: $Var(X_i) = \sigma^2$ and $corr(X_i, X_j) = \rho$, $i \neq j$. The variance in the commitee's decision is given by $\rho\sigma^2 + \frac{1}{T}(1-\rho)\sigma^2$.

Proof. As X is the average of T identically distributed random variables:

$$Var(X) = Var\left(\frac{1}{T}\sum_i X_i\right) = \frac{1}{T^2}\left[\sum_i Var(X_i) + 2\sum_{i<j} Cov(X_i, X_j)\right]$$

Recall that the correlation between two random variables is defined as:

$$corr(A,B) := \frac{Cov(A,B)}{\sqrt{Var(A)\,Var(B)}}$$

and therefore for any $i \neq j$:

$$Cov(X_i, X_j) = corr(X_i, X_j)\sqrt{Var(X_i)\,Var(X_j)} = \rho\sigma^2$$

Plugging this back into the variance:

$$Var(X) = \frac{1}{T^2}\left[T\sigma^2 + 2\binom{T}{2}\rho\sigma^2\right] = \frac{\sigma^2}{T} + \left(1 - \frac{1}{T}\right)\rho\sigma^2 = \rho\sigma^2 + \frac{1}{T}(1-\rho)\sigma^2$$

■

All together, we have seen analytically and quantitatively that given a committee of members deciding by majority vote, where decisions of members are correlated with correlation ρ and each member is correct with probability p:

- If $p > 0.5$ the decision made by the committee improves with T in two ways: higher probability of being right, and its decision will be more consistent.
- If $\rho > 0$ then increasing T will increase the probability of the decision made by the committee being right up to a certain point.

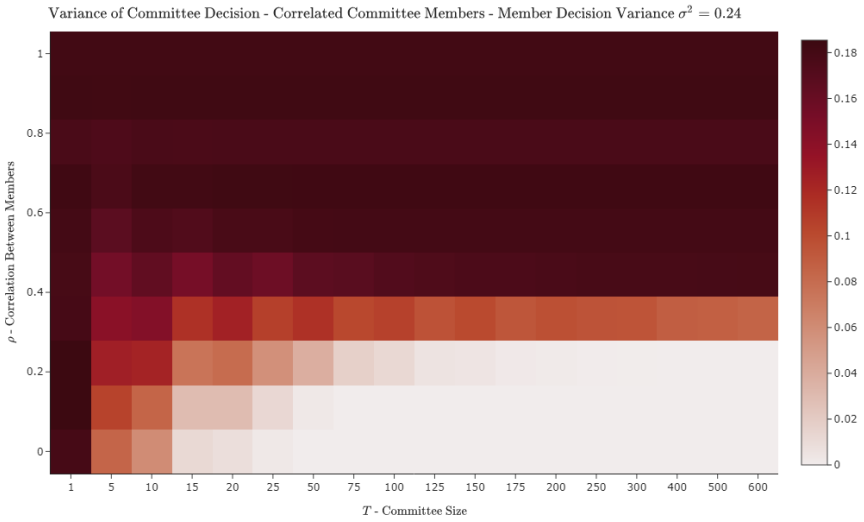


Figure 5.5: Variance of Committee Decision: *with correlated members, as function of* T, ρ. *Chapter 5 Examples - Source Code*

5.2.3 Committee Methods In Machine Learning

Let us apply these ideas to machine learning applications. Suppose we have T training samples $S_1, \ldots, S_T$ of size m chosen independently from $\mathcal{X}$ according to some distribution $\mathcal{D}$. Let $\mathcal{A}$ be a learning algorithm and train it on each of the training samples, to obtain $h_{S_1}, \ldots, h_{S_T}$. Let us consider $h_{S_t}(x)$ for some $x \in \mathcal{X}$. As $S_t \overset{i.i.d}{\sim} \mathcal{D}^m$ we can think of the training set as a random variable. This means that the also h_{S_t} obtained by training $\mathcal{A}$ over S_t is a random variable. Lastly, it means that we can think of the prediction $h_{S_t}(x)$ as a random variable, which has some distribution. In addition, notice that as the training samples are chosen independently, predictions of different h_{S_t} over x are also independent random variables. So, if we use $h_{S_1}, \ldots, h_{S_T}$ in a committee we have the situation described above. The generalization loss will be reduced as T grows as the variance of the prediction will decrease as a rate of $1/T$.

However, in batch learning we don't have T training samples, but rather just one, so how would we accuire such different hypotheses? We cannot train $\mathcal{A}$ over S multiple times as we will get identical predictions, which are perfectly correlated. Instead, what we would like to do is to create T training samples from the original one. If we could mimic fresh independent draws of new traning samples of size m according to $\mathcal{D}$.

Definition 5.2.1 — Committee Methods. Let $\mathcal{A}$ be some learner predicting labels in $\{\pm 1\}$. A committee method over $\mathcal{A}$ is the function:

$$h(x) = sign\left(\sum_{t=1}^{T} h_t(x)\right)$$

That is, in committee methods (or ensembles) we take an existing "base" learner and apply it ot a sequence of T training samples. For the remaining of this chapter we will introduce two very different ideas for building the committee member rules.

5.3 Bagging

5.3.1 The Bootstrap

For the first committee method we begin with introducing a concept from statistics: *The Bootstrap*. This is one of the most groundbreaking ideas of statistics in the 20th century, where we create new "artificial" training samples from the one training sample at hand.

Given a training sample $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$ we are going to construct a new training sample, called a *bootstrap sample* S^{*1}. We sample m times from S *with replacement* and denote this "new" sample by:

$$S^{*1} = \left\{\left(\mathbf{x}_i^{*1}, y_i^{*1}\right)\right\}_{i=1}^m$$

Of course, since we sampled from S with replacements, there might be repeated samples in S^{*1}, even if S itself had no repeated samples. Now we can repeat this process B times, obtaining B training samples, each of length m: $S^{*1}, \ldots, S^{*B}$. The samples in the b-th training sample will be denoted

$$S^{*b} = \left\{\left(\mathbf{x}_i^{*b}, y_i^{*b}\right)\right\}_{i=1}^m$$

Using the newly created bootstrap samples we can now train our base learner $\mathcal{A}$ over each one separately, obtain B prediction rules and form an ensemble. But so how is it that bootstrap actually works? Assume the samples in our learning problem are *i.i.d* samples from an unknown distribution $\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$. We are hoping that each Bootstrap from S somehow behaves like a fresh *i.i.d* sample from $\mathcal{D}$ itself. Given a training sample S we can define the *empirical distribution* $\widehat{\mathcal{D}}_S$ induced by S on $\mathcal{X} \times \mathcal{Y}$ as the following probability distribution on $\mathcal{X} \times \mathcal{Y}$: for a subset $C \subset \mathcal{X} \times \mathcal{Y}$, define:

$$\widehat{\mathcal{D}}_S\left((X,Y) = (x,y)\right) := \begin{cases} \frac{1}{m} & (x,y) \in S \\ 0 & (x,y) \notin S \end{cases}$$

or equivalently, for any $C \subset \mathcal{X} \times \mathcal{Y}$:

$$\widehat{\mathcal{D}}_S(C) := \frac{|C \cap S|}{m}$$

where for simplicity we assume all samples in S are unique. Observe that this is equivalent to putting a probability mass of $1/m$ on each of the points of S, and zero mass on all other points in $\mathcal{X} \times \mathcal{Y}$. Observe that a bootstrap sample S^{*b} is just an *i.i.d* draw of m points from the *empirical distribution* $\widehat{\mathcal{D}}_S$ induced by the one training sample we have, S. As m grows, namely as S becomes larger, the empirical distribution $\widehat{\mathcal{D}}_S$ converges in distribution to $\mathcal{D}$. The idea behind the bootstrap is that, if $\widehat{\mathcal{D}}_S$ is not so different from $\mathcal{D}$, then m *i.i.d* draws from $\widehat{\mathcal{D}}_S$ is a good approximation to m *i.i.d* draws from $\mathcal{D}$.

One way to see the convergence of the empirical distribution to the underlying distribution is on the real line. Figure 5.6 shows the empirical CDF of samples drawn from a standard normal distribution and compares it with the theoretical CDF of the distribution. As the number of samples increases the empirical CDF converges to the CDF of the standard distribution.

5.3.2 Bagging

The idea of Bootstrap samples can be used in any scenario where we wish to create new artificial samples from our only training sample S. It has many uses throughout machine learning, statistics and data science. **Bagging** is a nickname of one such usage where we use Boostrap, to improve the accuracy of an existing supervised machine learning algorithm.

We start with a "base" learning algorithm $\mathcal{A}$ and a training sample S. We then form T bootstrap training samples, $S^{*1}, \ldots, S^{*T}$, each of size m. We then train our learner *separately* on each of the T bootstrap training

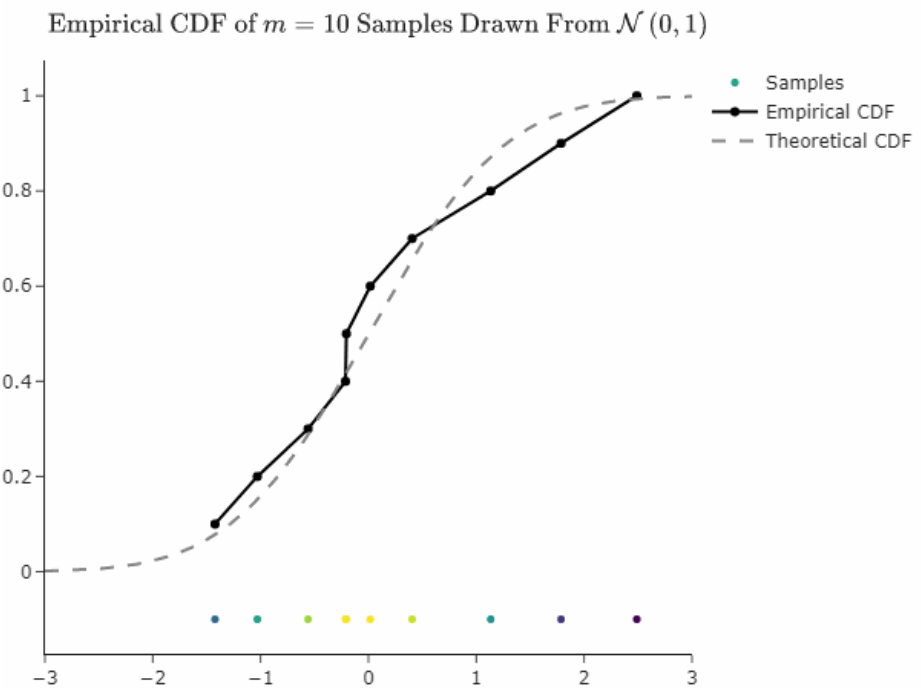


Figure 5.6: Empirical CDF: *of i.i.d samples drawn from a standard normal distribution. Chapter 5 Examples - Source Code*

samples. We form the committee $h_{S^*1}, \ldots, h_{S^*T}$ and store all T trained models. When we need to classify a new test sample $x \in \mathcal{X}$, we run x through all the rules and classify using the majority vote of the committee,

$$h_{bag}(x) \coloneqq sign\left(\sum h_{S^*t}(x)\right)$$

For example, if we run Bagging on top of the Decision Tree classifier, we'll obtain a committee of decision trees:

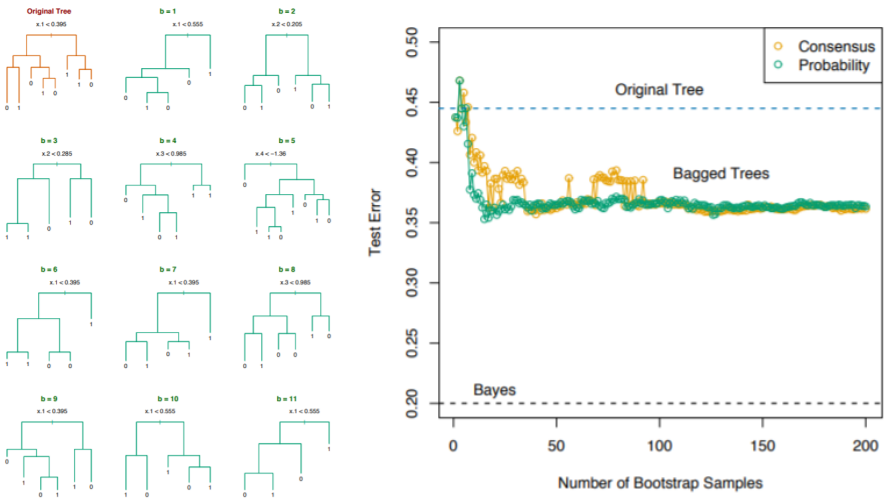


Figure 5.7: *Collection of Bagged Decision Trees. (Source: ESL)*

Note that our learner $\mathcal{A}$ must know how to handle repeated samples. We may have them anyway in S, but running on a bootstrap sample we are sure to have them. Some learning algorithms suffer when there are repeated samples - as they cause numerical problems (for example, linear and logistic regression), while for others it isn't a problem (for example, decision trees and k-NN).

5.3.3 Bagging Reduces Variance

We saw that a committee majority vote reduces variance, but as seen in Figure 5.6 only to a certain degree. The amount of variance reduced is determined by the correlation between committee members. Therefore we can expect bagging to reduce variance as T increases, which will reduce the generalization error, but only proportionate to the correlation between the bagged prediction rules.

5.3.4 Random Forests - Bagging and De-correlating Decision Trees

As such we would like to find a way to de-correlate the committee members - namely, cause their predictions to somehow be less correlated. One way to do so is by slightly restricting each learner, in a random way, and hope that the performance gain (in bagging them) due to de-correlation is more than the performance loss to each learner by the restrictions. The most well know example of this principle is *Random Forests*.

Recall the Decision Tree classification algorithm over $\mathcal{X} = \mathbb{R}^d$. We have a training sample S with m points. The Random Forest classifier is obtained by using Bagging on top of the Decision Tree algorithm, *with the important step* that drives the de-correlation: the algorithm has a tuning parameter $k \leq d$. When growing each decision tree, in each split, we choose uniformly at random a subset of k out of the d features. We choose the split only among these k features. Formally:

Algorithm 5 Random Forests

procedure RANDOM-FOREST(training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, maximal tree depth $R \in \mathbb{N}$, minimal training samples in any leaf m_{min}, number of trees T, number of coordinates to choose from in each split k)
  for $t = 1, \ldots, T$ **do**
    Draw a Bootstrap sample S^{*t} from S
    Train a decision tree $h_{S^{*t}}$ on the sample S^{*t} where at each split
    if Not reached maximal depth R or minimal number of samples m_{min} **then**
      Select uniformly at random k features from $[d]$
      Choose the best feature to split by from the st of k features
      Split based on selected feature and threshold
    end if
  end for
  return $h_S(\mathbf{x}) = sign\left(\sum_{i=1}^T w_t h_t(\mathbf{x})\right)$
end procedure

This de-correlation trick works: pretty much on every classification problem you will work on, you will observe something like the next plot: Bagging trees is much better than a single tree, and Random Forest (Bagging with the de-correlation trick) is better than just Bagging trees.

Bagging - Discussion Points

- **Can Bagging harm our prediction?** Always remember that a committee of fools (a committee where each member has probability $p < 0.5$ to make the right decision) makes worse decisions than a single member. So, when our base learner is so poor that its generalization loss is less than 0.5 we shouldn't use Bagging.

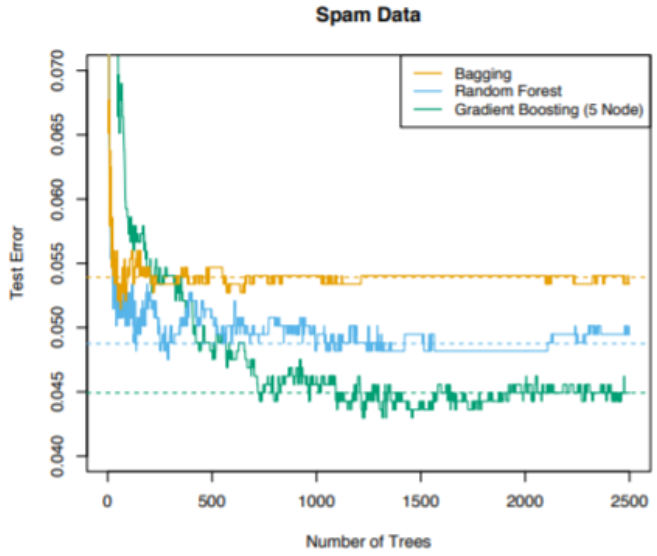


Figure 5.8: *Test error of simple Bagging of decision trees (no de-correlation), Random Forests, and Gradient Boosting of Trees. (Source: ESL)*

- **What are the disadvantages of Bagging?** As we train not one but T models we need to train all T of them. This directly increases time complexity by a factor proportionate to T. In addition, for predictions, as we need all T models we must store all T of them. Lastly, we loose interpretability as it is much harder to understand why the committee made the decision. We need to understand the decision of each of the T members.
- **Parallelizem** From the computational perspective, it is important to note that Bagging in general (and Random Forests in particular) is *embarrassingly parallelizable*. When training a Bagging model with T committee members, we can use T machines in parallel, each using its own random seed to select Bootstrap samples (and random splits, in Random Forest). The machines do not need to interact; when each machine is done, it returns the committee member h_t to the master node.
- **Predicted Class Probabilities:** Can we use the *proportion* of the committee members who voted $+1$ as a predicted class probability? Estimated class probabilities are estimates of $\mathbb{P}\{Y = +1, | X = x\}$. The proportion of members who voted $+1$ estimates $\mathbb{P}\{h_S(x) = +1\}$, which is a different quantity.

5.4 Boosting

Bootstrap and Bagging produce an ensemble of classifiers each trained over a "new" artificial training sample generated from the original one. Boosting on the other hand utilizes the single training sample and produces different classifiers by assuming different distribution over these samples. In Boosting we take a "weak" learning algorithm, an algorithm with better-than-random but possibly not so good accuracy (i.e. generalization error) and *boost* it using a clever committee method to obtain a learning algorithm with good accuracy.

In Bagging, we *pretended* to have fresh training samples $S_1, \ldots, S_T$, and each committee member trained on a different sample. In Boosting on the other hand, we go even further and *pretend* to have *different underlying distributions* $\mathcal{D}$ from which the training sample is drawn. More specifically, in Boosting each committee member h_t is the result of running $\mathcal{A}$ against a training sample S_t that mimics an $i.i.d$ sample of size m from a *different distribution* $\mathcal{D}^t$. Whereas in Bagging each committee member is trained independently of all other members, in Boosting the committee members are trained sequentially, one after the other, and each is an improvement, in some sense, on the previous one.

The clever idea behind Boosting is that after we finish training h_t, based on the distribution $\mathcal{D}^t$, we update the distribution in a way that increases the measure of samples where h_t was wrong. This way, we force h_{t+1} to try do better on those particular samples.

What is meant by "running $\mathcal{A}$ against the training sample S with distribution $\mathcal{D}^t$"? One way to interpret this is to take a *weighted Bootstrap* sample from S, where the probability of selecting $(x,y) \in S$ is proportional to $\mathcal{D}^t(x,y)$. A simpler way to interpret this is as follows. If $\mathcal{A}$ uses the ERM principle, say for standard misclassification ($0-1$ loss), namely, looking to minimize the empirical risk,

$$L_S(h) = \sum_{i=1}^{m} \mathbb{1}_{y_i \neq h(\mathbf{x}_i)}$$

then we can use S itself and have the base learner minimize the *weighted* empirical risk

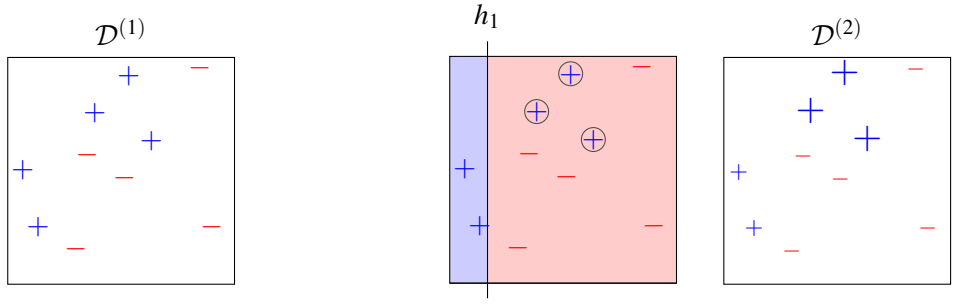
$$L_{S,\mathcal{D}^t}(h) = \sum_{i=1}^{m} \mathcal{D}_i^t \mathbb{1}_{y_i \neq h(\mathbf{x}_i)}$$

where for each $(\mathbf{x}_i, y_i) \in S$ we write $\mathcal{D}_i^t := \mathcal{D}^t(\mathbf{x}_i, y_i)$, so that $\sum_{i=1}^m \mathcal{D}_i^t = 1$.

Observe that these two interpretations are equivalent in expectation. Indeed, the expected number of times for a sample $(\mathbf{x}_i, y_i)$ to appear in the weighted Bootstrap sample is $\mathcal{D}_i^t$, and so it would (in expectation) appear $\mathcal{D}_i^t$ times in the empirical risk sum.

R Note that we usually prefer second option (using weighted empirical risk) to the first option (using weighted bootstrap). It's more computationally efficient, and does not require worrying about repeated samples. However, the first option (using weighted bootstrap) is always available. The second option (using weighted empirical risk) is not always possible, and is implemented ad-hoc for the particular base learner we are boosting.

To understand this idea consider the following scenario. Suppose we begin with a training sample S of five positive and five negative samples as seen in Figure 5.9. At first we define a uniform distribution over the samples. Then suppose we fit a threshold classifier over S and $\mathcal{D}^{(1)}$ producing h_1. Notice that h_1 misclassified 3 samples. As such we update the distribution of weights over the samples increasing the weights of the misclassified samples and decreaseing the weights of the correctly classified samples, forming $\mathcal{D}^{(2)}$.

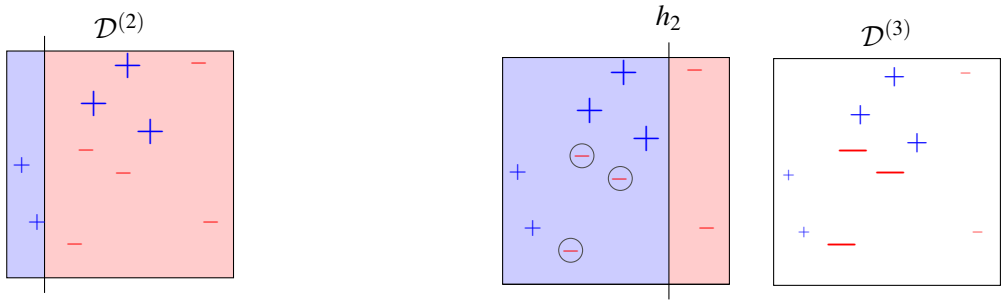


(a) *Initial uniform distribution over training sample*

(b) *Fitting h_1 over $\mathcal{D}^{(1)}$ and producing $\mathcal{D}^{(2)}$*

Figure 5.9: Boosting illustration: *Initial sample distribution and first iteration*

Next, we use $\mathcal{D}^{(2)}$ as the assumed sample distribution over S. By fitting a new threshold function, this time using $\mathcal{D}^{(2)}$ over S and minimizing the weighted misclassification error, we produce h_2. Similar to before based on the results of h_2 we form $\mathcal{D}^{(3)}$ where we increase the weights of the misclassified samples and decrease the weights of the correctly classified samples. This operation is done with respect to $\mathcal{D}^{(2)}$ (and not $\mathcal{D}^{(1)}$) as this is the distribution over which h_2 was produced. Notice that samples where both h_1 and h_2 have correctly classified are now with very low weights in $\mathcal{D}^{(3)}$.

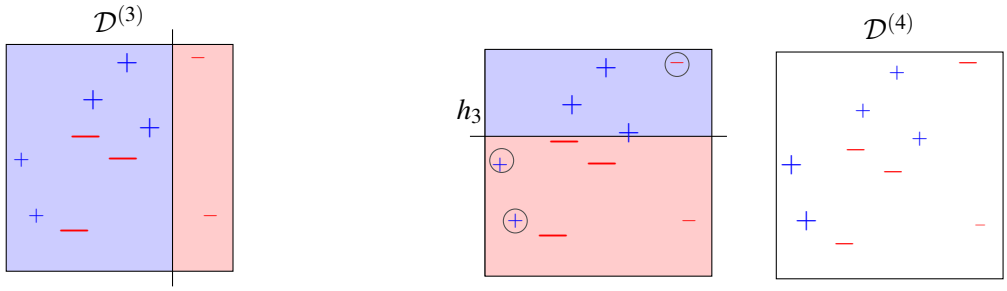


(a) *Current distribution over training sample*

(b) *Fitting h_2 over $\mathcal{D}^{(2)}$ and producing $\mathcal{D}^{(3)}$*

Figure 5.10: Boosting illustration: *second iteration over results of first iteration*

Performing a third iteration the learner this time outputs h_3 which is able to correctly classify the samples misclassified in the previous iteration. Then we update the sample weights distribution based on the classification of h_3. Focusing for example on the bottom left negative sample, notice that all three learners have correctly classified this sample. Therefore, its weight under $\mathcal{D}^{(4)}$ is very low.



(a) *Current distribution over training sample*

(b) *Fitting h_3 over $\mathcal{D}^{(3)}$ and producing $\mathcal{D}^{(4)}$*

Figure 5.11: Boosting illustration: *third iteration over results of second iteration*

Then, if we used the three classifiers produced above h_1, h_2, h_3 and predict based on all of them we achieve a classifier with decision boundaries as in Figure **??**. Even though each single classifier has a simple decision boundary of a threshold function, the ensemble is able to describe much more complex data scenarios. Classifying based on all three classifiers is done by

$$h_{boost}(\mathbf{x}) := sign\left(\sum w_i h_i(\mathbf{x})\right)$$

where w_i are weights given to each classifier and reflect how successful that classifier is.

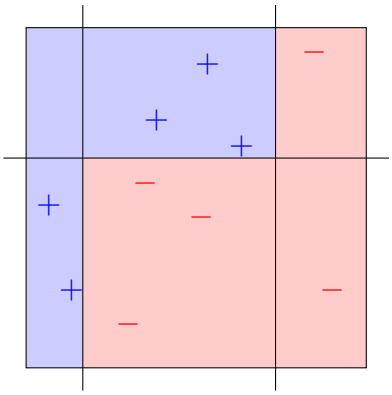


Figure 5.12: Boosting illustraion: *Decision boundaries of the ensemble of classifiers* h_1, h_2, h_3.

5.4.1 AdaBoost Algorithm

The original boosting meta-algorithm is known as **Ada**ptive **Boost**ing. The illustration above follows the operations done by the AdaBoost algorithm.

Algorithm 6 Adaptive **Boost**ing

procedure ADABOOST(training set $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^m$, base learner $\mathcal{A}$, number of rounds T)
  Set initial distribution to be uniform: $\mathcal{D}^{(1)} \leftarrow \left(\frac{1}{m}, \ldots, \frac{1}{m}\right)$ ▷ Initialize parameters
  for $t = 1, \ldots, T$ **do**
    Invoke base learner $h_t = \mathcal{A}\left(\mathcal{D}^{(t)}, S\right)$
    Compute $\varepsilon_t = \sum \mathcal{D}^{(t)} \mathbb{1}_{y_i \neq h_t(\mathbf{x}_i)}$
    Set $w_t = \frac{1}{2} \ln\left(\frac{1-\varepsilon_t}{\varepsilon_t}\right) = \frac{1}{2} \ln\left(\frac{1}{\varepsilon_t} - 1\right)$.
    Update sample weights $\mathcal{D}_i^{(t+1)} = \mathcal{D}_i^{(t)} \exp\left(-y_i \cdot w_t h_t\left(\mathbf{x}_i\right)\right), \quad i = 1, \ldots, m$
    Normalize weights $\mathcal{D}_i^{(t+1)} = \frac{\mathcal{D}_i^{(t+1)}}{\sum_j \mathcal{D}_j^{(t+1)}} \quad i = 1, \ldots, m$
  end for
  return $h_S(\mathbf{x}) = sign\left(\sum_{t=1}^T w_t h_t(\mathbf{x})\right)$
end procedure

The idea is simple: from iteration t to iteration $t+1$, we want to **increase** the weights of samples misclassified by h_t (where $y_i h_t(\mathbf{x}_i) = -1$) and **decrease** the weights of samples correctly classified by h_t. We want to make the classification problem "maximally hard" in the sense that weighted empirical risk of h_t, with respect to the updated weights $\mathcal{D}^{t+1}$, is the worse possible, namely $1/2$. Finally, the prediction rules vote in the committee with weights w_t.

Claim 5.4.1 For the weighting factor of $w_t = \frac{1}{2} ln\left(\varepsilon_t^{-1} - 1\right)$ and $\varepsilon = \sum_{i=1}^m \mathcal{D}_i^t \cdot \mathbb{1}_{y_i \neq h_t(\mathbf{x}_i)}$ the weighted empirical risk of h_t with respect to $\mathcal{D}^{t+1}$ is $1/2$:

$$\sum_{i=1}^m \mathcal{D}_i^{t+1} \cdot \mathbb{1}_{y_i \neq h_t(\mathbf{x}_i)} = \frac{1}{2}$$

Proof. Directly expressing the weighted empirical risk:

$$\begin{aligned}
\sum_{i=1}^{m} \mathcal{D}_i^{t+1} \cdot \mathbb{1}_{y_i \neq h_i(\mathbf{x}_i)} &= \frac{\sum_{i=1}^{m} \mathcal{D}_i^t \exp\left(-\mathbf{w}_t y_i h_t(\mathbf{x}_i) \mathbb{1}_{y_i \neq h_t(\mathbf{x}_i)}\right)}{\sum_{j=1}^{m} \mathcal{D}_j^t \exp\left(-\mathbf{w}_t y_j h_t(\mathbf{x}_j)\right)} \\
&= \frac{\exp(\mathbf{w}_t \varepsilon_t)}{\exp(\mathbf{w}_t \varepsilon_t) + \exp(-\mathbf{w}_t)(1-\varepsilon_t)} \\
&= \frac{\varepsilon_t}{\varepsilon_t + \exp(-2\mathbf{w}_t)(1-\varepsilon_t)} \\
&= \frac{\varepsilon_t}{\varepsilon_t + \frac{\varepsilon_t}{1-\varepsilon_t}(1-\varepsilon_t)} = \frac{1}{2}
\end{aligned}$$

■

Figure 5.13: Adaboost fitting animation: *Chapter 5 Examples - Source Code*

5.4.2 PAC View of Boosting - Weak Learnability

Historically, Boosting appeared as an answer to a fascinating question for which we first need to define **Weak Learnability**:

Definition 5.4.1 — γ-Weak-Learner. A learning algorithm $\mathcal{A}$ is a γ-weak-learner for an hypothesis class $\mathcal{H}$ if there exists a function $m_{\mathcal{H}} : (0,1) \to \mathbb{N}$ such that

- For every $\delta \in (0,1)$
- For every distribution $\mathcal{D}$ over the sample space $\mathcal{X}$
- For every labeling function $f : \mathcal{X} \to \{\pm\}$

if the realizabiity assumption holds with respect to $\mathcal{H}, \mathcal{D}, f$, then when running $\mathcal{A}$ on a training sample of $m \geq m_{\mathcal{H}}(0,1)$ *i.i.d* samples drawn according to $\mathcal{D}$ and labeled by f, the algorithm returns an hypothesis $h_S = \mathcal{A}(S)$ such that with probability at least $1-\delta$ (with respect to choice of the training sample S), we have $L_{\mathcal{D},f}(h_S) \leq 1/2 - \gamma$.

Definition 5.4.2 An hypothesis class $\mathcal{H}$ is γ-weak-learnable if there exits a γ-weak-learner for $\mathcal{H}$.

How is this different than PAC-learnability? If an hypothesis class $\mathcal{H}$ is PAC-learnable, then for **every** (ε, δ) there exists a learner $\mathcal{A}$. This means that we can learn and generalize a labeling function from $\mathcal{H}$ to any accuracy ε we want. But if $\mathcal{H}$ is γ-weak-learnable, for any δ **and just for** $\varepsilon = 1/2 - \gamma$ there is a learner $\mathcal{A}$. We may not be able to find a learner that has better accuracy (lower ε).

The question that motivated Boosting was the following:

- Suppose that $\mathcal{H}$ is PAC-learnable. Then we know that the rule $ERM_{\mathcal{H}}$ will learn (namely, will be probably approximately correct etc) with a near-minimal number of samples.
- But what if $ERM_{\mathcal{H}}$ is computationally hard? (we've seen examples)
- Assume we can find a **simple** hypothesis class (a "base hypothesis class") $\mathcal{H}_{base}$, such that $ERM_{\mathcal{H}_{base}}$ (choosing the hypothesis in $\mathcal{H}_{base}$ with lowest empirical risk) is computationally efficient, and is γ-weak-learner for $\mathcal{H}$ for some γ.
- This means that we have a computationally efficient way to learn with accuracy $1/2 - \gamma$, for some γ. Maybe we can't find an efficient learner with better γ.
- Is there a way to **boost** $ERM_{\mathcal{H}_{base}}$ in a computationally efficient way, and create a computationally efficient learner $\mathcal{A}$ which is close to minimizing ERM over $\mathcal{H}$?

For example, think about Decision trees. We saw that the ERM learner is not computationally feasible on this hypothesis class. But a small tree may be able to achieve accuracy (over a sample labeled by a larger tree) which is not great, but better than random. Well, as the following theorem shows, Adaboost does just that (for the full proof refer to UML 10.2)

Theorem 5.4.2 Let S be a training set. Assume that at each iteration of Adaboost, the base learner returns a prediction rule (hypothesis h_t) for which the weighted empirical risk satisfies:

$$\sum_{i=1}^{m} \mathcal{D}_i^t \mathbb{1}_{y_i \neq h(\mathbf{x}_i)} \leq \frac{1}{2} - \gamma$$

Then the (standard, non-weighted) empirical risk of the output prediction rule of Adaboost, h_{boost}, (the weighted committee vote) satisfies:

$$L_S(h_{boost}) \equiv \frac{1}{m} \sum_{i=1}^{m} \mathbb{1}_{y_i \neq h_{boost}(\mathbf{x}_i)} \leq \exp\left(-2\gamma^2 T\right)$$

5.4.3 Gradient Boosting

Add section about Gradient Boosting

5.4.4 Bias-Variance in Boosting

The hope is, of course, that we are not overfitting, so that low empirical risk will imply low generalization loss. Suppose we run T iterations of Adaboost over a learner $\mathcal{A}_{base}$ that returns hypothesis from $\mathcal{H}_{base}$. We would like to know what is the effective hypothesis class and how large is it. Adaboost with T iterations will return a function from the hypothesis class

$$\mathcal{H}_T := \left\{ \mathbf{x} \mapsto \sum_{t=1}^{T} w_t h_t(\mathbf{x}) \,\middle|\, w_t \in [0,\infty),\ \sum_t w_t = 1,\ h_t \in \mathcal{H}_{base} \right\}$$

namely convex combinations of hypotheses from $\mathcal{H}_{base}$. Therefore $\mathcal{H}_T$ becomes larger as T grows. Fortunately it does not grow too fast with T. Suppose for example we have a canonical way to measure the "size" of $\mathcal{H}_T$. It is possible to show that under certain conditions $VCdim(\mathcal{H}_T)$ is roughly $T \cdot VCdim(\mathcal{H}_{base})$. So we can expect Boosting to increase the variance (compared with the base learner) as T increases, but "not too fast".

On the other hand, it is clear that Boosting decreases bias. This is seen from the fact that the empirical risk decreases as T grows, meaning that $\mathcal{H}_T$ is able to come closer and closer to the labeling function on the training set. The fact that empirical risk decreases **exponentially** with T tells us that the bias decreases quite fast. Overall, Boosting typically decreases bias much faster than it increases variance, which is why it typically improves generalization loss quite dramatically. But the question that remains is if we use T too large, will boosting overfit?

Very often we see that boosting ERM over a very simple base hypothesis class is better than boosting ERM over a more complicated class. Figure 5.14 shows the example of the test error of boosting decision stumps (i.e. decision trees with a single split) with Adaboost over number of boosting iterations T, compared with the test errors of a single stump and of a single large decision tree. We are able to see that boosting this very simple base hypothesis class still achieves much better results compared to the very complex hypothesis class of trees with 244 nodes.

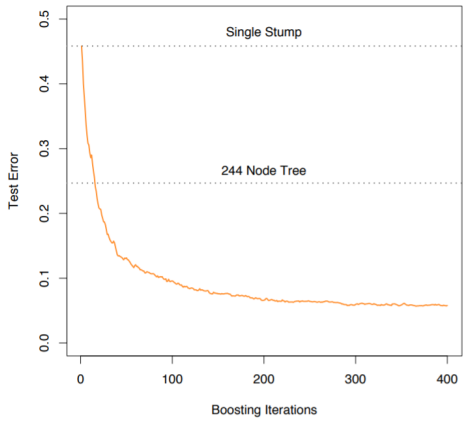


Figure 5.14: *Test error of boosting decision stumps with Adaboost over the number of boosting iterations*

5.5 Summary and Exercises

In this chapter we discussed committee based decisions and saw that a committe of learners using majority vote will achieve better accuracy compared to a single member, given that each member decides better than a random guess. We also saw that this improvement increases as the size of the committee grows bu tthat is bounded by the correlation between the members. To apply this concept we introduced three general methods:

- *Bootstrap:* A method to generate "new" tranining samples from the one training sample we have.
- *Bagging:* A committee method where we run some base learner against bootstrap samples. Learners are unrelated to each other and all committee members have equal voting weight.
- *Boosting:* A committee method where we run some base learner sequentially on weighted bootstrap samples. Sample weights change between iterations such that samples that the learner misclassified will increase in weight for the next iteration. The committee decision is based on the weighted vote of the members with weights related to their empirical loss.

These methods implement three general principles:

- We can create "artificial" training sets from our one training set S by sampling from S with replacements. This method is known as The Bootstrap. In a typical Bootstrap sample, about a third of the points a left out and others appear more than once.
- We can create a learner with improved accuracy and reduced variance by averaging better than random base learners. when the base learner gets a Bootstrap sample it is called Bagging. Bagging can be done in parallel as each prediction rule is created independently of the others. The prediction accuracy of the Bagging learner improves if the different prediction rules used are as de-correlated as possible. For example Random Forest achieves de-correlation by restricting each split in each tree to a random subset of coordinates.
- We can create a learner with with improved accuracy by boosting a base learner. The key idea behind Boosting is working with a probability distribution over S. Boosting means creating a weighted committee of prediction rules. Rules are created sequentially (not in parallel). Each rule is created the previous rule by modifying the distribution in such a way that misclassified training samples get an increased weight. For example Adaboost is a Boosting method that uses exponential updates to the probability distribution on S, such that the weighted empirical risk of the previous rule according to the updated distribution is exactly $1/2$ - the worse it can be.

	Bagging	**Boosting**
Learns committee members	In parallel	Sequentially
Datasets for each member	Bootstrap samples	Weighted bootstrap or original sample with weighted ERM
De-correlation	Recommented	Not necessary
If T too large	Does not overfit	May overfit
Reduces	Variance	Bias
Committee vote is done	Unweighted	Weighted
Parallel computation implementation	Yes	No
With decision trees use	Deep trees	Shallow trees

Table 5.1: *Comparison of Bagging and Boosting*

Exercises

1. Consider the concept of boosting where we run $\mathcal{A}$ against a training sample with some distribution $\mathcal{D}$. Describe a possible implementation of a decision tree for each of the two interpretations:
   - Using weighted empirical risk: How would you change the CART algorithm to work with a given weight vector $\mathcal{D}^t$ over the training sample S? Hint: what is the best splitting now that we have weights?
   - Using weighted Bootstrap: How would you change the CART algorithm to work with a given weight vector without changing the splitting algorithm, namely, by giving the algorithm a different training sample selected by weighted Bootstrap? Will the algorithm work with repeated samples?
2. Fill out a "Learner ID Card" for the Random Forest classifier specifying the following: hypothesis class; learning principle; computational implementation; making predictions, interpretability; providence of

class probabilities; family of models; time complexity of training and predicting; storing the model.

Appendices

A Linear Algebra

A.1 Norms & Inner Products

A *metric* (or distance function) is a function defined over an arbitrary set X that associates each pair of items in the set with a non-negative scalar quantity. Formally a function $d : X \times X \to \mathbb{R}$ is called a *metric* if and only if for all $x, y, z \in X$ the following properties hold:

- Identity of indiscernibles: $d(x,y) = 0 \iff x = y$
- Symmetry: $d(x,y) = d(y,x)$
- Triangle inequality $d(v,u) \leq d(v,w) + d(w,u)$.

These conditions imply that a metric is a non-negative function returning values in $[0,\infty)$. Some common metric functions are the Euclidean distance, graph distance and string edit distance.

■ **Example .1** Consider the vector space $\mathbb{R}^d$ let us show that the absolute distance, defined as the sum of absolute element-wise subtraction between the vectors $d(\mathbf{v},\mathbf{u}) \coloneqq \sum_{i=1}^{d} |v_i - u_i|$, is a metric function. Firstly, notice that from the properties of the absolute value over $\mathbb{R}$, for any two scalars $a, b \in \mathbb{R}$ it holds that $|a-b| = 0$ if and only if $a = b$. Therefore d, being a sum of non-negative elements equals zero if and only if all summed elements are zero. This takes place if and only if $\mathbf{v} = \mathbf{u}$. Next, symmetry of d is achieved through symmetry of the absolute value function. Lastly, let $\mathbf{v}, \mathbf{u}, \mathbf{w} \in \mathbb{R}^k$ then:

$$d(\mathbf{v},\mathbf{u}) = \sum |v_i - u_i| = \sum |v_i - w_i + w_i - u_i| \leq \sum |v_i - w_i| + \sum |w_i - u_i| = d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{u})$$

and so also the triangle inequality property holds ■

A *norm* on vector space $\mathbb{R}^d$ is a function $||\cdot|| : \mathbb{R}^d \to \mathbb{R}_+$ that satisfies that for all $\alpha \in \mathbb{R}$ and for all $\mathbf{v}, \mathbf{u} \in \mathbb{R}^d$ the following properties hold:

- Positive definiteness: $||\mathbf{v}|| \geq 0$ and $||\mathbf{v}|| = 0$ if and only if $\mathbf{v}$ is the zero vector
- Absolute homogeneity: $||\alpha\mathbf{v}|| = |\alpha| \cdot ||\mathbf{v}||$
- Triangle inequality: $||\mathbf{v} + \mathbf{u}|| \leq ||\mathbf{v}|| + ||\mathbf{u}||$

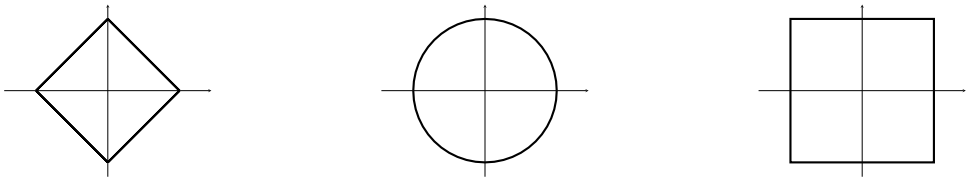
It is helpful to think of a norm as the distance of a vector from the origin. A few commonly used norms are:

- Absolute norm (ℓ_1): $||\mathbf{v}||_1 \coloneqq \sum |v_i|$.

- Euclidean norm (ℓ_2): $||\mathbf{v}||_2 \coloneqq \sqrt{\sum v_i^2}$.
- Infinity norm (ℓ_∞): $||\mathbf{v}||_\infty \coloneqq \max_i |v_i|$.

R These norms are part of a wider family of norms called the L_p norms, defined as $||\mathbf{v}||_p \coloneqq \left(\sum |v_i^p|\right)^{1/p}$ for $p \in \mathbb{N}$. The infinity norm is obtained by taking the limit as $p \to \infty$.

Given a norm on a vector space, i.e. a normed vector space $(V, ||\cdot||)$ we specify the *unit ball* of $||\cdot||$ as the set of vectors such that: $B_{||\cdot||} = \{\mathbf{v} \in V : ||\mathbf{v}|| \leq 1\}$. The use of different norms, and thus different shapes of their unit ball influence the outcome of optimization algorithms using them (**??**).



(a) $||\cdot||_1$ ***(b)*** $||\cdot||_2$ ***(c)*** $||\cdot||_\infty$

Figure 15: *Unit balls of norms on* $\mathbb{R}^2$

Similar to a metric, an *inner product* provides a scalar quantity associated with two given vectors. An inner product space is a vector space V over $\mathbb{R}$ together with a map $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{R}$ satisfying that $\forall \mathbf{v}, \mathbf{u}, \mathbf{w} \in V, \alpha \in \mathbb{R}$ the following properties hold:

- Symmetry: $\langle \mathbf{v}, \mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$
- Linearity: $\langle \alpha\mathbf{v} + \mathbf{w}, \mathbf{u} \rangle = \alpha \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{w}, \mathbf{u} \rangle$
- Non-negativity : $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$ and $\langle \mathbf{v}, \mathbf{v} \rangle = 0 \iff \mathbf{v} = \mathbf{0}$

An example for an inner product is the *standard inner product* $\langle \mathbf{v}, \mathbf{u} \rangle \coloneqq \sum_i v_i u_i$. These definitions of a norm and an inner product are very similar. In fact, given an inner product space, we are also given a norm over this space. Given an inner product space H, the function $||\cdot|| : H \to \mathbb{R}_+$ that is defined by $||\mathbf{v}|| = \langle \mathbf{v}, \mathbf{v} \rangle^{\frac{1}{2}}$ for all $\mathbf{v} \in H$ is a norm on H. It is called the *induced norm*.

Using inner products we can further formulate other intuitive geometrical notions. We can describe the angle between vectors as $\cos\theta = \langle \mathbf{v}, \mathbf{u} \rangle / ||\mathbf{v}|| \cdot ||\mathbf{u}||$. Consider the norm of the vector $\mathbf{v} - \mathbf{u}$. Being the induced norm of some inner product then:

$$||\mathbf{v} - \mathbf{u}||^2 = \langle \mathbf{v} - \mathbf{u}, \mathbf{v} - \mathbf{u} \rangle = \langle \mathbf{v}, \mathbf{v} \rangle - 2\langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{u} \rangle = ||\mathbf{v}||^2 + ||\mathbf{u}||^2 - 2\langle \mathbf{v}, \mathbf{u} \rangle$$

On the other hand, by the Law of Cosines for the triangle defined by $\mathbf{v}, \mathbf{u}, \mathbf{v} - \mathbf{u}$ then

$$||\mathbf{v} - \mathbf{u}||^2 = ||\mathbf{v}||^2 + ||\mathbf{u}||^2 - 2||\mathbf{v}|| \cdot ||\mathbf{u}|| \cdot \cos\theta$$

Put together we obtain that:

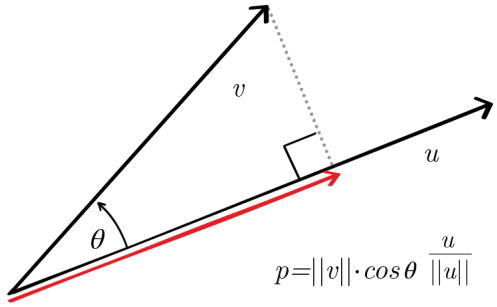
$$\langle \mathbf{v}, \mathbf{u} \rangle = ||\mathbf{v}|| \cdot ||\mathbf{u}|| \cdot \cos\theta \quad \Rightarrow \quad \cos\theta = \langle \mathbf{v}, \mathbf{u} \rangle / ||\mathbf{v}|| \cdot ||\mathbf{u}||$$

A special case if when the angle between two vectors is of 90° for which the result of the inner product between the vectors equals zero: $\theta = 90° \iff \langle \mathbf{v}, \mathbf{u} \rangle = 0$. In this case we say the vectors are *orthogonal* to each other and denote it as $\mathbf{v} \perp \mathbf{u}$.

Another geometric notion is that of *vector projection*. The vector projection of $\mathbf{v}$ onto $\mathbf{u}$ is the orthogonal

projection of $\mathbf{v}$ onto a line parallel to the vector $\mathbf{u}$. It is defined as $\mathbf{p} \coloneqq p \cdot \hat{\mathbf{u}}$ for $p \coloneqq \langle \mathbf{v}, \hat{\mathbf{u}} \rangle \hat{\mathbf{u}}$ and $\hat{\mathbf{u}} \coloneqq \mathbf{u}/||\mathbf{u}||$. p is called the *scalar projection* of $\mathbf{v}$ onto $\mathbf{u}$, and $\hat{\mathbf{u}}$ is the unit vector in the direction of $\mathbf{u}$. The vector $\mathbf{v} - \mathbf{p}$ that is perpendicular to $\mathbf{u}$ and completes a right-angle triangle is called the *vector rejection* of $\mathbf{v}$ from $\mathbf{u}$. Using the angle θ between the two vectors, we can write the vector projection as:

$$\mathbf{p} = \langle \mathbf{v}, \hat{\mathbf{u}} \rangle \hat{\mathbf{u}} = \langle \mathbf{v}, \mathbf{u} \rangle \cdot \frac{\mathbf{u}}{||\mathbf{u}||^2} = ||\mathbf{v}|| \, ||\mathbf{u}|| \cos\theta \cdot \frac{\mathbf{u}}{||\mathbf{u}||^2} = ||\mathbf{v}|| \cos\theta \cdot \hat{\mathbf{u}}$$



A.2 Matrices of Linear Transformations

Given two vector spaces V and W over a field $\mathbb{F}$, a *linear transformation* $T : V \to W$ is a function satisfying that $\forall \mathbf{v}, \mathbf{u} \in V$ and $\forall \alpha \in \mathbb{F}$:

- Additivity: $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{u})$
- Scalar multiplication: $T(\alpha \mathbf{v}) = \alpha \cdot T(\mathbf{v})$

In the case where V, W are of finite dimensions d and m, any linear map $T : V \to W$ is of the form $T(\mathbf{v}) = A\mathbf{v}$ for $\mathbf{v} \in V$ and some matrix $A \in \mathbb{R}^{m \times d}$. The matrix A is called is called the *representing matrix* of T. Extending linear transformations, an *affine transformation* is a transformation of the form $T(\mathbf{v}) = A\mathbf{v} + \mathbf{w}$ for $\mathbf{v} \in V, \mathbf{w} \in W$ and A the matrix associated with a linear transformation from V to W. Notice that an affine transformation is not a linear transformation as it does not map $\mathbf{0}_V$ to $\mathbf{0}_W$.

Using the representing matrix A of a linear transformation $T : V \to W$ we define four *fundamental subspaces*:

- Kernel- (or null-) space of A as $Ker(A) \coloneqq \{\mathbf{x} \in V | A\mathbf{x} = 0\}$. Also denotes as $\mathcal{N}(A)$.
- Image- (or column/range-) space of A as $Im(A) \coloneqq \{\mathbf{w} \in W | \mathbf{w} = A\mathbf{x}, \mathbf{x} \in V\}$. Also denotes as $Col(A)$ or $\mathcal{R}(A)$.
- Row space of A as $Im\left(A^\top\right) \coloneqq \left\{\mathbf{x} \in V | \mathbf{x} = A^\top \mathbf{w}, \mathbf{w} \in W\right\}$. Equivalently it can be defined as the column space of $A^\top$ and therefore denoted as $Col\left(A^\top\right)$.
- Null space of $A^\top$ as $Ker\left(A^\top\right) \coloneqq \left\{\mathbf{x} \in W | A^\top \mathbf{x} = 0\right\}$. This space is also referred to as the left null space of A.

Note that by definition, $Ker(A), Row(A) \subseteq V$ and $Im(A) \subseteq W$. Another quantity associated with matrices is the *rank* of a matrix. For $A \in \mathbb{R}^{m \times d}$ the rank of A is the maximum number of linearly independent rows of A and denoted by $rank(A)$. It holds that the rank of A equals both the dimension of the columns space and of the row space of A. As such, we refer to A being of *full rank* if and only if $rank(A) = \min\{m, d\}$. Otherwise we say that A is *rank deficient*.

For the case of a square matrix we define the notion of invertability. For $A \in \mathbb{R}^{d \times d}$ a square matrix, we say that A is invertible (or non-singular) if there exists a matrix $B \in \mathbb{R}^{d \times d}$ such that $AB = I_d = BA$. We denote the inverse by A^{-1}. Then, the following are equivalent:

- A is invertible (non-singular)
- A is full-rank
- $Det(A) \neq 0$
- $Im(A) = \mathbb{R}^m$ (i.e. the image is the whole space)
- $ker(A) = \vec{0}$ (i.e. the kernel is trivial)

A.2.1 Orthogonal Projection Matrices

We can extend the notion of vector projections to projecting a given vector onto a subspace of arbitrary dimension.

Definition A.1 Let V be a k-dimensional subspace of $\mathbb{R}^d$, and let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ be an orthonormal basis of V. The matrix $P := \sum_{i=1}^k \mathbf{v}_i \otimes \mathbf{v}_i = \sum_{i=1}^k \mathbf{v}_i \mathbf{v}_i^\top$ is an *orthogonal projection matrix* onto the subspace V.

where the operation performed on the vectors is the *outer product*. For two vectors $\mathbf{v} \in \mathbb{R}^n, \mathbf{u} \in \mathbb{R}^m$, the outer product of $\mathbf{v}$ and $\mathbf{u}$, which is denoted by $\mathbf{v} \otimes \mathbf{u}$ or $\mathbf{v}\mathbf{u}^\top$ is an $n \times m$ matrix with entries:

$$[\mathbf{v} \otimes \mathbf{u}]_{ij} = v_i \cdot u_j, \quad \mathbf{v} \otimes \mathbf{u} = \begin{bmatrix} v_1 u_1 & v_1 u_2 & \cdots & v_1 u_m \\ \vdots & \vdots & \ddots & \vdots \\ v_n u_1 & v_n u_2 & \cdots & v_n u_m \end{bmatrix}$$

That is, P is expressed as the sum of k one dimenional matrices. Another way to write P is as $P = AA^\top$ where the columns of A are $\mathbf{v}_1, \ldots, \mathbf{v}_k$ an orthonormal basis of V. The following lemma summarizes some useful properties of orthogonal projection matrices.

Lemma A.1 Let P be an orthogonal projection matrix then P has the following properties:

- P is symmetric
- $P^2 = P$
- The eigenvalues of P are either 0 or 1. $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are the eigenvectors of P which correspond to the eigenvalue 1.
- $(I - P)P = 0$
- $\forall \mathbf{x} \in \mathbb{R}^d$ and $\forall \mathbf{u} \in V$, $||\mathbf{x} - \mathbf{u}|| \geq ||\mathbf{x} - P\mathbf{x}||$
- $\mathbf{x} \in V \Rightarrow P\mathbf{x} = \mathbf{x}$

The outer product of two non-zero vectors defines a matrix with rank of 1. Notice, that the orthogonal projection matrix, being a sum of such matrices, is in fact a sum of rank 1 matrices.

A.2.2 Positive (Semi-) Definiteness

For square symmetric matrices we define the notion of definiteness and semi-definiteness.

Definition A.2 Let $A \in \mathbb{R}^{d \times d}$ be a symmetric matrix. A is a *positive semi-definite* (PSD) matrix if and only if

$$\forall \mathbf{x} \in \mathbb{R}^d \quad \mathbf{x}^\top A \mathbf{x} \geq 0$$

and denote so by $A \succeq 0$. Further, A is *positive definite* (PD) if and only if

$$\forall \mathbf{x} \in \mathbb{R}^d \quad \mathbf{x}^\top A \mathbf{x} > 0$$

and denote so by $A \succ 0$.

In addition, for a symmetric matrix A the following are equivalent:

- A is a PSD matrix
- For all $\mathbf{x} \in \mathbb{R}^d$ then $\mathbf{x}^\top A \mathbf{x} \geq 0$

- For λ an eigenvalue of A then $\lambda \geq 0$
- A can be written as the product $A = B^\top B$ for some matrix $B \in \mathbb{R}^{k\times d}$

Similarly, these conditions can be defined for PD matrices restricting that $\mathbf{x}^\top A\mathbf{x} > 0$, strictly positive eigenvalues and $A = B^* B$ for B^* being the conjugate transpose of B. There are many useful properties for PSD matrices such as that for $\alpha \geq 0$ also αA is a PSD matrix; the sum of PSD matrices is a PSD matrix; and for M, N two PSD matrices also the products MNM and NMN are PSD matrices.

A.3 Matrix Factorizations

Matrix factorization/decomposition is a strong tool with many theoretical as well as practical usages. The core idea is to find a representation of a given matrix as the product of several different matrices which have certain desired properties. For example, in the case of a PSD matrix $A \in \mathbb{R}^{d\times d}$ we have seen that there exists a matrix $B \in \mathbb{R}^{k\times d}$ such that $A = B^\top B$. Here we were able to decompose A into the product of the matrices $B^\top$ and B. We could now try and find if there exists a matrix B with some property. For example, if B is a lower triangular matrix, i.e. $B_{ij} = 0\ \forall j > i$, it is called the *Cholesky decomposition*.

A.3.1 Eigenvalue Decomposition

Let A be a square matrix. We say that a vector $\mathbf{0} \neq \mathbf{v} \in \mathbb{R}^d$ is an *eigenvector* of A corresponding to an *eigenvalue* $\lambda \in \mathbb{R}$ if and only if $A\mathbf{v} = \lambda\mathbf{v}$. To find the eigenvectors and eigenvalues of A we therefore wish to solve the linear system of $(A - \lambda I)\,\mathbf{v} = \mathbf{0}$. This system has a non-zero solution if and only if $\det(A - \lambda I) = 0$. These solutions if exist, are the roots of the *characteristic polynomial* of A: $p_A(\lambda) := |A - \lambda I|$. From the fundamental theorem of algebra we learn that the characteristic polynomial can be factored as the product

$$|A - \lambda I| = (\lambda_1 - \lambda) \cdot \ldots \cdot (\lambda_d - \lambda)$$

for λ_i the roots of the characteristic polynomial and the eigenvalues of A. Given λ and eigenvalue of A we define the set of eigenvectors corresponding to λ as $E_\lambda := \{\mathbf{v} \mid (A - \lambda I)\,\mathbf{v} = \mathbf{0}\}$. This linear subspace is the *eigenspace* of A associated with the eigenvalue λ. The dimension of E is termed the *geometric multiplicity* of λ.

The idea of matrix decomposition relates to that of *matrix diagonalization*. For a square matrix $A \in \mathbb{R}^{d\times d}$, we say that A is diagonalizable if there exists an invertible matrix P such that $P^{-1}AP$ is diagonal. In the case of a symmetric matrix, the Eigenvalue Decomposition (EVD) provides a diagonalization of a matrix using its eigenvalues and eigenvectors.

Theorem A.2 Let $A \in \mathbb{R}^{d\times d}$ be a real symmetric matrix. Then, there exist an orthogonal matrix $U \in \mathbb{R}^{d\times d}$ and a diagonal matrix $D \in \mathbb{R}^{d\times d}$ such that $A = UDU^\top$. Furthermore, it holds that

- The diagonal entries of D are the eigenvalues of A (with their multiplicities).
- The columns of U are eigenvectors for A corresponding the eigenvalues on the diagonal of D. These form an orthonormal basis of $\mathbb{R}^d$.

This decomposition is called the *Eigenvalue Decomposition* (EVD) or the *Spectral Decomposition* of A.

Namely, $A\mathbf{u}_i = D_{ii}\mathbf{u}_i,\ i \in [d]$. Without loss of generality, we arrange the elements of D (and respectively, the columns of U) such that the eigenvalues are in decreasing order $D_{ii} \geq D_{i+1,i+1}$.

■ **Example .2** Consider the following symmetric matrix

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

To find the EVD of A we solve its eigenvalue problem by finding λ such that $\det(A - \lambda I) = 0$, yielding the equation $(2-\lambda)^2 - 1 = 0$ with the solutions $\lambda = 3, 1$. Now, to find the eigenvectors we search for $\mathbf{v} \neq 0$ such that $(A - \lambda I)\mathbf{v} = 0$ for $\lambda = 3, 1$. We find that the eigenvector corresponding eigenvalues $\lambda = 3$ is $\mathbf{v}_3 = (1,1)^\top$

and the eigenvector corresponding eigenvalue $\lambda = 1$ is $\mathbf{v}_1 = (1,-1)^\top$. We normalize the eigenvectors and obtain the EVD of A:

$$A = UDU^\top \quad U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}, D = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$$

By multiplying $UDU^\top$ we validate that indeed we achieve the matrix A and the correctness of the decomposition. ∎

To gain a deeper understanding into the EVD, consider the linear transformations represented by the matrix A and the matrices U and D. It holds that for a square matrix, the eigenspace corresponding eigenvalue zero spans the kernel space of A, while the eigenspace corresponding non-zero eigenvalues spans the range of A. Thus, for $rank(A) = k \leq d$:

$$\mathcal{R}(A) = \text{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}, \quad \mathcal{N}(A) = \text{span}\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_d\}$$

As these vectors are orthogonal to each other, we have an orthonormal basis of eigenvectors of A to $\mathbb{R}^d$. Now consider a unit vector $\mathbf{x} \in \mathbb{R}^d$, $||\mathbf{x}|| = 1$. The image of $\mathbf{x}$ under A is

$$A\mathbf{x} = (UDU^\top)\mathbf{x} = UD \begin{bmatrix} \langle \mathbf{x}, \mathbf{u}_1 \rangle \\ \vdots \\ \langle \mathbf{x}, \mathbf{u}_d \rangle \end{bmatrix} = U \begin{bmatrix} \lambda_1 \langle \mathbf{x}, \mathbf{u}_1 \rangle \\ \vdots \\ \lambda_d \langle \mathbf{x}, \mathbf{u}_d \rangle \end{bmatrix} = \sum_{i=1}^{d} \lambda_i \langle \mathbf{x}, \mathbf{u}_i \rangle \mathbf{u}_i$$

Namely, A provides a representation of $\mathbf{x}$ in terms of the orthonormal basis $\mathbf{u}_1, \ldots, \mathbf{u}_d$, and dialites or contracts components (i.e directions in space) according to the magnitude of the eigenvalues. If the matrix is not of full rank, in some of the directions (those corresponding the null space) we are left with the zero vector.

The spectral decomposition has many useful properties. Just by observing the decomposition itself we are able to "read" the spectrum of A - the unique values along the diagonal of D - with their algebraic multiplicity, and the range- and null-spaces of A. In addition, the determinant and trace of A are obtained from D by:

$$det(A) = \prod_i D_{ii}, \quad tr(A) = \sum_i D_{ii}$$

Furthermore, taking A to the power is simply done by raising each of the eigenvalues to that power. And in the case of an invertible matrix A, the inverse is simply

$$A^{-1} = (UDU^\top)^{-1} = UD^{-1}U^\top, \quad D_{ii}^{-1} = (D_{ii})^{-1}$$

A.3.2 Singular-Values Decomposition

The *Singular-Values Decomposition* is a decomposition related to the EVD for an arbitrary real matrix $A \in \mathbb{R}^{m \times d}$. We say that $\mathbf{u} \in \mathbb{R}^m$ and $\mathbf{v} \in \mathbb{R}^d$ are left- and right singular values of A, corresponding singular value $\sigma \in \mathbb{R}_+$ if and only if $A\mathbf{v} = \sigma\mathbf{u}$.

Theorem A.3 Let $A \in \mathbb{R}^{m \times d}$ be a real matrix. Then, there exists:

- An orthogonal matrix $U \in \mathbb{R}^{m \times m}$ whose columns are the left singular vectors of A.
- An othrogonal matrix $V \in \mathbb{R}^{d \times d}$ whose columns are the right singular vectors of A.
- A diagonal matrix $\Sigma \in \mathbb{R}^{m \times d}$ whose diagonal entries are the non-negatve singular values of A such that $A\mathbf{v}_i = \Sigma_{ii}\mathbf{u}_i$.

$$A = U\Sigma V^\top = \overbrace{\begin{bmatrix} | & & | \\ \mathbf{u}_1 & \cdots & \mathbf{u}_m \\ | & & | \end{bmatrix}}^{m \times m} \overbrace{\begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_d \end{bmatrix}}^{m \times d} \overbrace{\begin{bmatrix} - & \mathbf{v}_1^\top & - \\ & \vdots & \\ - & \mathbf{v}_d^\top & - \end{bmatrix}}^{d \times d}$$

This is called the *Singular-Value Decomposition* of A.

Without loss of generality, we arrange the elements of Σ (and respectively, the columns of U, V) such that the singular values are in decreasing order $\Sigma_{ii} \geq \Sigma_{i+1,i+1}$.

Geometric Interpretation

As we have done for the EVD, let us consider the linear transformations represented by A. In this case the transformation takes $\mathbb{R}^d$ to a different space $\mathbb{R}^m$. When represented using the decomposition, similar to the EVD, the nature of the transformation becomes clear. For V, U whose columns are orthonormal basis of the domain $\mathbb{R}^d$ and range $\mathbb{R}^m$ of A it can be shown that Ex.7

$$\begin{aligned} \mathcal{R}(A) &= \text{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}, \quad \mathcal{N}(A^\top) = \text{span}\{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_m\} \\ \mathcal{R}(A^\top) &= \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}, \quad \mathcal{N}(A) = \text{span}\{\mathbf{v}_{k+1}, \ldots, \mathbf{v}_d\} \end{aligned}$$

where $rank(A) = k \leq \min\{m, d\}$. Then, for a general element in $\mathbb{R}^d$, represented in this basis $\mathbf{x} = \sum_i \langle \mathbf{x}, \mathbf{v}_i \rangle \mathbf{v}_i$ we see that:

$$A\mathbf{x} = A \sum_i \langle \mathbf{x}, \mathbf{v}_i \rangle \mathbf{v}_i = \sum_i \langle \mathbf{x}, \mathbf{v}_i \rangle U \Sigma V^\top \mathbf{v}_i = \sum_i \langle \mathbf{x}, \mathbf{v}_i \rangle U \Sigma \mathbf{e}_i = \sum_i \sigma_i \langle \mathbf{x}, \mathbf{v}_i \rangle U \mathbf{e}_i = \sum_i \sigma_i \langle \mathbf{x}, \mathbf{v}_i \rangle \mathbf{u}_i$$

That is, the SVD simply scales (expands or contracts) some of the components according to the magnitude of the singular values, and discards components corresponding to the null-spaces. Now, to understand the manner in which A deforms the space consider its action on the unit sphere in $\mathbb{R}^d$. Suppose $\mathbf{x}$ is on the unit sphere, i.e $\mathbf{x} = x_1\mathbf{v}_1 + \ldots + x_d\mathbf{v}_d$, $||\mathbf{x}||_2^2 = \sum x_i^2 = 1$. The image of the unit sphere under A is therefore $A\mathbf{x} = y_1\mathbf{u}_1 + \ldots + y_k\mathbf{u}_k$ for $y_i := \sigma_i x_i$ where

$$||A\mathbf{x}||_2^2 = \frac{y_1^2}{\sigma_1^2} + \ldots + \frac{y_k^2}{\sigma_k^2} = \sum_{i=1}^{k} x_i^2 \leq 1$$

Namely, A maps the unit k-sphere in $\mathbb{R}^d$ into an ellipsoid with axes in the directions of $\mathbf{u}_i$ and with magnitudes σ_i (collapsing $d-k$ dimensions of the domain) and then embeds the ellipsoid in $\mathbb{R}^m$.

The connection between SVD and EVD

The natural question at this point is how to choose the basis $\{\mathbf{v}_1, \ldots, v_d\}$ and $\{\mathbf{u}_1 \ldots, \mathbf{u}_m\}$. Since $A\mathbf{v}_i = \sigma_i\mathbf{u}_i$ it is simple to obtain the diagonal representation of A. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ be some orthonormal basis of $\mathbb{R}^d$ such that the first k elements span the row space of A while the remaining $d-k$ elements span the null space of A. We can now obtain $\mathbf{u}_i$ as a unit vector parallel to $A\mathbf{v}_i$, and extend this to a basis of $\mathbb{R}^m$. Relative to these basis we have achieved a diagonalization of A:

$$U^\top AV = U^\top U \Sigma V^\top V = \Sigma \tag{2}$$

In general however, even for orthonormal v's there is no guarantee for orthogonality to be preserved under A. Therefore the key point is in finding the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ for which $\mathbf{u}_1, \ldots, \mathbf{u}_k$ are orthonormal. We find such a basis using the EVD of the $d \times d$ symmetric matrix $A^\top A$. Let $A^\top A = VDV^\top$ be the EVD of $A^\top A$, where the columns of V, $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$, (i.e the eigenvectors of $A^\top A$) are an orthonormal basis of $\mathbb{R}^d$. Then

$$\langle A\mathbf{v}_i, A\mathbf{v}_j \rangle = (A\mathbf{v}_i)^\top (A\mathbf{v}_j) = \mathbf{v}_i^\top \left(A^\top A\mathbf{v}_j\right) = \mathbf{v}_i^\top (\lambda_j \mathbf{v}_j) = \lambda_j \mathbf{v}_i^\top \mathbf{v}_j = 0$$

Thus, the image set of applying A over the basis of eigenvectors of $A^\top A$, $\{A\mathbf{v}_1, \ldots, A\mathbf{v}_d\}$, is orthogonal with the nonzero vectors forming a basis for the range of A. Namely, the images under A of the eigenvectors of $A^\top A$ provide an orthogonal bases allowing the diagonalization of A as seen in (2). By normalizing the non-zero vectors we obtain $\{u_1, \ldots, u_k\}$

$$\mathbf{u}_i := \frac{A\mathbf{v}_i}{||A\mathbf{v}_i||} = \frac{A\mathbf{v}_i}{\sqrt{\lambda_i \mathbf{v}_i^\top \mathbf{v}_i}} = \frac{1}{\sqrt{\lambda_i}} A\mathbf{v}_i, \quad i \in [k]$$

completing the construction of the orthonormal bases for $\mathbb{R}^d$ and $\mathbb{R}^m$. By setting $\sigma_i = \sqrt{\lambda_i}$ we also achieve that $A\mathbf{v}_i = \sigma_i \mathbf{u}_i$ or in matrix notation $A = U\Sigma V^\top$.

Conversely, given the SVD of $A = U\Sigma V^\top$ we can recover the EVD of $A^\top A$ or of $AA^\top$:

$$A^\top A = \left(U\Sigma V^\top\right)^\top \left(U\Sigma V^\top\right) = V\Sigma^\top U^\top U\Sigma V^\top = V\Sigma^\top \Sigma V^\top$$
$$AA^\top = \left(U\Sigma V^\top\right) \left(U\Sigma V^\top\right)^\top = U\Sigma V^\top V\Sigma^\top U^\top = U\Sigma\Sigma^\top U^\top$$

where $\Sigma^\top\Sigma$ and $\Sigma\Sigma^\top$ are both square matrices whose first k diagonal entries are σ_i^2. We therefore conclude that the left singular values of A are the eigenvectors of $AA^\top$; the right singular values of A are the eigenvectors of $A^\top A$; and the singular values of A are the square root of the eigenvalues of $AA^\top$ and $A^\top A$. Furthermore, it can be shown that up to orthogonal transformations of $A^\top A$ and $AA^\top$ the SVD of A is uniquely determined.

Compact SVD Form

When writing the SVD of a matrix A, with rank $rank(A) = k < min\{m,d\}$, it becomes evident that we can express the SVD in a more compact way. Without loss of generality, suppose $d \leq m$. Notice that Σ consists of zero rows and columns as $\sigma_{k+1}, \ldots, \sigma_d$ are all zero.

$$A = \left[\begin{array}{ccc|ccc} \mathbf{u}_1 & \cdots & \mathbf{u}_k & \mathbf{u}_{k+1} & \cdots & \mathbf{u}_m \end{array}\right] \left[\begin{array}{ccc|c} \sigma_1 & & & \\ & \ddots & & \mathbf{0} \\ & & \sigma_k & \\ \hline & \mathbf{0} & & \mathbf{0} \end{array}\right] \left[\begin{array}{c} \mathbf{v}_1^\top \\ \vdots \\ \mathbf{v}_k^\top \\ \hline \mathbf{v}_{k+1}^\top \\ \vdots \\ \mathbf{v}_d^\top \end{array}\right]$$

When we partition the multiplication as follows it becomes evident that the left and right singular vectors $\mathbf{u}_{k+1}, \ldots, \mathbf{u}_m$ and $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_d$ do not make any contribution to A. Their purpose is to expand the leading left and right singular vectors into orthonormal bases of $\mathbb{R}^m$ and $\mathbb{R}^d$ respectively.

$$A = \left[\begin{array}{ccc} \mathbf{u}_1 & \cdots & \mathbf{u}_k \end{array}\right] \left[\begin{array}{ccc} \sigma_1 & & \\ & \ddots & \\ & & \sigma_k \end{array}\right] \left[\begin{array}{c} \mathbf{v}_1^\top \\ \vdots \\ \mathbf{v}_k^\top \end{array}\right] + \left[\begin{array}{ccc} \mathbf{u}_{k+1} & \cdots & \mathbf{u}_m \end{array}\right] \left[\begin{array}{c} \mathbf{0} \end{array}\right] \left[\begin{array}{c} \mathbf{v}_{k+1}^\top \\ \vdots \\ \mathbf{v}_d^\top \end{array}\right]$$

Thus, we eliminate left and right singular vectors corresponding zero singular values to obtain the *Compact SVD* form.

$$A = \overbrace{\left[\begin{array}{ccc} | & & | \\ \mathbf{u}_1 & \cdots & \mathbf{u}_k \\ | & & | \end{array}\right]}^{m\times k} \overbrace{\left[\begin{array}{ccc} \sigma_1 & & \\ & \ddots & \\ & & \sigma_k \end{array}\right]}^{k\times k} \overbrace{\left[\begin{array}{ccc} - & \mathbf{v}_1^\top & - \\ & \vdots & \\ - & \mathbf{v}_k^\top & - \end{array}\right]}^{k\times d} \tag{3}$$

A.4 Exercises

Theoretical Questions

1. Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V \subset \mathbb{R}^d$ be an orthonormal basis of V. Let A be the matrix whose columns are $\mathbf{v}_1, \ldots, \mathbf{v}_k$. Prove that $\sum \mathbf{v}_i \mathbf{v}_i^\top = AA^\top$.

2. Let $V \subset \mathbb{R}^d$ be a vector space of dimension k and P an orthogonal projection matrix onto V. Prove the properties of an orthogonal projection matrix described in Lemma A.1.

3. Let $A \in \mathbb{R}^{d\times d}$ be a square matrix of rank $k \leq d$. Let $\mathbf{u}_1,\ldots,\mathbf{u}_k$ be eigenvectors of A corresponding non-zero eigenvalues and $\mathbf{u}_{k+1},\ldots,\mathbf{u}_d$ be eigenvectors of A corresponding eigenvalue zero. Show that $\mathcal{R}(A) = \text{span}\{\mathbf{u}_1,\ldots,\mathbf{u}_k\}$ and that $\mathcal{N}(A) = \text{span}\{\mathbf{u}_{k+1},\ldots,\mathbf{u}_d\}$.

4. Let $A \in \mathbb{R}^{d\times d}$ be a symmetric matrix.
   - Show that $det(A) = \prod D_{ii}$.
   - Show that $tr(A) = \sum D_{ii}$.

5. Let $A = UDU^\top$ be the EVD of A. Provide an expression for A^k for $k \in \mathbb{N}$, using the eigenvalues of A.

6. Let $U \in \mathbb{R}^{d\times d}$ be an orthogonal matrix. Show that U is isometric, that is $||U\mathbf{x}||_2 = ||\mathbf{x}||_2 \ \forall \mathbf{x} \in \mathbb{R}^d$.

7. Let $A \in \mathbb{R}^{m\times d}$ be a real matrix of rank k and $A = U\Sigma V^\top$ an SVD of A. Show that the four fundamental subspaces of A are given by:

$$\begin{array}{lcllcl} \mathcal{N}(A) & = & \text{span}\{\mathbf{v}_{k+1},\ldots,\mathbf{v}_d\}, & \mathcal{R}(A) & = & \text{span}\{\mathbf{u}_1,\ldots,\mathbf{u}_k\} \\ \mathcal{N}(A^\top) & = & \text{span}\{\mathbf{u}_{k+1},\ldots,\mathbf{u}_m\}, & \mathcal{R}(A^\top) & = & \text{span}\{\mathbf{v}_1,\ldots,\mathbf{v}_k\} \end{array}$$

B Calculus

B.1 Gradients, Jacobians & Hessian

Derivatives The *derivative* of a function measures the degree in which the function changes in a small area around a point of interest. For a scalar function $f : \mathbb{R} \to \mathbb{R}$, the derivative of f at point $x \in \mathbb{R}$ is defined as

$$\frac{d}{dx} f(x) := \lim_{a\to 0} \frac{f(x+a) - f(x)}{a}$$

■ **Example .3** Consider the **R**ectified **L**inear **U**nit function defined as the positive part of its argument: $f(x) = \max(0,x)$. The derivative if this function is:

$$\frac{\partial}{\partial x} f(x) = \mathbb{1}_{x>1}$$

Note that at $x = 0$ the derivative of ReLU is undefined. To deal with such cases we will later define sub-gradients. ■

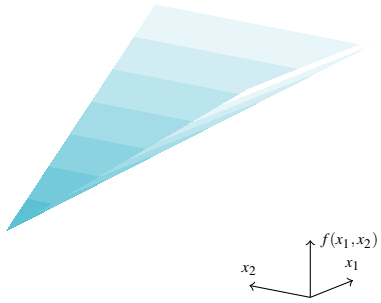
In the case of multivariate functions where $f : \mathbb{R}^d \to \mathbb{R}$ the notion of derivative is generalized to the degree in which a function changes in each of the input coordinates. The *partial derivative* of f at point $\mathbf{x} \in \mathbb{R}^d$ with respect to x_i is defined as

$$\begin{aligned} \frac{\partial}{\partial x_i} f(\mathbf{x}) &:= \lim_{a\to 0} \frac{f(\mathbf{x}+a\mathbf{e}_i) - f(\mathbf{x})}{a} \\ &= \lim_{a\to 0} \frac{f(x_1,\ldots,x_i+a,\ldots,x_d) - f(x_1,\ldots,x_i,\ldots,x_d)}{a} \end{aligned}$$

where $\mathbf{e}_i$ is the i-th standard basis vector. Namely, a partial derivative of a function is its derivative with respect to one of its variables, while all others are kept constant.

■ **Example .4** For $f(\mathbf{x}) = \max_i(x_1,\ldots,x_d)$ the partial derivatives of f at x_i are:

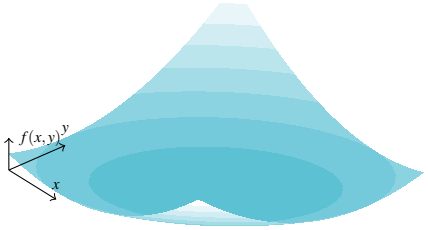
$$\frac{\partial}{\partial x_i} f(\mathbf{x}) = \mathbb{1}_{i=\text{argmax}\,(x_1,\ldots,x_d)}$$



■

■ **Example .5** For $f(x,y) = x^2 + xy + y^2$ the partial derivatives of f at (x_0, y_0) are

$$\frac{\partial}{\partial x} f(x_0,y_0) = 2x_0 + y_0, \quad \frac{\partial}{\partial y} f(x_0,y_0) = 2y_0 + x_0$$



■

Gradients Then the notion of *gradient* of $f : \mathbb{R}^d \to \mathbb{R}$ at $\mathbf{x}$ is simply the vector of all partial derivatives. It is as a convention that we define the gradient as a column vector.

$$\nabla f(\mathbf{x}) := \left(\frac{\partial f(\mathbf{x})}{\partial x_1}, \ldots, \frac{\partial f(\mathbf{x})}{\partial x_d} \right)^\top$$

■ **Example .6** Let $\mathbf{w} \in \mathbb{R}^d$ and $f : \mathbb{R}^d \to \mathbb{R}$ be a linear functional defined by $f(\mathbf{x}) = \mathbf{w}^\top \mathbf{x}$. To calculate the gradient of f at point $\mathbf{x}$ we derive the partial derivatives of f. From linearity of the derivative:

$$\frac{\partial}{\partial x_j} f(\mathbf{x}) = \sum_i \frac{\partial}{\partial x_j} [f(\mathbf{x})]_i = \sum_i \frac{\partial}{\partial x_j} \mathbf{w}_i \mathbf{x}_i = \mathbf{w}_j$$

Therefore, in vector notation $\nabla f(\mathbf{x}) = \mathbf{w}$. ■

■ **Example .7** Let $f : \mathbb{R}^d \to \mathbb{R}$ be defined by $f(\mathbf{x}) = ||\mathbf{x}||^2$. Using linearity of the derivative then

$$\frac{\partial}{\partial x_j} f(x) = \sum_i \frac{\partial}{\partial x_j} x_i^2 = 2x_j$$

which in vector notation can be written as $\nabla f(\mathbf{x}) = 2\mathbf{x}$. ■

Jacobians The Jacobian is the generalization of the gradient for multivariate vector-valued functions, that is, functions that receive and output vectors. So for $\mathbf{f}:\mathbb{R}^d \to \mathbb{R}^m$ where $\mathbf{f}(\mathbf{x}) = (f_1(\mathbf{x}),\ldots,f_m(\mathbf{x}))^\top$, the *Jacobian* of f is the $m \times d$ matrix of all partial derivatives:

$$J_{\mathbf{x}}(\mathbf{f}) \coloneqq \begin{bmatrix} \frac{\partial f_1(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\mathbf{x})}{\partial x_d} \\ \vdots & & \vdots \\ \frac{\partial f_m(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial f_m(\mathbf{x})}{\partial x_d} \end{bmatrix}$$

■ **Example .8** Let $f:\mathbb{R}^2 \to \mathbb{R}$ be defined as $f(\mathbf{x}) = x_1^2 + x_2^2$. The Jacobian of f is:

$$J_x(\mathbf{f}) = \begin{bmatrix} \frac{\partial f_1(\mathbf{x})}{\partial x_1} & \frac{\partial f_1(\mathbf{x})}{\partial x_2} \end{bmatrix} = [2x_1, 2x_2] = \nabla f(\mathbf{x})^\top$$

■

Notice that for any function where $k = 1$ the Jacobian is in fact the transposed gradient vector: $J_{\mathbf{x}}(f) = \nabla f(\mathbf{x})^\top$.

■ **Example .9** Let $f:\mathbb{R}^d \to \mathbb{R}^m$ defined as $f(\mathbf{x}) = A\mathbf{x}$ where $A \in \mathbb{R}^{m\times d}$ and denote the rows of A as $\mathbf{a_1},\ldots,\mathbf{a_m}$. To find the Jacobian of of f, $J_{\mathbf{x}}(f))$, define the set of functions computing each coordinate in the output vector $\forall i \in [m] \quad f_i(\mathbf{x}) = \langle \mathbf{a}_i, \mathbf{x}\rangle$. Then the Jacobian of f is comprised of the gradients of $f_1,\ldots,f_m$ as rows. Notice that we have already computed the gradient of linear functionals in Example .6 so:

$$J_{\mathbf{x}}(f) = \begin{bmatrix} \nabla f_1(\mathbf{x})^\top \\ \vdots \\ \nabla f_d(\mathbf{x})^\top \end{bmatrix} = \begin{bmatrix} -\mathbf{a}_1- \\ \vdots \\ -\mathbf{a}_m- \end{bmatrix} = A$$

■

Hessians Similar to the gradient we can consider the second derivative of a function with respect to each of its partial first derivatives. Let $f:\mathbb{R}^d \to \mathbb{R}$ be a twice differential function. The *Hessian* matrix H of f is the square matrix of second derivative:

$$H[f] \coloneqq \begin{bmatrix} \frac{\partial^2 f}{\partial^2 x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_d} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_d \partial x_1} & \cdots & \frac{\partial^2 f}{\partial^2 x_d} \end{bmatrix}$$

■ **Example .10** Let us calculate the Hessian of the polynomial function $f(x_1,x_2) = x_1^2 + x_1x_2 + x_2^2$. We begin with calculating the first partial derivatives of f: $\frac{\partial f(x_1,x_2)}{\partial x_i} = 2x_i + x_j$ for $i \in \{1,2\}$ and $j \neq i$. Next, we calculate the derivative a second time with respect to each of the parameters:

$$\frac{\partial^2 f(x_1,x_2)}{\partial x_i \partial x_j} = \begin{cases} 2 & x_i = x_j \\ 1 & x_i \neq x_i \end{cases}$$

We therefore conclude that the Hessian of f is :

$$H = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

■

B.2 Chain Rules

Many times a given function of interest is the composition of other functions. In that case, when we calulate the derivatives we apply the chain rule. In the case of a scalar function, let $f:\mathbb{R}\to\mathbb{R}$ and $g:\mathbb{R}\to\mathbb{R}$ be two differential functions, then the derivative of the composite $f\circ g$ is:

$$(f\circ g)' := \left(f'\circ g\right)\cdot g'$$

Namely, for $h(x)=f(g(x))$ then $\forall x\in\mathbb{R}\ h'(x)=f'(g(x))\cdot g'(x)$. We can extend this to the multivariate case where the composite receives a vector and outputs another.

Theorem B.1 Let $f:\mathbb{R}^d\to\mathbb{R}^m$ and $g:\mathbb{R}^k\to\mathbb{R}^d$. The Jacobian of the composition $(f\circ g):\mathbb{R}^k\to\mathbb{R}^m$ at $\mathbf{x}$ is

$$J_{\mathbf{x}}(f\circ g)=J_{g(\mathbf{x})}(f)J_{\mathbf{x}}(g):=\begin{bmatrix}\frac{\partial f_1(g(\mathbf{x}))}{\partial g_1(\mathbf{x})} & \cdots & \frac{\partial f_1(g(\mathbf{x}))}{\partial g_d(\mathbf{x})}\\ \vdots & & \vdots\\ \frac{\partial f_m(g(\mathbf{x}))}{\partial g_1(\mathbf{x})} & \cdots & \frac{\partial f_m(g(\mathbf{x}))}{\partial g_d(\mathbf{x})}\end{bmatrix}=\begin{bmatrix}\frac{\partial g_1(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial g_1(\mathbf{x})}{\partial x_k}\\ \vdots & & \vdots\\ \frac{\partial g_d(\mathbf{x})}{\partial x_1} & \cdots & \frac{\partial g_d(\mathbf{x})}{\partial x_k}\end{bmatrix}$$

In element-wise notation:

$$J_{\mathbf{x}}(f\circ g)_{i,j}:=\sum_l \frac{\partial f_i(g(\mathbf{x}))}{\partial g_l(\mathbf{x})}\frac{\partial g_l(\mathbf{x})}{\partial x_j}$$

■ **Example .11** Next, let us calculate the gradient of the following function: $f(\mathbf{x})=\frac{1}{2}||A\mathbf{x}-\mathbf{y}||^2$. Let's define $g(\mathbf{x})=A\mathbf{x}-\mathbf{y}$ and $h(\mathbf{x})=\frac{1}{2}||\mathbf{x}||^2$ and notice that $f=h\circ g$. As g an affine transformation, we have see in Example .9 that $J_{\mathbf{x}}(g)=A$. Notice, that as $Im(f)\subseteq\mathbb{R}$, the Jacobian of f equals to the transpose of its gradient. As seen in Example .7, $J_{g(\mathbf{x})}(f)=(2g(\mathbf{x}))^\top$. Now, applying the chain rule:

$$J_{\mathbf{x}}(f)=J_{\mathbf{x}}(h\circ g)=J_{g(\mathbf{x})}(h)J_{\mathbf{x}}(g)=(A\mathbf{x}-\mathbf{y})^\top A$$

$$\nabla_{\mathbf{x}}(f)=J_{\mathbf{x}}(f)^\top=A^\top(A\mathbf{x}-\mathbf{y})$$

■

■ **Example .12** The softmax function defined over $S:\mathbb{R}^d\to[0,1]^d$ returns a vector that its coordinates sum up to 1. It is defined by

$$S(\mathbf{a})_j=\frac{e^{a_j}}{\sum_{k=1}^d e^{a_k}}$$

Let us calculate the derivative of the softmax function. Denote $g_i(\mathbf{a}):=e^{a_i}$ and $h(\mathbf{a}):=\sum_k g_k(\mathbf{a})$. So:

$$\frac{\partial S_i}{\partial a_j}=\frac{\partial}{\partial a_j}\frac{e^{a_i}}{\sum_d e^{a_k}}=\frac{\partial}{\partial a_j}\frac{g_i}{h}$$

Note that for any a_j the derivative of h is e^{a_j}. In the case of g_i, when deriving with respect to a_j we get that the derivative is e^{a_j} only if $i=j$. Otherwise, the derivative is 0. Therefore, the derivative of S_i in the case where $i=j$ is:

$$\frac{\partial}{\partial a_j}\frac{e^{a_i}}{\sum_k e^{a_k}}=\frac{e^{a_i}(\sum_k e^{a_k})-e^{a_i}e^{a_j}}{(\sum_k e^{a_k})^2}=\frac{e^{a_i}}{(\sum_k e^{a_k})}\cdot\frac{(\sum_k e^{a_k})-e^{a_j}}{(\sum_k e^{a_k})}=S_i(1-S_j)$$

It is left to show the derivative in the case where $i\neq j$. Intuitively, the softmax function is a "soft" version of the argmax function. Instead of just selecting one maximal element, the softmax breaks the vector into segments with the maximal input element getting a proportionally larger portion, but the other elements getting some of it as well. ■

B.3 Function Approximations

Consider a function $f:\mathbb{R}\to\mathbb{R}$ and recall the definition of the Taylor series of f at x_0 near x:

$$T(x)=\sum_{n=0}^{\infty}\frac{f^{(n)}(x-x_0)}{n!}x^n=f(x_0)+f'(x_0)(x-x_0)+\frac{1}{2}f''(x_0)(x-x_0)^2+\ldots$$

A linear approximation (or first order approximation) is an approximation of a general function using a linear function. For a differentiable function $f:\mathbb{R}\to\mathbb{R}$, Taylor's theorem implies that for a close enough x then

$$f(x)\approx f(x_0)+f'(x_0)(x-x_0)$$

We can now extend this theorem to define linear approximations of multivariate functions.

Definition B.1 Let $f:\mathbb{R}^d\to\mathbb{R}$ and $\mathbf{x}\in\mathbb{R}^d$. The *linear approximation* of f for every $\mathbf{x}\in\mathbb{R}$ near $\mathbf{x}_0$ is defined as

$$f(\mathbf{x})=f(\mathbf{x}_0)+\langle\nabla f(\mathbf{x}_0),\mathbf{x}-\mathbf{x}_0\rangle$$

So if for example, we consider a bivariate function $f:\mathbb{R}^2\to\mathbb{R}$, the linear approximation of f near the point (x_0,y_0) is:

$$f(x_0+x,y_0+y)\approx f(x_0,y_0)+x\cdot\frac{\partial f(x_0,y_0)}{\partial x}+y\cdot\frac{\partial f(x_0,y_0)}{\partial y}$$

Now, if f is a linear function, intuition dictates that the linear approximation of f would be the function itself. Let $\mathbf{b}\in\mathbb{R}^d$ and let $f:\mathbb{R}^d\to\mathbb{R}$ be defined by $f(\mathbf{x})=\mathbf{b}^\top\mathbf{x}$. Then, the linear approximation of f near $\mathbf{x}$ is

$$\begin{aligned}f(\mathbf{x})+\langle\nabla f(\mathbf{x}),\mathbf{x}-\mathbf{x}'\rangle &= \mathbf{b}^\top\mathbf{x}+\langle\mathbf{b},\mathbf{x}-\mathbf{x}'\rangle\\ &= \mathbf{b}^\top(\mathbf{x}+\mathbf{x}'-\mathbf{x})=f(\mathbf{x}')\end{aligned}$$

■ **Example .13** Let $f:R^2\to\mathbb{R}$ be defined by $f(x,y)=\sqrt{x^2+y^2}$. Let us calculate the linear approximation of f near $(3,4)$. We begin with expressing the gradient of f. So, the partial derivative of f with respect to first argument at point x is:

$$\frac{\partial}{\partial x}=f(x_0,y_0)=2x_0\cdots\frac{1}{2\sqrt{x_0^2+y_0^2}}$$

Therefore the gradient of f is $\nabla f(\mathbf{x})=\left(\frac{x_0}{\sqrt{x_0^2+y_0^2}},\frac{y_0}{\sqrt{x_0^2+y_0^2}}\right)^\top$. So for a point (x,y) in the vicinity of $(3,4)$ the linear approximation is:

$$f(3+x,4+y)\approx 5+\frac{3}{5}x+\frac{4}{5}y$$

If for example $x=0.1,y=0.2$ then $f(3+0.1,4+0.2)=5.2201..\approx 5.22=5+3/5\cdot 0.1+4/5\cdot 0.2$ ■

Using the gradient of a function we are able to provide a first order (linear) approximation of a function. Similarly, we can also provide a second order approximation of a function. The second order Taylor expansion of f near $\mathbf{x}$ is given by:

Definition B.2 Let $f:\mathbb{R}^d\to\mathbb{R}$ be a twice differentiable function and $\mathbf{x}\in\mathbb{R}^d$. The *second order approximation* (also referred to as quadratic approximation) of f for every $\mathbf{x}\in\mathbb{R}$ near $\mathbf{x}_0$ is defined as

$$f(\mathbf{x})=f(\mathbf{x}_0)+\langle\nabla f(\mathbf{x}_0),\mathbf{x}-\mathbf{x}_0\rangle+\tfrac{1}{2}(\mathbf{x}-\mathbf{x}_0)^\top H[f(\mathbf{x}_0)](\mathbf{x}-\mathbf{x}_0)$$

■ **Example .14** Returning to the second order polynomial function defined in Example .10, let us find the first- and second-order approximations of f near point $\mathbf{x}_0 = (x_0, y_0)^\top$. The first order approximation is given by:

$$\begin{aligned} f(\mathbf{x}_0+\mathbf{x}) &\approx f(\mathbf{x}_0)+\nabla f(\mathbf{x}_0)^\top \mathbf{x} \\ &= x_0^2+x_0y_0+y_0^2+\begin{bmatrix} 2x_0+y_0 \\ 2y_0+x_0 \end{bmatrix}^\top \begin{bmatrix} x \\ y \end{bmatrix} \\ &= x_0^2+x_0y_0+y_0^2+2x_0x+y_0x+2y_0y+x_0y \end{aligned}$$

The second order approximation is given by

$$\begin{aligned} f(\mathbf{x}_0+\mathbf{x}) &\approx x_0^2+x_0y_0+y_0^2+2x_0x+y_0x+2y_0y+x_0y+\tfrac{1}{2}\begin{bmatrix} x \\ y \end{bmatrix}^\top \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\ &= x_0^2+x_0y_0+y_0^2+2x_0x+y_0x+2y_0y+x_0y++x^2+yx+y^2 \\ &= (x_0+x)^2+(x_0+x)(y_0+y)+(y_0+y)^2 \end{aligned}$$

Notice that since f is a second order polynomial then the calculated value is the exact value of the function at $\mathbf{x}_0+\mathbf{x}$. ■

B.4 Convexity

Convex Sets A set $C \subseteq \mathbb{R}^d$ is called a *convex set* if and only if $\forall \mathbf{v}, \mathbf{u} \in C$, $\forall \alpha \in [0,1]$ then $\alpha\mathbf{v}+(1-\alpha)\mathbf{u} \in C$. That is, if the line segment between any two vectors $\mathbf{v}, \mathbf{u} \in C$, is contained in C. The vector $\alpha\mathbf{v}+(1-\alpha)\mathbf{u}$ is called a *convex combination* of $\mathbf{v}$ and $\mathbf{u}$.

■ **Example .15** Let V be a vector space and $U \subseteq V$. U is a convex set as for every $\mathbf{v}, \mathbf{u} \in U$ and $\alpha \in [0,1]$ $\alpha\mathbf{v}+(1-\alpha)\mathbf{u}$ is a linear combination of vectors in U and therefore is also in U. ■

■ **Example .16** Consider the unit ball of some norm $B_{||\cdot||} = \{\mathbf{v} \in V : ||\mathbf{v}|| \leq 1\}$. This is a convex set as for any $\mathbf{v}, \mathbf{u} \in B$ and $\alpha \in [0,1]$, the triangle inequality imples that:

$$\begin{aligned} \|\alpha\mathbf{v}+(1-\alpha)\mathbf{u}\| &\leq \|\alpha\mathbf{v}\|+\|(1-\alpha)\mathbf{u}\| \\ &= \alpha\|\mathbf{v}\|+(1-\alpha)\|\mathbf{u}\| \\ &\leq \alpha+1-\alpha = 1 \end{aligned}$$

■

■ **Example .17** Let $(\mathbf{w}, b)$ be a hyperplane for $\mathbf{w} \in \mathbb{R}^d$ and $b \in \mathbb{R}$. The closed halfspace $W := \{\mathbf{v} : \mathbf{w}^\top \mathbf{v} \leq b\}$ is a convex set. For any $\mathbf{v}, \mathbf{u} \in W$ and $\alpha \in [0,1]$ it holds that:

$$\langle \mathbf{w}, \alpha\mathbf{v}+(1-\alpha)\mathbf{u} \rangle = \alpha \langle \mathbf{w}, \mathbf{v} \rangle + (1-\alpha) \langle \mathbf{w}, \mathbf{u} \rangle \leq \alpha b + (1-\alpha) b = b$$

■

Convexity is preserved under several operations. The claim below demonstrates a few such operations.

Claim B.2 Convexity is preserved under the following operations:
1. The intersection $C := \bigcap_{i \in I} C_i$ for $\{C_i : i \in I\}$ a collection of convex sets.
2. The vector sum $C_1 + C_2 := \{c_1 + c_2 : c_1 \in C_1, c_2 \in C_2\}$ of two convex sets.
3. The set $\lambda C := \{\lambda c : c \in C\}$ is convex, for any convex set C, and every scalar λ.

Proof. Proving directly from definition:
1. Let $\mathbf{v}, \mathbf{u} \in C$, and let $\alpha \in [0,1]$. As C is the intersection of $\{C_i\}$ it holds that $\mathbf{v}, \mathbf{u} \in C_i$ for any $i \in I$. Since $\{C_i\}$ are convex sets then for any $\alpha \in [0,1]$ it holds that $\alpha\mathbf{v}+(1-\alpha)\mathbf{u} \in C_i$. Thus $\alpha\mathbf{v}+(1-\alpha)\mathbf{u} \in \bigcap_{i \in I} C_i = C$.

2. Let $\mathbf{v},\mathbf{u} \in C_1 + C_2$, then there exists $\mathbf{v}_1,\mathbf{v}_2$ and $\mathbf{u}_1,\mathbf{u}_2$ for which

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 \text{ s.t. } \mathbf{v}_1 \in C_1, \mathbf{v}_2 \in C_2, \quad \mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2 \text{ s.t. } \mathbf{u}_1 \in C_1, \mathbf{u}_2 \in C_2$$

Let $\alpha \in [0,1]$ then:

$$\begin{aligned} \alpha\mathbf{v} + (1-\alpha)\mathbf{u} &= \alpha(\mathbf{v}_1 + \mathbf{v}_2) + (1-\alpha)(\mathbf{u}_1 + \mathbf{u}_2) \\ &= [\alpha\mathbf{v}_1 + (1-\alpha)\mathbf{u}_1] + [\alpha\mathbf{v}_2 + (1-\alpha)\mathbf{u}_2] \end{aligned}$$

where, from convexity of C_1, C_2 it holds that:

$$\alpha\mathbf{v}_1 + (1-\alpha)\mathbf{u}_1 \in C_1, \quad \alpha\mathbf{v}_2 + (1-\alpha)\mathbf{u}_2 \in C_2$$

and therefore $\alpha\mathbf{v} + (1-\alpha)\mathbf{u} \in C_1 + C_2$

3. Let $\mathbf{v},\mathbf{u} \in \lambda C$, then there exists $\mathbf{x},\mathbf{y} \in C$ such that $\mathbf{v} = \lambda\mathbf{x}$ and $\mathbf{u} = \lambda\mathbf{y}$. Let let $\alpha \in [0,1]$ them:

$$\alpha\mathbf{v} + (1-\alpha)\mathbf{u} = \lambda(\alpha\mathbf{x} + (1-\alpha)\mathbf{y}) \in \lambda C.$$

■

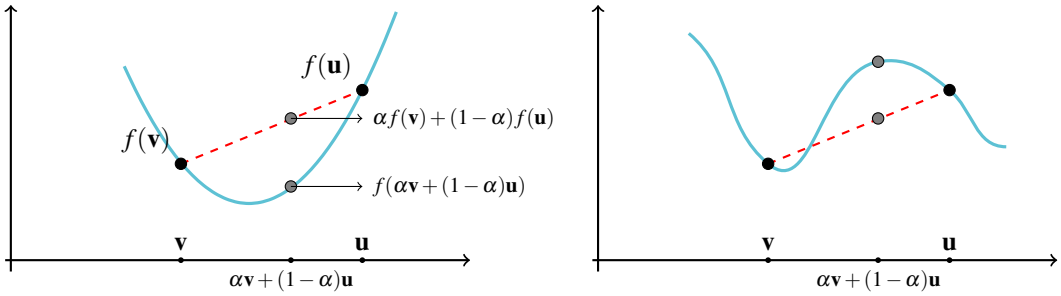
In a similar manner we can show that the vector sum of a finite set of convex sets is convex, giving a convex combination of arbitrary length.

(a) *convex sets examples* ***(b)*** *Non-convex sets examples*

Figure 16: *Examples of convex- and non-convex sets*

Convex Functions Given a convex set, we can define the notion of a convex function. A function $f : C \to \mathbb{R}$ is *convex* if and only if $C \equiv \text{dom} f$ is convex and for every $\mathbf{u},\mathbf{v} \in C$ and every $\alpha \in [0,1]$ then $f(\alpha\mathbf{v} + (1-\alpha)\mathbf{u}) \leq \alpha f(\mathbf{v}) + (1-\alpha)f(\mathbf{u})$.

This means that the line segment connecting any two points on the curve of a convex function f lies fully above that curve. In other words, the value of a convex function f at any convex combination $\mathbf{v}$ and $\mathbf{u}$ is always smaller than the convex combination of the values of f at $\mathbf{v}$ and $\mathbf{u}$.



(a) *Convex function* ***(b)*** *Non-convex function*

Figure 17: *Illustrating convex vs. non-convex function*

■ **Example .18** Let $||\cdot|| : \mathbb{R}^d \to \mathbb{R}$ be a norm, $\mathbf{v}, \mathbf{u} \in \mathbb{R}^d$ and $\alpha \in [0,1]$. From, the triangle inequality it holds that:

$$\|\alpha\mathbf{v} + (1-\alpha)\mathbf{u}\| \leq \|\alpha\mathbf{v}\| + \|(1-\alpha)\mathbf{u}\| = \alpha\|\mathbf{v}\| + (1-\alpha)\|\mathbf{u}\|$$

■

■ **Example .19** Let $f : \mathbb{R}^d \to \mathbb{R}$ be an affine transformation, that is $f(\mathbf{x}) = \langle \mathbf{w}, \mathbf{x} \rangle + b$ for $\mathbf{w} \in \mathbb{R}^d$ and $b \in \mathbb{R}$. Let $\mathbf{v}, \mathbf{u} \in \mathbb{R}^d$ and $\alpha \in [0,1]$ then:

$$\begin{aligned} f(\alpha\mathbf{v} + (1-\alpha)\mathbf{u}) &= \langle \mathbf{w}, \alpha\mathbf{v} + (1-\alpha)\mathbf{u} \rangle + b \\ &= \alpha(\langle \mathbf{w}, \mathbf{v} \rangle + b) + (1-\alpha)(\langle \mathbf{w}, \mathbf{u} \rangle + b) \\ &= \alpha f(\mathbf{v}) + (1-\alpha) f(\mathbf{u}) \end{aligned}$$

■

■ **Example .20** Let $f(\mathbf{w}) \coloneqq ||\mathbf{X}\mathbf{w} - \mathbf{y}||^2$ for $\mathbf{X} \in \mathbb{R}^{m \times d}, \mathbf{y} \in \mathbb{R}^m$ and $\mathbf{w} \in \mathbb{R}^d$. Let us show that f is convex in $\mathbf{w}$. Let $\mathbf{v}, \mathbf{u} \in \mathbb{R}^d$ and $\alpha \in [0,1]$ then:

$$\begin{aligned} f(\alpha\mathbf{v} + (1-\alpha)\mathbf{u}) &= ||\mathbf{X}[\alpha\mathbf{v} + (1-\alpha)\mathbf{u}] - \mathbf{y}|| \\ &= ||\alpha(\mathbf{X}\mathbf{v} - \mathbf{y}) + (1-\alpha)(\mathbf{X}\mathbf{v} - \mathbf{y})|| \\ &\leq \alpha||\mathbf{X}\mathbf{v} - \mathbf{y}|| + (1-\alpha)||\mathbf{X}\mathbf{u} - \mathbf{y}|| \\ &= \alpha f(\mathbf{v}) + (1-\alpha) f(\mathbf{u}) \end{aligned}$$

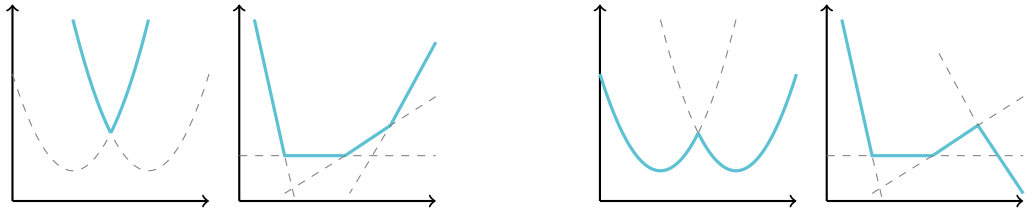
■

Some commonly used convex functions are the exponent $x \to e^{ax}, \forall a$, $x \to x^a, \forall a \notin (0,1)$ and negative logarithm $x \to -\log(x)$. Furthermore, as can be seen from Example .20 affine transformations $\mathbf{x} \to \mathbf{w}^\top \mathbf{x} + \mathbf{b}$ are convex as well as quadratic tarnsformations are convex $\mathbf{x} \to \mathbf{x}^\top A\mathbf{x} + \mathbf{w}^\top \mathbf{x} + \alpha$ for $A \succcurlyeq 0$. The family of ℓ_p norms (Example A.1) defined as $||\mathbf{x}||_p \coloneqq \left(\sum x_i^p\right)^{1/p}$ is convex for $p \geq 1$.

On the basis of some known convex functions, we can define a set of closure properties of convexity. The following are a few of such operations that preserve convexity:

- Non-negative linear combinations preserve convexity. That is, for $g(\mathbf{x}) = \sum \alpha_i f_i(\mathbf{x})$, then g is convex if f_i are convex functions are a_i are non-negative.
- The function $g(\mathbf{x}) = \sup_i f_i(\mathbf{x})$ is convex if f_i are convex functions.
- Partial minimization of a function preserves convexity. That is, for a convex function $g : \mathbb{R}^{d+k} \to \mathbb{R}$ defined by $(\mathbf{x}_1|\mathbf{x}_2) \to g(\mathbf{x}_1|\mathbf{x}_2)$ for $\mathbf{x}_1 \in \mathbb{R}^d, \mathbf{x}_2 \in \mathbb{R}^k$, then the partial minimization function $h : \mathbb{R}^d \to \mathbb{R}$ defined by $h(\mathbf{x}_1) = \min_{\mathbf{x}_2 \in C} g(\mathbf{x}_1, \mathbf{x}_2)$ (where $C \subset \mathbb{R}^k$ is a convex set) is a convex function.
- For $g : \mathbb{R}^d \to \mathbb{R}$ convex function and $h : \mathbb{R} \to \mathbb{R}$ convex and nondecreasing, the composition $h \circ g$ is a convex function.
- For $h : \mathbb{R}^k \to \mathbb{R}$ convex and nondecreasing in each of its coordinates and $g_1, \ldots, g_k : \mathbb{R}^d \to \mathbb{R}$ convex functions, then $f(\mathbf{x}) = h(g_1(\mathbf{x}), \ldots, g_k(\mathbf{x}))$ is a convex function.

Properties of Convex Functions Convex functions have many useful properties, making them simple to optimize, i.e. finding the input that minimizes them.



(a) *Convex functions* ***(b)*** *Non-convex functions*

Figure 18: *Examples of convex- and non-convex functions illustrating closure properties*

Claim B.3 — First order characterization. Let $f:\mathbb{R}^d\to\mathbb{R}$ be a differential function, then f is convex if and only if $\mathrm{dom}f\subseteq\mathbb{R}^d$ is a convex set and $f(\mathbf{u})\geq f(\mathbf{w})+\langle\mathbf{u}-\mathbf{w},\nabla f(\mathbf{w})\rangle\ \ \forall\mathbf{u},\mathbf{w}\in\mathrm{dom}f$.

Proof. Without loss of generality, assume $\mathbf{w}=\mathbf{0}$ since otherwise we could simply shift the axis. Therefore, it is enough to show that for any $\mathbf{u}$ $f(\mathbf{u})\geq f(\mathbf{0})+\langle\nabla f(\mathbf{0}),\mathbf{u}\rangle$. As f is convex it holds that

$$\begin{aligned} f(\alpha\mathbf{u}) &\leq (1-\alpha)f(\mathbf{0})+\alpha f(\mathbf{u}) \\ &\Downarrow \\ \frac{f(\alpha\mathbf{u})-f(\mathbf{0})}{\alpha} &\leq f(\mathbf{u})-f(\mathbf{0}) \end{aligned}$$

This holds for any $\alpha\in[0,1]$ and thus taking the limit of both sides, with $\alpha\to 0$, and recalling that $\lim_{\alpha\to 0}\frac{f(\alpha\mathbf{u})-f(\mathbf{0})}{\alpha}=\langle\mathbf{u},\nabla f(\mathbf{0})\rangle$ concluding the proof. ■

Namely, at any point on the graph of a convex (and differential) function f, the tangents lie below the graph of the function.

■ **Example .21** Let $f:\mathbb{R}^d\to\mathbb{R}$ be a linear functional defined by $f(\mathbf{x})=\langle\mathbf{w},\mathbf{x}\rangle$ for $\mathbf{w}\in\mathbb{R}^d$. Let us show that f is convex using the characterization above. For any $\mathbf{x}\in\mathbb{R}^d$ it holds that $\nabla f(\mathbf{x})=\mathbf{w}$. Therefore, for a point $\mathbf{y}\in\mathbb{R}^d$ it holds that

$$f(\mathbf{y})=\langle\mathbf{w},\mathbf{y}\rangle=\langle\mathbf{w},\mathbf{x}\rangle+\langle\mathbf{y}-\mathbf{x},\mathbf{w}\rangle=f(\mathbf{x})+\langle\nabla f(\mathbf{x}),\mathbf{y}-\mathbf{x}\rangle$$

■

Notice that the affine transformation of $\mathbf{u}$ that is given by $f(\mathbf{w})+\langle\mathbf{u}-\mathbf{w},\nabla f(\mathbf{w})\rangle$ is the first-order Taylor approximation of f near $\mathbf{x}$. Suppose we wish to estimate (i.e approximate) the value of f near a point of interest. We therefore learn that for a convex f the first-order Taylor approximation is a *global underestimator*. Furthermore it shows that in the case of a convex function, the *local* information about the function (i.e the gradient at $f(\mathbf{w})$) allows us to derive *global* information about it. An example for such information is seen in the following claim.

Claim B.4 Let $f:\mathbb{R}^d\to\mathbb{R}$ be a convex function. If $f(\mathbf{u})$ is a local minimum then it is a global minimum.

Proof. Let $f:C\to\mathbb{R}$. and denote $B(\mathbf{u},r)$ the intersection of C and a sphere of radius r around the point $\mathbf{u}$:

$$B(\mathbf{u},r):=\{\mathbf{v}:\mathbf{v}\in C,\|\mathbf{v}-\mathbf{u}\|\leq r\}$$

Let $\mathbf{u}$ be a local minimizer of f (i.e. $f(\mathbf{u})$ is a local minimum). Therefore, there exists $r>0$ such that for any $\mathbf{v}\in B(\mathbf{u},r)$ it holds that $f(\mathbf{u})\leq f(\mathbf{v})$. Note that since f is a convex function, its domain, C, is a convex set - otherwise, the convex combination of two vectors in C may not belong to C and the convexity condition in definition would not be well-defined. Let $\mathbf{v}\in C$ (not necessarily in B) and take $\alpha>0$ close enough to 1

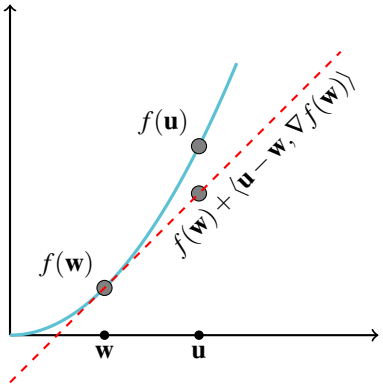


Figure 19: *Tangent of Convex Function*

such that $\alpha\mathbf{u} + (1-\alpha)\mathbf{v}$ is inside B. Since C is convex, $\alpha\mathbf{u} + (1-\alpha)\mathbf{v}$ is in C. It follows that to ensure that $\alpha\mathbf{u} + (1-\alpha)\mathbf{v}$ is in B it is enough to choose an α close enough to 1 so that the distance between $\alpha\mathbf{u} + (1-\alpha)\mathbf{v}$ and $\mathbf{u}$ is smaller than r. Since $\alpha\mathbf{u} + (1-\alpha)\mathbf{v}$ is inside B and by definition, one has

$$f(\mathbf{u}) \leq f(\alpha\mathbf{u} + (1-\alpha)\mathbf{v}) \ \leq \ \alpha f(\mathbf{u}) + (1-\alpha) f(\mathbf{v}) \ .$$

Hence, $(1-\alpha) f(\mathbf{u}) \ \leq \ (1-\alpha) f(\mathbf{v})$, that is, $f(\mathbf{u}) \ \leq \ f(\mathbf{v})$. This holds for every $\mathbf{v}$, hence $f(\mathbf{u})$ is also a global minimum of f. ■

Claim B.5 — Second order characterization. Let $f : \mathbb{R}^d \to \mathbb{R}$ be a twice differentiable function, then f is convex if and only of $\text{dom} f \subset \mathbb{R}^d$ is a convex set and $\nabla^2 f(\mathbf{x}) \succcurlyeq 0$, $\forall \mathbf{x} \in \text{dom} f$

■ **Example .22** Let $A \in \mathbb{R}^{d \times d}$ be a symmetric matrix and let $f : \mathbb{R}^d \to \mathbb{R}$ defined as $f(\mathbf{x}) = \mathbf{x}^\top A\mathbf{x}$. Let us show that f is convex using the characterization above. To do so we find the first and second derivatives of f. Denote $g(\mathbf{x}) = A\mathbf{x}$ and $h(\mathbf{x}) = \mathbf{x}$ so we can write f as $f \equiv h^\top g$. Using the product rule then:

$$\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}} = \frac{\partial h(\mathbf{x})^\top}{\partial \mathbf{x}} \cdot g(\mathbf{x}) + \frac{\partial g(\mathbf{x})}{\partial \mathbf{x}} \cdot h(\mathbf{x})$$

As the derivative of g by $\mathbf{x}$ is A then:

$$\nabla f(\mathbf{x}) = A^\top \mathbf{x} + A\mathbf{x} = \left(A + A^\top\right)\mathbf{x}$$

Since A is symmetric then $\nabla f(\mathbf{x}) = 2A\mathbf{x}$. Next, let us compute the second derivative:

$$\nabla^2 f(\mathbf{x}) = \frac{\partial^2 f}{\partial^2 \mathbf{x}} = \frac{\partial 2A\mathbf{x}}{\partial \mathbf{x}} = 2A$$

Thus, by the characterization above f is convex if and only if $A \succeq 0$. That is, if and only if A is a PSD matrix. ■

■ **Example .23** Recall the function $f(\mathbf{w}) := ||\mathbf{X}\mathbf{w} - \mathbf{y}||^2$ for $\mathbf{X} \in \mathbb{R}^{m \times d}, \mathbf{y} \in \mathbb{R}^m$ and $\mathbf{w} \in \mathbb{R}^d$ seen in Example .20. Let us show that f is convex using the characterization above. In Example .11 we have shown that the gradient of f is:

$$\nabla_{\mathbf{w}} f(\mathbf{w}) = J_{\mathbf{w}}^\top (f(\mathbf{w})) = \left(J_{g(\mathbf{w})}(h) J_{\mathbf{w}}(h)\right)^\top = 2\mathbf{X}^\top (\mathbf{X}\mathbf{w} - \mathbf{y})$$

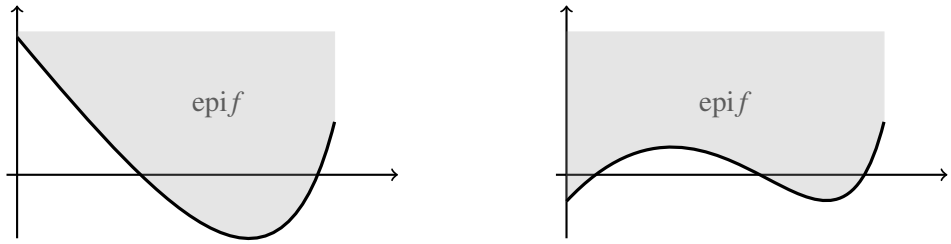
for $g(\mathbf{w}) := \mathbf{X}\mathbf{w} - \mathbf{y}$ and $h(\mathbf{z}) := ||\mathbf{z}||^2$. Next, we calculate the second derivative of f, namely, we calculate the partial derivatives of the graident of f with respect to each of its coordinates.

$$H_{\mathbf{w}}[f(\mathbf{w})] = \frac{\partial}{\partial \mathbf{w}} \nabla_{\mathbf{w}} f(\mathbf{w}) = 2\mathbf{X}^\top \mathbf{X}$$

Since $\mathbf{X}^\top \mathbf{X} \succeq 0$ we conclude that the hessian of f is PSD and thus f is a convex function. ∎

R Notice that the requirement of $\mathrm{dom} f$ to be a convex set is necessary in both the first- and second-order characterizations.

Given a function $f : \mathbb{R}^d \to \mathbb{R}$, the *graph* of the function is defined as the set $\{(\mathbf{x}, f(\mathbf{x})) \,|\, \mathbf{x} \in \mathrm{dom} f\} \subseteq \mathbb{R}^{d+1}$. The *epigraph* of f is the set of all points above f $\mathrm{epi} f := \{(\mathbf{x}, \beta) \,|\, \mathbf{x} \in \mathrm{dom} f, f(\mathbf{x}) \leq \beta\}$. The connection between convex sets and convex functions is through the epigraph of the function. A function $f : \mathbb{R}^d \to \mathbb{R}$ is convex if and only if *epi f* is a convex set.



(a) *Convex function & convex epigraph*

(b) *Non-convex function & non-convex epigraph*

B.5 Exercises

Theoretical Questions

1. Show that the set of real PSD matrices $V := \{A \in \mathbb{R}^{d \times d} | A \in PSD\}$is a convex set.
2. Show that the image and pre-image of an affine transformation are convex sets.
3. Show that the image and pre-image of the linear-fraction function are convex sets. The linear-fraction function is defined as $f(\mathbf{x}) = \frac{A\mathbf{x}+\mathbf{b}}{\mathbf{c}^\top \mathbf{x}+\mathbf{d}}$
4. Show that quadratic functions $\mathbf{x} \to \mathbf{x}^\top A\mathbf{x} + \mathbf{w}^\top \mathbf{x} + \alpha$ are convex if and only if $A \succcurlyeq 0$.
5. Show that for any $p \geq 1$ the norm $||\mathbf{x}||_p := \left(\sum x_i^p\right)^{1/p}$ is a convex function.
6. Show that the log-sum-exp function, defined as $f(\mathbf{x}) = \log\left(\sum_{i=1}^k \exp\left(\mathbf{w}_i^\top \mathbf{x} + b_i\right)\right)$ is a convex function. Hint: use the fact that affine compositions preserve convexity and the second order characterization.
7. Show that the following function is a convex function: $f(\mathbf{w}) := \frac{1}{m}\sum_i \log(1 + \exp(-y_i \langle \mathbf{w}, \mathbf{x}_i \rangle))$ for $\mathbf{w}, \mathbf{x}_i \in \mathbb{R}^d$ and $y_i \in \mathbb{R}$. This function is the loss function used in the logistic regression optimization problem (3.28).

8. Let $f(\mathbf{w})$ be a differentiable convex function. Show that, beside the tangent at $\mathbf{w}$, no other line passing through the point $(\mathbf{w}, f(\mathbf{w}))$ lies fully below $f(\mathbf{w})$. In other words, show that if $\forall \mathbf{u} \in \mathbb{R}^d$, $f(\mathbf{u}) \geq f(\mathbf{w}) + \langle \mathbf{u} - \mathbf{w}, \mathbf{a} \rangle$ then $\mathbf{a} = \nabla f(\mathbf{w})$.

9. Show that $f(\mathbf{w}) \coloneqq \min_{i \in [m]} \left| \mathbf{w}^\top \mathbf{x}_i \right|$ for $\mathbf{x}_1, \ldots, \mathbf{x}_m$ is a concave function. Namely, that $-f$ is a convex function. This function is the margin which maximized in the Hard-SVM optimization problem (3.13).

10. Show that in both the first- and second-order characterization of a convex function, the requirement that $dom(f)$ is a convex set is necessary. That is, describe non-convex functions f whose domain is not a convex set and that $\nabla f \geq 0$ or $\nabla^2 f \succcurlyeq 0$.