

Machine Learning for High Energy Physics

Notes taken by Manuel Morales & James Moore
at the MLHEP summer school

1	Competition: Dark matter searches	3
1.1	Introduction to dark matter <i>Background information on dark matter.</i>	3
1.2	Direct detection of dark matter <i>Dark matter flux on Earth. Directionality and detection. Background events vs signal events. Electron recoil and nuclear recoil.</i>	3
1.3	Dark matter detection with a time projection chamber <i>Gas tank detection. Images of electron recoil tracks and nuclear recoil tracks. Goal of the school's competition.</i>	5
I	Introduction to machine learning	7
2	Introduction to supervised learning	7
2.1	Problem setup <i>Problem setup for supervised learning. Basic examples.</i>	7
2.2	Feature types <i>Features and the design matrix. Numeric, categorical nominal, categorical ordinal and binary features. One-hot encoding.</i>	8
2.3	Learning algorithms <i>Definition of a learning algorithm. Loss functions, e.g. least squares error. Examples of k nearest neighbours and linear regression.</i>	10
2.4	Assumptions about data and model complexity <i>Training and test data. The curse of dimensionality. Model complexity.</i>	12
3	Linear models	14
3.1	Linear models and linear regression <i>Linear models and examples. 'Hidden power' of linear models via feature transformation. Examples of loss functions: MSE, MAE, MAPE and MSLE.</i>	14
3.2	Analytic solution <i>Analytic solution for linear models. Ill-conditioning and flat directions. Bias terms.</i>	16
3.3	Numerical and stochastic optimisation: gradient descent <i>The gradient and its geometric interpretation. The gradient descent algorithm; convex functions. Overfitting and early stopping. Stochastic gradient descent.</i>	18
3.4	Feature expansion <i>General description of feature transformation. Examples of polynomial feature transformations.</i>	20
4	Classification with linear models	21
4.1	Classification with linear regression <i>Classification problems; naïve approach with MSE loss. Better approach with smooth approximations to 0-1 loss.</i>	21
4.2	Logistic regression <i>Logistic regression from class probabilities and maximum log likelihood. The sigmoid function and the logistic regression loss function.</i>	23
4.3	Multinomial logistic regression	25

	<i>Logistic regression for many classes using class probabilities; symmetry of the parameters. The multinomial logistic regression loss function.</i>	
4.4	Multiclass classification: general approach	26
	<i>One-versus-rest multiclass classification. Comparison with logistic regression.</i>	
5	Model regularisation	28
5.1	The problem of overfitting	28
	<i>Recap of overfitting and test set.</i>	
5.2	Prediction error decomposition	28
	<i>Decomposition of error sources: model variance, bias, and irreducible error. The bias-variance tradeoff. Bias and variance of linear models.</i>	
5.3	Regularisation	30
	<i>Regularisation methods: L2 regularisation, L1 regularisation, and elastic net regression. Comparison of methods; sparsity vs weight-sharing.</i>	
5.4	Probabilistic view	32
	<i>Relationship of regularisation to probabilities and maximum likelihood.</i>	
5.5	Bayesian view	33
	<i>Relationship of regularisation to Bayesian priors.</i>	
6	Quality metrics for regression and classification	34
6.1	Quality metrics for regression models	34
	<i>Effect of outliers.</i>	
6.2	Quality metrics for classification models	36
7	Model tests	42
7.1	Train/test split	42
7.2	Cross-validation methods	44
7.3	Quality metric uncertainty estimation	47
7.4	Statistical model comparison	48
8	Decision trees	51
8.1	Decision tree training	51
8.2	Stopping rules for decision tree learning	53
9	Feature engineering, importance and selection	54
9.1	Feature engineering	54
9.2	Feature importance	56
9.3	Feature selection	60
10	Clustering	61
10.1	Clustering vs classification	61
10.2	K-means	62
10.3	Quality metrics	65

1 Competition: Dark matter searches

1.1 Introduction to dark matter

Less than 5% of the total mass and energy in the universe is the stuff we know about: stars, planets, galaxies, gases. Most of the universe is made of *dark matter* (dark because it does not interact with light), whilst the rest is *dark energy*.

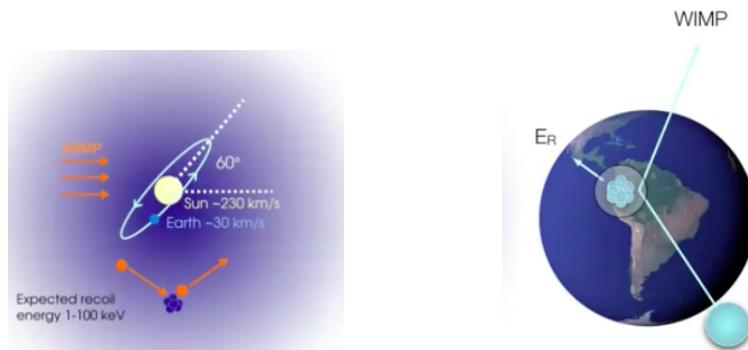
There is significant evidence for this dark matter (from rotational curves of galaxies, the CMB, velocity of galaxies, big bang nucleosynthesis, cluster collisions) at various scales. It was even hypothesised in the 1930s - but we still don't know what it is! We can, however, comment on *where* dark matter is. Our galaxy is surrounded by an approximately spherical halo of dark matter, with the Sun moving through this halo.

Certainly, dark matter is not one of the Standard Model elementary particles (i.e. dark matter is not a quark, lepton, gauge boson, or the Higgs boson). Quarks, leptons and the W -boson are all charged (dark matter is neutral - it is 'dark'), neutrinos are too light (and move too fast), and the Z and Higgs are too short-lived.

There are many models which have been proposed to explain dark matter. One hypothesis is that dark matter is made of *weakly interacting massive particles* (abbreviated to WIMPs).

1.2 Direct detection of dark matter

Since the Earth is moving through the dark matter halo surrounding the galaxy, we should expect to be able to detect dark matter here on Earth.



One can perform a rough calculation to determine how many dark matter particles we expect to detect:

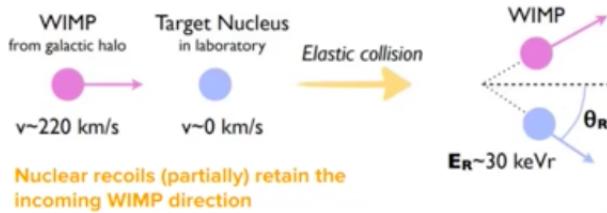
- The dark matter density is given experimentally by $\rho = 0.3 \text{ GeV/cm}^3$
- The average velocity of the Sun is given by $\langle v \rangle = 220 \text{ km/s}$.
- We don't know the mass of the dark matter particles, but in the WIMP models we expect that the mass is around $m \approx 100 \text{ GeV}$.

We can then determine the *flux* of WIMPs on Earth:

$$\phi = \frac{\rho}{m} \langle v \rangle \approx 10^5 \text{ cm}^{-2}\text{s}^{-1}.$$

Thus tens of millions of dark matter particles are flying through your hand every second!

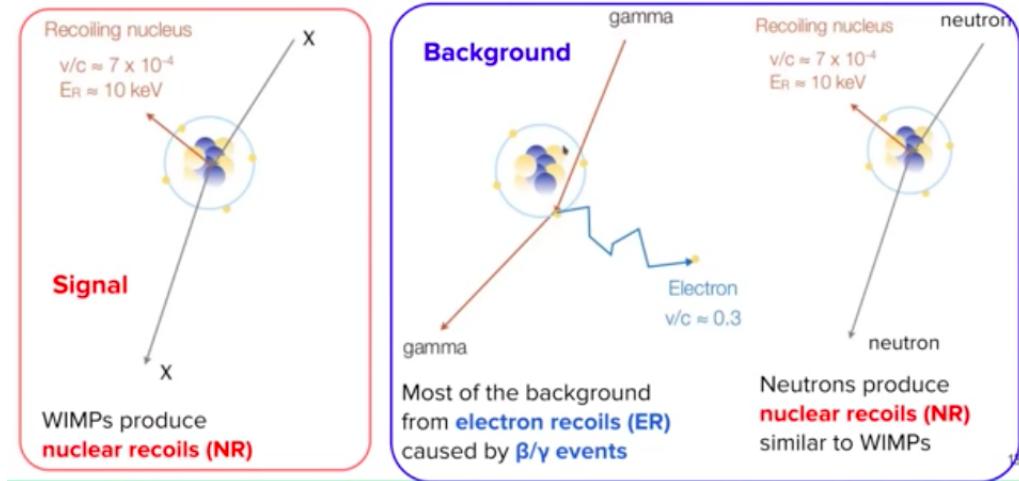
One important strategy we can employ in the detection of dark matter is *directionality*. From our position on Earth, we know that dark matter particles arrive from a *precise direction* in the sky, namely the *Cygnus constellation*. They travel at velocities around 220 km/s. When they hit some special nuclei that forms part of our detector, there is an *elastic collision* that results in movement of the nuclei - this is measurable because the nuclei is visible (unlike the WIMP).



If we see nuclei moving in a direction that is compatible with the direction that we expect dark matter to arrive from, this could be evidence of dark matter detection.

The direction is very important because there are many other things that can hit a nucleus, and the nucleus can move for other reasons unrelated to dark matter. The general problem is that *whilst the flux of WIMPs is high, the probability of interaction is very low*. In a sensitive detector we expect 1 event per kilogram per year (compare this with placing a banana near the detector - this causes around 100 events per kilogram per year, because of the radiation from the potassium in the banana!). Therefore, the experimental challenge is to detect a *tiny signal over a large background*.

There are some differences between signal and background events. A dark matter signal comprises only *nuclear recoil*, whilst most of the background is comprised of *electron recoil* caused by photon interactions. On the other hand the background does also include nuclear recoil events caused by neutrons, which are similar to WIMP nuclear recoil events.



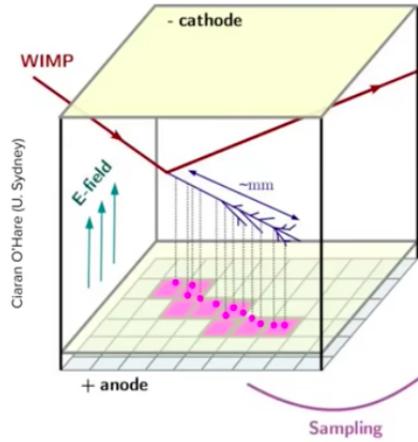
There are two main sources of background:

- (1) *Cosmic rays*. These are a problem if you would like to do your measurement on the Earth's surface. To mitigate the effect, we can work in underground laboratories.
- (2) *Environmental radioactivity* (mainly from potassium, uranium and thorium). This comes even from the walls of your lab! To mitigate this effect, we can shield the equipment, and carefully choose materials with low levels of radioactivity in the setup.

1.3 Dark matter detection with a time projection chamber

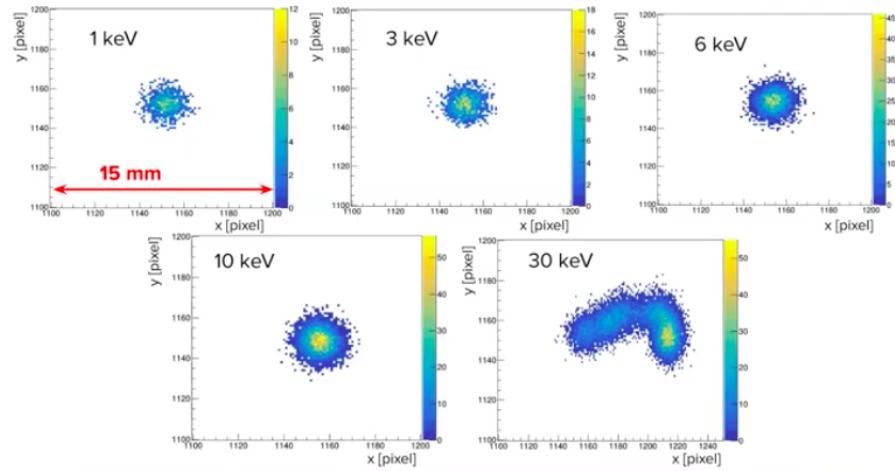
We will now describe in more detail the detection of dark matter via nuclear recoil.

The general idea is to use a *gas target*; for example the gas used in the CYGNO experiment, based in Italy, is a mixture of helium He and carbon tetrafluoride CF_4 . The advantage of using a gas target is that it is not very dense, so the recoiling nucleus can travel several millimetres. This direction can be measured.

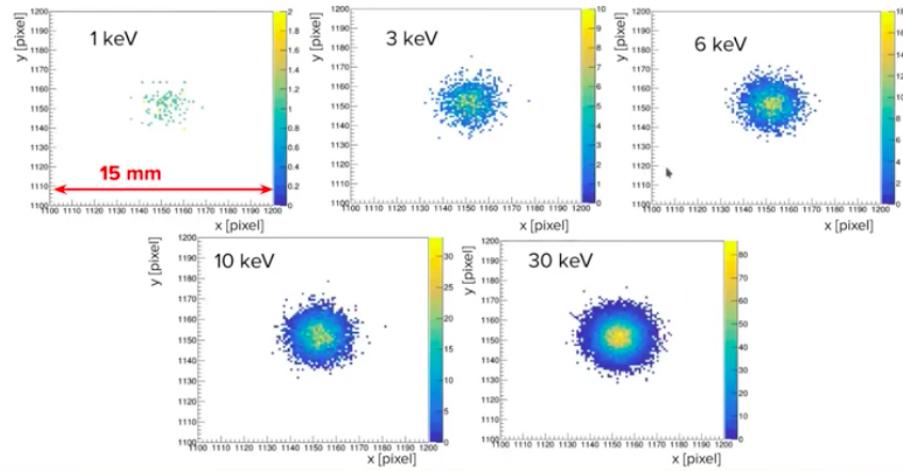


The way the measurement works is as follows. Electrons from the struck nucleus are ionised, and an electric field is applied to the detector such that the electrons move towards the *anode* of the detector. The amount of electrons that reach the anode is proportional to the released energy, which implies we can measure energy deposits and their position in the xy -plane, giving a 2D projection of the particles' track.

Here are some examples of (simulated, cleaned) tracks from electron recoils in the CYGNO experiment:

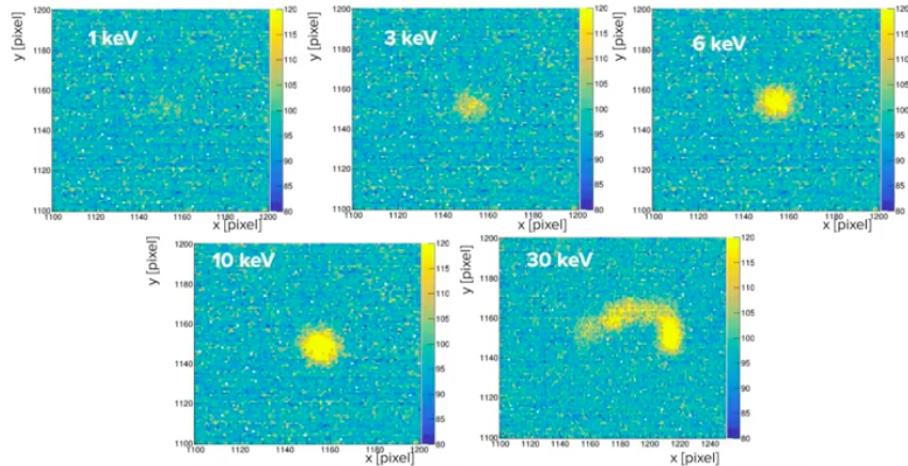


Here are some examples of (simulated, cleaned) tracks from helium recoils in the CYGNO experiment:



As you can see from the figures, there is a somewhat visible difference between electron recoil and helium recoil.

When noise is added, the figures become slightly more complicated:



For smaller energies it can be difficult by eye to even find the track!

The goal of the competition at the school is to devise a machine learning procedure to distinguish between electron recoil (ER) and helium nuclear recoil (NR) in such tracks. The events will have energies ranging from 1 to 30 keV (the most important energy range for dark matter searches, and also the most challenging region for background rejection), together with a random initial angle. There will be precisely one particle for each image in each case.

Part I

Introduction to machine learning

2 Introduction to supervised learning

2.1 Problem setup

Definition 2.1: Consider a set \mathcal{X} of objects and a set of targets \mathcal{Y} . Suppose also that there is an unknown function $f : \mathcal{X} \rightarrow \mathcal{Y}$ mapping objects into targets (which may be stochastic - by which we mean the objects and targets are drawn from some joint probability distribution).

A *dataset* is a finite collection $D = \{(x_i, f(x_i)) : i = 1, \dots, N\} \subseteq \mathcal{X} \times \mathcal{Y}$. The goal of *supervised learning* is to approximate f given a dataset D (i.e. learn to recover targets from objects).

Example 2.2:

- (i) **Classification of iris flower species.** The objects \mathcal{X} are individual flowers, described by the length and width of their sepals and petals. The targets \mathcal{Y} are the species to which the flowers belong. The mapping $f : \mathcal{X} \rightarrow \mathcal{Y}$ takes a flower to its species (and depends on different shapes of sepals, petals, etc corresponding to the different species). Note this is a *non-deterministic* mapping because the growth of a certain flower is associated with a number of random processes.
- (ii) **Spam filtering.** The objects \mathcal{X} are emails (sequences of characters). The targets are the categories $\mathcal{Y} = \{\text{spam, not spam}\}$. The mapping $f : \mathcal{X} \rightarrow \mathcal{Y}$ tells us whether a particular email $x \in \mathcal{X}$ is spam or not, and is again *non-deterministic* (the style and content can vary from author to author).
- (iii) **CAPTCHA recognition.** The set of objects \mathcal{X} is a set of CAPTCHA images (which are really vectors of pixel level brightness). The set of targets \mathcal{Y} are sequences of characters, relating to the correct word that the CAPTCHA shows. The mapping $f : \mathcal{X} \rightarrow \mathcal{Y}$ is the inverse of the algorithm used to generate the CAPTCHA - this is *almost deterministic*, but depends on the level of distortion (very high distortion can make the map less deterministic).
- (iv) **Particle identification in a HEP experiment.** The objects \mathcal{X} are particles, described by the detector experiments (e.g. track parameters, calorimeter energy, deposit, etc.). The targets \mathcal{Y} are the types of the particles (e.g. electrons, muons, protons, etc.). The mapping $f : \mathcal{X} \rightarrow \mathcal{Y}$ is the inverse of the physical process generating the detector response (by definition, this is a stochastic process).

2.2 Feature types

Typically the objects in our set \mathcal{X} will have some structure.

Definition 2.3: Let \mathcal{X}, \mathcal{Y} be the sets of objects and targets in a supervised learning problem. Suppose that \mathcal{X} is a collection of *tuples*, so that given a dataset $D \subseteq \mathcal{X} \times \mathcal{Y}$, for each $(x_i, f(x_i)) \in D$ we can write x_i as:

$$x_i = (x_i^1, x_i^2, \dots, x_i^d),$$

for some d (which need not be the same for all $x_i \in \mathcal{X}$). We say that x_i^j is a *feature* of the object x_i (note we use the upper index for the *feature*, and the lower index to label the object in the dataset).

Many algorithms require that the *dimensionality* d of the data is the same for all objects. In this case, the dataset can be represented by a *design matrix*:

$$X = \begin{pmatrix} x_1^1 & x_1^2 & \cdots & x_1^d \\ x_2^1 & x_2^2 & \cdots & x_2^d \\ \vdots & \vdots & \ddots & \vdots \\ x_N^1 & x_N^2 & \cdots & x_N^d \end{pmatrix}.$$

The column index corresponds to the features, and the row index corresponds to the position of the object in the dataset.

Example 2.4: Consider the problem of classifying species of irises. In this case, features might include *sepal length*, *sepal width*, *petal length* and *petal width*. In this case, all of the features are real numbers.

Since each flower will have these features, we can describe all objects as 4-tuples, and hence we can organise the data into a $N \times 4$ design matrix.

Definition 2.5: In general, features x_i^j might be of varying natures. We give special names to some common cases:

- *Numeric features* take values in (for example) the real numbers. For example sepal length in the classification of iris species, building height, or particle transverse momentum.
- *Categorical nominal features* take values in a finite set, with no natural ordering. For example colour, city of birth or particle type.
- *Categorical ordinal features* take values in a set equipped with a natural order, for example level of education, age, or particles passing loose, medium or tight selection criteria.
- *Binary features* take values in a set of size 2, for example $\{\text{true}, \text{false}\}$, $\{0, 1\}$, $\{-1, +1\}$.

A natural question that arises in the handling of data is how one might convert a categorical nominal feature into a binary or numeric feature (since binary or numeric features can be more easily handled).

A naïve approach would be to assign each category a number (e.g. red= 1, green= 2, etc). However, this introduces an ordering on the feature, which could have a negative effect on learning algorithms later on.

A better solution is *one-hot encoding*:

Definition 2.6: Let $x_i = (x_i^1, \dots, x_i^{j-1}, x_i^j, x_i^{j+1}, \dots, x_i^d)$ be an object in a dataset, and let x_i^j be a categorical nominal feature for the object, taking values in some finite set S . A *one-hot encoding* replaces the feature x_i^j with $|S|$ binary features $\{x_i^{j,s} : s \in S\}$ obeying:

$$x_i^{j,s} = \begin{cases} 0 & \text{if } x_i^j \neq s, \\ 1 & \text{if } x_i^j = s. \end{cases}$$

The new object then takes the form

$$x_i = (x_i^1, \dots, x_i^{j-1}, x_i^{j,s_1}, \dots, x_i^{j,s_{|S|}}, x_i^{j+1}, \dots, x_i^d),$$

where $s_i \in S$ are the elements of S .

Example 2.7: Suppose x is a categorical nominal feature taking values in the set $\{\text{red, blue, green}\}$. A one-hot encoding of the object is:

$$(x^{\text{red}}, x^{\text{blue}}, x^{\text{green}}),$$

where $x^{\text{red}} = 0$ if $x \neq \text{red}$, 1 if $x = \text{red}$, etc.

For example, $x = \text{red}$ is replaced by $(1, 0, 0)$, whilst $x = \text{green}$ is replaced by $(0, 0, 1)$.

One-hot encoding can also be applied to categorial ordinal features:

Definition 2.8: Let $x_i = (x_i^1, \dots, x_i^{j-1}, x_i^j, x_i^{j+1}, \dots, x_i^d)$ be an object in a dataset, and let x_i^j be a categorical *ordinal* feature for the object, taking values in some finite set S with ordering $<$. Suppose that the elements of S are ordered as $s_1 < s_2 < \dots < s_{|S|}$. A *one-hot encoding* replaces the feature x_i^j with $|S|$ binary features $\{x_i^{j,s} : s \in S\}$ obeying:

$$x_i^{j,s} = \begin{cases} 0 & \text{if } s < x_i^j, \\ 1 & \text{if } x_i^j \leq s. \end{cases}$$

The new object then takes the form

$$x_i = (x_i^1, \dots, x_i^{j-1}, x_i^{j,s_1}, \dots, x_i^{j,s_{|S|}}, x_i^{j+1}, \dots, x_i^d).$$

Example 2.9: Suppose x is a categorical ordinal feature taking values in the ordered set $\{\text{bachelors, masters, PhD}\}$, with ordering $\text{bachelors} < \text{masters} < \text{PhD}$. A one-hot encoding of the object is:

$$(x^{\text{bachelors}}, x^{\text{masters}}, x^{\text{PhD}}).$$

For example, $x = \text{bachelors}$ is replaced by $(1, 0, 0)$, whilst $x = \text{PhD}$ is replaced by $(1, 1, 1)$.

Note that this *retains* the ordering of the original categorical ordinal feature.

2.3 Learning algorithms

Definition 2.10: Let $\mathcal{X}, \mathcal{Y}, f$ be the respective objects, targets and function of a supervised learning problem. Given a dataset $D = \{(x_i, f(x_i)) : i = 1, 2, \dots, N\} \subseteq \mathcal{X} \times \mathcal{Y}$, a *learning algorithm* \mathcal{A} returns an approximation $\hat{f} = \mathcal{A}(D)$ (which depends on the dataset) to the true function f .

Definition 2.11: The *k nearest neighbours algorithm* can be applied when the features of the objects have some notion of distance (i.e. a *metric*). We then define:

$$\hat{f}(x) = \frac{1}{k} \sum_{i:x_i \in D_x^k} f(x_i),$$

where D_x^k is the set of k objects in the dataset D closest to x .

Example 2.12: Consider a *classification problem* where the target space \mathcal{Y} consists of only two values. In this case the *k* nearest neighbours algorithm approximates the function $f : \mathcal{X} \rightarrow \mathcal{Y}$ by:

$$\hat{f}(x) = \operatorname{argmax}_C \sum_{i:x_i \in D_x^k} 1_{\{f(x_i)=C\}},$$

where $1_{\{f(x_i)=C\}}$ is the relevant indicator function. Note that instead of averaging the target, we take the value of C which maximises the sum, either 0 or 1.

In general, how does one find an algorithm \mathcal{A} giving an approximation $\hat{f} = \mathcal{A}(D)$ to the true mapping function? Many algorithms work by solving an *optimisation task* - namely, minimising a *loss function*:

Definition 2.13: Let $\hat{f} = \mathcal{A}(D)$ be the approximation to the true mapping function for a supervised learning problem $f : \mathcal{X} \rightarrow \mathcal{Y}$, with dataset $D \subseteq \mathcal{X} \times \mathcal{Y}$ given. A *loss function* is a function $\mathcal{L} : \mathcal{Y} \times \mathcal{Y} \rightarrow \mathbb{R}$, chosen to measure the quality of predictions. The *loss* of our approximation at the point $x_i \in \mathcal{X}$ in the dataset is given by $\mathcal{L}(f(x_i), \hat{f}(x_i))$.

Example 2.14: An example of a loss function is *least squares error*, given by $\mathcal{L}(f(x_i), \hat{f}(x_i)) = (f(x_i) - \hat{f}(x_i))^2$, where the target space $\mathcal{Y} = \mathbb{R}$.

Definition 2.15: Given a loss function $\mathcal{L} : \mathcal{Y} \times \mathcal{Y} \rightarrow \mathbb{R}$ for a supervised learning problem, we can obtain an approximation $\hat{f} = \mathcal{A}(D)$ of the true mapping $f : \mathcal{X} \rightarrow \mathcal{Y}$ from a dataset D via *loss minimisation*:

$$\hat{f} = \operatorname{argmin}_{\tilde{f}} \mathbb{E}_{(x_i, f(x_i)) \in D} \mathcal{L}(f(x_i), \tilde{f}(x_i)),$$

where the argmin is taken over all functions $\tilde{f} : \mathcal{X} \rightarrow \mathcal{Y}$, and the notation \mathbb{E} means the expected value of the loss over the dataset (in the case that the mapping is stochastic, this is important).

Example 2.16: An example is *linear regression*, where we take $\mathcal{X} = \mathbb{R}^d$, $\mathcal{Y} = \mathbb{R}$. In this case, the functions \tilde{f} which could constitute possible mappings $\mathcal{X} \rightarrow \mathcal{Y}$ are restricted to simply be *linear functions*, of the form:

$$\tilde{f}_{\mathbf{w}, \mathbf{b}}(\mathbf{x}) = \mathbf{w}^T \mathbf{x} + \mathbf{b}.$$

Given a dataset $D \subseteq \mathcal{X} \times \mathcal{Y}$ of size N , minimising the least squared loss corresponds to determining \mathbf{w}, \mathbf{b} such that:

$$\frac{1}{N} \sum_{i=1, \dots, N} \left(f(x_i) - \hat{f}_{\mathbf{w}, \mathbf{b}}(x_i) \right)^2$$

is minimised.

2.4 Assumptions about data and model complexity

Given no assumptions about a dataset, there are typically infinitely many solutions to a loss minimisation problem. For example, if we wish to interpolate a finite set of points for a one-dimensional function, infinitely many curves will perfectly minimise the loss (defined in this case as the sum of the distances between the curve and the point at each point).

To combat these, we introduce the concept of *test data*:

Definition 2.17: A set of *test data* is an independent dataset drawn from the same population as the dataset used to construct the solution of our loss minimisation problem (this original set is called the *training data*).

We then demand that our expected loss on the whole population (i.e. both the test and training data) is minimised.

Example 2.18: Consider a linear interpolation problem in \mathbb{R}^d which we solve both with the k nearest neighbour algorithm, and with linear regression. Suppose the true dependence is also linear.

It turns out that if we validate our approaches using a test set, the error on the test set for k nearest neighbour and linear regression agree well for lower dimensions d , but k nearest neighbour becomes much worse for larger numbers of dimensions.

This feature is called the *curse of dimensionality* - as the number of dimensions of the feature space grows, the data becomes very sparse, and the k nearest neighbour approach begins to fail. In this case, to keep the error low, the number of training points would have to increase exponentially with the dimension.

The reason we get the distinction is that the two algorithms have different assumptions:

- The k nearest neighbour (kNN) approach assumes that *similar objects have similar targets*.
- The linear regression approach assumes that *targets are linear in features*.

In this case, both assumptions are correct, but linearity is much stronger which allows us to fight the curse of dimensionality.

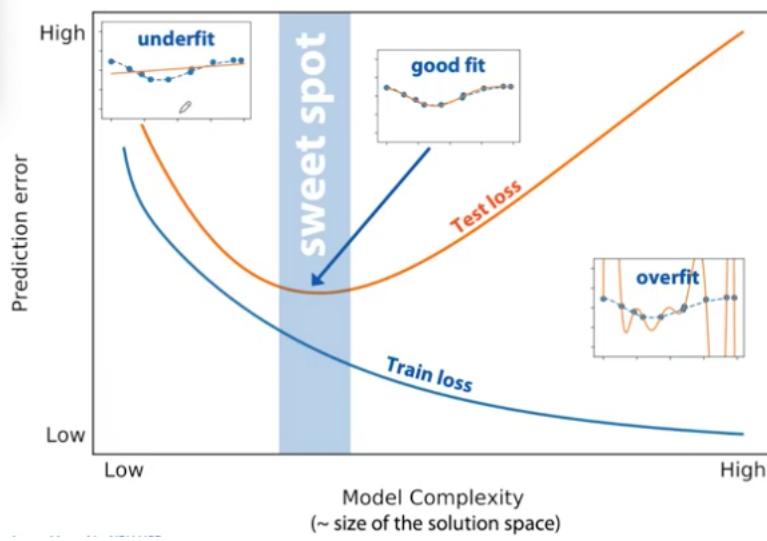
In particular, imposing assumptions about the data *restricts the possible function space of solutions* \tilde{f} for the loss minimisation problem:

$$\hat{f} = \operatorname{argmin}_{\tilde{f}} \mathbb{E}_{(x_i, f(x_i)) \in D} \mathcal{L}(f(x_i), \tilde{f}(x_i)),$$

Linearity is a much stronger constraint than kNN imposes (kNN allows for a much more flexible functional form), restricting the space of functions much more. Sometimes these restrictions help us to *overcome the curse of dimensionality*.

Definition 2.19: The *complexity* of a model refers to the heuristic size of the function space over which we minimise in the loss minimisation problem. A larger complexity means a larger function space, whilst a smaller complexity means a smaller function space.

In general, changing the model complexity can allow us to find the ‘sweet spot’ where expected loss on both the training and test data sets is minimised:



The goal is to find the *right level of limitations* - not too strict, not too loose.

3 Linear models

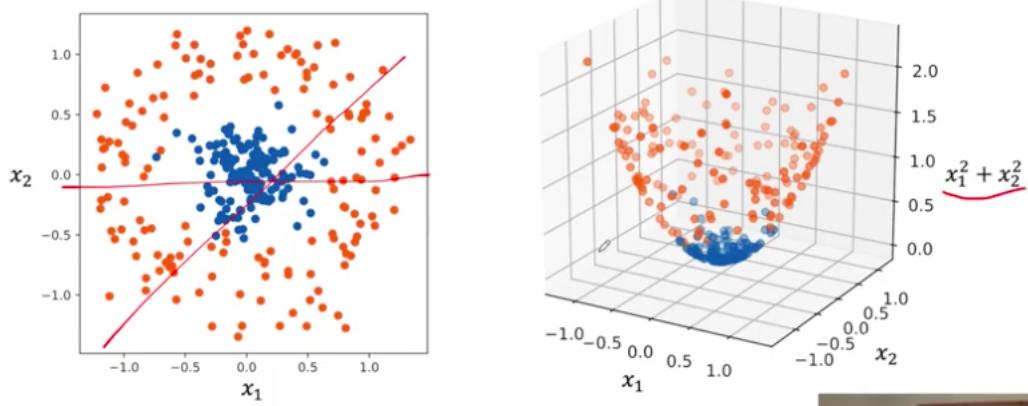
3.1 Linear models and linear regression

Definition 3.1: A *linear model* is a model $\hat{f}(x)$ which is linear in its input (note this assumes a vector space structure on both the objects and targets).

Example 3.2: Examples include:

- Linear regression, for example $\hat{f}(\mathbf{x}) = \boldsymbol{\theta}^T \mathbf{x}$.
- Classification, for example $\hat{f}(\mathbf{x}) = 1_{\{\boldsymbol{\theta}^T \mathbf{x} > 0\}}$. This is non-linear as a function, but divides the target space by a line.

Linear models have a *hidden power*. Problems which appear linearly inseparable (i.e. cannot be solved with linear models) can be made into problems which are tractable with linear models by *transforming the features*. As an example, the data on the left below can be made linearly separable by introducing a new feature based on the sum of the squares of the coordinates of the points:



Now a hyperplane separates the blue and orange sets.

In general, linear models motivate the construction of *deep models*. Neural networks are just linear models with *activation functions* between them (effecting some transformation). Thus better understanding linear models will help us understand deep neural networks.

We have already introduced linear regression as a linear model. Here, we update the notation:

Definition 3.3: The *model prediction* is $\hat{f}_{\boldsymbol{\theta}}(\mathbf{x}) = \boldsymbol{\theta}^T \mathbf{x}$, where $\boldsymbol{\theta} \in \mathbb{R}^d$ is our *parameter vector*, $\mathbf{x} \in \mathcal{X} \subseteq \mathbb{R}^d$ is our *features vector*, and:

$$\frac{1}{N} \sum_{i=1,\dots,N} \left(f(\mathbf{x}_i) - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i) \right)^2$$

is our mean squared error loss, given a dataset. We wish to minimise this over $\boldsymbol{\theta}$.

Other loss functions are available. For example:

- **Mean absolute error (MAE).** This is given by:

$$\frac{1}{N} \sum_{i=1,\dots,N} |f(\mathbf{x}_i) - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)|.$$

This grows linearly for large errors, rather than quadratically like mean squared error loss. In particular, it doesn't penalise large errors as much as mean squared error loss - it might be more suitable if there are outliers in your data which you do not wish to be biased against.

- **Mean absolute percentage error (MAPE).** This is given by:

$$\frac{1}{N} \sum_{i=1,\dots,N} \left| \frac{f(\mathbf{x}_i) - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)}{f(\mathbf{x}_i)} \right|.$$

- **Mean squared logarithmic error (MSLE).** This is given by:

$$\frac{1}{N} \sum_{i=1,\dots,N} (\log(f(\mathbf{x}_i) + 1) - \log(\hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i) + 1))^2.$$

The 1's are there just to allow zero values of the targets.

Both MAPE and MSLE provide a means of computing *relative error*, so are useful when the targets span through a large range of magnitudes.

In general, applying different loss functions are also related to different assumptions about the data. A different loss function might be more suitable to a particular dataset.

3.2 Analytic solution

Recall that earlier we defined the design matrix X , a matrix with rows given by the objects and columns given by the features. We can use this to rewrite the mean squared error loss as:

$$\mathcal{L}_{\text{MSE}} = \frac{1}{N} \sum_{i=1,\dots,N} (f(\mathbf{x}_i) - \boldsymbol{\theta}^T \mathbf{x}_i)^2 = \frac{1}{N} \|\mathbf{y} - X\boldsymbol{\theta}\|^2,$$

where $\mathbf{y} = (f(\mathbf{x}_1), \dots, f(\mathbf{x}_N))^T$.

To minimise this function, we can ignore the $1/N$ as it plays no role. Thus we wish to minimise $\|\mathbf{y} - X\boldsymbol{\theta}\|^2$ over $\boldsymbol{\theta}$. Analytically, the requirements are:

$$\frac{\partial}{\partial \boldsymbol{\theta}} \mathcal{L}_{\text{MSE}} = \mathbf{0}, \quad \text{the matrix } \frac{\partial^2}{\partial \theta_i \partial \theta_j} \mathcal{L}_{\text{MSE}} \text{ of second derivatives should be positive definite.}$$

The first condition ensures we have an extremum, the second condition ensures that extremum is a minimum.

Proposition 3.4: If the columns of X are linearly independent, the solution to the above minimisation problem is $\boldsymbol{\theta} = (X^T X)^{-1} \mathbf{y}$.

Proof: Note that in general, the matrix $X^T X$ is always *positive semi-definite*, since:

$$\mathbf{v}^T X^T X \mathbf{v} = \|X\mathbf{v}\|^2 \geq 0$$

for arbitrary \mathbf{v} . We see it is *precisely* positive definite when the columns of X are linearly independent (imagine the expression $X\mathbf{v}$ to be a linear combination of the columns of X). This additionally implies X is invertible (e.g. all its eigenvalues are positive).

We can now consider the optimisation problem. The first derivative of \mathcal{L}_{MSE} is easily computed:

$$\frac{\partial}{\partial \boldsymbol{\theta}} \mathcal{L}_{\text{MSE}} = \frac{1}{N} \frac{\partial}{\partial \boldsymbol{\theta}} (\mathbf{y} - X\boldsymbol{\theta})^T (\mathbf{y} - X\boldsymbol{\theta}) = -\frac{2}{N} X^T (\mathbf{y} - X\boldsymbol{\theta}) = \mathbf{0}.$$

This implies that $X^T \mathbf{y} - X^T X \boldsymbol{\theta} = \mathbf{0}$. Since $X^T X$ is invertible, we can compute the solution:

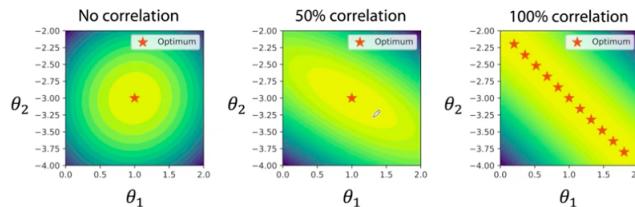
$$\boldsymbol{\theta} = (X^T X)^{-1} X^T \mathbf{y}.$$

To check that this is a minimum, we must look at the second derivative. We find that the matrix of second derivatives is precisely:

$$2X^T X.$$

In particular, this matrix is positive definite by the above. \square

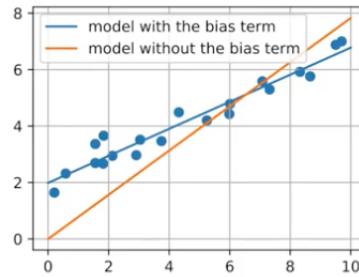
In practice, there may be some linear dependence of the columns of X (i.e. there may be some ‘feature correlations’). This affects the invertibility of the matrix $X^T X$ - we get *flat directions*, and hence multiple solutions to the problem.



In the above we also assumed that our model took the form $\hat{f}_{\theta}(\mathbf{x}) = \boldsymbol{\theta}^T \mathbf{x}$ for ease of calculation, but actually we can consider the more general linear model $\hat{f}_{\theta}(\mathbf{x}) = \boldsymbol{\theta}^T \mathbf{x} + \theta_0$, where the term θ_0 is called the *bias term*. There is no need to redo any calculations here; we simply add a constant feature to the design matrix to account for this:

$$X = \begin{pmatrix} x_1^1 & x_1^2 & \cdots & x_1^d \\ x_2^1 & x_2^2 & \cdots & x_2^d \\ \vdots & \vdots & \ddots & \vdots \\ x_N^1 & x_N^2 & \cdots & x_N^d \end{pmatrix} \rightarrow X = \begin{pmatrix} 1 & x_1^1 & x_1^2 & \cdots & x_1^d \\ 1 & x_2^1 & x_2^2 & \cdots & x_2^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_N^1 & x_N^2 & \cdots & x_N^d \end{pmatrix}$$

Now when we multiply $X\boldsymbol{\theta}$, one of the parameters will play the role of the bias term.



3.3 Numerical and stochastic optimisation: gradient descent

We have now discussed the analytic solution for the mean squared error loss minimisation problem in the context of a linear model. However, most loss functions do not allow an analytic solution, so it is important to discuss numerical solutions.

We begin with some revision of the *gradient*. Recall that the gradient of a scalar function on \mathbb{R}^d is given by:

$$\nabla f(\mathbf{x}) = \left(\frac{\partial f}{\partial x_1}(\mathbf{x}), \dots, \frac{\partial f}{\partial x_d}(\mathbf{x}) \right).$$

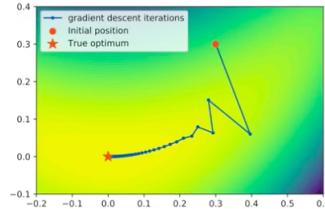
The gradient always points in the *direction of greatest increase* of the function. Hence if we start at a point, and move in the opposite direction to the gradient, we will get closer to a local minimum - this aids optimisation.

Let us formalise this:

Definition 3.5: Given a smooth function $f : \mathbb{R}^d \rightarrow \mathbb{R}$ and an initial point $\mathbf{x}^{(0)}$, we define a recursive sequence of points via:

$$\mathbf{x}^{(k)} = \mathbf{x}^{(k-1)} - \alpha \nabla f(\mathbf{x}^{(k-1)}),$$

where $\alpha \in \mathbb{R}_{>0}$ is a constant called the *learning rate*. This construction is called *gradient descent iteration*.



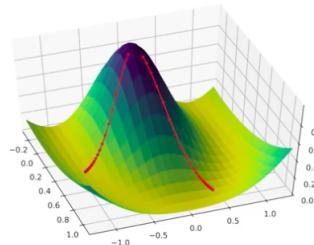
It is possible to show that:

Proposition 3.6: For smooth, *convex* functions with a single minimum $\mathbf{x}^* \in \mathbb{R}^d$, we have:

$$f(\mathbf{x}^{(k)}) - f(\mathbf{x}^*) = O\left(\frac{1}{k}\right),$$

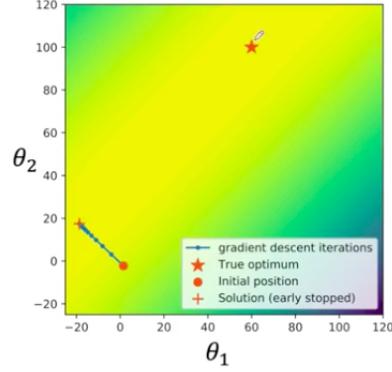
i.e. as we take more and more points, we approach the true minimum of the function.

Gradient descent may also be applied to non-convex functions, but we may reach a minimum which is not *global*, and the result may *depend on the starting point*.



A useful property of gradient descent is that it can be used for *regularisation* when our loss function is ill-defined; for example, when our $X^T X$ matrix above is not invertible (or not stably invertible).

In such cases, the true minimum typically has very large parameter values. These often correspond to *overfitting*. To avoid this, we can start from a point where our initial parameters are *small* and we can stop the gradient descent early (this is called *early stopping*). This will typically be a better solution than the true minimum.



There is an important modification to the gradient descent algorithm called *stochastic gradient descent*. Recall that in machine learning we typically optimise loss functions which are averages over some set of objects:

$$L = \frac{1}{N} \sum_{i=1, \dots, N} \mathcal{L} \left(f(x_i), \hat{f}_\theta(x_i) \right).$$

For large N , gradient descent is computationally inefficient and may be unfeasible in terms of memory consumption. Stochastic gradient descent deals with this problem:

Definition 3.7: Given a function $\hat{f}_\theta : \mathcal{X} \rightarrow \mathcal{Y}$ which depends on a parameter $\theta \in \mathbb{R}^d$, a starting point $\theta^{(0)}$, and a set of objects $x_1, \dots, x_N \in \mathcal{X}$, we define a recursive sequence of points as follows:

- At step k of the process, pick some $l_k \in \{1, \dots, N\}$ at random.
- Define:

$$\theta^{(k)} = \theta^{(k-1)} - \alpha \nabla_\theta \mathcal{L} \left(f(x_{l_k}), \hat{f}_{\theta^{(k-1)}}(x_{l_k}) \right).$$

This is called *stochastic gradient descent iteration*.

In the case of a smooth convex function, stochastic gradient descent also leads you to the unique minimum, but at a slower rate of $O(1/\sqrt{k})$ instead. This *can* be improved by ‘batching’ and other tricks.

3.4 Feature expansion

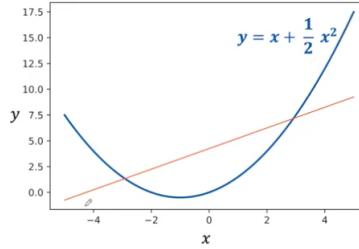
Let us now see how linear models can be made more powerful by transforming their features.

Definition 3.8: Given a design matrix X of dimension $N \times d$, a *feature transformation* via the function $\Phi : \mathbb{R}^d \rightarrow \mathbb{R}^{d'}$ is the induced map of the design matrix:

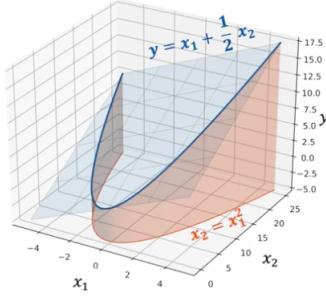
$$X = \begin{pmatrix} x_1^1 & x_1^2 & \cdots & x_1^d \\ x_2^1 & x_2^2 & \cdots & x_2^d \\ \vdots & \ddots & & \vdots \\ x_N^1 & x_N^2 & \cdots & x_N^d \end{pmatrix} \quad \rightarrow \quad \Phi(X) = \begin{pmatrix} \Phi^1(x_1^1, \dots, x_1^d) & \cdots & \Phi^{d'}(x_1^1, \dots, x_1^d) \\ \Phi^1(x_2^1, \dots, x_2^d) & \cdots & \Phi^{d'}(x_2^1, \dots, x_2^d) \\ \vdots & \ddots & \vdots \\ \Phi^1(x_N^1, \dots, x_N^d) & \cdots & \Phi^{d'}(x_N^1, \dots, x_N^d) \end{pmatrix}$$

Finding good functions Φ to transform with is called *feature engineering*. It is an important part of machine learning and requires a deep understanding of the underlying problem and the data.

Example 3.9: (Polynomial features.) Consider trying to fit the curve $y = x + \frac{1}{2}x^2$. This cannot be solved using only linear regression; a single line will not work.



However, we can introduce a new feature via a feature transformation. Let $(x_1, x_2) = (x, x^2)$. Then in the new feature space, a linear estimate is really an estimate of the form $\hat{f}(\mathbf{x}) = \theta_1 x_1 + \theta_2 x_2 = \theta_1 x + \theta_2 x^2$, which facilitates fitting.



Example 3.10: (Polynomial features - general case) Let $(x_i^1, x_i^2, \dots, x_i^d)$ be the original features of a dataset. We introduce as new features all unique multiplicative combinations of the form:

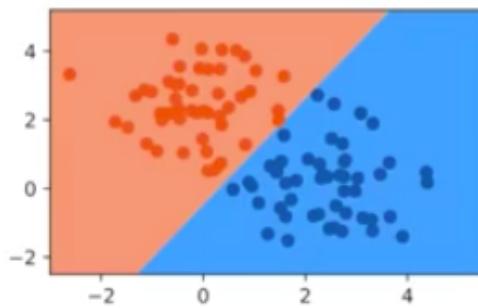
$$(x_i^1)^{p_1} (x_i^2)^{p_2} \cdots (x_i^d)^{p_d},$$

where $p_1 + p_2 + \cdots + p_m \leq p$ (with p the degree we expect to work).

4 Classification with linear models

4.1 Classification with linear regression

Consider a classification problem, with two classes, as shown below:

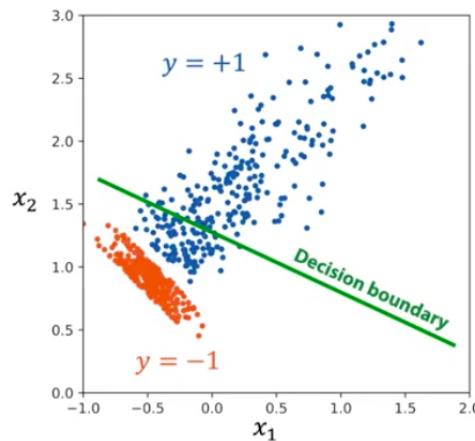


Since there are only two classes, we can assign numeric values to the classes - for our convenience, we choose $y = +1$ for one class (the ‘positive’ class) and $y = -1$ for the other class (the ‘negative’ class)

We can try to predict these targets with a linear model. To do so, we solve a linear regression problem using the model $\hat{y}_\theta(\mathbf{x}) = \theta^T \mathbf{x}$. To obtain the classified function, we then simply take the sign of the result:

$$\hat{f}(\mathbf{x}) = \text{sign}(\hat{y}(\mathbf{x})).$$

This may seem like a reasonable approach, but you can face problems. Consider the following set:



Here, the MSE loss makes the model avoid high errors, at the price of *pushing the decision boundary* towards the class with higher spread.

Therefore, we might try to use a different loss function. A good first example is *0-1 loss*.

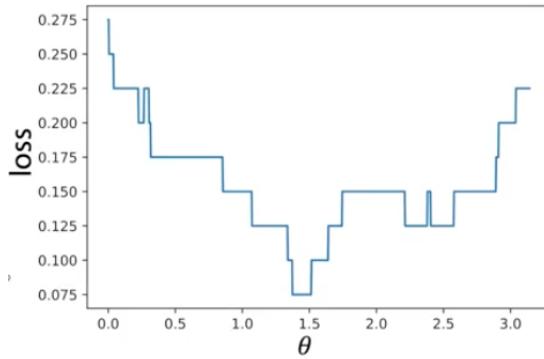
Definition 4.1: For the above classification problem, we define the *0-1 loss* by:

$$\mathcal{L}_{0-1} = \frac{1}{N} \sum_{i=1,\dots,N} 1_{\{\theta^T \mathbf{x}_i y_i < 0\}}$$

where $y_i \in \{-1, +1\}$. We call $M = \theta^T \mathbf{x}_i y_i$ the *margin*. When $M > 0$, we have a *correct* classification, but when $M < 0$ we have an *incorrect* classification. The higher the magnitude of M , the further an object is from the decision boundary.

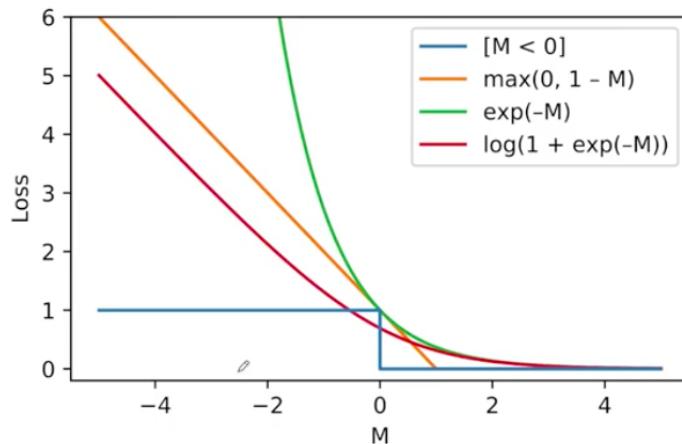
The sum computes the number of times our linear regression misclassifies a point.

Unfortunately, the resulting 0-1 loss function is a piecewise constant function of θ :



This means that we cannot use *gradient descent* to minimise our loss (of course, there are other methods - we will discuss them later).

Instead of using 0-1 loss then, we could replace the sharp 'step' function described by the loss by a *differentiable upper bound*:



Examples are shown in the above figure (the red line can be scaled to be above the step function). We will discuss the red line (*log loss*) in much more detail as we discuss *logistic regression*.

4.2 Logistic regression

Let's depart from the discussion above, and approach things from a different way to start with. Consider modelling the *class probabilities*: we introduce a function $\hat{f}_{\boldsymbol{\theta}}(\mathbf{x})$ that gives the probability of an object \mathbf{x} being in the class $y = +1$, so that:

$$\mathbb{P}(y = +1|\mathbf{x}) = \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}), \quad \mathbb{P}(y = -1|\mathbf{x}) = 1 - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}).$$

How can we optimise such a model? We can fit with the *maximum log likelihood*.

Recall that the *likelihood* is defined by:

$$\text{likelihood} = \prod_{i=1,\dots,N} \mathbb{P}(y_i|\mathbf{x}_i) = \prod_{i=1,\dots,N} \left(1_{\{y_i=+1\}} \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i) + 1_{\{y_i=-1\}} (1 - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)) \right).$$

Maximising the logarithm likelihood allows us to obtain the best values of the parameter $\boldsymbol{\theta}$:

$$\boldsymbol{\theta} = \underset{\boldsymbol{\theta}}{\operatorname{argmax}} \sum_{i=1,\dots,N} \left(1_{\{y_i=+1\}} \log(\hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)) + 1_{\{y_i=-1\}} \log(1 - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)) \right).$$

Note that the indicator functions can be moved out of the logarithm because only one of them is equal to 1 at a time.

Once we have fitted the parameter values, we can for example predict the class the *highest probability* for each $\mathbf{x} \in \mathcal{X}$ in the object space. More generally, we could not just choose the highest probability class but try to use a probability threshold that is suitable for our problem.

Let's try to relate this back to linear models now. We need to ask: how can we map a linear model output to a probability value in $[0, 1]$? A common choice is the *sigmoid function*:

Definition 4.2: The *sigmoid function* is defined by:

$$\sigma(x) = \frac{1}{1 + e^{-x}}.$$

It has the useful property that $1 - \sigma(x) = \sigma(-x)$.

This can be applied to the above example, since we can define:

$$\mathbb{P}(y = +1|\mathbf{x}) = \sigma(\boldsymbol{\theta}^T \mathbf{x}).$$

where $\boldsymbol{\theta}^T \mathbf{x}$ is our linear model. The linear model $\boldsymbol{\theta}^T \mathbf{x}$ then has the meaning of *log odds ratio* between the two classes:

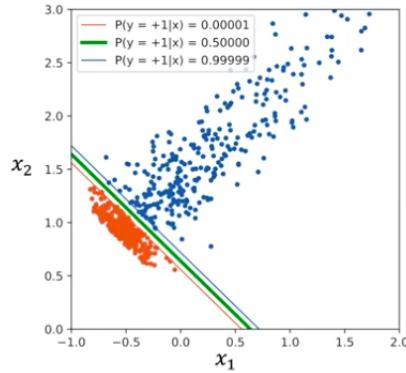
$$\log \left(\frac{\mathbb{P}(y = +1|\mathbf{x})}{\mathbb{P}(y = -1|\mathbf{x})} \right) = \log \left(\frac{1}{1 + e^{-\boldsymbol{\theta}^T \mathbf{x}}} \cdot \frac{1 + e^{-\boldsymbol{\theta}^T \mathbf{x}}}{e^{-\boldsymbol{\theta}^T \mathbf{x}}} \right) = \boldsymbol{\theta}^T \mathbf{x}.$$

Therefore to bring everything together, we use the negative log likelihood as our loss function:

$$\begin{aligned} \mathcal{L} &= - \sum_{i=1,\dots,N} \left(1_{\{y_i=+1\}} \log(\hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)) + 1_{\{y_i=-1\}} \log(1 - \hat{f}_{\boldsymbol{\theta}}(\mathbf{x}_i)) \right) \\ &= - \sum_{i=1,\dots,N} \left(1_{\{y_i=+1\}} \log(\sigma(\boldsymbol{\theta}^T \mathbf{x}_i)) + 1_{\{y_i=-1\}} \log(1 - \sigma(\boldsymbol{\theta}^T \mathbf{x}_i)) \right) \\ &= - \sum_{i=1,\dots,N} \log(\sigma(\boldsymbol{\theta}^T \mathbf{x}_i y_i)) = \sum_{i=1,\dots,N} \log(1 + e^{-\boldsymbol{\theta}^T \mathbf{x}_i y_i}). \end{aligned}$$

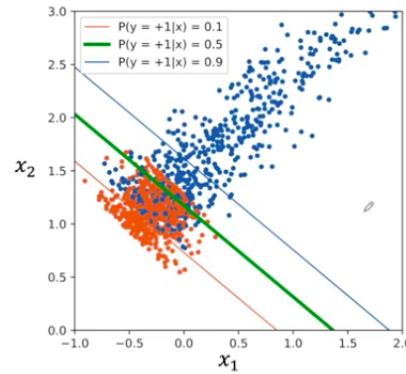
This is the same as the 'red' example we used above when we discussed upper bounds on 0-1 loss. We can apply gradient descent or stochastic gradient descent here.

Applying to the dataset above, the decision boundary is in the correct place with logistic regression:



Note that when the classes are linearly separable as above, for any correct decision boundary, mapping $\theta \rightarrow C \cdot \theta$ for some $C > 1$ keeps the boundary at the same place, yet improves the loss. The ideal fit is when the sigmoid turns into a step function (at infinitely large θ).

If the classes overlap however, the predicted class probability changes smooth, and the loss has a finite minimum.



4.3 Multinomial logistic regression

Similarly to the binary case, we can model the class probabilities when there are more classes than 2. Let's model the *unnormalised* class probabilities as:

$$\tilde{\mathbb{P}}(y = k|\mathbf{x}) = \exp(\boldsymbol{\theta}_k^T \mathbf{x}),$$

where we now have K parameter vectors, $k = 1, \dots, K$. The normalised probabilities can be straightforwardly obtained:

$$\mathbb{P}(y = k|\mathbf{x}) = \frac{\exp(\boldsymbol{\theta}_k^T \mathbf{x})}{\sum_{k'=1, \dots, K} \exp(\boldsymbol{\theta}_{k'}^T \mathbf{x})}$$

This function is called *softmax* and is commonly used in neural networks.

Note that there is a transformational symmetry here: transforming $\boldsymbol{\theta}_k \mapsto \boldsymbol{\theta}_k + \mathbf{v}$ by some constant vector \mathbf{v} does not affect the normalised probability. We have:

$$\tilde{\mathbb{P}}(y = k|\mathbf{x}) = e^{\boldsymbol{\theta}_k^T \mathbf{x}} \rightarrow e^{\mathbf{v}^T \mathbf{x}} \cdot e^{\boldsymbol{\theta}_k^T \mathbf{x}} = e^{\mathbf{v}^T \mathbf{x}} \cdot \tilde{\mathbb{P}}(y = k|\mathbf{x}).$$

The remaining exponential cancels out in the ratio in the normalised probabilities. Therefore, we have some extra degree of freedom, which we are free to choose - we can therefore set $\boldsymbol{\theta}_K = \mathbf{0}$ without loss of generality for example (i.e. we set the last parameter to zero). We are left with $K - 1$ parameter vectors.

Individual linear outputs $\boldsymbol{\theta}_k^T \mathbf{x}$ now have the meaning of *log odds ratio* between the classes k and K :

$$\log \left(\frac{\mathbb{P}(y = k|\mathbf{x})}{\mathbb{P}(y = K|\mathbf{x})} \right) = \log \left(\frac{\tilde{\mathbb{P}}(y = k|\mathbf{x})}{\tilde{\mathbb{P}}(y = K|\mathbf{x})} \right) = \log \left(\frac{e^{\boldsymbol{\theta}_k^T \mathbf{x}}}{e^0} \right) = \boldsymbol{\theta}_k^T \mathbf{x}.$$

Putting everything into the negative log likelihood function, we again get our loss function:

$$\mathcal{L} = - \sum_{i=1, \dots, N} \log \left(\frac{\exp(\boldsymbol{\theta}_{y_i}^T \mathbf{x}_i)}{1 + \sum_{k'=1, \dots, K-1} \exp(\boldsymbol{\theta}_{k'}^T \mathbf{x}_i)} \right),$$

where $\boldsymbol{\theta}_K = \mathbf{0}$. Again, this can be optimised *numerically* using gradient descent or stochastic gradient descent.

4.4 Multiclass classification: general approach

In fact, you are not limited to use logistic regression for multiclass classification - you are able to use any linear model.

For a problem with K classes, introduce K predictors:

$$\hat{f}_k(\mathbf{x}) : \mathcal{X} \rightarrow \mathbb{R}$$

for $k = 1, \dots, K$ each of which outputs a corresponding *class score*. We can use this to predict the class with the *highest score*:

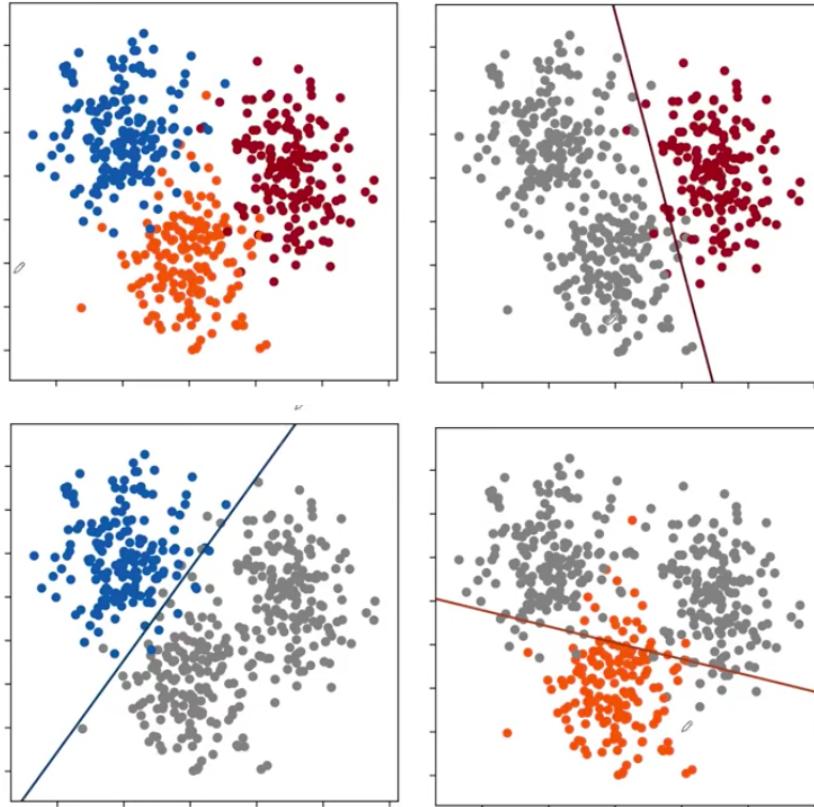
$$\hat{y}_i = \operatorname{argmax}_k \hat{f}_k(\mathbf{x}_i).$$

For example, any binary linear classification model can be converted to a multiclass classification with the *one-versus-rest* strategy:

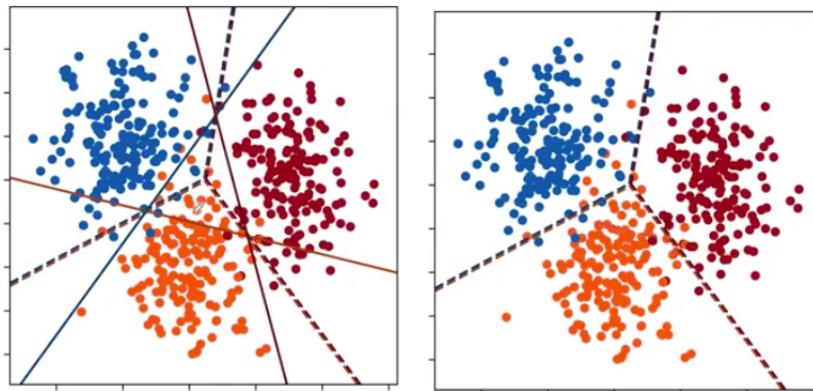
- For each class k train a binary model $\hat{f}_k(\mathbf{x}) = \boldsymbol{\theta}_{(k)}^T \mathbf{x}$ separating the given class from all others, $\hat{y}_{(k)}^{\text{one-vs-rest}} = \operatorname{sign}(\hat{f}_k(\mathbf{x}))$.
- Use the outputs of \hat{f}_k as class scores for multiclass classification:

$$\hat{y}_i = \operatorname{argmax}_k \hat{f}_k(\mathbf{x}_i).$$

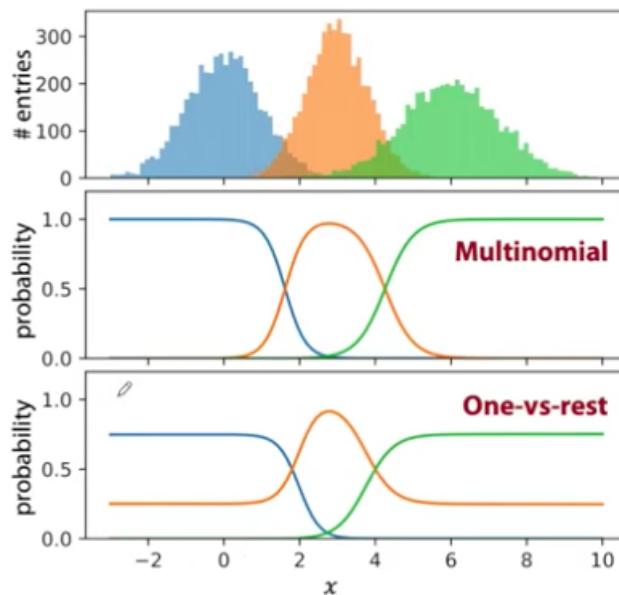
Example 4.3: In the following three-class classification, the one-versus-rest splits given by using the appropriate binary classifiers are shown below:



The resulting decision boundaries can be built up as follows:



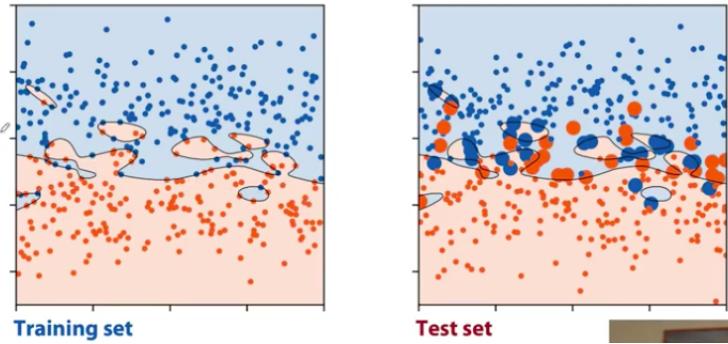
Is the one-vs-rest approach better than multinomial logistic regression however? Some problems are not linearly separable, so one-vs-rest results in biased class probabilities whilst logistic regression is still quite accurate:



5 Model regularisation

5.1 The problem of overfitting

Overfitting is the tendency of a model to adjust to random fluctuations in the data. This can be detected by a model making poor predictions on the *test set*.



Recall that we need to use a model complexity such that we don't underfit, and we don't overfit - we need to find the 'sweet spot' in between.

5.2 Prediction error decomposition

Before talking about regularisation, let's discuss the prediction error of a model. Assume that there's the following unknown relation between features and targets:

$$y = f(x) + \epsilon,$$

where ϵ is some random noise, $\mathbb{E}[\epsilon] = 0$ and $\text{Var}[\epsilon] = \sigma_\epsilon^2$. Let's denote a training set as τ . We want to study the *expected squared error* for the model \hat{f}_τ trained on the dataset τ :

$$\text{exp.sq.err}(x) = \mathbb{E}_{\tau,y} \left[(\hat{f}_\tau(x) - y)^2 | x \right].$$

The target y is sampled independently of the training set.

We can rewrite this expression in the following form, by adding and subtracting the 'prediction of the expected model' and the 'ground truth' $f(x)$ (without the noise):

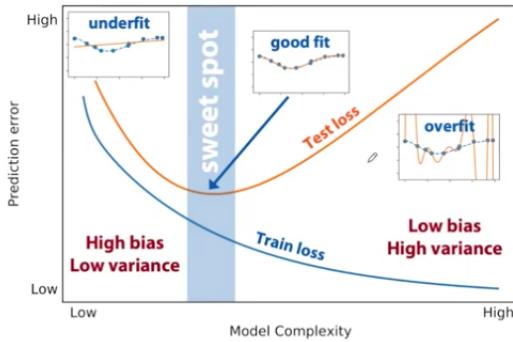
$$\begin{aligned} \text{exp.sq.err}(x) &= \mathbb{E}_{\tau,y} \left[(\hat{f}_\tau(x) - y)^2 | x \right] \\ &= \mathbb{E}_{\tau,y} \left[\left((\hat{f}_\tau(x) - \mathbb{E}_{\tau'}[\hat{f}_{\tau'}(x)]) + (\mathbb{E}_{\tau'}[\hat{f}_{\tau'}(x)] - f(x)) + (f(x) - y) \right)^2 | x \right] \\ &= \mathbb{E}_\tau \left[\left(\hat{f}_\tau(x) - \mathbb{E}_{\tau'}[\hat{f}_{\tau'}(x)] \right)^2 \right] + \left(\mathbb{E}_{\tau'}[\hat{f}_{\tau'}(x)] - f(x) \right)^2 + \mathbb{E}_y[(f(x) - y)^2 | x]. \end{aligned}$$

In the final step, we have expanded everything and used the fact that the cross-term expectation are 0 (this follows from the fact that τ, y are sampled independently).

The remaining terms have important interpretations:

- The first term is the *variance of the model*. It quantifies how ‘unstable’ the model is with respect to the noise in the training data.
- The second term is the *squared bias*. It is how much the ‘expected model’ differs from the ground truth.
- The third term is the *irreducible error*. Substituting the true dependence y , we find it is just given by σ_ϵ^2 . This error cannot be eliminated.

The first two errors on the other hand, can be removed by changing the model. Typically there’s a *tradeoff* between the two types of errors:



For low model complexity, the *bias* is high because we are artificially simplifying the model - it doesn’t depend much on the data (it has ‘low variance’). The opposite is true for high model complexity. This tradeoff is called the *bias-variance tradeoff*.

Example 5.1: Let’s compute the bias and variance of a linear model. For each expectation \mathbb{E} with respect to τ , we will assume that the features are *fixed*, i.e. $X_\tau = X$ (i.e. the design matrix is constant), and only the target vector y_τ is random. This simplification allows us to analytically compute the result.

Recall the solution for the linear regression model with the MSE loss:

$$\hat{f}_\tau(\mathbf{x}) = \boldsymbol{\theta}_\tau^T \mathbf{x}, \quad \boldsymbol{\theta}_\tau = (X^T X)^{-1} X^T \mathbf{y}_\tau.$$

The *bias term* from the above error decomposition is:

$$\text{bias}(\mathbf{x}) = \mathbb{E}_\tau[\hat{f}_\tau(\mathbf{x})] - f(\mathbf{x}) = \mathbb{E}_\tau[\mathbf{x}^T (X^T X)^{-1} X^T \mathbf{y}_\tau] - \mathbf{x}^T \boldsymbol{\theta}_{\text{true}}$$

We also assume that the true dependence is indeed linear, i.e. $f(\mathbf{x}) = \mathbf{x}^T \boldsymbol{\theta}_{\text{true}}$ for some $\boldsymbol{\theta}_{\text{true}}$.

Since X does not depend on the sampling dataset τ , we can move lots of things out of the expectation, leaving:

$$\mathbf{x}^T (X^T X)^{-1} X^T \mathbb{E}_\tau[\mathbf{y}_\tau - \mathbf{x}^T \boldsymbol{\theta}_{\text{true}}] = \mathbf{x}^T (X^T X)^{-1} X^T X \boldsymbol{\theta}_{\text{true}} - \mathbf{x}^T \boldsymbol{\theta}_{\text{true}} = \mathbf{x}^T \boldsymbol{\theta}_{\text{true}} - \mathbf{x}^T \boldsymbol{\theta}_{\text{true}} = 0.$$

Hence we see that the linear regression model is *unbiased*, provided the true dependence is linear.

Now let's consider the *variance term*:

$$\text{variance}(\mathbf{x}) = \mathbb{E}_{\tau} \left[\left(\hat{f}_{\tau}(\mathbf{x}) - \mathbb{E}_{\tau'}[\hat{f}_{\tau'}(\mathbf{x})] \right)^2 \right].$$

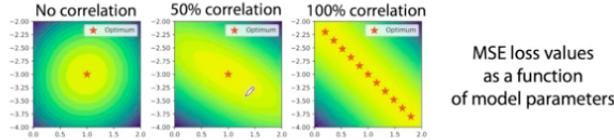
It can be shown that:

$$\text{variance}(\mathbf{x}) = \sigma_{\epsilon}^2 \mathbf{x}^T (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{x},$$

so that the variance error component is a *quadratic form*, defined by the $(\mathbf{X}^T \mathbf{X})^{-1}$ matrix. We can diagonalise $\mathbf{X}^T \mathbf{X}$ giving:

$$\text{variance}(\mathbf{x}) = \sigma_{\epsilon}^2 \tilde{\mathbf{x}}^T \Lambda^{-1} \tilde{\mathbf{x}},$$

where $\Lambda = \text{diag}\{\lambda_1, \dots, \lambda_d\}$ is the diagonal matrix of eigenvalues of $\mathbf{X}^T \mathbf{X}$. This means that *small eigenvalues amplify the model variance*. This happens when $\mathbf{X}^T \mathbf{X}$ is ill-defined, e.g. when the features are correlated.



In a high variance model, we expect that a small perturbation data will lead to a large change in the prediction.

5.3 Regularisation

How can we reduce the variance of a model? If only we could *increase the eigenvalues* of the matrix $\mathbf{X}^T \mathbf{X}$. In fact, we can do this manually:

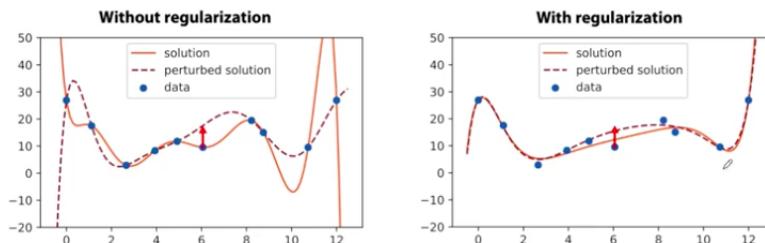
$$\mathbf{X}^T \mathbf{X} \rightarrow \mathbf{X}^T \mathbf{X} + \alpha I,$$

for $\alpha > 0$, with I a unit $d \times d$ matrix. This is called *L2 regularisation*.

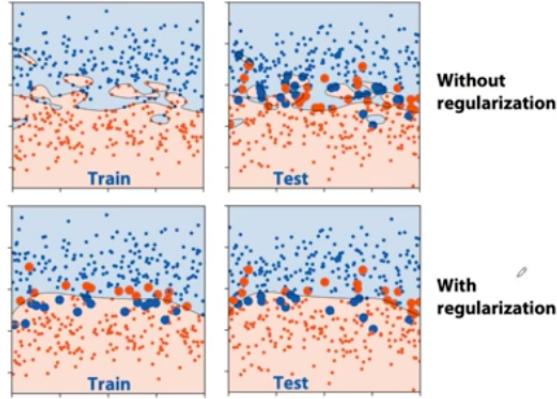
In this case, we change the solution to:

$$\hat{f}_{\tau}(\mathbf{x}) = \mathbf{x}^T (\mathbf{X}^T \mathbf{X} + \alpha I)^{-1} \mathbf{X}^T \mathbf{y}_{\tau}.$$

Now the model is *no longer biased*. We increased bias to reduce variance (we no longer get zero for the bias term of this model).



By regularising the model, we increase the training loss and decrease the test loss. This improves the *generalisability* of the model.



In order to understand this trick better, let's reverse engineer the loss function it optimises. We have the solution $\hat{f}_\tau(\mathbf{x}) = \mathbf{x}^T (X^T X + \alpha I)^{-1} X^T \mathbf{y}_\tau$, so the $\boldsymbol{\theta}_\tau$ vector should be given by:

$$\boldsymbol{\theta}_\tau = (X^T X + \alpha I)^{-1} X^T \mathbf{y}_\tau.$$

Regrouping the terms, we have:

$$(X^T X + \alpha I) \boldsymbol{\theta}_\tau = X^T \mathbf{y}_\tau \quad \Rightarrow \quad X^T (X \boldsymbol{\theta}_\tau - \mathbf{y}_\tau) + \alpha \boldsymbol{\theta}_\tau = \mathbf{0}.$$

In fact, this is the equation $\partial \mathcal{L} / \partial \boldsymbol{\theta}_\tau = \mathbf{0}$ for the loss function:

$$\mathcal{L} = \|X \boldsymbol{\theta}_\tau - \mathbf{y}_\tau\|^2 + \alpha \|\boldsymbol{\theta}_\tau\|^2.$$

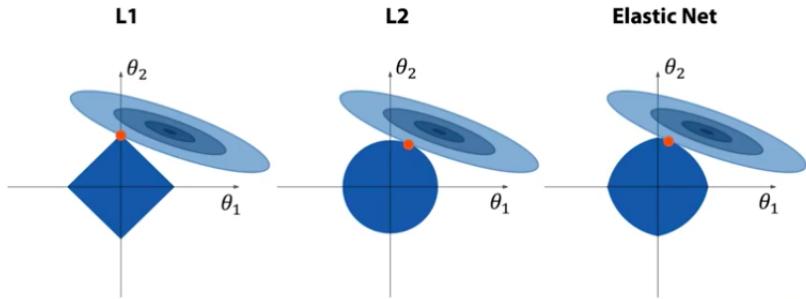
This explains the origin of the term *L2 regularisation*. The model minimises the MSE loss with an *L2 penalty theorem* (this model is also called *ridge regression*).

There are other similar regularisation methods:

- *L2 regularisation* or *ridge regression* takes as the loss function $\mathcal{L} = \|X \boldsymbol{\theta}_\tau - \mathbf{y}_\tau\|^2 + \alpha \|\boldsymbol{\theta}_\tau\|^2$.
- *L1 regularisation* or *lasso regularisation* takes as the loss function $\mathcal{L} = \|X \boldsymbol{\theta}_\tau - \mathbf{y}_\tau\|^2 + \alpha \|\boldsymbol{\theta}_\tau\|_1$ (where $\|\cdot\|_1$ denotes the *L1 norm*).
- *Elastic net regression* is a combination of the two:

$$\mathcal{L} = \|X \boldsymbol{\theta}_\tau - \mathbf{y}_\tau\|^2 + \alpha \|\boldsymbol{\theta}_\tau\|^2 + \beta \|\boldsymbol{\theta}_\tau\|_1.$$

The introduction of regularisation methods drive the parameters towards smaller values, yet they *induce different properties* of the solution.



For example, the L_1 regularisation term has unit ball given by a diamond in θ_1, θ_2 space (i.e. the surface where $\|\theta\|_1 = 1$). It's quite likely that among all the points at the perimeter of the diamond (where the penalty term does not change), the intersection is most likely at the coordinate axes. This means that this loss tends to *sparsify the solution* - it tends to set some parameters to zero.

For the L_2 regularisation, we instead have *weight sharing* - it uniformly drags the values of the parameters towards zero.

The elastic net is a compromise between the two approaches.

5.4 Probabilistic view

Let's revisit our assumption about the data, $y = f(x) + \epsilon$. Let's now assume that the label noise is *normally distributed*, $\epsilon \sim \mathcal{N}(0, \sigma_\epsilon^2)$. This means that the targets, given the objects, are also normally distributed:

$$y|x \sim \mathcal{N}(f(x), \sigma_\epsilon^2).$$

We want our model $\hat{f}_\theta(x)$ to fit the true dependence $f(x)$, i.e. we define a *probabilistic model*:

$$y|x \sim \mathcal{N}(\hat{f}_\theta(x), \sigma_\epsilon^2),$$

where the mean of the normal distribution is described by our function.

Our model can be fitted with the maximum likelihood approach:

$$L = \prod_{i=1,\dots,N} \mathcal{N}(y_i | \hat{f}_\theta(x_i), \sigma_\epsilon^2).$$

Maximising this with respect to θ is equivalent to minimising the negative log likelihood,

$$\begin{aligned} -\log(L) &= \sum_{i=1,\dots,N} \log(\mathcal{N}(y_i | \hat{f}_\theta(x_i), \sigma_\epsilon^2)) = - \sum_{i=1,\dots,N} \left[\log \left(\exp \left(-\frac{(y_i - \hat{f}_\theta(x_i))^2}{2\sigma_\epsilon^2} \right) \right) - \log(\sqrt{2\pi}\sigma_\epsilon^2) \right] \\ &= C \cdot \sum_{i=1,\dots,N} (y_i - \hat{f}_\theta(x_i))^2 + \text{constant}. \end{aligned}$$

Thus we just get MSE loss! Thus MSE loss is equivalent to modelling the probability with a normal label noise.

You can do similar tricks for other loss functions and show that different probabilistic models lead to different loss functions.

5.5 Bayesian view

In the Bayesian view, we treat both data (X, y) and model parameters (θ) as random variables. We estimate the parameter distribution given the observed data via Bayes' rule:

$$p(\theta|X, y) = \frac{p(y|\theta, X)p(\theta)}{\int (p(y|\theta, X)p(\theta)) d\theta}$$

We assume that θ, X are independent variables here. Here, $p(\theta)$ is our prior knowledge about the model parameters (our belief about how they are distributed before we see any data). The function $p(y|\theta, X)$ is our likelihood function. The distribution $p(\theta|X, y)$ is called the *posterior distribution*, and is our knowledge about the model after seeing data. The denominator is called 'evidence' (the probability of observing the data when the parameter uncertainty is integrated out).

To get some estimate of the parameter, we can calculate the *maximum a posteriori* (where we ignore the denominator since it is integrated over θ - the maximum is the same as the maximum of the numerator):

$$\hat{\theta} = \operatorname{argmax}_{\theta} p(y|\theta, X)p(\theta) = \operatorname{argmin}_{\theta} [-\log(p(y|\theta, X)) - \log(p(\theta))]$$

Similarly, the maximum is the same as the minimum negative log likelihood. The term $\log(p(\theta))$ is called a *regularising term*.

Example 5.2: Suppose we model the data with a normal distribution $y|x \sim \mathcal{N}(\hat{f}_\theta(x), \sigma_\epsilon^2)$. Suppose the prior is normal too $\theta \sim \mathcal{N}(0, \sigma_\theta^2 I)$, where I is the unit matrix so that the parameters are uncorrelated. Then maximum a posteriori estimate corresponds to minimising the following loss:

$$\mathcal{L} = -\log(p(y|\theta, X)) - \log(p(\theta)) = C_1 \sum_{i=1, \dots, N} (\hat{f}_\theta(x_i) - y_i)^2 + C_2 \|\theta\|^2 + \text{constant.}$$

In other words a normal prior is equivalent to *L2* regularisation of the parameters.

Choosing different priors will lead to different regularisation of the parameters.

6 Quality metrics for regression and classification

6.1 Quality metrics for regression models

Consider a dataset described by design matrix X and target values \mathbf{y} , and a linear regression model:

$$\hat{\mathbf{y}} = X\mathbf{w},$$

where \mathbf{w} are the parameters (weights) of the model (previously denoted as θ). Our goal is to *measure the quality* of this model - in other words, estimate how close predictions $\hat{\mathbf{y}}$ are to the real target values. This is measured by a *loss function*, also called a *quality metric* in this section of the course.

We have already seen some examples of quality metrics: for example, mean squared error (MSE) and mean absolute error (MAE). Sometimes MSE is replaced by *root mean squared error* (RMSE):

$$\sqrt{\frac{1}{N} \sum_{i=1}^N (\hat{y}_i - y_i)^2}.$$

With these metrics, it can be hard to tell if a model is good: for example, if RMSE = 1, the model quality can be different for mean target values of $\bar{y} = 100$ and $\bar{y} = 1$.

Another popular metric is MAPE, which we also saw before. It is defined by:

$$\frac{100}{N} \sum_{i=1}^N \left| \frac{\hat{y}_i - y_i}{y_i} \right|.$$

It measures the relative error of the prediction. It is easy to understand the quality of the model, but it is sensitive to the y scale.

Two other quality metrics are:

- **Relative square error (RSE).** This is given by:

$$\sqrt{\frac{\sum_{i=1}^N (y_i - \hat{y}_i)^2}{\sum_{i=1}^N (y_i - \bar{y})^2}}.$$

This metric measures how the average square error differs from the squared standard deviation of the real target values.

- **Relative absolute error (RAE).** This is given by:

$$\frac{\sum_{i=1}^N |y_i - \hat{y}_i|}{\sum_{i=1}^N |y_i - \bar{y}|}.$$

Similarly, this metric measures how the average absolute error of the model differs from the median value of the real target values.

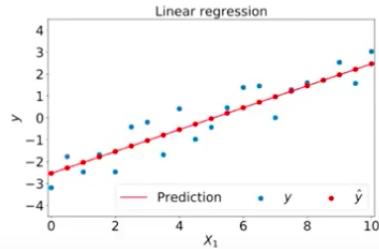
The main advantage of these metrics is that they are robust to the scale of the target values y .

The final quality metric we will consider is *root mean squared logarithmic error* (RMSLE), which we also saw before:

$$\sqrt{\frac{1}{N} \sum_{i=1}^N (\log(y_i + 1) - \log(\hat{y}_i + 1))^2}.$$

It is similar to root mean square error, but uses logarithmic values instead. It is used in cases when the target changes by several orders of magnitude - in such cases, the other quality metrics will measure quality less accurately.

Example 6.1: Consider the linear regression shown below:

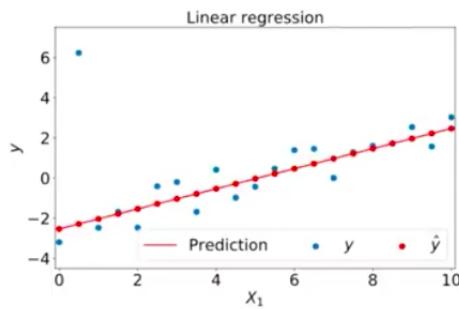


Computing all of the quality metrics in this case, we have:

Metric	No outliers
RMSE	0.67
MAE	0.59
MAPE, %	1035
RSE	0.39
RAE	0.40

Note that MAPE fails because of the y scale, and the fact that some y_i are close to zero.

Now consider adding a single outlier to the dataset:



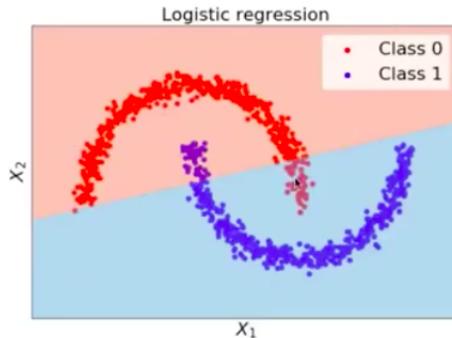
The outlier significantly affects the metrics:

Metric	No outliers	With outlier
RMSE	0.67	1.93 [↑]
MAE	0.59	0.96
MAPE, %	1035	1040
RSE	0.39	0.92
RAE	0.40	0.58

However, we note that MAE and RAE are the most robust against the addition of the outlier.

6.2 Quality metrics for classification models

Consider a binary classification problem with a data sample and a classifier (into two classes ‘positive’ and ‘negative’), as shown in the figure. We use a logistic regression model to find the decision boundary.



The goal is to measure the quality of the classifier, i.e. to estimate how well it separates objects of different classes.

To measure the model's quality, we introduce a *confusion matrix*:

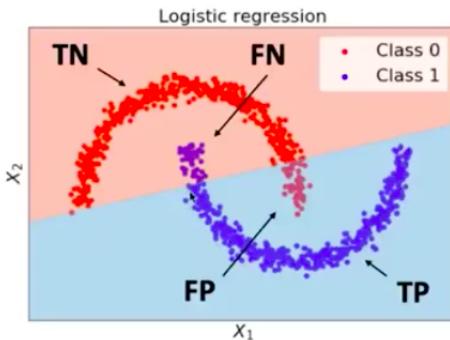
Definition 6.2: A *confusion matrix* is a matrix of the form:

$$\begin{pmatrix} \text{TP} & \text{FN} \\ \text{FP} & \text{TN} \end{pmatrix}.$$

The element TP represents the number of objects which are positive and are correctly predicted as positive (*true positives*). The element FN represents the number of objects which are positive and are incorrectly predicted as negative (*false negatives*).

The element FP represents the number of objects which are negative and are incorrectly predicted as positive (*false positives*). The element TN represents the number of objects which are negative and are correctly predicted as negative (*true negatives*).

In the example above, we have the following assignments:



We also define some additional quantities:

- The number of all positives is Pos = TP + FN.
- The number of all negatives is Neg = TN + FP.
- The number of all positive predictions is PosPred = TP + FP.
- The number of all negative predictions is NegPred = TN + FN.

Using these quantities, we can define different quality metrics. The first metric we define is *accuracy*:

Definition 6.3: The *accuracy* of a classifier is defined by:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{TN} + \text{FP}} = \frac{\text{TP} + \text{TN}}{\text{Pos} + \text{Neg}}.$$

A complementary quality metric is *error rate*, defined by:

$$\text{Error rate} = 1 - \text{Accuracy}.$$

These metrics are symmetric and measure quality of classification of both classes equally.

Other metrics measure how well a classifier identifies positive objects only (i.e. they are asymmetric). Examples include:

Definition 6.4:

- *Precision* of a classifier is defined by:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} = \frac{\text{TP}}{\text{PosPred}}.$$

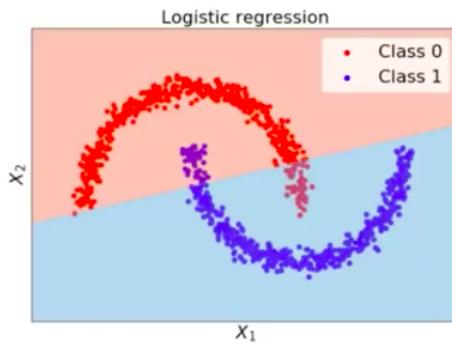
- *Recall* of a classifier is defined by:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} = \frac{\text{TP}}{\text{Pos}}.$$

- The F_1 -score of a classifier is the harmonic mean of precision and recall, defined by:

$$F_1 = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}.$$

Example 6.5: Consider the classifier example we showed at the start of this section:



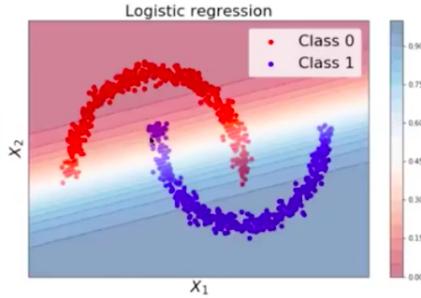
Computing all of the above metrics on this example, we find:

Metric	Value
Accuracy	0.89
Precision	0.89
Recall	0.89 ⁱ
F_1	0.89

All them metrics give the same value in this case, because of the symmetry of the problem. Later we will see other cases.

Recall that when we did classification problems with logistic regression earlier, we could also have based our ideas on *probabilities*. If an object has a probability p of being in the positive class, we predict it to have value 1 if $p \geq 0.5$ and value 0 if $p < 0.5$.

The probability in the above example is distributed as a gradient instead of a hard cutoff like the decision boundary:



We can use these probabilities to define quality metrics.

Definition 6.6: The *receiver operating characteristic curve* (ROC curve) is a curve relating the *true positive rate* $\text{TPR}(\mu)$ and the *false positive rate* $\text{FPR}(\mu)$ for different ‘thresholds’ μ of the predicted probabilities p . We make the following definitions first:

- The *true positive rate* is defined by:

$$\text{TPR}(\mu) = \frac{1}{\text{Pos}} \sum_{i \in \text{Pos}} 1_{\{p_i \geq \mu\}} = \frac{\text{TP}(\mu)}{\text{Pos}},$$

where $\text{TP}(\mu)$ is the number of true positives which have predicted probability of being positive greater than μ .

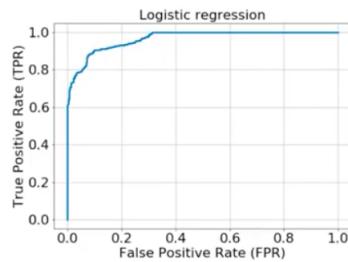
- The *false positive rate* is defined by:

$$\text{FPR}(\mu) = \frac{1}{\text{Neg}} \sum_{i \in \text{Neg}} 1_{\{p_i \geq \mu\}} = \frac{\text{FP}(\mu)}{\text{Neg}},$$

where $\text{FP}(\mu)$ is the number of false positives which have predicted probability of being positive greater than μ .

The ROC curve is the curve in the TPR, FPR plane parametrised by the threshold μ .

Example 6.7: For our example above, with the ‘gradient of probabilities’ shown in the figure, the ROC curve looks like:

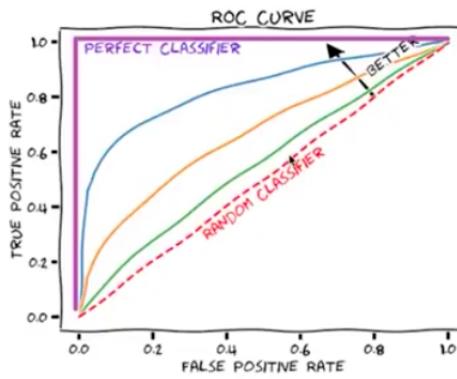


In high energy physics, we very often plot dependency of *background reduction* from *signal efficiency*. In this case, *signal efficiency* is to be interpreted as the true positive rate and *background reduction* is to be interpreted as one minus the false positive rate. The resulting curves are very similar to the ROC curve.

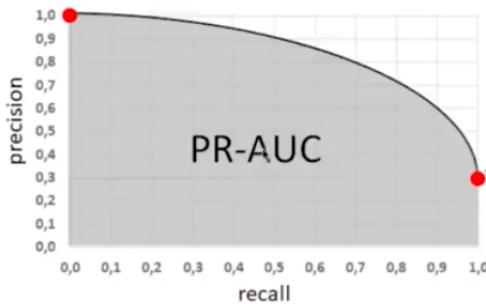
Next, we should comment on the interpretation of the ROC curve. The quality of a classifier is related to *area under the ROC curve*.

Definition 6.8: We define the quality metric ROC AUC to be the *area under the ROC curve*. We note that:

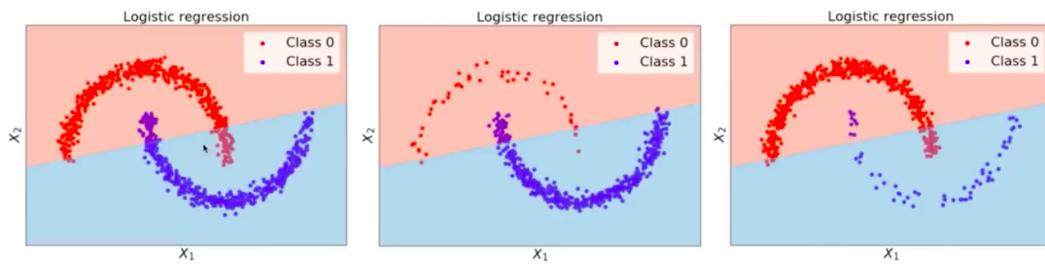
- $\text{ROCAUC} \in [0, 1]$.
- $\text{ROCAUC} = 0.5$ corresponds to random guessing.
- $\text{ROCAUC} = 1$ means ideal classification.
- $\text{ROCAUC} = 0$ also means ideal classification, but for opposite labels!



Similarly to the ROC curve, we can also define a *precision-recall curve* (PR), the curve with coordinates $(\text{Recall}(\mu), \text{Precision}(\mu))$ as the probability threshold μ is varied. This also induces a quality metric using the area under the curve (PR AUC).



Example 6.9: We can investigate each of these quality metrics by *fixing a model* but *changing the class balance* in the test sample. Let's choose to make the balances 1 : 1, 1 : 10 and 10 : 1 as shown below:



The resulting quality metrics are given by:

Metric	1:1	1:10	10:1
Accuracy	0.89	0.89	0.89
Precision	0.89	0.99	0.47
Recall	0.89	0.89	0.89
F_1	0.89	0.94	0.61
ROC AUC	0.97	0.97	0.97

With the class balance changing, some metrics change. We note that:

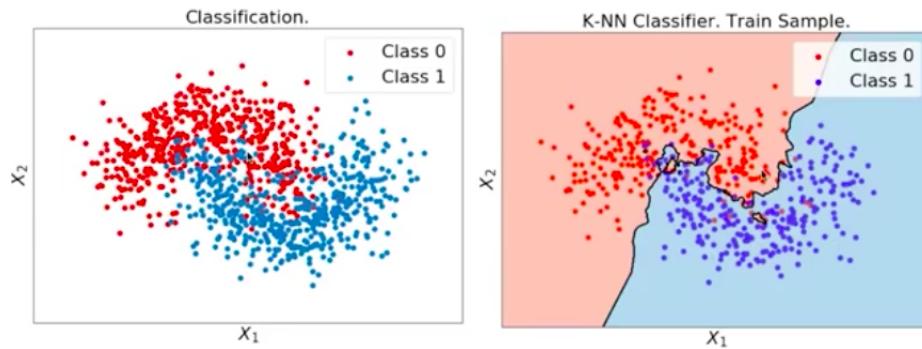
- Recall and ROC AUC do not change with the class balance changing. This is a general feature.
- Accuracy did not change with the class balance changing - however, this isn't true in general.

7 Model tests

7.1 Train/test split

We have already discussed the need for splitting our data into a training set and a test set. This is a quick reminder of how we can use this in regression and classification.

Example 7.1: Consider a binary classification problem. We randomly divide our data into two equal samples: *train* and *test*. We use the train sample to fit a classifier.



Note that in our case, the fitted model has quite an irregular decision boundary - this suggests that some overfitting has taken place, and the model may not be very generalisable.

After fitting the model, we can evaluate quality metrics on both the train and test sets. We find:

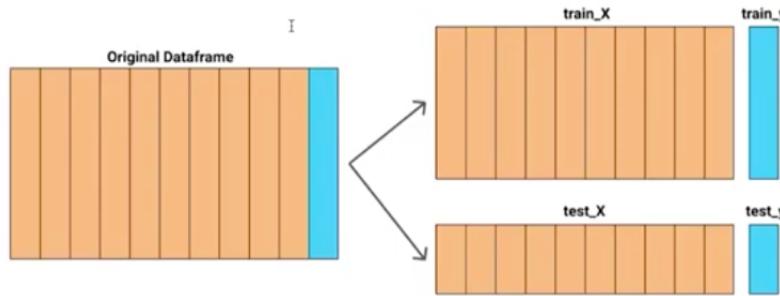
Metric	Train	Test
Accuracy	0.93	0.89
Precision	0.92	0.90
Recall	0.95	0.88
F_1	0.93	0.89
ROC AUC	0.99	0.94

The values on the training set are greater than on the test set. The reason that this has occurred is that the classifier has learned the training sample specifics, i.e. it has *overfitted*.

As a result, the quality metrics are larger on the training set, but since these specifics are *not* properties of the classes, they are not observed in the test sample - thus the classifier makes more mistakes on the test set, and the quality metrics are smaller on that set.

As a general rule: the larger differences between the metrics on the train and test set, the greater the extent of model overfitting.

Let's consider train/test splits in general. We would like to divide our original dataset (written as (X, y) where X is our design matrix and y is our tuple of predictions) into a train set (used to fit and tune a model) and a test set (used to measure the quality of the model).



We can then tune *hyperparameters* in our model, for example coefficients in some regularisation method, refit the model on the training and measure its quality on the test. Overall our aim is to increase quality on the test.

How do we come up with a strategy for dividing data between a train and test set? In general we do the following:

- Data is divided between the train and test *randomly* to ensure distributions on the train and test are similar.
- Usually we take the train size greater than or equal to the test size. Typical proportions include 1 : 1 or 2 : 1.
- The larger the training size, the better the model will fit. However, if the test size is larger, our quality measurements on the test set will be more accurate.
- The test size can also be *estimated* based on a desired acceptable uncertainty of the quality metrics.

In general, a large part of the data is not used for the model fit. This might be crucial for small dataset.

Even when we have a train/test split, if we turn our model too long using the same *test* sample, we can find values of the model's hyperparameters such that we *overfit* on the *test* set! To prevent this, we can split our data into *train*, *validation* and *test* sets.

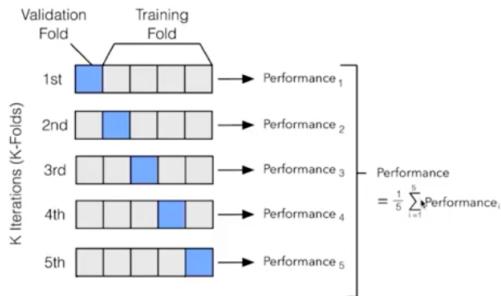


As before, the *train* set is used to fit and tune the model. The *validation* set is used to measure the quality of the model during its tuning when we are searching for the best hyperparameter values. The *test* set is used only for the final quality measurement (after tuning). This quality is considered the quality of the model.

7.2 Cross-validation methods

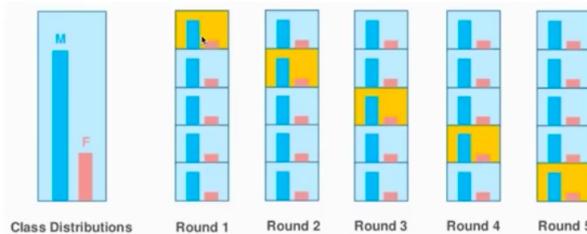
We will now discuss various methods of *cross-validation*. The first we consider is *k-folding*.

Definition 7.2: In the method of *k-folding*, the dataset is split into k parts, or k ‘folds’. One fold is used to measure quality of the model (as a *validation set*), whilst the other $k - 1$ folds are used to train the model. This procedure is repeated k times, and the average quality metric on the validation sets is computed to estimate the final quality; we can also collect the standard deviation of the quality metrics (or different confidence levels for example).



The main disadvantage of this procedure is that it is very time-consuming - it requires fitting the model k -times. Typical numbers of folds are around 5-10.

A useful modification is *stratified k-folding*. This works exactly the same as normal *k*-folding, but when the folds are created, the *same* class balance is used across all folds. This method is useful when we have large class imbalances and small datasets.



An extreme case of *k*-folding is *leave one out* cross-validation. This is *k*-folding where the number of folds is equal to the size of the dataset, and can be useful for very small sample sizes.



In detail, consider a sample with N objects. For N iterations, remove the i th object from the sample, and fit the model using the remaining $N - 1$ objects. Using the model, make a prediction for the i th object and save it. Collect all predictions and measure the quality of the model.

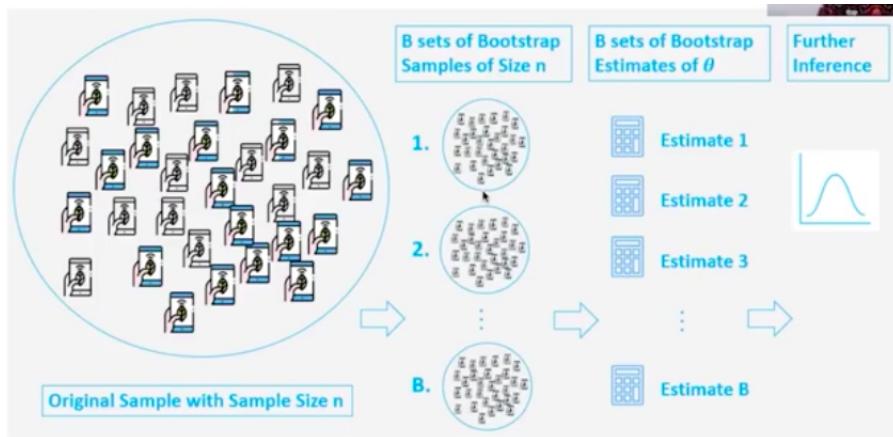
Note that the models from each iteration will be approximately the same (since we hardly change the dataset). Therefore, the predictions will demonstrate a very small variance.

Yet another similar approach is *leave p out* cross-validation. Here, we simply remove p randomly selected objects instead of one, for each iteration. As a result, fewer iterations are required.



The *bootstrap method* is described as follows:

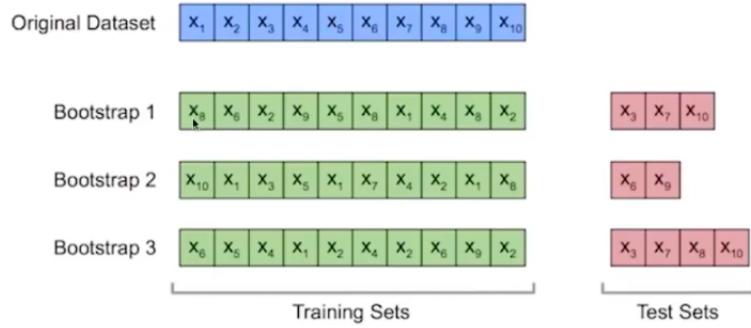
- Consider a sample of size n as shown in the figure below. We generate B sets of 'bootstrap samples' also of size n ; these are generated by randomly sampling objects from the original sample *with replacement*. Thus an object can appear in a bootstrap sample several times.
- For each of the B bootstrap samples, a target is estimated (e.g. if we wanted to estimate the mean of the whole sample, we could compute the mean on each of the B bootstrap sets).
- Compile a list of the B target estimates. Make further inference from these values, e.g. compute their mean, standard deviation, or even plot their distribution.



The bootstrap method can be used for a cross-validation method called *out-of-bag bootstrap*. The method is as follows:

- Given a dataset of size n , we create B random bootstrap samples of size n by sampling *with replacement* as usual. These samples become *training sets*.
- For each of the B bootstrap samples, determine which elements of the original dataset are not present in the particular sample. These objects comprise *test sets* for each of the corresponding training sets; we can compute required quality metrics on these sets.

Once we are done, we can estimate the mean and standard deviation of the quality metrics.



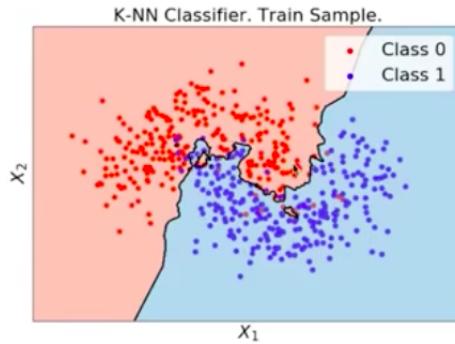
7.3 Quality metric uncertainty estimation

Our goal in this section is to estimate uncertainty of the quality metric on the test set. Again, we can use the bootstrap method:

- Suppose we are given a model fitted on a training set. Suppose that there are N objects in a corresponding test set.
- For $i = 1, \dots, B$ bootstrap sample (typically of the order of hundreds or thousands):
 - Sample *with replacement* a subsample with N objects from the test sample.
 - Calculate quality metrics on this subsample.
- Estimate statistics of this metrics, for example *mean, variance, confidence intervals*.

The main advantage of this approach is that it is completely universal - it can be used for any model and any metric. It also does not require fitting the model times.

Example 7.3: In the binary classification example before, with model:



applying the bootstrap method gives the following uncertainties:

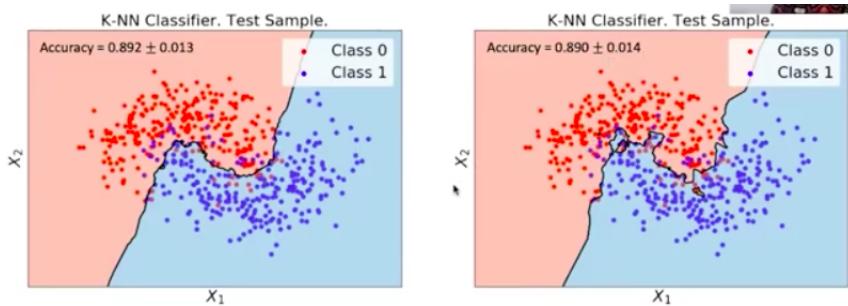
Metric	Train	Test	Bootstrap
Accuracy	0.93	0.89	0.89 ± 0.01
Precision	0.92	0.90	0.90 ± 0.02
Recall	0.95	0.88	0.88 ± 0.02
F_1	0.93	0.89	0.89 ± 0.02
ROC AUC	0.99	0.94	0.94 ± 0.01

The means are the same as those computed on the test set, but now we have uncertainties on these values.

We can also use cross-validation methods as previously described to estimate the quality metric uncertainties. For example, k -folding or out of bag bootstrap can be applied in similar ways - however, these require fitting a model several times.

7.4 Statistical model comparison

Consider two different models fitted on the same training sample:



How do we know which model is statistically better? Visually, the model in the left figure has more of a regular separation surface. Additionally, the mean accuracy of the model on the left is higher, but it has a lower uncertainty on accuracy than the model on the right hand side.

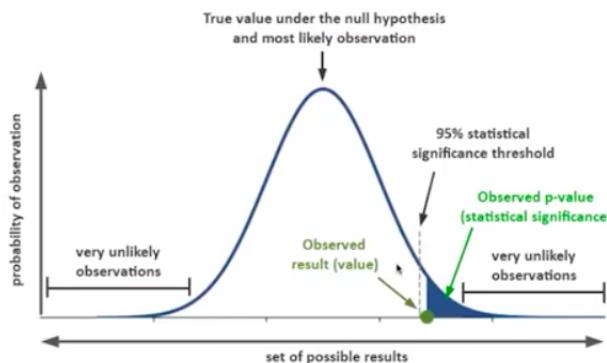
To distinguish between the models, we use *hypothesis testing*. We have two hypotheses in this case:

- H_0 : the models have the same quality (the *null hypothesis*).
- H_1 : the models have different qualities.

To test whether to reject the null hypothesis H_0 or not, we do the following:

- Select a test statistic, and calculate its value under the null hypothesis.
- Estimate the *p-value* for the observed statistic value.
- Compare the *p-value* with the given *significance level*.
- Based on a decision rule, reject H_0 and accept H_1 or do not reject H_0 .

These steps are illustrated in the following image:



Examples of tests and statistics are described as follows. First, consider the *resampled paired t-test*:

- Given two models A and B , for $i = 1, \dots, k$:
 - Randomly split the data into training and test samples.
 - Fit the models A and B on the training sample.
 - Compute quality metrics q_{Ai} and q_{Bi} for the models on the test sample.
- Compute the following t -statistic with $k - 1$ degrees of freedom under the null hypothesis that the models have equal quality:

$$t = \frac{\bar{q}\sqrt{k}}{\sqrt{\sum_{i=1}^k (q_i - \bar{q})^2 / (k - 1)}},$$

where $q_i = q_{Ai} - q_{Bi}$ and $\bar{q} = \sum_{i=1}^k q_i$.

- Given the estimate t -statistic value, we compute the p -value for this statistic using *Student's distribution* for $k - 1$ degrees of freedom. We compare this p -value with the chosen *significance level* (e.g. $\alpha = 0.05$).
- If the p -value is less than α , the null hypothesis is rejected. This means that there is a significant difference between the models.

Example 7.4: For the two models at the start of this section, we can compute the t -statistic to be $t = 1.930$. The p -value is then given by 0.063. This is larger than 0.05, so the null hypothesis is not rejected. The models are *not* significantly different in terms of accuracy.

Another test is *Dietterich's 5 × 2-fold CV paired test*:

- Given two models A and B , for $i = 1, \dots, 5$:
 - Randomly split the data into training and test samples. Fit the models A and B on the training sample. Compute quality metrics $q_{Ai}^{(1)}$ and $q_{Bi}^{(1)}$ for the models on the test sample.
 - Rotate the training and test samples: fit the models on the test, compute the metrics $q_{Ai}^{(2)}$ and $q_{Bi}^{(2)}$ on the training sample.
 - Compute the following values:

$$q_i^{(1)} = q_{Ai}^{(1)} - q_{Bi}^{(1)}, \quad q_i^{(2)} = q_{Ai}^{(2)} - q_{Bi}^{(2)}, \quad \bar{q}_i = \frac{q_i^{(1)} + q_i^{(2)}}{2}, \quad s_i^2 = (q_i^{(1)} - \bar{q}_i)^2 + (q_i^{(2)} - \bar{q}_i)^2.$$

- Then calculate the following t -statistic with 5 degrees of freedom and the null hypothesis that the models A and B have equal qualities:

$$t = \frac{q_1^{(1)}}{\sqrt{\frac{1}{5} \sum_{i=1}^5 s_i^2}}.$$

- Compute the p -value for this statistic using Student's distribution for 5 degrees of freedom. Compare the p -value with the chosen significance level α . If the p -value is less than α , the null hypothesis is rejected and there is a significant difference between the two models.

Example 7.5: Applying this test to the above example, we find that $t = 2.073$ and the p -value is 0.093. We see that the null hypothesis is *not* rejected, and again we conclude that the models are not significantly different in terms of accuracy.

There are many other available tests, including:

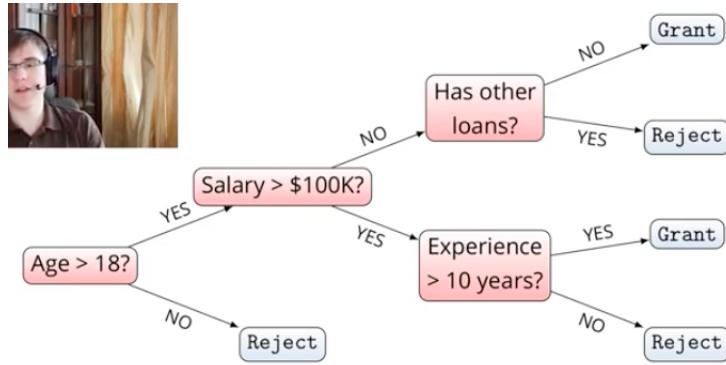
- Alpaydin's combined 5×2 CV F -test.
- Cochran's Q -test.
- Friedman's test.

However, a detailed discussion is beyond the scope of these lectures.

8 Decision trees

8.1 Decision tree training

Decision trees are a machine learning algorithm for classification and regression. Decision trees themselves predate machine learning, and can be used to make a decision e.g.



In our case, we would like to build a decision tree for example for classification problems, to decide which class a given element belongs to (hence a decision tree determines a decision boundary).

In general, building an optimal decision tree is an NP-complete problem. Therefore, in practice we use a *greedy algorithm* to build a decision tree - on each iteration, we partition the data as if the split was final (we don't think ahead at all). There are two key components:

- A split criterion to compare different ways to partition the data.
- A stopping condition to decide when to stop building the tree.

Formally:

Definition 8.1: We define *greedy decision tree learning* as follows. Suppose we are given an input training set $D = \{(x_i, y_i) : i = 1, \dots, N\}$. For each node in the tree u , we write $R_u \subseteq D$ as the data subset associated with this node. To build each R_u we do the following:

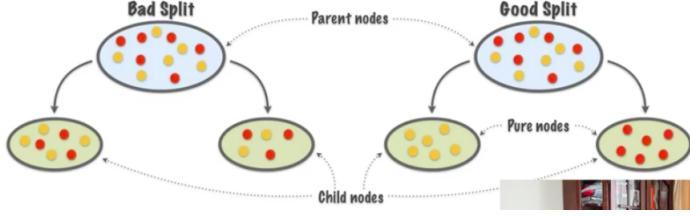
- (1) Set the first node in the tree $R_{\text{start}} = D$ to be equal to the whole dataset.
- (2) Given R_u left unsplit and not a leaf, we greedily split R_u into R_l and R_r given by:

$$R_l(j, t) = \{\mathbf{x} \in R_u : x^j \leq t\}, \quad R_r(j, t) = \{\mathbf{x} \in R_u : x^j > t\},$$

where j is a particular feature, optimising a given loss $Q(R_u, j, t)$ over (j, t) .

- (3) If a stopping criterion is satisfied for u , declare it a *leaf* of the tree.
- (4) If not, create an internal node u corresponding to the predicate $x^j \leq t$ and repeat from Step 2 for $R_u = R_l(j, t)$ and $R_u = R_r(j, t)$.

A good split at any point in the building of a decision tree is one that maximises *purity*; i.e. objects in the split are as uniform as possible:



We can formalise the purity by carefully discussing the loss function $Q(D, j, t)$ above. Recall that R_u is the subset of D corresponding to the node u . With the current split, let $R_l \subseteq R_u$ go left and $R_r \subseteq R_u$ go right. We choose a predicate to maximise:

$$Q(R_u, j, t) = H(R_u) - \frac{|R_l|}{|R_u|} H(R_l) - \frac{|R_r|}{|R_u|} H(R_r),$$

where $H(R)$ is some impurity criterion. Generally, we take:

$$H(R) = \min_{c \in \mathcal{Y}} |R|^{-1} \sum_{(x_i, y_i) \in R} \mathcal{L}(y_i, c),$$

where \mathcal{L} is a loss function, penalising wrong predictions.

Example 8.2: Some examples of impurity criterion include:

- For regression, we might choose MSE:

$$H(R) = \min_{c \in \mathcal{Y}} |R|^{-1} \sum_{(x_i, y_i) \in R} (y_i - c)^2.$$

This is minimised by $c = |R|^{-1} \sum_{(x_j, y_j) \in R} y_j$, which makes the impurity the variance of the target.

- For classification, we can enumerate $\mathcal{Y} = \{y_1, \dots, y_N\}$. We then let:

$$p_k = |R|^{-1} \sum_{(x_i, y_i) \in R} 1_{\{y_i = y_k\}}$$

be the share of examples belonging to the k th class.

We could choose the impurity to be the *miss rate* (inaccuracy):

$$H(R) = \min_{c \in \mathcal{Y}} |R|^{-1} \sum_{(x_i, y_i) \in R} 1_{\{y_i \neq c\}}.$$

We could also choose the impurity to be the *Gini index*:

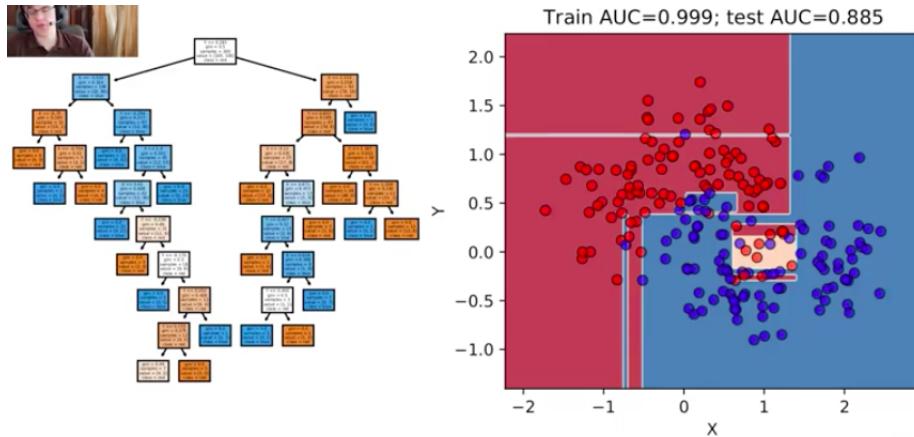
$$H(R) = \sum_{k=1}^N p_k (1 - p_k).$$

Finally, we could choose the impurity to be the *cross-entropy*:

$$H(R) = - \sum_{k=1}^N p_k \log(p_k).$$

8.2 Stopping rules for decision tree learning

What will happen if we build a decision tree to minimise the impurity to the greatest possible extent? The tree will be built until all leaves are 100% pure, with some leaves only containing a single example. This corresponds to a *dramatic overfitting*. For example:

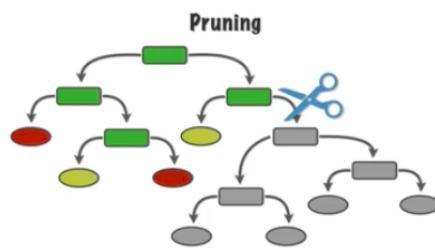


Clearly we need to know when to stop the training to avoid overfitting. There are multiple choices available:

- Impose a maximum tree depth.
- Impose a minimum number of objects in a leaf.
- Impose a maximum number of leaves in a tree.
- Stop if all objects fall into the same leaf.
- Constrain *quality improvement* (stop when improvement gains drop below a defined threshold).

There is no general way to select the best choice. It is typically decided by exhaustive search and cross-validation.

A useful technique that can help to avoid overfitting is *decision tree pruning*.



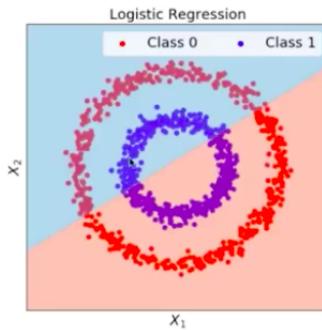
We train a very large tree (effectively overfitting the training set), then remove the least important nodes. This often leads to better result than simply training a small tree.

The reason why is as follows. When we build a tree, we use a greedy algorithm - we never look ahead or plan smart moves. In particular, pruning allows us to recover some of this missing foresight.

9 Feature engineering, importance and selection

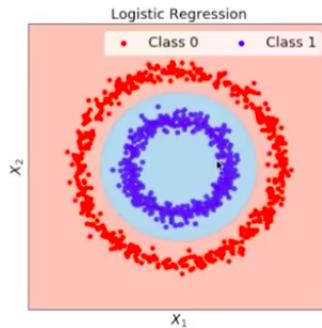
9.1 Feature engineering

Example 9.1: Consider a binary classification problem in 2D with a logistic regression classifier:



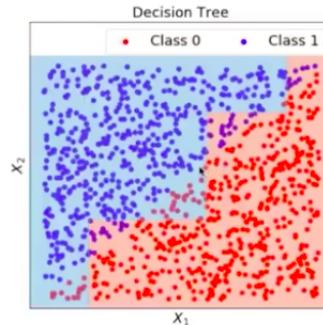
The classes are concentric circles, and the classifier *cannot* separate them using only the input features X_1, X_2 - they are not linearly separable.

Let's create the new feature $X_3 = X_1^2 + X_2^2$. This feature helps to separate the circles by a straight line. Now, logistic regression can solve the classification problem ideally using all three features X_1, X_2 and X_3 .



The above example shows how 'feature engineering' can improve the predictions of linear models.

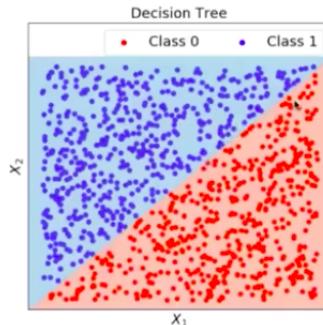
Example 9.2: Consider another example where the two classes are separated by the surface $X_2 - X_1 = 0$.



These classes are linearly separable, and can be found using a logistic regression model.

However, the problem is difficult to solve with a decision tree classifier (as shown above - it splits input feature space with *rectangles*). It requires larger depth of the tree to separate the classes properly.

If we introduce the new feature $X_3 = X_2 - X_1$, we help the classifier. Now the classes can be separated using just one predicate $X_3 > 0$. It requires a decision tree with depth 1 to solve the problem ideally.



These two examples show that creating new features can:

- Improve the quality of a model.
- Reduce the complexity of a model (see the shorter decision tree in the second example).
- Speed up model training (due to reduced complexity).
- Reduce dimensionality of a problem by removing less informative features (e.g. X_1, X_2 in previous examples - these can be removed without losing the model's quality!).

But how do we choose which new features will be useful? There are some general principles:

- Use any information about the problem we have. In the above examples the information we had was the shape of the classes and the border between them.
- Create features with physical meaning (e.g. $\sqrt{X_1^2 + X_2^2}$ is radius). For example in high energy physics, we might like to use momenta, mass, angles, etc.
- Remove limitations of a model (like with the decision tree in example 2).

Given an initial set of input features X_1, \dots, X_n , typical feature combinations include:

- Powers and products, e.g. $X_i^p, X_1 X_2$.
- Sums and differences of squares, e.g. $X_1^2 \pm X_2^2$.
- Sums and differences, e.g. $X_1 \pm X_2$.
- Sum and difference quotients, e.g.

$$\frac{X_1 \pm X_2}{X_1 \mp X_2}$$

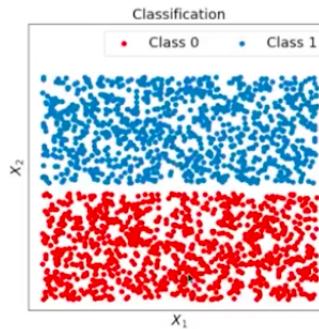
- More complicated functions, e.g.

$$\sin(X_1), \quad \cos(X_1).$$

9.2 Feature importance

Let us try to address the problem of which features are important more carefully.

A dataset can have a lot of features, but not all features are equally useful for a given regression or classification task. Some of them are more informative than others. Consider the example below:



We see that the feature X_1 is completely uninformative for the classification problem, and can be skipped. We can easily spot this from the plot of the data, but how can we do this in multi-dimensional cases? Our goal should be to measure the importance of each feature in the general case somehow.

There are several different methods to achieve this:

- Correlations between features and target values.
- Probabilistic distances.
- Decision tree-based feature importance.
- Linear model-based feature importances.

Finally we will consider a completely general algorithm which can be applied for any classification or regression problem.

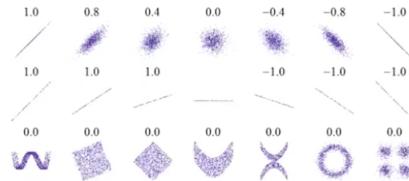
We begin with correlations:

Definition 9.3: Let f be a feature and let y be a target. Denote by f_i the value of the feature for the i th object in a dataset, and by y_i the value of the target for the i th object in a dataset (this corresponds to labels 0 or 1 for example in a binary classification problem, or to the target values in a regression problem). We define the *Pearson correlation coefficient* by:

$$\rho(f, y) = \frac{\sum_i (f_i - \bar{f})(y_i - \bar{y})}{\sqrt{\sum_i (f_i - \bar{f})^2 \sum_i (y_i - \bar{y})^2}},$$

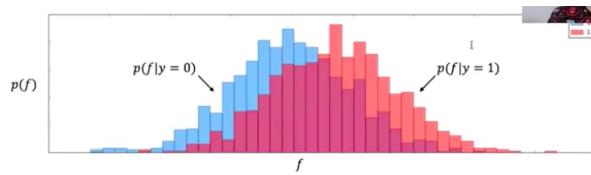
where \bar{f} is the mean of the feature over the dataset, and \bar{y} is the mean of the target values over the dataset.

This measurement of feature importance is very easy to compute, but captures only linear dependencies in dataset:



Another simple approach is based on *probabilistic distance*:

Definition 9.4: Let f be a feature, and let y be a target taking values 0 or 1 (i.e. a binary classifier).

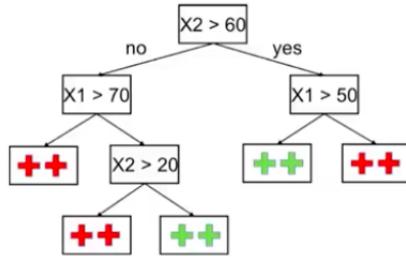


We define the *total variation* between the probability distributions $\mathbb{P}(f|y = 0)$ and $\mathbb{P}(f|y = 1)$ to be:

$$\text{Imp}(f) = \int |\mathbb{P}(f|y = 1) - \mathbb{P}(f|y = 0)| df.$$

There are other methods of measuring the distance between probability distributions - we will consider these later in the school.

Another approach is based on *decision trees*. Recall from the previous lectures that a decision tree is a binary tree where each node t has two children. Each node uses one feature to make a split into the two children nodes. For each node, we compute the number of objects n_t which satisfy the criteria in the node; then for each node we can compute *impurity* functions $I(t)$ (e.g. Gini, cross-entropy, MSE) for the node.



Definition 9.5: Let $T(f)$ be the set of all nodes which use feature f to make a split. Then feature importance can be estimated by:

$$\text{Imp}(f) = \sum_{t \in T(f)} n_t \Delta I(t),$$

where the *information* $\Delta I(t)$ contained in the node t is defined by:

$$\Delta I(t) = I(t) - \sum_{c \in \text{children}(t)} \frac{n_c}{n_t} I(c).$$

This statistic is one of the most popular and important for feature estimation. It takes into account dependencies between different input features, and can capture complicated dependencies between features and the target. It is also implemented in almost all decision tree libraries.

Another method is *linear-model based*.

Definition 9.6: Consider a linear model with regularisation (e.g. an $L1$ or $L2$ penalty). The model makes predictions:

$$\hat{y} = w_0 + w_1 f_1 + w_2 f_2 + \cdots + w_k f_k.$$

If features are normalised (have the same ranges, e.g. by scaling), the feature importance of f_i is defined to be equal to:

$$\text{Imp}(f_i) = |w_i|.$$

This method is very simple, but has the same limitations as Pearson correlation - it cannot capture complicated dependencies.

Now let's consider a completely general approach. Suppose we have a model used for classification or regression.

- We train the model to some training set.
- We calculate the quality measure Q_0 on some validation set.
- For a given feature f , we:
 - Replace the given values of this feature with random values from the same distribution (for example, you can perform random shuffling of the value of the feature).

	REISpend	Administration Spend	Marketing Spend	Profit	state_California
1	165349.2	136997.8	471784.1	192261.83	0
2	162597.7	151377.59	443886.53	191792.06	1
3	153441.51	101145.55	407934.54	191050.39	1
...
48	0	135426.92	0	42559.73	1
49	542.05	51743.15	0	36873.41	0
50	0	116983.8	45173.06	14881.4	1

- Compute the new quality measure Q_f on the validation set, and estimate the feature importance as the difference between the initial and current quality metric values:

$$\text{Imp}(f) = Q_0 - Q_f.$$

This is the most powerful method for computing feature importance. It can capture complicated dependencies, and works for any model - e.g. neural networks, which we shall see soon.

There is a slight modification to this method which also works:

- We train the model on the *full set of features* (as normal)
- We calculate the quality measure Q_0 on some validation set.
- For a given feature f , we:
 - Remove the feature f from the dataset, then *refit the model without this feature*.

	REISpend	Administration Spend	Marketing Spend	Profit	state_California
1	165349.2	136997.8	471784.1	192261.83	0
2	162597.7	151377.59	443886.53	191792.06	1
3	153441.51	101145.55	407934.54	191050.39	1
...
48	0	135426.92	0	42559.73	1
49	542.05	51743.15	0	36873.41	0
50	0	116983.8	45173.06	14881.4	1

- Compute the new quality measure Q_f on the validation set, and estimate the feature importance as the difference between the initial and current quality metric values:

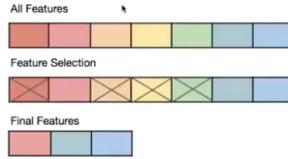
$$\text{Imp}(f) = Q_0 - Q_f.$$

The advantage of this approach is that it estimates the feature importances more precisely, and works better for highly correlated input features. However, it requires refitting the model several times - this might be difficult for large models and datasets.

There are many other approaches to estimate feature importance which we don't have time to discuss here - for example the method of *Shapley values*, which has a Python implementation.

9.3 Feature selection

The goal of *feature selection* is to reduce the number of features with minimal loss of model quality. For example, we might want to keep the best K of D features, or we might want to remove as many features as possible but keeping the quality $Q \geq Q_{\min}$ for some Q_{\min} .



Three of the most popular methods are the *filter method*, *embedded methods* and *recursive feature elimination*.

Definition 9.7: The *filter method* involves estimating the importance of individual features $\text{Imp}(f_1), \text{Imp}(f_2), \dots, \text{Imp}(f_D)$ via some method (e.g. correlation, probability distance). We then simply select the required number of features with the highest importances.

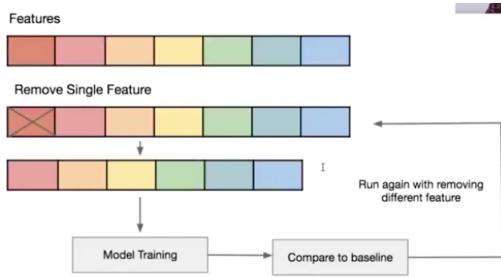
This is simple to implement and is quite fast. However, it is bad for highly correlated features, since it may take many redundant features.

Definition 9.8: An *embedded method* selects features based on the feature importance of a model.

- In a linear model, an embedded method selects the best features using the weights of the model (as above).
- For a decision tree, the best features are selected using their decision tree importance (as above).

Embedded methods are widely used and take into account correlation between features.

Finally, we have *recursive feature elimination*. Uninformative features are removed one by one, based on deleting the least important feature at each step.



The steps are as follows:

- Train a model on the full set of features, and estimate the importance of each feature based on the model.
- Remove the least important features (or several features).
- Repeat until we have the desired number of features remaining.

In combination with the general method for feature importance estimation, this is one of the most powerful methods for feature selection. It is applicable to any regression or classification problem.

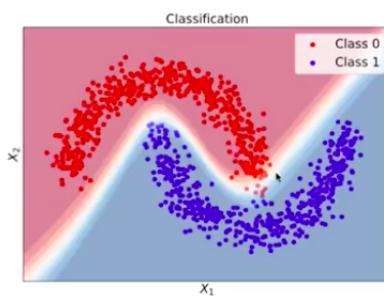
10 Clustering

So far, we have studied classification and regression models. These are models of ‘supervised learning’ where we know exactly what to predict - class labels for classification or real labels for regression.

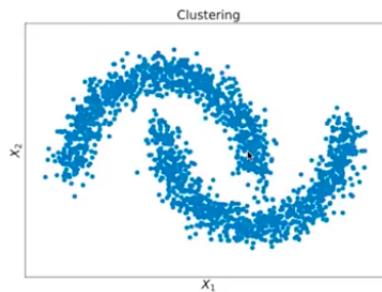
In this section, we will discuss *clustering*, where we do not have any target values for predictions. Therefore clustering is a topic of ‘unsupervised machine learning’.

10.1 Clustering vs classification

Consider a binary classification problem, where we have object features X and class labels $y \in \{0, 1\}$. A classifier learns a decision rule f , so that $f(X) \approx y$. The trained classifier predicts class labels for the new objects.



In clustering, we don't have class labels y . The goal is to divide all objects into separate groups using only object features X - these groups are called *clusters*.



We would like to cluster the objects such that *objects inside clusters are similar*, and *objects from different clusters are dissimilar*. In the above figure, ‘similarity’ can be defined as proximity to the other objects.

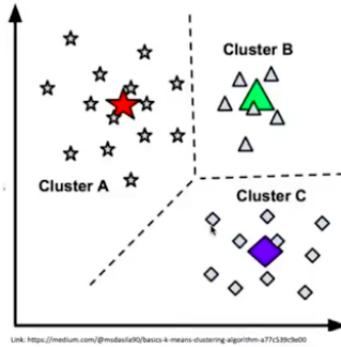
Most clustering algorithms are based on the following assumptions:

- Objects form *dense* clusters. This means that the object density inside one cluster is larger than between the clusters.
- Objects from one cluster are somehow similar, whilst objects from different clusters are somehow dissimilar. Often similarity between objects is based on ‘distance’ between them.
- Distances between neighbours within one cluster are smaller than between objects from different clusters.

10.2 K-means

The most popular clustering approach is the approach of *K-means*. We develop intuition for this approach as follows.

We suppose that each cluster is represented by a *centre*. All objects are assigned to a cluster according to the closest centre. The goal of the problem is therefore to *find centres that form the most compact clusters*.



Let's define some notation which we will use throughout this section. Consider a sample with N objects, written $\{x_n\}_{n=1}^N$ (where x_n denotes a tuple of features). We will search for K clusters with centres $\{\mu_1, \dots, \mu_K\}$. The criterion to find the best centres is minimising the *within-cluster distance* over μ_1, \dots, μ_K :

$$Q = \sum_{n=1}^N \min_k \rho(x_n, \mu_k).$$

Each object is then assigned to a cluster $z_n \in \{1, 2, \dots, K\}$ via:

$$z_n = \operatorname{argmin}_k \rho(x_n, \mu_k).$$

A general algorithm that achieves this is as follows (called the *K-centroid algorithm*):

- (1) Initialise the centres μ_1, \dots, μ_K by randomly selecting k objects from the sample.
- (2) Assign each object of the sample to the nearest centre:

$$z_n = \operatorname{argmin}_k \rho(x_n, \mu_k),$$

where ρ is the 'distance' between two objects.

- (3) Update the centres by minimising the within cluster distance, i.e. determining:

$$\mu_k = \operatorname{argmin}_\mu \sum_{n:z_n=k} \rho(x_n, \mu).$$

- (4) If the algorithm has not converged to within some tolerance, go to Step 2 and repeat. Otherwise return z_1, \dots, z_N .

The above algorithm can use difference distances ρ :

Definition 10.1: If $\rho(x_n, \mu_k) = \|x_n - \mu_k\|_2^2$, the above algorithm is called the *K-means algorithm*. If $\rho(x_n, \mu_k) = \|x_n - \mu_k\|_1$, the above algorithm is called the *K-medians algorithm*.

The *K*-means algorithm can be implemented efficiently as follows:

- (1) Initialise the centres μ_1, \dots, μ_K by randomly selecting k objects from the sample.
- (2) Assign each object of the sample to the nearest centre:

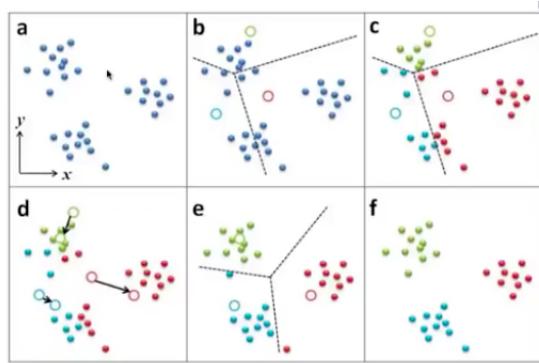
$$z_i = \operatorname{argmin}_{j \in \{1, 2, \dots, K\}} \|x_i - \mu_j\|_2^2.$$

- (3) Update the centres using the following minimisation (this choice minimises the within-cluster distance):

$$\mu_j = \frac{\sum_{n=1}^N 1_{\{z_n=j\}} x_i}{\sum_{n=1}^N 1_{\{z_n=j\}}}.$$

- (4) If the algorithm has not converged to within some tolerance, go to Step 2 and repeat. Otherwise return z_1, \dots, z_N .

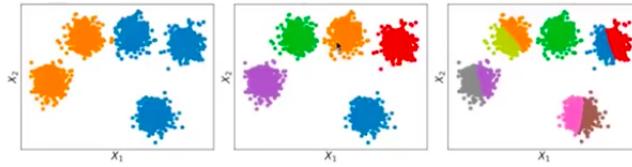
Below is an example of the convergence of the algorithm:



Let's discuss the properties of the *K*-means algorithm in more detail:

- **Initialisation.** The centres $\{\mu_k\}_{k=1}^K$ are usually initialised randomly from training objects. The number of clusters (and centres) K is usually fixed.
- **Convergence criteria.** There are various methods we could use to check for convergence. For example, we could set some limit on the number of iterations of the algorithm, we could demand that the centres stop changing significantly within some tolerance, or we could ask that the cluster assignments $\{z_n\}_{n=1}^N$ stop changing.
- **Solution.** The solution depends on the starting positions of the centres. In particular, this means that the algorithm is sensitive to outliers, and may create single-object clusters. To prevent this it is recommended to run the algorithm with several different initialisations, and select the solution with the minimal within-cluster distance Q .

Now we understand how K -means works, we can ask some interesting questions about it. For example - how do we know how many clusters K to split the data into? Using the wrong number of clusters can lead to bad results, e.g.

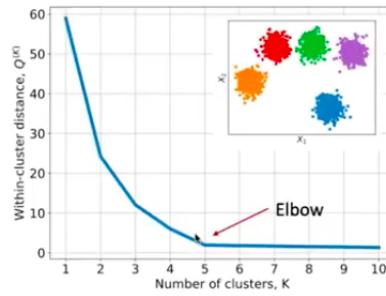


Let $Q^{(K)}$ denote the within-cluster distances for each possible number of clusters K ,

$$Q^{(K)} = \sum_{n=1}^N \|x_n - \mu_{z_n}\|_2^2.$$

We wish to minimise this over $z_1, \dots, z_N, \mu_1, \dots, \mu_K$.

The dependency of $Q^{(K)}$ on K is demonstrated in the figure below for the above example.

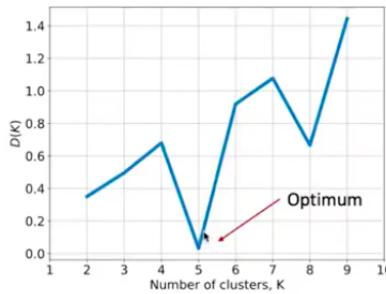


The dependence has an 'elbow' at the optimal number of clusters, $K = 5$. Let's try to formalise this notion.

We define the function $D(K)$ by:

$$D(K) = \frac{|Q^{(K+1)} - Q^{(K)}|}{|Q^{(K)} - Q^{(K-1)}|}.$$

This function takes its smallest value for the optimal number of clusters.



10.3 Quality metrics

Now we know one clustering algorithm. How do we measure the quality of a clustering algorithm?

There are two kinds of quality metrics for clustering models: *supervised* and *unsupervised*.

- *Supervised* quality metrics are based on the ground truth of the object labels. They are invariant to cluster naming. Unfortunately, very often the true labels are unknown and hence it is impossible to use these metrics in this case.
- *Unsupervised* quality metrics are based on intuition about ‘good’ clusters. They assume that objects from the same cluster are similar to one another, and objects from different clusters are dissimilar to one another.

One supervised quality metric is the *Rand index*:

Definition 10.2: The *Rand index* is the supervised quality metric defined as:

$$RI = \frac{TP + TN}{TP + TN + FP + FN}.$$

Here, TP denotes *true positives*, the number of pairs in the same cluster in predictions and the ground truth. TN denotes *true negatives*, the number of pairs from different clusters in predictions and the ground truth. FP denotes *false positives*, the number of pairs in the same cluster in predictions, but from different clusters in the ground truth. FN denotes *false negatives*, the number of pairs in the same cluster in the ground truth, but from different clusters in predictions.

The Rand index takes values in $[0, 1]$, where 1 means perfect clustering. It is similar to accuracy score, but for pairs.

A slight modification is:

Definition 10.3: The *adjusted Rand index* (ARI) is defined by:

$$ARI = \frac{RI - RI_{\text{expected}}}{RI_{\text{max}} - RI_{\text{expected}}}.$$

The expected Rand index is taken by averaging the Rand index over all possible object assignments to the clusters.

The ARI has a value close to 0 for random labelling, independently of the number of clusters and sample, and exactly 1 when the clustering is ideal.

As we have just seen Rand index is very similar to accuracy score. We can compute similar metrics like precision, recall, or F_1 -score in the same sorts of ways by just considering pairs.

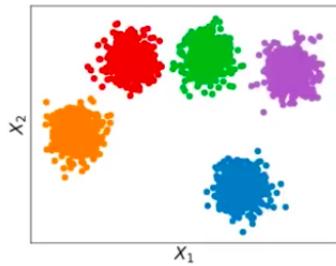
One of the most popular unsupervised metrics is the *silhouette metric*:

Definition 10.4: The *silhouette metric* is defined by:

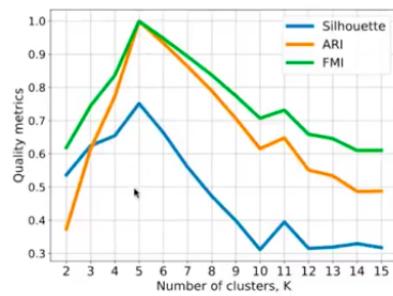
$$\text{Silhouette} = \frac{1}{N} \sum_{i=1}^N \frac{d_i - s_i}{\max(d_i, s_i)}$$

where s_i is the mean distance between the i th object and all objects in the same cluster, and d_i is the mean distance between the i th object and all objects in the nearest (distinct) cluster. It is based on the idea that objects in one cluster should be closer to one another than objects in different clusters.

Example 10.5: Consider clustering of the following data with K clusters:



The quality metrics for the clustering are given below:



Each quality metric predicts the optimum number of clusters is $K = 5$.
