Machine Learning

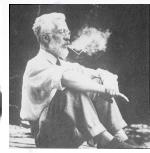
An introduction





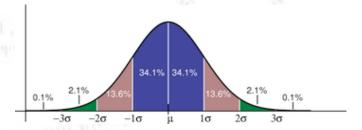








Troels C. Petersen (NBI)





What is Machine Learning?

While there is no formal definition, an early attempt is the following intuition:

"Machine learning programs can perform tasks without being explicitly programmed to do so."

[Arthur Samuel, US computer pioneer 1901-1990]

What is Machine Learning?

While there is no formal definition, an early attempt is the following intuition:

"Machine learning programs can perform tasks without being explicitly programmed to do so."

[Arthur Samuel, US computer pioneer 1901-1990]

An attempt at a more formal definition is:

"A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E."

[T. Mitchell, "Machine Learning" 1997]

What is Machine Learning?

While there is no formal definition, an early attempt is the following intuition:

"Machine learning programs can perform tasks without being explicitly programmed to do so."

[Arthur Samuel, US computer pioneer 1901-1990]

An attempt at a more formal definition is:

"A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E."

[T. Mitchell, "Machine Learning" 1997]

Under all circumstances, ML allows the analysis and understanding of data, that is complex in terms of both size, dimensionality, quality, and relations [TP].

Two main ingredients

The Universal Approximation Theorem

Theorem 5.1.1 (Universal Approximation Theorem) ¹⁰ Let σ be a non-constant, bounded, and monotone-increasing continuous function. Let I_{m_0} denote the m_0 -dimensional unit hypercube $[0,1]^{m_0}$. The space of continuous functions on I_{m_0} is denoted as $C(I_{m_0})$. Then given any function $f \in C(I_{m_0})$ and $\epsilon > 0$ there exists a set of real constants a_i, b_i and w_{ij} , where $i = 1, \ldots, m_1$ and $j = 1, \ldots, m_0$ such that we may define

$$F(x_1, \dots, x_{m_0}) = \sum_{i=1}^{m_1} a_i \sigma \left(\sum_{j=1}^{m_0} w_{ij} x_j + b_i \right)$$
 (5.6)

as an approximate realization of the function f; that is,

$$|F(x_1,\ldots,x_{m_0})-f(x_1,\ldots,x_{m_0})|<\epsilon$$
 (5.7)

for all $x_1, x_2, \ldots, x_{m_0}$ that lie in the input space.

Universal Approx. Theorems

One main ingredient behind ML are Universal Approximation Theorems (UAT).

These imply that Neural Networks can approximate a very wide variety of functions given simple function constraints and enough degrees of freedom.

This typically entails a large amount of weights, for which the UATs give no recipe on how to find - only that such a construction is possible.

Universal Approx. Theorems

One main ingredient behind ML are Universal Approximation Theorems (UAT).

These imply that Neural Networks can approximate a very wide variety of functions given simple function constraints and enough degrees of freedom.

This typically entails a large amount of weights, for which the UATs give no recipe on how to find - only that such a construction is possible.

Part of this course is learning how to find these!

Decision Trees and K-Nearest Neighbour algorithms are also capable of "universal approximation" (i.e. have forms of UATs).

A UAT has also been worked out for Graph Neural Networks... in 2020!

Universal Approx. Theorems

Regarding UATs, as far as learning is concerned, whether the class is really universal or not is not overly important:

If one assumes that there is no noise in the training set, then there will still be infinitely many functions that passes through all training points and not all of them will have the same error on an unseen point (i.e. the test set).

Thus, one can ask for what sort of functions the approximation applies. All differentiable functions? Typically, NNs are restricted to this class. All continuous functions? All measurable functions? All computable functions?

As it turns out, the real deal is characterising that class of functions that can be approximated.

However, we don't really care about that - we simply assume, that with enough liberty/complexity, the functions can approximate what we want.

Stochastic Gradient Descent

The way to obtain the parameters/weights of ML algorithms, is generally by **Stochastic Gradient Descent**.

This "back propagation" algorithm works by computing the gradient of the loss function (to be optimised) with respect to each weight using the chain rule.

One thus computes the gradient one layer at a time, iterating backwards from the last layer (avoiding redundancies). See Goodfellow et al. for details.

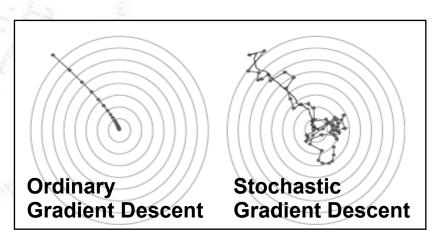
Stochastic Gradient Descent

The way to obtain the parameters/weights of ML algorithms, is generally by **Stochastic Gradient Descent**.

This "back propagation" algorithm works by computing the gradient of the loss function (to be optimised) with respect to each weight using the chain rule.

One thus computes the gradient one layer at a time, iterating backwards from the last layer (avoiding redundancies). See Goodfellow et al. for details.

The gradient descent is made stochastic (and fast) by only considering a fraction (called a "batch") of the data, when calculating the step in the search for optimal parameters for the algorithm.

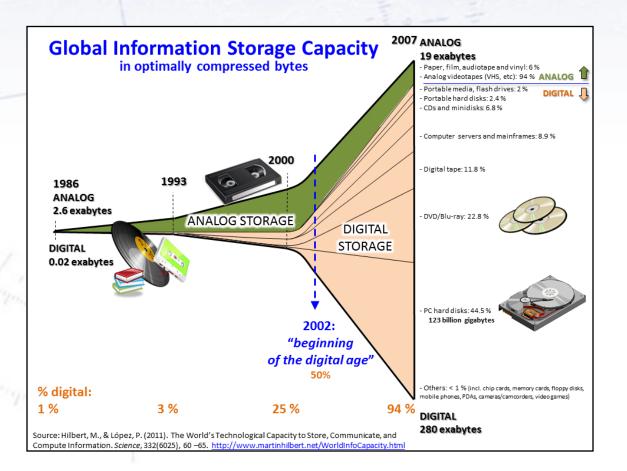


Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron (2016). <u>"6.5 Back-Propagation and Other Differentiation Algorithms"</u>. *Deep Learning*. MIT Press. pp. 200–220. ISBN 9780262035613.



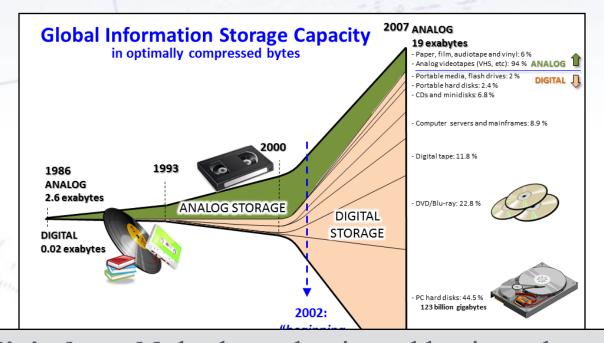
Why Machine Learning?

Part of the "rising" of Machine Learning has been the explosion in data volume, and the easy access to mine it (i.e. internet-of-things), but also the growth in data storage and processing capabilities.



Why Machine Learning?

Part of the "rising" of Machine Learning has been the explosion in data volume, and the easy access to mine it (i.e. internet-of-things), but also the growth in data storage and processing capabilities.



In a digital world, both academia and business has an advantage in understanding their (growing) data volumes.

Machine Learning is a powerful tool to do exactly that!

Dimensionality and Complexity

Humans are good at seeing/understanding data in few dimensions! However, as dimensionality grows, complexity grows exponentially ("curse of dimensionality"), and humans are generally not geared for such challenges.

AND 10,12,M	Low dim.	High dim.
Linear	Humans: Computers:	Humans: Computers:
Non- linear	Humans: Computers:	Humans: Computers:

Computers, on the other hand, are OK with high dimensionality, albeit the growth of the challenge, but have a harder time facing non-linear issues.

However, through smart algorithms, computers have learned to deal with it all!

That is essentially what Machine Learning has enabled!

Dimensionality and Complexity

Humans are good at seeing/understanding data in few dimensions! However, as dimensionality grows, complexity grows exponentially ("curse of dimensionality"), and humans are generally not geared for such challenges.

WE 10,12,M	Low dim.	High dim.
Linear	Humans: ✓ Computers: ✓	Humans: ÷ Computers: ✓
Non- linear	Humans: Computers:	Humans: Computers:

Computers, on the other hand, are OK with high dimensionality, albeit the growth of the challenge, but have a harder time facing non-linear issues.

However, through smart algorithms, computers have learned to deal with it all!

That is essentially what Machine Learning has enabled!

Dimensionality and Complexity

Humans are good at seeing/understanding data in few dimensions! However, as dimensionality grows, complexity grows exponentially ("curse of dimensionality"), and humans are generally not geared for such challenges.

MS 10, 73, M	Low dim.	High dim.		
Linear	Humans: ✓ Computers: ✓	Humans: ÷ Computers: ✓		
Non- linear	Humans: ✓ Computers: (✓)	Humans: ÷ Computers: (✓)		

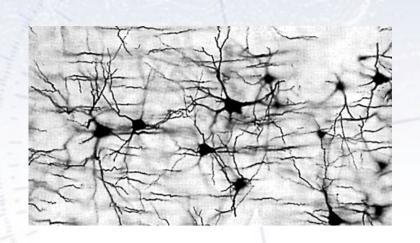
Computers, on the other hand, are OK with high dimensionality, albeit the growth of the challenge, but have a harder time facing non-linear issues.

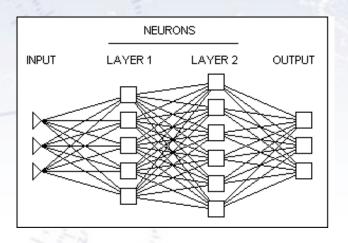
However, through smart algorithms, computers have learned to deal with it all!

That is essentially what Machine Learning has enabled!

Data Mining

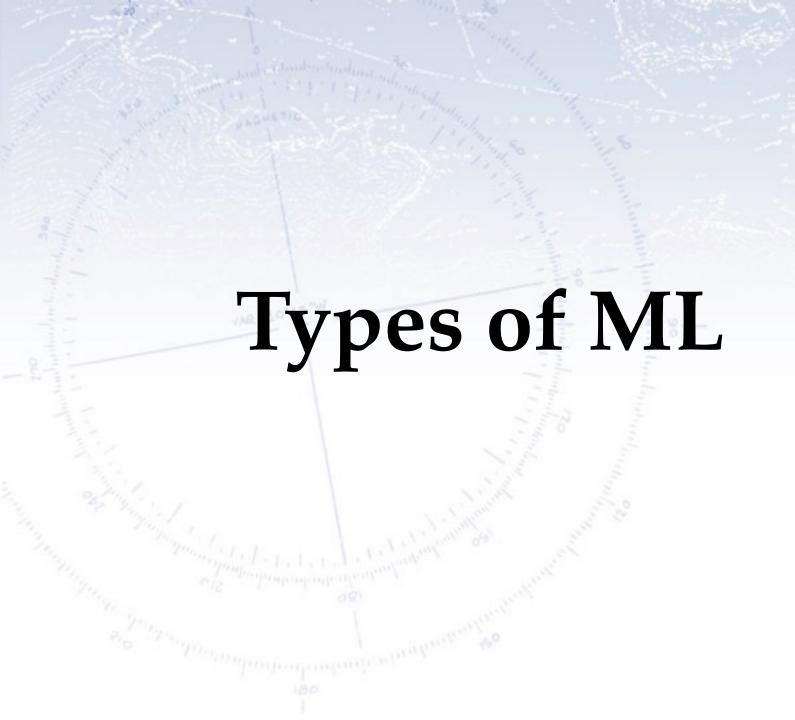
Seeing patterns in data and using it!





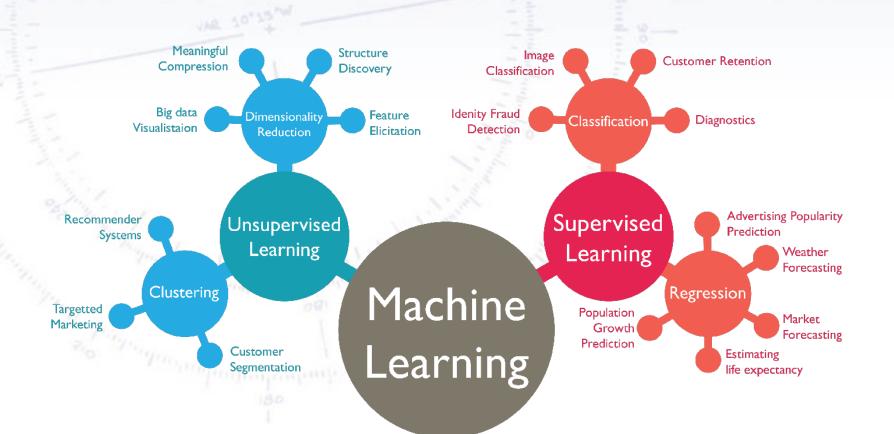
Data mining is the process of extracting patterns from data. As more data are gathered, with the amount of data doubling every three years, data mining is becoming an increasingly important tool to transform these data into information. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and **scientific discovery**.

[Wikipedia, Introduction to Data Mining]



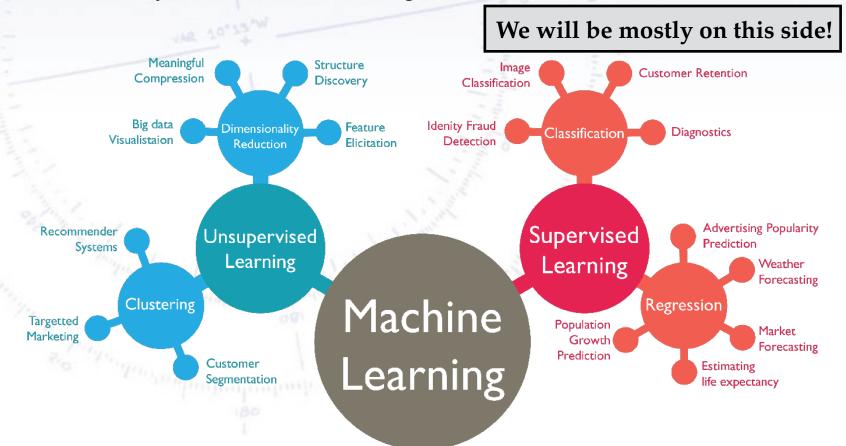
Unsupervised vs. Supervised Classification vs. Regression

Machine Learning can be supervised (you have correctly labelled examples) or unsupervised (you don't)... [or reinforced]. Following this, one can be using ML to either classify (is it A or B?) or for regression (estimate of X).

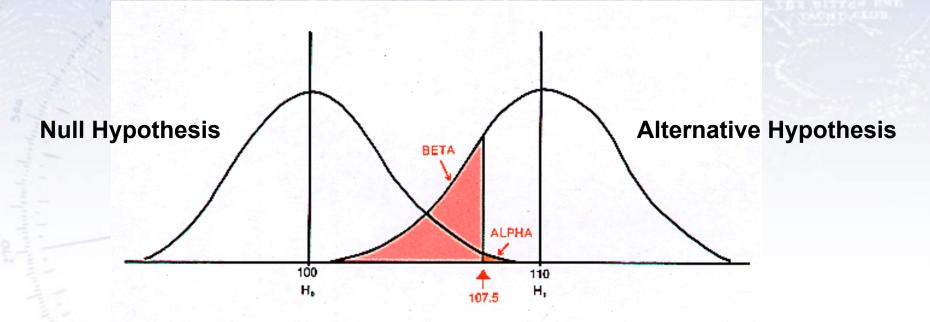


Unsupervised vs. Supervised Classification vs. Regression

Machine Learning can be supervised (you have correctly labelled examples) or unsupervised (you don't)... [or reinforced]. Following this, one can be using ML to either classify (is it A or B?) or for regression (estimate of X).



Classification/Hypothesis



REALITY

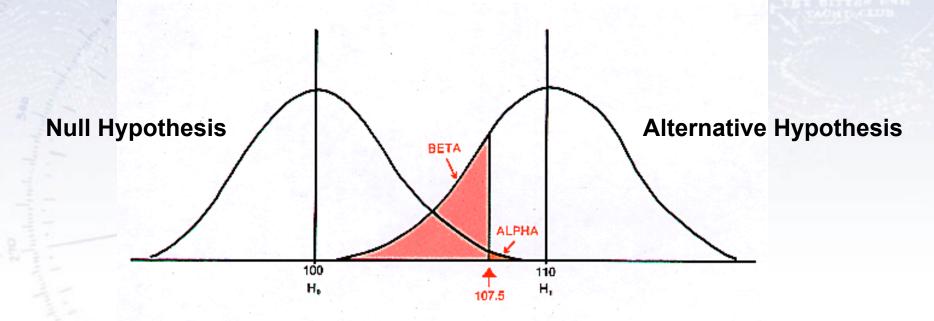
STATISTICAL DECISION:

Do Not Reject Null

Reject Null

Null is True	Null is False		
1 – α	β		
Correct	Type II error		
α	1 – β		
Type I error	Correct		

Classification/Hypothesis



Machine Learning typically enables a better separation between hypothesis

D	F	C	IS	O	N	•
_		•				

Reject Null

α	1 – β
Type I error	Correct

Hypothesis testing

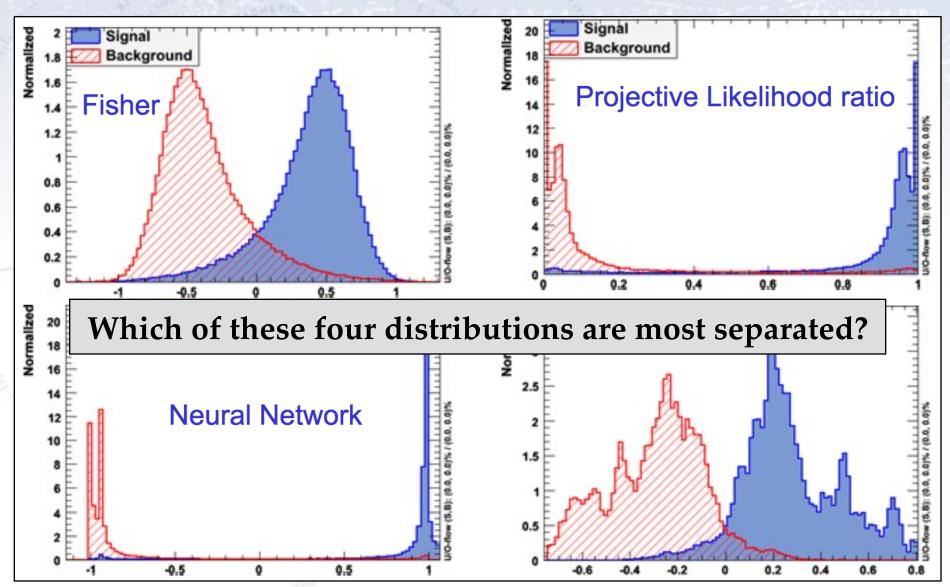
Hypothesis testing is like a criminal trial. The basic "null" hypothesis is **Innocent** (called H_0) and this is the hypothesis we want to test, compared to an "alternative" hypothesis, **Guilty** (called H_1).

Innocence is initially assumed, and this hypothesis is only rejected, if enough evidence proves otherwise, i.e. that the probability of innocence is very small ("beyond reasonable doubt").

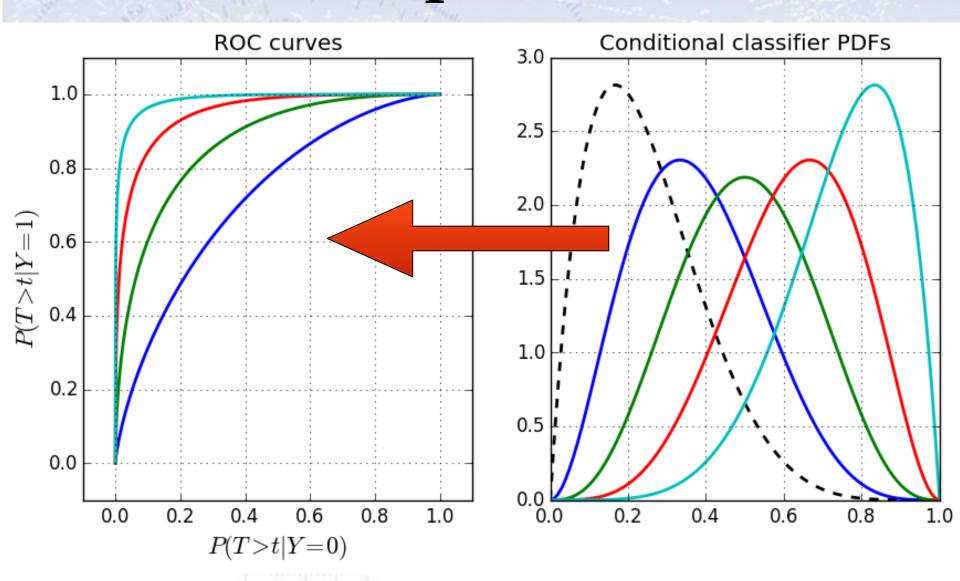
	Truly innocent (H ₀ is true)	Truly guilty (H ₁ is true)
Acquittal (Accept H ₀)	Right decision	Wrong decision Type II error
Conviction (Reject H ₀)	Wrong decision Type I error	Right decision

The rate of type I/II errors are correlated, and one can only choose one of these!

Measuring separation



Simple case



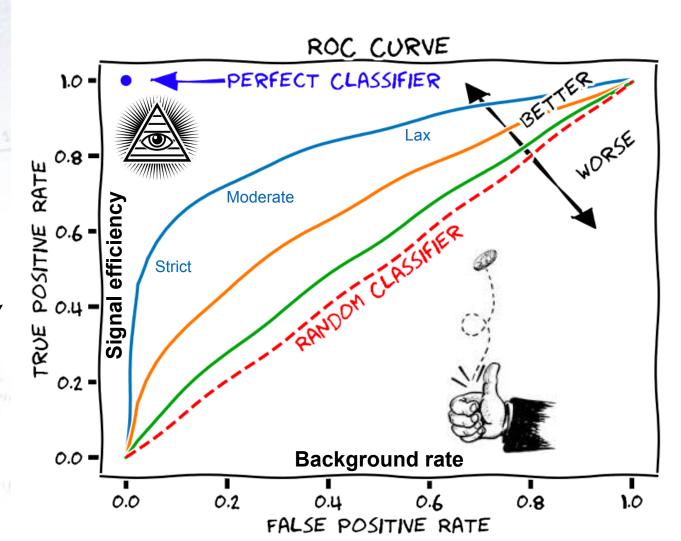
ROC curves

A Receiver Operating Characteristic or just ROC-curve is a graphical plot of the sensitivity, or true positive rate (TPR), vs. false positive rate (FPR).

It is calculated as the integral of the two hypothesis distributions, and is used to evaluate a test.

Given classification into two distributions, one may choose to make a strict or lax selection. This choice depends

on the case at hand.

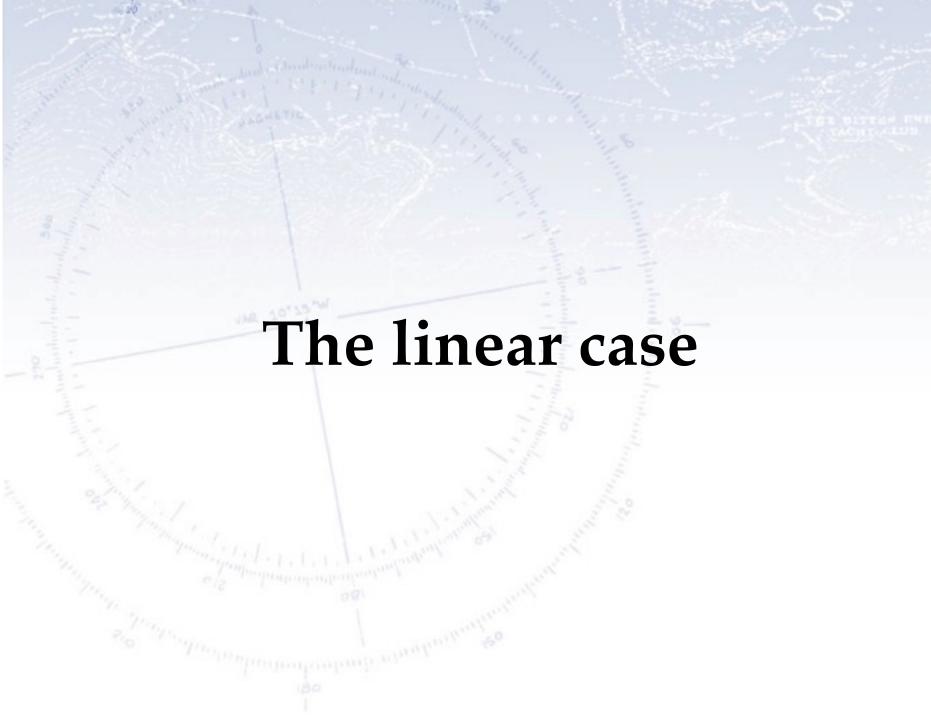


Which metric to use?

There are a ton of metrics in hypothesis testing, see below. However, those in the boxes below are the most central ones.

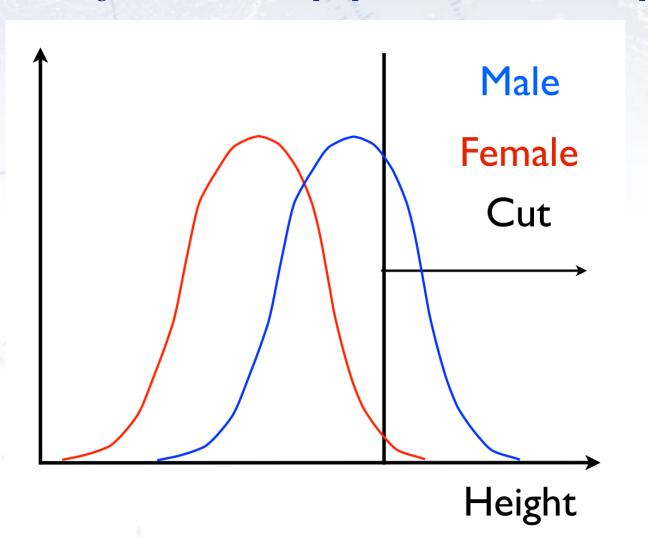
One metric - not mentioned here - is the Area Under the Curve (AUC), which is simply an integral of the ROC curve (thus 1 is perfect score). This is often used in Machine Learning to optimise performance (loss).

		True cond	ition				
	Total population	Condition positive	Condition negative	$\frac{\sum Condition \ positive}{\sum Total \ population}$	Accuracy (ACC) = $\frac{\Sigma \text{ True positive} + \Sigma \text{ True negative}}{\Sigma \text{ Total population}}$		
condition	Predicted condition positive	True positive	False positive, Type I error	Positive predictive value (PPV), Precision = Σ True positive Σ Predicted condition positive	False discovery rate (FDR) = Σ False positive Σ Predicted condition positive		
Predicted	Predicted condition negative	False negative, Type II error	True negative	False omission rate (FOR) = $\frac{\Sigma \text{ False negative}}{\Sigma \text{ Predicted condition negative}}$	Negative predictive value (NPV) = Σ True negative Σ Predicted condition negative		
		True positive rate (TPR), Recall, Sensitivity, probability of detection, Power $= \frac{\Sigma \text{ True positive}}{\Sigma \text{ Condition positive}}$	False positive rate (FPR), Fall-out, probability of false alarm $= \frac{\Sigma \text{ False positive}}{\Sigma \text{ Condition negative}}$	Positive likelihood ratio (LR+) = $\frac{TPR}{FPR}$	Diagnostic odds ratio (DOR) F ₁ score =		
		False negative rate (FNR), Miss rate $= \frac{\Sigma \text{ False negative}}{\Sigma \text{ Condition positive}}$	Specificity (SPC), Selectivity, True negative rate (TNR) $= \frac{\Sigma \text{ True negative}}{\Sigma \text{ Condition negative}}$	Negative likelihood ratio (LR-) = FNR TNR	$= \frac{LR+}{LR-}$ 2 · $\frac{Precision \cdot Recall}{Precision + Recall}$		



Simple Example

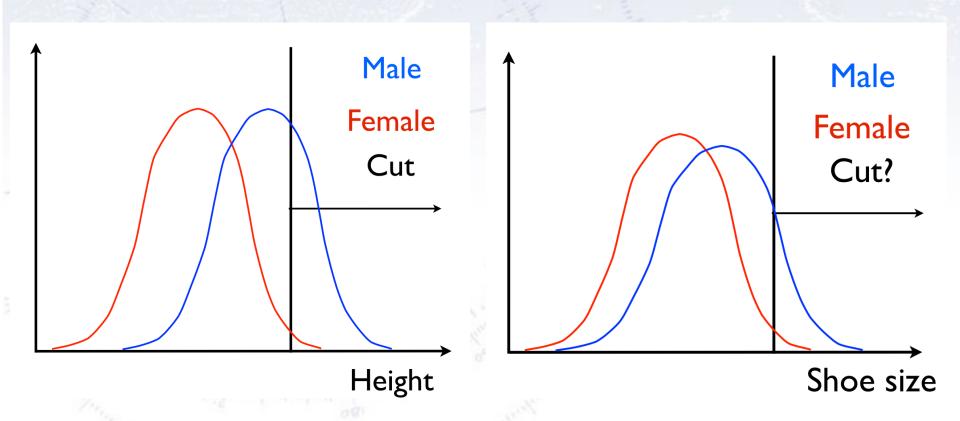
Problem: You want to figure out a method for getting sample that is mostly male! **Solution**: Gather height data from 10000 people, Estimate cut with 95% purity!



Simple Example

Additional data: The data you find also contains shoe size!

How to use this? Well, it is more information, but should you cut on it?



The question is, what is the best way to use this (possibly correlated) information!

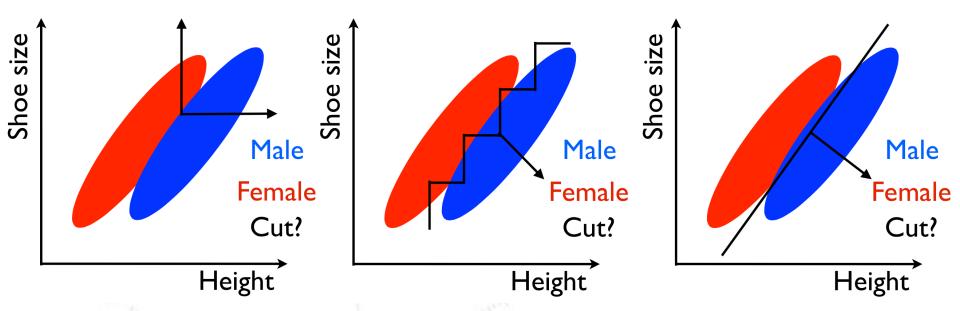
Simple Example

So we look if the data is correlated, and consider the options:

Cut on each var? Poor efficiency!

Advanced cut?
Clumsy and
hard to implement

Combine var?
Smart and
promising



The latter approach is the Fisher discriminant!

It has the advantage of being simple and applicable in many dimensions easily!

Separating data

Fisher's friend, Anderson, came home from picking Irises in the Gaspe peninsula...

180 MULTIPLE MEASUREMENTS IN TAXONOMIC PROBLEMS

Table I

Iris setosa				Iris versicolor			Iris virginica				
Sepal	Sepal	Petal	Petal	Sepal	Sepal	Petal	Petal	Sepal	Sepal	Petal	Petal
length	width										
5·1 4·9 4·7 4·6	3·5 3·0 3·2 3·1	1·4 1·4 1·3 1·5	0·2 0·2 0·2 0·2	7·0 6·4 6·9 5·5	3·2 3·2 3·1 2·3	4·7 4·5 4·9 4·0	1·4 1·5 1·5 1·3	6·3 5·8 7·1 6·3	3·3 2·7 3·0 2·9	6·0 5·1 5·9 5·6	2.5 1.9 2.1 1.8 2 1 7 8 8 8 5 0 9
5·8	4·0	1·2	0·2	5·6	2·9	3·6	1·3	5·8	2·8	5·1	2·4
5·7	4·4	1·5	0·4	6·7	3·1	4·4	1·4	6·4	3·2	5·3	2·3
5·4	3·9	1·3	0·4	5·6	3·0	4·5	1·5	6·5	3·0	5·5	1·8
5·1	3·5	1·4	0·3	5·8	2·7	4·1	1·0	7·7	3·8	6·7	2·2
5·7	3·8	1·7	0·3	6·2	2·2	4·5	1·5	7·7	2·6	6·9	2·3

Fisher's Linear Discriminant

You want to separate two types/classes (A and B) of events using several measurements.

Q: How to combine the variables?

<u>A</u>: Use the Fisher Discriminant:

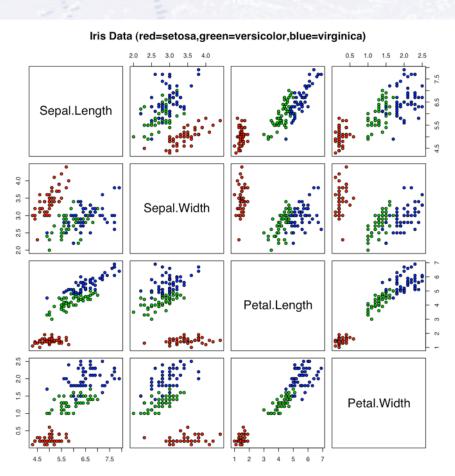
$$\mathcal{F} = w_0 + \vec{w} \cdot \vec{x}$$

Q: How to choose the values of w?

<u>A</u>: Inverting the covariance matrices:

$$\vec{w} = (\mathbf{\Sigma}_A + \mathbf{\Sigma}_B)^{-1} \ (\vec{\mu}_A - \vec{\mu}_B)$$

This can be calculated analytically, and incorporates the linear correlations into the separation capability.



Fisher's Linear Discriminant

You want to separate two types/classes (A and B) of events using several measurements.

Q: How to combine the variables?

A: Use the Fisher Discriminant:

Iris Data (red=setosa,green=versicolor,blue=virginica)

ments are given. We shall first consider the question: What linear function of the four measurements $X = \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 + \lambda_4 x_4$

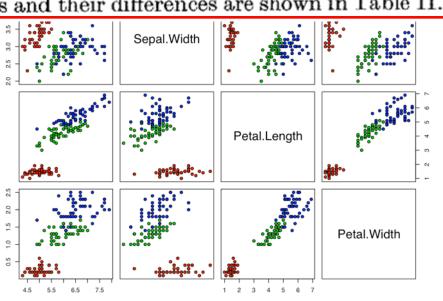
will maximize the ratio of the difference between the specific means to the standard deviations within species? The observed means and their differences are shown in Table II.

Q: How to choose the values of w?

<u>A</u>: Inverting the covariance matrices:

$$\vec{w} = (\mathbf{\Sigma}_A + \mathbf{\Sigma}_B)^{-1} \ (\vec{\mu}_A - \vec{\mu}_B)$$

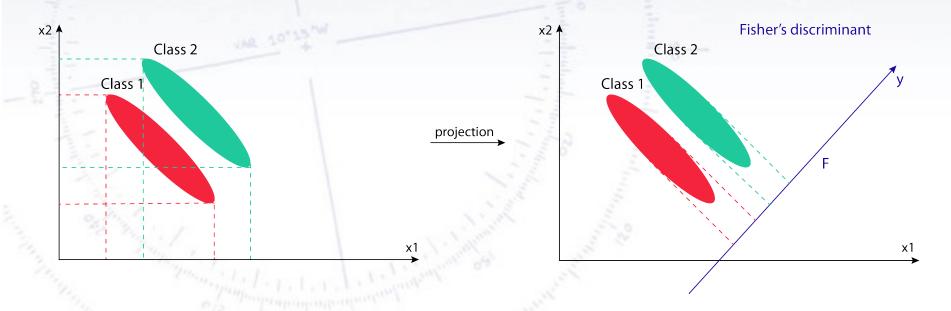
This can be calculated analytically, and incorporates the linear correlations into the separation capability.



Fisher's Linear Discriminant

Executive summary:

Fisher's Discriminant uses a linear combination of variables to give a single variable with the maximum possible separation (for linear combinations!).



It is for all practical purposes a projection (in a Euclidian space)!

Fisher's Linear Discriminant

The details of the formula are outlined below:

You have two samples, A and B, that you want to separate.

For each input variable (x), you calculate the mean (μ) , and form a vector of these.

$$\vec{w} = (\mathbf{\Sigma}_A + \mathbf{\Sigma}_B)^{-1} (\vec{\mu}_A - \vec{\mu}_B)$$

Using the input variables (x), you calculate the covariance matrix (Σ) for each species (A/B), add these and invert.

Given weights (w), you take your input variables (x) and combine them linearly as follows:

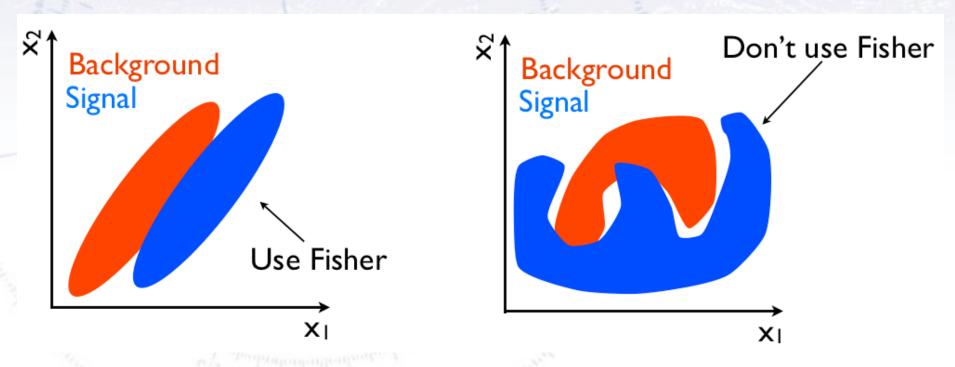
$$\mathcal{F} = w_0 + \vec{w} \cdot \vec{x}$$

F is what you base your decision on.

The non-linear case

Non-linear cases

While the Fisher Discriminant uses all separations and **linear correlations**, it does not perform optimally, when there are **non-linear correlations** present:



If the PDFs of signal and background are known, then one can use a likelihood. But this is **very rarely** the case, and hence one should move on to the Fisher. However, if correlations are non-linear, more "tough" methods are needed...

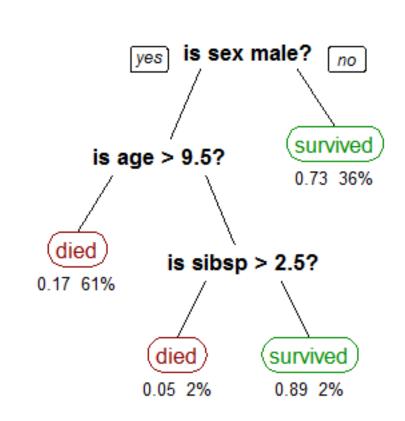
(Boosted) Decision Trees

Can become very complex.

Good for discrete problems. "Good for all problems!!!"

Not always highest efficiency.

Boosting adds to separation.



^{*} The example BDT shown is a simple example for predicting survival of Titanic!

Neural Networks

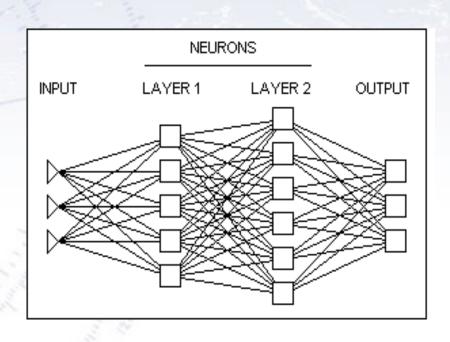
Can become very complex.

Good for continuous problems.

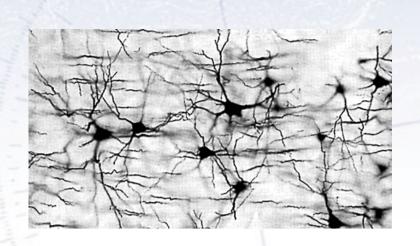
Sometimes hard to train!

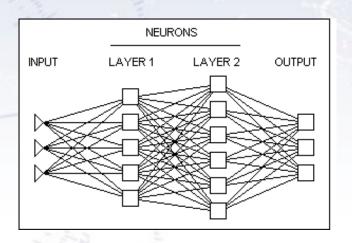
Can be used for images.

Easily produces multiple outputs.



Neural Networks (NN)





In machine learning and related fields, artificial neural networks (ANNs) are computational models inspired by an animal's central nervous systems (in particular the brain) which is capable of **machine learning** as well as **pattern recognition**.

Neural networks have been used to solve a wide variety of tasks that are hard to solve using ordinary rule-based programming, including **computer vision** and **speech recognition**.

Neural Networks

Neural Networks combine the input variables using a "activation" function s(x) to assign, if the variable indicates signal or background.

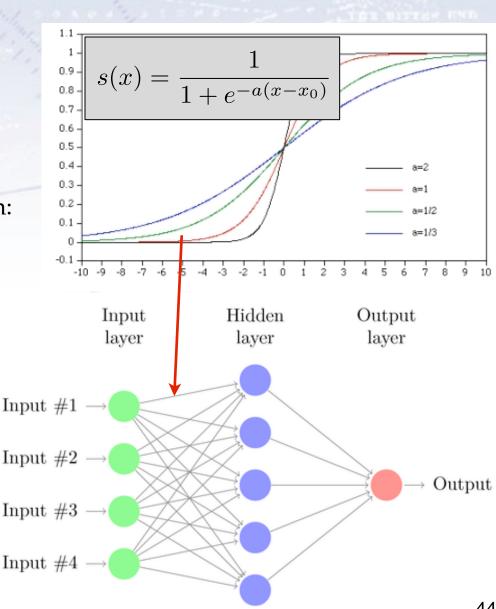
The simplest is a single layer perceptron:

$$t(x) = s\left(a_0 + \sum a_i x_i\right)$$

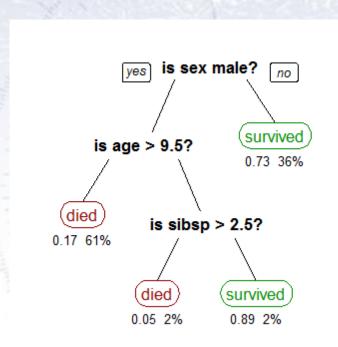
This can be generalised to a multilayer perceptron:

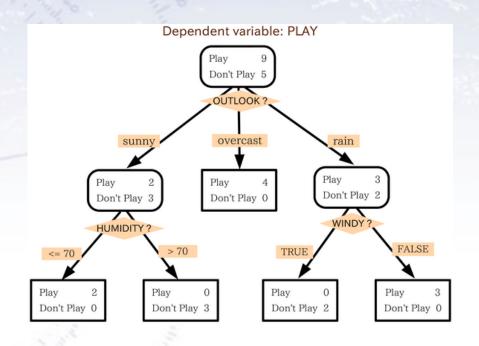
$$t(x) = s \left(a_i + \sum a_i h_i(x) \right)$$
$$h_i(x) = s \left(w_{i0} + \sum w_{ij} x_j \right)$$

Activation function can be any sigmoid function.



Boosted Decision Trees (BDT)





Decision tree learning uses a **decision tree** as a **predictive model** which maps observations about an item to conclusions about the item's target value. It is one of the predictive modelling approaches used in **statistics**, **data mining** and **machine learning**.

[Wikipedia, Introduction to Decision Tree Learning]

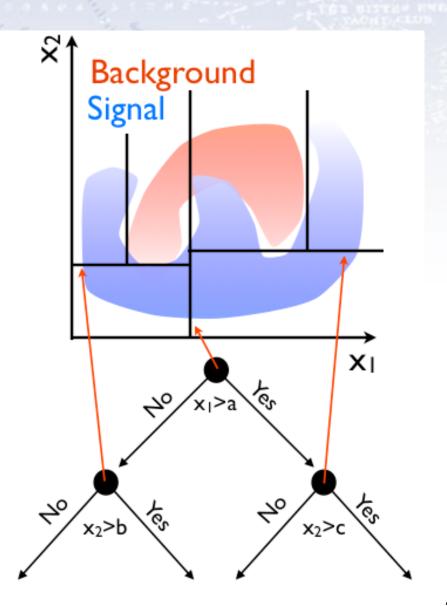
Boosted Decision Trees

A decision tree divides the parameter space, starting with the maximal separation. In the end each part has a probability of being signal or background.

- Works in 95+% of all problems!
- Fully uses non-linear correlations.

But BDTs require a lot of data for training, and is sensitive to overtraining (see next slide).

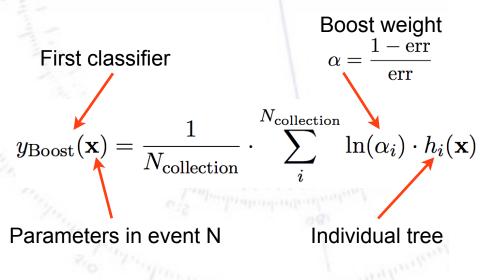
Overtraining can be reduced by limiting the number of nodes and number of trees.

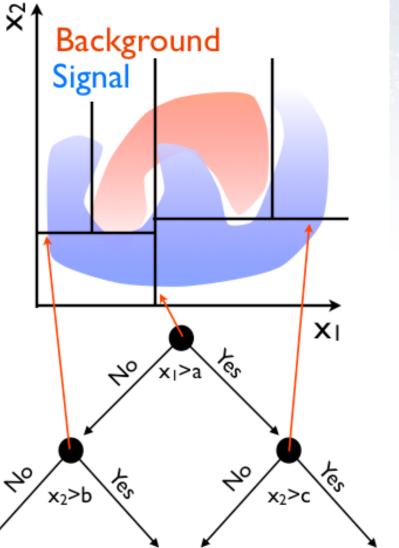


Boosting...

There is no reason, why you can not have more trees. Each tree is a simple classifier, but many can be combined!

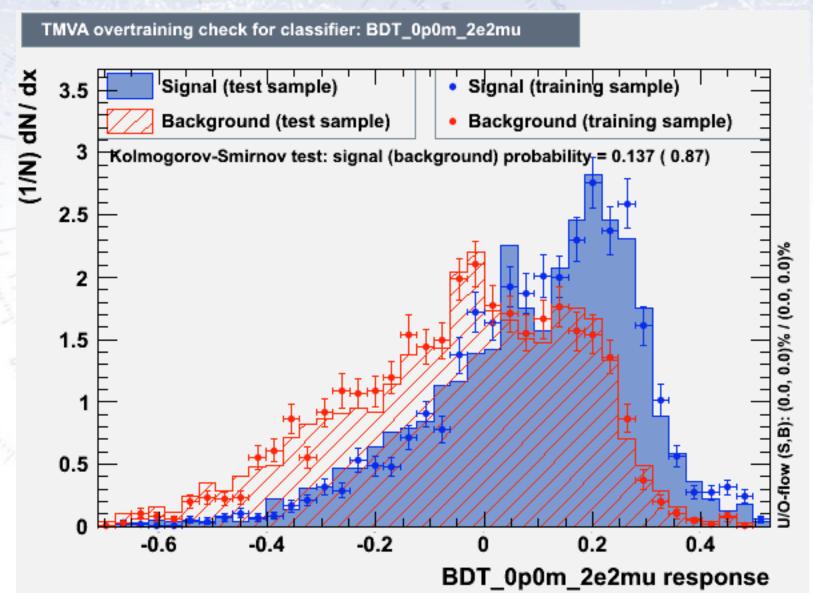
To avoid N identical trees, one assigns a higher weight to events that are hard to classify, i.e. boosting:





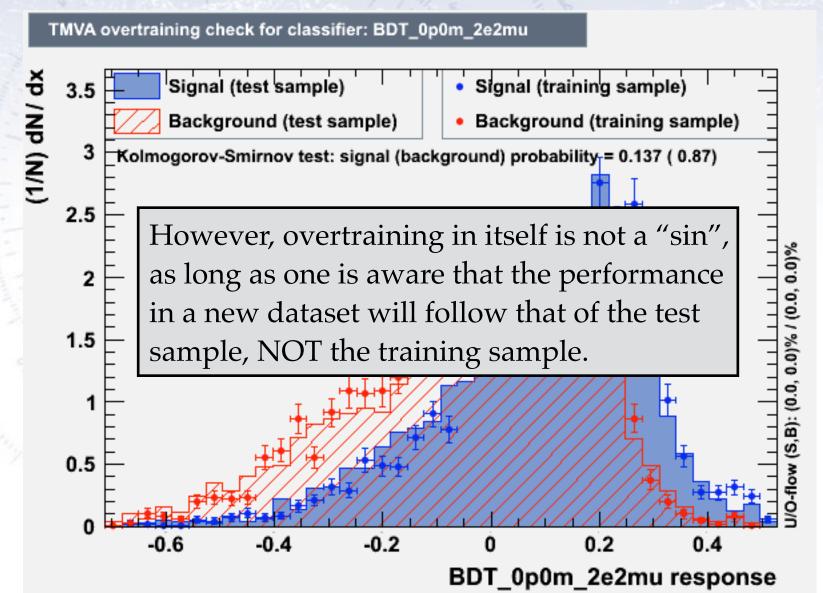
Test for simple overtraining

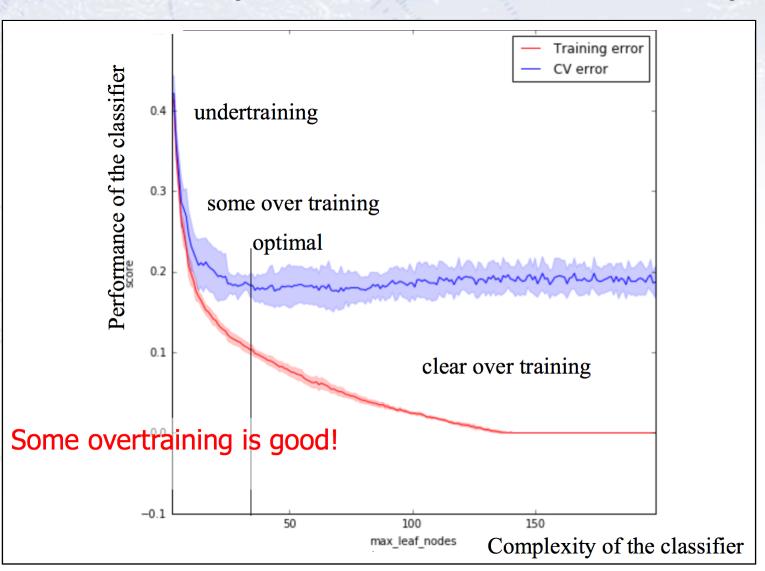
In order to test for overtraining, half the sample is used for training, the other for testing:

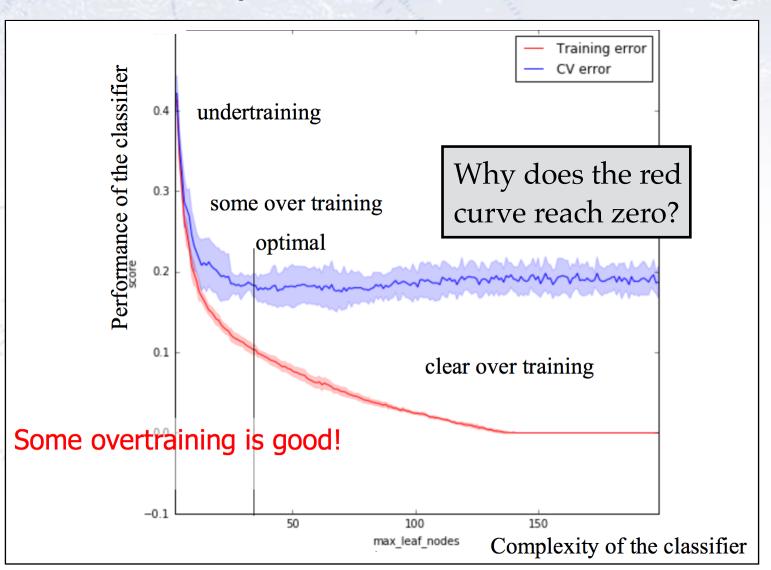


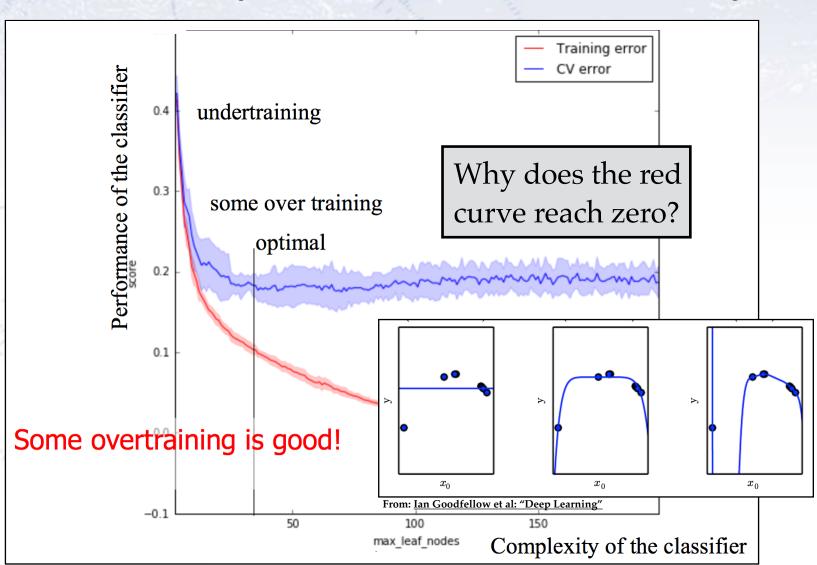
Test for simple overtraining

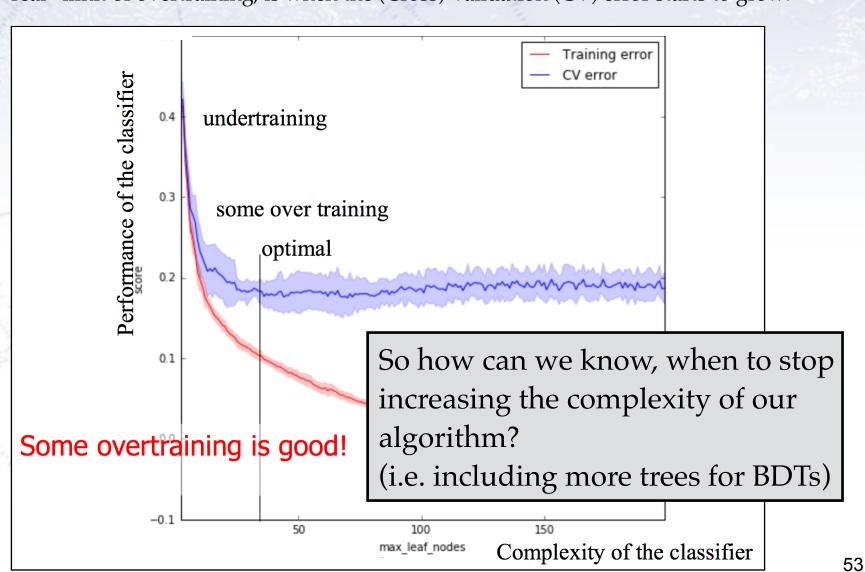
In order to test for overtraining, half the sample is used for training, the other for testing:

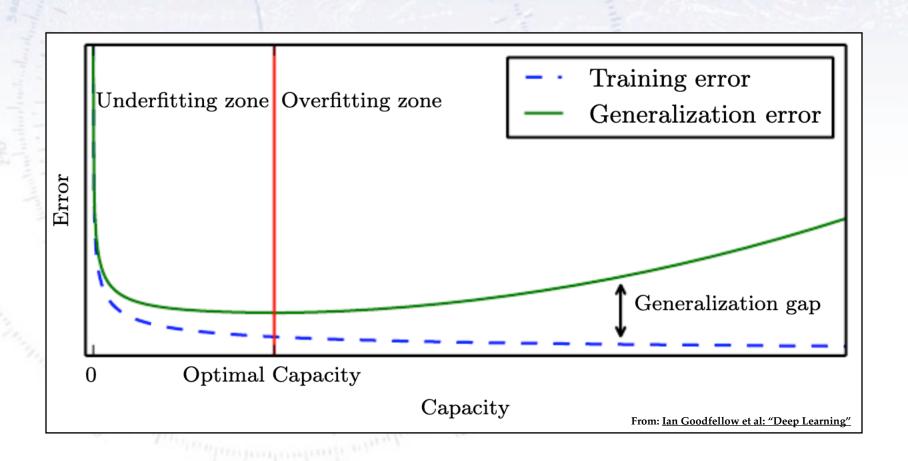












				111							
	CLASSIFIERS										
	CRITERIA	Cuts		PDE- RS	k-NN	H- Matrix		ANN	BDT	Rule- Fit	SVM
Perfor- mance	No or linear correlations	*	**	*	*	*	**	**	*	**	*
	Nonlinear correlations	0	0	**	**	0	0	**	**	**	**
Speed	Training	0	**	**	**	**	**	*	0	*	0
	Response	**	**	0	*	**	**	**	*	**	*
Robust- ness	Overtraining	**	*	*	*	**	**	*	0	*	**
	Weak variables	**	*	0	0	**	**	*	**	*	*
Curse of dimensionality		0	**	0	0	**	**	*	*	*	
Transparency		**	**	*	*	**	**	0	0	0	0
										•	

Table 1: Assessment of classifier properties. The symbols stand for the attributes "good" ($\star\star$), "fair" (\star) and "bad" (\circ). "Curse of dimensionality" refers to the "burden" of required increase in training statistics and processing time when adding more input variables. See also comments in text. The FDA classifier is not represented here since its properties depend on the chosen function.

Another comparison is done in Elements of Statistical Learning II (ESL II), where linear methods are not included.

As can be seen, Neural Networks are "difficult" in almost all respects, but performant.

For trees, the case is almost the opposite.

However, I don't agree with the evaluation of the predictive power of trees.

At least not for normal structured data.

Characteristic	Neural	SVM	Trees	MARS	k-NN,
	Nets				Kernels
Natural handling of data of "mixed" type	▼	V	A	A	▼
Handling of missing values	▼	•	A	A	A
Robustness to outliers in input space	▼	V	A	▼	A
Insensitive to monotone transformations of inputs	▼	V	A	▼	▼
Computational scalability (large N)	▼	•	A	A	▼
Ability to deal with irrelevant inputs	▼	•	A	A	▼
Ability to extract linear combinations of features	A	A	▼	▼	•
Interpretability	▼	▼	♦	A	▼
Predictive power	A	A	_	*	A

Another comparison is done in Elements of Statistical Learning II (ESL II), where linear methods are not included.

As can be seen, Neural Networks are "difficult" in almost all respects, but performant.

For trees, the case is almost the opposite.

However, I don't agree with the evaluation of the predictive power of trees.

At least not for normal structured data.

For tabular data, I disagree!

Characteristic	Neural	SVM	Trees	MARS	k-NN,
	Nets				Kernels
Natural handling of data of "mixed" type	▼	V	A	A	▼
Handling of missing values	▼	V	A	A	A
Robustness to outliers in input space	▼	▼	A	▼	A
Insensitive to monotone transformations of inputs	•	•	A	▼	▼
Computational scalability (large N)	▼	•	A	A	▼
Ability to deal with irrelevant inputs	•	•	A	A	▼
Ability to extract linear combinations of features	A	A	▼	▼	*
Interpretability	▼	V	•	A	▼
Predictive power	_			•	A

Another comparison is done in Elements of Statistical Learning II (ESL II), where linear methods are not included.

As can be seen, Neural Networks are "difficult" in almost all respects, but performant.

For trees, the case is almost the opposite.

However, I don't agree with the evaluation of the predictive power of trees.

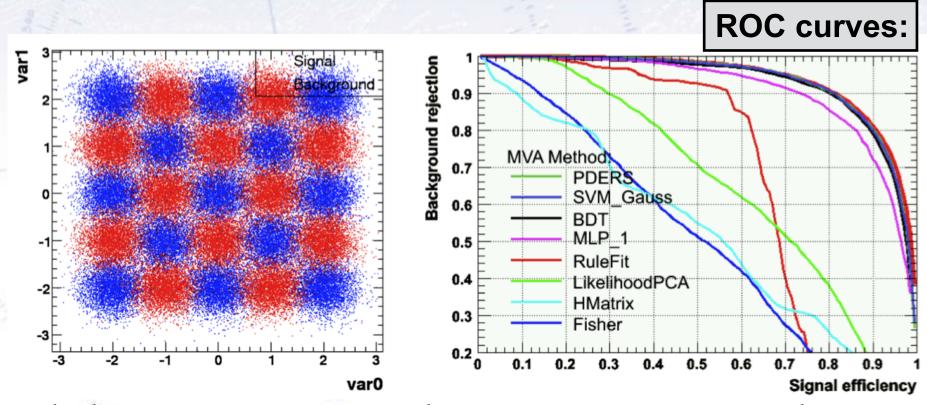
At least not for normal structured data.

For tabular data, I disagree!

Characteristic	Neural	SVM	Trees	MARS	k-NN,
	Nets				Kernels
Natural handling of data of "mixed" type	▼	•	A	A	•
Handling of missing values	▼	•	A	A	A
Robustness to outliers in input space	▼	V	A	▼	A
Insensitive to monotone transformations of inputs	▼	•	A	▼	▼
Computational scalability (large N)	▼	•	A	A	▼
Ability to deal with irrelevant inputs	•	•	A	A	•
Ability to extract linear combinations of features	A	A	▼	▼	•
Interpretability	▼	V	•	A	▼
Predictive power	_			•	A

Performance comparison

Left figure shows the distribution of signal and background used for test. Right figure shows the resulting separation using various MVA methods.

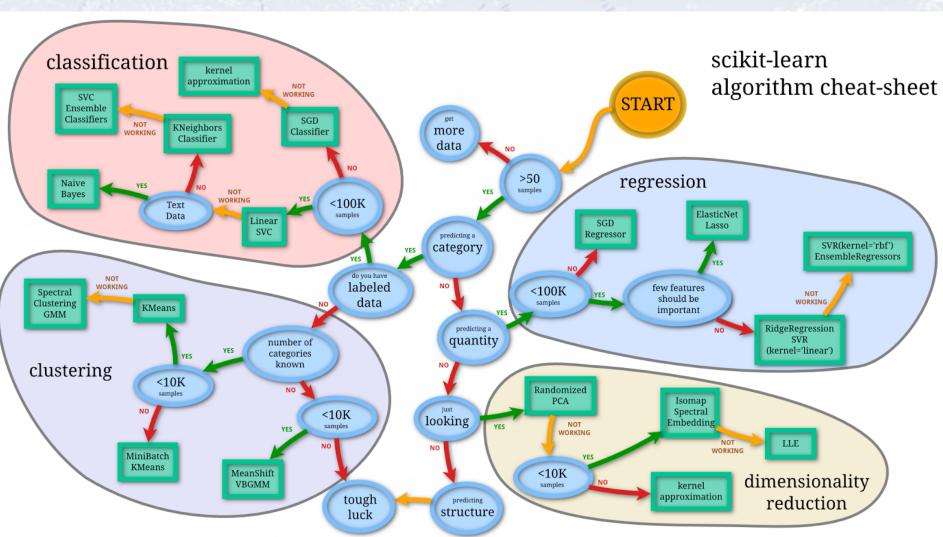


The theoretical limit is known from the Neyman-Pearson lemma using the (known/correct) PDFs in a likelihood.

In all fairness, this is a case that is great for the BDT...

Which method to use?

There is no good/simple answer to this, though people have tried, e.g.:



Which method to use?

There is no good/simple answer to this, though people have tried, e.g.:

