Machine Learning

Rudolf Mayer
mayer@ifs.tuwien.ac.at

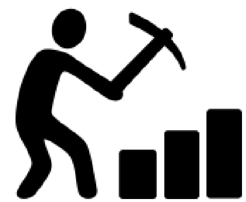
October 2^{nd}, 2025

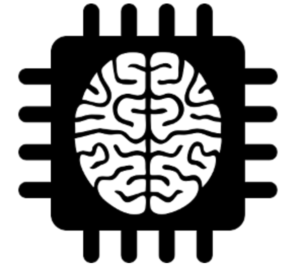
Outline

- Machine Learning: Intro
- Types of data & data preparation (very brief intro)

Defining the area

- Some related (?) terms
  - Data Mining
  - Predictive analytics
  - Knowledge discovery
  - Data Science
  - Statistics
  - Cluster Analysis
  - Artificial Intelligence
  - Reasoning / deduction
  - Regression
  - Classification
  - Supervised/ unsupervised learning
  - ...

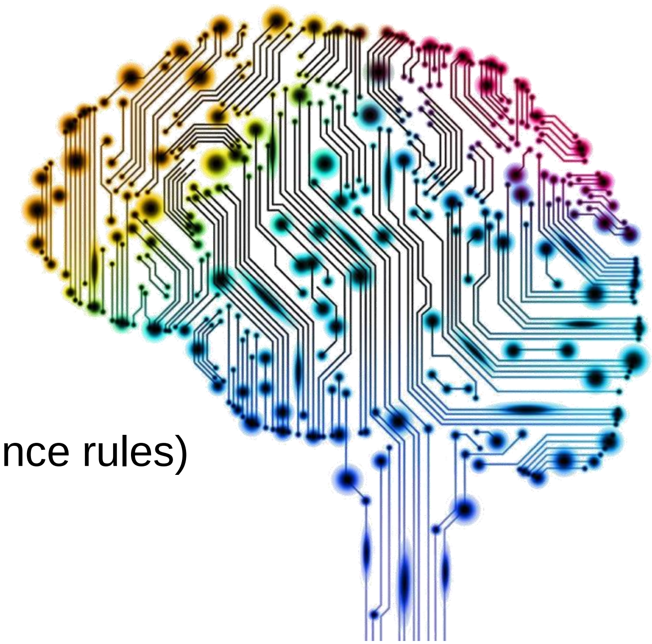




Artificial intelligence

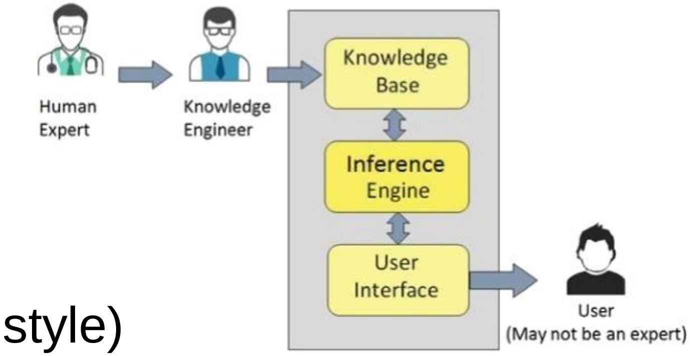
- Deals with intelligence of machines
  - *System that perceives its environment & takes actions that maximise its chances of success*

- Areas/problems of AI
  - Deduction, reasoning, problem solving
    - Often rule-based; manually created
  - Knowledge representation (reasoning)
    - Reasoning: generation of new knowledge (inference rules)
  - ***Machine learning***
  - Planning / scheduling
  - Natural language processing
  - …



Rule-based systems

- System that uses rules to make deductions or choices
  - E.g. domain-specific expert system

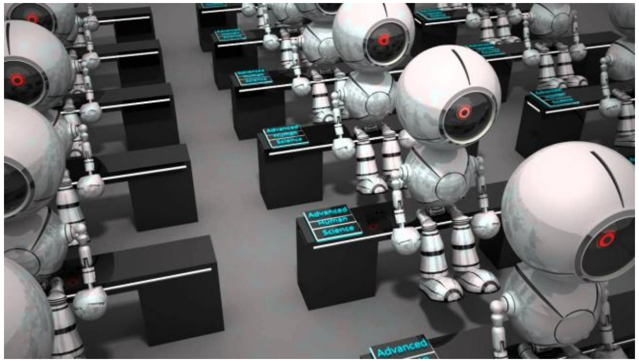


- Two components
  - Knowledge base: facts & rules (if → then style)
    - Knowledge representation (language)
    - Example rule: *IF (hot & smoke) THEN fire*
  - Inference engine: applies rules to deduce new facts
    - Forward chaining: assert new facts
    - Backward chaining: start with goal → determine which facts need to asserted
- Cf. Ontologies & reasoning
- Rules often manually specified (by expert)
  - Expensive, not easy to be complete
  - ***Does not scale well*** ➔ enter Machine Learning?

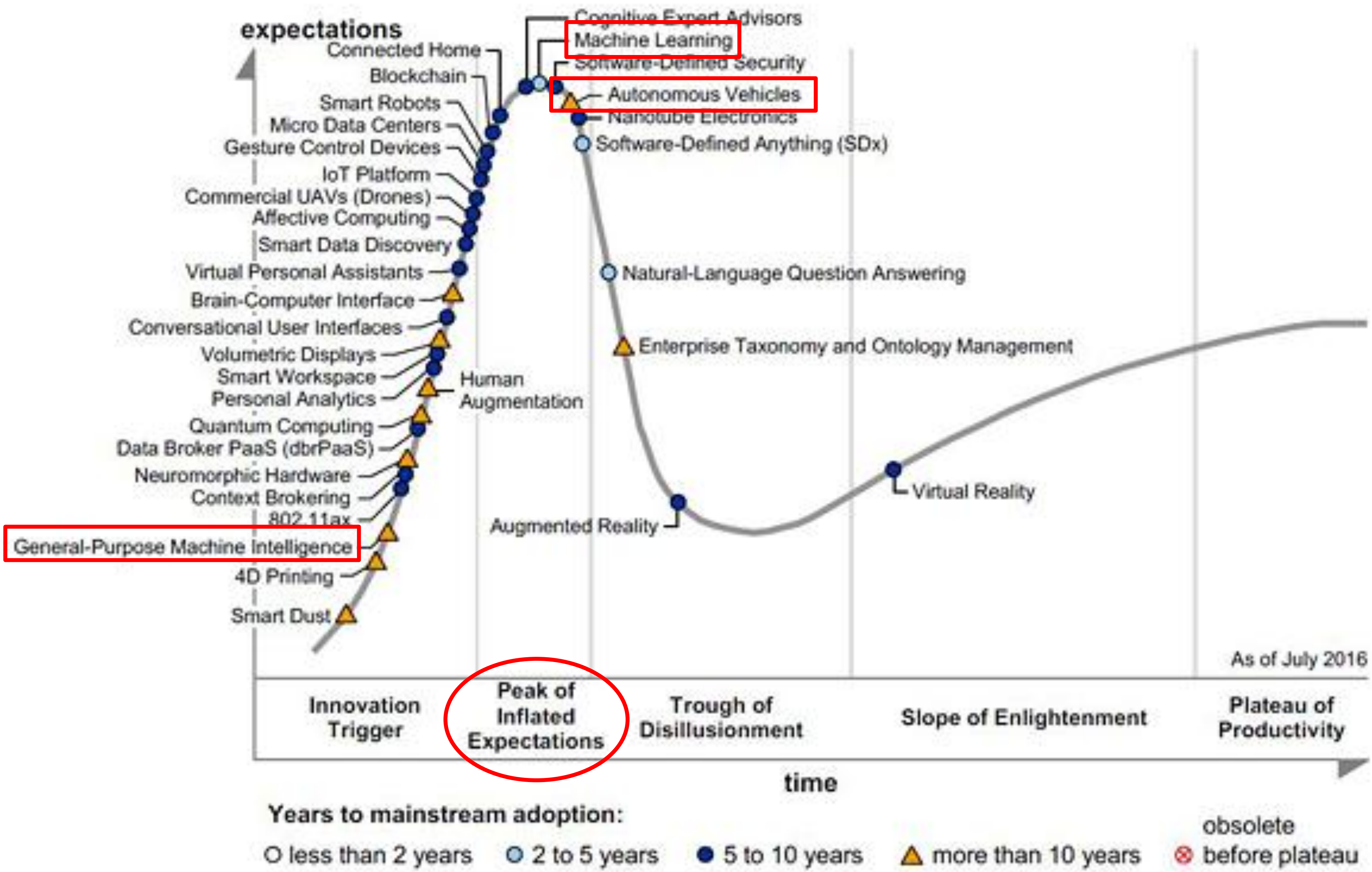
Machine learning

- Studies computer algorithms that can ***learn*** from data and make ***predictions*** on data
  - *"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" (Tom Mitchell)*

- Automatic methods – no human assistance in learning (i.e. no specification of rules!)
  - Human assistance generally required for
    - Defining problem
    - Gathering and assessing data

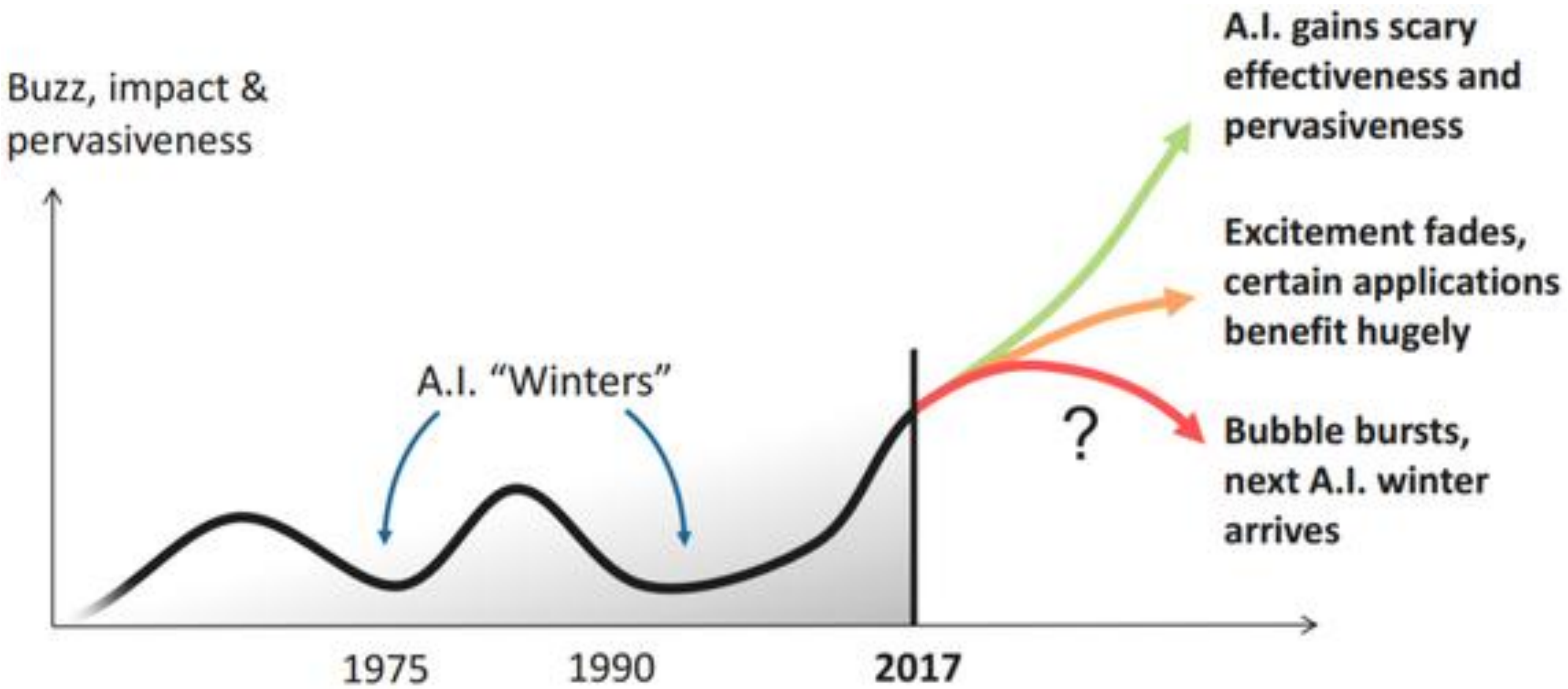


Machine learning – why?

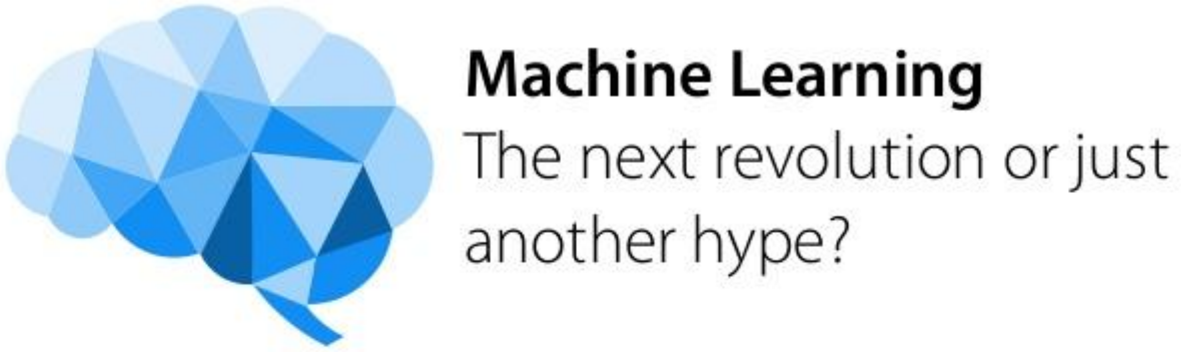


Source: Gartner (July 2016)

Machine learning – hype?



Machine learning – Hype



- A little bit of both ...

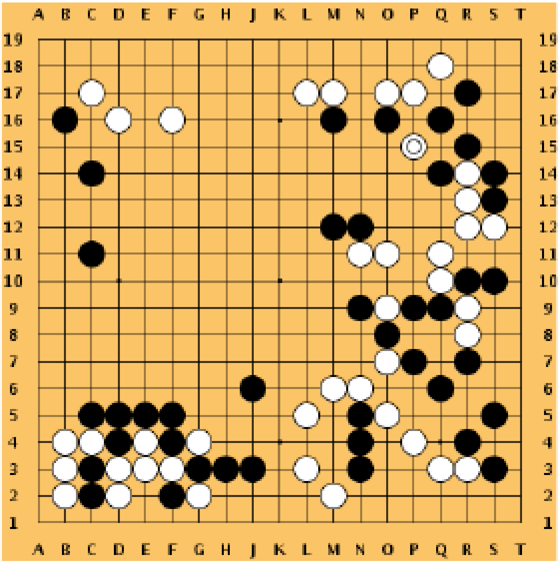
ML success stories: skin cancer diagnosis

- Deep Learning used to diagnose skin cancer from images
- Learns from examples
- Matched performance of certified dermatologists

Nature 542, 115–118
(02 February 2017),
doi:10.1038/nature21056

ML success stories: AlphaGo

- DeepMind’s AlphaGo beats Lee Sedol, one of the best Go players (March 2016)
  - Uses combination of Monte Carlo Simulation & Deep Learning



ML success stories: AlphaGo Zero

- AlphaGo Zero: not using any human generated *example* game data (October 2017)
  - Learns by playing “against itself” (from successful games)
  - Reaches level of 2016 AlphaGo (Lee Sedol) in 3 days
  - Implemented on very special hardware
    - Google’s TPU (Tensor Processing Unit)

science.ORF.at

Fernsehen TVthek Radio Debatte Österreich Wetter IPTV Sport News

Go-Champion ohne menschliches Zutun

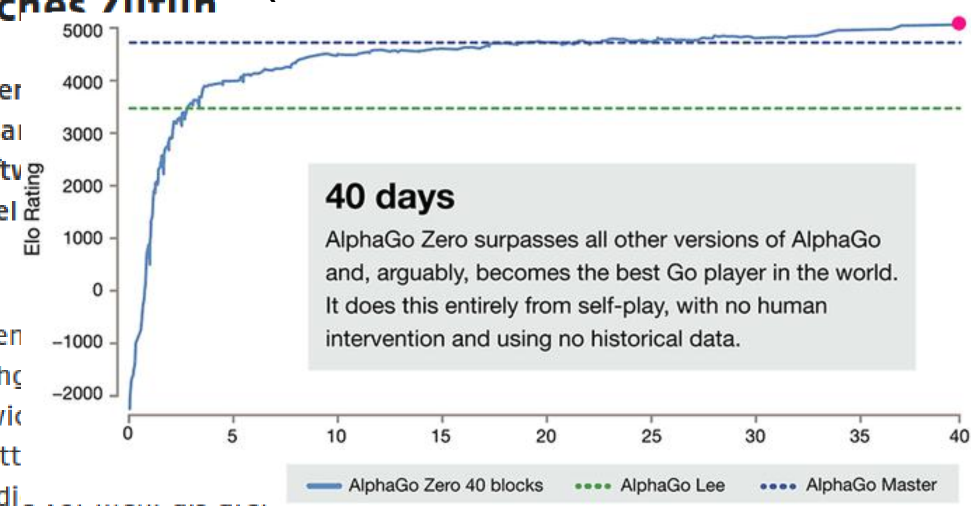
Das Aufsehen war groß, als AlphaGo 2016 der
Sedol im Brettspiel Go besiegte. Forscher, da
österreichischer Informatiker, haben die Softw
Ohne menschliches Zutun lernte sie das Spiel
Vorgängerversion.

AlphaGo hat sich heuer auch mit einem glatten
vermutlich weltbesten Go-Spieler Ke Jie durch
Erfolgen wurde ersichtlich, wie weit die Entwic
Künstlicher Intelligenz (KI) bereits fortgeschritt
stammt von der britischen Firma DeepMind, di
Jahren vom US-Konzern Google übernommen wurde.

Die Studie

„Mastering the game of Go without human knowledge“, Nature, 18.10.2017

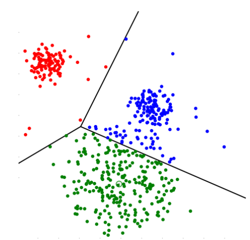
Besonders überraschend waren die Fähigkeiten von AlphaGo, weil das rund 3.000 Jahre alte asiatisch Spiel spezielle Anforderungen stellt, die bisher eher dem menschlichen Geist exklusiv zugebilligt wurden. Angesichts fast unbegrenzter Möglichkeiten für Züge, ist nämlich viel Intuition, kreatives Denken und Lernfähigkeit gefragt.



ML success stories: image manipulation

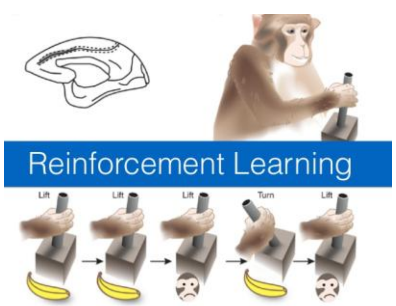
Machine learning: disciplines

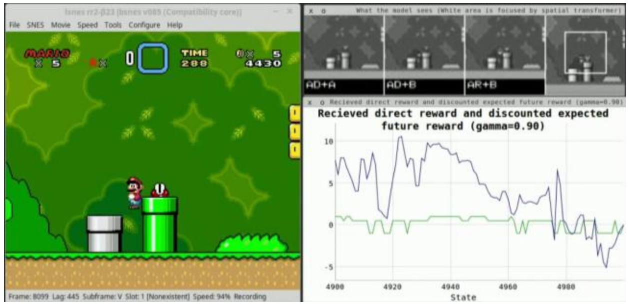
- ML can take several forms, depending on the data and the task
- Common sub-disciplines
  - Unsupervised Learning
    - Clustering, collaborative filtering, outlier detection, ...

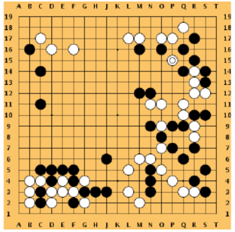


  - Supervised Learning
    - Classification, Regression, ...

  - Reinforcement Learning

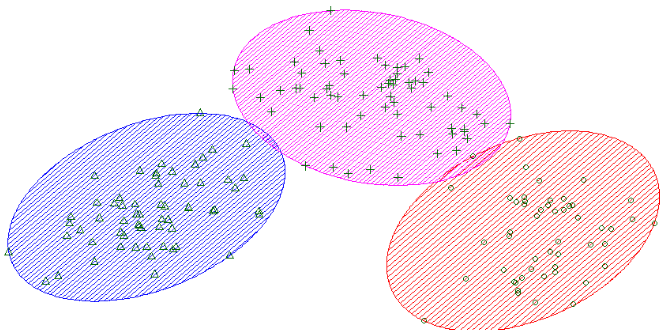






Unsupervised Learning

- Unsupervised learning
  - Data not ***labelled***
  - No information on which and how many classes or other structures, …
  - Goal:
    - Find structures (e.g. clustering)
    - Association rules learning
    - Find outliers (anomalies)

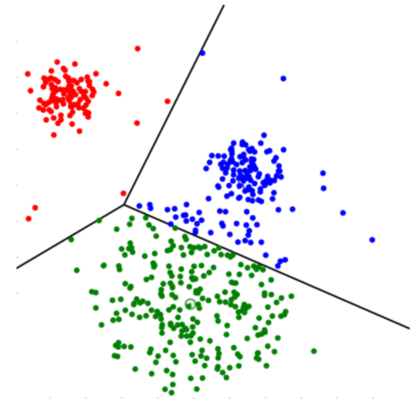


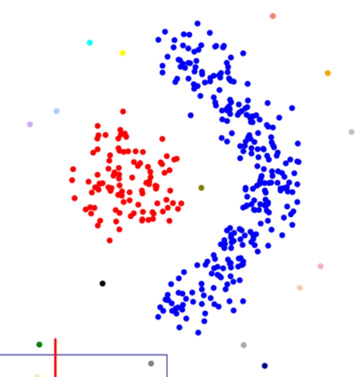
  - Often associated with ***Data Mining***

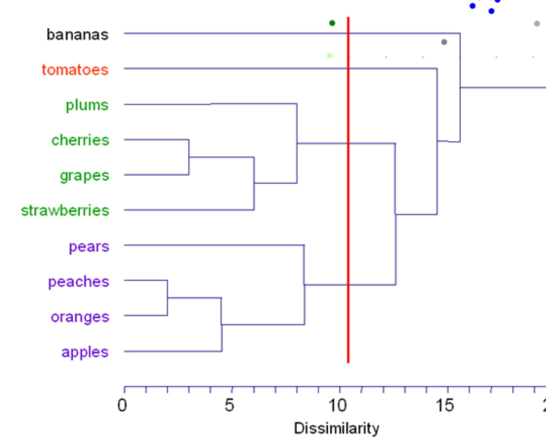
- *Not covered in this lecture*

Cluster analysis

- Explorative method
- Find groups of similar objects
- Applications: e.g. market segmentation







Cluster analysis

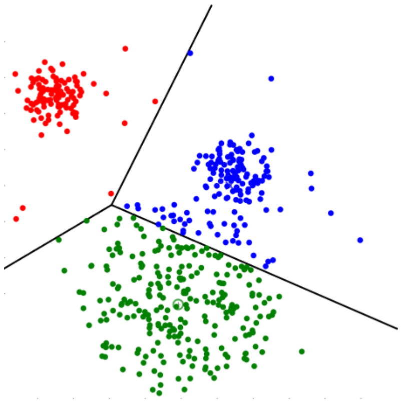
	size	*legs*	*feathers*	*eggs*
duck	small	2	yes	yes
dog	medium	4	no	no
spider	tiny	8	no	yes
ladybird	tiny	6	no	yes
cow	large	4	no	no
bee	tiny	6	no	no
sparrow	small	2	yes	yes

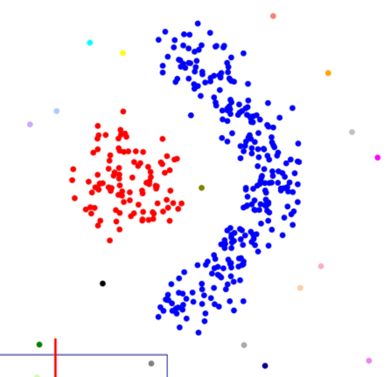
- Animal data set
  - Describes animal by some characteristics
    - Size (tiny, small, medium, big)
    - Number of legs (2, 4, 6, 8)
    - Feathers (yes/no)
    - Eggs (yes/no)
  - Instances: cow, duck, cat, bee, sparrow, ...

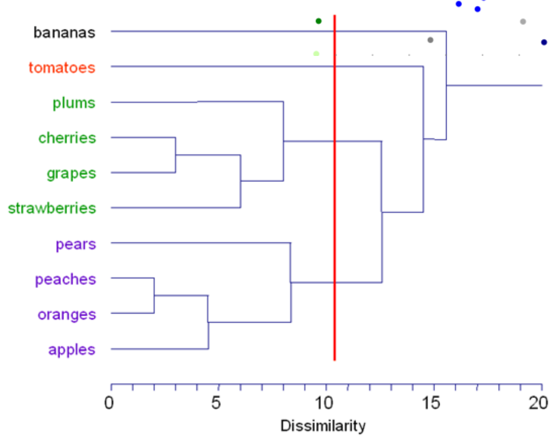
- Goal: find groups of related animals:
  - Cat, cow (Mammals)
  - Duck, sparrow (Birds)
  - Bee, ladybird (Insects)
  - Spider (Invertebrate)

Cluster analysis

- Explorative method
- Find groups of similar objects
- Applications: e.g. market segmentation
- Several popular algorithms
  - K-means clustering (centroid based)
  - DBSCAN (density-based)
  - Linkage (hierarchical)
    - single, complete, average, Ward, ..



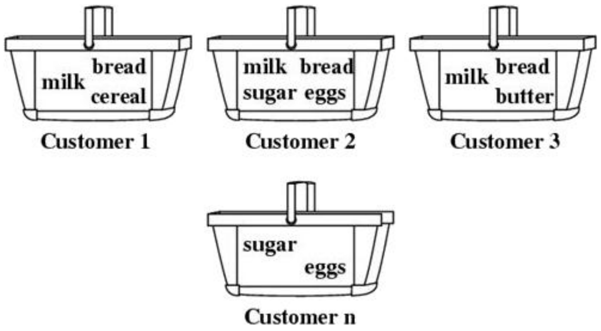




Association rule mining

- Discover relations between variables
  - E.g. market basket analysis: which items are frequently bought together

  ➔ Useful for marketing
  - Identify rules that are
    - Frequent (“support”)
    - Reliable (“confidence”)



  - Anecdotal example: beer & diapers

  - Related: collaborative filtering / recommender systems

Supervised Learning

- Supervised learning
  - Data labelled with actual ***output*** variable
  - Goal: correctly label ***unknown*** data

  - Sometimes equivalently used with “machine learning”
    - In some definitions, machine learning means both unsupervised and supervised learning
    - In other definitions, unsupervised learning mostly equals/is a subset of data mining; and rather seen as part of statistics

- *Types of supervised learning?*
  - Regression & Classification

Regression vs. Classification

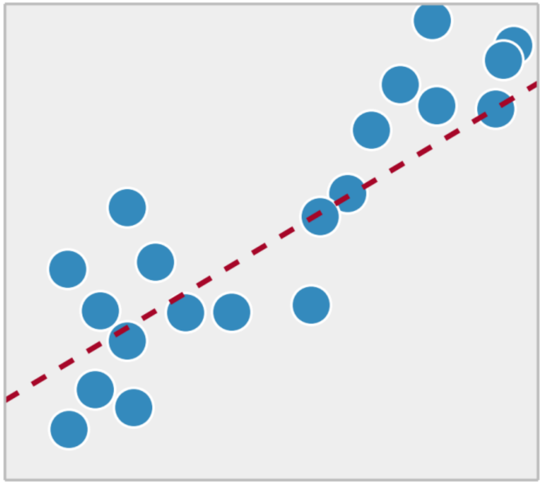
- Regression tries to predict a ***continuous*** variable

  – Examples?

Regression vs. Classification

- Regression tries to predict a ***continuous*** variable
  - *Income of a house hold* (depending on education, ...)
  - *Temperature* (depending on wind, humidity...)
  - *Housing price* (depending on e.g. size, age..)

  - Methods: e.g. *linear regression*
    - Mostly associated with statistics
  - Many classification methods can also be used for regression



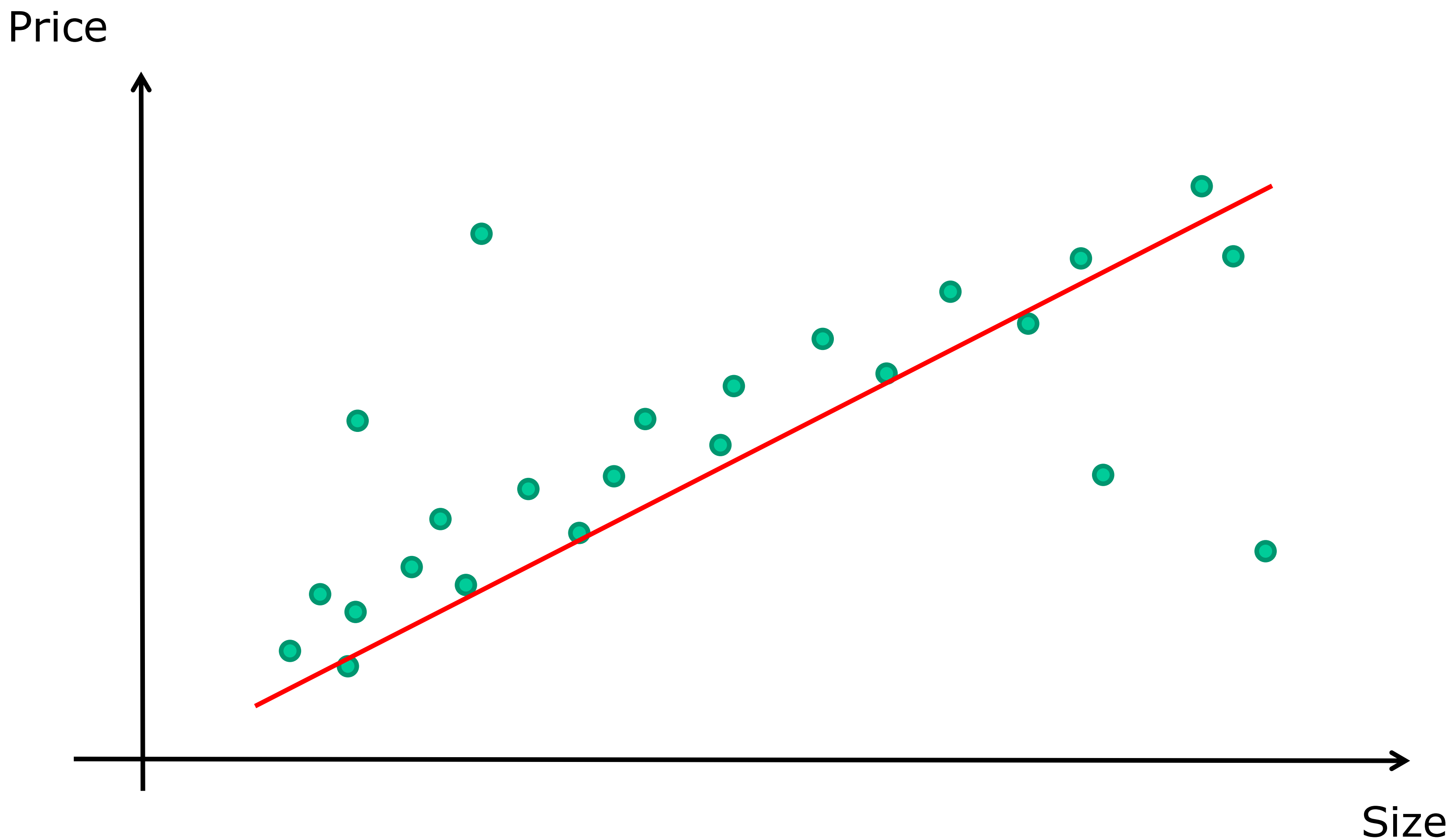
Regression example

- Data set about prices of houses (apartments)
- Input data e.g.
  - Size
  - Number of rooms
  - Size of garden/balcony/terrace
  - Year built / age of building
  - Location
- Goal: predict the expected price of the house in €

- Solution: multivariate regression
  - *If only one input: univariate regression*

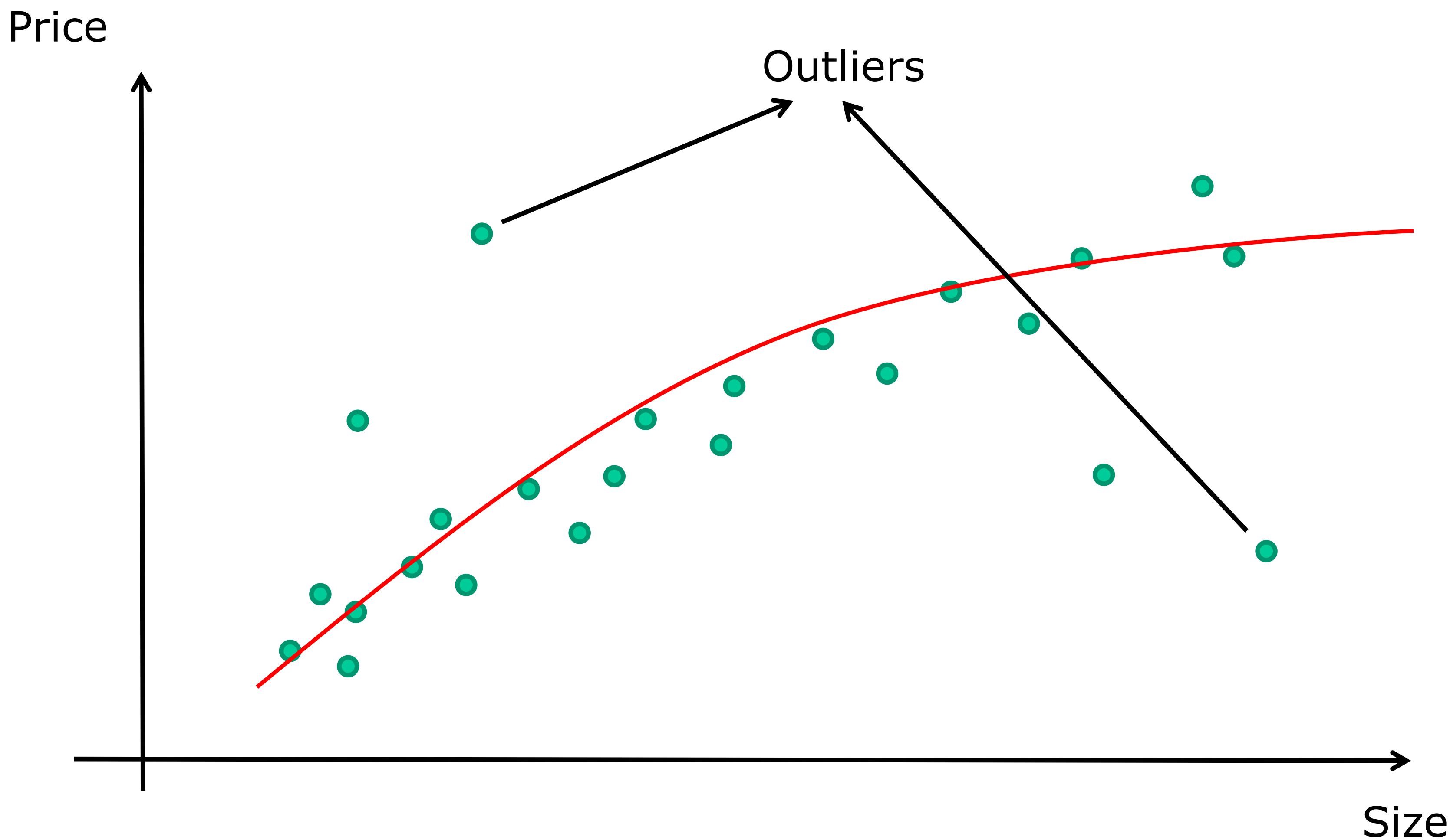
Regression example

Linear regression – find a “line” that describes the data



Regression example

Polynomial regression – find a "curve" that describes the data



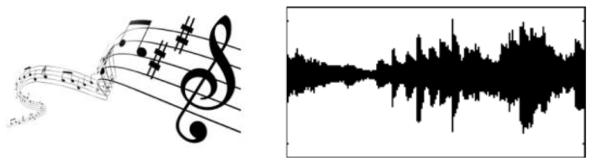
Regression vs. Classification

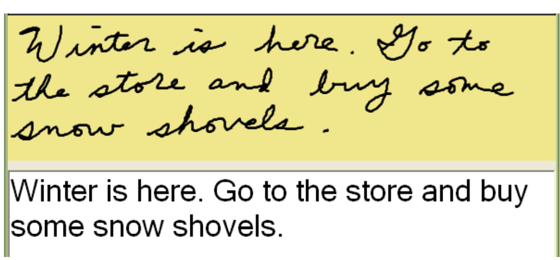
- If the output variable can take one of a predefined set of values: ***classification*** *(also: categorisation)*

  – Examples?

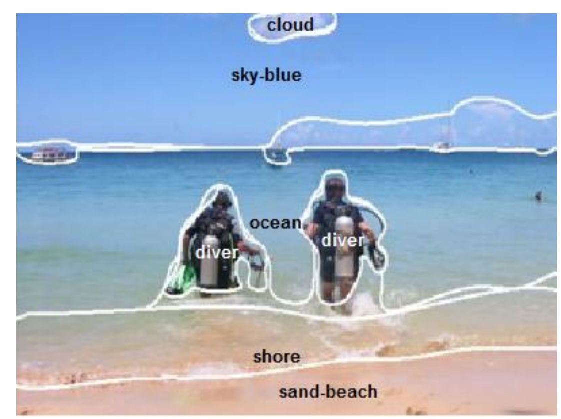
Regression vs. Classification

- If the output variable can take one of a predefined set of values: ***classification*** *(also: categorisation)*




Winter is here. Go to the store and buy some snow shovels.

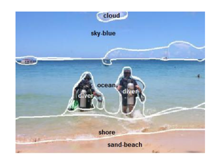
Winter is here. Go to the store and buy some snow shovels.



Regression vs. Classification

- If the output variable can take one of a predefined set of values: ***classification*** *(also: categorisation)*
  - ***Information***: SPAM filtering

  - ***Image***: classification of hand-written letters for OCR; automatic labelling of images



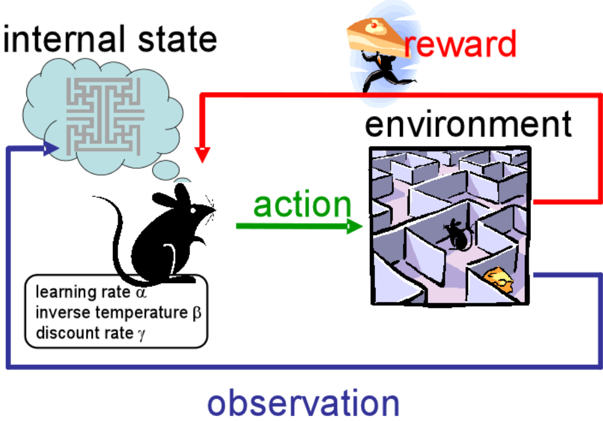
  - ***Music***: classification of music into genres

  - ***Medicine***: classification of whether a person has an illness, based e.g. on x-ray images, or other measurements

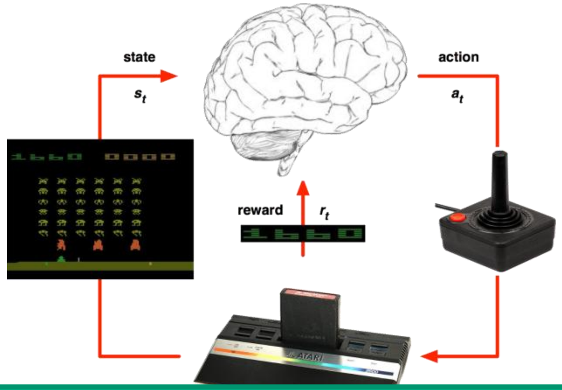
Reinforcement Learning

- Agent (e.g. computer program) takes actions in specified environment
  - – Not explicitly presenting input/output pair
  - – Reward (penalise) agent for actions

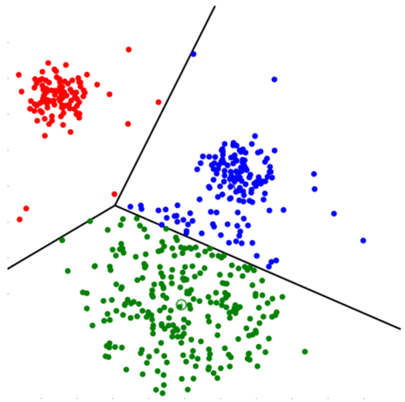
  ➔ Maximise cumulative reward

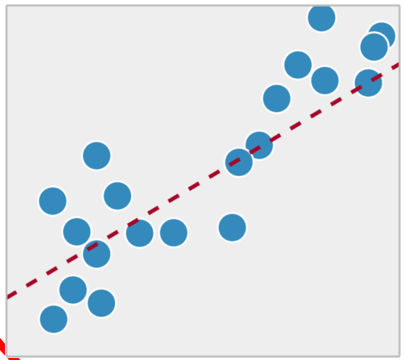


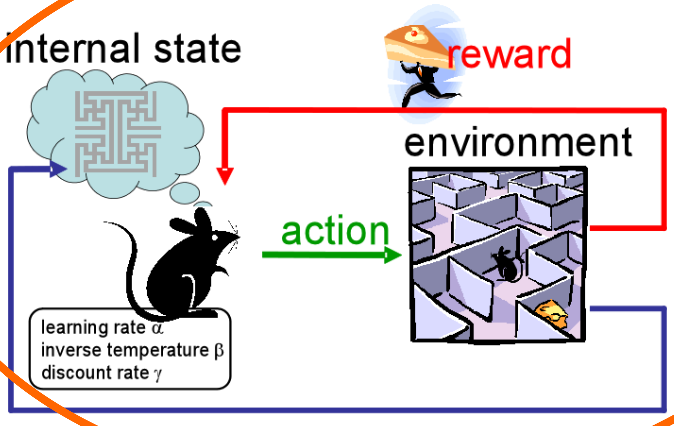
- Popular applications?



Scoping the lecture







Classification: Setting

- Example: data set describing characteristics of patients *("experience E")*
  - Sex
  - Age
  - Smoker yes/no
  - Eye colour
- Want to predict whether a person has lung cancer *("task T")*
  - Available: some data with a label / annotation (cancer yes(no)

- Measure the number of correct predictions (accuracy, *"performance P")*

Classification: Setting

Attributes / Variables / Features

Output Variable

Training Samples

sex	age	smoker	eye colour
male	19	yes	green
female	44	yes	grey
male	49	yes	blue
male	12	no	brown
female	37	no	brown
female	60	no	brown
male	44	no	blue
female	27	yes	brown
female	51	yes	green
female	81	yes	grey
male	22	yes	brown
male	29	no	blue

lung cancer
No
yes
yes
no
no
yes
no
no
yes
no
no
no

Ground Truth / Gold standard

male	77	yes	grey
male	19	yes	green
female	44	no	grey

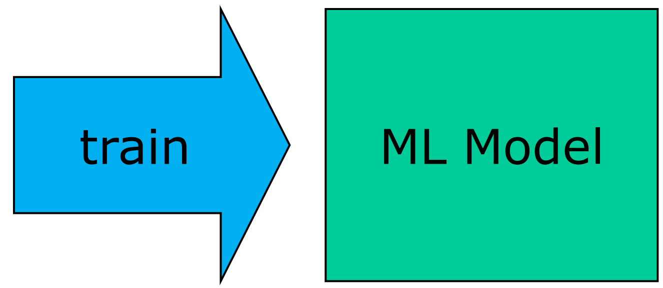
?
?
?

Prediction

Unlabelled samples

Classification: Setting

sex	age	smoker	eye colour	lung cancer
male	19	yes	green	No
female	44	yes	grey	yes
male	49	yes	blue	yes
male	12	no	brown	no
female	37	no	brown	no
female	60	no	brown	yes
male	44	no	blue	no
female	27	yes	brown	no
female	51	yes	green	yes
female	81	yes	grey	no
male	22	yes	brown	no
male	29	no	blue	no

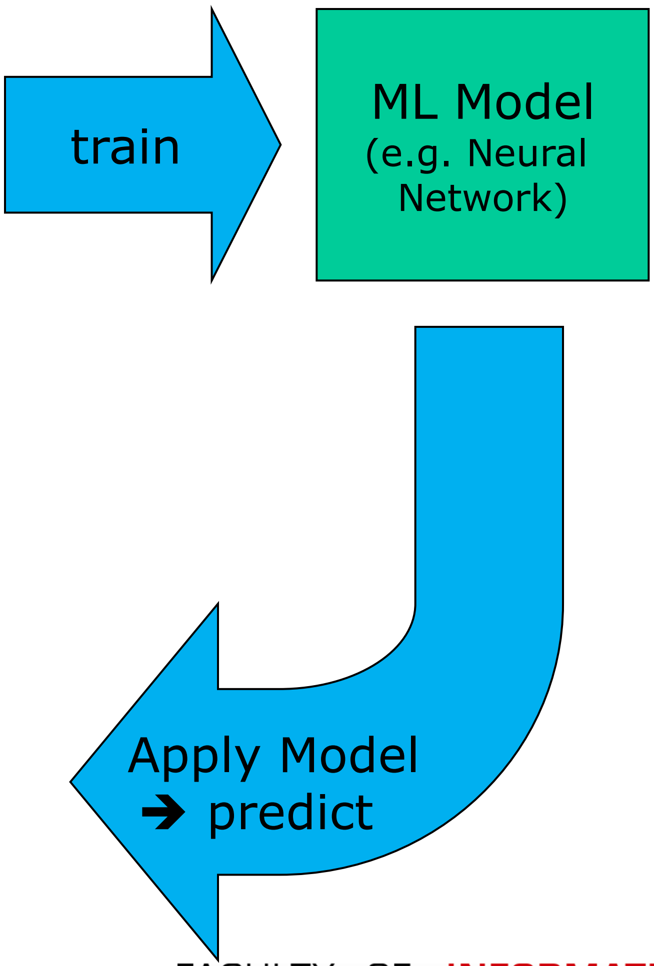


male	77	yes	grey	?
male	19	yes	green	?
female	44	no	grey	?

Classification: Setting

sex	age	smoker	eye colour	lung cancer
male	19	yes	green	No
female	44	yes	grey	yes
male	49	yes	blue	yes
male	12	no	brown	no
female	37	no	brown	no
female	60	no	brown	yes
male	44	no	blue	no
female	27	yes	brown	no
female	51	yes	green	yes
female	81	yes	grey	no
male	22	yes	brown	no
male	29	no	blue	no

male	77	yes	grey	yes
male	19	yes	green	no
female	44	no	grey	yes



Classification: Setting

Experience E

sex	age	smoker	eye colour
male	19	yes	green
female	44	yes	grey
male	49	yes	blue
male	12	no	brown
female	37	no	brown
female	60	no	brown
male	44	no	blue
female	27	yes	brown
female	51	yes	green
female	81	yes	grey
male	22	yes	brown
male	29	no	blue

lung cancer
No
yes
yes
no
no
yes
no
no
yes
no
no
no

train

ML Model
(e.g. Neural Network)

Apply Model
➔ predict

male	77	yes	grey
male	19	yes	green
female	44	no	grey

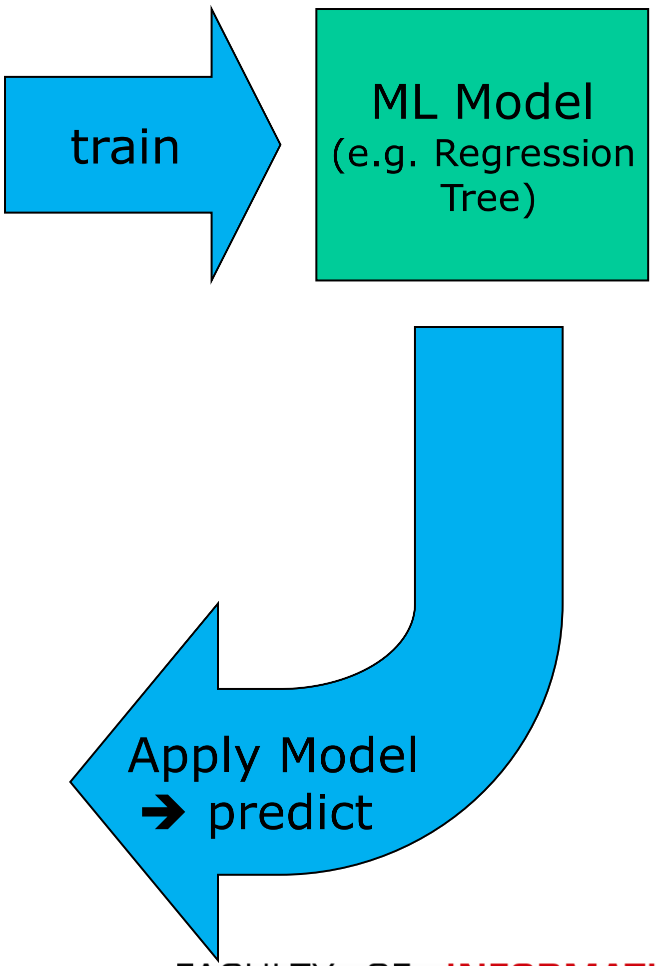
yes
no
yes

Task T

Regression: Setting

size	age	location	rooms	price
70	19	good	3	370000
60	44	good	2	165000
120	49	good	5	575000
90	12	bad	3	225000
80	37	bad	3	268000
45	60	bad	2	159000
52	44	bad	2	185000
85	27	good	4	472000
50	51	good	1	164000
35	81	good	1	155000
75	22	good	3	391000
95	29	bad	4	478000

35	77	good	4	274000
25	19	good	1	122000
85	44	bad	2	162000



Machine Learning: Setting

sex	age	smoker	eye colour
male	19	yes	green
female	44	yes	grey
male	49	yes	blue
male	12	no	brown
female	37	no	brown
female	60	no	brown
male	44	no	blue
female	27	yes	brown
female	51	yes	green
female	81	yes	grey
male	22	yes	brown
male	29	no	blue

lung cancer
No
yes
yes
no
no
yes
no
no
yes
no
no
no

male	77	yes	grey
male	19	yes	green
female	44	no	grey

?
?
?

- *Where do we get the data from?*

Machine Learning: Setting

sex	age	smoker	eye colour
male	19	yes	green
female	44	yes	grey
male	49	yes	blue
male	12	no	brown
female	37	no	brown
female	60	no	brown
male	44	no	blue
female	27	yes	brown
female	51	yes	green
female	81	yes	grey
male	22	yes	brown
male	29	no	blue

lung cancer
No
yes
yes
no
no
yes
no
no
yes
no
no
no

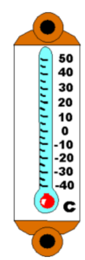
male	77	yes	grey
male	19	yes	green
female	44	no	grey

?
?
?

- Features:
  - Observation / measurement
  - *Extraction from media*
  - *(Transformation)*
- Labels (groundtruth):
  - Human experts
  - (Observation / measurement)

Machine Learning: Setting

Observation / Measurements



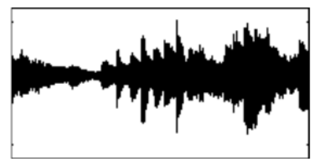
$

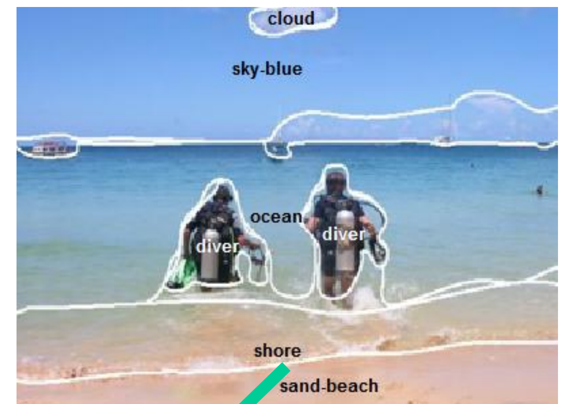
Annotations
(human experts)

Measurement/observation

Machine Learning: Setting

Feature Extraction





Human experts

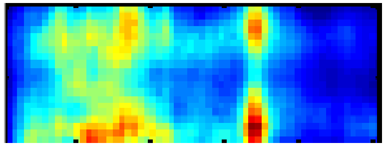
Machine Learning: Setting

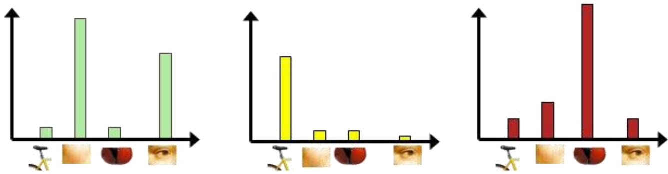
- Feature Extraction: description of complex content by derived, ***numeric*** values
  – Text: Bag of Words – counting term occurrences
  – Music: counting activity on various frequencies
  – Image: colour histograms, edge detection, “bag of visual words”, ...

- Important aspect of many data science applications
  – Overview/intro in this course
  – *More details e.g. Information retrieval (188.412), ...*

Machine Learning: Setting

	Word 1	Word 2	Word 3	Word 4	Word 5	...	Word n	∑
Doc 1	1	0	0	2	3		0	6
Doc 2	2	0	0	0	2		2	6
Doc 3	1	3	0	0	1		5	10
Doc 4	2	0	0	2	0		2	6
Doc 5	5	4	0	0	1		0	10
...							0	
Doc m	1	2	1	3	0		0	7

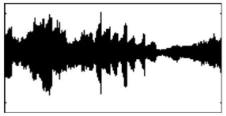


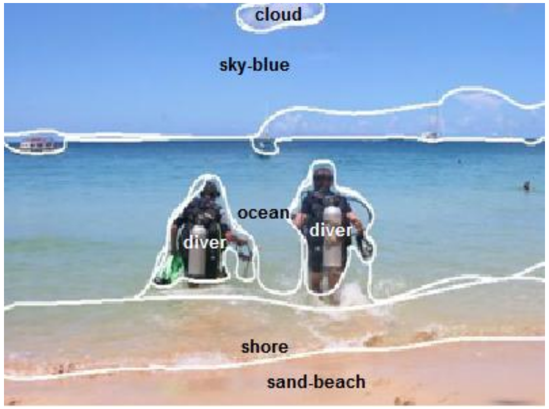


Text Feature Extraction

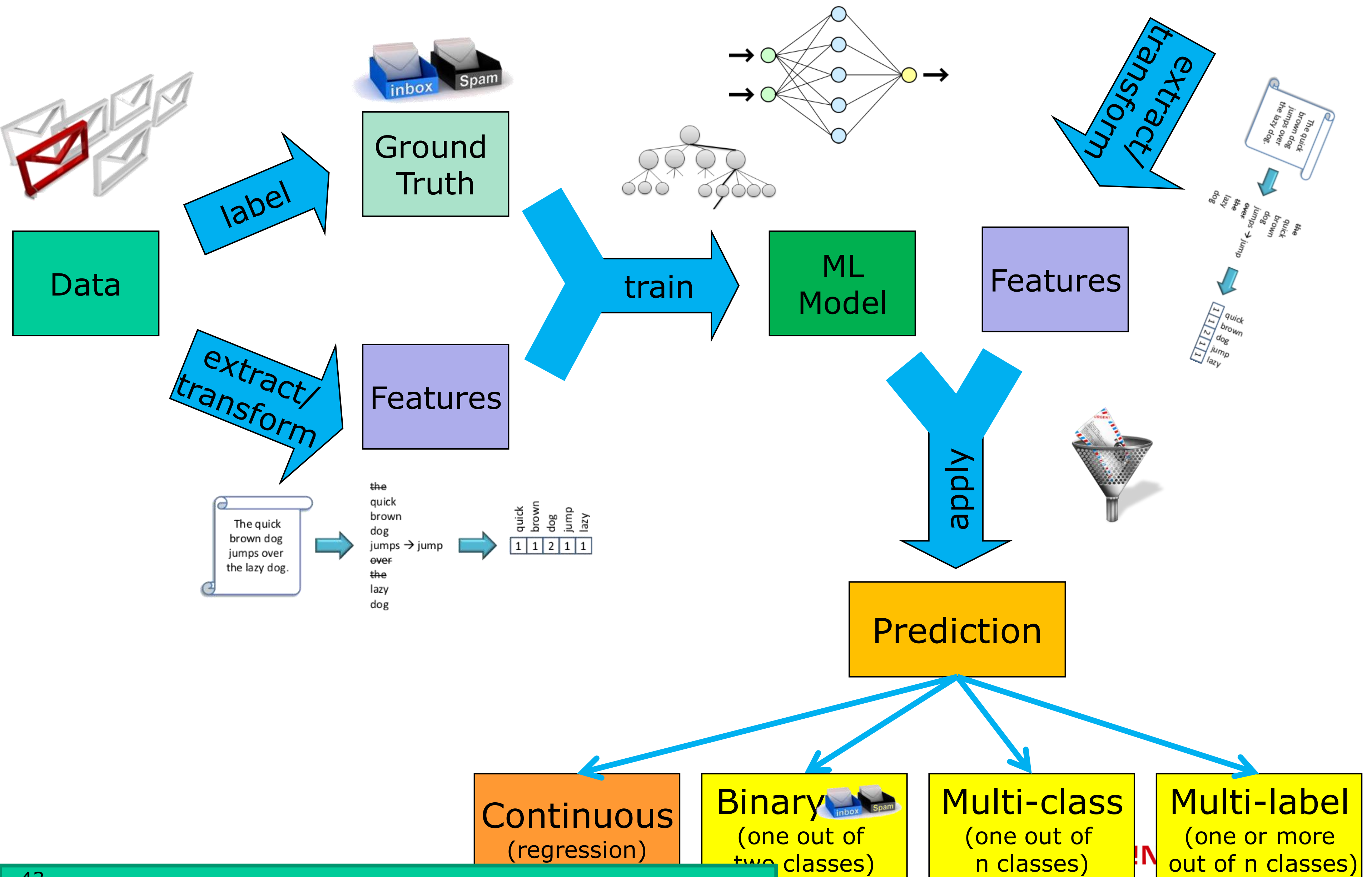
Music Feature Extraction

Image Feature Extraction



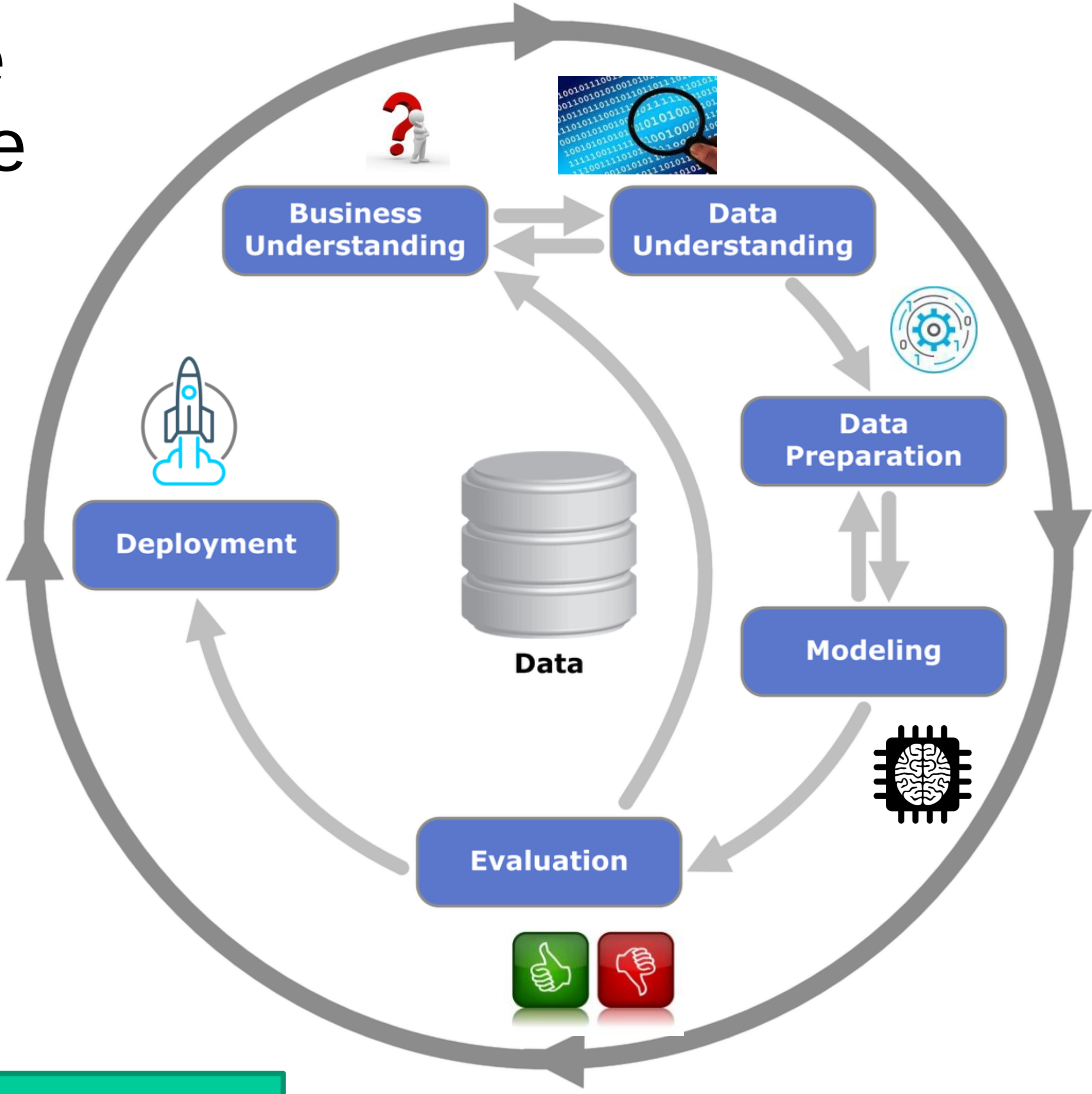


Machine Learning: steps

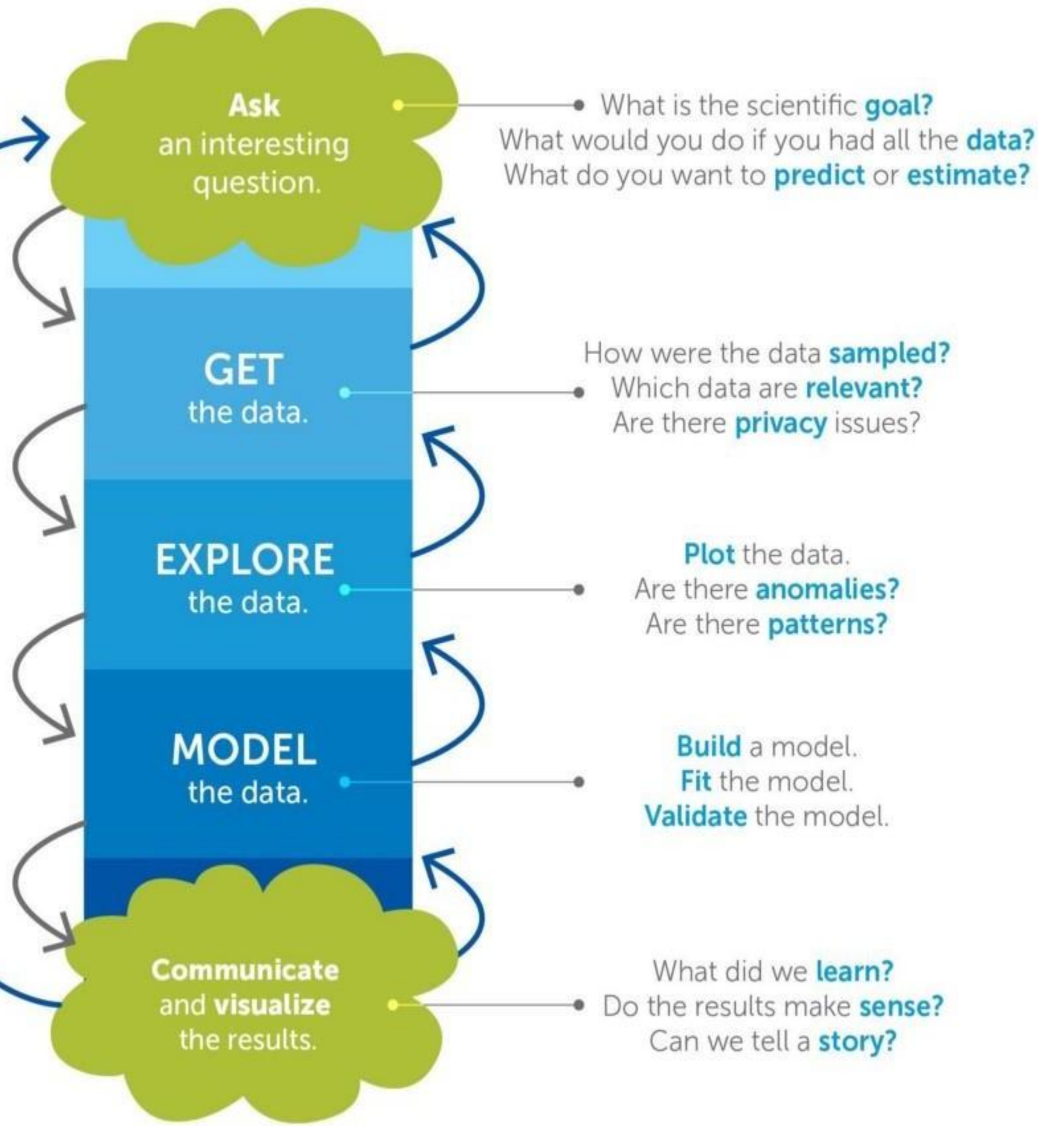


General analytical (data science) process

- E.g. CRISP Data Mining Model
- Modelling (machine learning) is only one of many important steps!



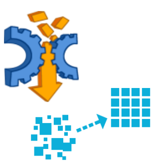
The Data Science Process



Derived from the work of Joe Blitzstein and Hanspeter Pfister, originally created for the Harvard data science course http://cs109.org/.

General analytical (data science) process

1. Identify problem / question
2. Identify & capture the available data



3. Prepare your data: clean & transform
4. Analyse your data ➔ actual machine learning

5. Create report with results, visualisation, insights
6. Embed results into business / decision making

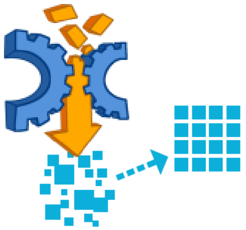
7. Plan for better data capturing in the future

General analytical (data science) process

1. Identify problem / question
   – What is the problem
   – Why does it need to be solved
   – How can it be solved **(as machine learning problem!)**

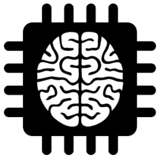
2. Identify & capture data
   – Select your data
   – Capture / extract your data

3. Clean & transform your data
   – Deal with missing values
   – Transform data: scale/normalise, attribute selection, ...



General analytical (data science) process

4. Analyse your data
   – Select fitting algorithms
   – Train and evaluate models, select best performing
   – Improve your results – parameter tuning, ...



5. Document & analyse your results
   – Problem definition, solutions, approach
   – Present & compare your results in graphs, tables, ...
   – Discoveries made during investigation
   – Methods that did / did not work
   – Limitations: when does the model not work? What questions can not be answered?

General analytical (data science) process

6. Embed results into business / decision making
   – Directly adjust your operation depending on the result
   – Use results for decision making
      • At various levels of the organisation

7. Plan for better data capturing in the future
   – Capture more data than currently available
   – Capture data in higher resolution (more detail, more frequent, ...)
   – Capture data in better quality

Scoping the lecture

Data types & feature extraction

Data preparation & transformation

Decision Trees & Random Forests

Support Vector Machines

Neural Nets & Deep Learning

Ensemble learning

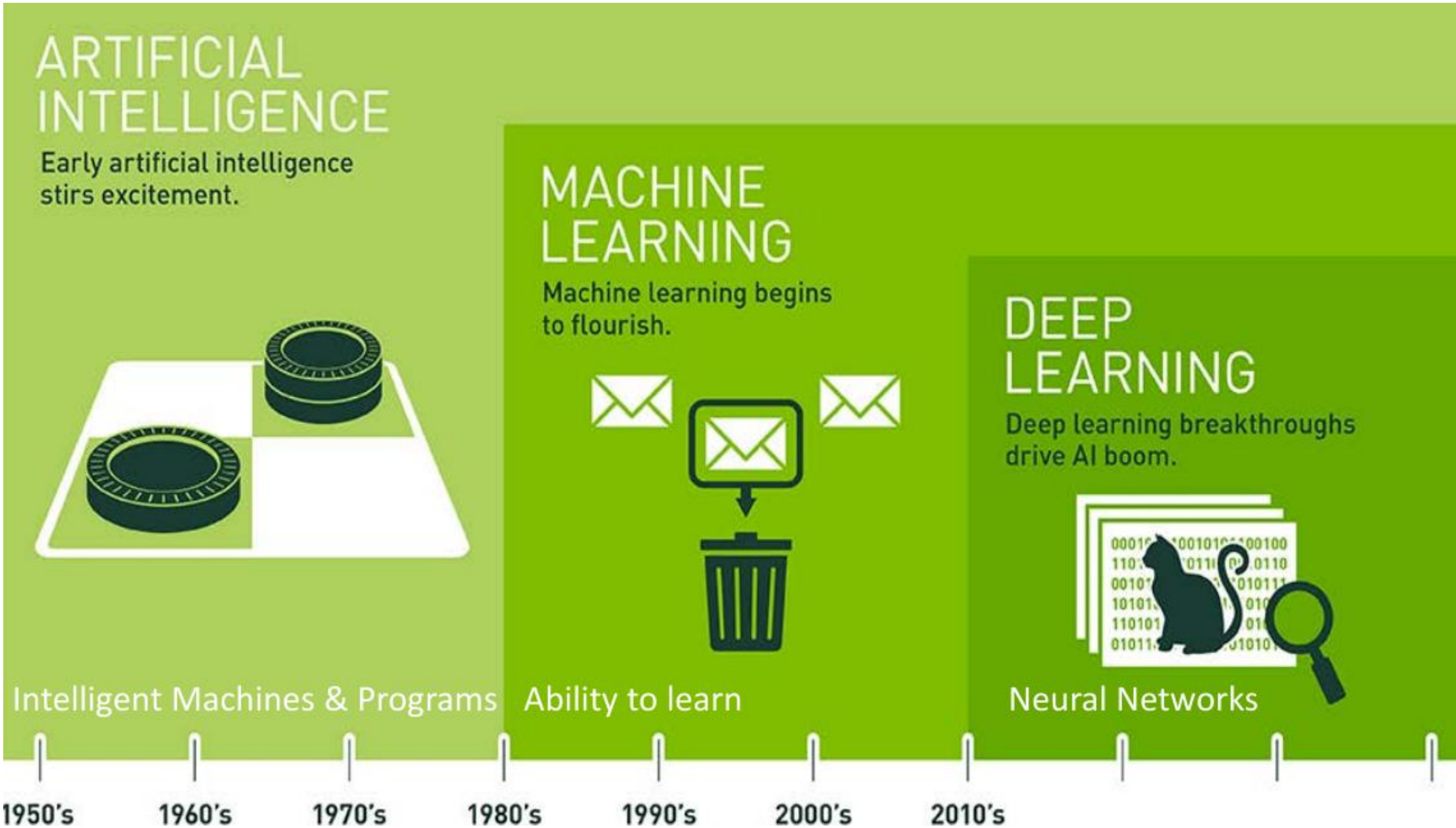
...

Evaluation

Model selection

Significance testing

AI & ML

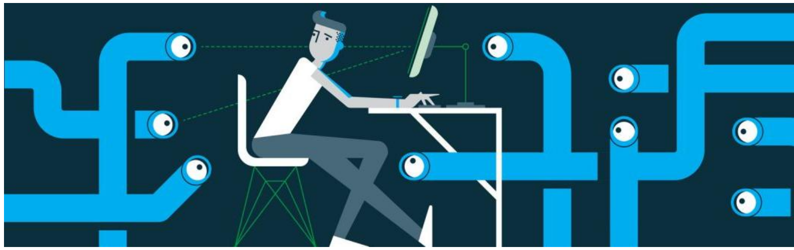

ARTIFICIAL INTELLIGENCE
Early artificial intelligence stirs excitement.
MACHINE LEARNING
Machine learning begins to flourish.
DEEP LEARNING
Deep learning breakthroughs drive AI boom.
Intelligent Machines & Programs
Ability to learn
Neural Networks
1950's
1960's
1970's
1980's
1990's
2000's
2010's

Scoping the lecture

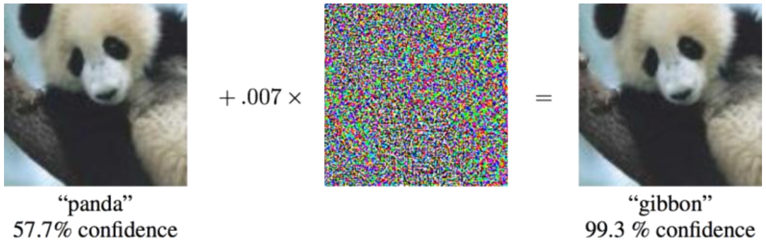
- Matching your expectations?

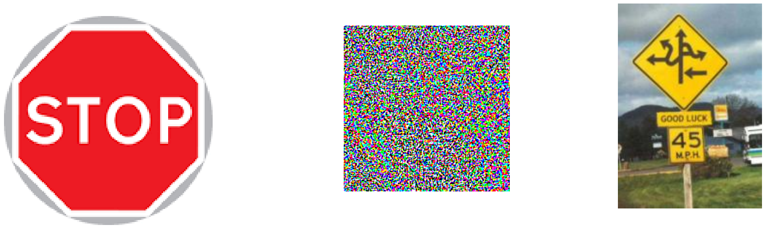
Advanced topics: Privacy

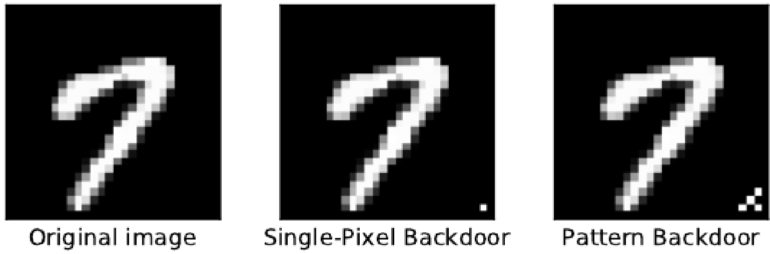
- Large amounts of personal data available
  - Collection & analysis often conflicting with data protection laws (more severe now: GDPR!)
- Especially with sensitive information
  - E.g. health data, financial data, ..
- Thus, often data needs to be anonymised before we can use it
  - E.g. generalisation of values (birthday ➔ month, year, decade)
  - Implications on the utility of the data & subsequent models...



Advanced topics: Robustness & Security





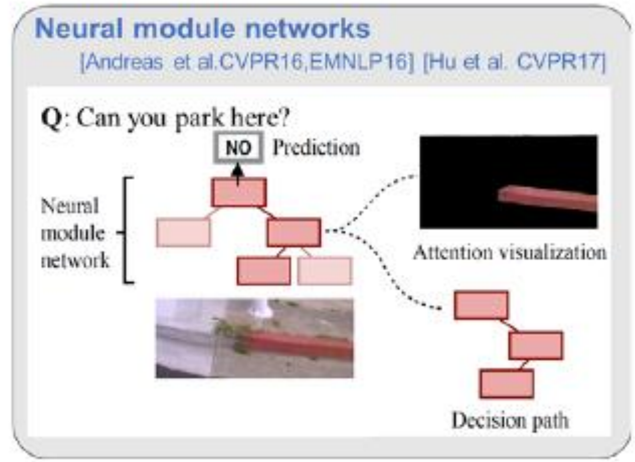


Tianyu Gu et al. BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain

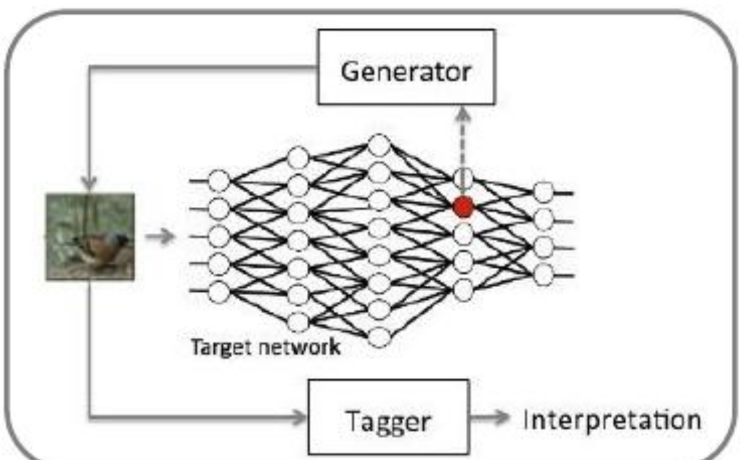
Advanced topics: XAI

Attention Mechanisms

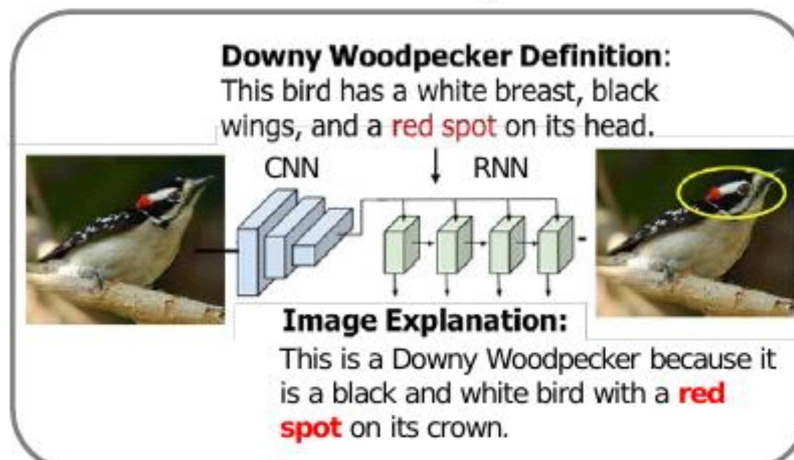
Modular Networks



Feature Identification



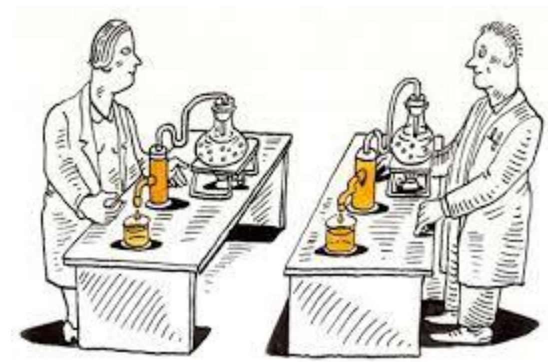
Learn to Explain



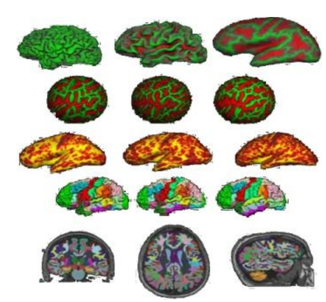
https://www.darpa.mil/attachments/XAIProgramUpdate.pdf

Other topics (out of scope): Reproducibility

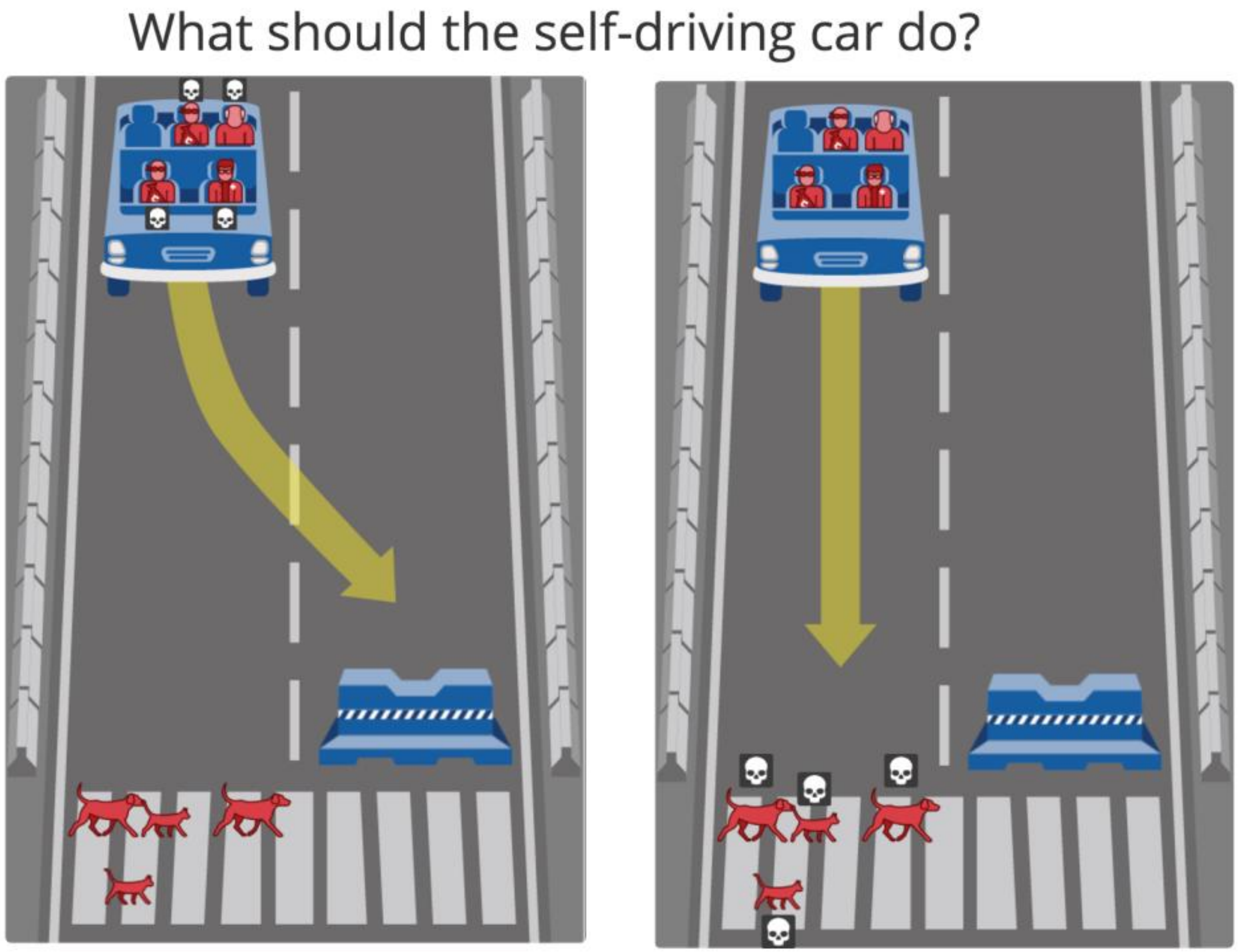
- For various reasons, we want to be able to achieve the same results as in a previous experiment (run)



- This is difficult, for various reasons
  - *Examples?*
  - Initialisation of algorithms (random number generation)
  - Order of data samples (e.g. for Perceptron)
  - Version of software used (bug fixes, improvements, etc..)
  - Version of operating system (e.g. a different C++ library..)
  - Any many more ...



Other topics (out of scope): Ethics



http://moralmachine.mit.edu/

Outline

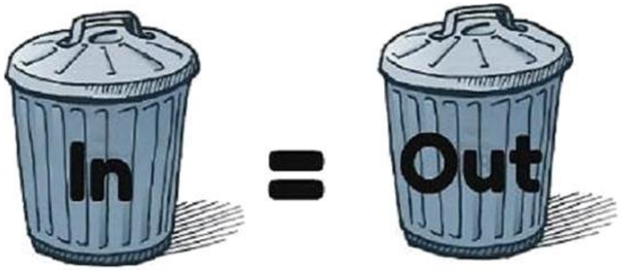
- Machine Learning: Intro
- Types of data & data preparation (very brief intro)

Data Preparation

- Vital step for machine learning (supervised and unsupervised)

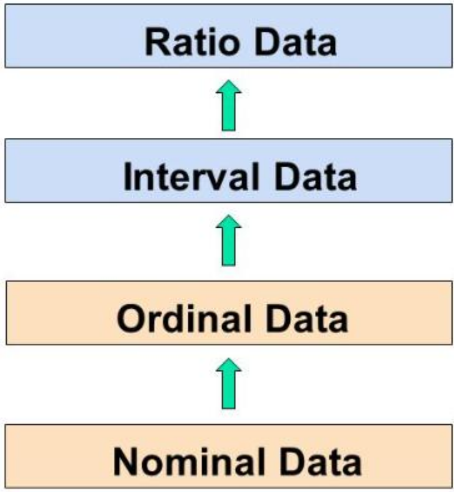
- ML algorithm will ***always*** give you a model
  – Quality of that model depends highly on the quality of the input data

- "Garbage in" ➔ "Garbage out"



- One major goal of data preparation:
  – Eliminate "wrong influence" of variables

Data Types



- Possible attribute/feature/variable types (*“levels of measurement”*)
  - Nominal, ordinal, interval and ratio

- Nominal quantities
  - Values are distinct symbols
  - Example: attribute “eye colour”: “green”,”grey”, “brown”,“blue”
    - Values themselves serve only as labels or names
    - Nominal comes from the Latin word for name
    - No relation among values (no ordering or distance measure)
    - Only (in)equality tests can be performed
    - *(You may encode it as number, but order is arbitrary; calculations on it (e.g. mean) are meaningless)*

Data Types

- Ordinal quantities
  - Impose order (rank) on values
  - (In)equality, additionally comparison (<, >) and median
  - But: no distance between values defined
  - Example:
    - attribute “size” in animals data
    - Values: “large” > “medium” > “tiny”
    - Note: addition and subtraction don’t make sense
    - Difference “large” to “medium” and “medium” to “tiny” not necessarily comparable
- *Distinction between nominal and ordinal not always clear*

Data Types

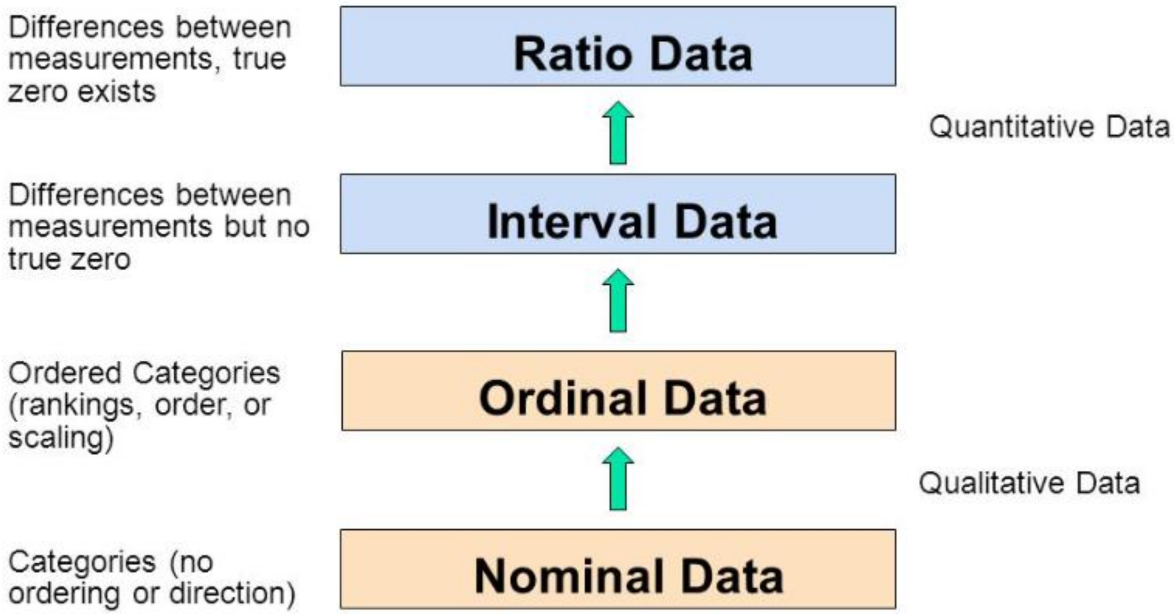
- Interval quantities
  - Interval quantities are not only ordered but measured in fixed and equal units
  - Difference between measurements meaningful
  - Example: Temperature, pH values, …
  - Difference of two values makes sense
  - Ratio not (20 is not twice as hot as 10)
  - Sum or product doesn’t make sense

Data Types

- Ratio quantities
  - The measurement scheme defines a zero point
  - Example: distance, mass, length
    - Temperature (Kelvin)

  - Distance between an object and itself is zero
  - All mathematical operations are allowed
  - Meaningful to have ratios: “twice as long”

Data Types



Can compute	Nominal	Ordinal	Interval	Ratio
Frequency distribution	Yes	Yes	Yes	Yes
Median and percentiles	No	Yes	Yes	Yes
Add or subtract	No	No	Yes	Yes
Mean, standard deviation, …	No	No	Yes	Yes
Ratios, coefficient of variation	No	No	No	Yes

Data Preparation

gender	age	height	smoker	eye colour
male	19	170	yes	green
female	44	162	yes	grey
male	49	185	yes	blue
male	12	178	no	brown
female	37	165	no	brown
female	?	157	no	?
male	44	190	no	blue
female	27	178	yes	brown
female	51	162	yes	green
female	81	168	?	grey
male	22	184	yes	brown
male	29	176	no	blue

- Example data set from earlier (lung cancer)
- Potential issues ?
  - Quantitative (continuous) data with different scales
  - Data type not fitting
    - Categorical (nominal, ordinal, ..) vs numerical (interval, ratio)
  - Missing values

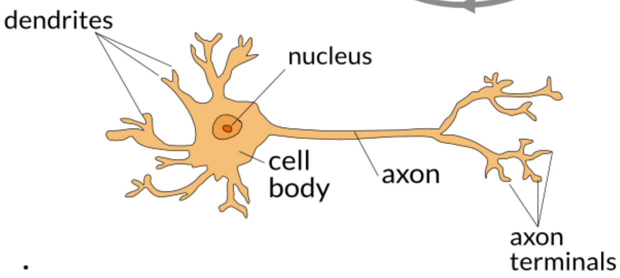
➔ More on that later!

Outline

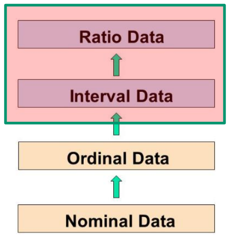
- Machine Learning: Intro
- Types of data & data preparation (very brief intro)
- Perceptron

Perceptron

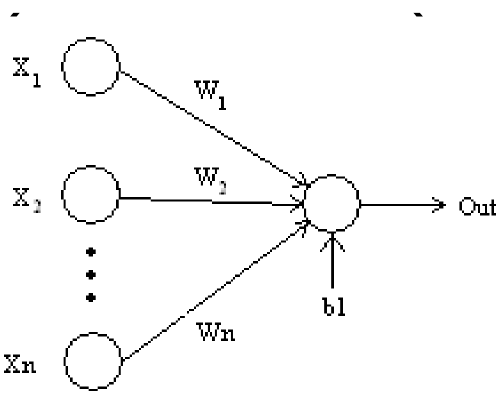
- Proposed in 1957
  - Predecessors already in late 40s
  - *Why is it relevant for you? ☺*



- Artificial (neural) network
  - only one neuron; “single-layer perceptron”



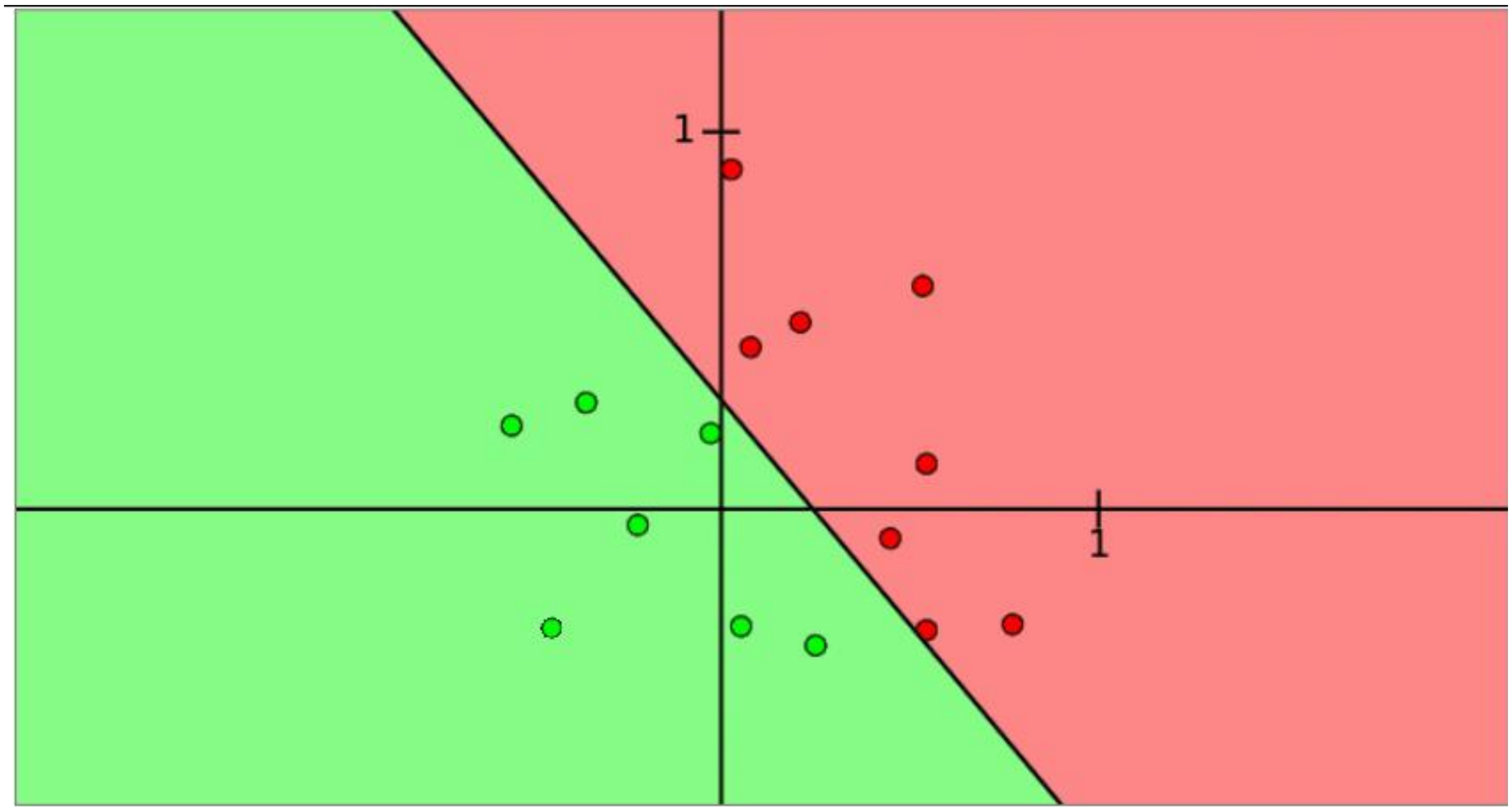
- Input: **continuous values** *X*



- Output: activation a
  - Boolean value 0 / 1

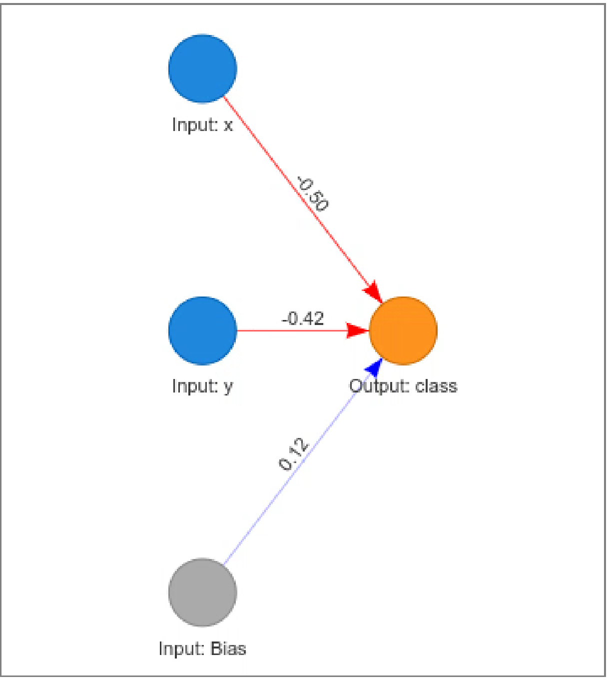
Perceptron (classification): Goal

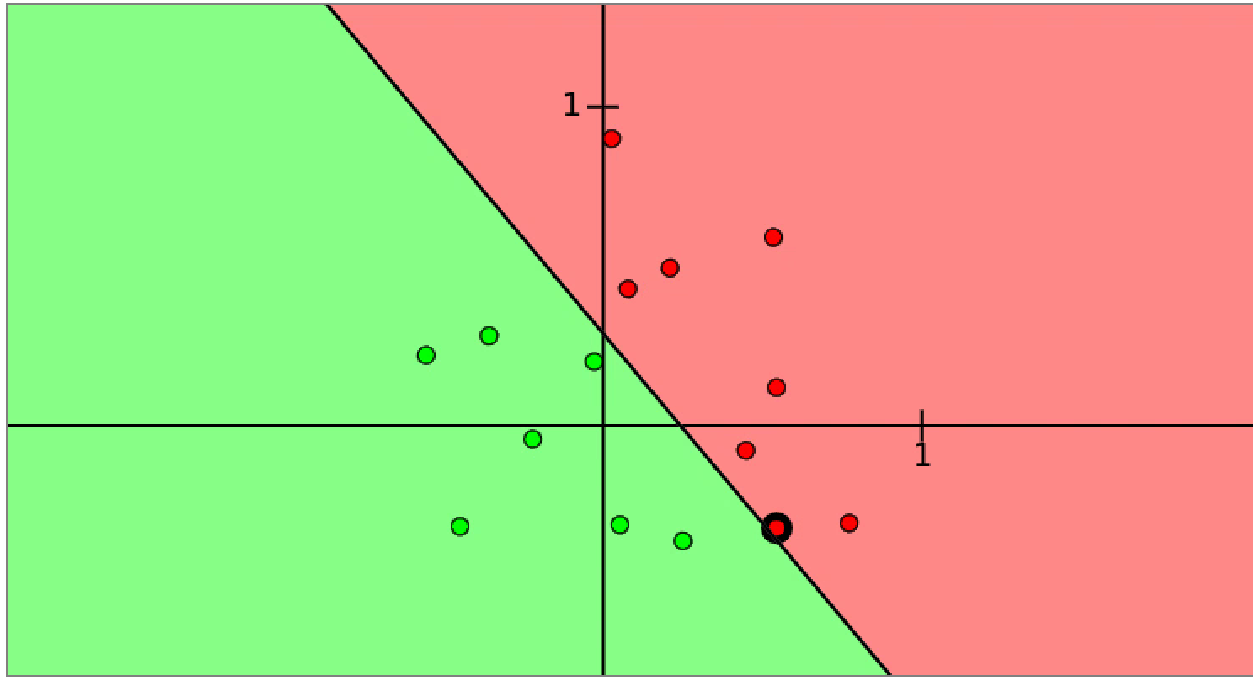
- What we want to achieve (in classification in general): "Partition" the input space into classes (categories)
  - Here: 2D Input (x, y coordinate), 2 classes (red & green)



Correct: 15/15

Perceptron: Demo

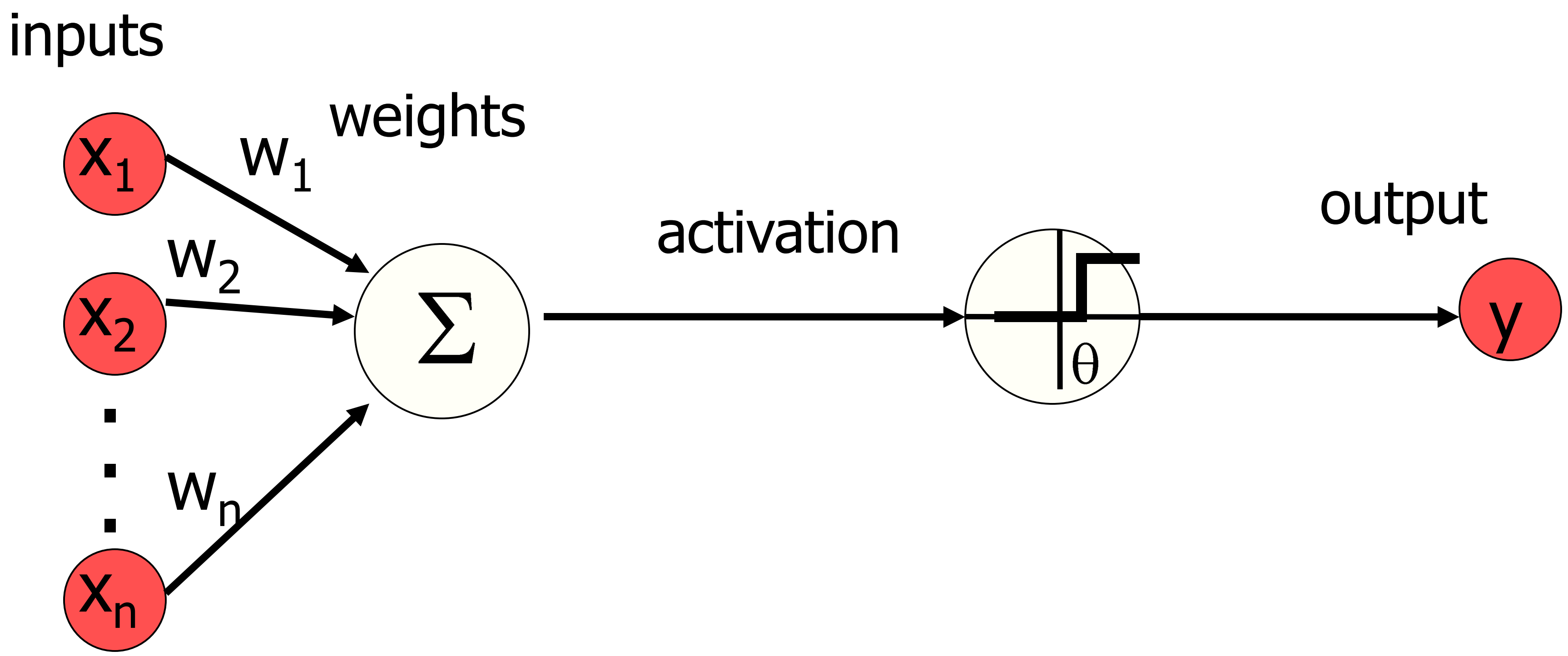




Stop Reset Train All Train Single

Correct: 15/15 — Iteration: 53

Perceptron


inputs
weights
x_1
w_1
x_2
w_2
x_n
w_n
Σ
activation
θ
output
y

Perceptron

- Linear combination of inputs
  - Using weights *W* $a = \sum_{i=1}^{n} w_i x_i$

- Pass through threshold activation function with threshold θ

$$y = f(x) = \begin{cases} 1 \text{ if } a \geq \theta \\ 0 \text{ if } a < \theta \end{cases}$$

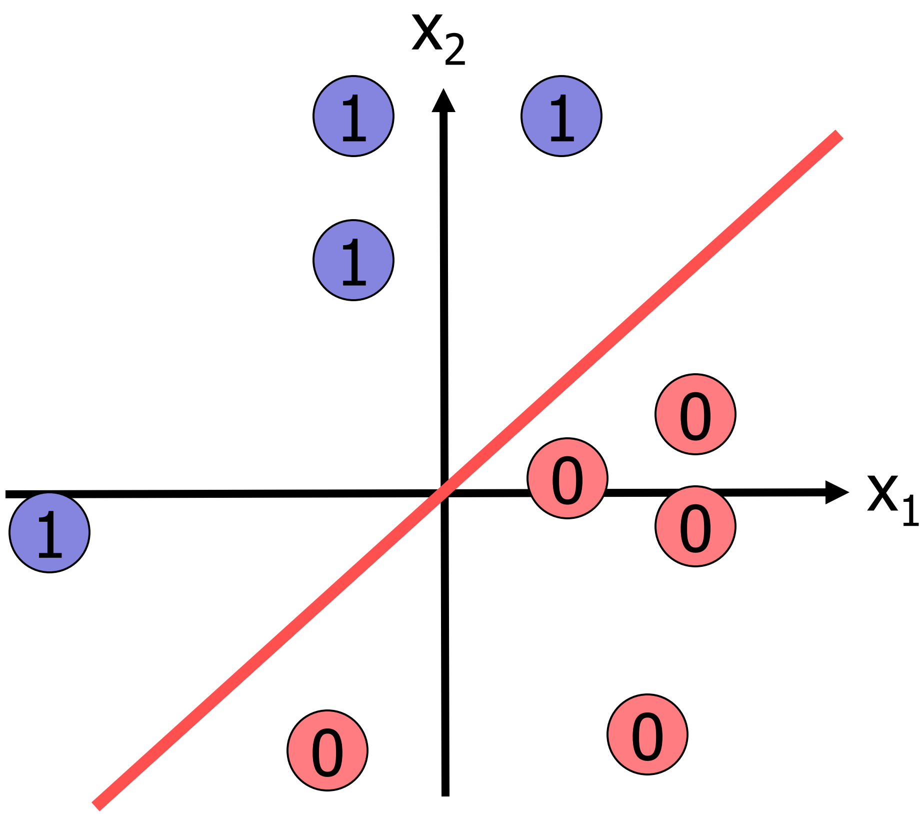
(Heaviside step function)

- Often: $\theta = 0$

Perceptron: simple example

- Two-dimensional data set
  - Variables x_1 & x_2
    - E.g. position on a map
- Weight vector also has two components
  - w_1 & w_2
- Data set can be easily visualised in Cartesian coordinate system
- Two classes: ***0*** and ***1*** (sometimes also -1 & 1)
  - Visualised as red & green

Perceptron visualised



Decision line

$w_1\, x_1 + w_2\, x_2 = \theta$

Perceptron: learning algorithm

- Training the model: learning the weights from labelled samples (label: **y**)

  - Initialise weights

  - Repeat
    - Present training sample **x**
    - Predict sample label: **y'** = f(x)
    - Prediction correct? Compare **y** and **y'**
      - if **y' ≠ y** ➔ Compute new weights **w'** as **w'**=**w** + α (y-y') **x**

  - Until prediction correct (y'=y) for all samples

Perceptron: learning algorithm

- Parameter α: *learning rate*
  - determines the magnitude of weight updates

- If output is correct (y=y')
  - weights **not** changed

- If output is incorrect (y ≠ y')
  - weights changed such that the output of the for the new weights **w'** is ***closer*** to the input x_i

Questions?

Upcoming topics:

- Decision trees
- Random Forests

....