# Al for Cyber-Physical Systems Part 1 – Introduction

Prof. Congduc Pham http://www.univ-pau.fr/~cpham









("WAZİUD")

IoT – from idea to reality

("WAZİDUD")

Horizon 2020 European Union funding for Research & Innovation



Paving for the next 10 years of innovation in IoT and Al







Advanced and disruptive IoT/AI technologies targeting the smallholder community for increased resilience



## Acknowledgements

- All is probably one of the hot topics with the most incredible amount of also incredible quality contributions & tutorials videos!
- Setting up this course would not have been possible without all these contributors!
- I've crawled the web for hours (days), trying to take knowledge from multiple sources and trying to present all these impressive resources in a simple and comprehensive way for my students
- I tried to mention the sources of materials I've borrowed from the web as much as I could
- A special "thank you" for all the incredible tutorial videos from Machine Learnia (<a href="https://machinelearnia.com/">https://machinelearnia.com/</a>, Guillaume Saint-Cirgue) and his YouTube channel (<a href="https://www.youtube.com/@MachineLearnia/videos">https://www.youtube.com/@MachineLearnia/videos</a>)
- A special "thank you" akso for the complete and very clear videos from freeCodeCamp.org, especially on DL (https://www.youtube.com/watch?v=dPWYUELwIdM)
- There are also all the articles from <a href="https://towardsdatascience.com/">https://towardsdatascience.com/</a>





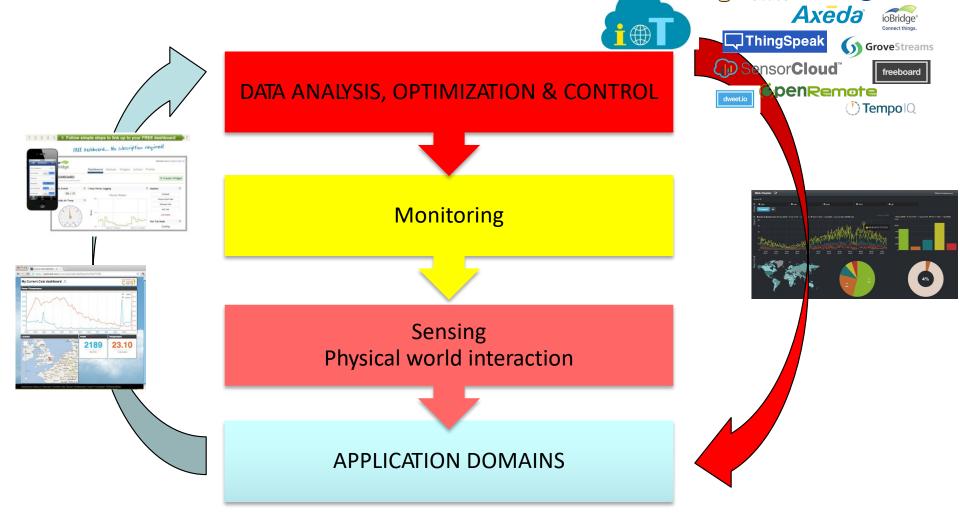
## IoT added-values come from interactions & linked data!







## IoT to monitor, optimize & control...



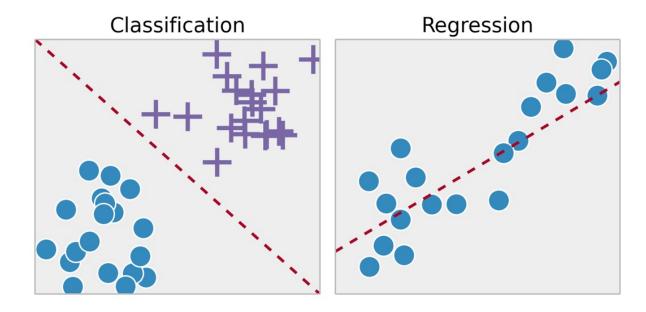
Firebase

**S**FIWARE



## ...but also how to analyse the data

- What is the meaning of the collected data?
  - Classification, ...
- Can we predict how the data will evolve?
  - Prediction using Regression methods





## Cyber-Physical Systems

- Norbert Wiener, early definition:
  "science of control and communication in machines and humans"
- From wikipedia:

"A cyber-physical system (CPS) or intelligent system is a computer system in which a mechanism is controlled or monitored by computer-based algorithms. In cyber-physical systems, physical and software components are deeply intertwined, able to operate on different spatial and temporal scales, exhibit multiple and distinct behavioral modalities, and interact with each other in ways that change with context"

• From NSF:

"Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other"



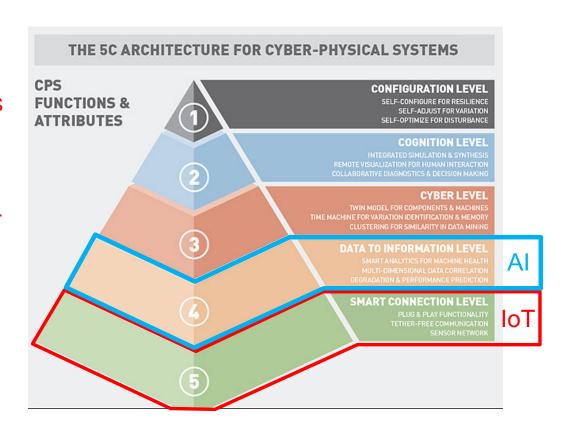
#### CPS & IoT

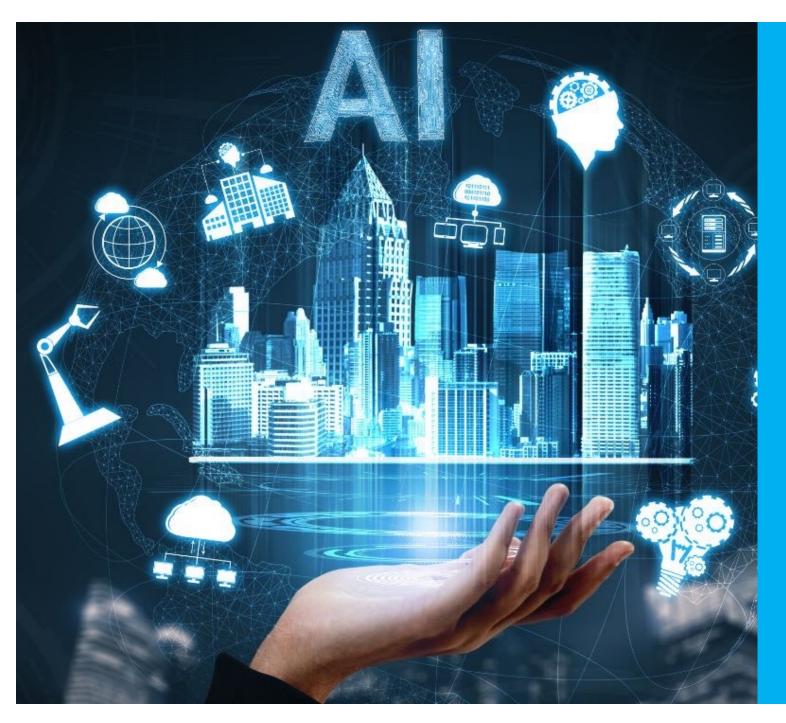
- The concepts of Internet of Things (IoT) and Cyber Physical Systems (CPS) are closely related to each other. IoT is often used to refer to small interconnected devices like those in smart home while CPS often refers to large interconnected devices like industry machines and smart cars"
- "Cyber Physical Systems represent a complex combination between physical and computational elements, and can be found in a multitude of areas such as manufacturing, aerospace, automotive, transportation, etc"
- "Sensors, computational and physical world are closely integrated in CPS. CPS includes both conventional embedded systems and control systems that are presumed to be remodelled by emerging methodologies and integration of the Internet of Things. IoT is the base or enabling technology for cyber-physical systems."
- "The intelligent Internet of Things (IoT) and cyber—physical systems (CPS) are evolving quickly as interdisciplinary technologies that combine physical components and computational devices to enable artificial intelligence (AI)based solutions"



## Some advanced CPS-related concepts

- Intelligent robot systems
- Augmented Reality, Virtual & Mixed Reality
- Real-time multi-agent systems
- Cooperative distributed simulations
- Coupling of Real-time and Cosimulation
- Digital Twins to create highfidelity virtual models of physical objects in order to simulate their behaviors in the real world and provide feedback





# INTRO

TO

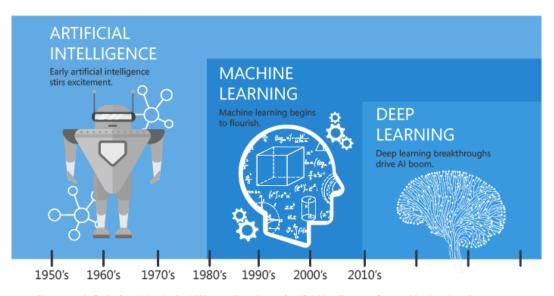
A



## The raise of Artificial Intelligence

- It is the science and engineering of making intelligent machines.
- In Computer Science, Artificial Intelligence (AI) research is defined as the study of « intelligent agents »
- From General AI to Narrow AI: from overhyping to fewer promises, but more realistic!



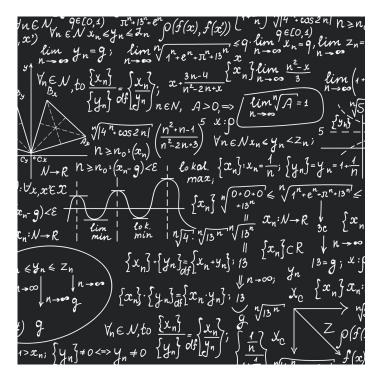


Since an early flush of optimism in the 1950's, smaller subsets of artificial intelligence - first machine learning, then deep learning, a subset of machine learning - have created ever larger disruptions.



## AI: (now) a serious science!

- General-purpose Al like the robots of science fiction is incredibly hard
  - Human brain appears to have lots of special and general functions, integrated in some amazing way that we really do not understand (yet)
- Special-purpose AI is more doable (nontrivial)
  - E.g., chess/poker playing programs, logistics planning, automated translation, speech and image recognition, web search, data mining, medical diagnosis, keeping a car on the road.





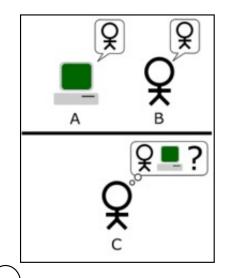
## The Turing Test

- Proposed By Alan Turing in 1950
- To be called intelligent, a machine must produce responses that are indistinguishable from those of a human.
- Human judge communicates with a human and a machine over text-only channel.
- Both human and machine try to act like a human. Judge tries to tell which is which.
- Is Turing Test the right goal?

"Aeronautical engineering texts do not define the goal of their field as making 'machines that fly so exactly like pigeons that they can fool even other pigeons."

[Russell and Norvig]









## Reflection

rational than
humans in some
cases, why not?



Systems that think	Systems that think
like humans	rationally
Systems that act	Systems that act
like humans	<u>rationally</u>

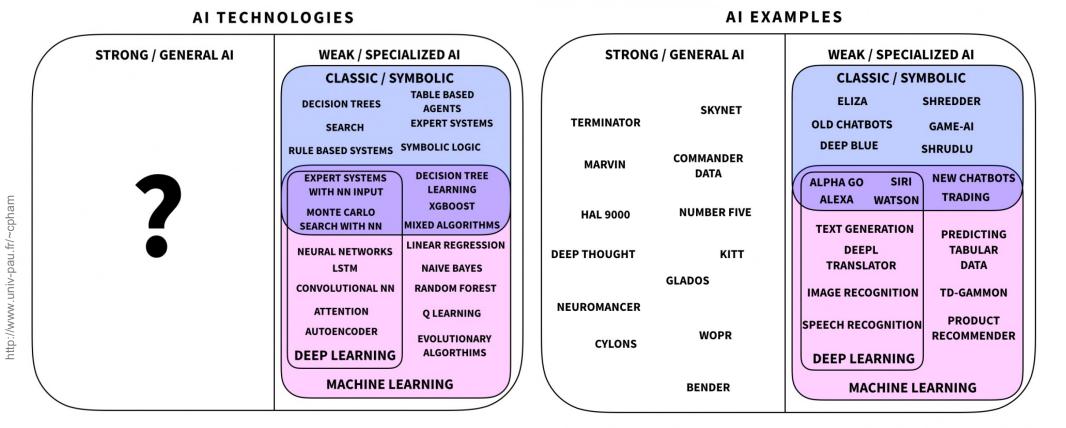
AI focus on action.

Avoids philosophical issues such as "is the system conscious" etc.



Congduc Pham

## Al Technologies

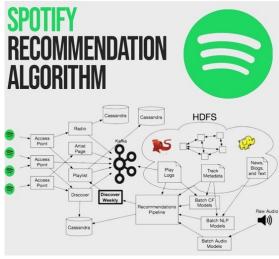


https://divis.io/en/2019/03/ai-for-laymen-part-2-symbolic-ai-neural-networks-and-deep-learning/



## Al in our daily life









Virtual Assistants





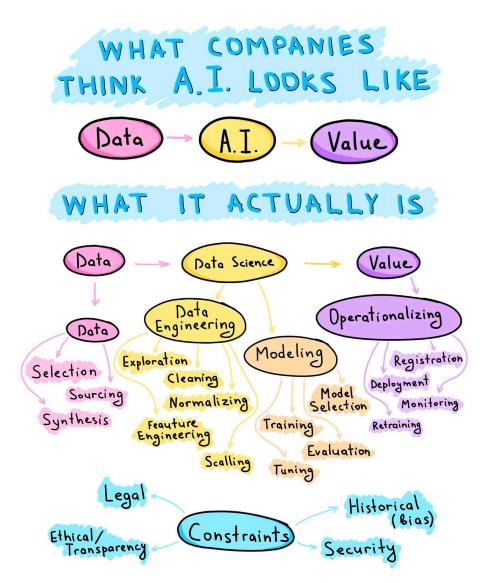






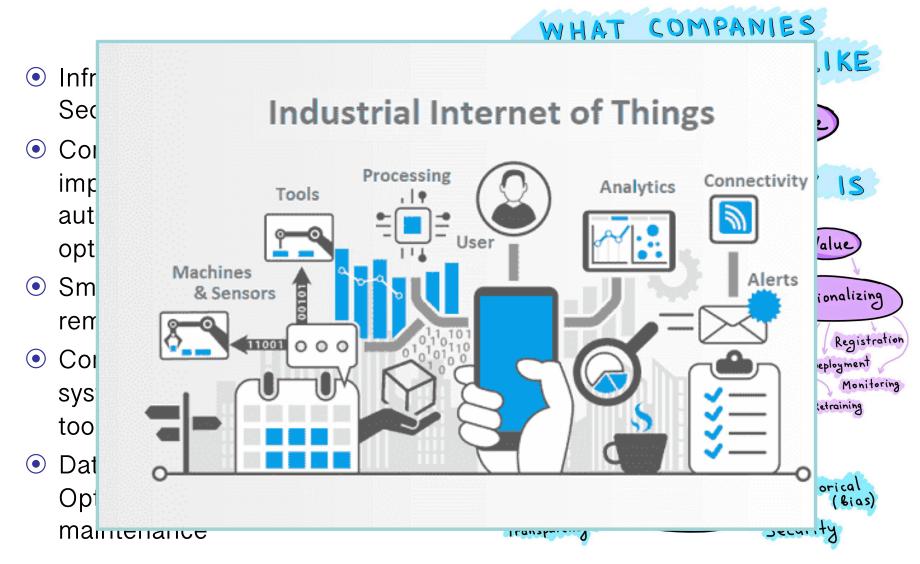
#### Al in industries

- Infrastructure monitoring, Security & Safety
- Continuous process improvement, Process automation, Process optimization
- Smart logistics management, remote management, tracking,
- Connectivity to back-end system, integration of smart tools, Interoperability
- Data analysis, Supply Chain Optimization, Predictive maintenance





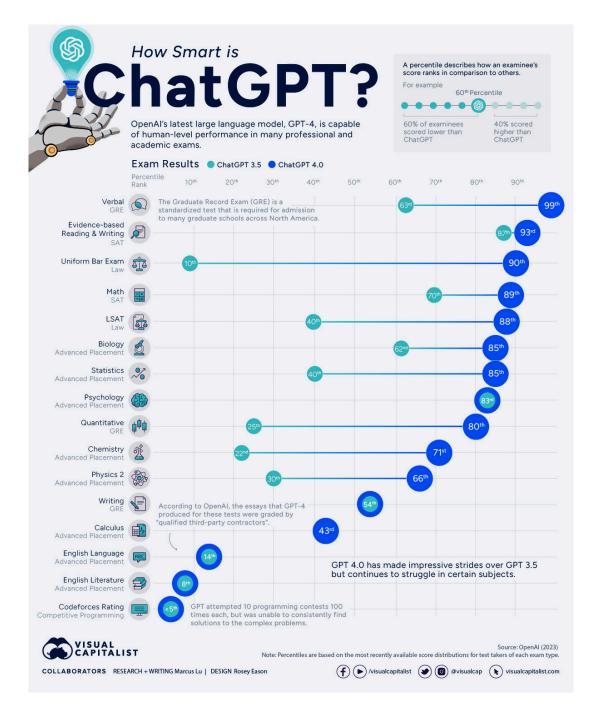
### Al in industries





## And ChatGPT?

- Chat Generative Pretrained Transformer, is a chatbot that simulates human conversation through text responses
- ChatGPT can generate text, making it useful for content creation tasks such as writing articles, stories, and even poetry
- It is a great tool to quickly get reviews or articles on specific domains!





## Let's try to be clear

- The majority of AI remains weak or narrow AI and is only able to complete a single task
- Most AI projects use Machine Learning techniques
- Machine Learning focuses on teaching computers how to learn without being programmed to do specific tasks — Deep Learning is a subset of Machine Learning!
- Deep Learning is differentiated from other types of machine learning based on how the algorithm learns and how much data the algorithm uses. Deep Learning requires large data sets, but it needs minimal manual human intervention
- Deep Learning is intended to mimic the structure of a human brain, with complex, multi-layered neural networks

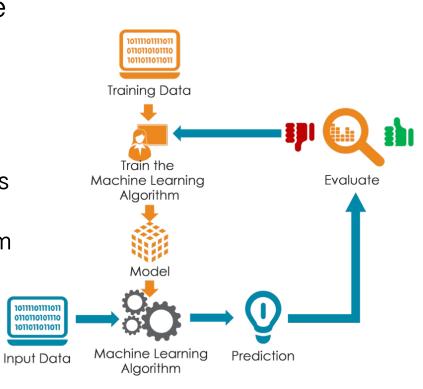


## Machine Learning

- Develops Narrow Artificial Intelligence systems through examples
  - A developer creates a model and then "trains" it by providing it with many examples
  - The machine learning algorithm processes the examples and creates a mathematical representation of the data that can perform prediction and classification tasks

#### Example

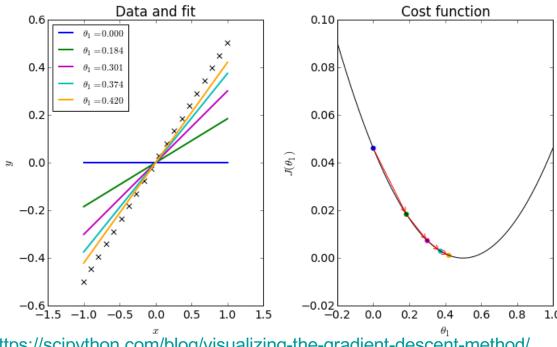
 A machine-learning algorithm trained on thousands of emails with their category (legitimate or spam) will be able to predict if a new mail is spam or not





## Optimization in Al

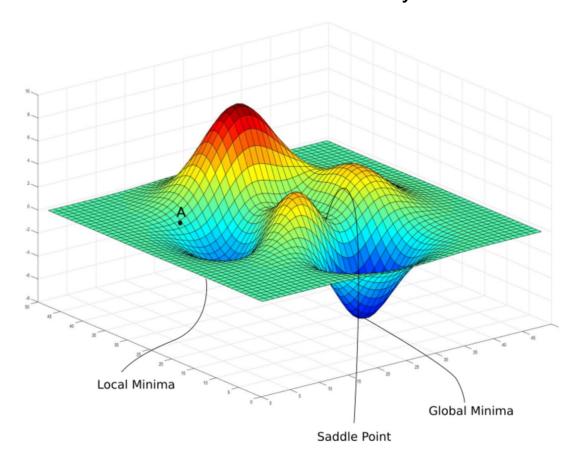
- Most AI problems consist of approximating a function that maps examples of inputs to examples of outputs
- Modern AI can be summarized as optimizing a performance criterion using example data or past experience





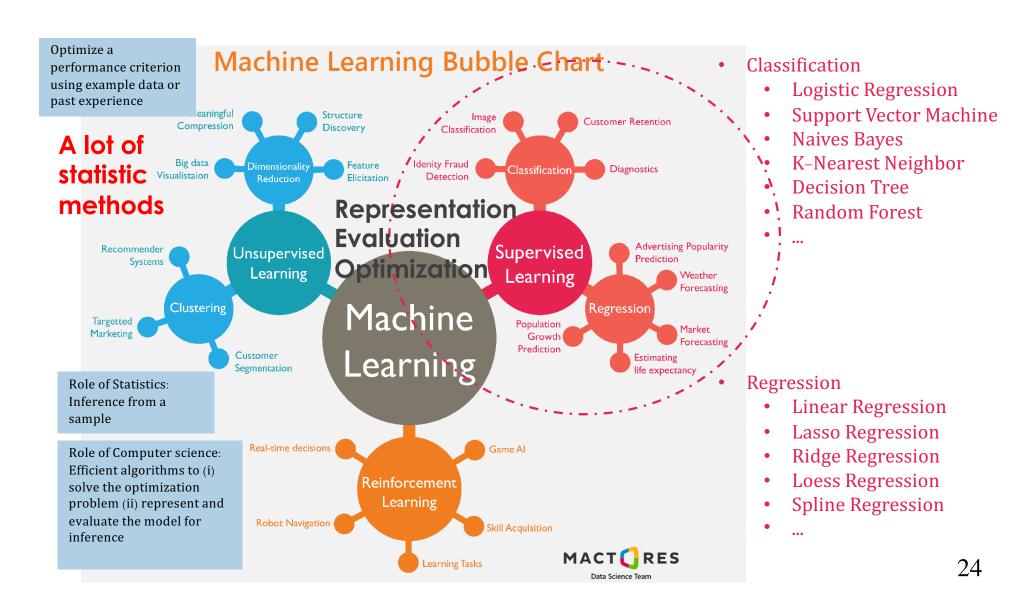
## Optimization can become complex!

• What if the inputs are very complex? Trying to find the best fittled function can become incredibly hard!





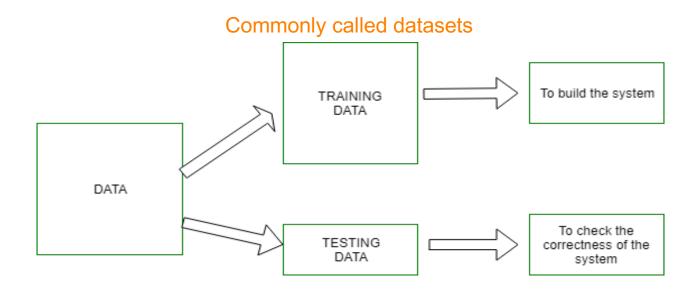
## Machine Learning Techniques





## Supervised Learning

- ML model is presented with input data which is labeled
  - Each input data is tagged with the correct label
- The goal is to approximate math operations in the ML model so well that when presented with new input data, the ML model can predict the output variables for that new input data





## Supervised learning- an alternative view

CAT!

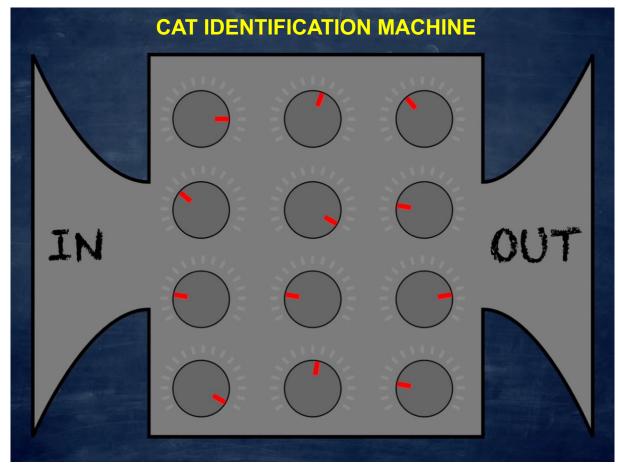
Pr. Congduc Pham http://www.univ-pau.fr/~cpham



90







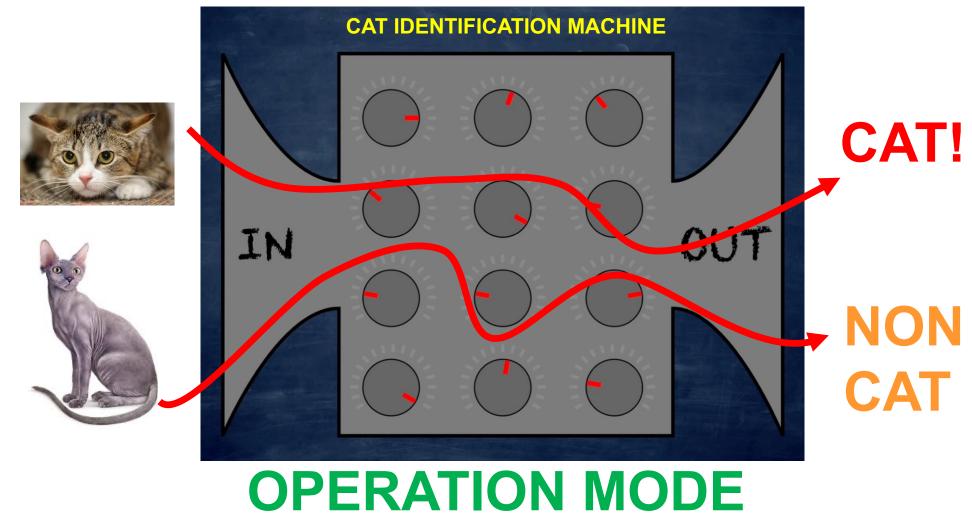
CAT

NON CAT

TRAINING MODE



## Supervised learning- an alternative view

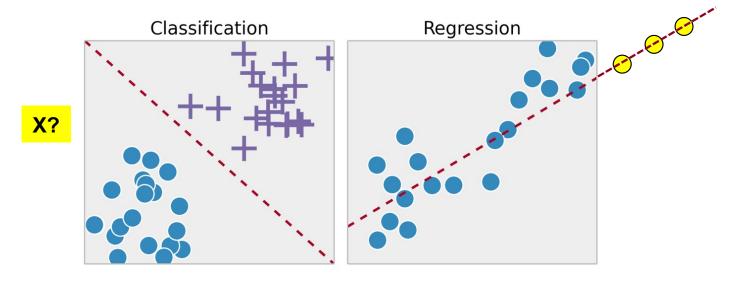


Pr. Congduc Pham http://www.univ-pau.fr/~cpham



## Classification vs Regression

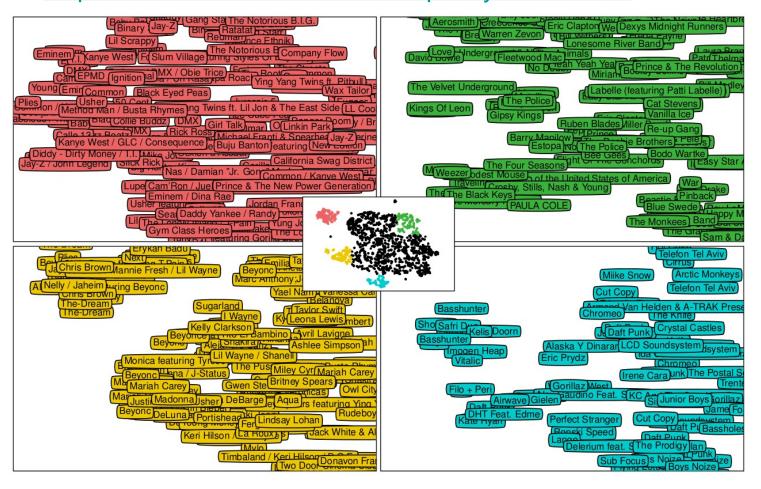
- Classification: A classification problem is when the output is a category, such as "red" or "blue" or "disease" and "no disease".
- Regression: A regression problem is when the output is a real number, such as "dollars" or "weight".





## Classification in real-world problem

https://sander.ai/2014/08/05/spotify-cnns.html



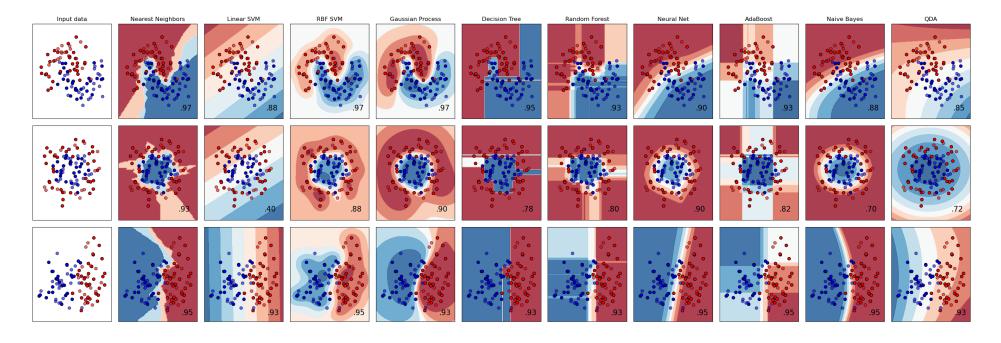


#### Classification methods?

 This is where the choice of a classification method is important: linear/nonlinear, categorical/continous, supervised/non-supervised,...

#### Classification

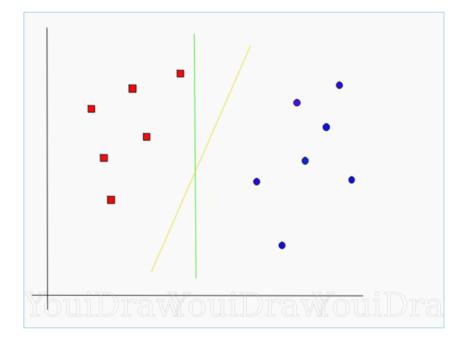
- Logistic Regression
- Support Vector Machine
- Naives Bayes
- K-Nearest Neighbor
- Decision Tree
- Random Forest
- ..

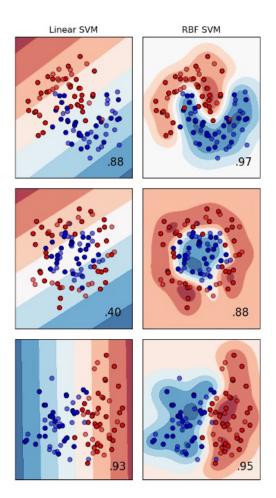




## Ex: Support Vector Machine

- SVM is an algorithm that takes the data as an input and outputs a line that separates those classes if possible
- But which line is better?

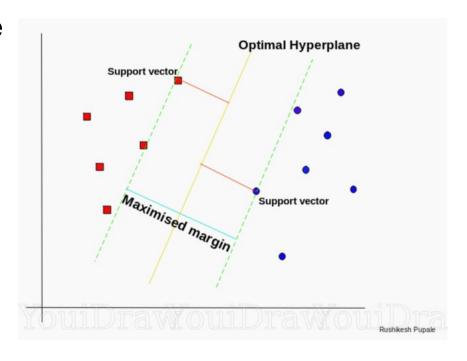






## SVM principle

- According to the SVM algorithm we find the points closest to the line from both the classes
- These points are called support vectors
- Now, we compute the distance between the line and the support vectors
- This distance is called the margin
- SVM tries to maximize the margin
- The hyperplane for which the margin is maximum is the optimal hyperplane.

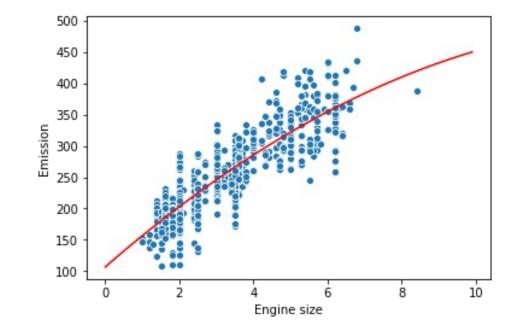


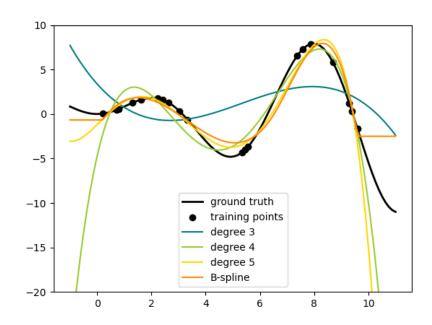


## Regression in real-world problem?

• Here again, the choice of the regression method has obviously high impact: linear/nonlinear, simple/multiple, error model, ...



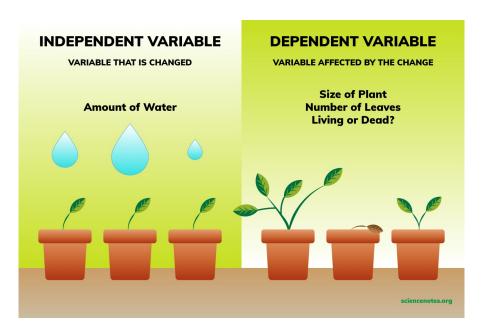






## More about regression

- **Dependent variables:** the main event or factor to understand or predict. Also known as *explanatory variable*.
- Independent variables: the events or factors suspected to have an impact on the dependent variable. Also known as *response* variable.





## Types of Regression

 Simple regression: single independent variable x for a single dependent variable Y.

*x*: number of cricket chirps

Y: temperature

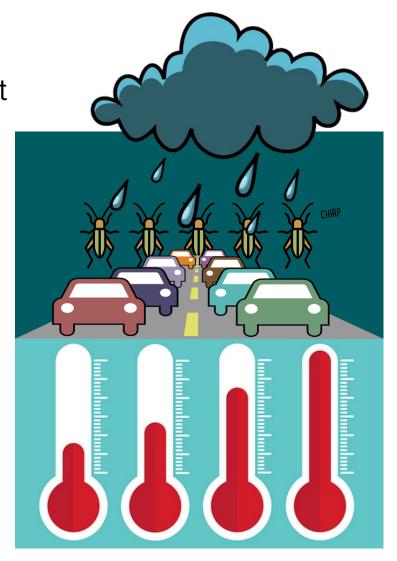
• Multivariable regression: multiple independent variables,  $x_1$ ,  $x_2$ ,  $x_3$ , for a dependent variable  $\mathbf{Y}$ .

 $x_1$ : number of cricket chirps

 $x_2$ : rainfall

 $x_3$ : automobile traffic

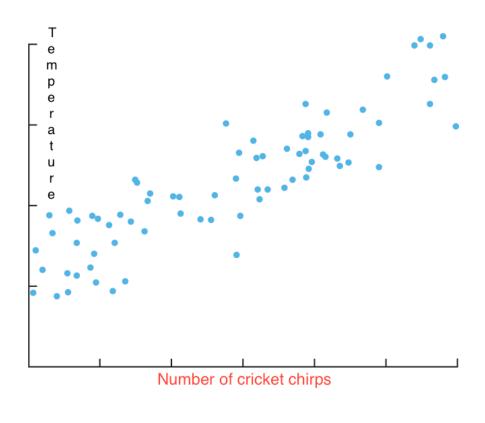
Y: temperature





#### Scatter Plot of datasets

- Data gathering on the variables in question
- The vertical scale represents one set of measurements and the horizontal scale the other



- Agriculture
  - Soil moisture for optimized irrigation
- Environment
  - Pollutant concentration for public safety and alarming system
- Electricity
  - Power demands for optimized production

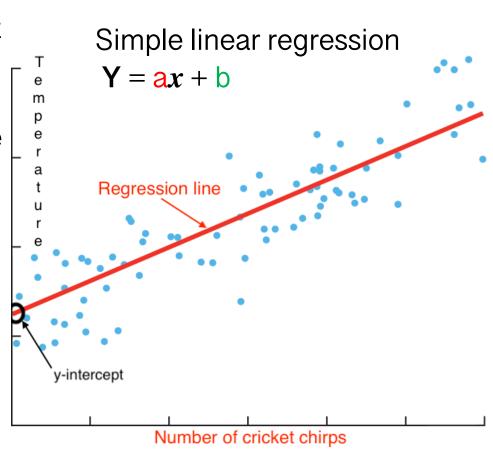
36



## Linear Regression

- A linear relationship to predict the (average) numerical value of Y for a given value of x using a straight line, called the regression line.
- Knowing the slope and the yintercept the objective is to predict the average Y from x.
- Real world problem can be multivariate
- Multiple linear regression

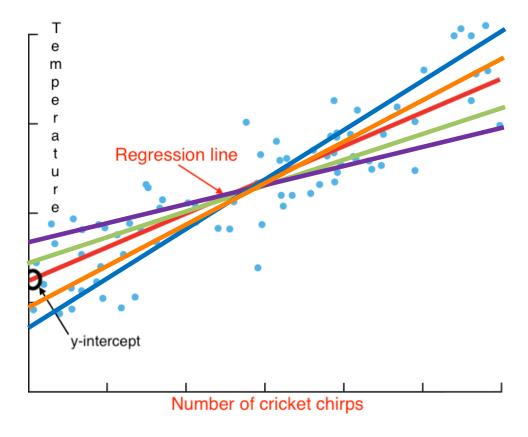
$$Y = a_1x_1 + a_2x_2 + a_3x_3 + ... + a_ix_i + b$$





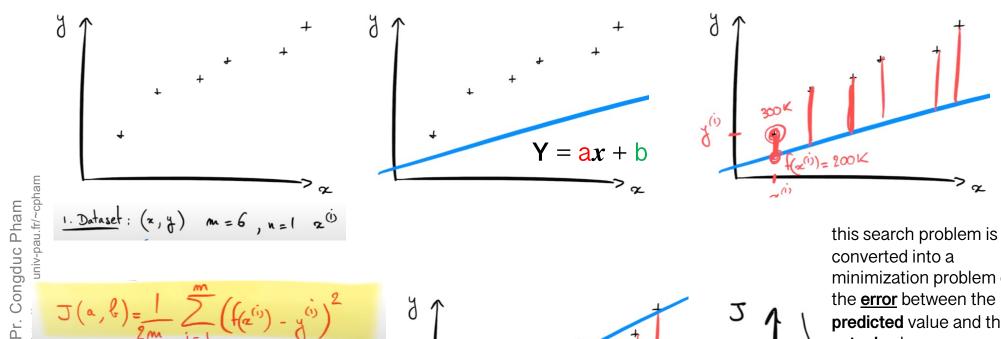
## Then what?

- What is the best regression line?
- How can we find it?



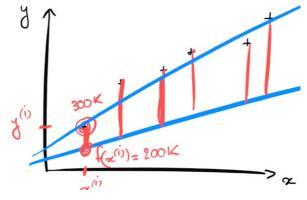


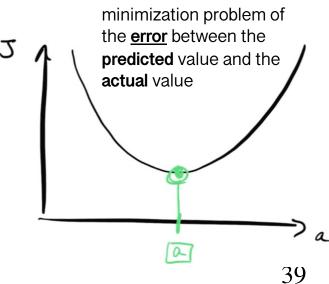
## The need for a cost function



A <u>cost function</u> will help to figure out the best possible values for a and b which would provide the best *regression line* for data points

Here, Mean Squared Error (MSE)



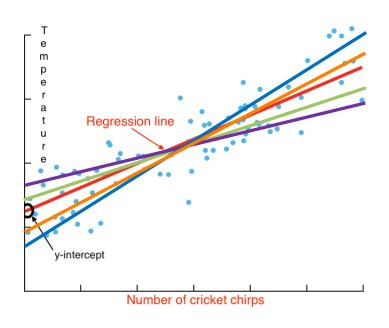


Pictures from <a href="https://www.youtube.com/watch?v=wg7-roETbbM">https://www.youtube.com/watch?v=wg7-roETbbM</a> (Machine Learnia)



# Why do we call it Machine Learning?

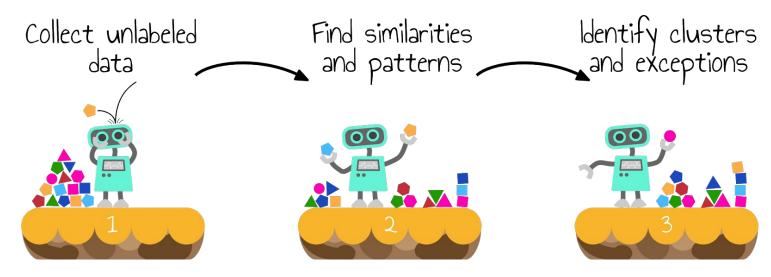
- The number of data points can be very large!
- The number of possible regression lines can be very large!
- Trying in a brute force approach can take years, even with state-of-the-art supercomputers!
- Exact methods also need very complex
   & long operations to be conducted!
- It is called AI/ML because we "tell" the machine to efficiently find the best solution
- "tell"=implement "intelligent" algorithms!





# Unsupervised Learning - clustering

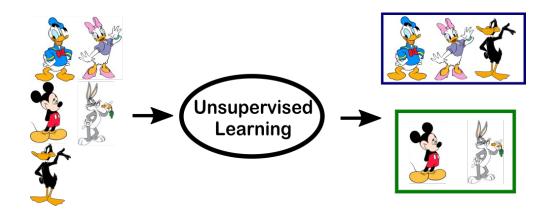
- Mainly used for clustering to learn patterns from untagged data
- Find natural groups in the feature space of input data
- No single best method for all datasets
- Models are computationally complex because they need a large training set to produce intended outcomes
- Still require some human intervention for validating output





## Ducks example

- In the below example, some cartoon characters are passed to the ML model where some of them are ducks
- No data label provided
- ML model is able to separate the characters into Duck and No Duck by looking at the type of data and models in the underlying data structure



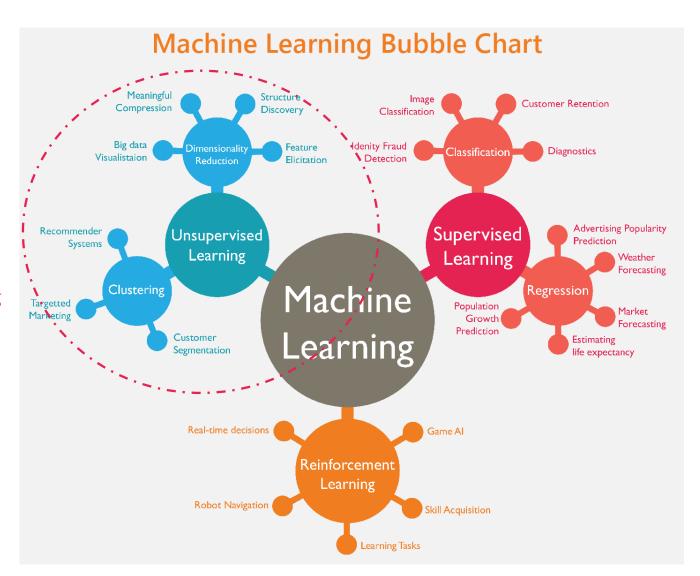


# Clustering algorithms



- Affinity Propagation
- Agglomerative Clustering
- BIRCH
- DBSCAN
- K-Means
- Mini-Batch K-Means
- Mean Shift
- OPTICS
- Spectral Clustering
- Mixture of Gaussians

•

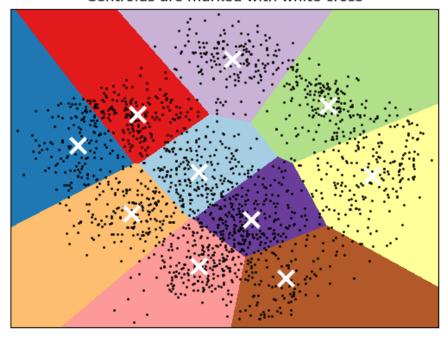


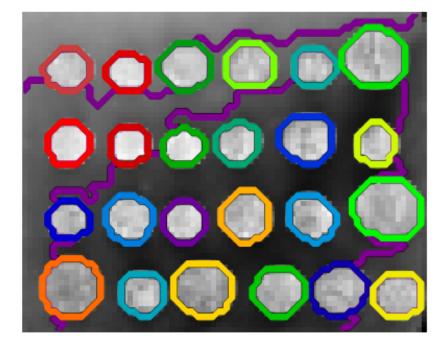


# Example of advanced clustering

 There is no best clustering algorithm, and no easy way to find the best algorithm for your data without using controlled experiments

K-means clustering on the digits dataset (PCA-reduced data)
Centroids are marked with white cross



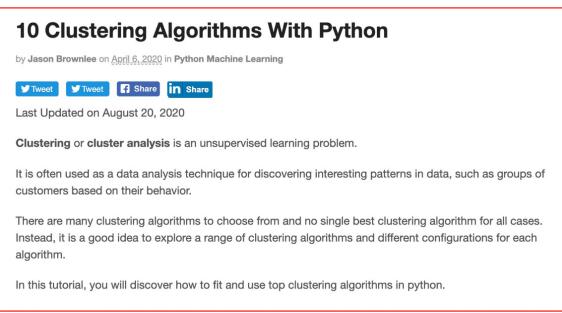




# Trying some clustering algorithms

#### Assignment to do in lab

- 10 Clustering Algorithms With Python
- https://machinelearningmastery.com/clustering-algorithms-withpython

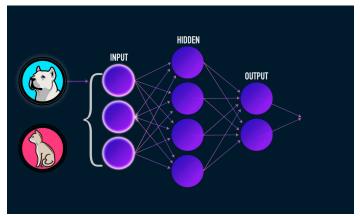


You can use Google Colab to test some clustering algorithms



# What about image recognition?

- Image recognition (or image classification) is probably the most known achievement of modern AI seen by the general public thanks to Google, Facebook, ...
- Image recognition is one of the tasks in which Deep Neural Networks (DNNs) excel
- DNN are at the foundation of so-called Deep Learning (DL) techniques which is a subset of ML techniques
- Most of image recognition approaches thus DL – belong to the supervised ML category

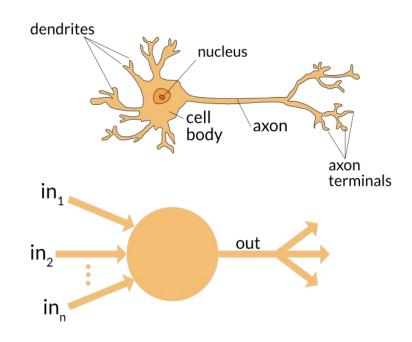


**TowardsDataScience** 



## More like humans? Towards DL!

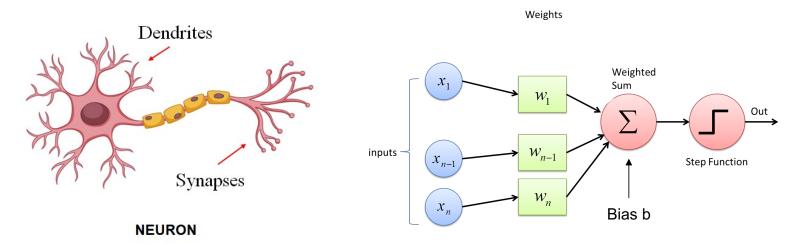
- In early AI ages, researchers wanted to mimic the human brain seen as a network of neurons
- Perceptron: Mathematical representation of a biological neuron
- First implementation by Frank Rosenblatt in 1958
- Rosenblatt's perceptron is activated when there is sufficient stimuli or input
- Neurons have been found to perform a similar process, in which experience strengthens or weakens dendrites' connections





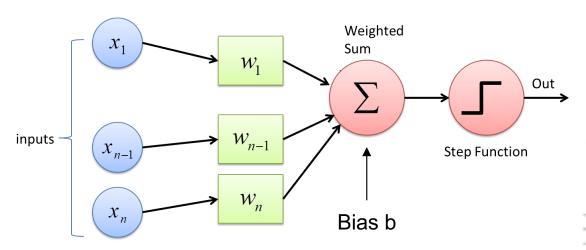
# How does a Perceptron work?

- Single Layer Perceptron (SLP) receives the value of the attributes of an input, just as dendrites do in a neuron
- Each attribute has a **weight** w that measures its *contribution* to the final result, which is the sum of the multiplications of inputs of each attribute by its corresponding weight
- The final output depends on the activation function: here, if the sum is >0 Perceptron returns a value of 1, otherwise it yields 0



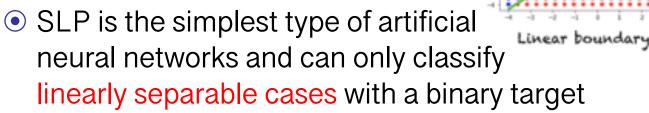
48

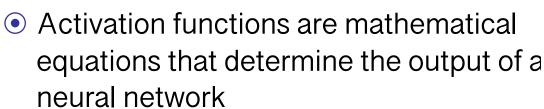
# What can an SLP do?



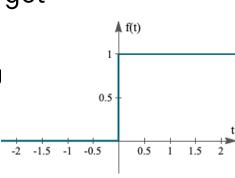
 $\hat{y} = \Theta(w_1 x_1 + w_2 x_2 + \dots + w_n x_n + b)$  $= \Theta(\mathbf{w} \cdot \mathbf{x} + b)$ 

where 
$$\Theta(v) = \begin{cases} 1 & \text{if } v \geqslant 0 \\ 0 & \text{otherwise} \end{cases}$$







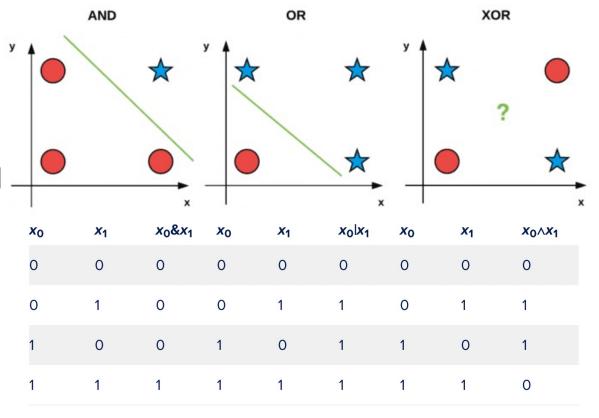


Non-linear boundary



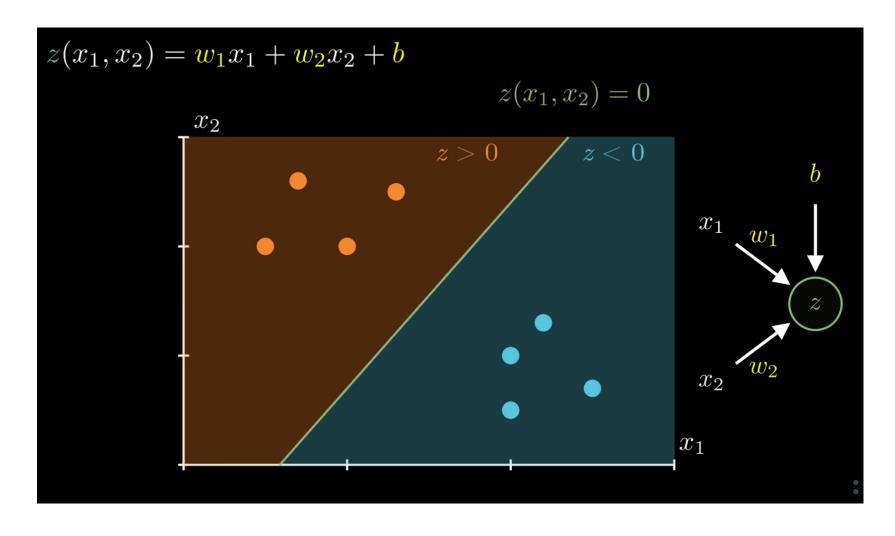
# Linearly vs nonlinearly separable

- Most real world problems are nonlinearly separable!
- OK, but can you find a clear example?
- Let's try to better understand nonlinearly separable cases on a very simple example
- Take the AND, OR and XOR logic gates
- AND and OR are linearly separable
- XOR is nonlinearly separable!



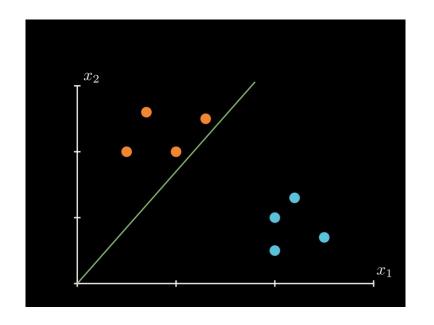


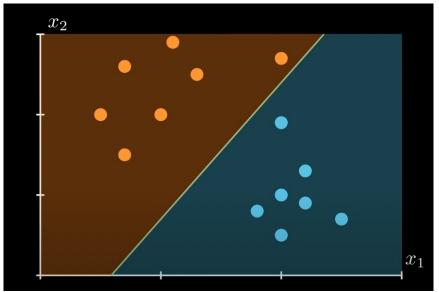
# The perceptron classifier





## The role of the bias b



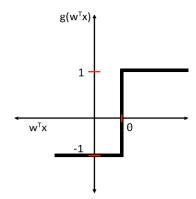


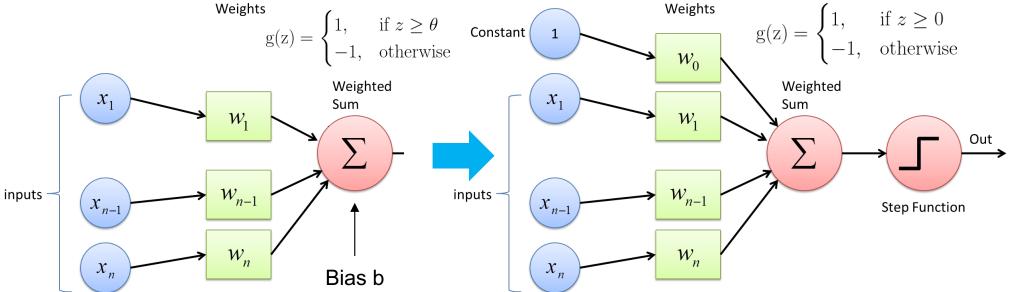
- When b=0, the separation line (decision boundary) goes from the origin
- With a bias b, it is possible to move the decision boundary to better divide the 2 target areas



# Adding the bias as an input

- In general, we define an activation function g(z), where if g(z) is greater than a defined threshold  $\theta$  we classify accordingly (1 or -1 for instance)
- To simplify the notation, we bring  $\theta$  to the left side of the equation and define  $w_0 = -\theta$  and  $x_0 = 1$  (also known as bias)

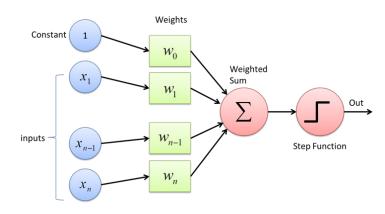






# Dot product and matrix notation

$$z = \sum_{j=0}^{m} x_j w_j = w^T x$$



The dot product of two vectors  $\mathbf{a} = [a_1, a_2, \dots, a_n]$  and  $\mathbf{b} = [b_1, b_2, \dots, b_n]$ ,

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

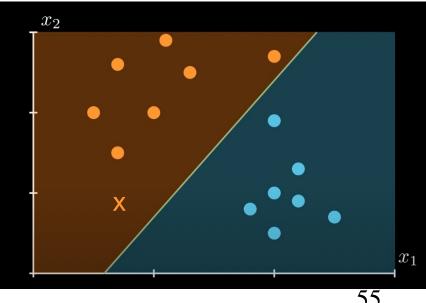
 If vectors are identified with column vectors, the dot product can also be written as a matrix product

$$\mathbf{a} \cdot \mathbf{b} = \mathbf{a}^\mathsf{T} \mathbf{b}, \qquad \begin{bmatrix} \mathbf{1} & \mathbf{3} & -\mathbf{5} \end{bmatrix} \begin{bmatrix} \mathbf{4} \\ -\mathbf{2} \\ -1 \end{bmatrix} = 3$$



#### How does it learn?

- Learning means for the perceptron to find the right w<sub>i</sub> and b to correctly divide the training dataset into 2 clear target classes
- Remind that the training dataset should be correctly labeled in supervised learning
- x₂ could be wheel size and x₁ could be vehicle length
- Then the 2 target classes could be truck (e.g. z > 0) and bus (e.g. z < 0)
- The training dataset would consist in a list of  $(x_1, x_2)$  that have been identified either as truck or car
- After training, the decision boundary should be able to still correctly divide the new  $(x_1, x_2)$  pair





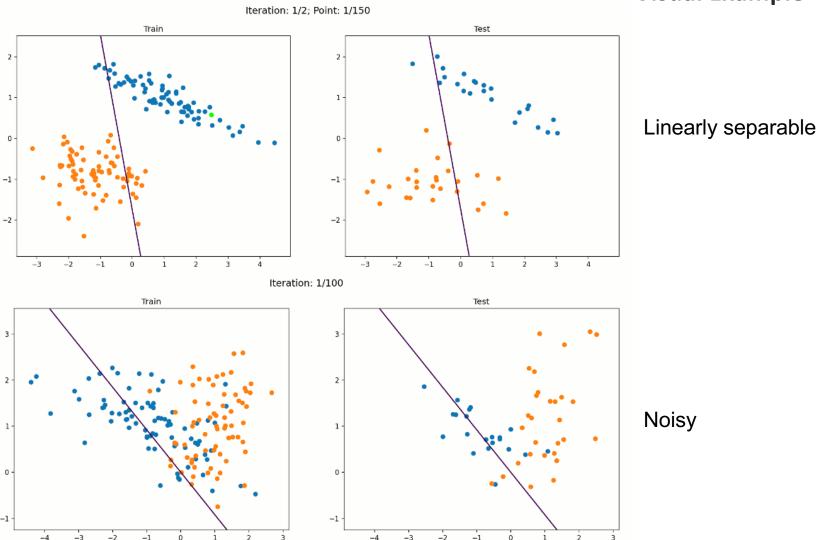
# Quick overview of learning process

- In the Perceptron Learning Rule, the predicted output is compared with the known output. If it does not match, the error is propagated backward to allow weight adjustment to happen
- At the beginning, initialize the w<sub>i</sub> to 0 or small random numbers
- For each training sample x<sup>i</sup>: calculate the output value and update the w<sub>i</sub>
- The output value is the class label predicted by the unit step function and the weight update can be written more formally as  $w_i = w_i + \Delta w_i$
- The value for updating the weights at each increment is calculated by the learning rule:  $\Delta w_i = \eta(target^i output^i) x_i^i$
- where η is the learning rate (a constant between 0.0 and 1.0), target is the true class label, and the output is the predicted class label
- In textual form: weight=weight+learning\_rate\*error\*input
- It can be time consuming and we will see that there are more efficient algorithms when the neural network becomes more complex



# Learning in image

#### Perceptron: Explanation, Implementation and a Visual Example



https://towardsdatascience.com/perceptron-explanation-implementation-and-a-visual-example-3c8e76b4e2d1

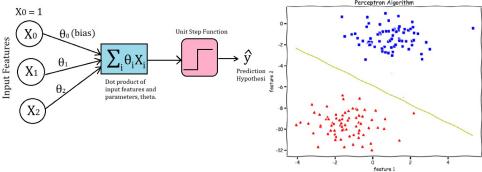
- -



# Coding a perceptron from scratch Assignment to do in lab

• <a href="https://towardsdatascience.com/perceptron-algorithm-in-python-f3ac89d2e537">https://towardsdatascience.com/perceptron-algorithm-in-python-f3ac89d2e537</a>

\*\*Total Company of the Property of the

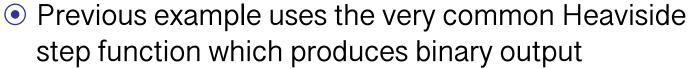


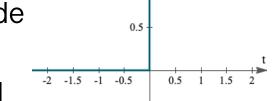
- You can use Google Colab to test the code. Need to add:
  - import matplotlib.pyplot as plt and import numpy as np
- Other links
  - https://medium.com/@becaye-balde/perceptron-building-it-from-scratch-in-python-15716806ef64
  - https://machinelearningmastery.com/implement-perceptron-algorithmscratch-python/
  - https://python.plainenglish.io/building-a-perceptron-from-scratch-a-stepby-step-guide-with-python-6b8722807b2e



## **Activation functions**

 SLP is a feed-forward network based on a threshold transfer function which is the decision making unit



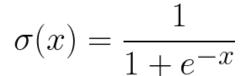


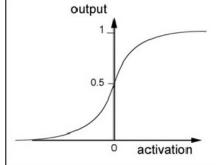
♠ f(t)

- The heaviside step function is typically only useful within SLP
- There are more functions available and their interest will be described later when we will present multi-layer NN
  - Sigmoid or Logistic (or squashing) Function



- Tanh or hyperbolic tangent Function
- ReLU or Rectified Linear Unit
- ...

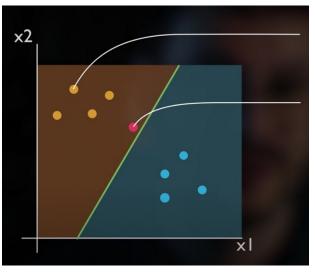






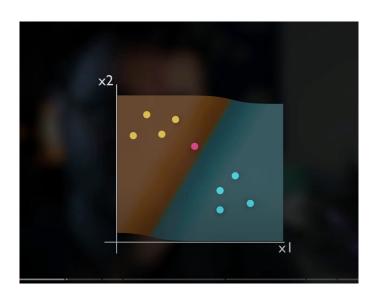
# Sigmoid Activation Function

- Sigmoid function can be used to represent a probabilistic output
- When classifying, some points can be considered as quite "sure" (to be truck or bus in the previous example)
- The farther they are from the decision boundary, the more sure we can be



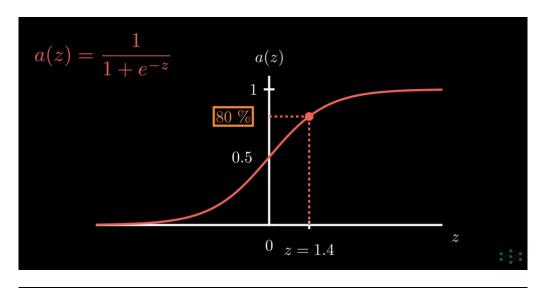
High probability

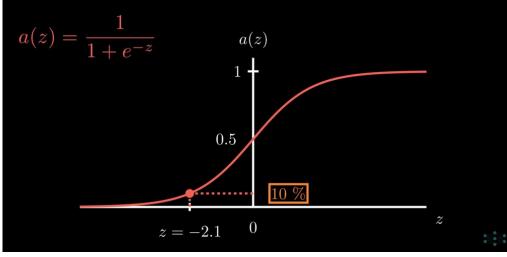
Lower probability





# Expressing a probability...and squashing!

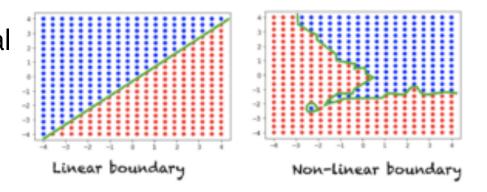






### SLP limitations and how to solve them?

 SLP is the simplest type of artificial neural networks and can only classify linearly separable cases with a binary target



To solve an non-linear problem, the output should be non-linear!

To solve a complex non-linear problem, a single non-linear

output is not sufficient!

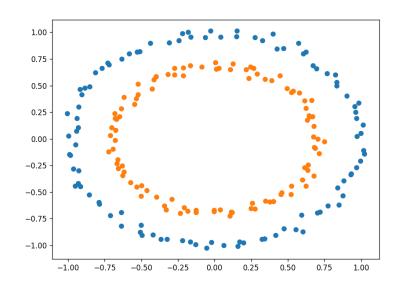
 e.g. a building is mainly made of concrete, but you probably need several competencies to make a building!





## Is non-linear out of reach for SLP?

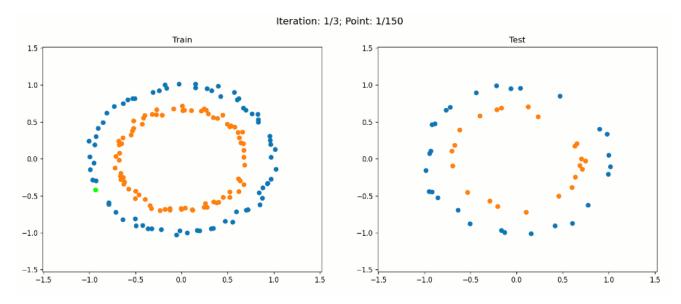
- Consider this dataset, it is separable, but clearly not linear
- We may think that a perceptron would not be good for this task
- But, decision boundary is linear in terms of the weights, not necessarily in terms of inputs
- We can augment our input vectors x so that they contain non-linear functions of the original inputs
- For example, in addition to the original inputs x<sub>1</sub> and x<sub>2</sub> we can add the terms x<sub>1</sub><sup>2</sup>, x<sub>1</sub> . x<sub>2</sub>, and x<sub>2</sub><sup>2</sup>



$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \quad \Longrightarrow \quad x = \begin{bmatrix} x_1 \\ x_2 \\ x_1^2 \\ x_1 x_2 \\ x_2^2 \end{bmatrix}$$



# Feature augmentation, see it in image



- The plotting uses the original inputs in order to keep it 2D. The decision boundary is still linear in the augmented feature space which is 5D now
- But when we plot that decision boundary projected onto the original feature space it has a non-linear shape



# So SLP is good for non-linear as well?

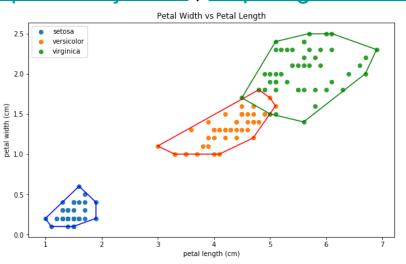
- With the previous method, our perceptron algorithm was able to correctly classify both training and testing examples without any modification of the algorithm itself – all we changed was the dataset
- With this feature augmentation method, we are able to model very complex patterns in our data by using algorithms that were otherwise just linear
- But, this method is not very efficient. Imagine what would happen if we had 1000 input features and we want to augment it with up to 10-degree polynomial terms!

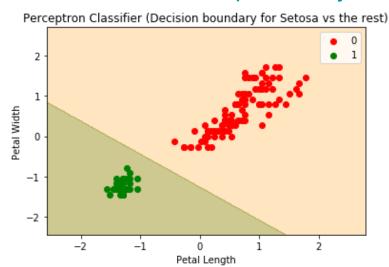


# Testing linear separability

#### Assignment to do in lab

 https://tatwan.github.io/blog/python/2017/12/31/linearseparability.html; https://github.com/tatwan/Linear-Separability



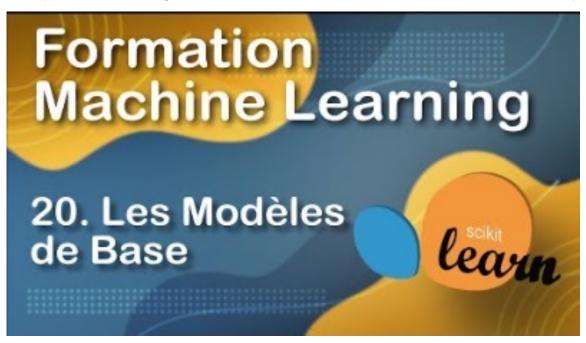


- You can use Google Colab to test the code
  - Replace from pandas.tools.plotting by from pandas.plotting
- What is a confusion matrix? For SVM RBF, change C and gamma parameters.



# Pre-requisite for previous assignment

https://www.youtube.com/watch?v=P6kSc3qVph0

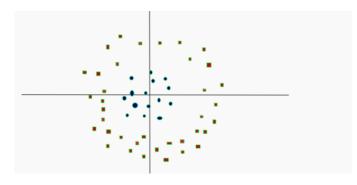


 Part of PYTHON SKLEARN playlist from MachineLearnia <u>https://www.youtube.com/playlist?list=PLO\_fdPEVlfKoHQ3Ua2</u> <u>NtDL4nmynQC8YiS</u>



# Pre-requisite for previous assignment

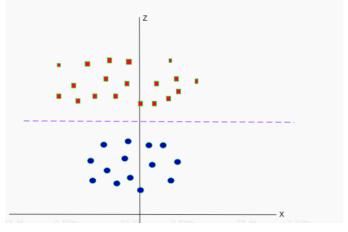
- Non-linear SVM, consider the following nonlinearly separable dataset
- This data can be converted to linearly separable data in higher dimension



- Lets add one more dimension and call it z-axis:  $z = x^2 + y^2$
- z coordinate is the square of distance of the point from origin.

Now the data is clearly linearly separable

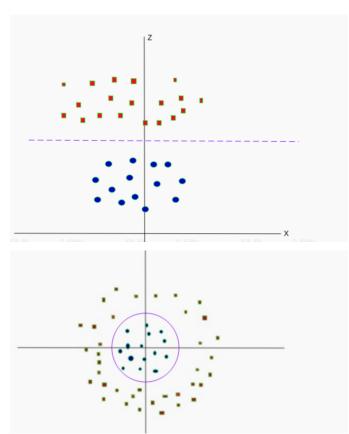
- Let the purple line separating the data in higher dimension be z=k, where k is a constant
- Since,  $z=x^2+y^2$  we get  $x^2 + y^2 = k$ ; which is an equation of a circle!





# Pre-requisite for previous assignment

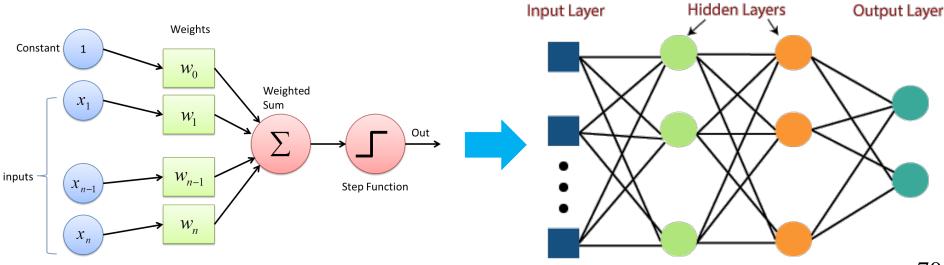
- Since,  $z=x^2+y^2$  we get  $x^2+y^2=k$ ; which is an equation of a circle!
- We can project this linear separator in higher dimension back in original dimensions using this transformation
- But finding the correct transformation for any given dataset isn't that easy
- Thankfully, we can use kernels in SKLEARN's SVM implementation to do this job
- For instance, the Radial Basis Function (RBF) kernel
- https://scikit-learn.org/stable/modules/svm.html#parameters-of-therbf-kernel





# Multi-Layer Perceptron - MLP

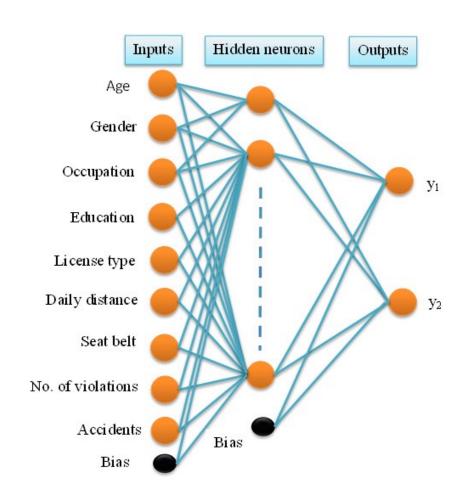
- Multi-Layer Perceptrons (and so-called neural networks) can be considered as more general function approximators and they are able to distinguish data that is not linearly separable
- MLP have several neuron layers with so-called hidden layers
- Hidden layers are "hidden" to the final user who only "see" inputs and outputs





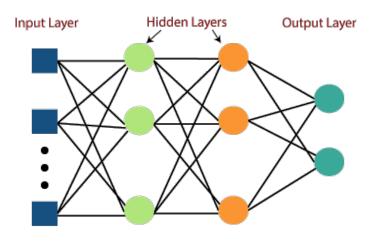
# Towards decision-making!

- MLP are more general function approximators, taking a large number of features in consideration
- The complex classification can become a simple decision-making process!
- Here, should an insurance company sign with a driver or not!
- With more outputs, we could also have more final decisions such as the insurance price!





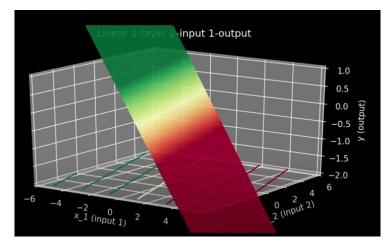
# Again, what output function?



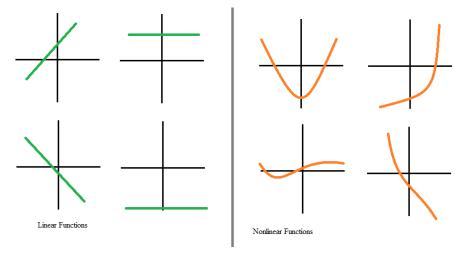
From SLP to MLP, regardless of the number of layers or weights, if outputs are linear, there is no way to have non-linear behavior!

$$\hat{y} = \Theta(w_1 x_1 + w_2 x_2 + \dots + w_n x_n + b)$$
$$= \Theta(\mathbf{w} \cdot \mathbf{x} + b)$$

 This is why MLP usually have non-linear output function



https://www.youtube.com/watch?v=dPWYUELwIdM

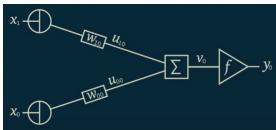


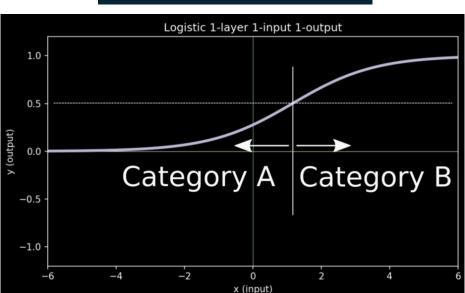


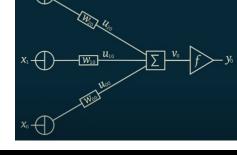
### Back to Logistic function

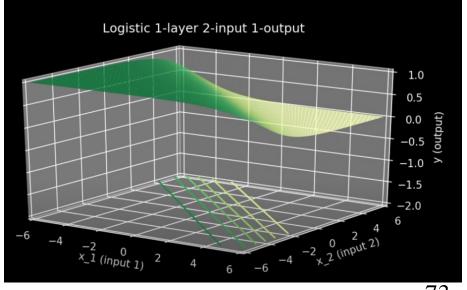
• The Logistic function (Sigmoid) is non-linear and can separate 2

categories





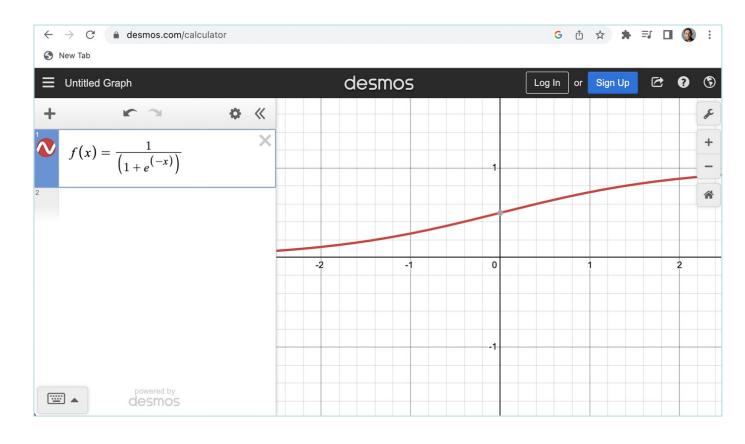






# Online function plotting

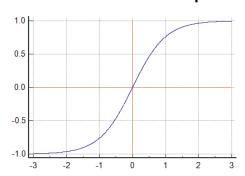
#### • www.desmos.com/calculator



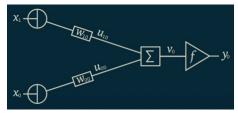


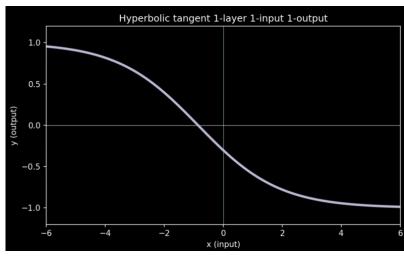
## The hyperbolic tangent - tanh

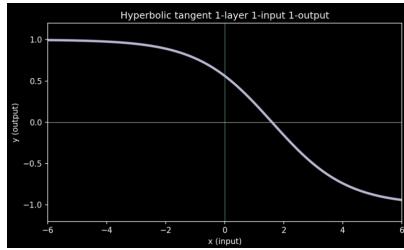
 It is basically a shifted sigmoid neuron. It takes a real valued number and squashes it between -1 and +1



$$\tanh(x) = \frac{(e^x - e^{-x})}{(e^x + e^{-x})} = \frac{2}{1 + e^{-2x}} - 1 = 2\text{sigmoid}(2x) - 1$$



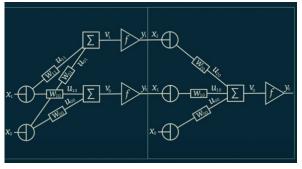


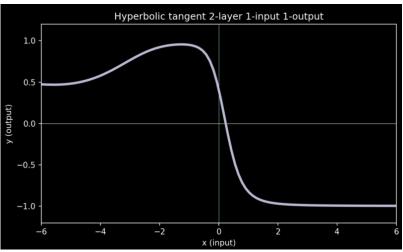


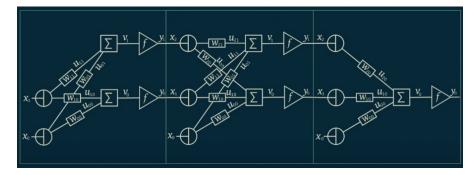


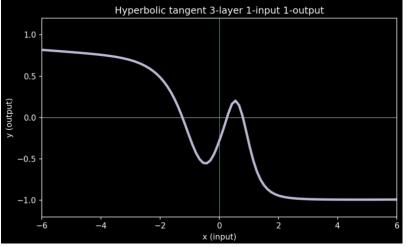
## Tanh with several layers

 When adding additional layers, the output can be much more complex, allowing for non-linear classification







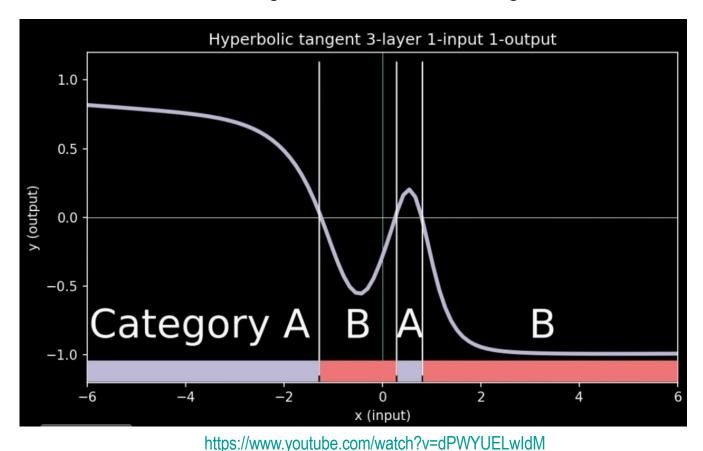


https://www.youtube.com/watch?v=dPWYUELwIdM



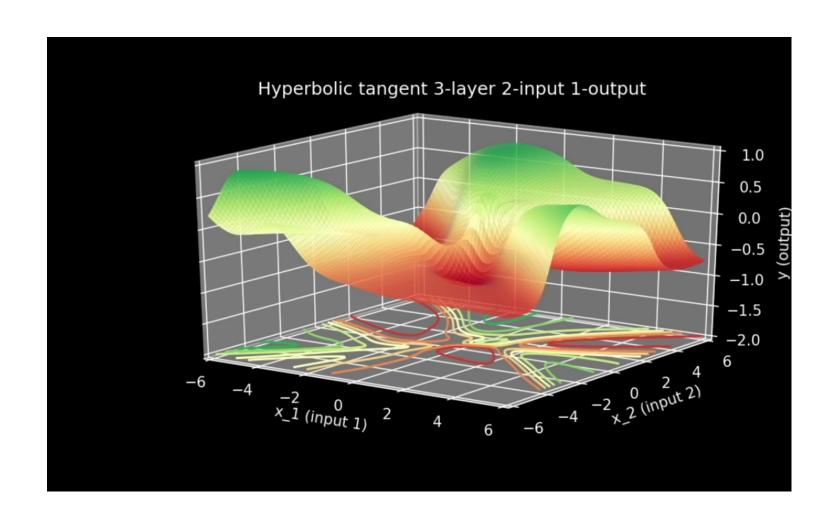
## New classification possibilities?

 The ability to create complex output enables the detection and the classification of a larger number of catagories



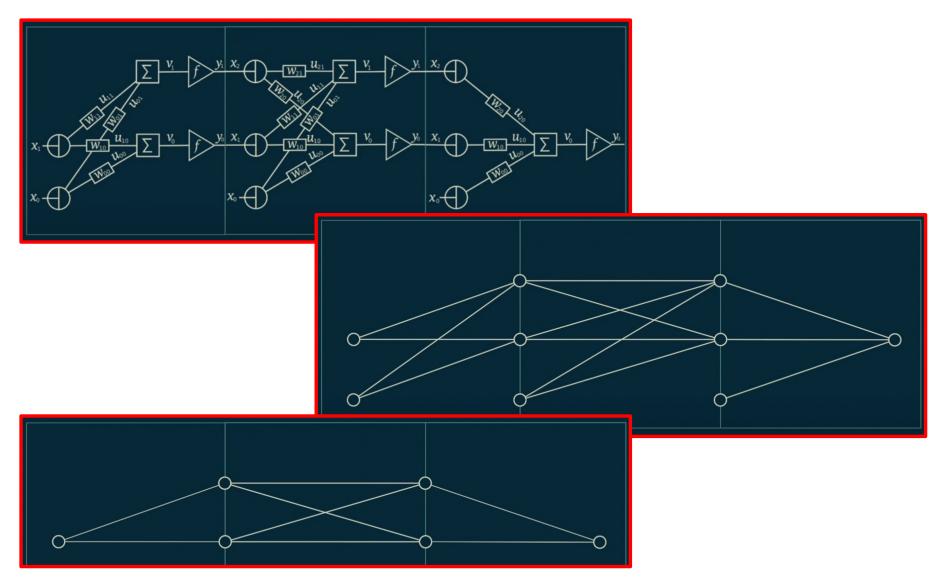


## See it in 3D – 3 layers, 2 inputs





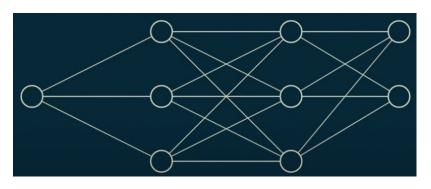
# Simplifying the representation of MLP

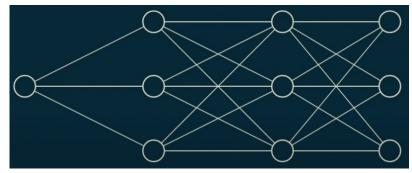


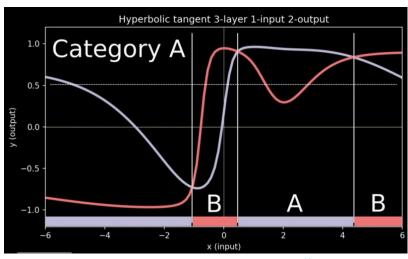


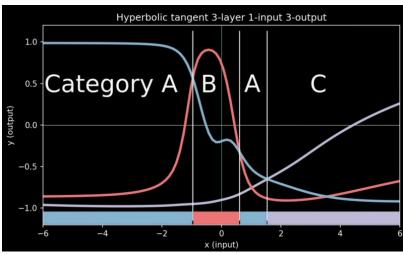
## Adding more outputs

2 and 3 outputs with tanh activation fonction







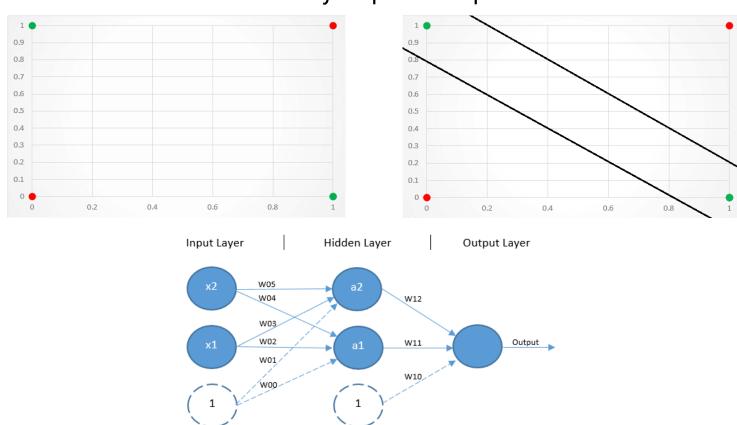


https://www.youtube.com/watch?v=dPWYUELwIdM



### Back to the XOR problem

- XOR is a nonlinearly separable problem so SLP won't work
- MLP can solve nonlinearly separable problems so MLP should work

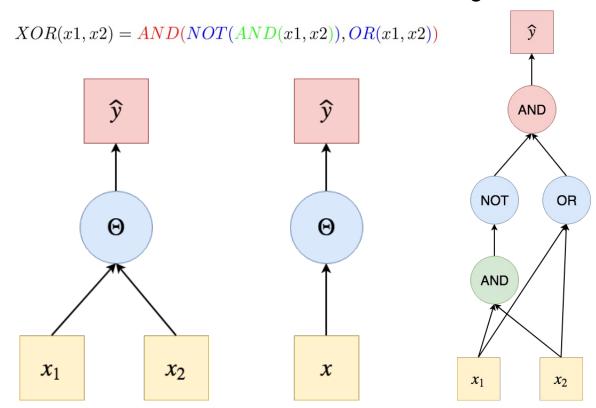




## XOR: example 1

#### Assignment to do in lab

- https://towardsdatascience.com/perceptrons-logical-functionsand-the-xor-problem-37ca5025790a
- View it as combination of NOT, AND and OR gates



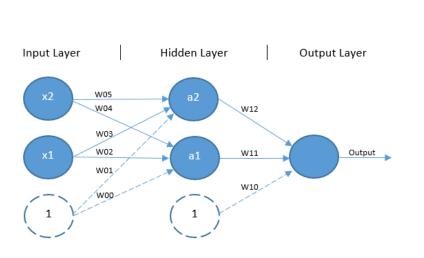


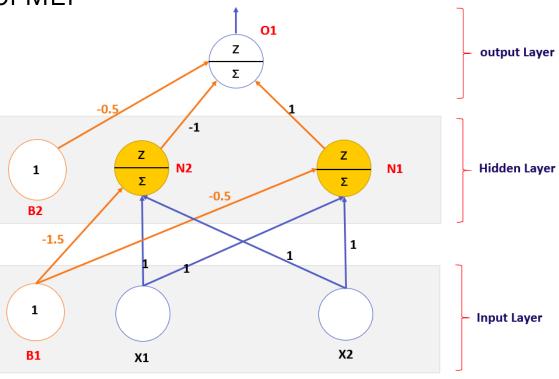
## XOR: example 2

### Assignment to do in lab

 https://medium.com/analytics-vidhya/xor-gate-with-multilayerperceptron-66e78671acd4

One step towards usage of MLP

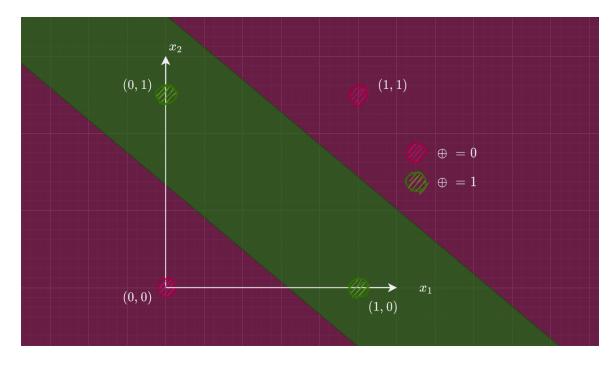






# XOR: example 3 Assignment to do in lab

- https://towardsdatascience.com/how-neural-networks-solvethe-xor-problem-59763136bdd7
- Finally, the MLP with training approach



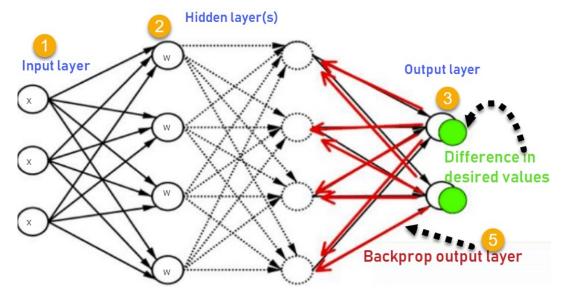


### Learning in MLP?

- With more layers, there are more parameters to optimize, so training an MLP is obviously more complex and will take much much more time, if not done in an intelligent way!
- A fundamental method in neural network is back-propagation!

The errors are first calculated at the output units where the formula is quite simple (based on the difference between the target and predicted values), and then propagated back through the network in a clever fashion, allowing us to efficiently update our weights during training and (hopefully) reach a minimum.

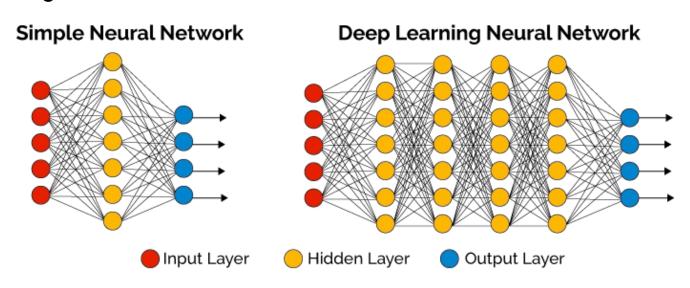
From <a href="https://www.toptal.com/machine-learning/an-introduction-to-deep-learning-from-perceptrons-to-deep-networks">https://www.toptal.com/machine-learning/an-introduction-to-deep-learning-from-perceptrons-to-deep-networks</a>





### Deep Neural Networks

- In the 1980s, most Artificial Neural Networks were single-layered due to the cost of computation and availability of data.
- Nowadays is possible to afford more hidden layers, hence the moniker "Deep Neural Networks".
- Regained popularity since ~2006 and rebranded as Deep Learning (DL)





### Hidden layers

• By the universal approximation theorem, a single hidden layer network with a finite number of neurons can be trained to approximate an arbitrarily random function. In other words, a single hidden layer is powerful enough to learn any function.

That said, we often learn better in practice with multiple hidden

layers (i.e., deeper nets)

 Hidden layers in a NN allows to create/store internal abstract representation of the training data

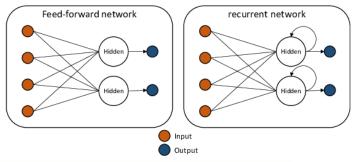
 The higher layers are "building" new abstractions on top of previous layers

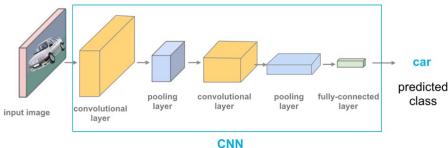
From <a href="https://www.toptal.com/machine-learning/an-introduction-to-deep-learning-from-perceptrons-to-deep-networks">https://www.toptal.com/machine-learning/an-introduction-to-deep-learning-from-perceptrons-to-deep-networks</a>

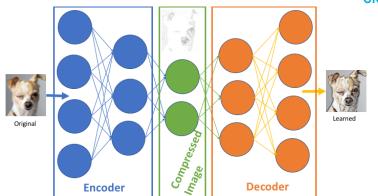


# Types of Deep Neural Networks

- Feedforward Neural Networks (FFNs, ANNs or NNs)
- Recurrent Neural Networks (RNNs)
- Convolutional Neural Networks (CNNs)
- Autoencoder Neural Networks (AEs)



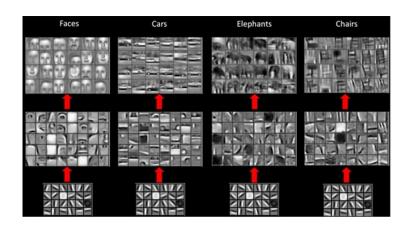


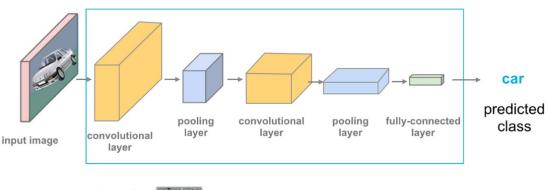


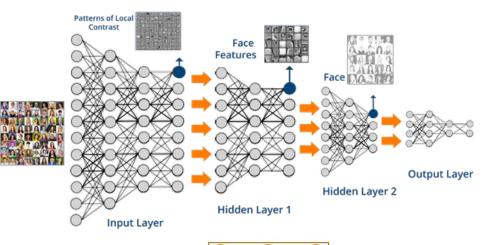


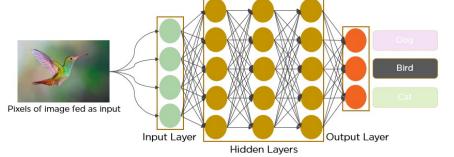
### Convolutional Neural Networks

- Contain five types of layers
- Each layer has a specific purpose, like summarizing, connecting or activating
- CNN are good at image classification and object detection







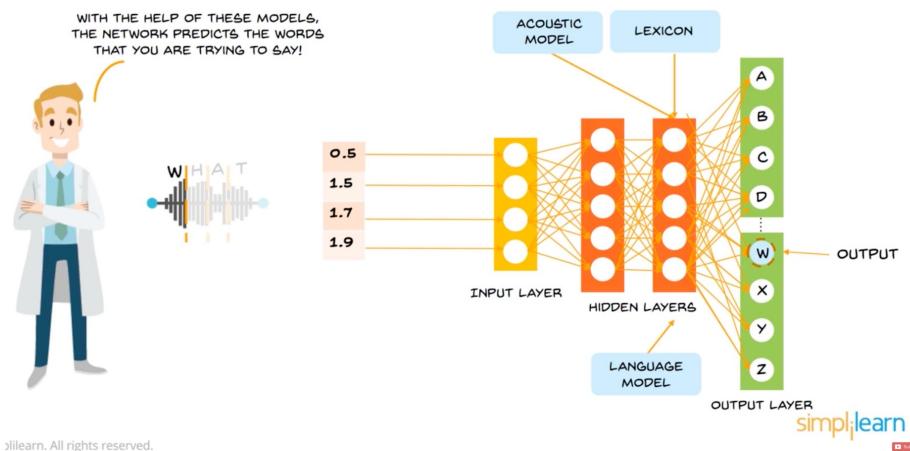


89



http://www.univ-pau.fr/~cpham Pr. Congduc Pham

# Examples for Deep Learning (1)

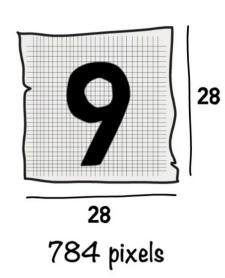


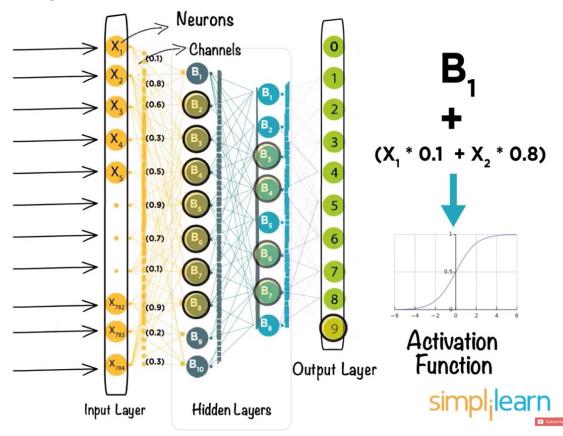


Pr. Congduc Pham http://www.univ-pau.fr/~cpham

# Examples for Deep Learning (2)

# Deep Learning



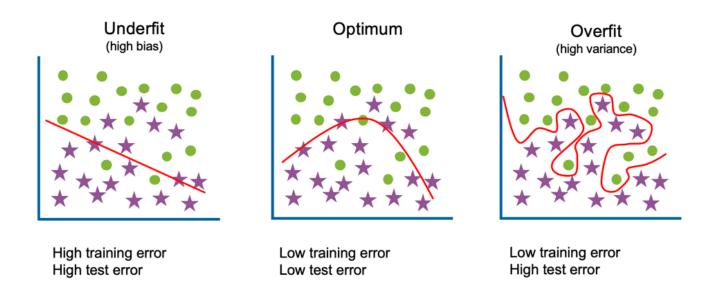


©Simplilearn. All rights reserved.



## Overfitting?

Overfitting describes the phenomenon of fitting the training data too closely, maybe with hypotheses that are too complex. In such a case, your learner ends up fitting the training data really well, but will perform much, much more poorly on real examples.





# Gradient

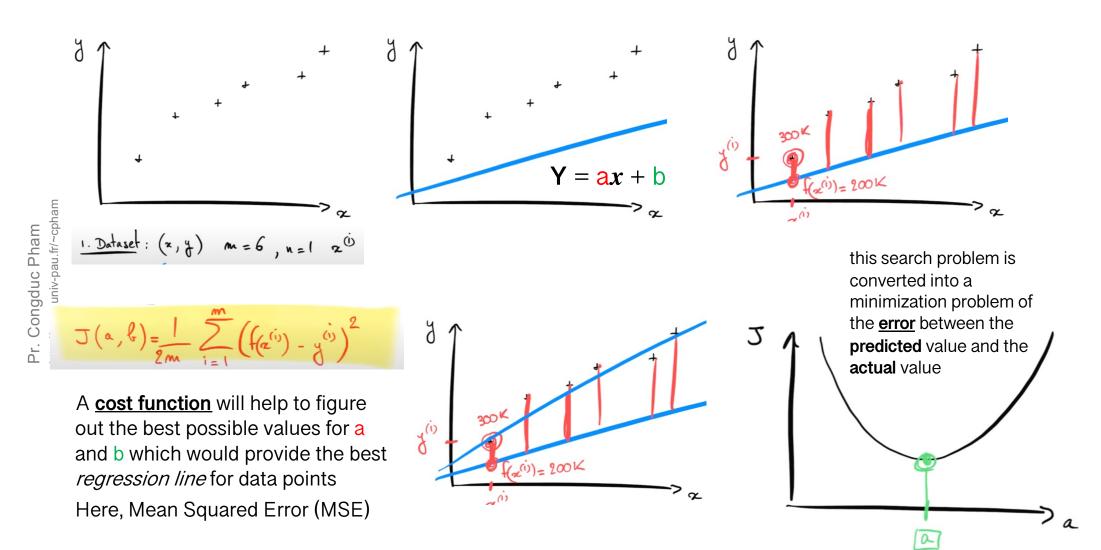
# Descent

in

AI



### Back to the cost function in regression



94

Pictures from <a href="https://www.youtube.com/watch?v=wg7-roETbbM">https://www.youtube.com/watch?v=wg7-roETbbM</a> (Machine Learnia)



### How to find the minimun?

 Exact methods can be used to find the minimum of the cost function

$$J(a,b) = \frac{1}{2m} \sum_{i=1}^{m} (f(a^{(i)}) - y^{(i)})^2$$

- But these exact methods needs a lot of complex maths
  - What if the size of the dataset is large, e.g. millions of points?
  - What if we have multiple variable, e.g. multivariate regression?
- Then these complex math operations will take a long, long, long time even for state-of-the-art supercomputers!



### Lost in the mountain?

Finding the lowest point...at the bottom of the valley



Get to a safe place, at the bottom of the valley







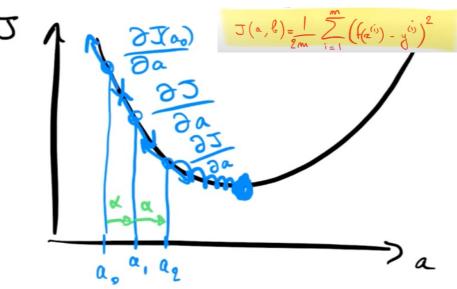
## Principle behind Gradient Descent

- From your position, look around you and find the direction with the highest slope
- Walk for 300m in that direction
- Re-iterate until you reach the bottom

#### **Machine version**

- Start at a<sub>0</sub> and compute the slope, i.e. the derivative
- Advance from  $a_0$  to  $a_1$  ( $\alpha$ =300m)
- Re-iterate until derivative is zero



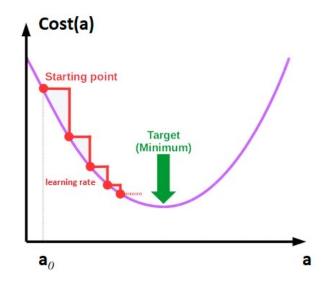




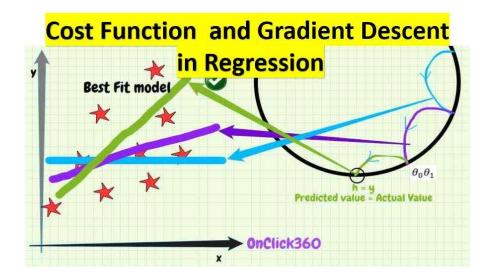
### Gradient Descent for linear regression

 $J(a, b) = \frac{1}{2m} \sum_{i=1}^{m} \left( f(a^{(i)}) - y^{(i)} \right)^{2}$ 

- Gradient Descent is a method of updating a and b to reduce the error (Cost Function)
- The idea is to start with arbitrary values for a and b then change these values iteratively to reduce the cost
- Gradient Descent helps on how to change the values



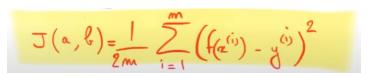


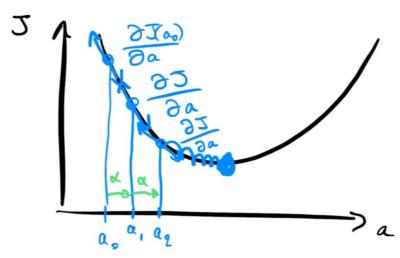




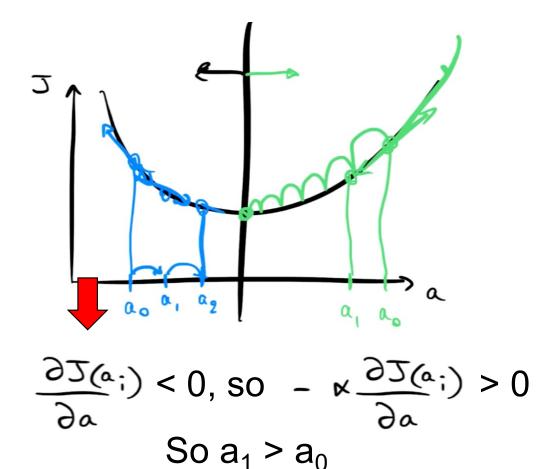
Pr. Congduc Pham http://www.univ-pau.fr/~cpham

## Why is it more "intelligent"?





$$a_{i+1} = a_i - \kappa \frac{\partial a_{(i)}}{\partial a_{(i)}}$$

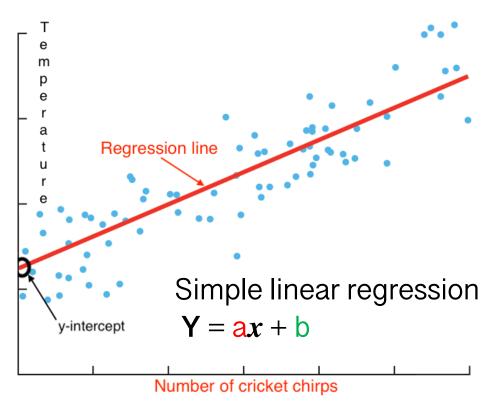


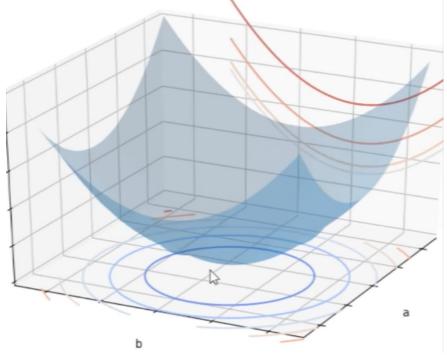
The algorithm converges automatically!



# Why do we need that "intelligence"?

- With a simple line, we need to search for both a and b
- That already gives a large surface!
- So the search space can be huge!

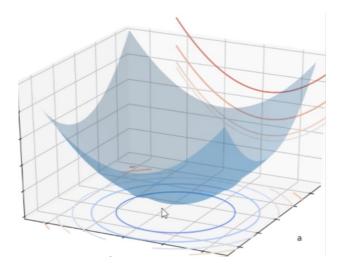


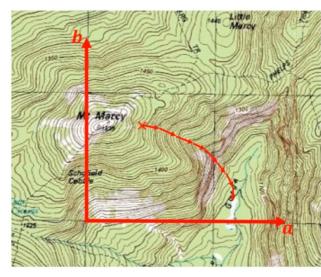


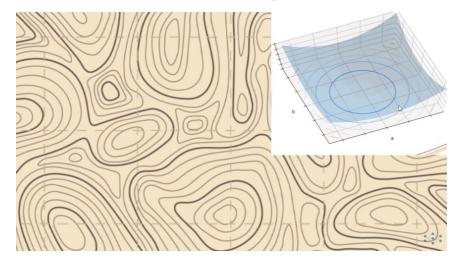
100

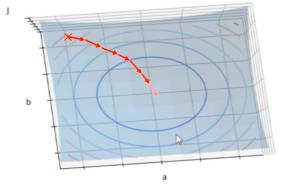


# Gradient Descent ~ outdoor map!





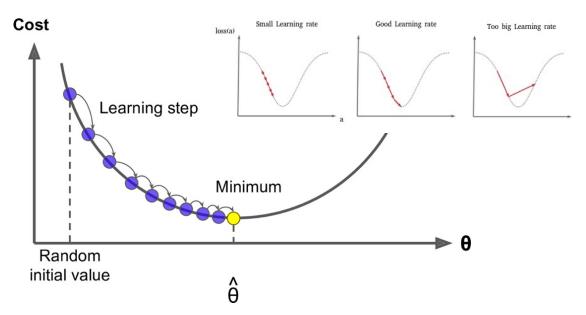


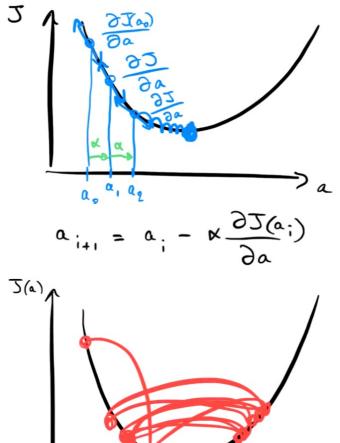




## Learning Rate $\alpha$ – hyperparameter

- A smaller *learning rate* could get closer to the *minima* but takes more time to reach the *minima* (300m -> 50m)
- A larger *learning rate* converges sooner but there is a chance that you could overshoot the *minima* (300m -> 800m)

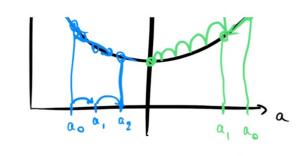




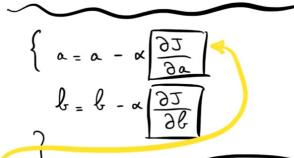
OBJECTIF

# Pr. Congduc Pham http://www.univ-pau.fr/~cpham

## Equation of GD for linear regression



$$\begin{cases} g = \beta - \alpha \sqrt{\frac{9\beta}{92}} \\ \alpha = \alpha - \alpha \sqrt{\frac{9\sigma}{92}} \end{cases}$$



$$\frac{\partial J}{\partial a}$$
:  $\frac{1}{m} \sum_{x} (\alpha x + b - y)$ 

$$f(a,b)=ax+b-y$$
  
 $g(f)=f^2$ 

$$(g \circ f)'=f' \cdot g'(f)$$

- Dataset: (x, y) avec m exemples
- Modèle: f(x) = ax + b
- Fonction Coût:  $J(a,b) = \frac{1}{2m} \sum_{i=1}^{m} (ax^{(i)} + b y^{(i)})^2$
- · Gradients:

$$\frac{\partial J(a,b)}{\partial a} = \frac{1}{m} \sum_{i=1}^{m} x^{(i)} \left( ax^{(i)} + b - y^{(i)} \right)$$
$$\frac{\partial J(a,b)}{\partial b} = \frac{1}{m} \sum_{i=1}^{m} \left( ax^{(i)} + b - y^{(i)} \right)$$

• Algorithme de Gradient Descent :

$$a = a - \alpha \frac{\partial J(a, b)}{\partial a}$$

$$b = b - \alpha \frac{\partial J(a,b)}{\partial b}$$



### Matrix notation with Gradient Descent





## Putting it altogether!

- Dataset: (x, y) avec m exemples
- Modèle: f(x) = ax + b
- Fonction Coût:  $J(a,b) = \frac{1}{2m} \sum_{i=1}^{m} (ax^{(i)} + b y^{(i)})^2$
- · Gradients:

$$\frac{\partial J(a,b)}{\partial a} = \frac{1}{m} \sum_{i=1}^{m} x^{(i)} (ax^{(i)} + b - y^{(i)})$$

$$\frac{\partial J(a,b)}{\partial b} = \frac{1}{m} \sum_{i=1}^{m} \left( ax^{(i)} + b - y^{(i)} \right)$$

· Algorithme de Gradient Descent :

$$a = a - \alpha \frac{\partial J(a, b)}{\partial a}$$

$$b = b - \alpha \frac{\partial J(a, b)}{\partial b}$$

#### Régression Linéaire: Résumé des équations

• Dataset: (x, y) avec m exemples, n variables

$$X = \begin{bmatrix} x^{(1)} & 1 \\ \dots & \dots \\ x^{(m)} & 1 \end{bmatrix} \qquad Y = \begin{bmatrix} y^{(1)} \\ \dots \\ y^{(m)} \end{bmatrix} \qquad \theta = \begin{bmatrix} a \\ b \end{bmatrix}$$

$$m \times (n+1) \qquad m \times 1 \qquad (n+1) \times 1$$

- Modèle :  $F = X.\theta$   $m \times 1$
- Fonction Coût:  $J(\theta) = \frac{1}{2m} \sum (X \cdot \theta Y)^2$   $1 \times 1$
- Gradients:  $\frac{\partial J(\theta)}{\partial \theta} = \frac{1}{m} X^T . (X.\theta Y) \quad (n+1) \times 1$
- Gradient Descent :  $\theta := \theta \alpha \frac{\partial J(\theta)}{\partial \theta}$  (n+1)×1

https://machinelearnia.com/



# Programming GD in Python

Assignment to do in lab



https://www.youtube.com/watch?v=vG6tDQc86Rs (Machine Learnia)

Code on github: <a href="https://github.com/MachineLearnia/Regression-lineaire-numpy/blob/master/R%C3%A9gression%20Lin%C3%A9aire%20Numpy.ipynb">https://github.com/MachineLearnia/Regression-lineaire-numpy/blob/master/R%C3%A9gression%20Lin%C3%A9aire%20Numpy.ipynb</a>



# Programming GD in Python

Assignment to do in lab

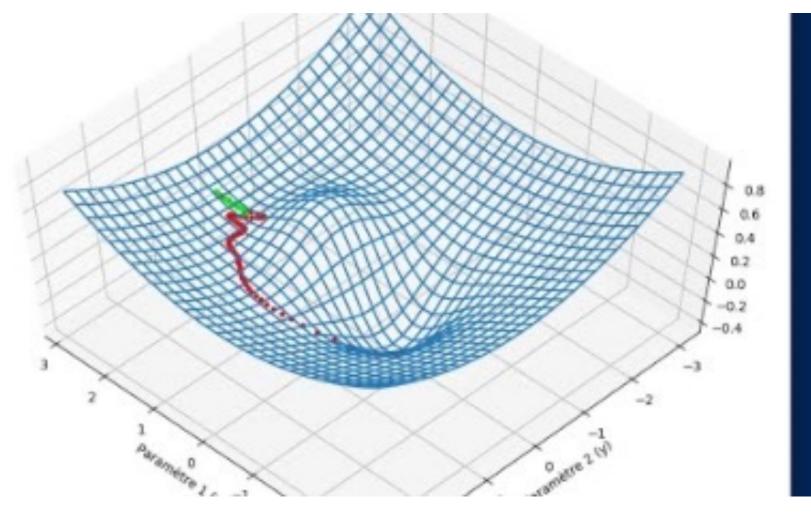


https://www.youtube.com/watch?v=cpltYCNLIt0 (Machine Learnia)

Code on github: <a href="https://github.com/MachineLearnia/Regression-lineaire-numpy/blob/master/R%C3%A9gression%20Lin%C3%A9aire%20Multiple.ipynb">https://github.com/MachineLearnia/Regression-lineaire-numpy/blob/master/R%C3%A9gression%20Lin%C3%A9aire%20Multiple.ipynb</a>



# Going deeper in GD



https://www.youtube.com/watch?v=0MEyDJa2GTc (L42Project)

Code on github: https://github.com/L42Project/Tutoriels/tree/master/Divers/descente\_gradient



## Gradient Descent & output functions

- The only non-linear function that can be used as an activation function in a neural network is one which is monotonically increasing. So for example, sin(x) or cos(x) cannot be used as activation functions.
- Also, the activation function should be defined everywhere and should be continuous everywhere in the space of real numbers. The function is also required to be differentiable over the entire space of real numbers
- $\bullet$  For instance Heaviside is not for x=0
- Typically a back propagation algorithm uses gradient descent to learn the weights of a neural network. To derive this algorithm, the derivative of the activation function is required

0.5

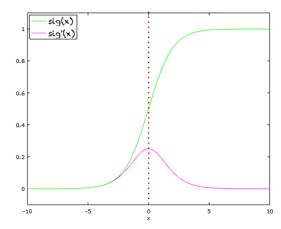


## Example: the Logistic function

• The graph of sigmoid function is an S-shaped curve as shown by the green line in the graph below. The figure also shows the graph of the derivative in pink color. The expression for the

derivative, along with some important properties are shown on the right

 The fact that the sigmoid function is monotonic, continuous and differentiable everywhere, coupled with the property that its



Plot of  $\sigma(x)$  and its derivate  $\sigma'(x)$ 

Domain:  $(-\infty, +\infty)$ Range: (0, +1) $\sigma(0) = 0.5$ 

Other properties

$$\sigma(x) = 1 - \sigma(-x)$$

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

$$\sigma'(x) = \sigma(x)(1 - \sigma(x))$$

derivative can be expressed in terms of itself, makes it easy to derive the update equations for learning the weights in a neural network when using back propagation algorithm

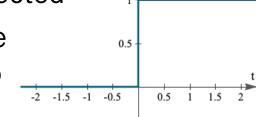


#### Choosing a right activation function (1)

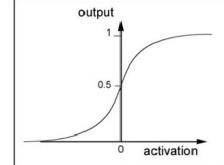
 Closely related to the efficiency of the learning phase, the choice of the activation function can have an important impact

For instance, the convergence of GD can be affected

 For instance, the derivative should provide some "information". Heaviside derivative is mainly 0 so GD will not perform well



 The Sigmoid function can "kill" gradient: Sigmoid neurons get saturated on the boundaries and hence the local gradients at these regions is almost zero (vanishing gradient problem)



 We also need to avoid saturation because, if the initial weights are too large the network will hardly learn



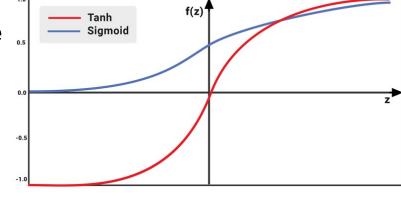
#### Choosing a right activation function (2)

 Sigmoid is also non zero-centered outputs: output after applying sigmoid is always positive so the gradient on the weights during backpropagation will always be either positive or negative which which makes optimization harder

• The Tanh or hyperbolic tangent Activation Function can

somehow be similar to Sigmoid and saturates at large positive and negative

 However, its output is always zerocentered which helps since the neurons in the later layers of the network would be receiving inputs that are zero-centered. Hence, in practice, t

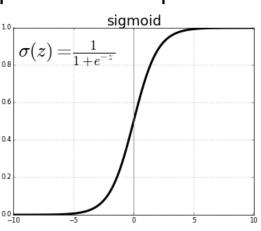


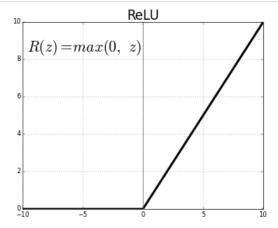
are zero-centered. Hence, in practice, tanh activation functions are preferred in hidden layers over sigmoid



#### The ReLU function

 Rectified Linear Unit (ReLU) become popular as it was found that it greatly accelerates the convergence of optimization process compared to Sigmoid or Tanh activation functions





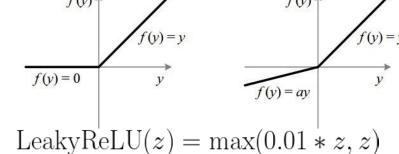
ReLU(z) = max(0, z)

- It is non-linear (although it's acts like a linear function for x > 0)
- ReLU is cheap to compute so model takes less time to run
- At a time only a few neurons are activated making the network sparse and usually efficient



#### ReLU is not perfect neither

- Because of the horizontal line in ReLu (for negative x), the gradient can go towards 0. Those neurons which go into that state will stop responding to variations in error/input (simply because gradient is 0, nothing changes). This is called dying ReLu problem. This problem can cause several neurons to just die and not respond making a substantial part of the network passive
- Leaky ReLU
  - We saw that for values less than 0, the gradient is 0 which results in "Dead Neurons" in those regions



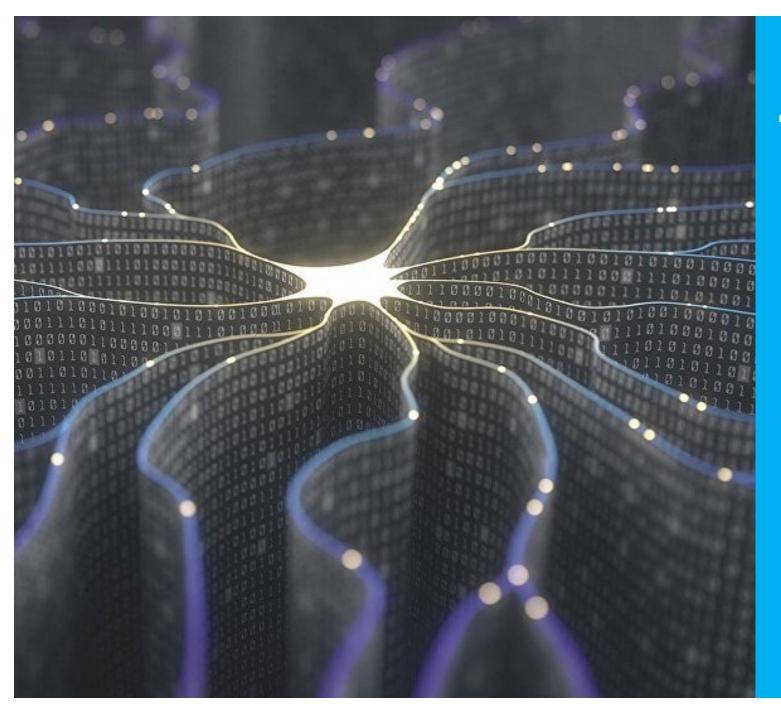
 Leaky ReLU addresses this problem: instead of defining values less than 0 as 0, we instead define negative values as a small linear combination of the input. The small value commonly used is 0.01.



## Synthesis

https://www.simplilearn.c om/tutorials/deeplearningtutorial/perceptron

Activation Fu	ınction	Equation	ř	Example	1D Graph
Linear		φ(z) = z		Adaline, linear regression	
Unit Step (Heaviside Function)	φ(z) =	0 0.5 1	z < 0 z = 0 z > 0	Perceptron variant	<del></del>
Sign (signum)	φ(z)=	{ -1 0 1	z < 0 z = 0 z > 0	Perceptron variant	上
Piece-wise Linear	$\phi(z) = \begin{cases} \\ \end{cases}$	0 z + ½ 1	$Z \le -\frac{1}{2}$ $-\frac{1}{2} \le Z \le \frac{1}{2}$ $Z \ge \frac{1}{2}$		<del></del>
Logistic (sigmoid)	φ(z	2)=	1 e <sup>-z</sup>	Logistic regression, Multilayer NN	
Hyperbolic Tangent (tanh)	φ(2	z)=	· e <sup>-z</sup>	Multilayer NN, RNNs	
ReLU	$\phi(z$	$z = \begin{cases} 0 \\ z \end{cases}$	z < 0 z > 0	Multilayer NN, CNNs	



# TOOLS & LIBS

**FOR** 

A



## The BigData & Al Landscape





#### Package: pandas

- Python Data Analysis Library
- pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language
- pandas provides fast, flexible, and expressive data structures designed to make working with "relational" or "labeled" data both easy and intuitive
- it aims to be the fundamental high-level building block for doing practical, real-world data analysis in Python.
- https://youtu.be/\_T8LGqJtuGc



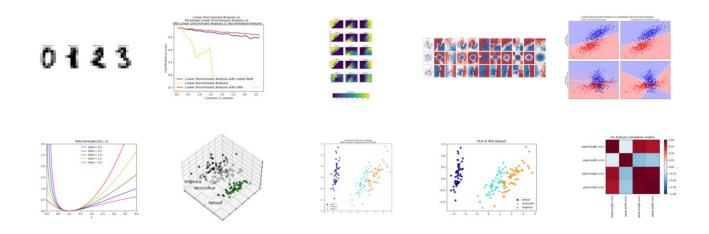
#### Package: Numpy

- <a href="https://numpy.org/">https://numpy.org/</a>
- NumPy is the fundamental package for scientific computing in Python
- It is a Python library that provides a multidimensional array object, various derived objects (such as masked arrays and matrices), and an assortment of routines for fast operations on arrays, including mathematical, logical, shape manipulation, sorting, selecting, I/O, discrete Fourier transforms, basic linear algebra, basic statistical operations, random simulation and much more.
- The Absolute Beginner's Guide: <a href="https://numpy.org/doc/stable/user/absolute\_beginners.h">https://numpy.org/doc/stable/user/absolute\_beginners.h</a> <a href="mailto:tml">tml</a>



## Package: Scikit-Learn

- Scikit-learn is an open source machine learning library that supports supervised and unsupervised learning
- It also provides various tools for model fitting, data preprocessing, model selection and evaluation, and many other utilities
- https://scikit-learn.org/stable/auto\_examples/index.html





#### Package: XGBoost

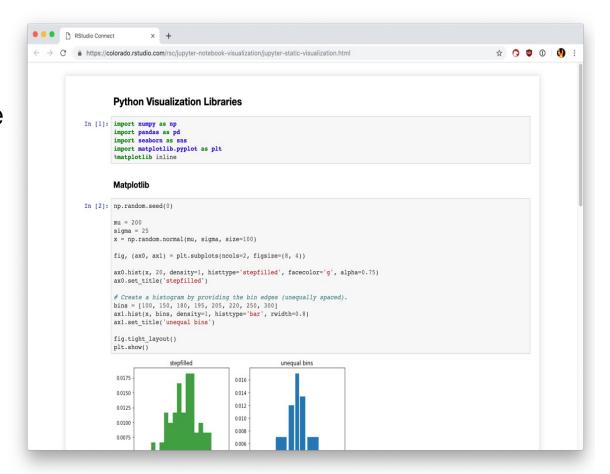
- eXtreme Gradient Boosting is an optimized open source implementation of the gradient boosting trees algorithm
- Gradient Boosting is a **supervised learning algorithm** whose principle is to combine the results of a set of data and weaker models in order to provide a **better prediction** (regression)
- XGBoost includes a large number of hyperparameters which can be modified and tuned for improvement
- XGBoost is not part of Scikit-Learn but works perfectly with it
- XGBoost behaves remarkably in machine learning competitions!
- Source: "XGBoost: The super star of algorithms in ML competition". See examples from <a href="http://aishelf.org/xgboost/">http://aishelf.org/xgboost/</a>



## Jupyter Notebook

Web application that allows to create and share documents that contain live code, equations, visualizations and narrative text

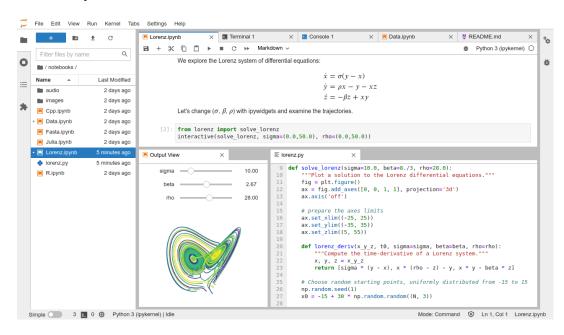
- Data cleaning and transformation
- Numerical simulation
- Statistical modeling
- Data visualization
- Machine learning, and more





#### JupyterLab

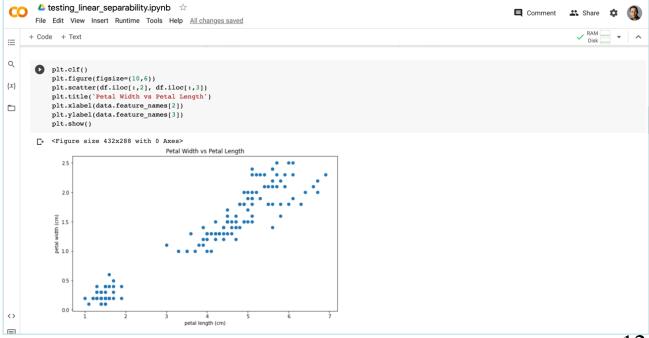
- Jupyter Notebook only offers a very simple interface using which users can open notebooks, terminals, and text files
- Jupyter Lab offers a very interactive interface that includes notebooks, consoles, terminals, CSV editors, markdown editors, interactive maps, and more





#### Colab

- Colab, or "Colaboratory", allows you to write and execute Python in your browser, with
  - Zero configuration required
  - Access to GPUs free of charge
  - Easy sharing





#### Binder

- Colab is an interactive editor environment (allowing you to edit and run your Jupyter notebooks)
- Binder is for running Jupyter notebooks as applications



## Package: TensorFlow

In mathematics, a tensor is an algebraic object that describes a multilinear relationship between sets of algebraic objects related to a vector space. Tensors may map between different objects such as vectors, scalars, and even other tensors.

W Wikipedia
https://en.wikipedia.org > wiki > Tensor :
Tensor - Wikipedia

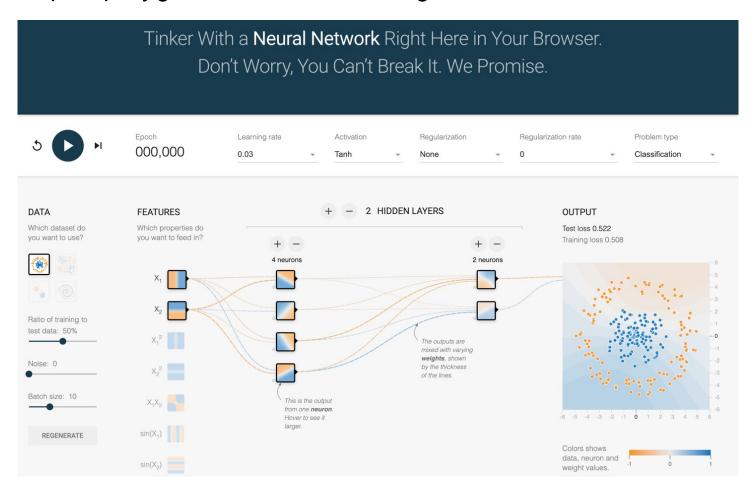
- TensorFlow is an end-to-end open source platform for machine learning and deep learning. It is developed by Google.
- It has a comprehensive, flexible ecosystem of tools, libraries and community resources that lets researchers push the state-ofthe-art in ML and developers easily build and deploy ML powered applications
- TensorFlow is more of a low-level library whereas Scikit-Learn comes with off-the-shelf algorithms, e.g., algorithms for classification such as SVMs, Random Forests, Logistic Regression, ..."
  [https://stackoverflow.com/questions/61233004]
- https://www.tensorflow.org/
- https://www.tensorflow.org/overview





## Want to try DeepLearning?

https://playground.tensorflow.org/





#### Package: Keras

- <u>https://keras.io/</u> Deep learning for humans
- Keras is an effective high-level neural network API written in Python
- This open-source neural network library is designed to provide fast experimentation with deep neural networks, and it can run on top of TensorFlow for instance
- It also has extensive documentation and developer guides
- Keras was adopted and integrated into TensorFlow in mid-2017.
   Users can access it via the tf.keras module. However, the Keras library can still operate separately and independently.



#### Package: PyTorch

- https://pytorch.org/
- PyTorch is a machine learning framework based on the Torch library used for applications such as computer vision and natural language processing originally developed by Meta AI and now part of the Linux Foundation umbrella [Wikipedia]
- PyTorch is used for many deep learning projects today, and its popularity is increasing among AI researchers