

# Big data science

## Day 3

F. Legger - INFN Torino

<https://github.com/leggerf/MLCourse-INFN-2021>



# Yesterday

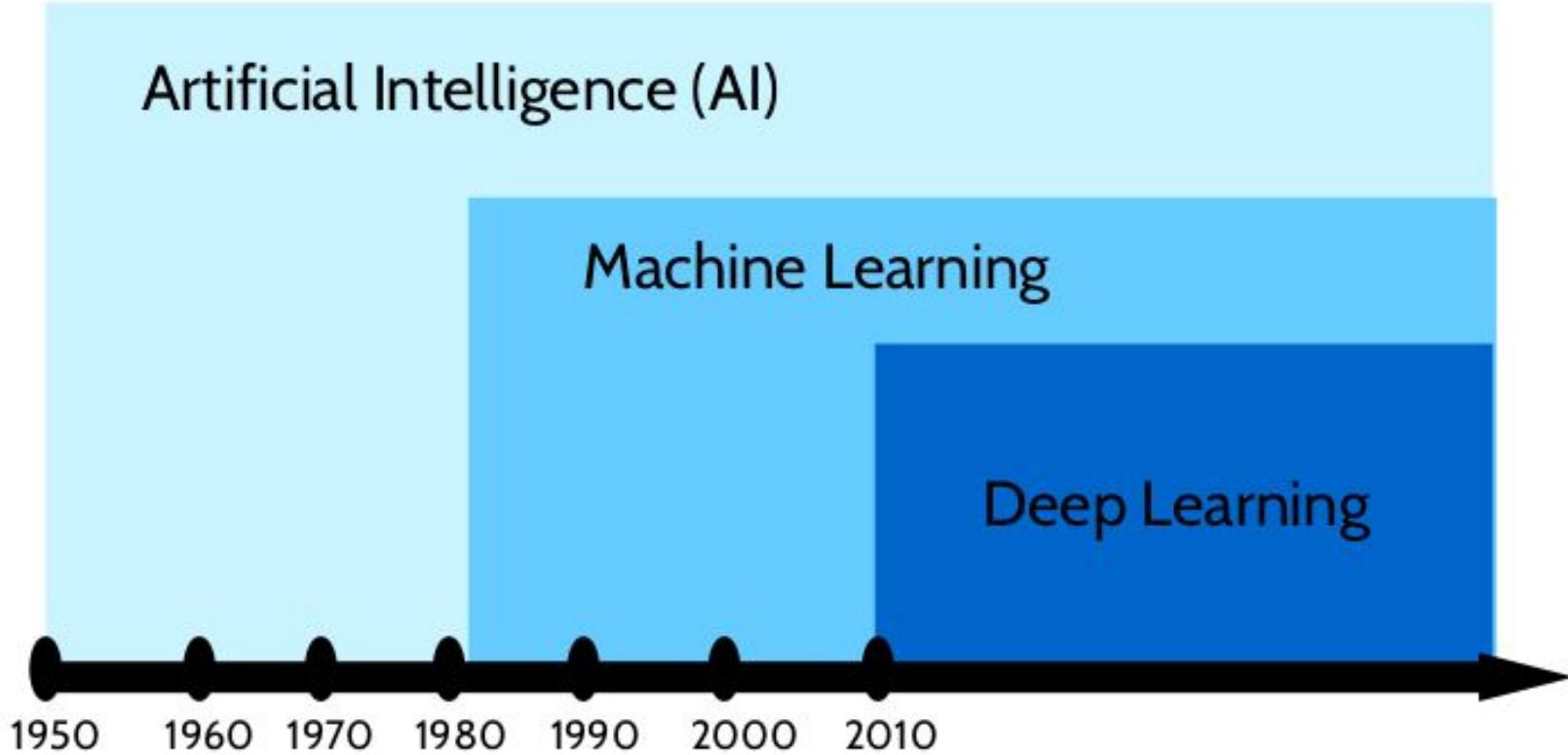
- Big data
  - Analytics
  - Machine learning

# Today

- Deep learning
  - Parallelisation
  - Heterogeneous architectures
  - Future directions



*Deep Learning is a subfield of ML concerned with algorithms inspired by the structure and function of the brain called artificial neural networks* [Jason Brownlee]

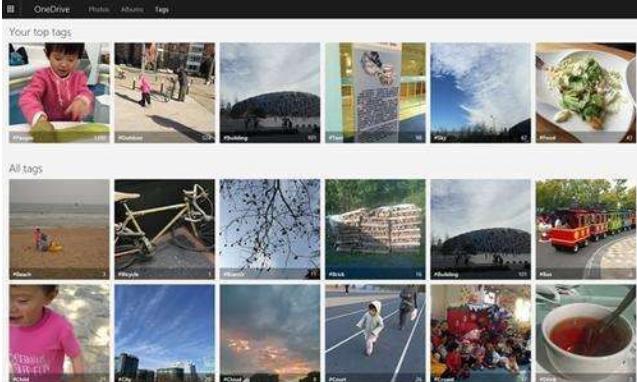


# Machine translation

Real-time translation into Mandarin Chinese (2012)



# Visual recognition



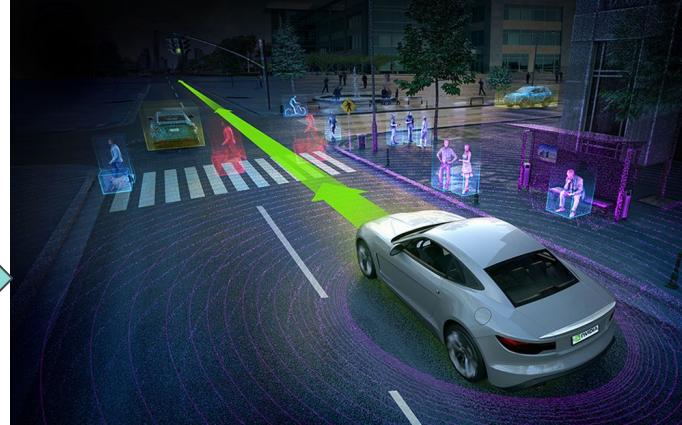
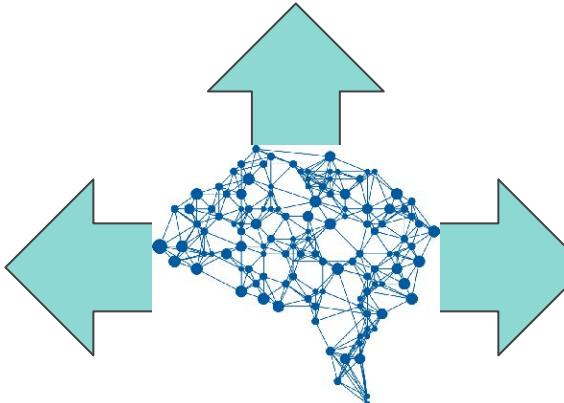
**Strategy games**  
DeepMind beats Go  
world champion (2017)



# Creativity

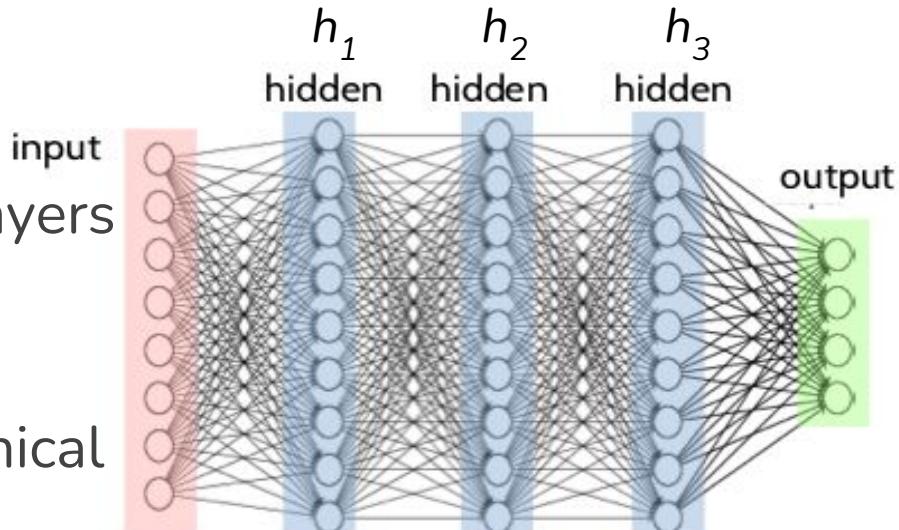


# Self driving cars



# Deep Learning

- Neural network with several layers
  - Deep vs shallow
- A family of parametric models which learn non-linear hierarchical representations:

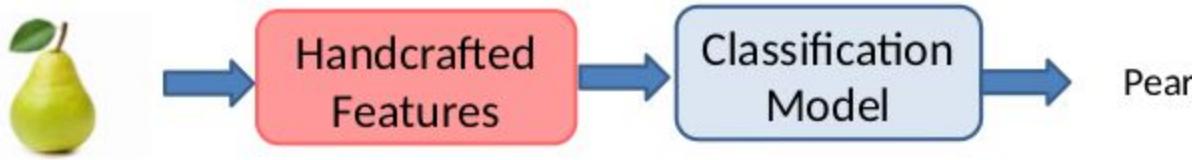


$$a_L(\mathbf{x}; \Theta) = h_L(h_{L-1}(\dots(h_1(\mathbf{x}, \theta_1), \theta_{L-1}), \theta_L)$$

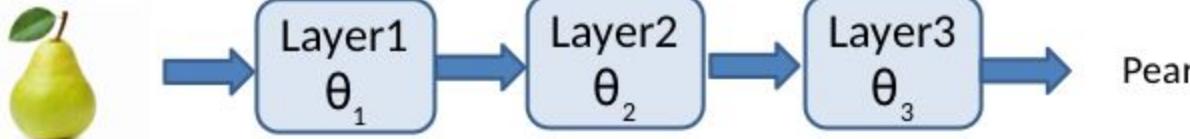
input      parameters of the network      non-linear activation function      parameters of layer  $L$

# Learning hierarchical representations

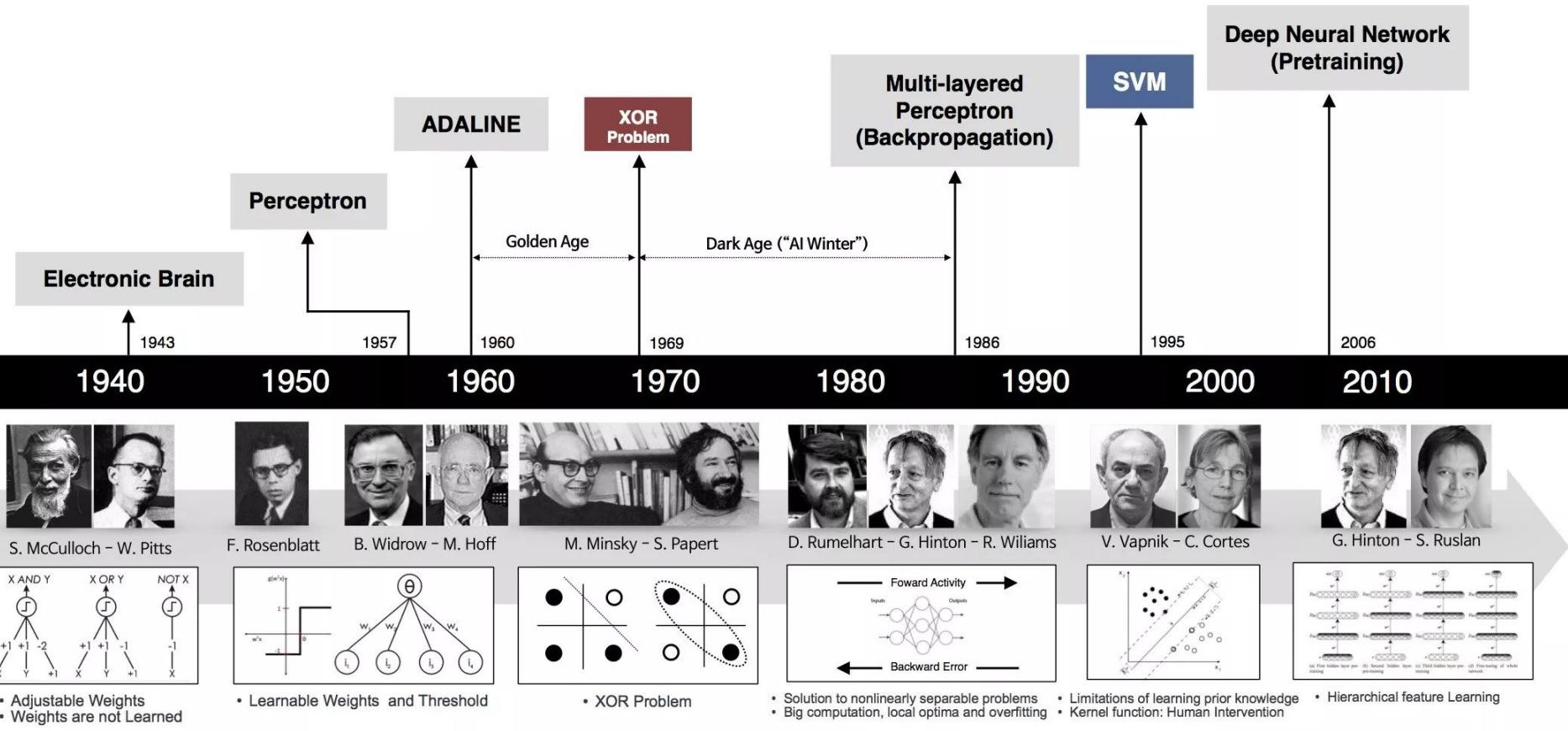
- Traditional framework



- Deep Learning

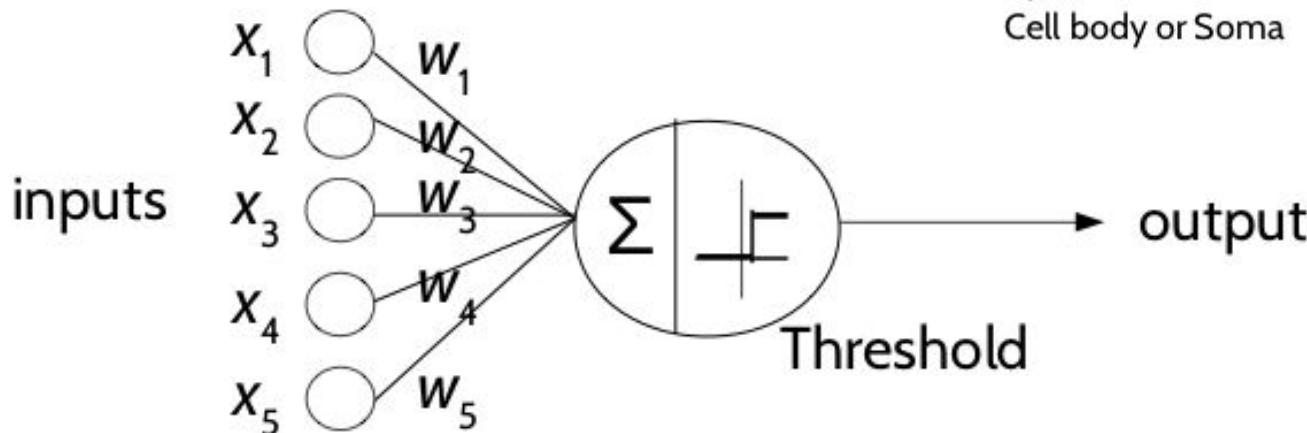
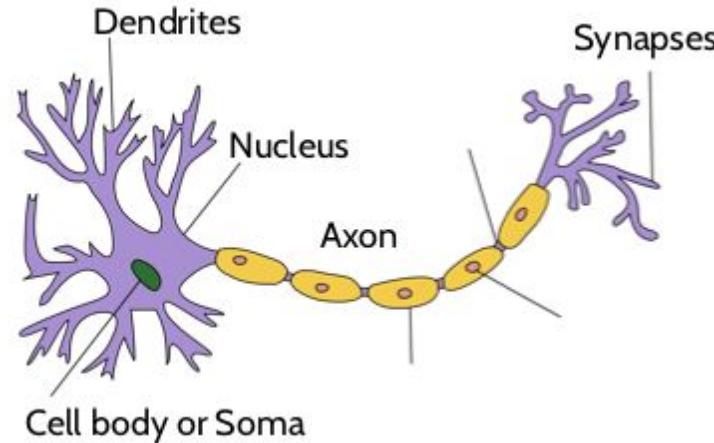


# Brief history of neural networks



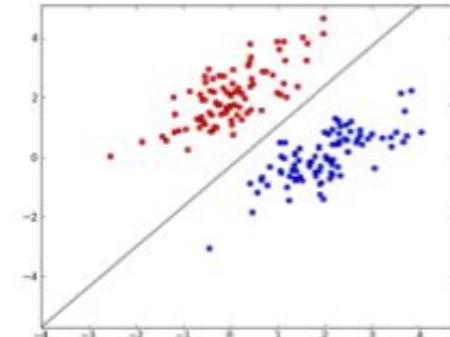
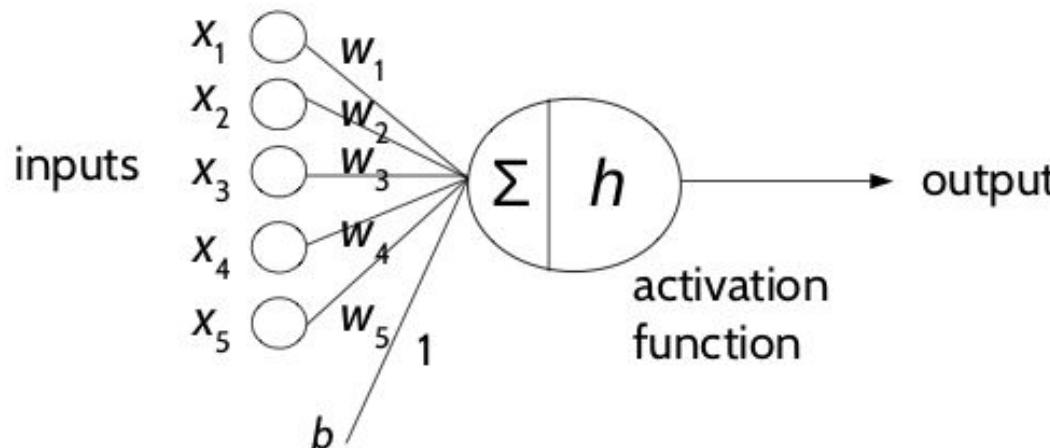
# 1943 – McCulloch & Pitts Model

- Early model of artificial neuron
- Generates a binary output
- The weights values are fixed



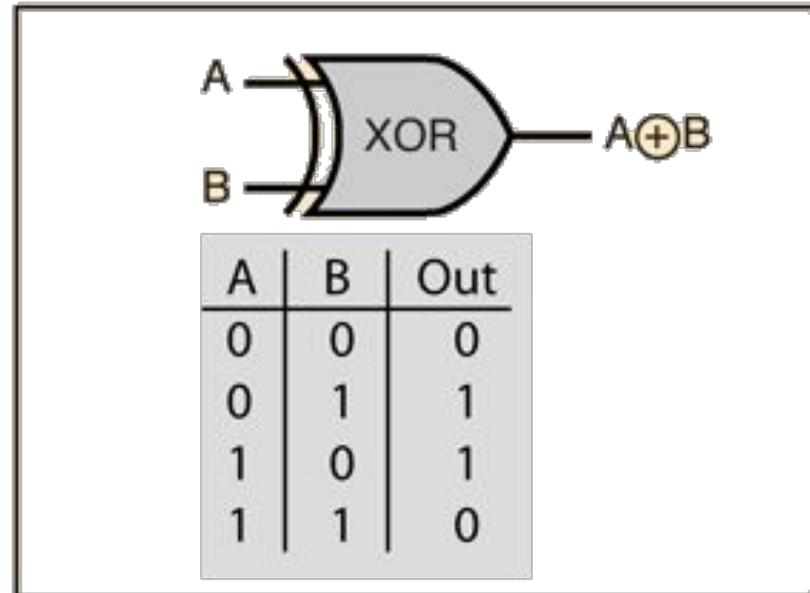
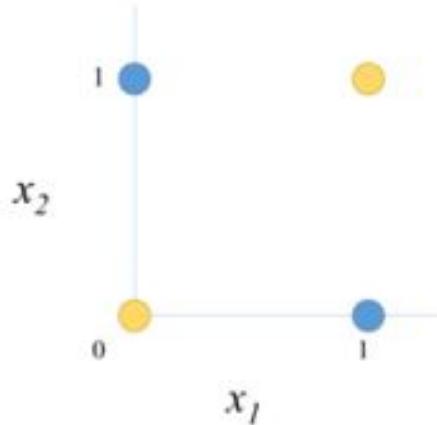
# 1958 – Perceptron by Rosenblatt

- Perceptron as a machine for linear classification
- Main idea: Learn the weights and consider bias.
  - One weight per input
  - Multiply weights with respective inputs and add bias
  - If result larger than **threshold** return 1, otherwise 0



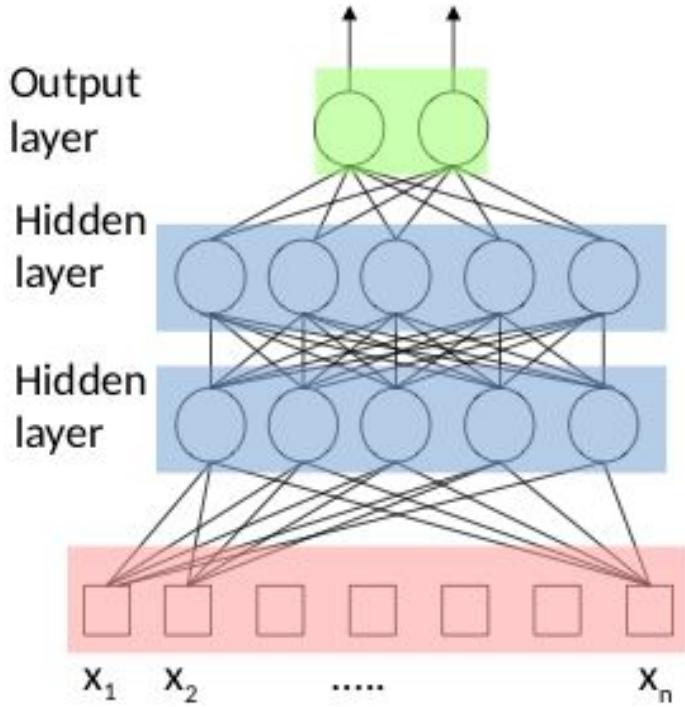
# First NN winter

- 1970- Minsky. The XOR cannot be solved by perceptrons.
- Neural models cannot be applied to complex tasks.



# Multi-layer Feed Forward Neural Network

- 1980s. Multi-layer Perceptrons (MLP) can solve XOR.
- ML Feed Forward Neural Networks:
  - Densely connect artificial neurons to realize compositions of non-linear functions
  - The information is propagated from the inputs to the outputs
  - The input data are usually  $n$ -dimensional feature vectors
  - Tasks: Classification, Regression



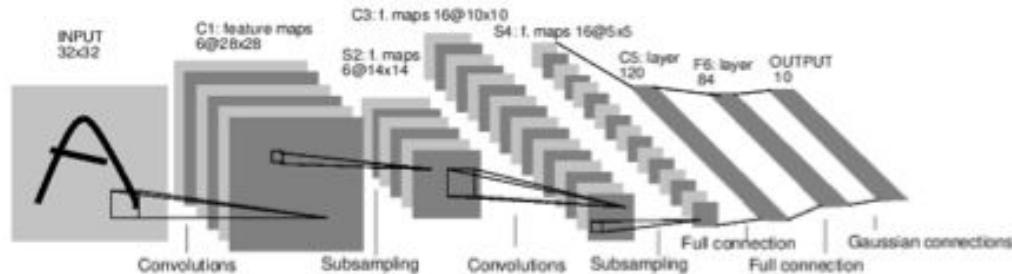
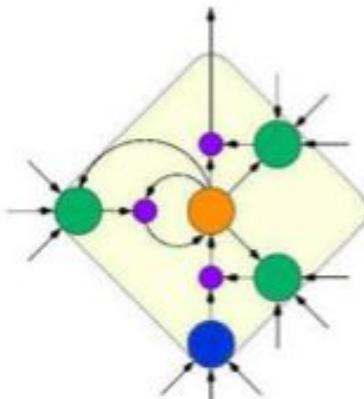
# How to train it?

- Rosenblatt algorithm\* not applicable, as it expects to know the desired target
  - For hidden layers we cannot know the desired target
- Learning MLP for complicated functions can be solved with **Back propagation (1980)**
  - efficient algorithm for complex NN which processes large training sets

\* Remember? Rosenblatt developed a method to train a single neuron

# 1990s - CNN and LSTM

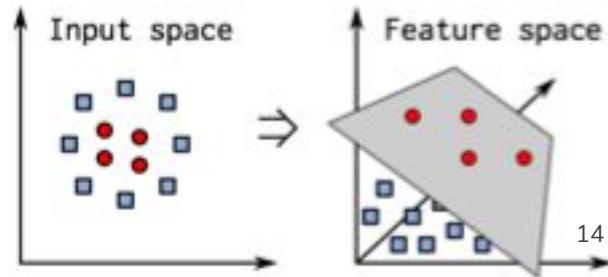
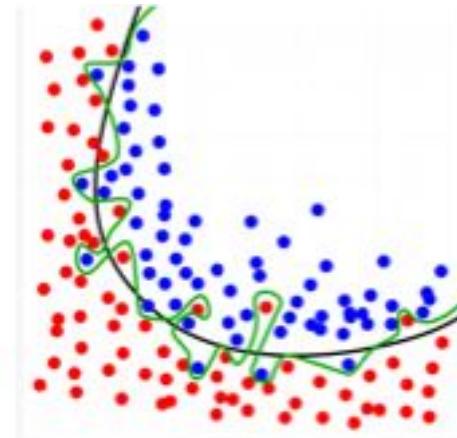
- Important advances in the field:
  - Backpropagation
  - Recurrent Long-Short Term Memory Networks (Schmidhuber, 1997)
  - Convolutional Neural Networks - LeNet: OCR solved before 2000s (LeCun, 1998).



OCR: Optical character recognition

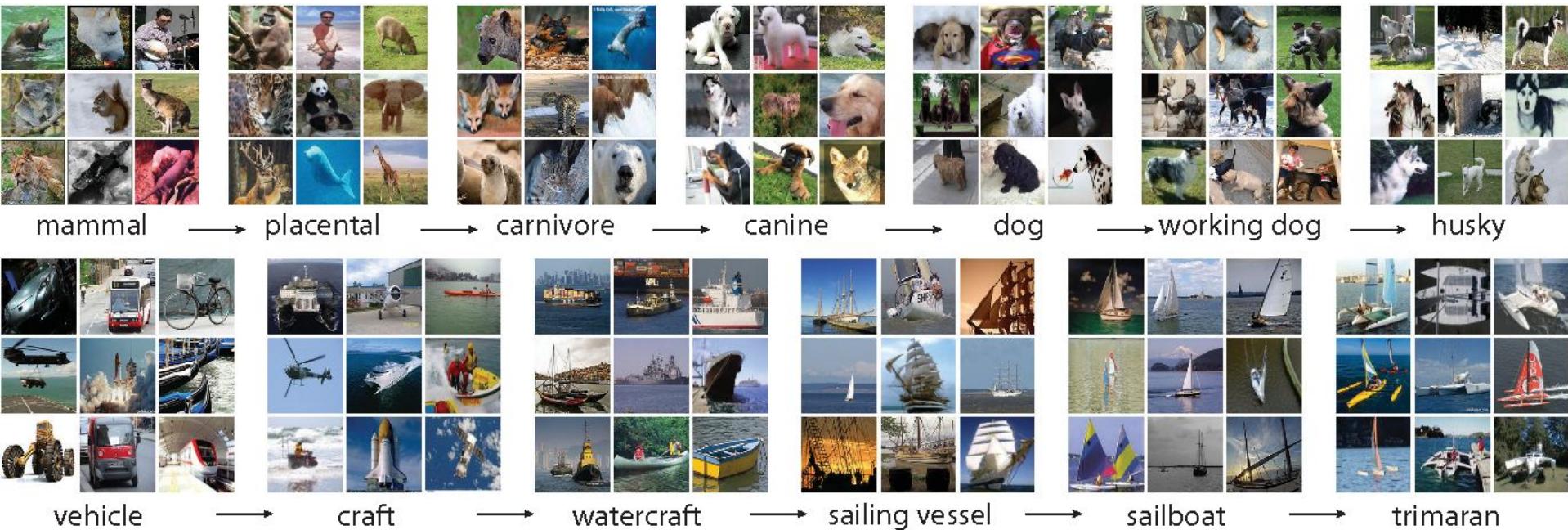
# Second NN Winter

- NN cannot exploit many layers
  - Overfitting
  - Vanishing gradient (with NN training you need to multiply several small numbers → they become smaller and smaller)
- Lack of processing power (no GPUs)
- Lack of data (no large annotated datasets)
- Kernel Machines (e.g. SVMs) suddenly become very popular°



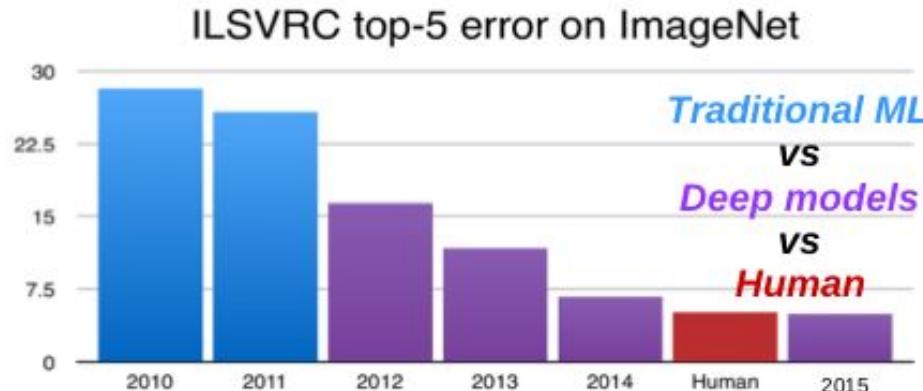
# ImageNet

A Large-Scale Hierarchical Image Database (2009)

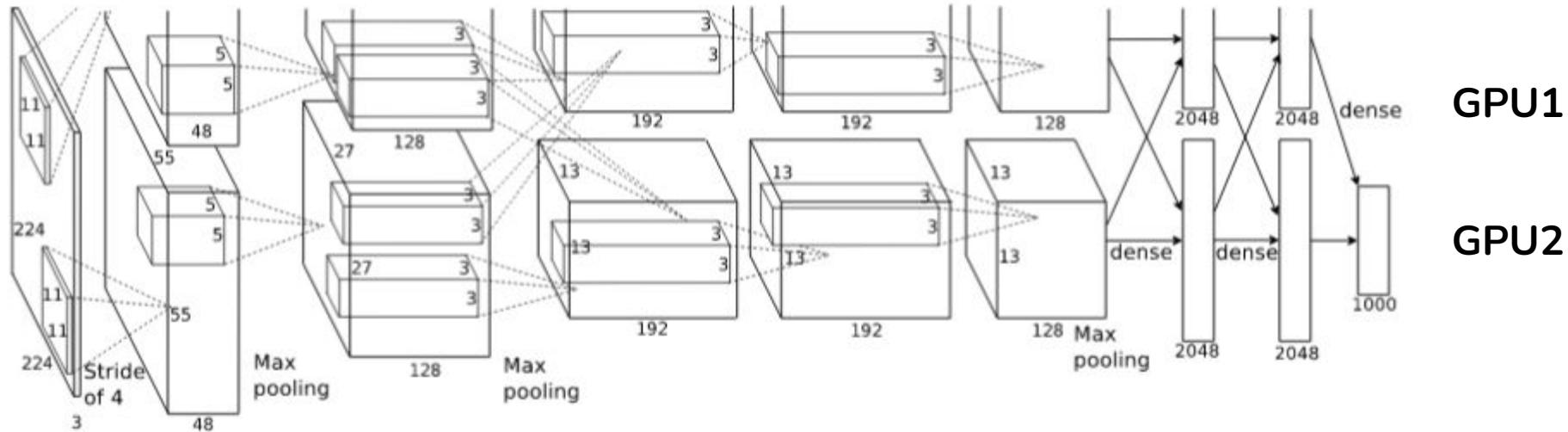


# 2012 - AlexNet

- Hinton's group implemented a CNN similar to LeNet [LeCun1998] but...
  - Trained on ImageNet (1.4M images, 1K categories)
  - With 2 GPUs
  - Other technical improvements (ReLU, dropout, data augmentation)



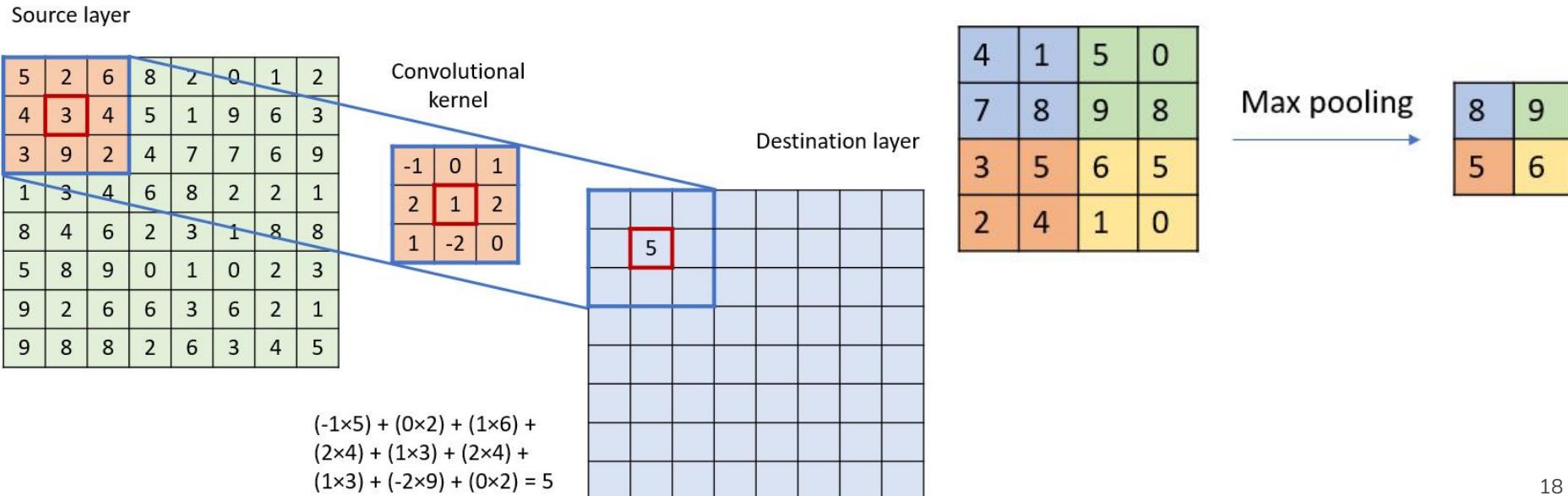
# AlexNet



- 60M parameters
- Limited information exchange between GPUs

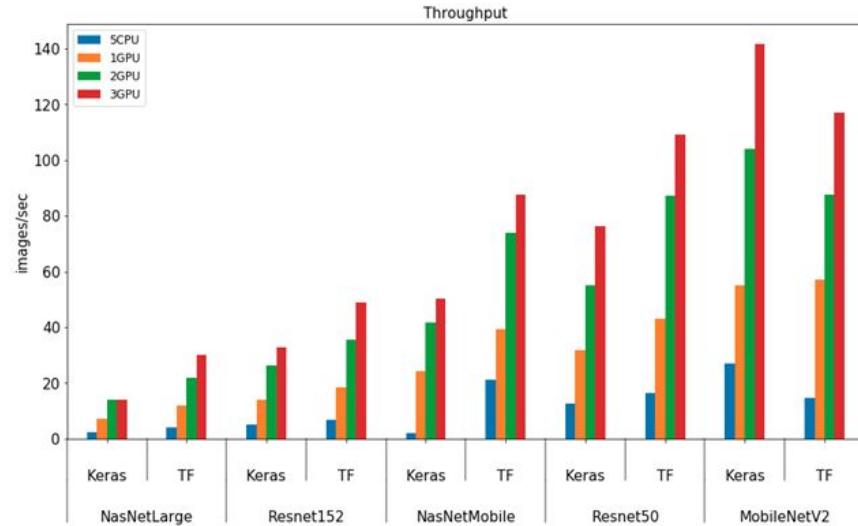
# Convolutional Neural Networks (CNN)

- **Convolutional** layer: two functions produce a third that describes how the shape of one is changed by the other
- **pooling** layer: reduce dimensionality



# Why Deep Learning now?

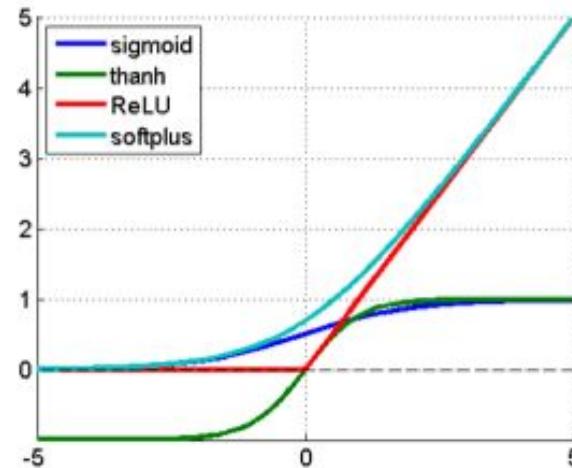
- Three main factors:
    - Better hardware
    - Big data
  - Technical advances:
    - Layer-wise pretraining
    - Optimization (e.g. Adam, batch normalization)
    - Regularization (e.g. dropout)
- ....



# Rectified Linear Units (2010)

$$f(x) = \max(0, x)$$

- More efficient gradient propagation:  
(derivative is 0 or constant)
- More efficient computation:  
(only comparison, addition and multiplication).
- Sparse activation: e.g. in a randomly initialized networks, only  
about 50% of hidden units are activated (having a non-zero output)



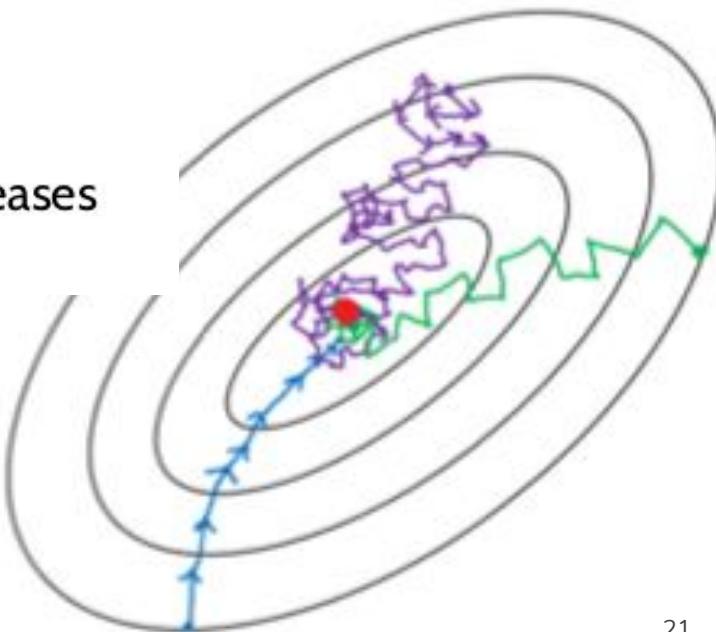
# Stochastic gradient descent (SGD)

- Use mini-batch **samples** in the dataset for gradient estimate.

$$\Theta^{t+1} = \Theta^t - \frac{\eta_t}{|\mathcal{B}|} \sum_{i \in \mathcal{B}} \nabla_{\Theta} \mathcal{L}_i$$

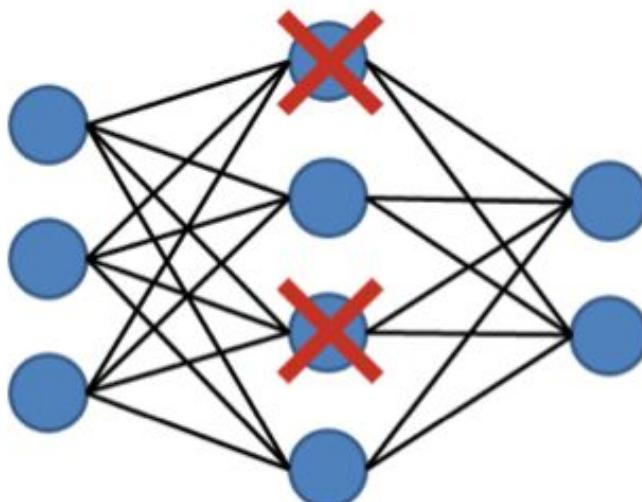
- Sometimes helps to escape from local minima
- Noisy gradients act as regularization
- Variance of gradients increases when batch size decreases
- Not clear how many sample per batch

- Batch gradient descent
- Mini-batch gradient Descent
- Stochastic gradient descent



# Regularization - Dropout

- For each instance drop a node (hidden or input) and its connections with probability  $p$  and train
- Final net just has all averaged weights (actually scaled by  $1-p$ )
- As if ensembling  $2^n$  different network substructures



# Data augmentation

- Techniques to significantly increase the diversity of data available for training models, without actually collecting new data
- Data augmentation techniques such as cropping, padding, and horizontal flipping are commonly used to train large neural networks



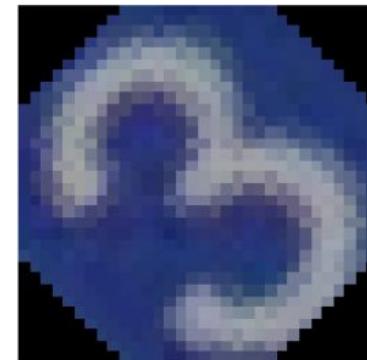
Original



Horizontal Flip



Pad & Crop



Rotate

# Training a neural network

Name	Weight (lb)	Height (in)	Gender
Alice	133	65	F
Bob	160	72	M
Charlie	152	70	M
Diana	120	60	F

- Predict gender from weight and height

# Feature engineering

- Symmetrize numeric values
- Category -> numbers

Name	Weight (lb)	Height (in)	Gender
Alice	133	65	F
Bob	160	72	M
Charlie	152	70	M
Diana	120	60	F

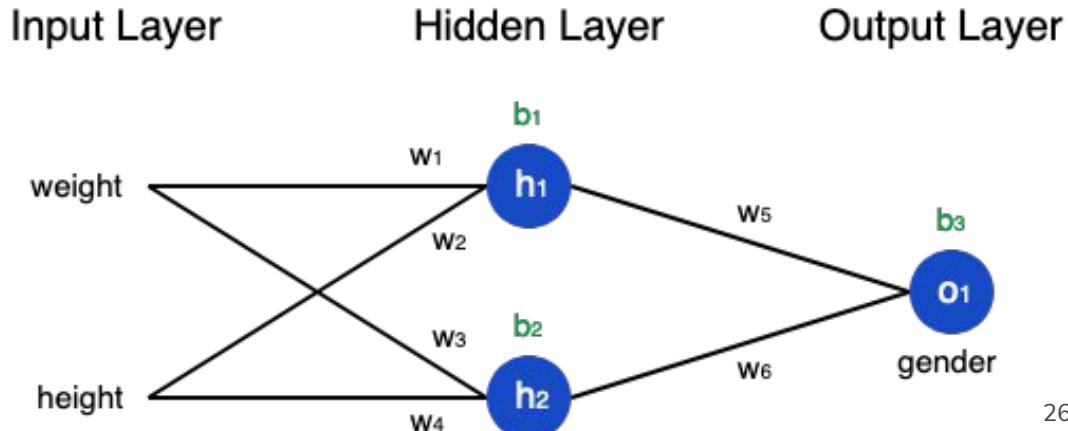


Name	Weight (minus 135)	Height (minus 66)	Gender
Alice	-2	-1	1
Bob	25	6	0
Charlie	17	4	0
Diana	-15	-6	1

# Ingredients

- $n$  : 4, number of samples (Alice, Bob, Charlie, Diana)
- $y$  : variable being predicted (Gender)
- $y_{true}$  : true value of  $y$ ,  $y_{pred}$  : predicted value of  $y = o$
- Loss function  $L$ : MSE
- Activation function  $f$
- Outputs of the hidden layer  $h$
- Unknown parameters: weights  $w$  and biases  $b$

$$\text{MSE} = \frac{1}{n} \sum_{i=1}^n (y_{true} - y_{pred})^2$$



# Back propagation

- Training the network == minimize the loss
  - Find weights  $w$  and biases  $b$
  - $L(w_1, w_2, w_3, w_4, w_5, w_6, b_1, b_2, b_3)$
- Minimization taking partial derivatives (back propagation)

$$\frac{\partial L}{\partial w_1} = \frac{\partial L}{\partial y_{pred}} * \frac{\partial y_{pred}}{\partial h_1} * \frac{\partial h_1}{\partial w_1}$$

For very simple case: with  
only Alice in the dataset, n=1

$$L = (1 - y_{pred})^2$$

$$\frac{\partial L}{\partial y_{pred}} = \frac{\partial(1 - y_{pred})^2}{\partial y_{pred}}$$

$$y_{pred} = o_1 = f(w_5 h_1 + w_6 h_2 + b_3)$$

$$\frac{\partial y_{pred}}{\partial h_1} = w_5 * f'(w_5 h_1 + w_6 h_2 + b_3)$$

$$h_1 = f(w_1 x_1 + w_2 x_2 + b_1)$$

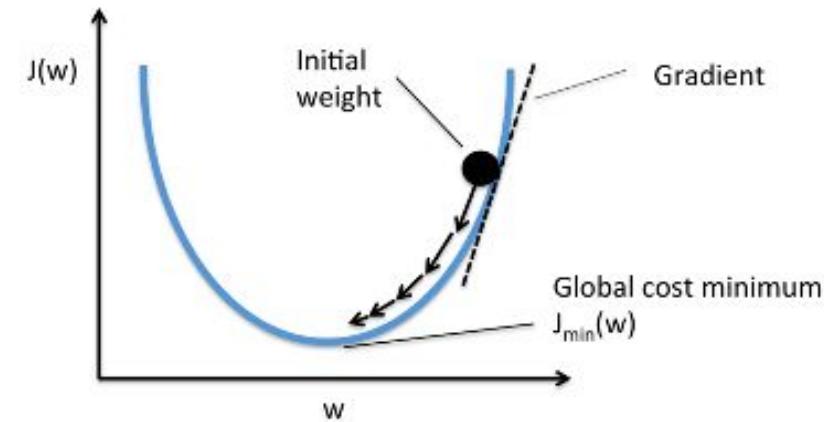
$$\frac{\partial h_1}{\partial w_1} = x_1 * f'(w_1 x_1 + w_2 x_2 + b_1)$$

# Stochastic Gradient Descent (SGD)

- optimization algorithm to find weights and biases to minimize loss
- update equation:

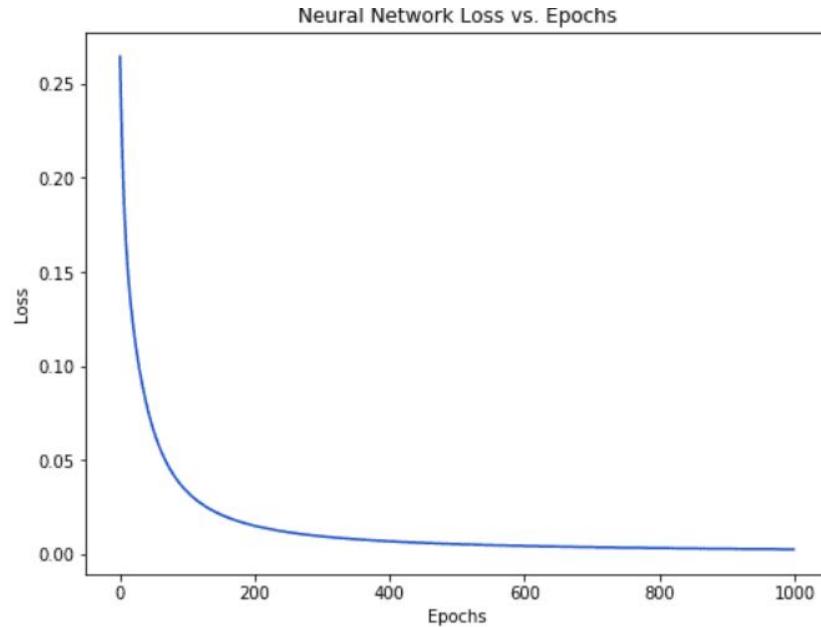
$$w_1 \leftarrow w_1 - \eta \frac{\partial L}{\partial w_1}$$

- $\eta$  is a constant called the **learning rate**
- If  $\frac{\partial L}{\partial w_1}$  is positive,  $w_1$  will decrease, which makes  $L$  decrease.
- If  $\frac{\partial L}{\partial w_1}$  is negative,  $w_1$  will increase, which makes  $L$  decrease.
- **Stochastic** -> the parameters are updated using only a single training instance (usually randomly selected) in each iteration



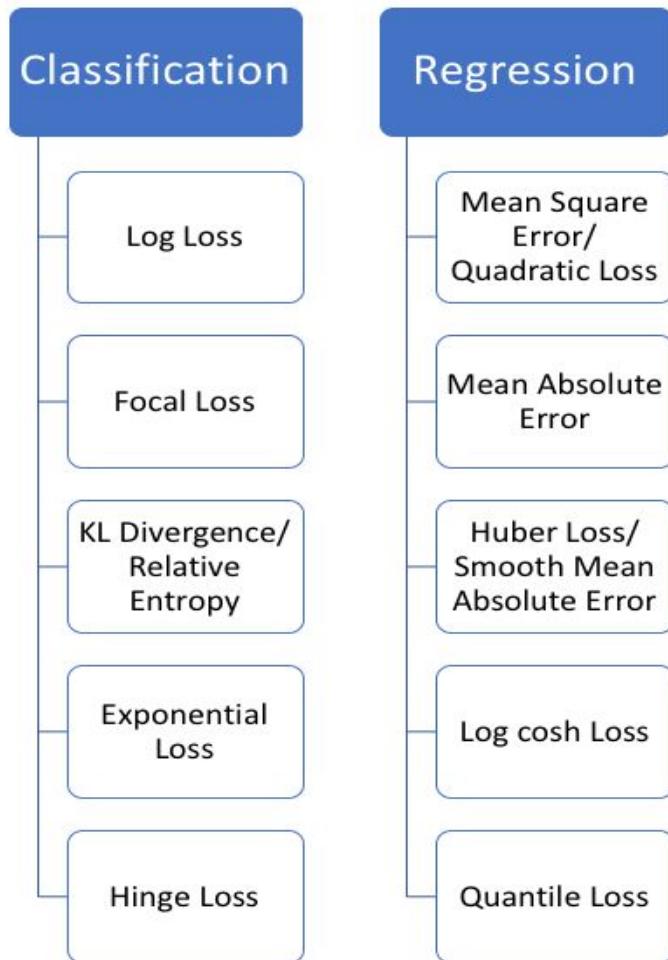
# Training the network

- Choose one sample from our dataset
  - This is what makes it stochastic gradient descent - only operate on one sample at a time
- Calculate all the partial derivatives of loss with respect to weights or biases
- Use the update equation to update each weight and bias
- Iterate



# LOSS functions

- <https://heartbeat.fritz.ai/5-regression-loss-functions-all-machine-learners-should-know-4fb140e9d4b0>
- [https://www.wikiwand.com/en/Loss\\_functions\\_for\\_classification](https://www.wikiwand.com/en/Loss_functions_for_classification)



# Regularization

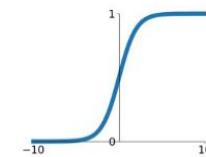
- One of the major aspects of training the model is overfitting -> the ML model captures the noise in your training dataset
- The **regularization** term is an addition to the loss function which helps generalize the model
  - **L1** or Lasso regularization adds a penalty which is the sum of the absolute values of the weights
    - L1+MSE
$$\text{Min} \left( \sum_{i=1}^n (y_i - w_i x_i)^2 + p \sum_{i=1}^n |w_i| \right)$$
  - **L2** or Ridge regularization adds a penalty which is the sum of the squared values of weights
    - L2+MSE
$$\text{Min} \left( \sum_{i=1}^n (y_i - w_i x_i)^2 + p \sum_{i=1}^n (w_i)^2 \right)$$
- **Dropout** in NN context: hidden nodes are dropped randomly
- **Early Stopping** is a time regularization technique which stops training based on given criteria

# Activation functions

- Classification: sigmoid functions
  - sigmoids and tanh functions are sometimes avoided due to the vanishing gradient problem
- ReLU function is a general activation function
- dead neurons in our networks -> the leaky ReLU
- ReLU function should only be used in the hidden layers
- As a rule of thumb, start with ReLU

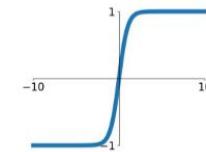
**Sigmoid**

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



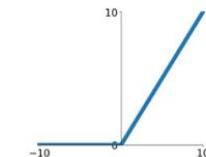
**tanh**

$$\tanh(x)$$



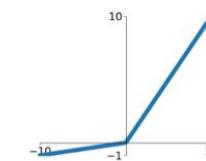
**ReLU**

$$\max(0, x)$$



**Leaky ReLU**

$$\max(0.1x, x)$$

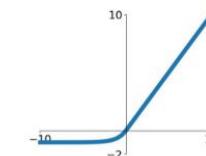


**Maxout**

$$\max(w_1^T x + b_1, w_2^T x + b_2)$$

**ELU**

$$\begin{cases} x & x \geq 0 \\ \alpha(e^x - 1) & x < 0 \end{cases}$$



# Neural Networks

©2019 Fjodor van Veen &amp; Stefan Leijnen asimovinstitute.org

- Input Cell
- Backfed Input Cell
- △ Noisy Input Cell
- Hidden Cell
- Probabilistic Hidden Cell
- △ Spiking Hidden Cell
- Capsule Cell
- Output Cell
- Match Input Output Cell
- Recurrent Cell
- Memory Cell
- △ Gated Memory Cell
- Kernel
- Convolution or Pool

Perceptron (P)



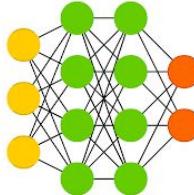
Feed Forward (FF)



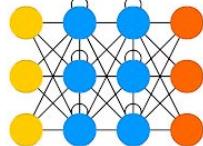
Radial Basis Network (RBF)



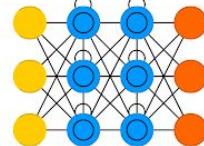
Deep Feed Forward (DFF)



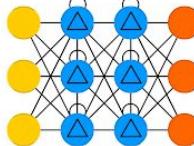
Recurrent Neural Network (RNN)



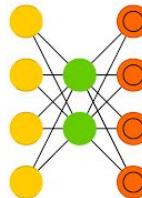
Long / Short Term Memory (LSTM)



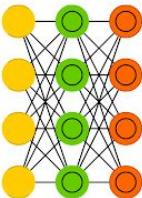
Gated Recurrent Unit (GRU)



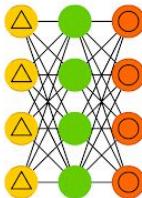
Auto Encoder (AE)



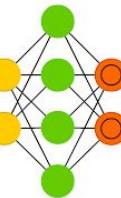
Variational AE (VAE)



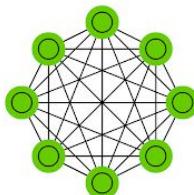
Denoising AE (DAE)



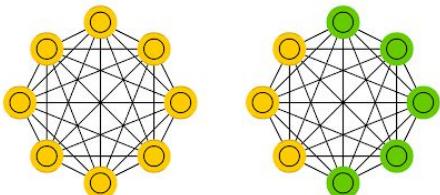
Sparse AE (SAE)



Markov Chain (MC)



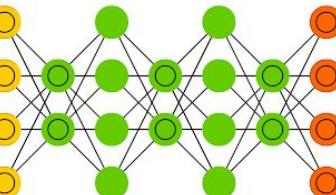
Hopfield Network (HN) Boltzmann Machine (BM)



Restricted BM (RBM)

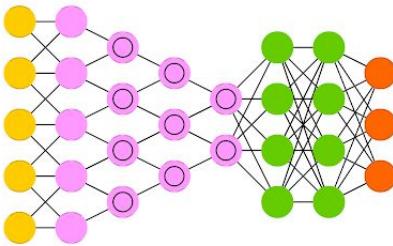


Deep Belief Network (DBN)

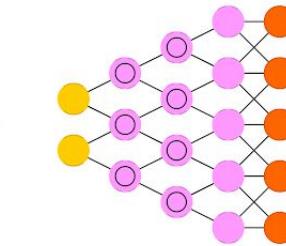


- Input Cell
- Backfed Input Cell
- △ Noisy Input Cell
- Hidden Cell
- Probabilistic Hidden Cell
- △ Spiking Hidden Cell
- Capsule Cell
- Output Cell
- Match Input Output Cell
- Recurrent Cell
- Memory Cell
- △ Gated Memory Cell
- Kernel
- Convolution or Pool

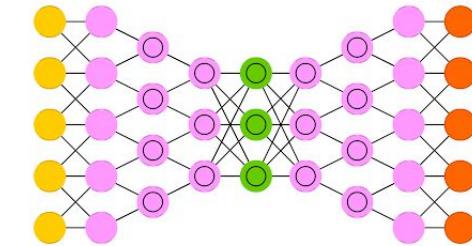
Deep Convolutional Network (DCN)



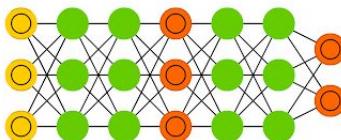
Deconvolutional Network (DN)



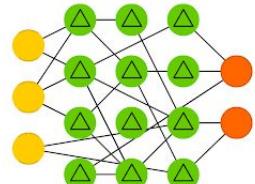
Deep Convolutional Inverse Graphics Network (DCIGN)



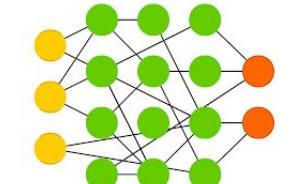
Generative Adversarial Network (GAN)



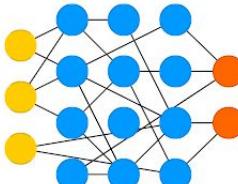
Liquid State Machine (LSM)



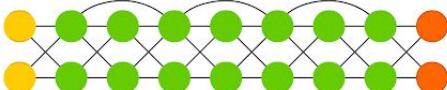
Extreme Learning Machine (ELM)



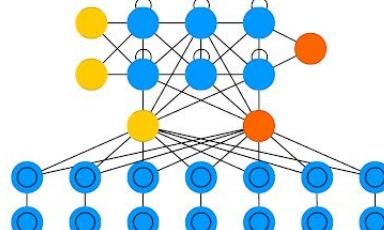
Echo State Network (ESN)



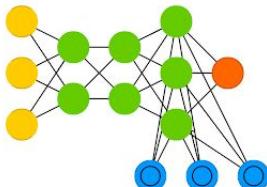
Deep Residual Network (DRN)



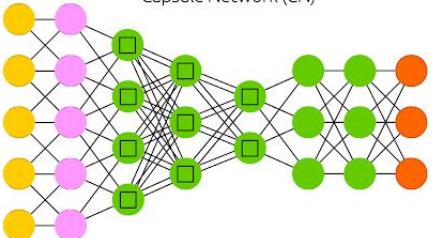
Differentiable Neural Computer (DNC)



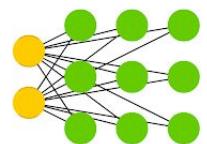
Neural Turing Machine (NTM)



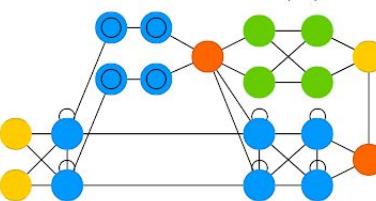
Capsule Network (CN)



Kohonen Network (KN)



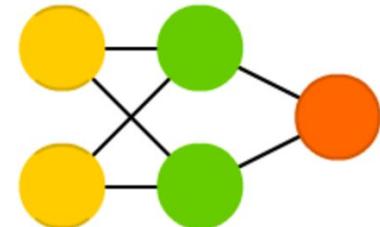
Attention Network (AN)



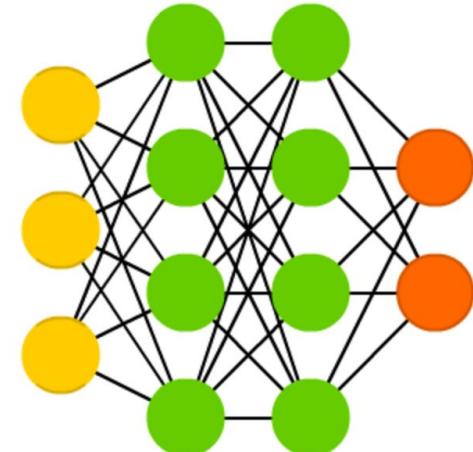
# Feed Forward

- Supervised, simplest form of NN
- The data passes through input nodes and exits on the output nodes
- Easy to implement and combine with other type of ML algorithms
- Typically trained with backpropagation
- Used in many ML tasks, speech, image recognition, classification, computer vision
- input/outputs are vectors of fixed length
- **DFF** is a FF NN with more than one hidden layer

Feed Forward (FF)

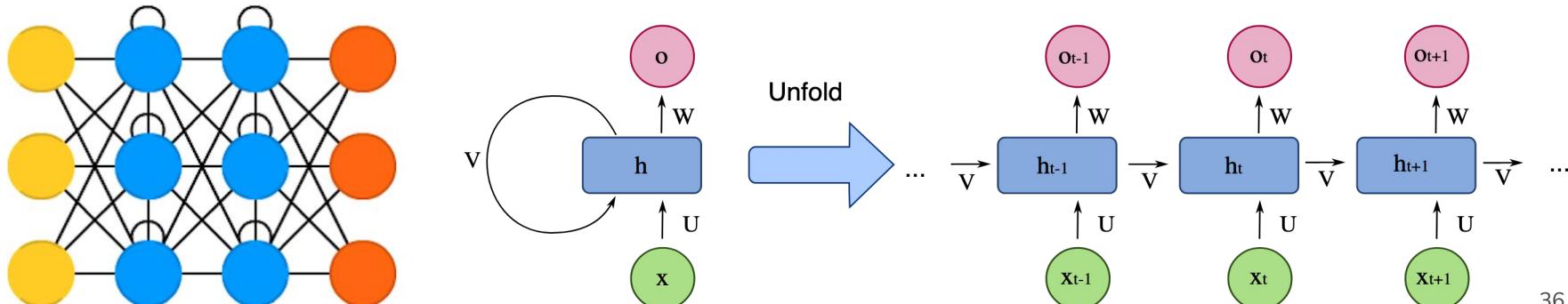


Deep Feed Forward (DFF)



# Recurrent Neural Network (RNN)

- FFNN with **Recurrent Cells**: hidden cell that receives its own output with fixed delay
- RNNs permit to operate on **sequences of vectors** (in the input, the output, or both)
- RNNs, once unfolded in time, can be seen as very deep FF networks in which all the layers share the same weights



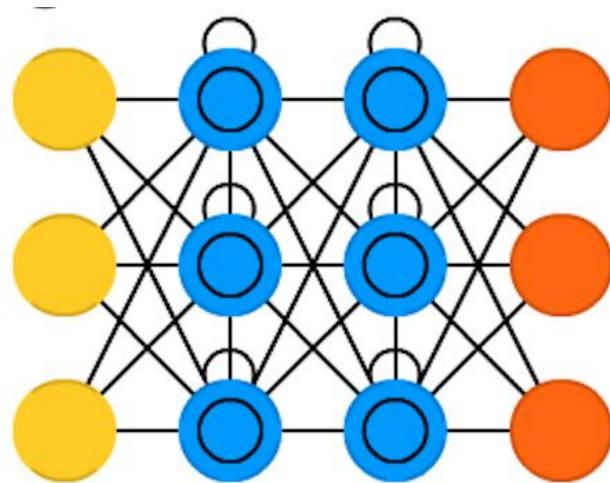
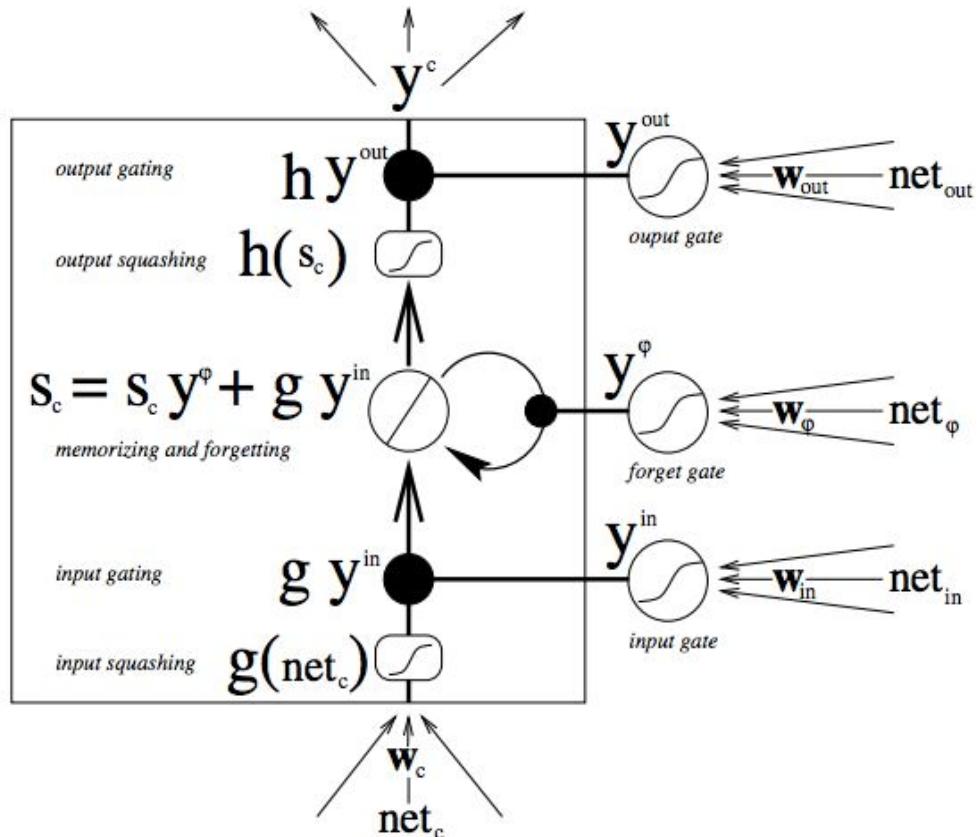
# Recurrent Neural Network (RNN)

- The parameters to be learned are shared by all time steps in the network
- The gradient at each output depends also on the calculations of the previous time steps
- context is important, decision from past iterations can influence current state
- a word can be analyzed only in context of previous words or sentences

# Long/Short Term Memory (LSTM)

- RNNs not really capable of learning long term dependencies
  - Due to vanishing gradient with increasing time steps
  - -> add cells with memory: “keep in mind” previous info, e.g. something that happened many frames ago
- A common LSTM unit is made of a **cell**, an **input**, an **output** and a **forget** gate
- The cell remembers values over arbitrary time intervals and the three gates regulate the flow of information into and out of the cell

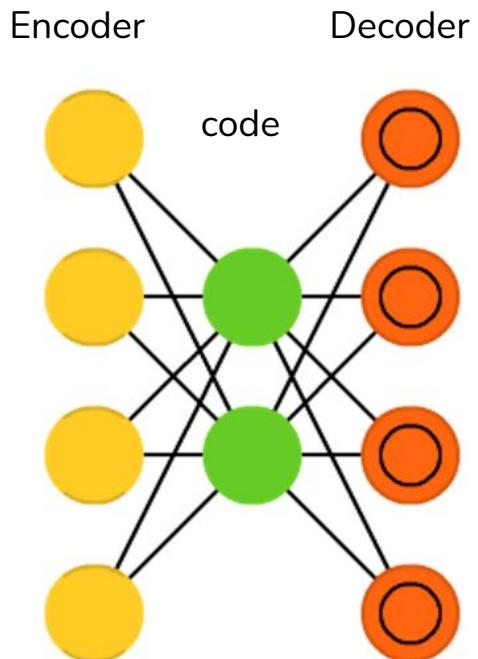
# Long/Short Term Memory (LSTM)



# Auto Encoders

- **Unsupervised** learning
  - find smaller representation of given input and search for common patterns
- Compress (encode) information automatically.
- An **encoder** is a deterministic mapping  $f$  that transforms an input vector  $x$  into hidden representation  $y$
- A **decoder** maps back the hidden representation  $y$  to the reconstructed input  $z$  via  $g$ .
- **Autoencoder**: compare the reconstructed input  $z$  to the original input  $x$  and try to minimize the reconstruction error
- used for classification, clustering and feature compression

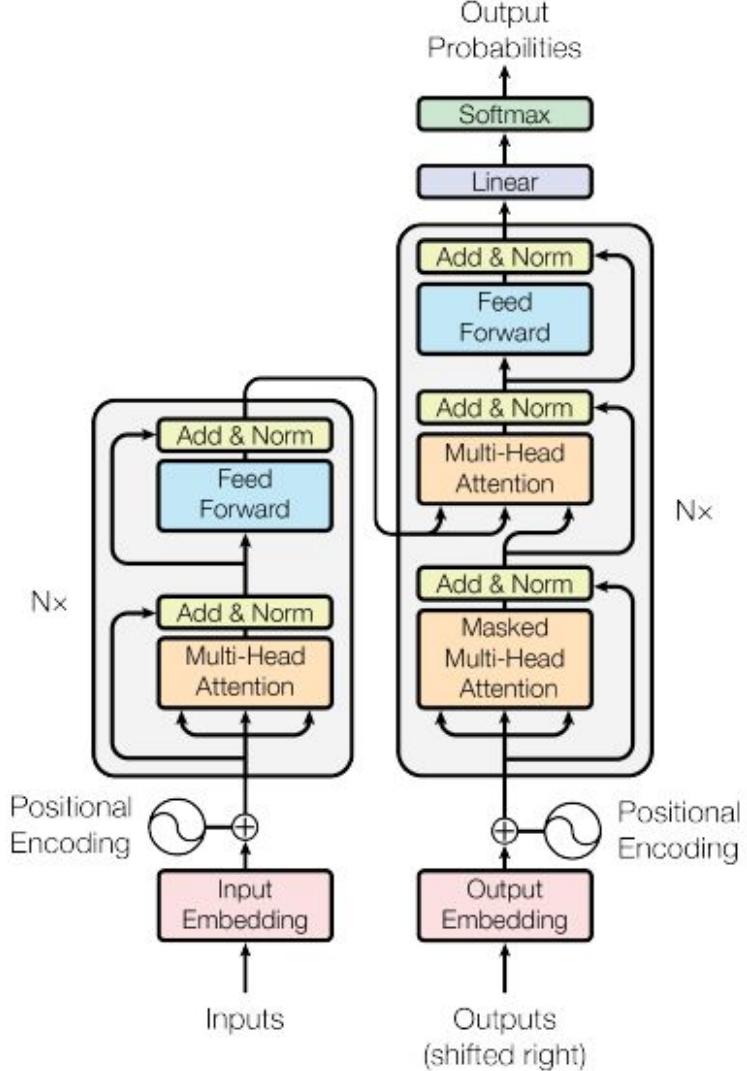
# Auto Encoders



# TRANSFORMERS (2017)

- All you need is attention
- **Self-attention: query, key, value:**
  - the output is a weighted sum of the values, where the weight assigned to each value is determined by the dot-product of the query with all the keys:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

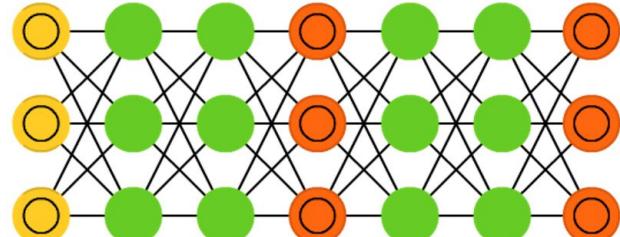
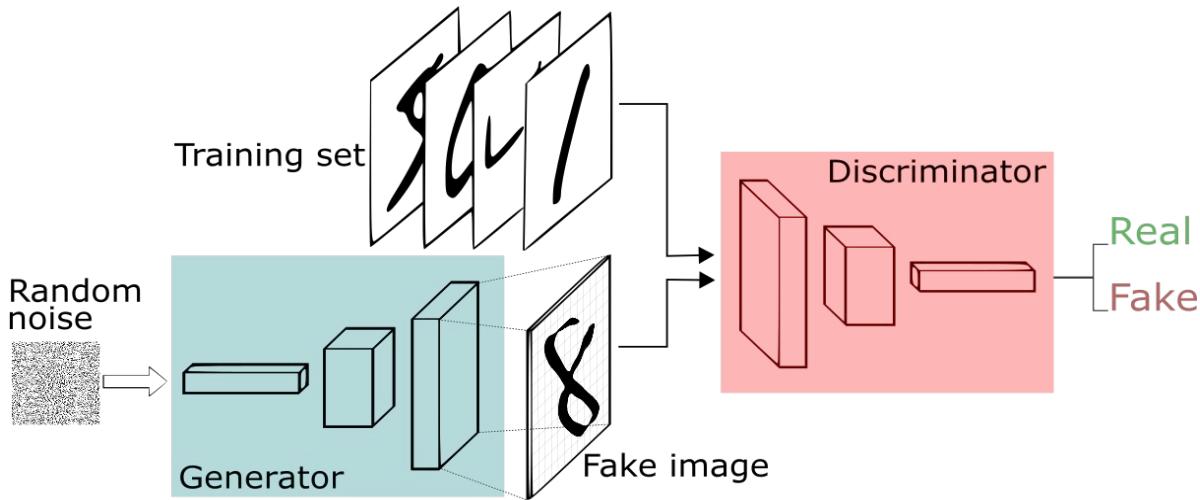


# Generative Adversarial Networks (GAN)

- GANs represent a huge family of double networks that are composed from a **generator** net and a **discriminator** net
  - The generator produces samples close to training samples
  - Discriminator net (adversary) must differentiate between samples from the generative net and the training set
  - Use error feedback to improve task of both nets, until discriminator can no longer distinguish
  - Discriminator net is discarded at test time
- Can be used to generate samples of data without prior knowledge of the data

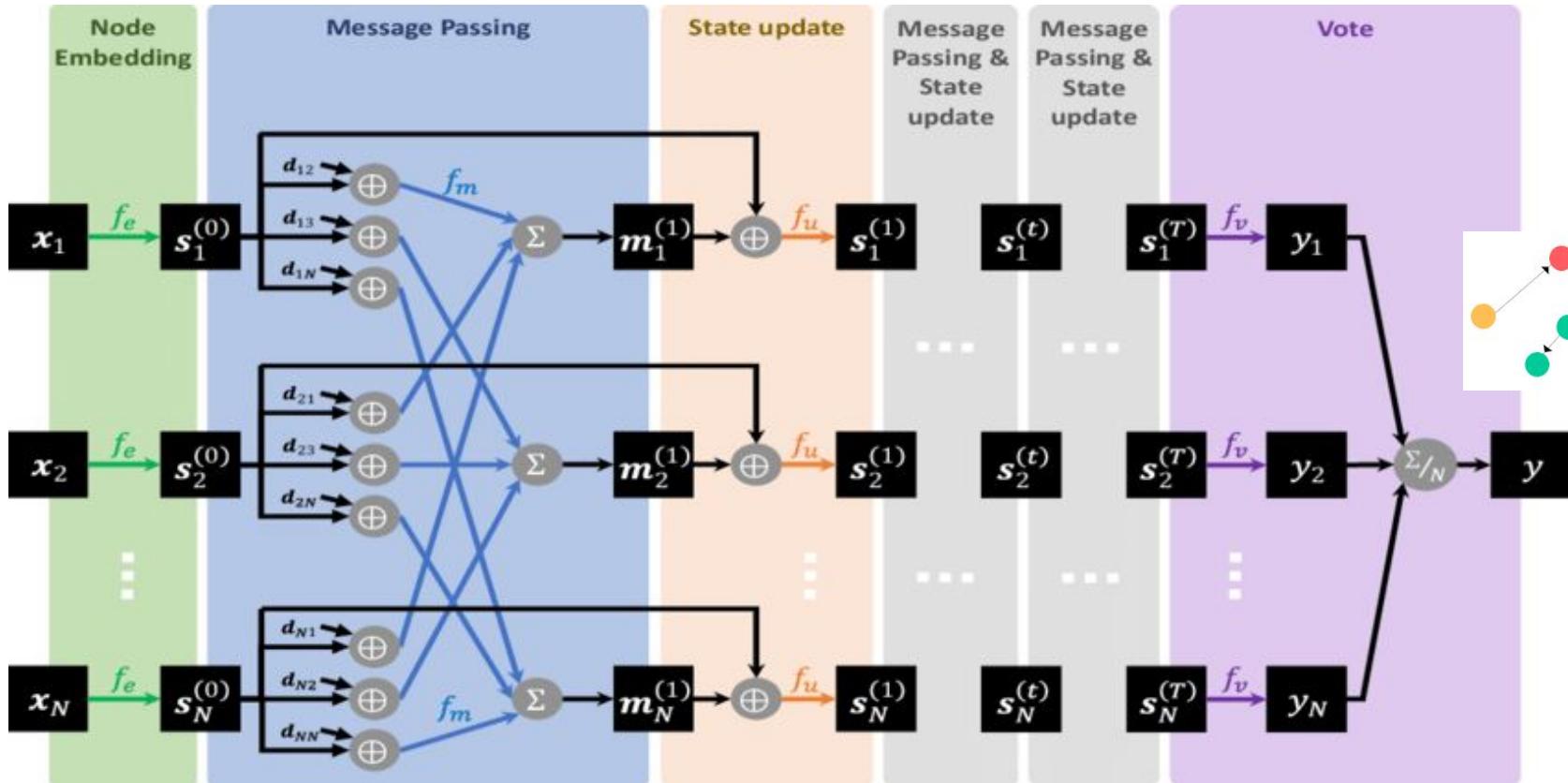
# Generative Adversarial Networks (GAN)

- Double network: generator net and discriminator net
  - generator produces samples close to training samples
  - discriminator differentiates samples from generator and training set
  - training until discriminator can no longer distinguish



# GRAPH NEURAL NETWORK (GNN)

- Node prediction
- Edge prediction
- Graph prediction



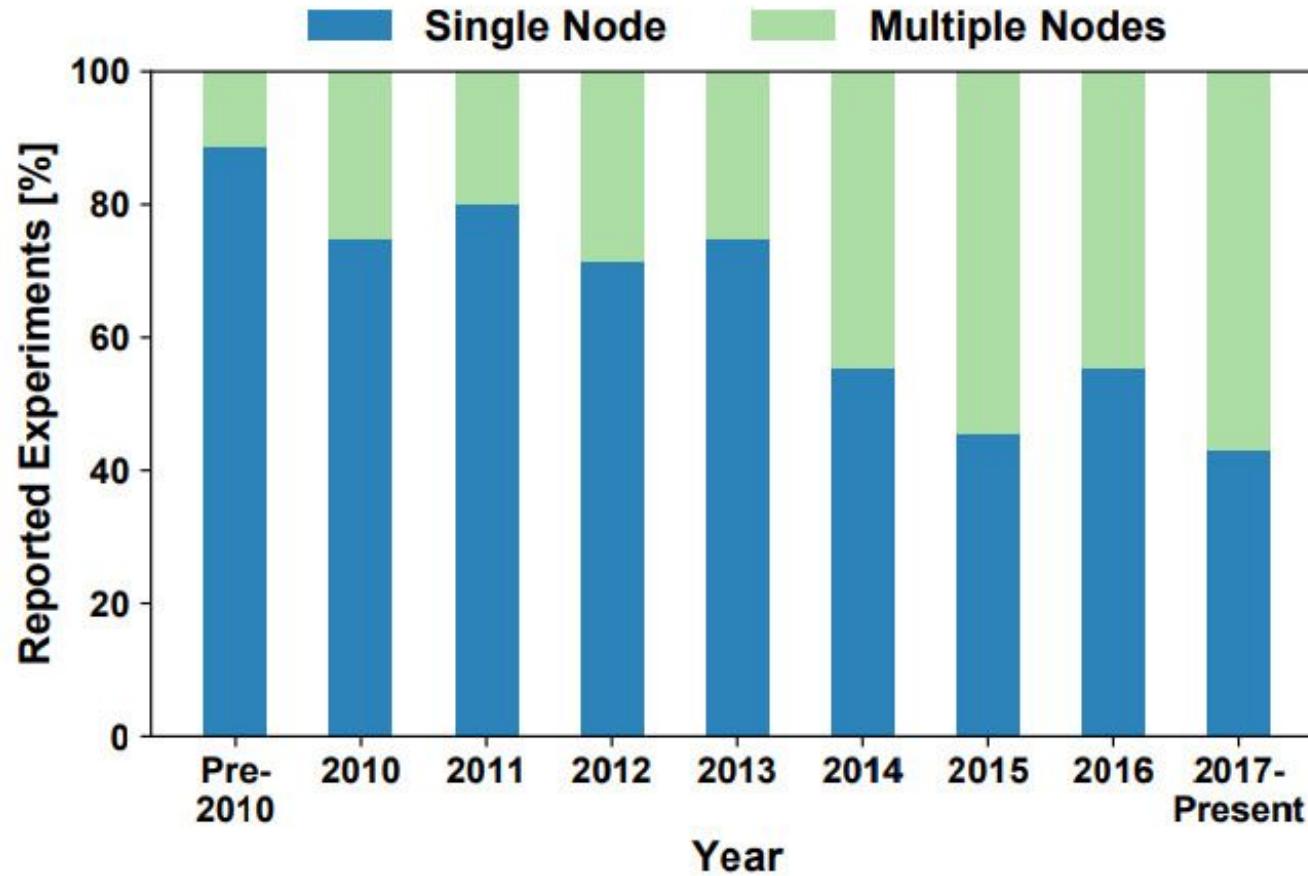
# NN evolution in the past 10 years

- 2009: handwriting recognition prizes with LSTM
- 2011 DanNet (CNN) beats humans in **visual pattern recognition**
- 2014: GANs, Alexa, Tesla AutoPilot
- 2015: FaceNet starts facial recognition programs
- 2016: AlphaGo **beats Go champion**
- 2017: Google **Translate** and Facebook Translate based on two LSTMs
- 2018: Cambridge analytica, deep fakes
- 2019: DeepMind defeats professional StarCraft players with RL + LSTM, Rubik's Cube solved with a Robot Hand

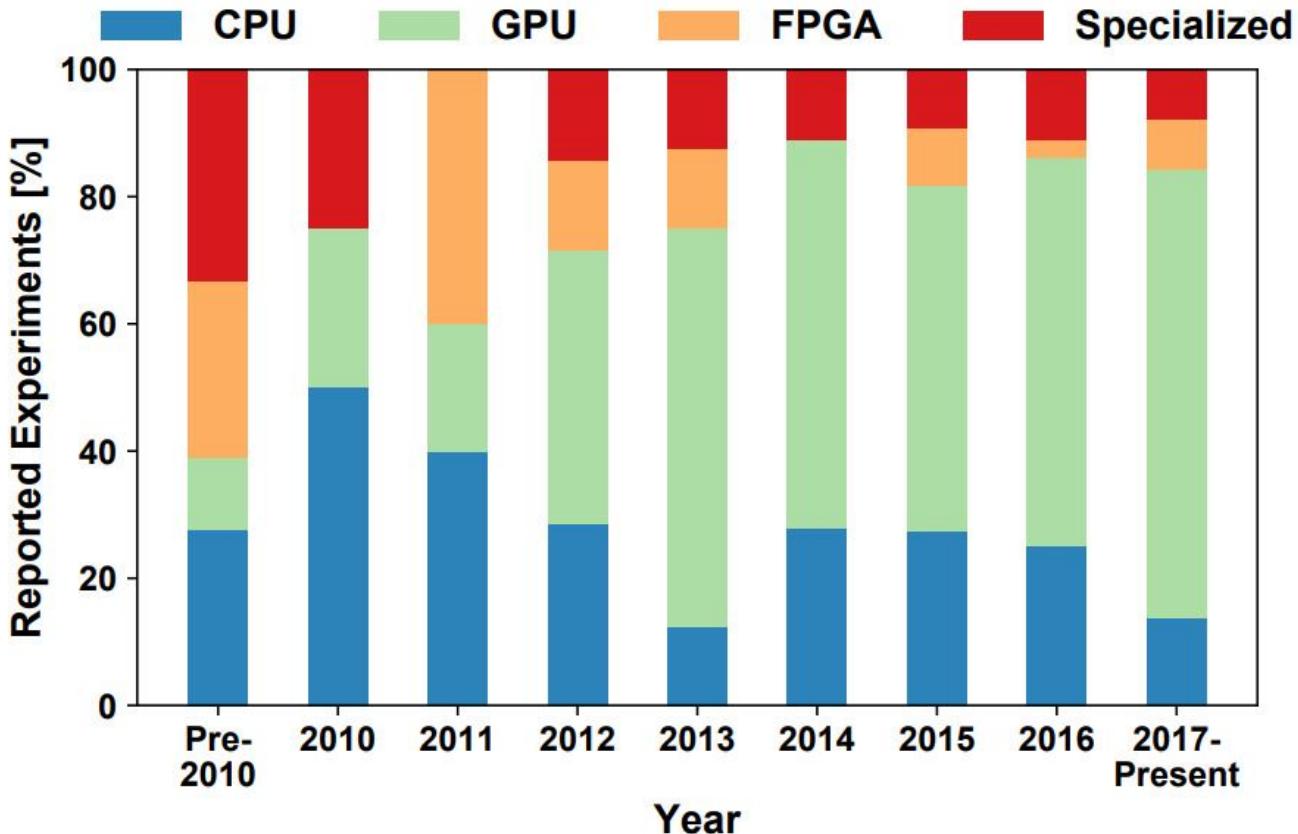
# Summary

- Machine learning (ML): family of algorithms with ability to automatically learn and improve from experience without being explicitly programmed
  - potential to approximate linear and non-linear relationships
- For a given problem:
  - find algorithm that will give the best results
  - Train model
  - Tune hyperparameters
  - Do cross-validation
  - Do inference

- Most ML algorithms require significant amount of CPU, RAM and sometimes GPU in order to be applied efficiently
- **Does it fit on your laptop?**



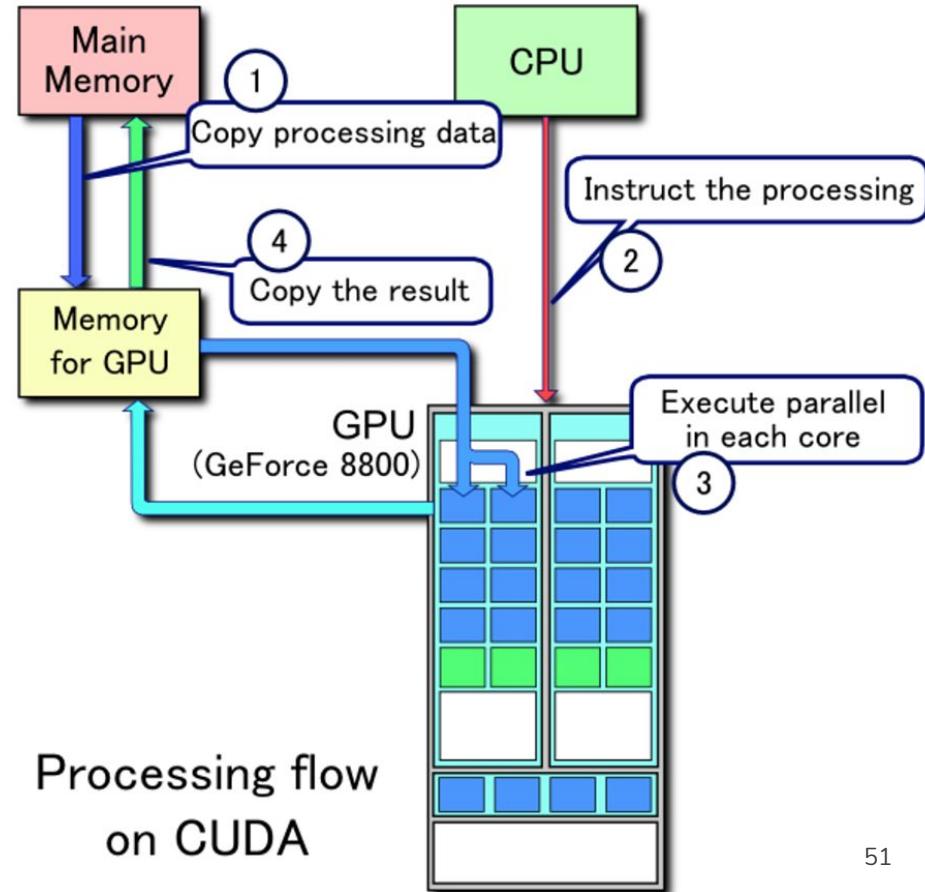
Fraction of non-distributed vs distributed deep learning over time



Use of hardware for deep learning

# GPU (Graphical Processing Unit)

- Typically composed of thousands of logical cores
- Excels at matrix and vector operations
  - Gaming, rendering...and ML
- Main vendor: NVidia
  - CUDA: parallel computing platform and programming model



# Options

- **NVIDIA CUDA**

- Market leader, large user community, best support from DL frameworks
- Can be used in python, C/C++, fortran, Matlab

- **AMD HIP**

- Limited support for pyTorch and Tensorflow
- Slightly behind in terms of performances

- **INTEL**

- Xeon Phi: Poor support
- Habana Gaudi-based AWS EC2 instances will be available in 2021!

- **Google TPU**

- Good performances, more powerful than cloud GPUs
- best for training, for prototype and inference better use cheaper alternatives

- **Amazon AWS and Microsoft Azure**

- Powerful, easy to scale, expensive

# How to choose hardware

- **GPUs** have high performance for floating point arithmetic
  - limited amount of memory available
  - rate at which data can be moved from CPU to GPU
  - **memory bandwidth for GPUs must be seen relative to the amount of FLOPS:** if one has more floating point units, a higher bandwidth is needed to keep them occupied
- **Matrix operations:** typically bandwidth cost is larger than multiplication cost
  - Particularly important for many small multiplications

# How to choose hardware

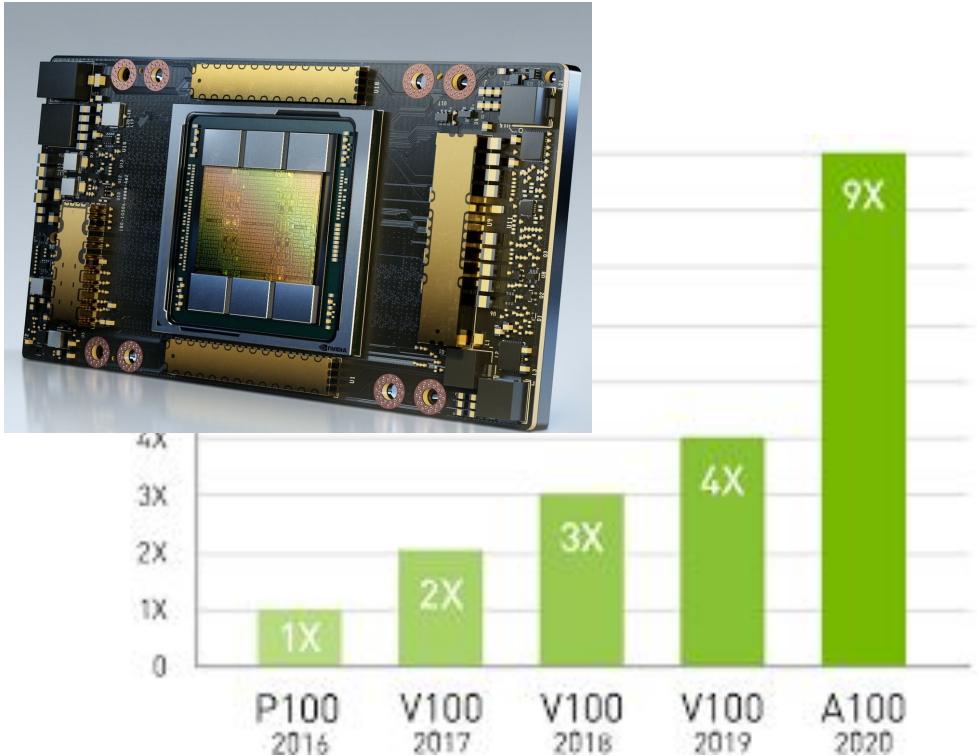
- CNN need a lot of computing power (need high number of cores, FLOPS)
- LSTM and RNN are made of small matrix multiplication: memory bandwidth matters
- Be aware of power consumption and overheating when placing multiple GPUs close to one another!

# Performances

Architecture	INT8 [TOPS]	FP16 [TFLOPS]	FP32 [TFLOPS]	FP64 [TFLOPS]	Memory [GB]	Memory Bandwidth [GB/s]	PCIe [GB/s] <sup>[a]</sup>	Proprietary Interconnect [GB/s] <sup>[a]</sup>
AMD Instinct MI25 <a href="#">[65]</a>	–	24.6	12.29	0.77	16	484	15.75	–
AMD Instinct MI50 <a href="#">[66]</a>	53.6	26.8	13.4	6.7	16	1024	31.51	200 (2 x 100)
AMD Instinct MI60 <a href="#">[67]</a>	58.9	29.5	14.7	7.4	32	1024	31.51	200 (2 x 100)
NVIDIA P100[b] <a href="#">[68]</a> <a href="#">[69]</a> <a href="#">[71]</a>	–	21.2	10.6	5.3	16	732	15.75	160 (4 x 40)
NVIDIA V100 <sup>[b]</sup> <a href="#">[71]</a> <a href="#">[70]</a> <a href="#">[72]</a>	62.8[c]	31.4 <sup>[c]</sup> / 125 <sup>[d]</sup>	15.7	7.8	16 / 32	900	15.75	300 (6 x 50)
Intel Xeon Scalable 8180 (per socket) <a href="#">[73]</a> <a href="#">[74]</a>	–	–	3.0 / 4.2[e]	1.5 / 2.1 <sup>[e]</sup>	768 (max)	119 (max)	15.75	–
AMD EPYC 7601 (per socket) <a href="#">[61]</a> <a href="#">[62]</a>	–	–	1.1 / 1.4[f]	0.56 / 0.69 <sup>[f]</sup>	2000 (max)	159	15.75	–

<sup>[a]</sup> PCIe bandwidths are unidirectional. NVlink speeds are aggregated bidirectional bandwidth. For Infinity Fabric (IF) the bandwidth for one Infinity Fabric link is quoted; it is unspecified whether this is unidirectional, or aggregated bidirectional bandwidth.

# NVIDIA GPUs



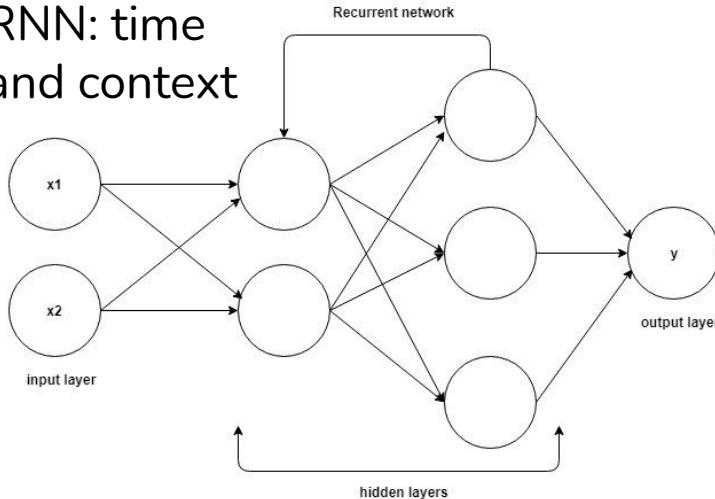
	Peak Performance
Transistor Count	54 billion
Die Size	826 mm <sup>2</sup>
FP64 CUDA Cores	3,456
FP32 CUDA Cores	6,912
Tensor Cores	432
Streaming Multiprocessors	108
FP64	9.7 teraFLOPS
FP64 Tensor Core	19.5 teraFLOPS
FP32	19.5 teraFLOPS
TF32 Tensor Core	156 teraFLOPS   312 teraFLOPS*
BFLOAT16 Tensor Core	312 teraFLOPS   624 teraFLOPS*
FP16 Tensor Core	312 teraFLOPS   624 teraFLOPS*
INT8 Tensor Core	624 TOPS   1,248 TOPS*
INT4 Tensor Core	1,248 TOPS   2,496 TOPS*
GPU Memory	40 GB
GPU Memory Bandwidth	1.6 TB/s
Interconnect	NVLink 600 GB/s PCIe Gen4 64 GB/s
Multi-Instance GPUs	Various Instance sizes with up to 7MIGs @5GB
Form Factor	4/8 SXM GPUs in HGX A100
Max Power	400W (SXM)

With its multi-instance GPU (MIG) technology, A100 can be partitioned into up to seven GPU instances, each with 10GB of memory.

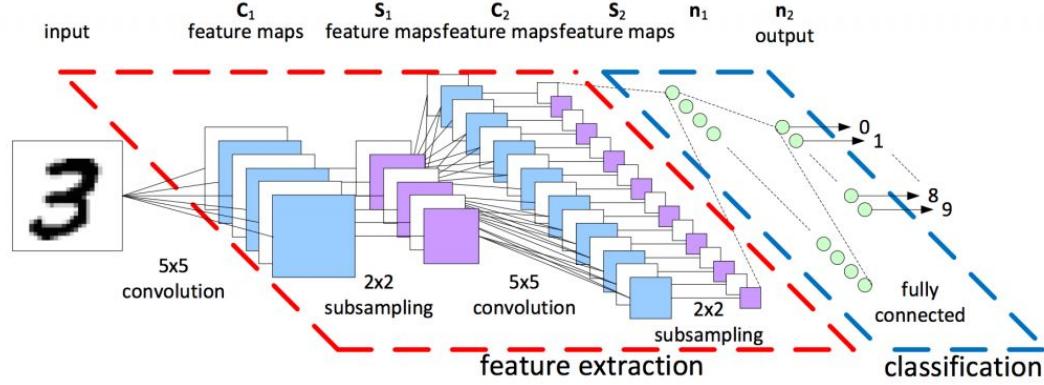
# Parallelisation on multiple GPUs

- ‘Easy’ for RNNs and CNNs
- Fully connected networks with transformers poorer performances
- multiple GPUs can be used for tasks trivial to parallelise such as hyperparameter scan

RNN: time  
and context



CNN: image recognition



# Local training

- Both model and data fit on a **single machine (multi cores + GPU)**
  - Multi-core processing:
    - *Embarrassingly parallel process*: use the cores to process multiple images at once, in each layer
    - Use multiple cores to perform SGD of multiple mini-batches in parallel.
  - Use GPU for computationally intensive subroutines like matrix multiplication.
  - Use both multi-core processing and GPU where all cores share the GPU and computationally intensive subroutines are pushed to the GPU.

# Distributed training

- Data or model stored across multiple machines
- **Data parallelism:** data is distributed across multiple machines
  - data is too large to be stored on a single machine or to achieve faster training
  - **Synchronous update:** all loss gradients in a given mini-batch are computed using the same weights and full information of the average loss in a given mini-batch is used to update weights
  - **Asynchronous update:** as soon as a machine finishes computing updates, the parameters in the driver get updated. Any machine using the parameters will fetch the updated parameters from the server.

# Data parallelism

- large batch of input data split across a collection of workers, each holding the full model
  - the forward pass involves no communication
  - the backward pass involves aggregating the gradients computed by each individual worker with respect to its separate part of the “global batch”
- scaling out:
  - the “global batch size” (i.e. the total number of examples across all workers that are seen in a single forward pass) increases
  - Affects convergence of DL algorithms and does not reach same accuracy levels that can be obtained with smaller batch sizes

# Model parallelism

- model layers split across a collection of workers
- the batch size stays constant, and large models that would not fit the memory of a single device can be trained
- active communication also in the forward pass, thus requiring a lot more communication than a data parallel approach
- unless the advantages of model parallelism are absolutely critical (model doesn't fit on one machine), most research on large-scale training is done using data parallelism.
- Schemes involving a mix of data and model parallelism also exist: *hybrid parallelism*.

# Hardware issues

- **I/O contention** with large data sets, or data sets with many small examples, and the data has to be physically stored on shared storage facilities.
- **Communication** bottlenecks during gradient-aggregation, due to high ratio between the number of parameters and amount of computation
- **Memory** bottlenecks for large networks, particularly when using memory-limited GPUs
- On large system such as **HPCs**, data are typically stored on shared file systems
  - Might be faster to copy data locally to worker node

# Architectural choices

- **Your model doesn't fit in the GPU memory?**
  - tune the model e.g. by reducing its connectivity (if that is acceptable) to fit the hardware
  - use model parallelism to distribute the model over multiple GPUs
  - use a data parallel approach on CPUs (if it does fit in CPU memory)
- **Your dataset doesn't fit in the GPU memory?**
  - Make sure your data arrives fast enough to the GPU, otherwise revert to CPU
- **Do you have access to a system with a few GPU nodes, but thousands of CPUs?**
  - Development stage: run a limited number of examples (potentially even with a smaller model) on a single GPU, which allows quick development cycles
  - Production: may require CPUs because of memory constraints

# Requirements for ML framework

- Run any ML algorithm of our choice in parallel
- Large datasets to be processed
- Multi-tenancy, so different users can request simultaneously ML pipelines
- An efficient resource management system for the cluster
- Support heterogeneous architectures
  - CPUs, GPUs, ...

# ML as a Service (MLaaS)

## CHALLENGES

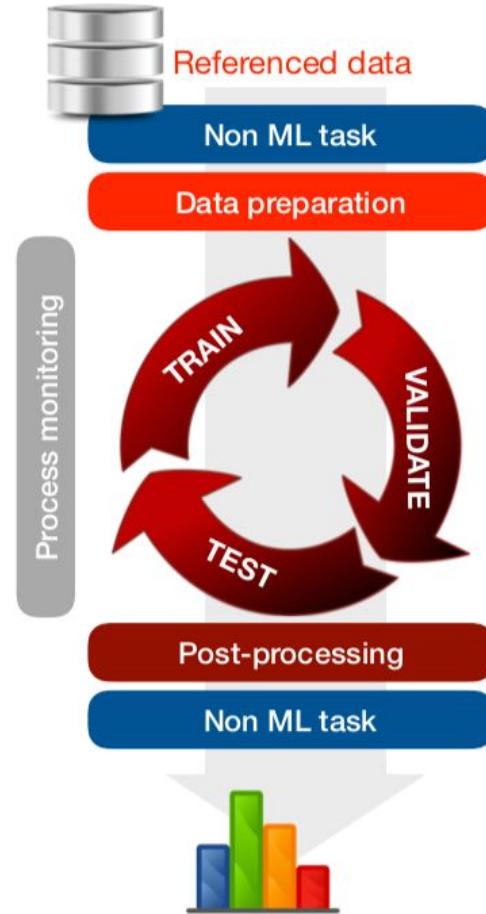
- Reconstruction
- Analysis
- Trigger
- Data quality
- Detector monitoring
- Computing operations
- Monte Carlo tuning
- ...

## REQUIREMENTS

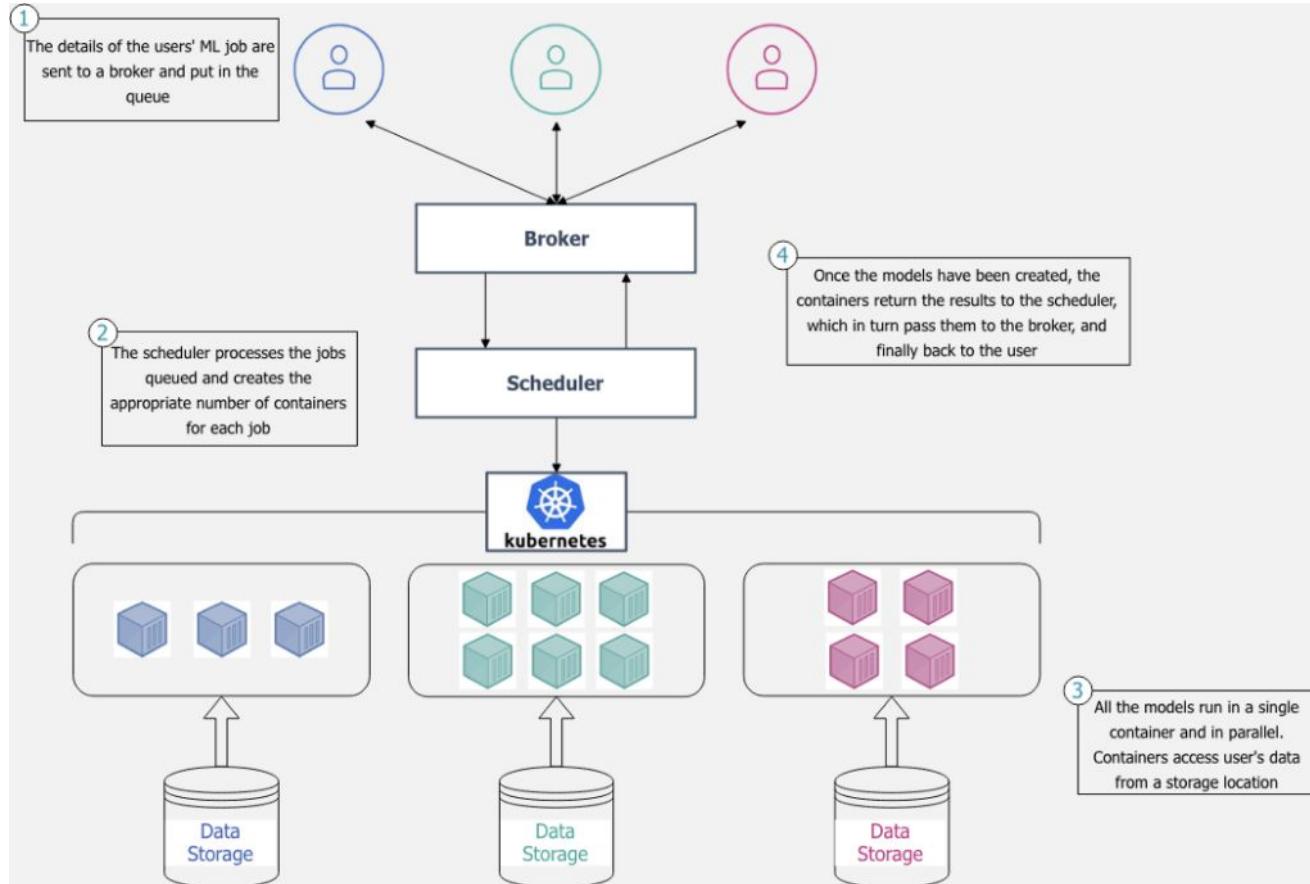
- Workflow definition
  - Results reproducibility
- Multi-tenancy (scheduling, authentication...)
- Parallel execution and scaling
- Data handling
- Ease of use and management
- ...

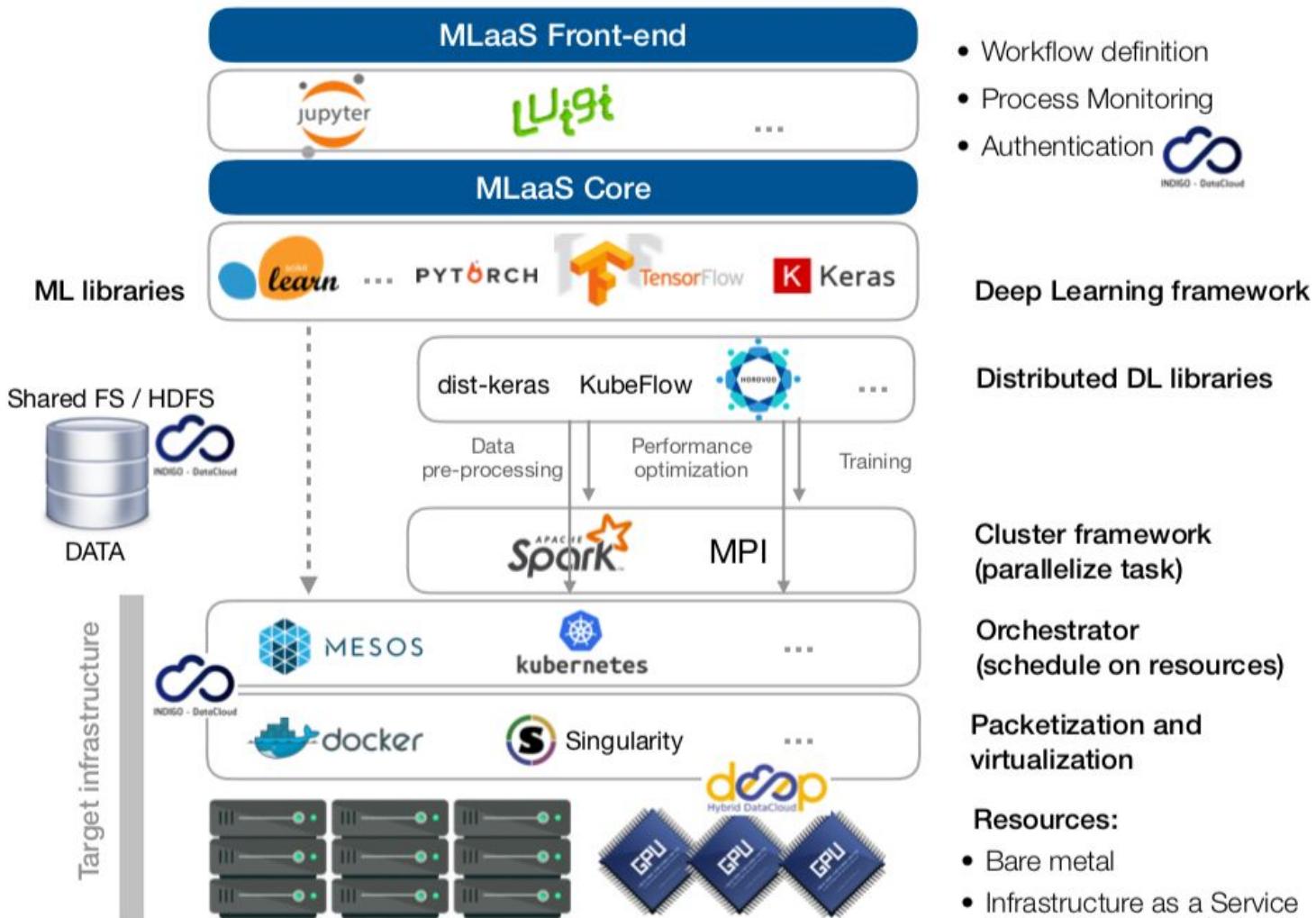
## IMPLEMENTATION

- Lightweight virtualization
- Modularity
- Flexibility
- Heterogeneous back-end infrastructures
- ...



# Example architecture





- Workflow definition
- Process Monitoring
- Authentication



Deep Learning framework

Distributed DL libraries

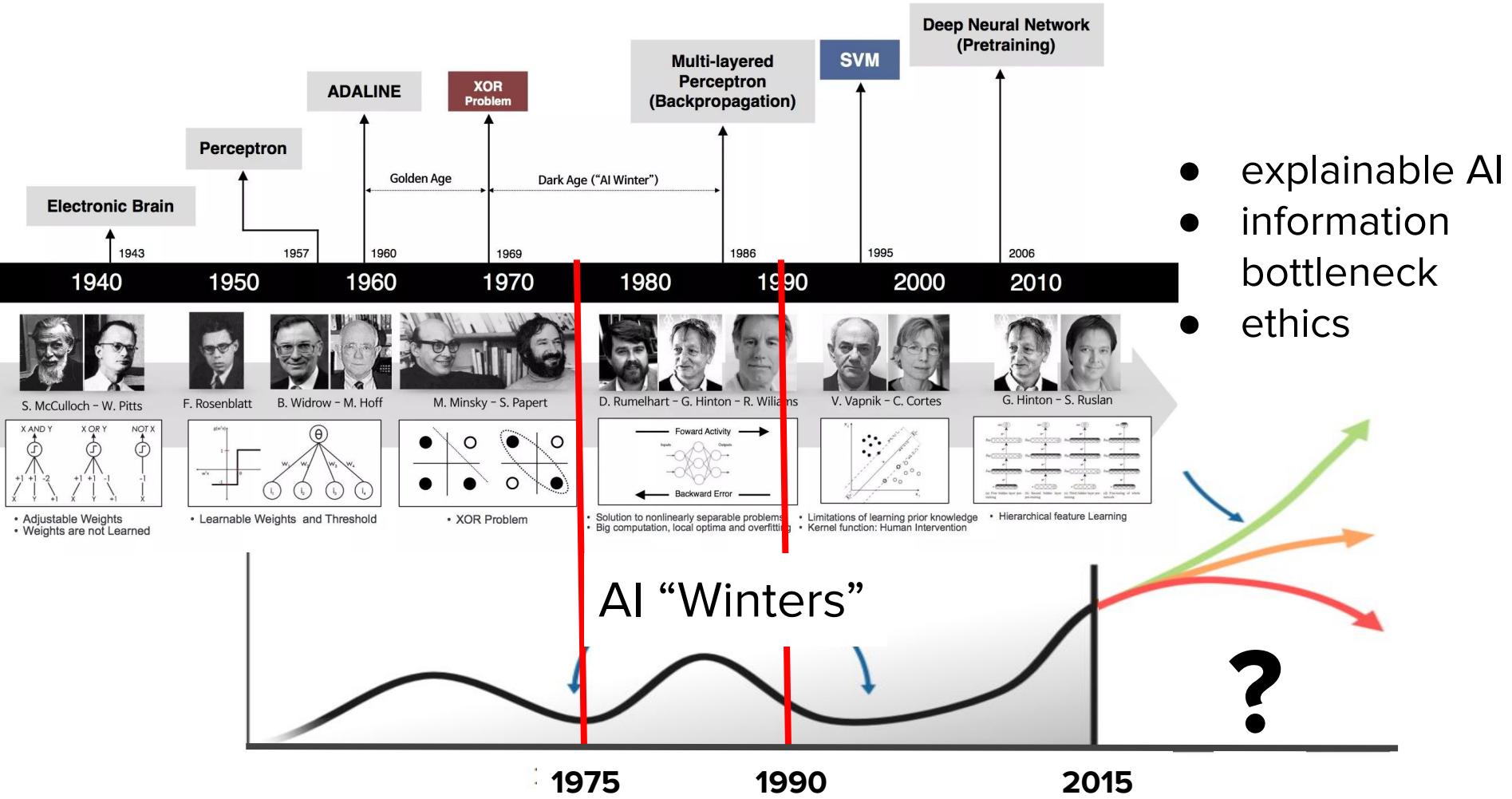
Cluster framework  
(parallelize task)

Orchestrator  
(schedule on resources)

Packetization and  
virtualization

Resources:

- Bare metal
- Infrastructure as a Service



# Artificial General Intelligence

- **Common sense:**
  - Current systems may be easily fooled by just slight changes in the input data (for example image taken from another viewpoint)
  - Embed coordinate systems, whole-part relationship (capsules)
- **Abstract concepts:**
  - Current models may be able to distinguish between a jet and a tau, but do not know what a particle is
- **Creativity:**
  - Current models highly specialised and engineered to solve specific problems

# Self Supervised Learning

- Supervised learning needs many labeled data
- Reinforced learning:
  - Not practical to train in real world (when no simulation is available)
  - takes longer than an average human for a machine to learn a new task
- **Self supervised learning:** Predict everything from everything else - learn representations, rather than learning specific tasks
  - Very large networks trained with large amount of data
  - Filling the blanks - Word2Vec, Transformer architecture for NLP
  - Not (yet) so successful for continuous problems (image, video)

# Consciousness Prior

- Current deep learning:
  - **System 1:** fast, unconscious task solving
- Future deep learning:
  - **System 2:** slow, conscious task solving like reasoning, planning
- How?
  - Learn by predicting in abstract space
  - Learn representations (low dimensional vector), derived using attention from a high dimensional vector
  - The prior: the factor graph (joint distribution between a set of variables) is sparse

$$P(S) = \frac{\prod_j f_j(S_j)}{Z}$$

# Outlook

- The field of AI/ML/DL is steadily progressing
  - Mainly driven by industry applications
  - Science should not stay behind
- Physics applications in a wide range of domains, and growing
- Great opportunities for cooperation with both industry and diverse scientific sectors, and to engage students
  - Foster the use of common tools/technologies

A PROPOSAL FOR THE  
DARTMOUTH SUMMER RESEARCH PROJECT  
ON ARTIFICIAL INTELLIGENCE

J. McCarthy, Dartmouth College  
M. L. Minsky, Harvard University  
N. Rochester, I.B.M. Corporation  
C. E. Shannon, Bell Telephone Laboratories

August 31, 1955