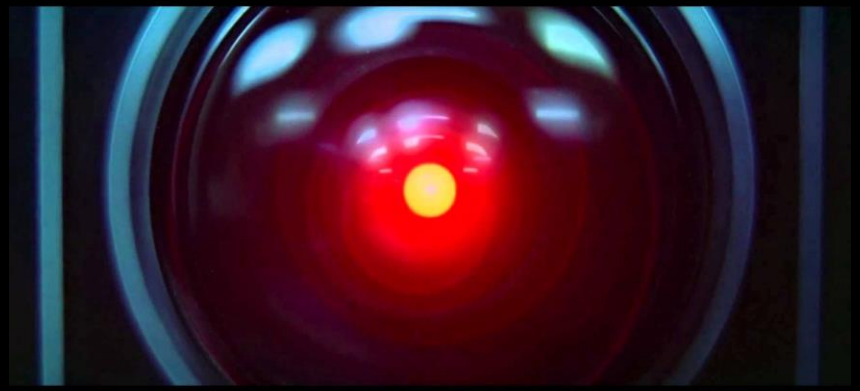
Deep Learning Workshop

Introduction



Instructor: Aaron Low

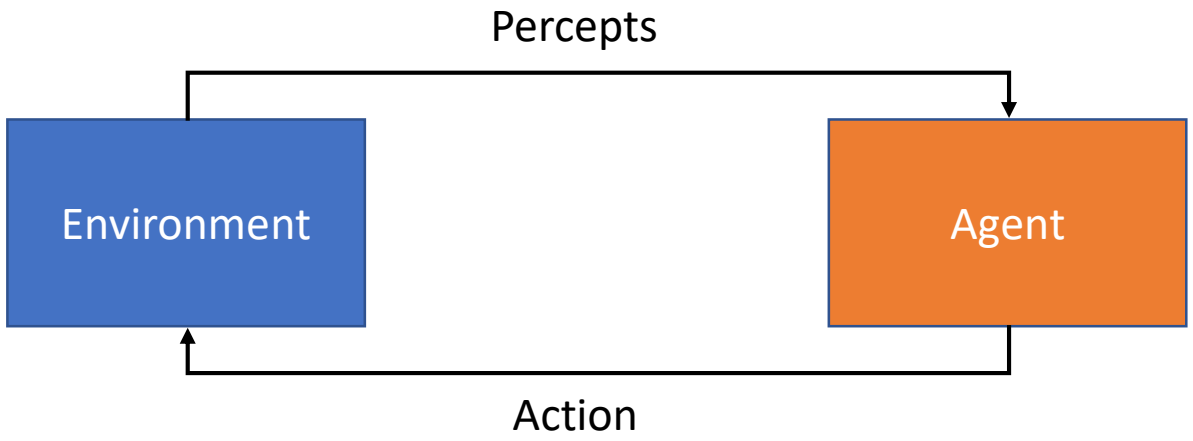
HELP University, Faculty of Computing and Digital Technology

Workshop Overview

- Introduction to Artificial Intelligence
- What is Deep Learning?
- What is all the fuss?
- Deeper dive into the “Black box”
- High level overview of the relevant topics
- Have fun!

What is Artificial Intelligence?

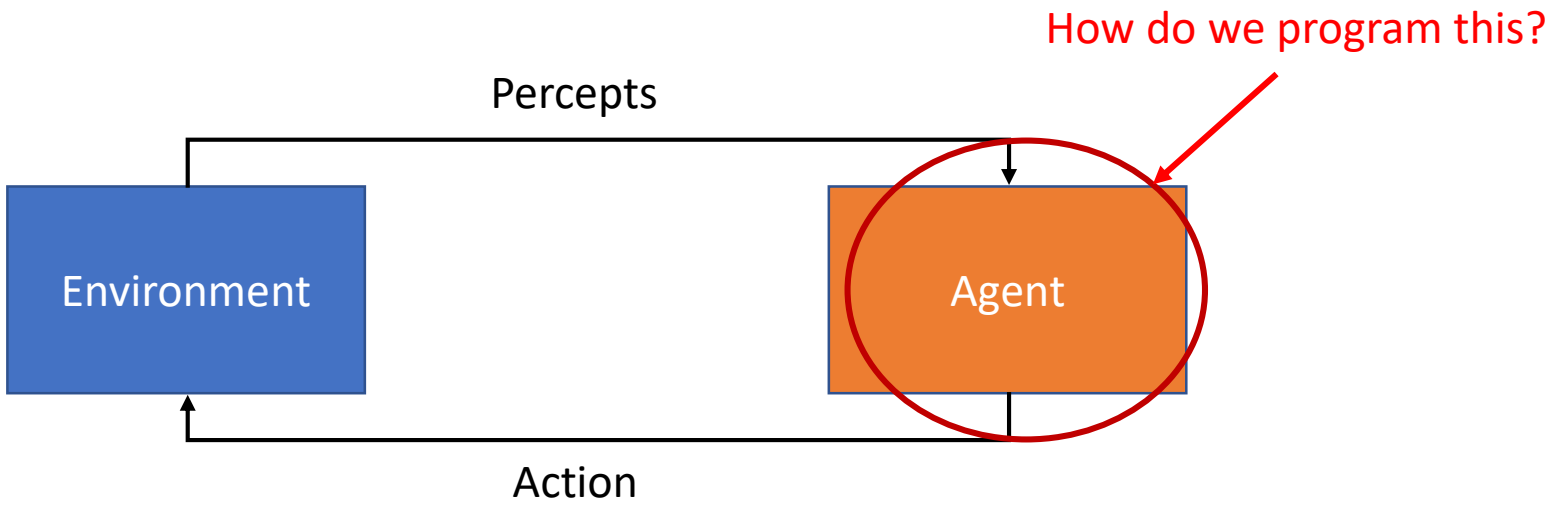
Defined as: *The study of agents that receive percepts from the environment and perform actions*[1]



1: Russell, S. and Norvig, P. Artificial Intelligence: A Modern Approach (3rd Edition). 2010

What is Artificial Intelligence?

Defined as: *The study of agents that receive percepts from the environment and perform actions*[1]



1: Russell, S. and Norvig, P. Artificial Intelligence: A Modern Approach (3rd Edition). 2010

Brief History of AI

- **Pre-20th Century:** AI ideas formed in Mythos, in Fiction
- **1941**: First Program-controlled Computer
- **1943**: Neural Networks
- **1957**: Perceptron
- **1970**: Backpropagation
- **1979**: Convolutional Neural Network
- **1982**: Recurrent Neural Network
- **1989**: Reinforcement Learning
- **1997**: Deep Blue defeats world chess champion Garry Kasparov
- **2014**: Generative Adversarial Networks
- **2016**: AlphaGo beats world Go champion Lee Sedol
- **2017**: AlphaZero
- **2019**: GPT-2

* dates are for perspective, not as definitive historical record of invention or credit

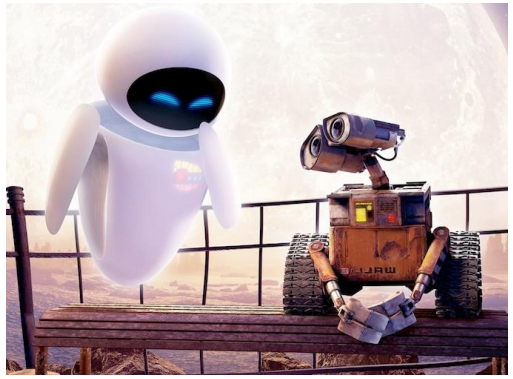
"ARTIFICIAL INTELLIGENCE BEGAN WITH AN ANCIENT WISH TO FORGE THE GODS"
-PAMELA MCCORDUCK

AI in Pop Culture

GLaDOS (Portal)

Agent Smith (Matrix)

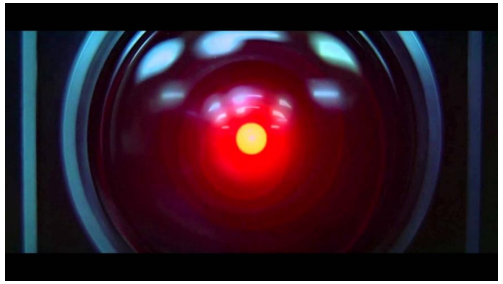
T-800 (Terminator)



WALL-E and EVE (WALL-E)

C-3PO and R2-D2 (Star Wars)

Ava (Ex Machina)



HAL 9000 (2001: A Space Odyssey)

Ultron (Marvel)

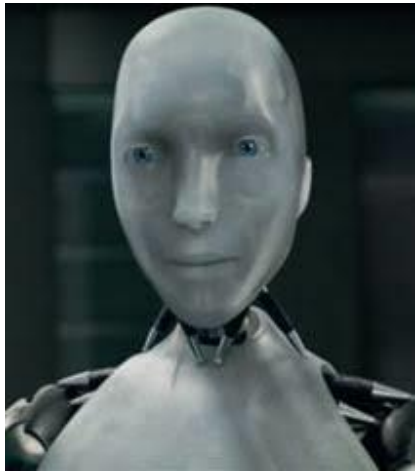
AI in Pop Culture

Samantha (Her)

Roy Batty (Blade Runner)

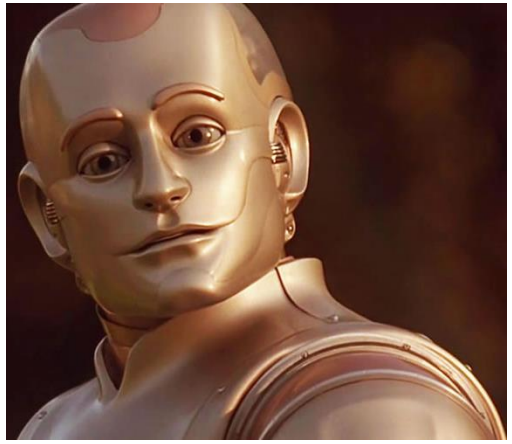
David (A.I. Artificial Intelligence)

CHAPPiE (Chappie)



Sonny (I, Robot)

WOPR (WarGames)

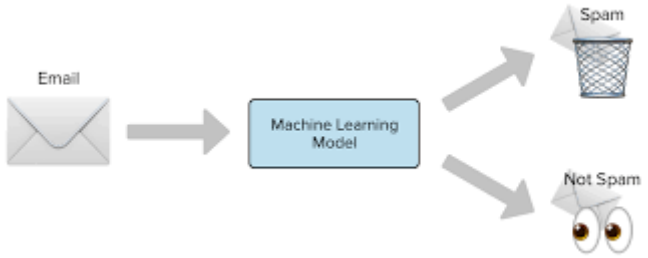


Andrew (Bicentennial Man)

Dolores (Westworld 2016)

Why should you care about AI?

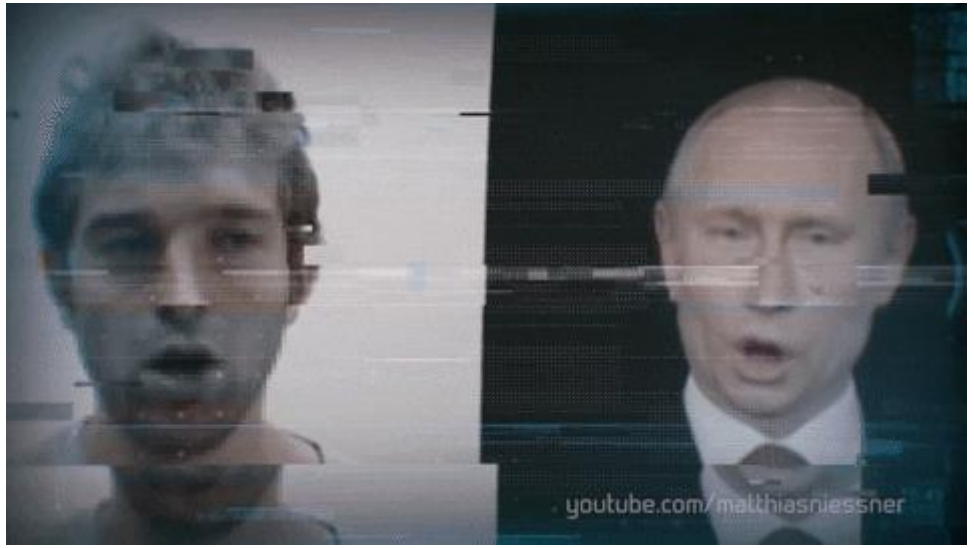
- "Artificial Intelligence is the new Electricity"[1]
- Artificial Intelligence is transforming industry
- It permeates most aspects of technology nowadays
  - Search engines
  - Language translation
  - Spam detection
  - Personalized marketing and advertising
- It could be **useful** to you
- It could be **harmful** to you



[2]

1: Andrew Ng https://www.youtube.com/watch?v=CS4cs9xVecg&list=PLkDaE6sCZn6Ec-XTbcX1uRg2_u4xOEky0&index=1
2: https://www.snopes.com/fact-check/hong-kong-protesters-projectors/

Why should you care about AI?: DeepFake



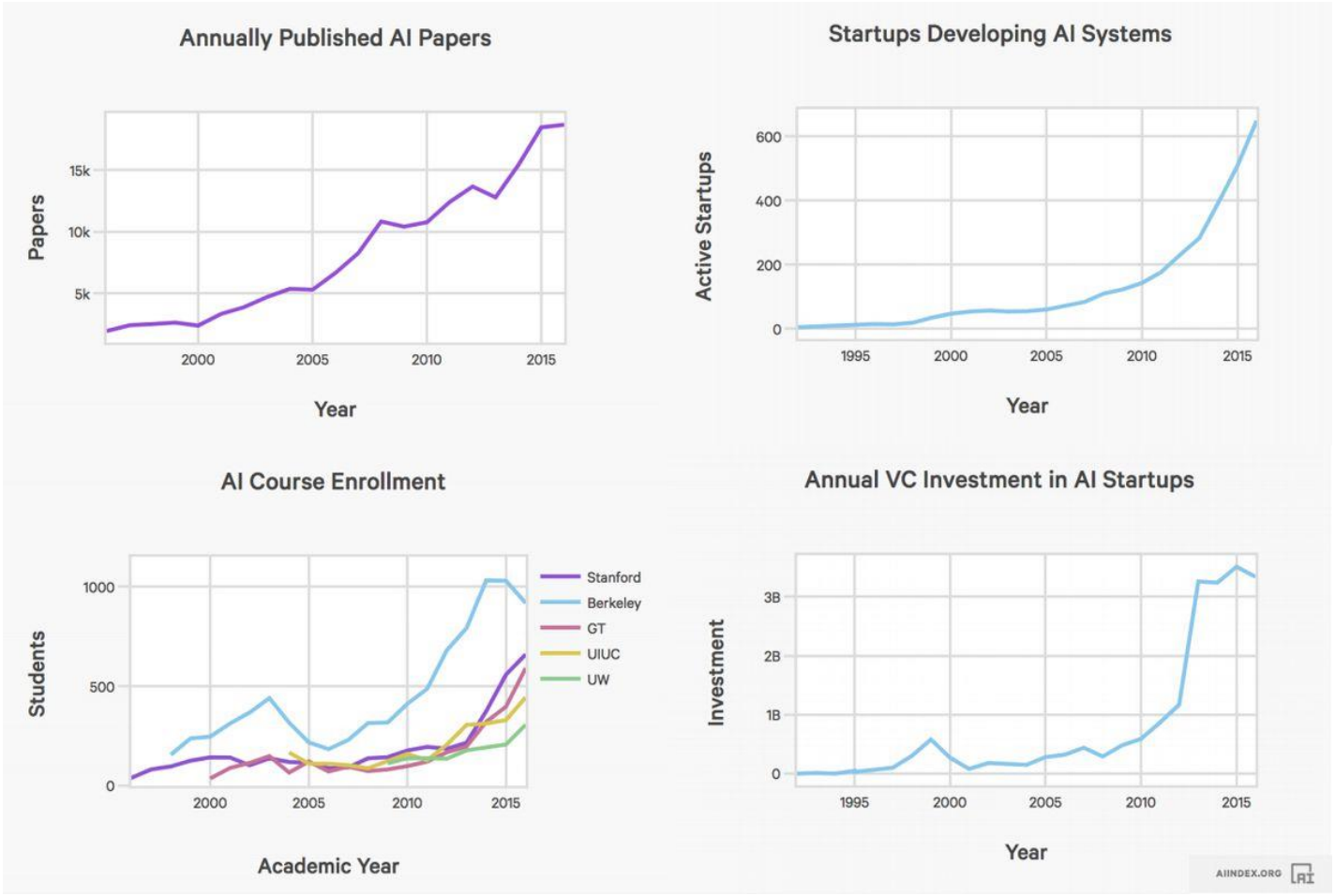
1: DeepFake: https://lab.witness.org/projects/synthetic-media-and-deep-fakes/

Why should you care about AI?: Governance and Privacy

- Facial Recognition pushback in America
- Alleged facial recognition in Hong Kong surveillance system

1: https://www.activistpost.com/2020/01/interview-michael-maharrey-on-facial-recognition-pushback.html
2: https://asia.nikkei.com/Spotlight/Hong-Kong-protests/Hong-Kongers-wreck-smart-lampposts-on-surveillance-fears

Why should you care about AI?



Graphs from https://www.forbes.com/sites/louiscolumbus/2018/01/12/10-charts-that-will-change-your-perspective-on-artificial-intelligences-growth/#94ee80e47583

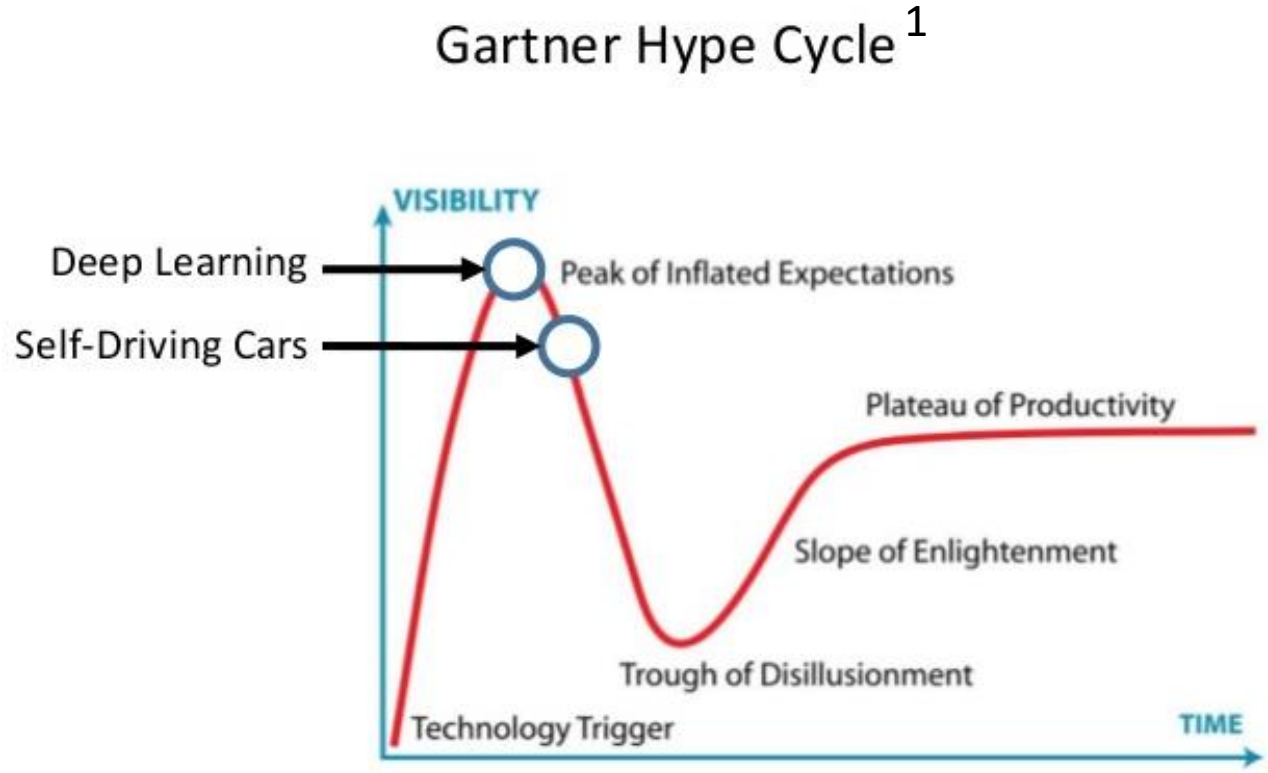
Be careful what you read about AI

- **AI snake oil[1]**
  - Obfuscation of facts
  - Overselling what AI can do
  - There is a lot of commercial interest in AI these days
  - Sometimes it's too good to be true
  - Sometimes it can be done easily with simpler methods
- **AI Hype[2]**
  - The term 'AI' is thrown around very loosely
  - Sometimes it's not totally autonomous; humans still play an important role
  - There is always some sort of limitation

Think critically

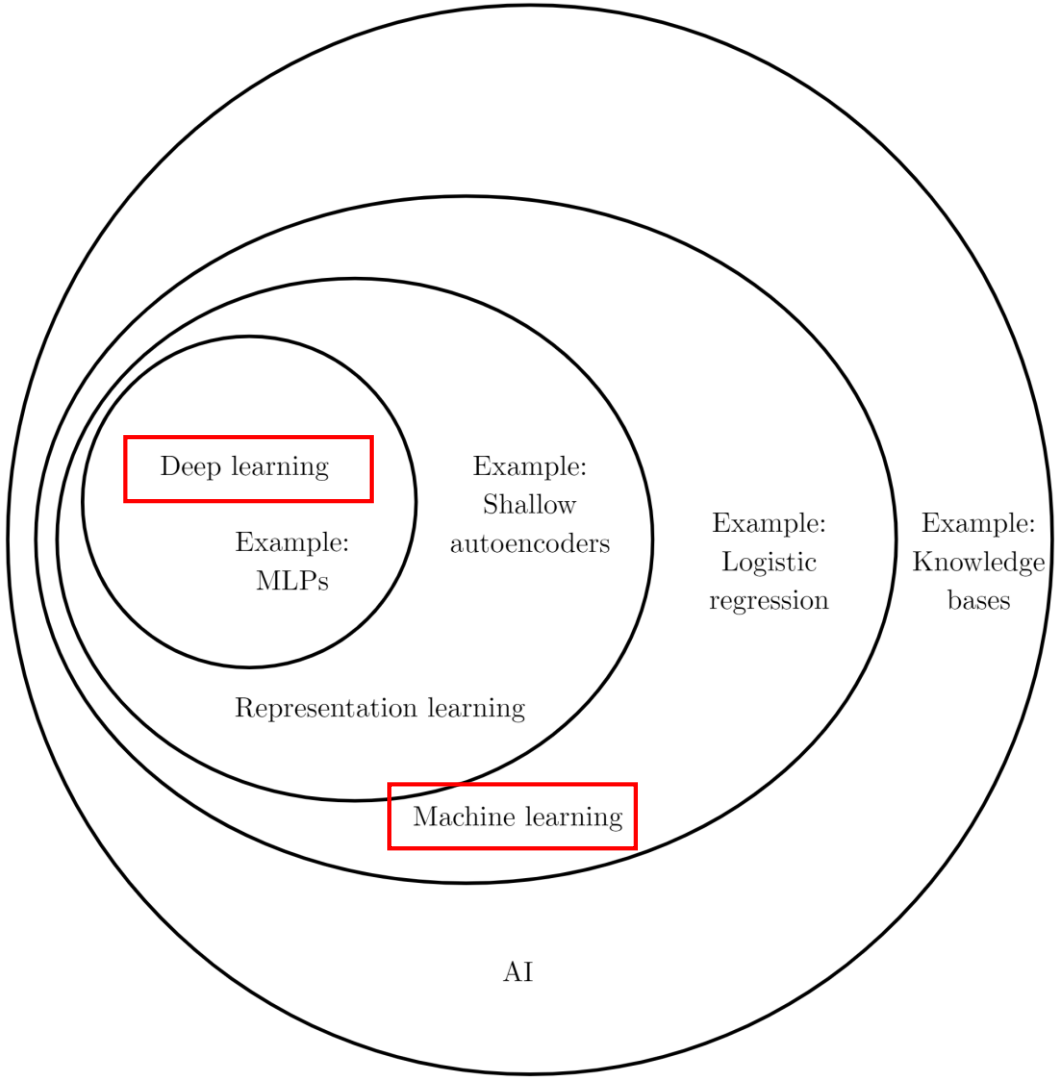
1: https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf
2: https://www.skynettoday.com/editorials/ai-coverage-best-practices

Be careful what you read about AI



1: MIT Deep Learning Basics: Introduction and Overview Lex Fridman https://www.youtube.com/watch?v=O5xeyoRL95U

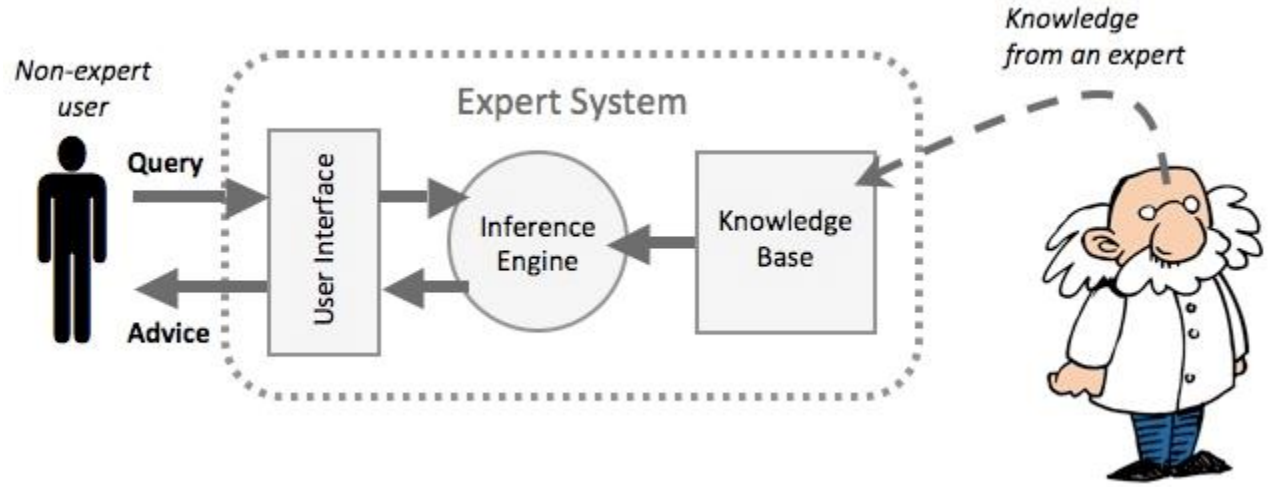
Machine Learning and Artificial Intelligence



AI Venn diagram from http://www.deeplearningbook.org/contents/intro.html

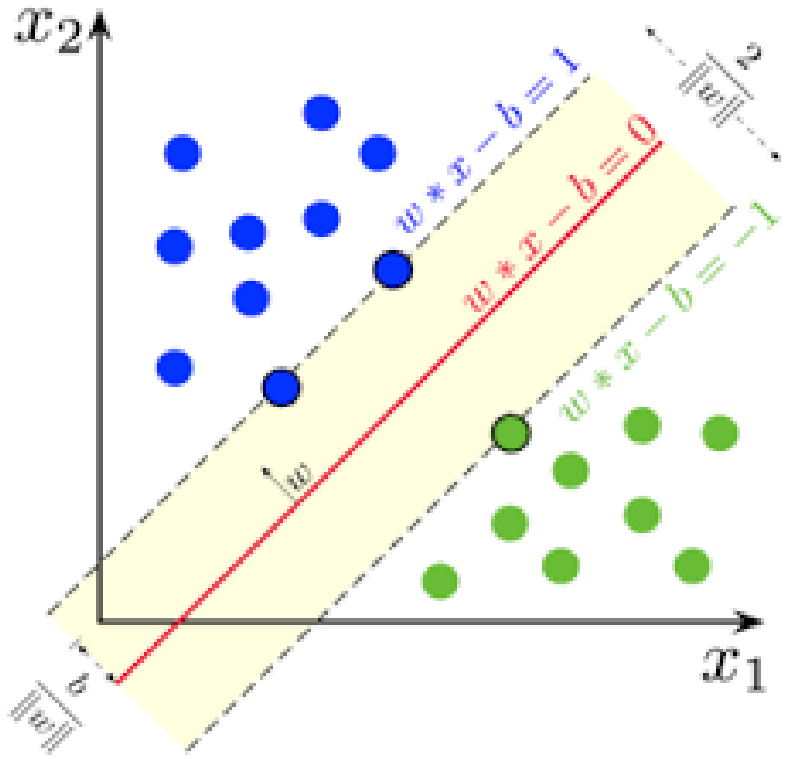
“Classical” AI: Expert Systems

The knowledge base is created from **information** provided by **human experts**



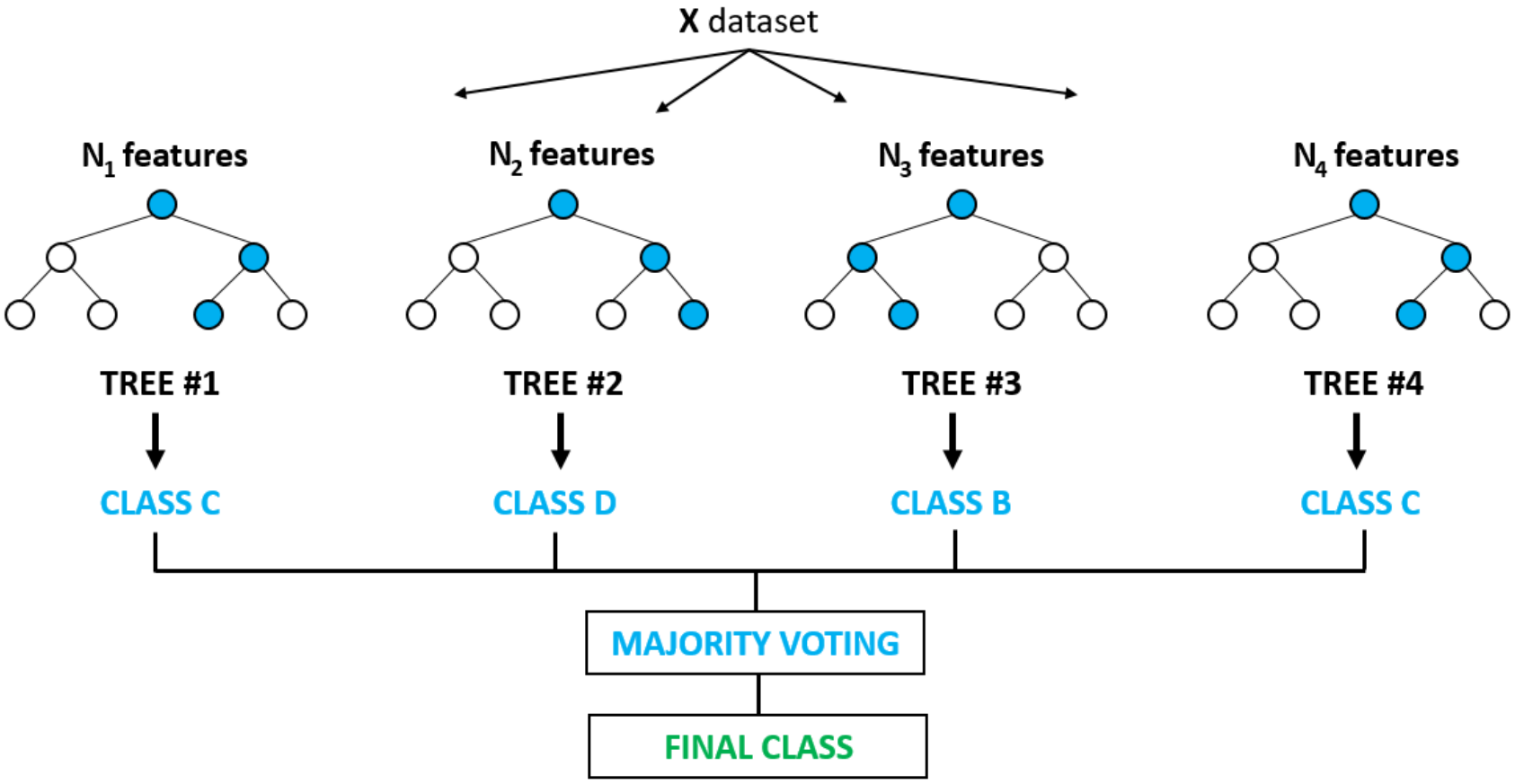
1: Expert System Diagram https://www.igcseict.info/theory/7_2/expert/

“Traditional” Machine Learning: Support Vector Machines



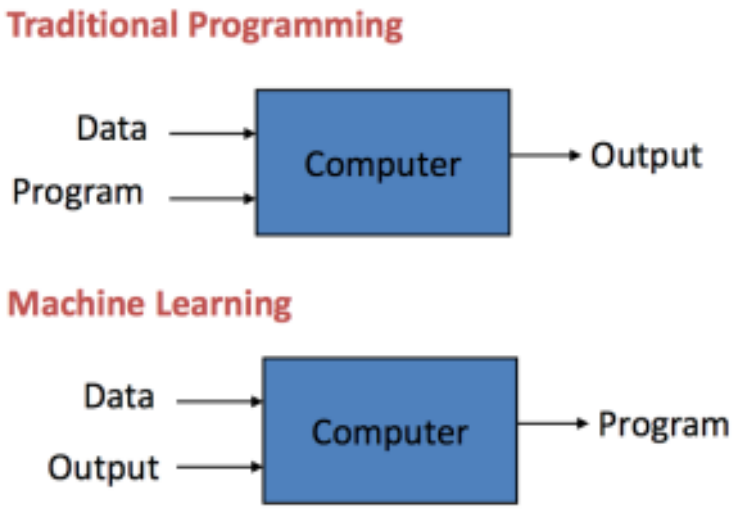
1: Cortes, Corinna, and Vladimir Vapnik. "Support-vector networks." *Machine learning* 20.3 (1995): 273-297.

“Traditional” Machine Learning: Random Decision Forest



What is Machine Learning?

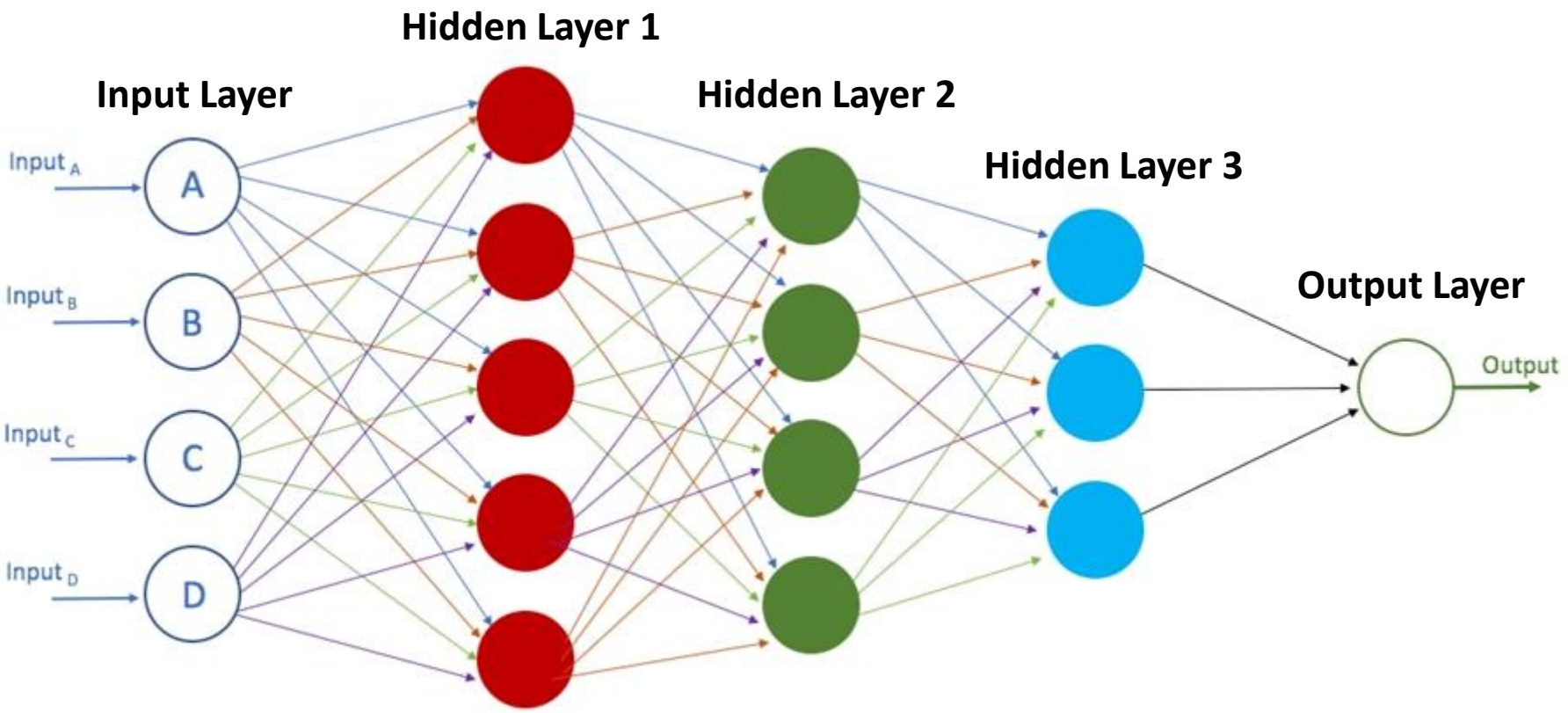
Defined as: *The science of getting computers to learn and act like humans do, and improve their learning over time in autonomous fashion, by feeding them data and information in the form of observations and real-world interactions*[1]



Deep Learning is a subclass of machine learning which involves the usage of multiple layers of **neural networks**

1: https://emerj.com/ai-glossary-terms/what-is-machine-learning/

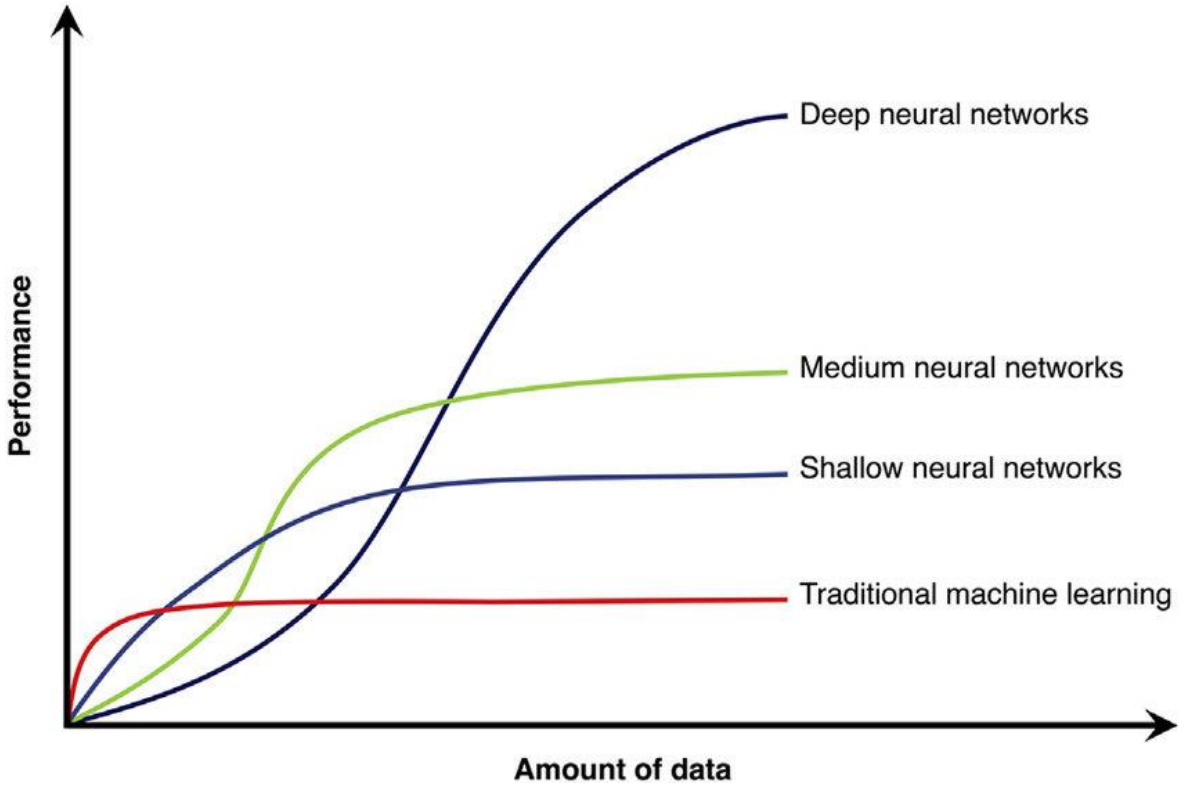
Neural Network



Deep Neural Network from https://developer.oracle.com/databases/neural-network-machine-learning.html

Why Deep Learning?

- **Reduce time spent programming**
  - Hand coded rules are mostly unnecessary
- **Customize and scale products**
  - Only need to collect data for new market
- **Solve seemingly “unprogrammable” tasks**
  - Face recognition and classification
  - Human pose estimation
  - Beat the world’s best player at Go
- **Improvement in computational speed**
  - Better hardware (GPUs)
  - Data parallelism
- **Increase in quantity of data**
  - Web services
  - Mobile apps
  - Research and industry



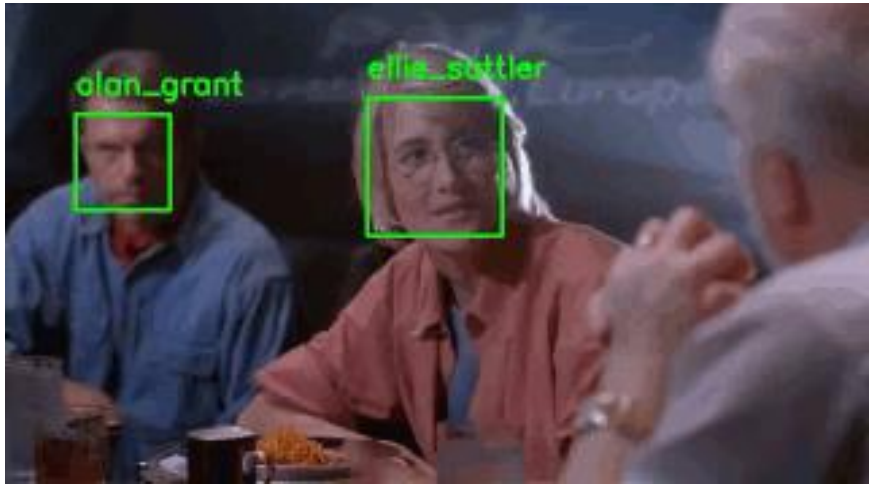
Broad Goals

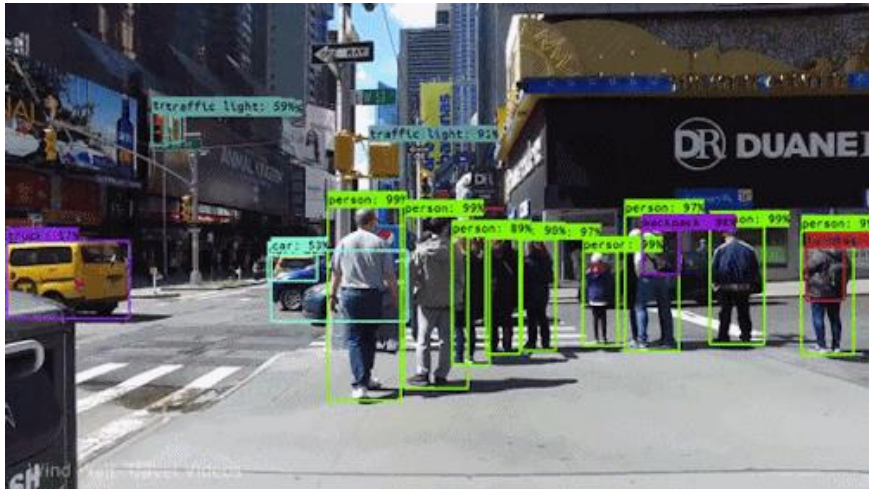
- **Automation**
  - Reduce tedious human labour
  - Improve efficiency
  - e.g. Algorithm trading, Automatic spam mail detection, Self-driving cars

- **Solve problems**
  - Solve problems too complex or tedious for humans to solve in a direct manner
  - Discovery of useful features in complex data
  - e.g. Translate English to Chinese, Facial detection

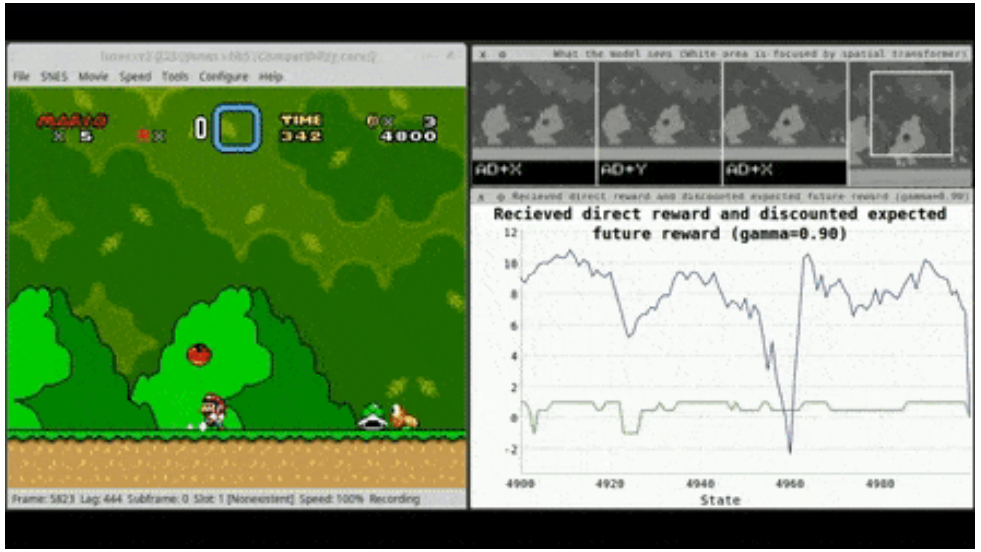
- **Simulation and Modelling**
  - Create models that can accurately predict future events
  - e.g. Weather prediction, Stock market prediction
- **Improved tools**
  - Tools that can provide advice with increased precision and rigour
  - Tools that can reduce risk in dangerous situations
  - e.g. Computer-aided interpretation of medical images, Disaster relief robots

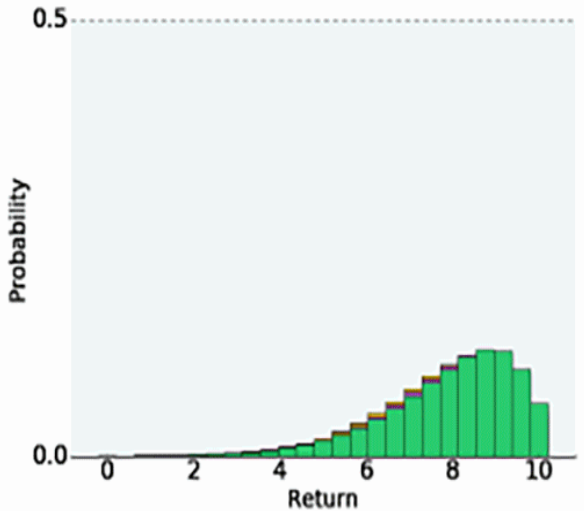
What can Deep Learning do?: Computer Vision



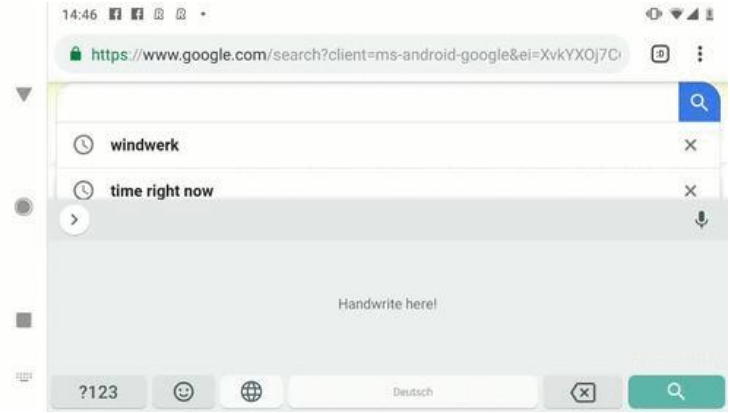


What can Deep Learning do?: Game Playing

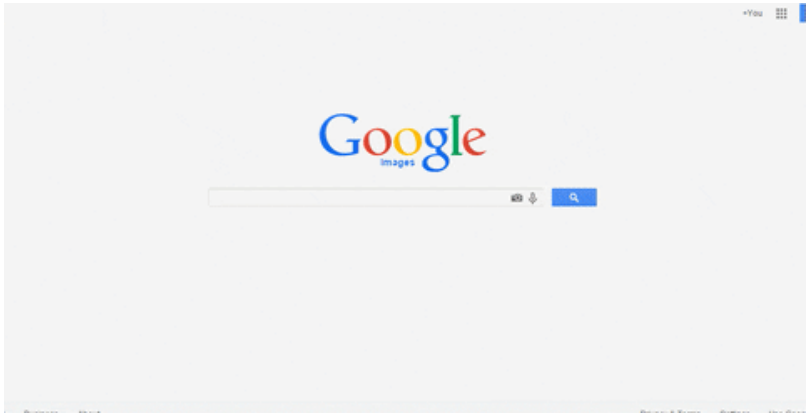




What can Deep Learning do?: Many More!



Handwriting Transcription



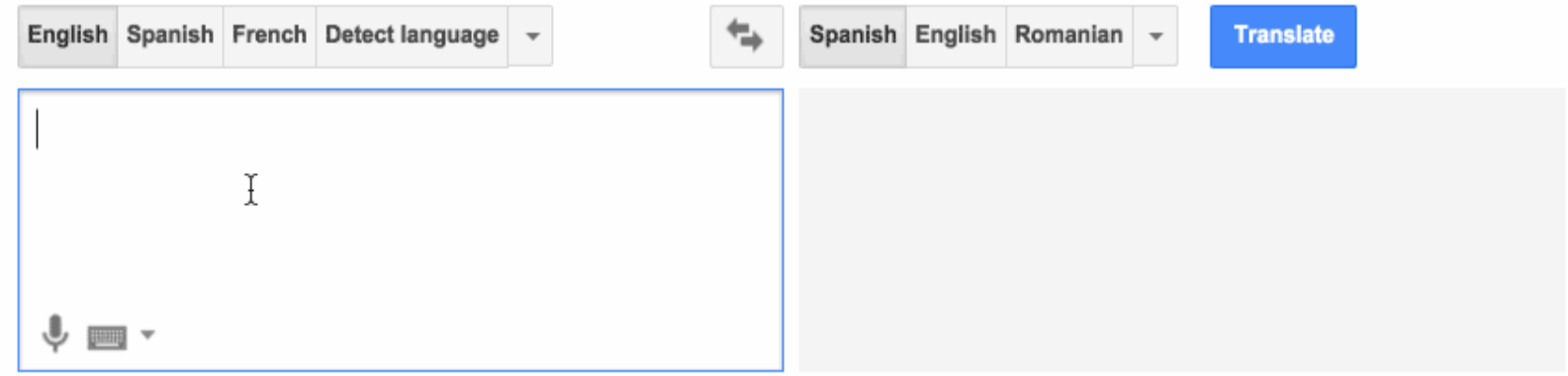
Search by Image

Generate fake images

What can Deep Learning do?: Many More!

AlphaGo beats Lee Sedol (2016)

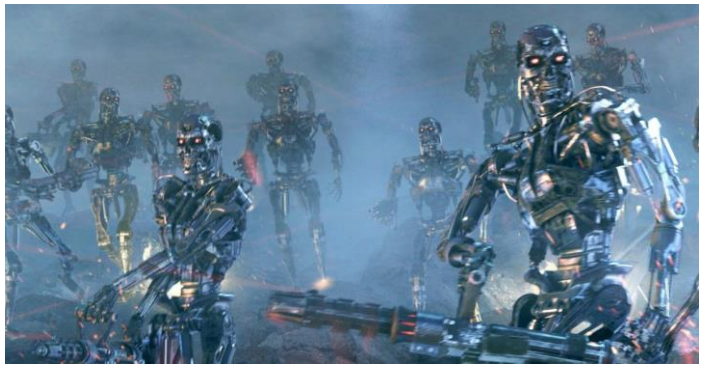
Self-driving car (Tesla)



Machine Translation

What CAN'T Deep Learning do? (as of 2019)

Love



World domination

Tell intentionally funny jokes

Beat humans at debate[1]
(IBM Project Debater)

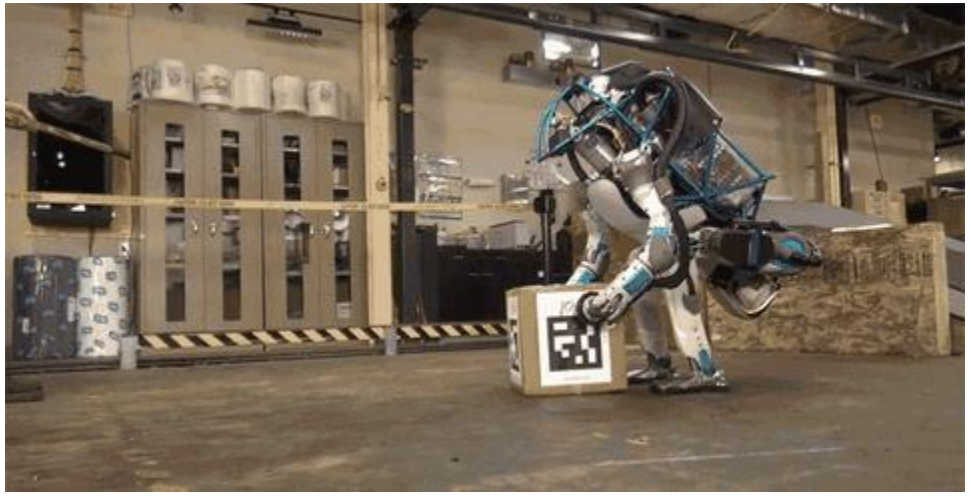
Make ethical decisions

Save the environment[2] **(?)**

1: https://edition.cnn.com/2019/11/21/tech/ai-cambridge-university-debate/index.html
2: https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/

What ISN’T ENTIRELY Deep Learning?

- Deep Learning is **not** necessarily used in certain real world applications
- **Not all** autonomous systems, robotics are entirely reliant on Deep Learning
- Efforts are being made to improve existing applications with Deep Learning

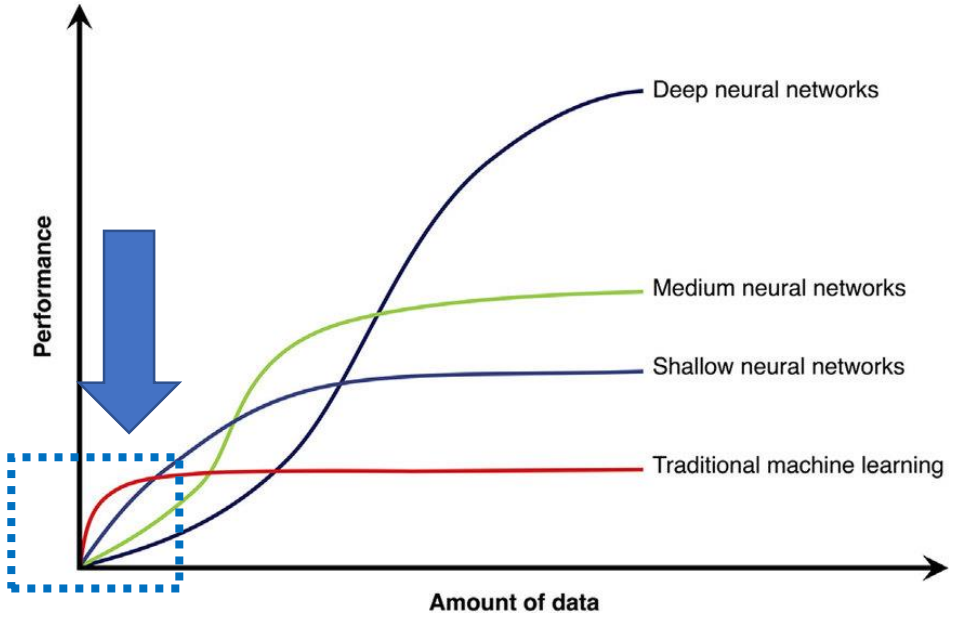


1: https://www.bostondynamics.com/
2: https://www.vox.com/2018/2/28/17059184/alphabet-google-waymo-self-driving-consumer-trust

When to use Deep Learning?

(Rules of thumb) [1]

- **When you have a lot of data**
- **When you have unstructured data**[2]
  - e.g. audio signals, images, text
- **Supervised learning**[3]
  - This is where AI is most lucrative
- **Reinforcement learning**
  - Great success has been shown in playing games

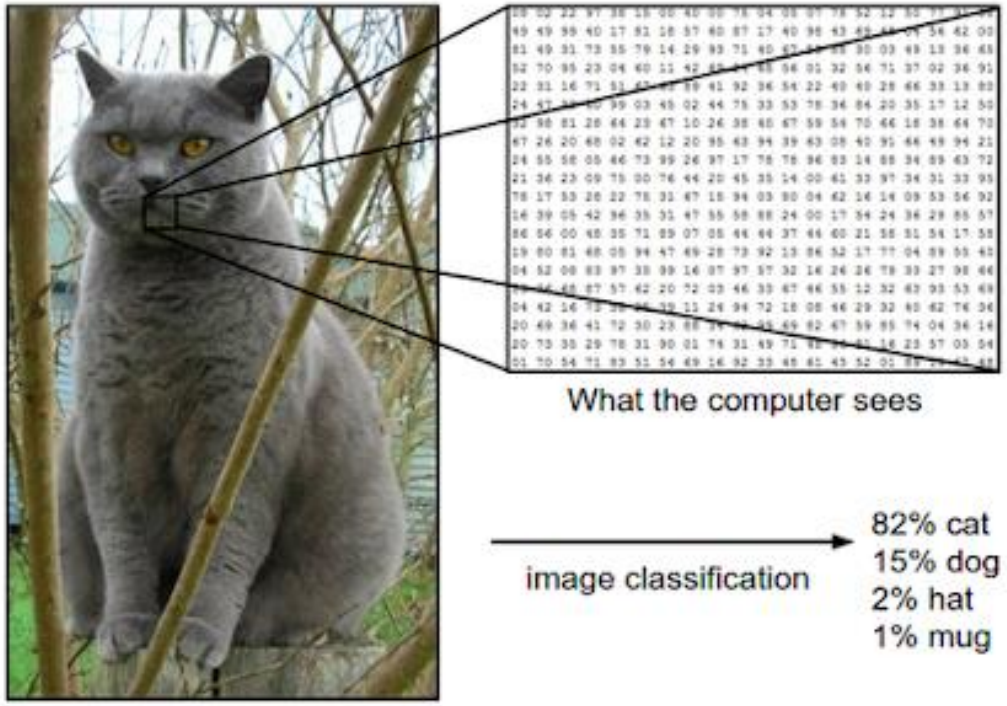


Sometimes using classical methods can yield similar or better results

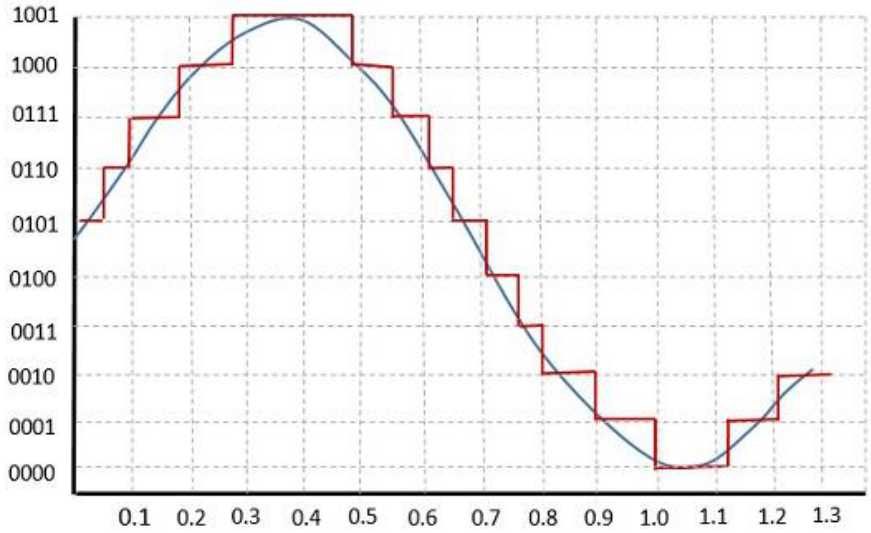
1: Deep Learning is currently in very active research so you can still use it for other problems but there's no guarantee it will be better than classical methods
2: Structured data works well with both deep learning and classical methods whereas unstructured generally works better with deep learning
3: Unsupervised/Semi-supervised learning has shown success in research but not commercial as far as I know

Unstructured data

Image



Audio



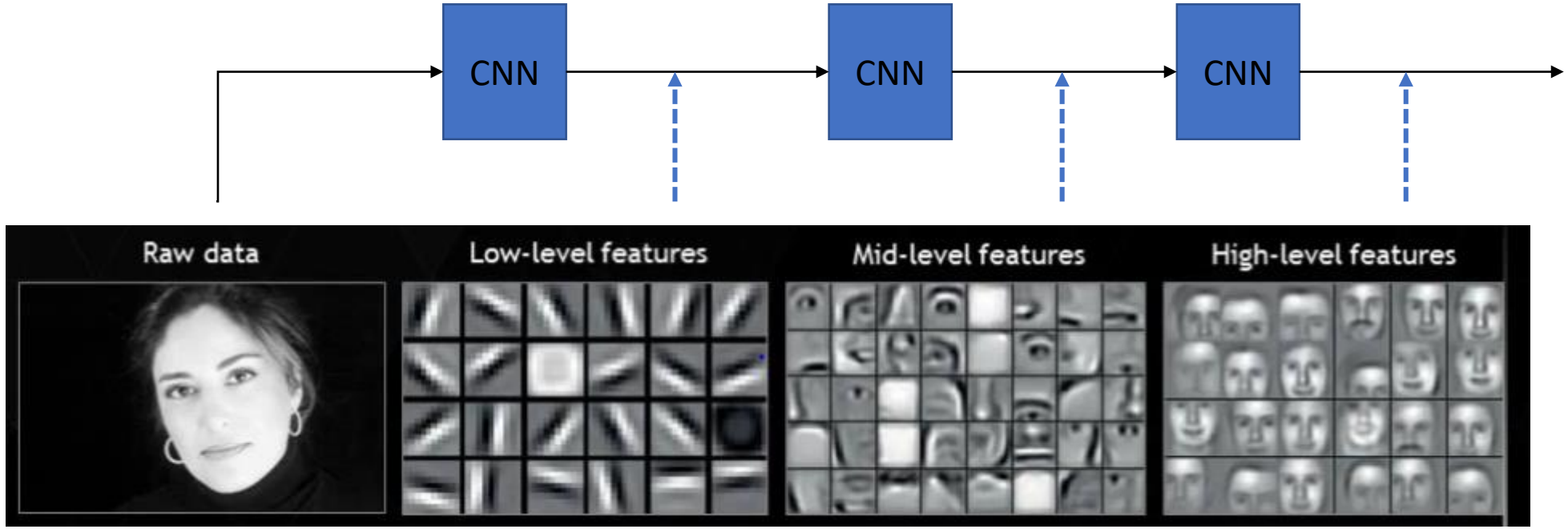
Are Humans Obsolete?

- Certain factors in Deep Learning can sometimes lead to **unintended consequences**[1]
- Humans are still necessary to ensure the safety and functionality of AI systems

1: MIT Deep Learning Basics: Introduction and Overview Lex Fridman https://www.youtube.com/watch?v=O5xeyoRL95U

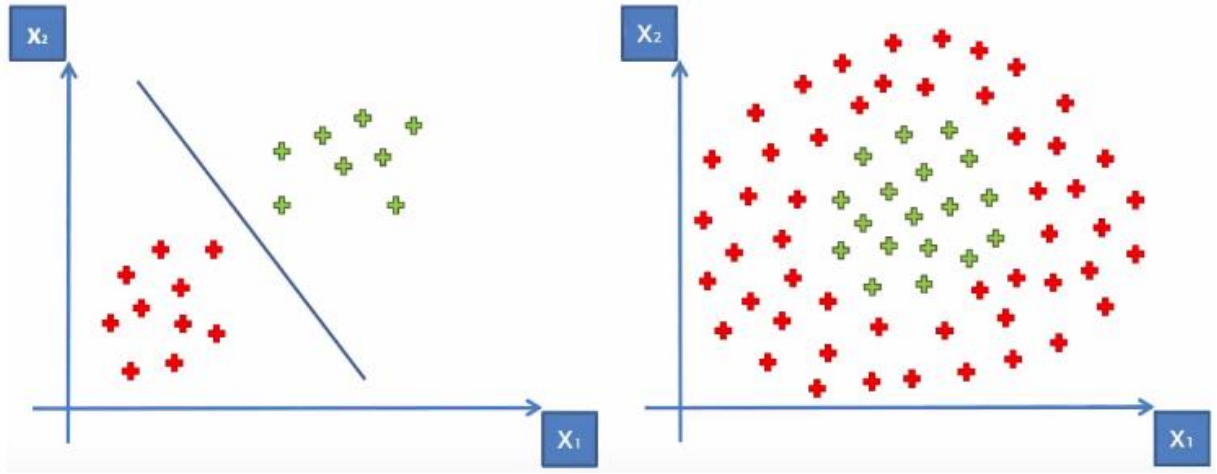
Deep Learning Intuition

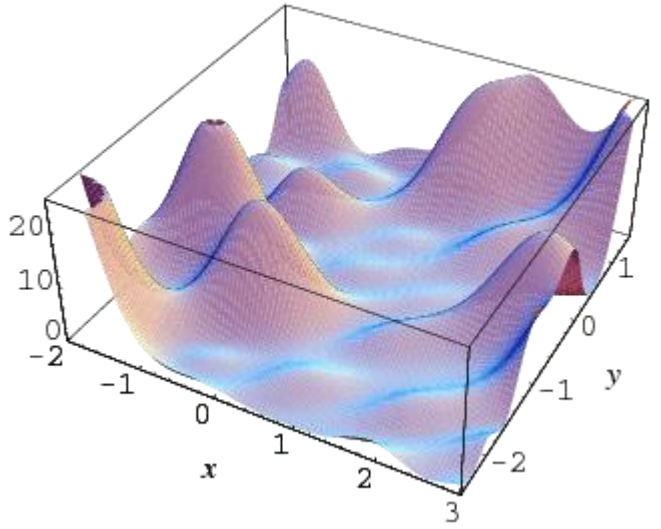
- Deep Learning is **Representation/Feature Learning**



Deep Learning Intuition

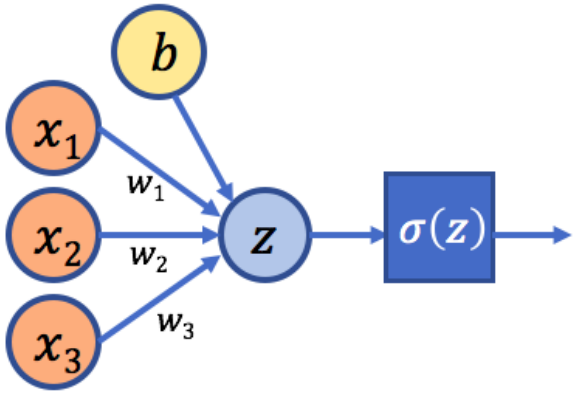
- We would like to learn a **model** or **function** that will give us a desired output given a specific input
- Usually these functions will be **too complex** and highly dimensional for humans to design by hand

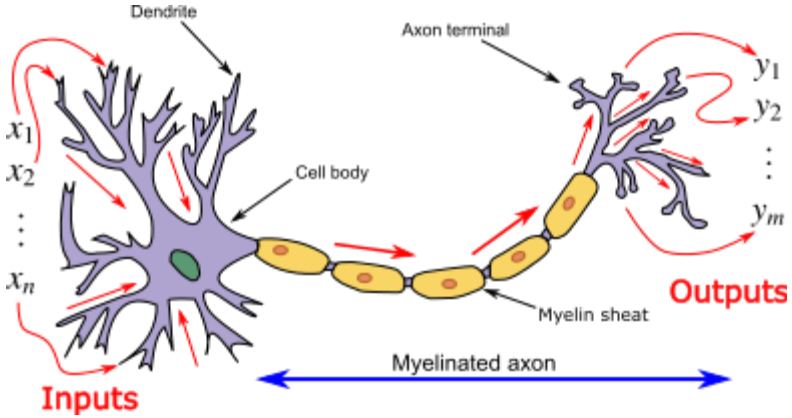




Deep Learning and the Human Brain

- **Not** entirely similar
- Artificial Neural Networks are **vaguely inspired** by biological neural networks
- A lot of effort being put in to understand how exactly our brain works

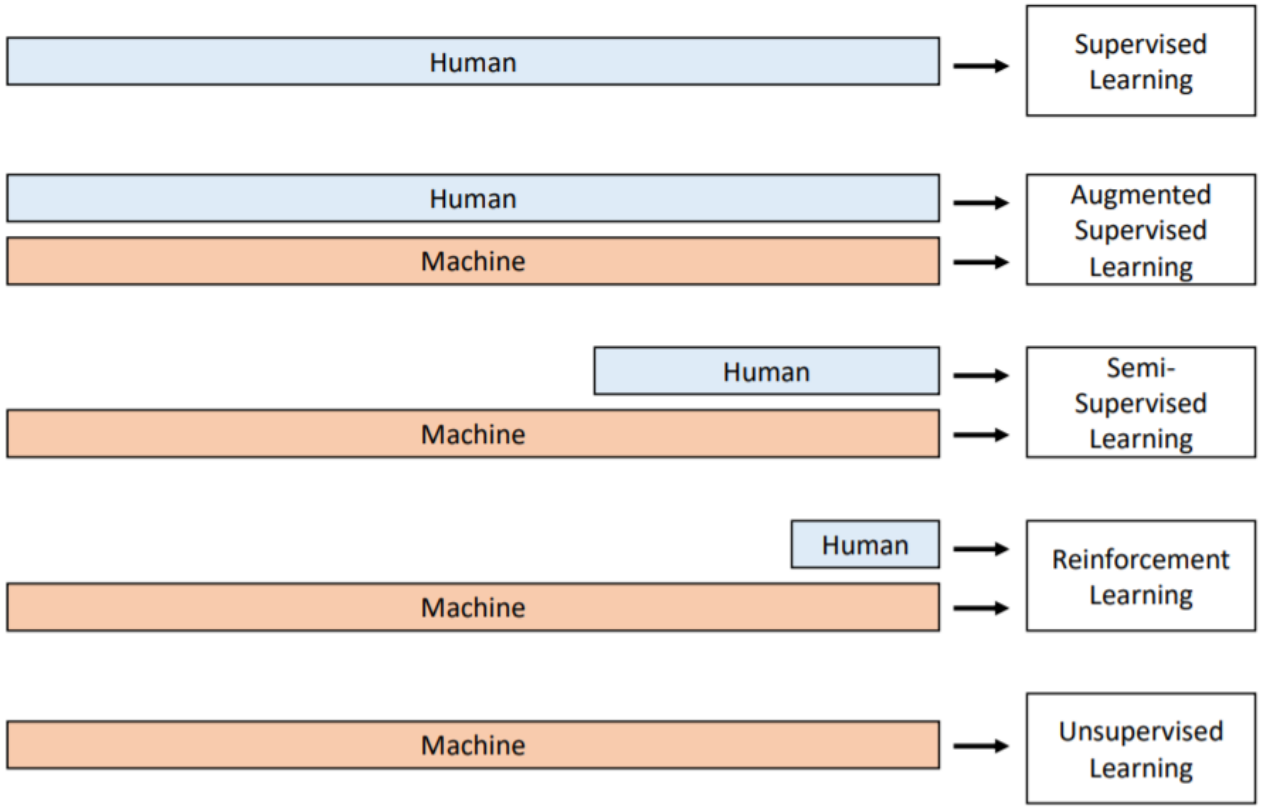




Types of Learning

- **Supervised Learning**
  - Learn from labelled data (input and target)
  - e.g. map English sentences to corresponding sentences in Mandarin
- **Unsupervised Learning**
  - Learn from unlabelled data
  - e.g. learning important features in data without labels
- **Self-supervised Learning**
  - Learn from data labelled by extracting information from the input data
  - e.g. predict future frames in videos
- **Reinforcement Learning**
  - Learn the optimal decision given the current environment
  - e.g. playing chess, driving a car

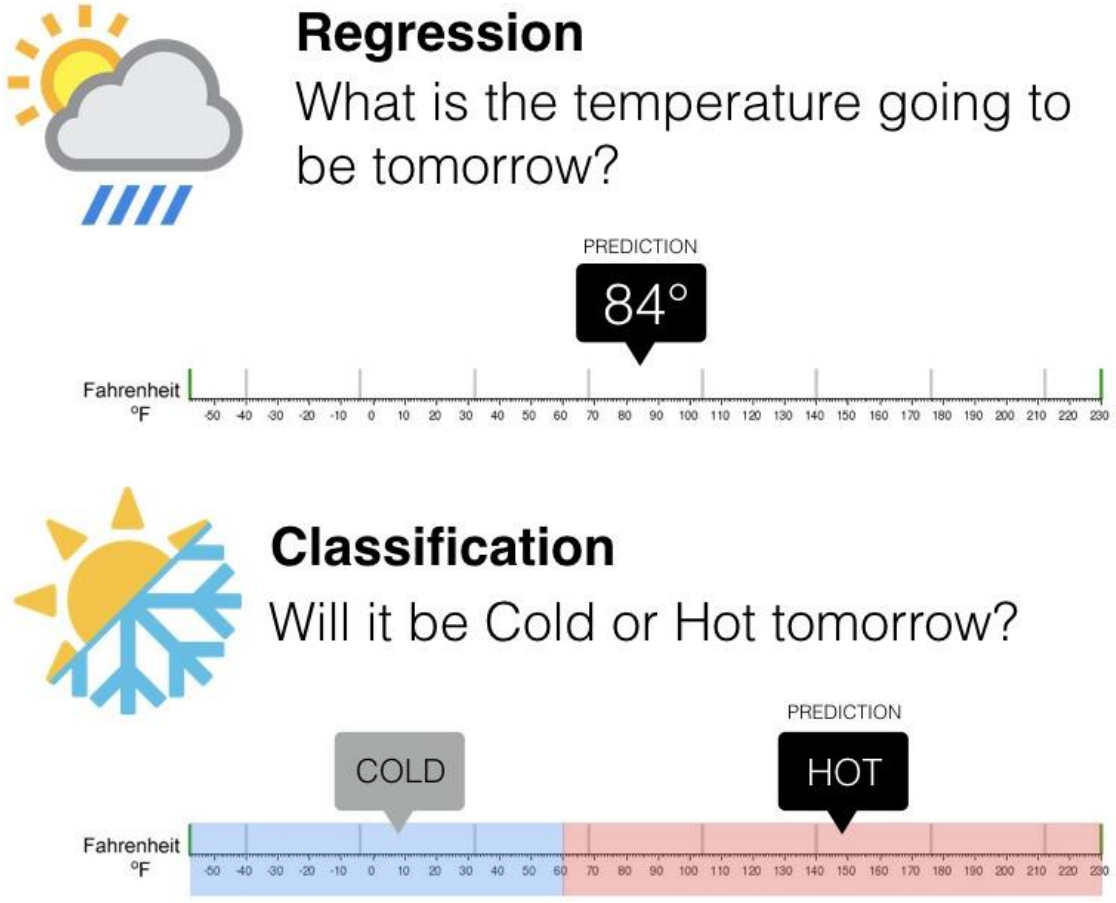
Types of Learning



1: MIT Deep Learning Basics: Introduction and Overview Lex Fridman https://www.youtube.com/watch?v=O5xeyoRL95U

Reinforcement Learning

Learning Tasks: Regression vs Classification



Deep Learning Frameworks

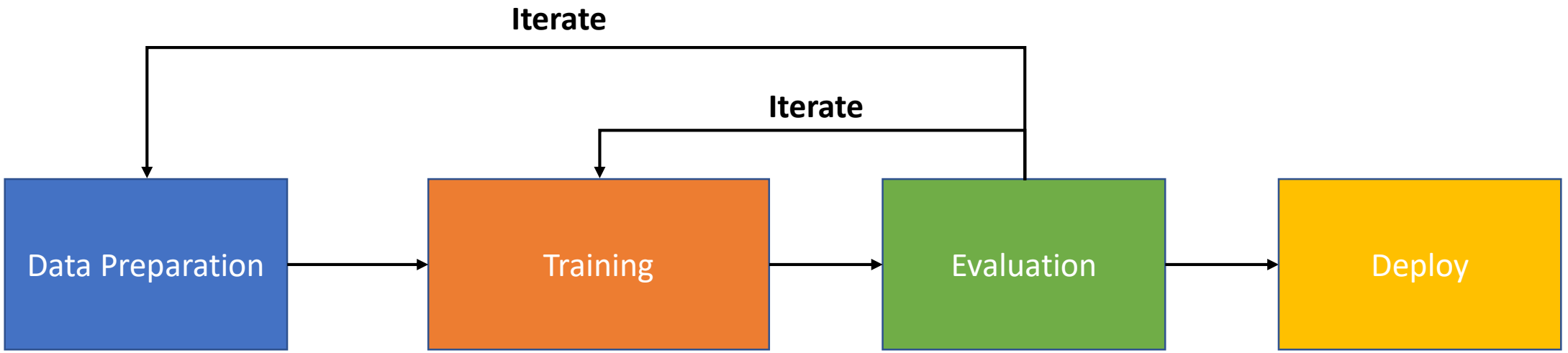
- **TensorFlow**
  - Developed by Google
  - Dominant in industry[1]
- **PyTorch**
  - Developed by Facebook
  - Dominant in research[1]
- **Both**
  - Primarily used with Python
  - Active development
  - Free and open source
  - Flexible libraries
  - Transferable skills

TensorFlow

PyTorch

1: https://thegradient.pub/state-of-ml-frameworks-2019-pytorch-dominates-research-tensorflow-dominates-industry/

Deep Learning Steps: Supervised Learning



- **Data collection**
- **Data splitting**
- **Data preprocessing**
  - Normalization
  - Augmentation

- **Implementation**
  - Network architecture
  - Loss function
  - Optimizer
- **Hyperparameter tuning**

- **Quantitative**
  - Accuracy
  - Loss
- **Qualitative**

- **App**
- **Web service**
- **Embedded system**

Data collection

“Data is the new Gold”[1]

1: https://info.kpmg.us/news-perspectives/future-ready/future-ready-data-is-the-new-gold.html

Data collection

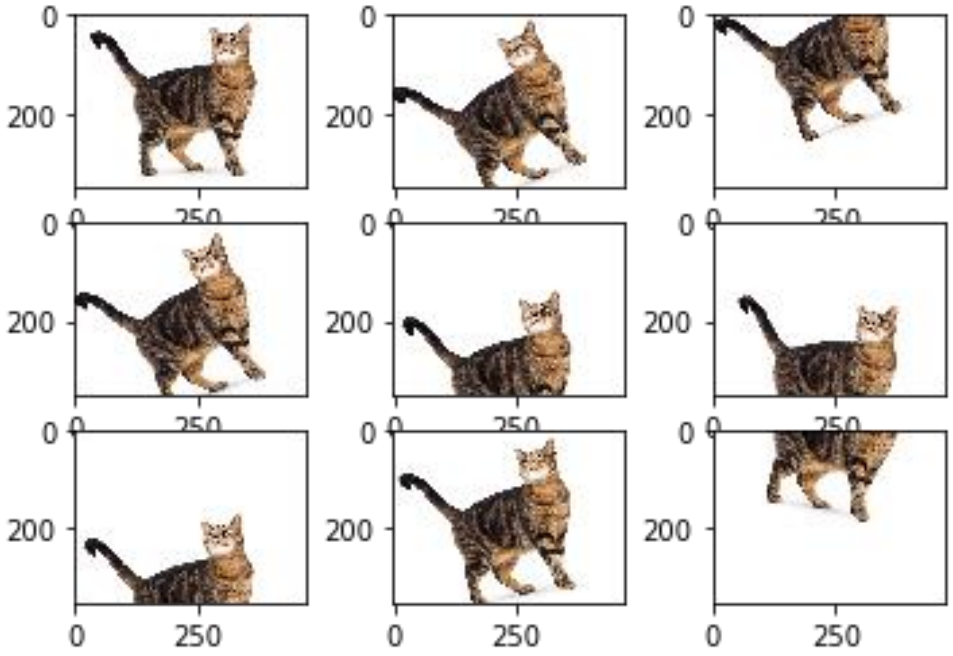
- **Collect input data and labels**
  - e.g. collect cat and dog pictures online and label cats as 0 and dogs as 1

( , 0) ( , 1)

- **There are <u>many</u> publicly available datasets online**
  - Collected and released by research groups
  - e.g Image Classification (ImageNet), Automatic Speech Recognition (LibriSpeech), Object Segmentation (MS-COCO)
- **Good resources**
  - Kaggle
  - GitHub
  - Google Dataset Search

Data preprocessing

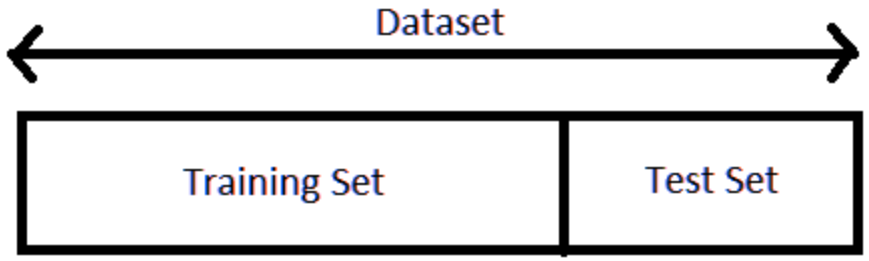
- **Data Cleaning**
  - Remove duplicates
  - Remove bad labels
  - Remove redundant data
- **Data Transformation**
  - Scaling
  - Normalization
  - Augmentation
  - Dimension reduction



Example of image augmentation

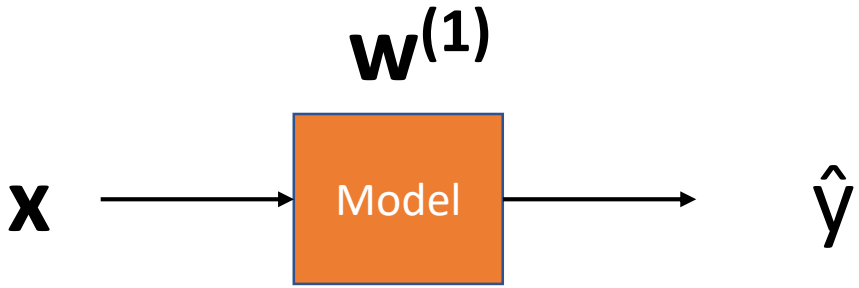
Data splitting

- Split into **training/testing** sets
- **Training** set: Training the model
- **Testing** set: Unbiased final evaluation of the model
- **Prevent overfitting!**



How do we train the model?

1. Forward pass to obtain prediction



2. Calculate error using cost function, J

$$e = J(\boldsymbol{w})$$

3. Use backpropagation to calculate gradient

$$\frac{\partial e}{\partial \boldsymbol{w}^{(1)}}$$

4. Update weights using an optimization algorithm (typically a variant of gradient descent)

$$\mathbf{w}^{(2)} = \mathbf{w}^{(1)} - \alpha \frac{\partial e}{\partial \boldsymbol{w}^{(1)}}$$

Binary Classification

: 0

: 1

Forward propagation

x

model

$\sigma(z)$

activation layer

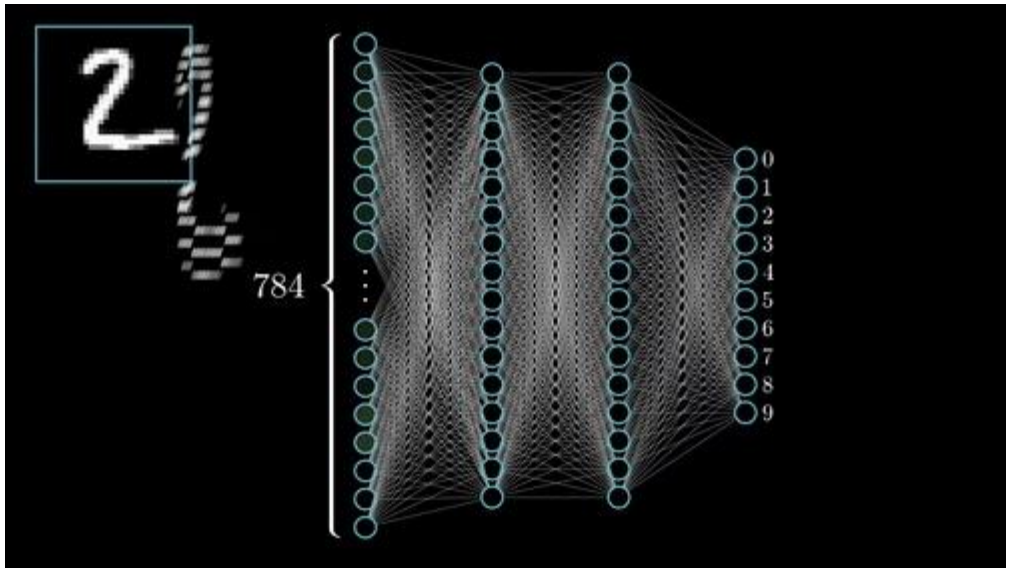
$P(y = 1|x) = 0.85$

$0.85 > 0.5$

$\hat{y} = 1$

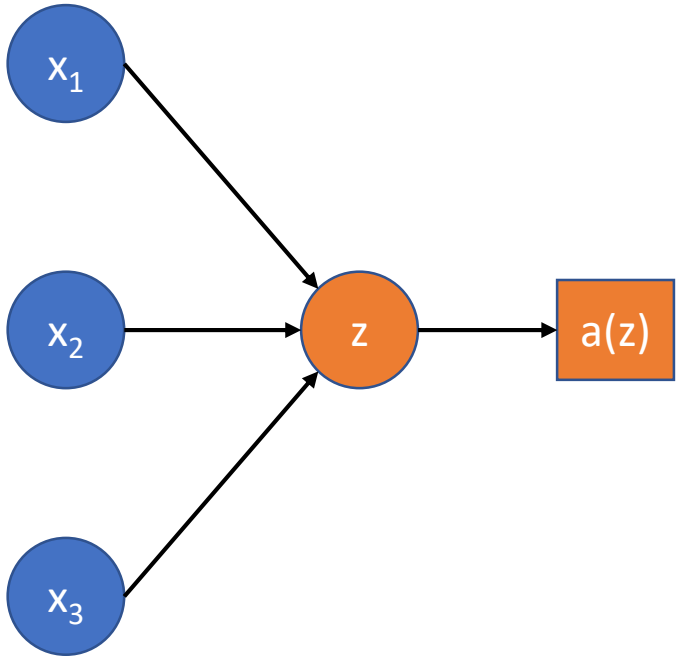
Loss function: Binary cross-entropy loss

Neural Network

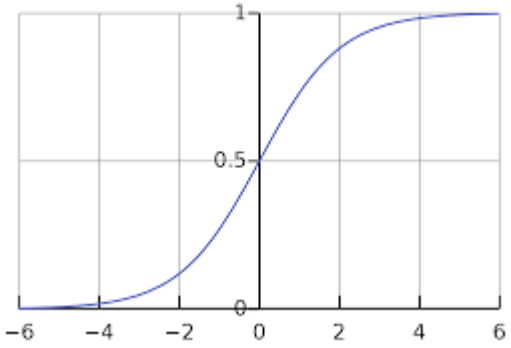


Neural Network GIF from https://www.youtube.com/channel/UCYO_jab_esuFRV4b17AJtAw

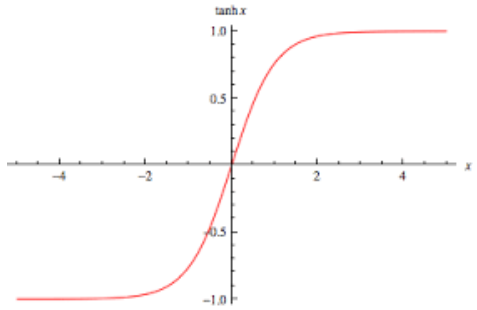
Activation Functions



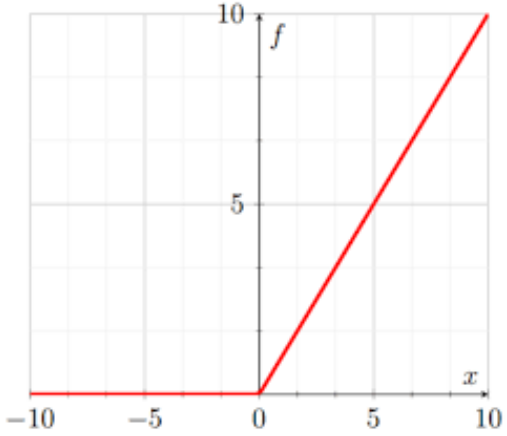
Sigmoid(z) = $\frac{1}{1+e^{-z}}$



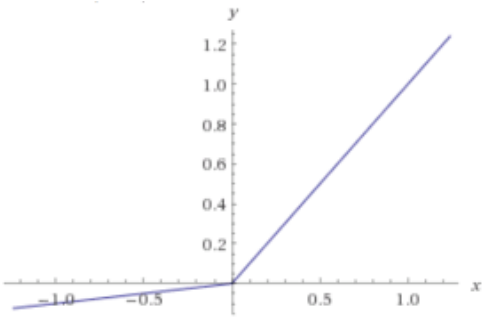
Tanh(z) = $\frac{e^{z}-e^{-z}}{e^{z}+e^{-z}}$



ReLU(z) = max(0, z)

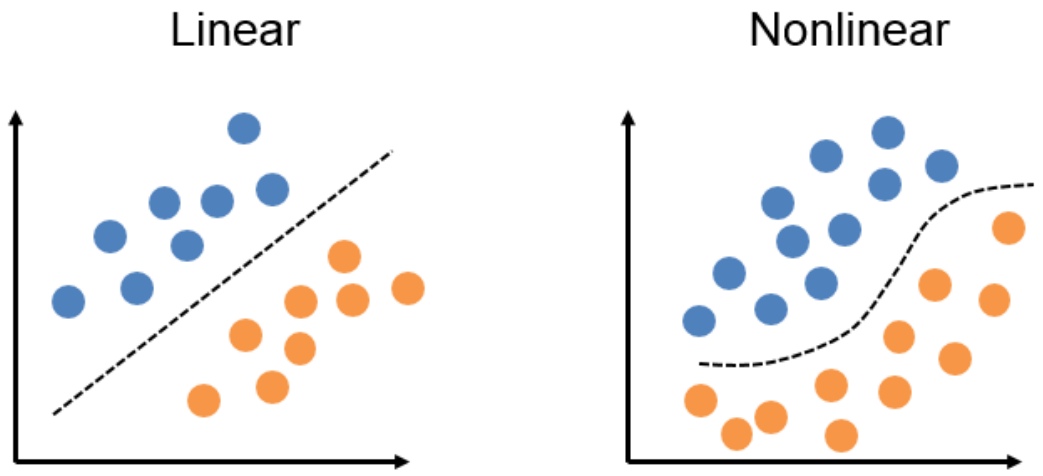


Leaky_ReLU(z) = max(0.1z, z)



Why Activation Functions?

- Specifically we want **non-linear** activation functions
- To allow our model to learn **non-linear** mappings
- Most input-output mappings we would like to learn are **non-linear**



* The activation function should also be **differentiable**

Optimization: Loss Calculation and Back Propagation

x

Forward Propagation

model

$\sigma(z)$

$P(y = 1|x)$

predicted

= 0.85

Loss

Error

Back Propagation

Update model weights

Error Gradient

$y = 1$

target

Optimization: Cost function

A measure of how **different** our **predicted** value is to the **actual** value

Examples

Mean Squared Error

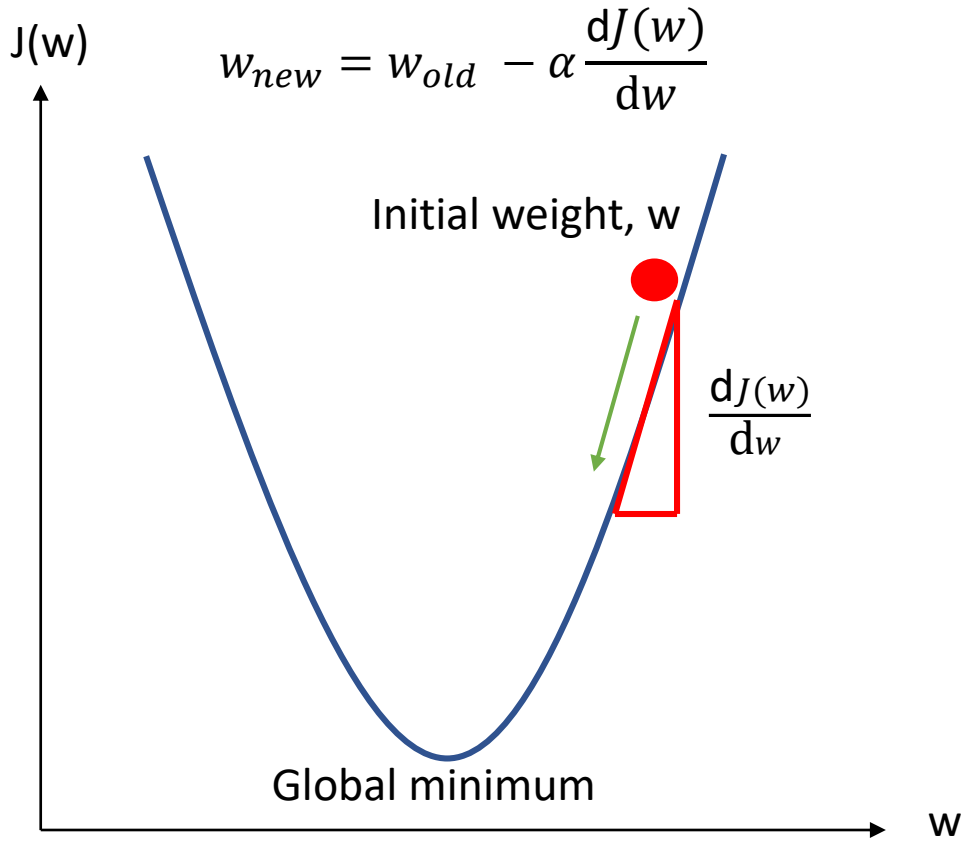
Regression : $(y_i - \hat{y}_i)^2$

Binary Cross-Entropy

Classification : $-y_i \log \hat{y}_i - (1 - y_i) \log(1 - \hat{y}_i)$

Optimization: Gradient Descent

- Method to optimize our model and find our optimal weights
- We want to find the weights, w that minimize our cost function, J(w)
- Currently, there are many variants to improve standard gradient descent

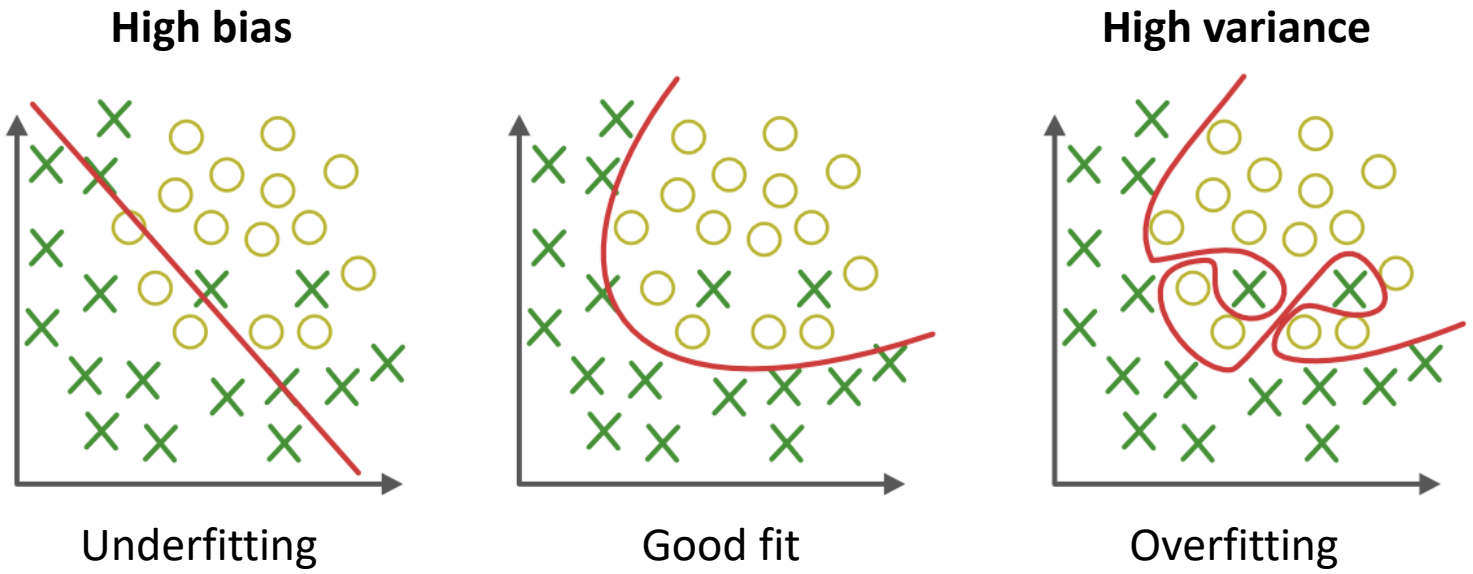


Evaluating your Model

- **Identify how well the model performs**
- **Identify how well the model generalizes to unseen data samples**
- **Quantitative analysis**
  - Use performance metrics
- **Qualitative analysis**
  - Useful for visual based output

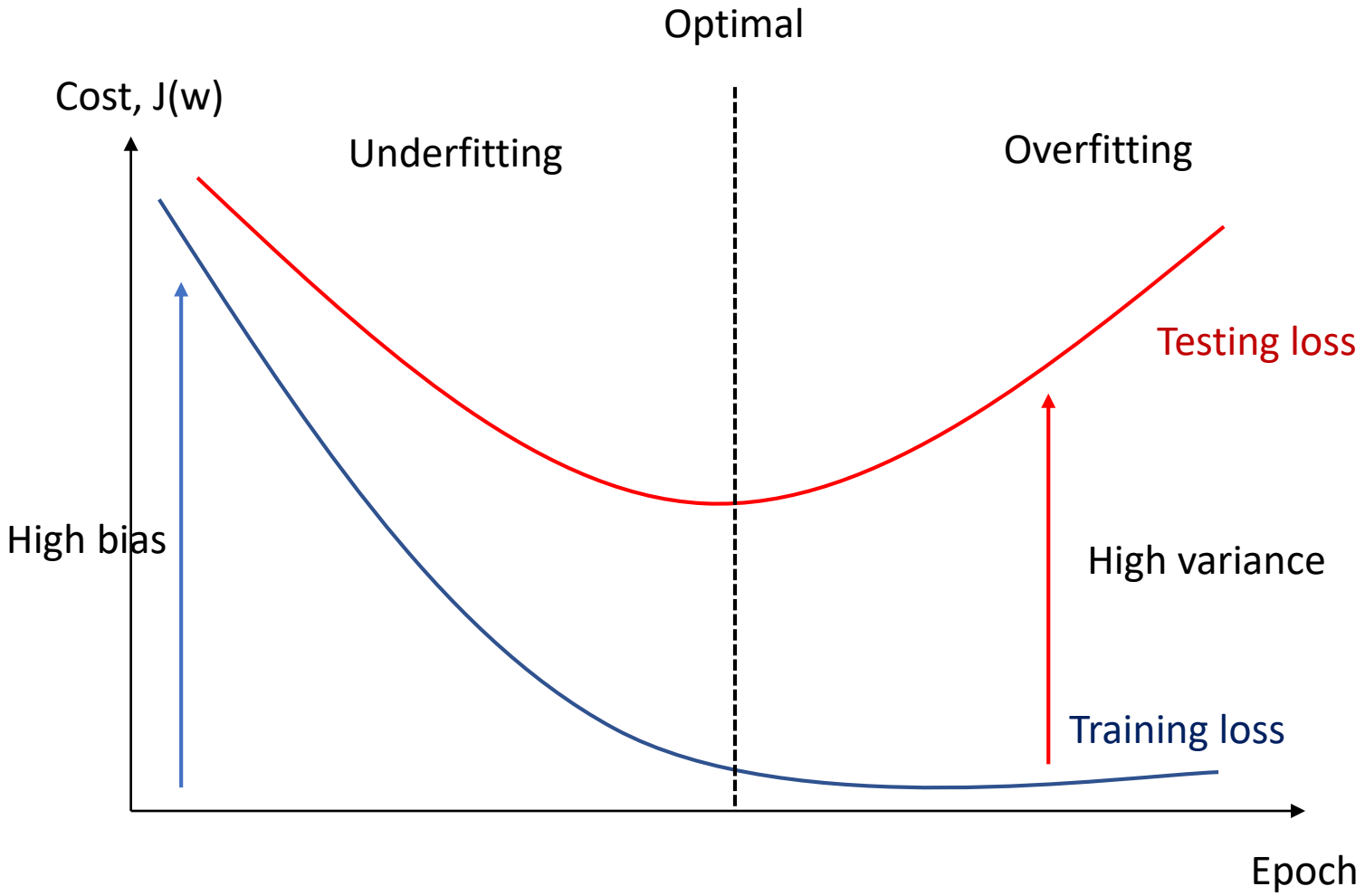
Possible Issues: Underfitting and Overfitting

Understanding the model's ability to **generalize** to unseen data



Graphs from https://towardsdatascience.com/underfitting-and-overfitting-in-machine-learning-and-how-to-deal-with-it-6fe4a8a49dbf

Possible Issues: Underfitting and Overfitting



How do we deal with overfitting? - **Regularization**

Next Steps

- **Fix Problems**
  - Is the model performing as expected?
- **Dataset**
  - Fix mislabeled data
  - Add more data to cover the worst performing samples
    - e.g. add more cloudy images
- **Hyperparameter tuning**
  - Find the best performing model
- **Regularization**
  - Prevent overfitting
- **Improving the model**
  - Updating the loss function
  - Updating the model architecture

Cat?

Model Tuning

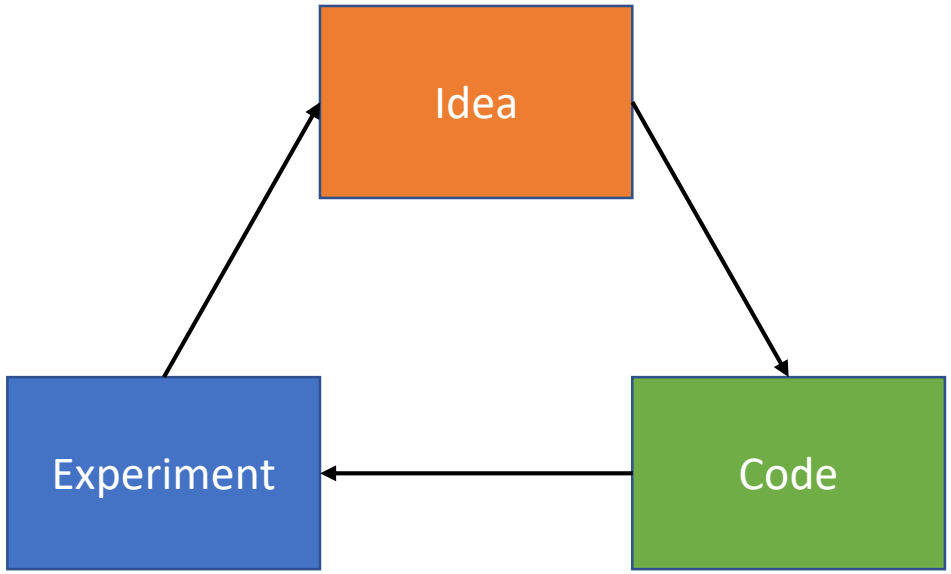
Tweak the network until we find the configuration that gives us the best performance

We can tune

- **Size of network**
  - Number of hidden units
  - Number of layers
- **Activation function**
- **Cost function**
- **Optimizer**
- **Weight initialization**
- **Types of layers**
- **Batch size**
- **Learning rate schedule**
- **…. a lot more!**

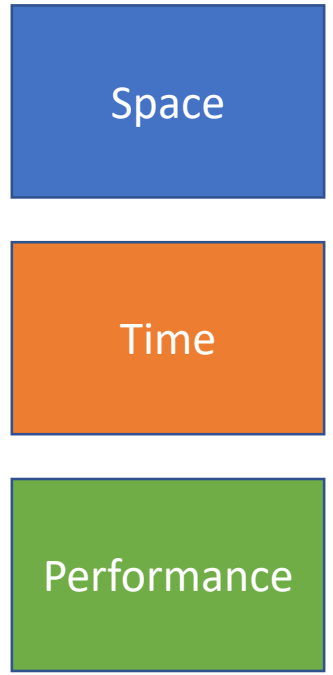
Machine Learning Research is Iterative

- **Finding good models is empirical**
- **Research cycle:**
  1. Develop algorithm
  2. Implement algorithm and train model
  3. Evaluate model and identify weakness
  4. Repeat until satisfied

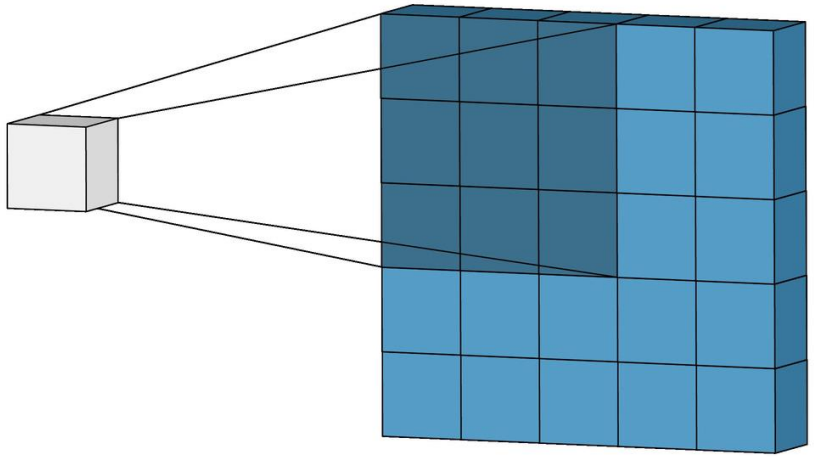


Improving Neural Networks

- **Model size**
- **Model training time**
- **Model performance**
  - Accuracy
  - Inference speed

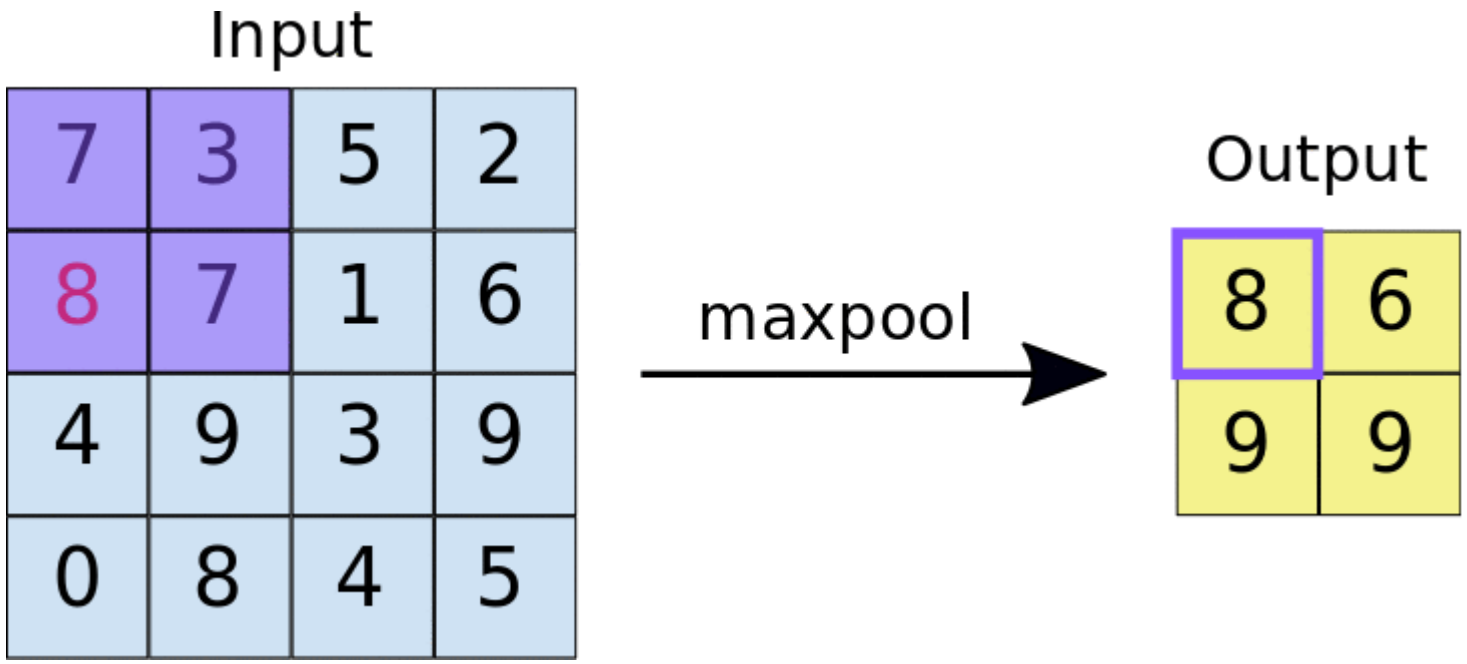


Convolutional Neural Networks: Convolutional Layer



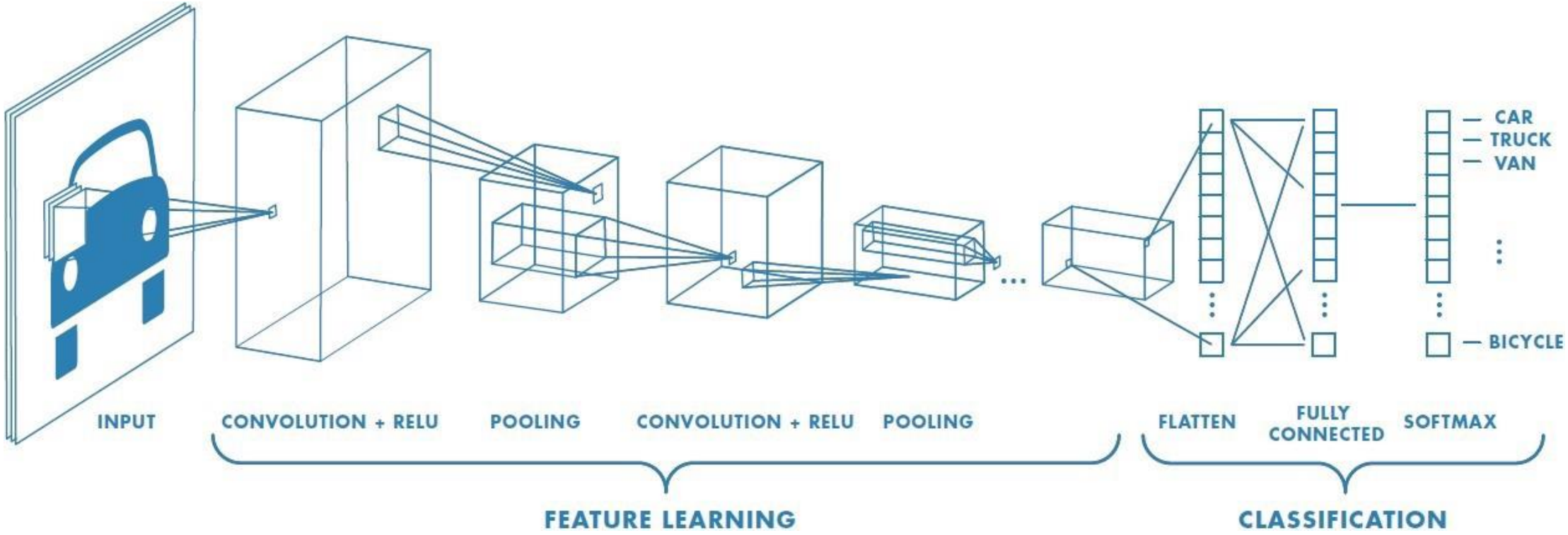
Convolutional Layer GIF from https://blog.usejournal.com/convolutional-neural-networks-why-what-and-how-f8f6dbebb2f9?gi=3faa9b8cfe4c

Convolutional Neural Networks: Max Pool



Max Pool layer from https://developers.google.com/machine-learning/practica/image-classification/convolutional-neural-networks

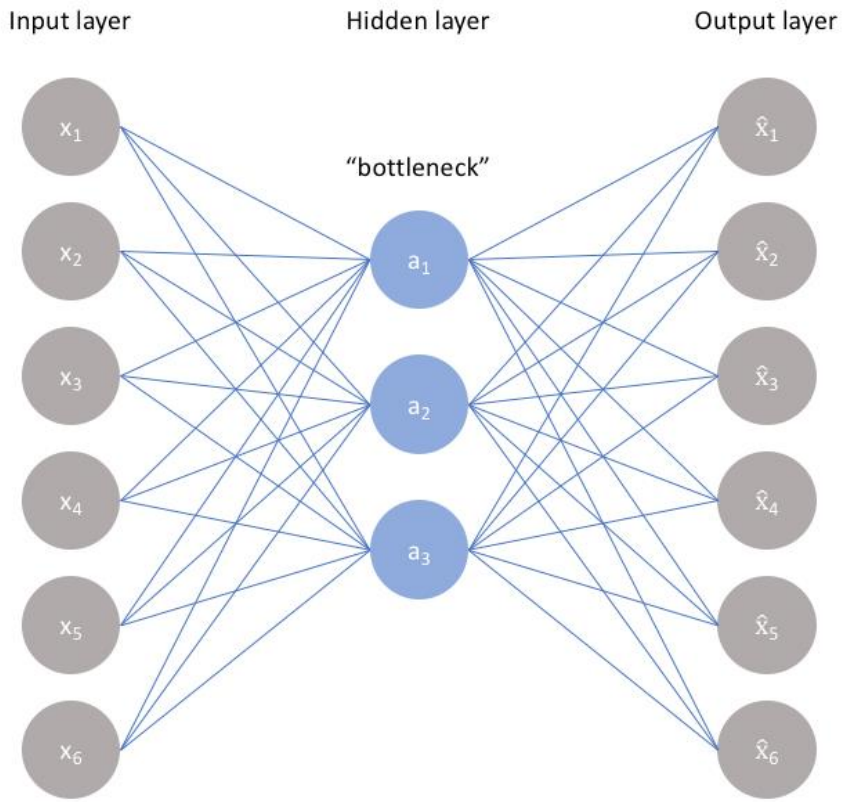
Convolutional Neural Networks: Putting it all together



Convolutional Network from https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

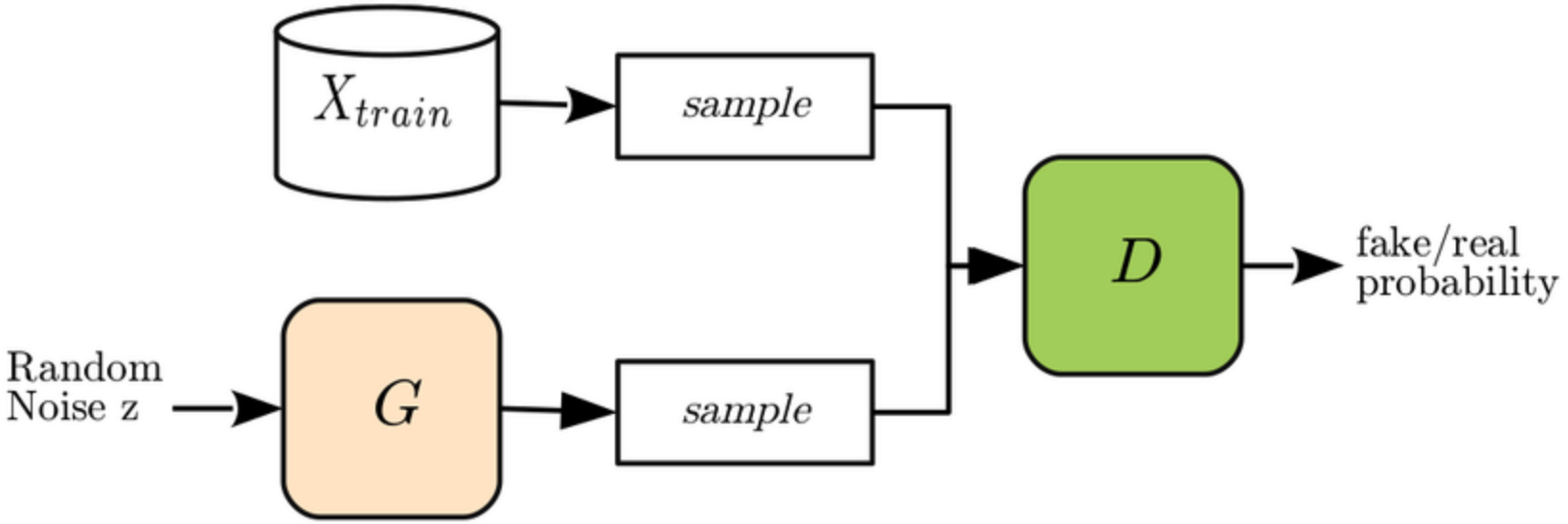
Popular Networks: Autoencoders

- Learn a **latent** representation of the data by **reconstructing** the original input
- Unsupervised learning



Popular Networks: Generative Adversarial Networks

Discriminator tries to distinguish real from fake



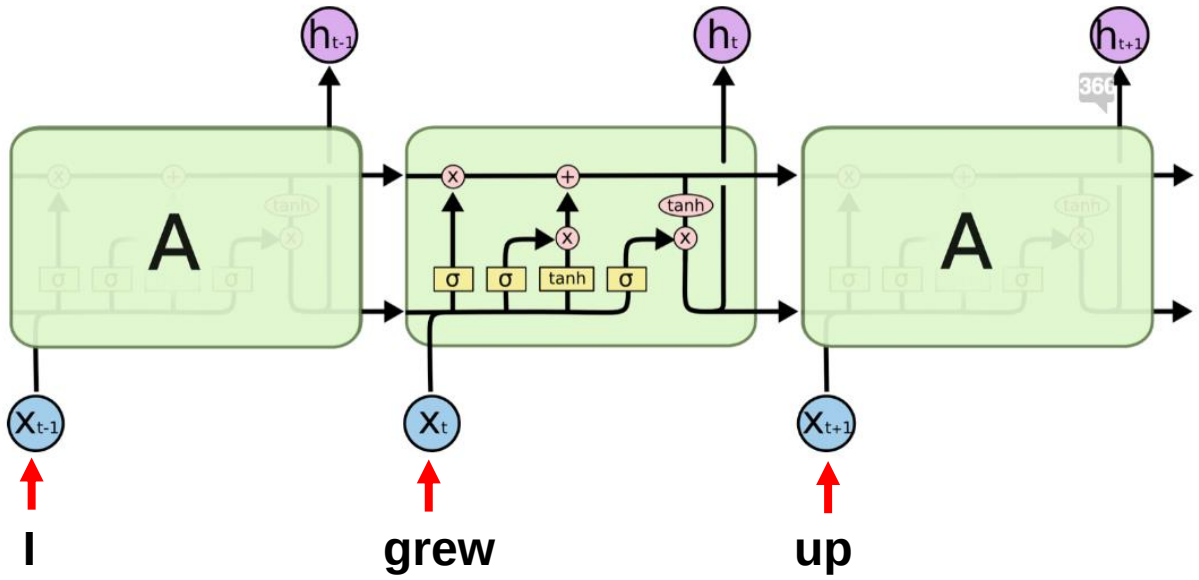
Generator tries to fool the **Discriminator**

1: Goodfellow, Ian, et al. "Generative adversarial nets." Advances in neural information processing systems. 2014.

Popular Networks: Long Short-Term Memory (LSTM)

- Conceived from a family of networks called Recurrent Neural Networks
- Useful for sequence learning e.g. Natural Language Processing
- Learn what to remember and what to forget

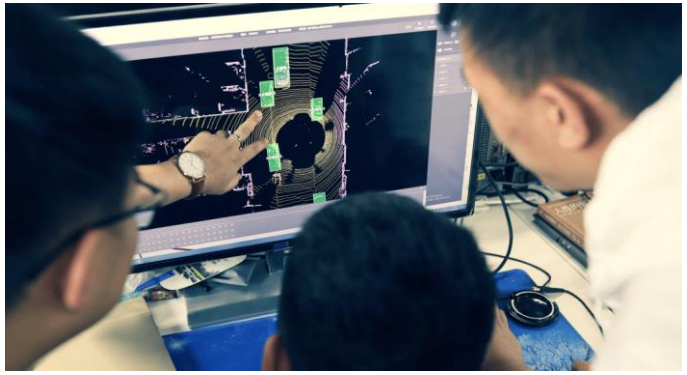
“I grew up in France. My name is Teddy. I speak fluent French”



Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." *Neural computation* 9.8 (1997): 1735-1780.

Barrier to Entry

- **Computational resources**
  - Deep learning research is computationally intensive
  - Finding a good model requires a lot of iteration
  - Good GPUs can cost a lot
- **Datasets**
  - Deep learning models are data hungry
  - Generally, the more data you have, the better your model will be
  - Some types of data are not easy to collect[1]
- **Expertise**
  - A lot of resources online makes it easy to learn
  - In-depth understanding takes some time
  - Competing with large companies for graduates



1: https://time.com/5518339/china-ai-farm-artificial-intelligence-cybersecurity/

Where are we now?

- Most big questions of intelligence have not been answered nor properly formulated[1]
- Research is happening all over the world
- Deep Learning Frameworks are constantly being improved
- More industries are adopting deep learning into their systems
- We have come a long way and we still have much left to do!

1: MIT Deep Learning Basics: Introduction and Overview Lex Fridman https://www.youtube.com/watch?v=O5xeyoRL95U

Key Points

- **Deep Learning** is a subset of **Machine Learning** which is a subset of **Artificial Intelligence**
- Deep Learning refers to learning with **many layers** of **Neural Networks**
- **Neural Networks** are a Machine Learning model that learns from data
- Deep Learning is **big** now and **growing**. It is impacting the world **globally**, affecting many aspects i.e. society, politics, economics, finance, industry, academics
- Deep Learning is **not magic**
- Deep Learning generally **benefits** from greater computation and large quantities of data
- There are various barriers to **large-scale** deep learning
- Deep Learning **is easy to get into if you are interested**! There are many courses available for **free** online.

Useful Resources

- **Coursera Deep Learning Specialization by deeplearning.ai**
  - Introductory course to Deep Learning
  - Good for beginners
- **Coursera TensorFlow in Practice Specialization by deeplearning.ai**
  - Tutorials on using TensorFlow
- **PyTorch Tutorials at pytorch.org**
  - Tutorials on using PyTorch
- **Deep Learning Book by Ian Goodfellow, Yoshua Bengio and Aaron Courville**
  - Introductory textbook on Deep Learning
- **GitHub**
  - Code examples
  - Datasets
- **Quora** or **Stack Overflow**
  - Asking questions
- **Lex Fridman Youtube Channel**
  - Podcasts
  - Lectures

Deep Learning is really big now so there's **a lot** of resources out there if you search for it!

Questions?