Introduction to AI

AR & BA

Contents

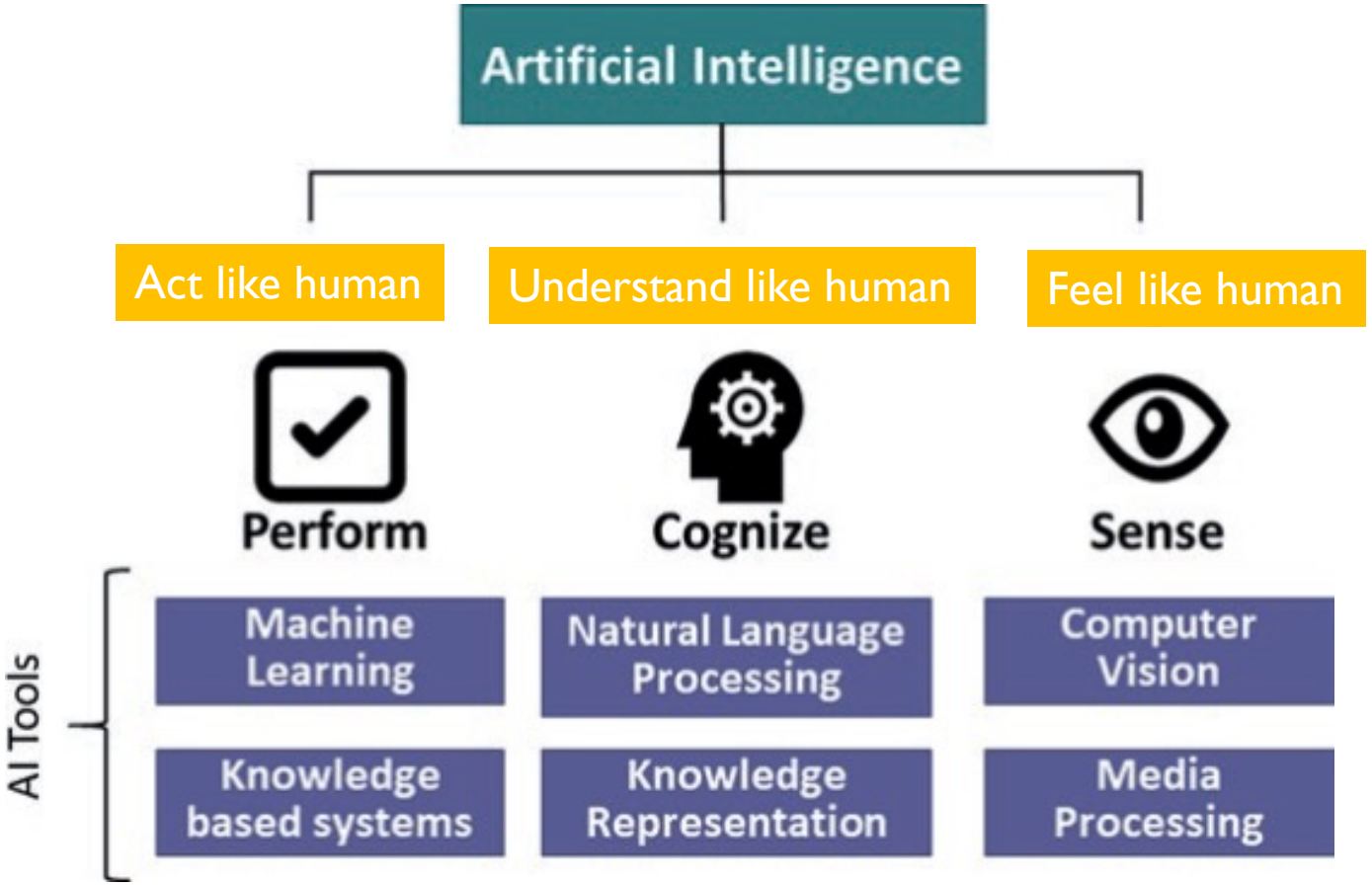
- Overview of AI Development
- The AI Capacity Framework
- Associated Technologies
- Challenges to AI

Artificial Intelligence

The theory and development of computer systems able to perform tasks normally requiring human intelligence.

-- Oxford Dictionary

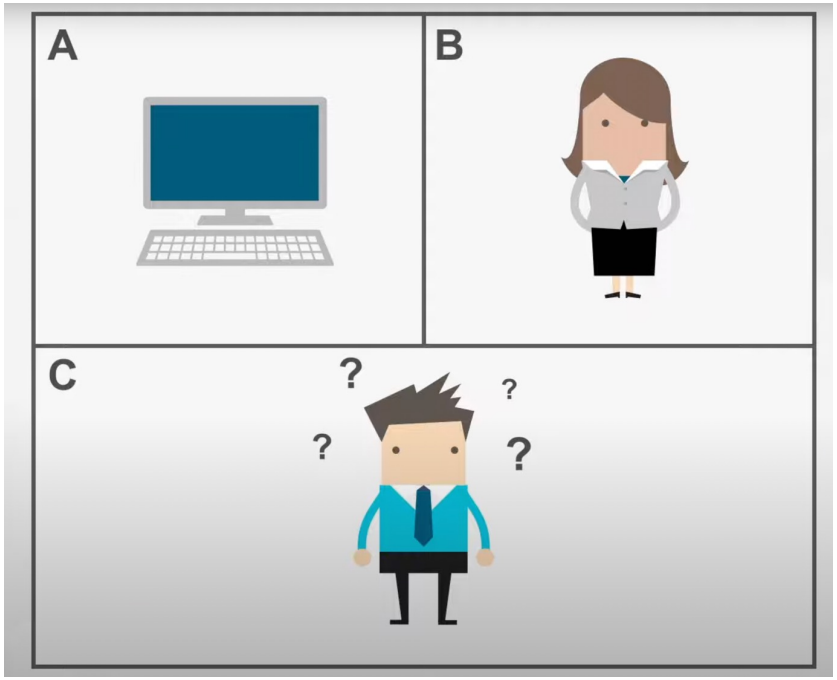
Artificial Intelligence



Whether a Machine is Intelligent?

- The Turing Test (1950)

Machine Respondent Human Respondent



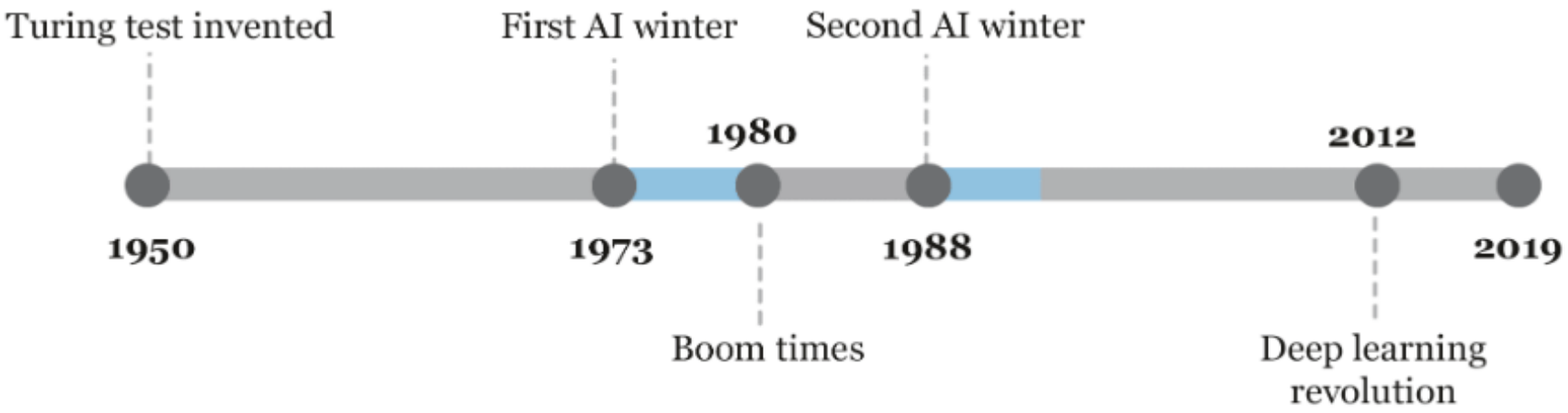
Human Questioner

Development of Artificial Intelligence

- The **Dartmouth Summer Research Project on Artificial Intelligence** in 1956, organized by John McCarthy, is the founding event of artificial intelligence as a research field.

- John McCarthy also founded the **Stanford Artificial Intelligence** Lab (SAIL) in 1963.

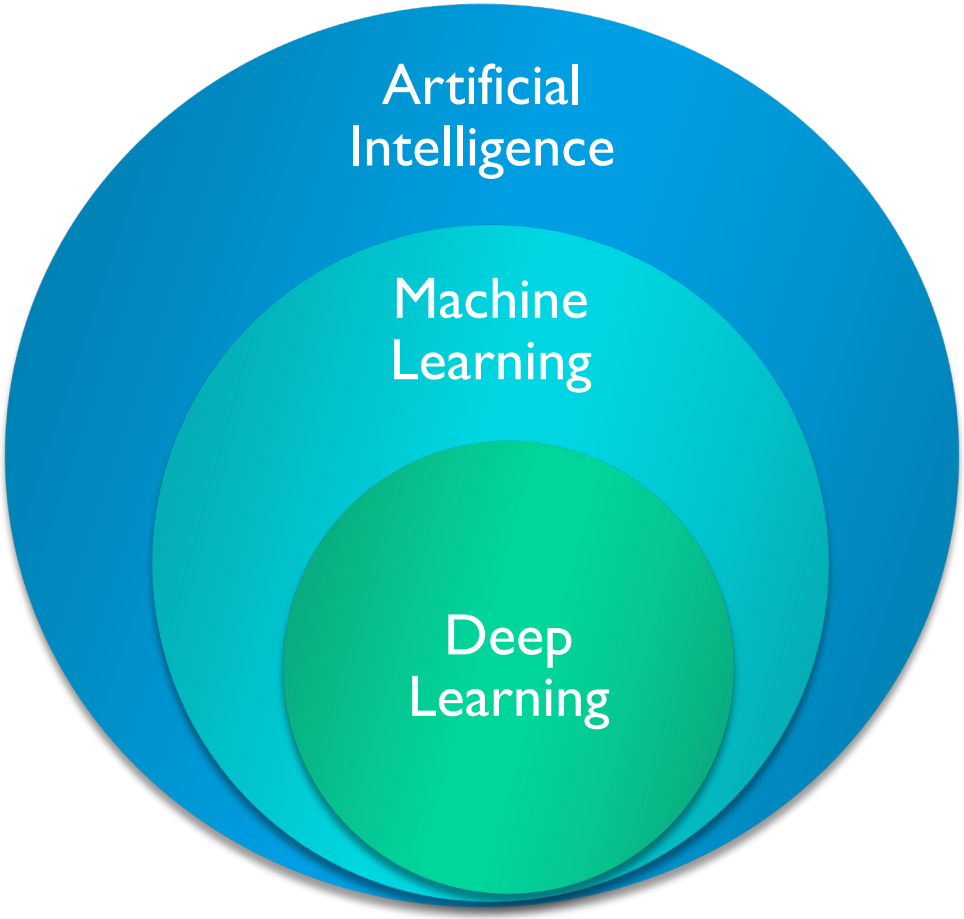
A Turbulent Journey of AI



Increased interest in 1950-60s and mid 1980s, both followed by an AI winter

An inflection point: expectations went high again.

Machine Learning vs. Deep Learning



Ability of a machine to imitate intelligent human behavior

A branch of AI technology, which allows a machine to automatically learn from data.

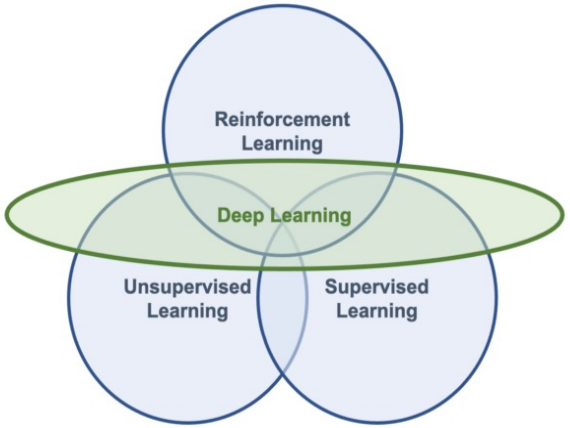
A particular ML method based on artificial neural networks.

Main Machine Learning Approaches

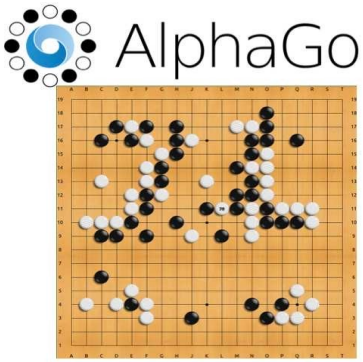
- **Supervised learning:** learn from labelled data, aiming to make predictions of a specific target.
  - Regression, classification

- **Unsupervised learning:** learn from unlabelled data.
  - Clustering, dimension reduction, association learning.

- **Reinforcement learning:** learn from its own experience (trial & errors), instead of training data.
  - e.g., learn the optimal actions in a dynamic environment to maximize the cumulative reward.



The Rise of Deep Learning
2010- onwards



Can AI Detect Deepfakes To Help Ensure Integrity of U.S. 2020 Elections?

Startup Deeptrace is racing to develop automated detection of fake videos and images as U.S. 2020 elections loom

By **Jeremy Hsu**

PRESS RELEASE

Stock Market Forecast: AI-Based Algorithm Shows Accuracy Up To 97% In S&P 500 and Nasdaq Predictions

Published: Aug 12, 2019 3:44 p.m. ET

CADE METZ BUSINESS 09.27.16 01:00 PM

An Infusion of AI Makes Google Translate More Powerful Than Ever

ACM TECHNEWS

How an AI 'cat-and-Mouse Game' Generates Believable Fake Photos

HEALTH AND SCIENCE

Google's DeepMind A.I. beats doctors in breast cancer screening trial

PUBLISHED THU, JAN 2 2020·8:13 AM EST

David Reid
@DAVYREID73

SHARE

Why Resurgence of Deep Learning Now?

- Though, Neural Networks date back decades (at least late 1950s), their resurgence in the last decade has been due to three main drivers:
  - **Big Data**: Access to larger (usually "digital") datasets and the ability to collect and store large datasets.
  - **Hardware**: Graphical Processing Units (GPU) which is super helpful for massive parallelization became commercially viable.
  - **Better algorithms**: Improved techniques implemented in public analytical frameworks e.g., TensorFlow, Keras, PyTorch, MxNet.

AI Winters

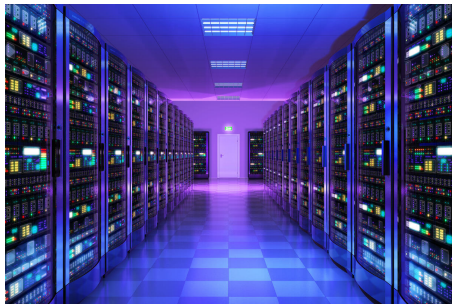
- First wave of AI winter (1974-1980)
  - Failure of a key project for Advanced Research Projects Agency (ARPA) and the **Mansfield Amendment** (1969) requiring ARPA to only fund projects with clear missions and objectives.
  - **Lighthill report** (1973) criticizing AI community's failure to reach its "grandiose objectives".

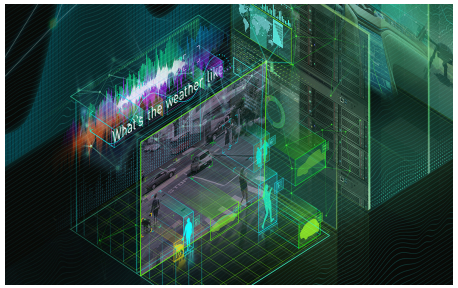
- Second wave of AI winter (1987-1993)
  - Failure of **expert systems** to meet the over-inflated expectations of large corporations.
  - Collapse of the associated hardware market (e.g., **Lisp machines**).

Lisp machines

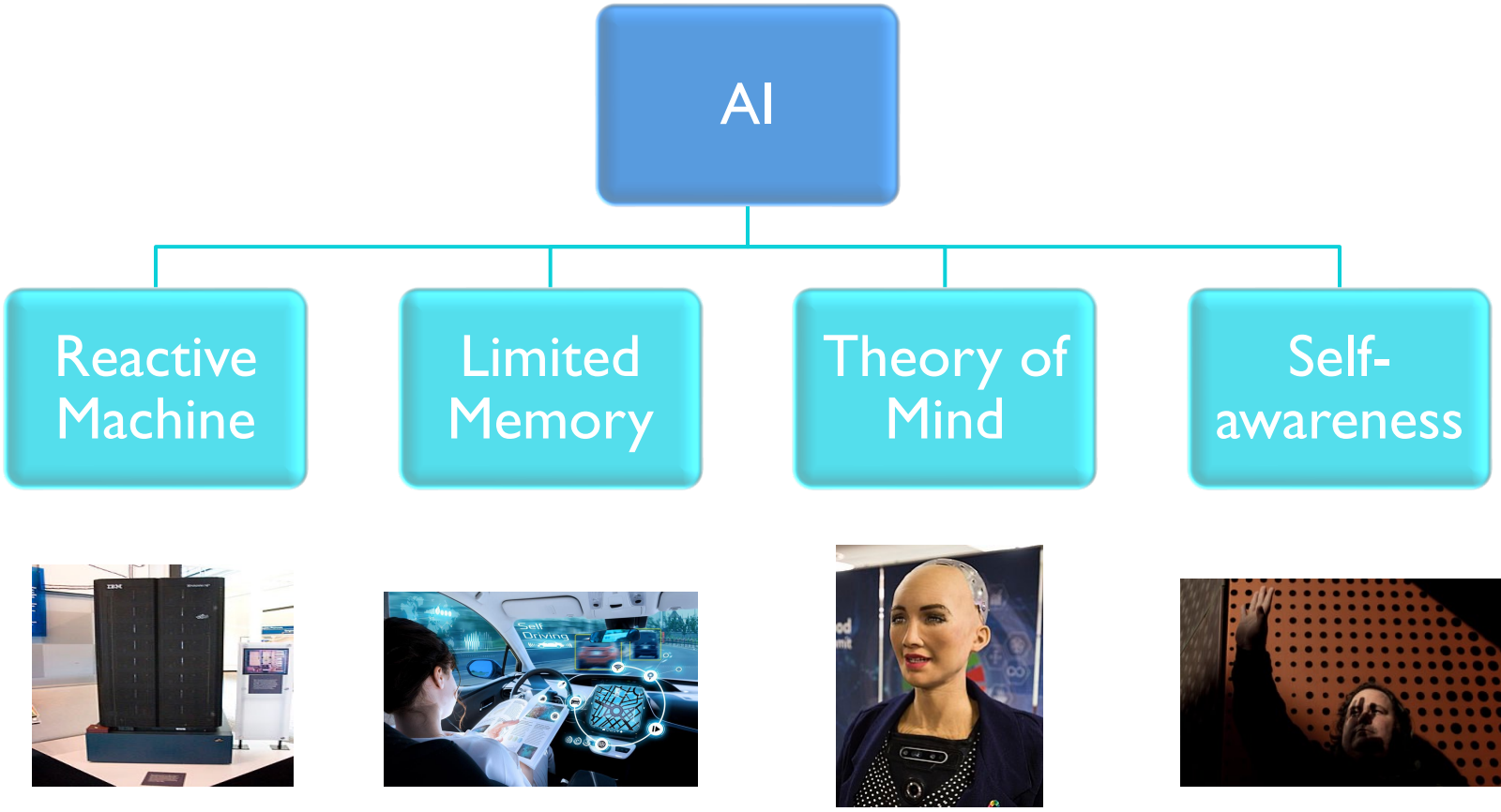
Drivers of Current Boom in AI

- The rise of big data
  - AI is worthless without data
- The role of cheap storage
  - Diminishing cost of data storage
  - The speed data can be accessed
- The role of fast processors
  - Chip performance doubled every 18 months
- Ubiquitous connectivity
  - Distributed computing & real-time processing
  - AI + Cloud Computing





Four Type of Artificial Intelligence



Reactive Machine

- **Reactive Machine** is the most basic form of AI. It works only with present data and doesn't store memories for future actions.
  - IBM Deep Blue sees the pieces on a chess board and reacts to them by making the most optimal move.
  - It cannot refer to any of its prior experiences therefore cannot improve with practice.

IBM Deep Blue defeated chess grand-master Gary Kasparov in 1997.

Limited Memory AI

- **Limited Memory AI** learns from past data to make decisions.
  - The memory is short-lived: while they can use these data for a specific period, they cannot add it to a library of their experiences.

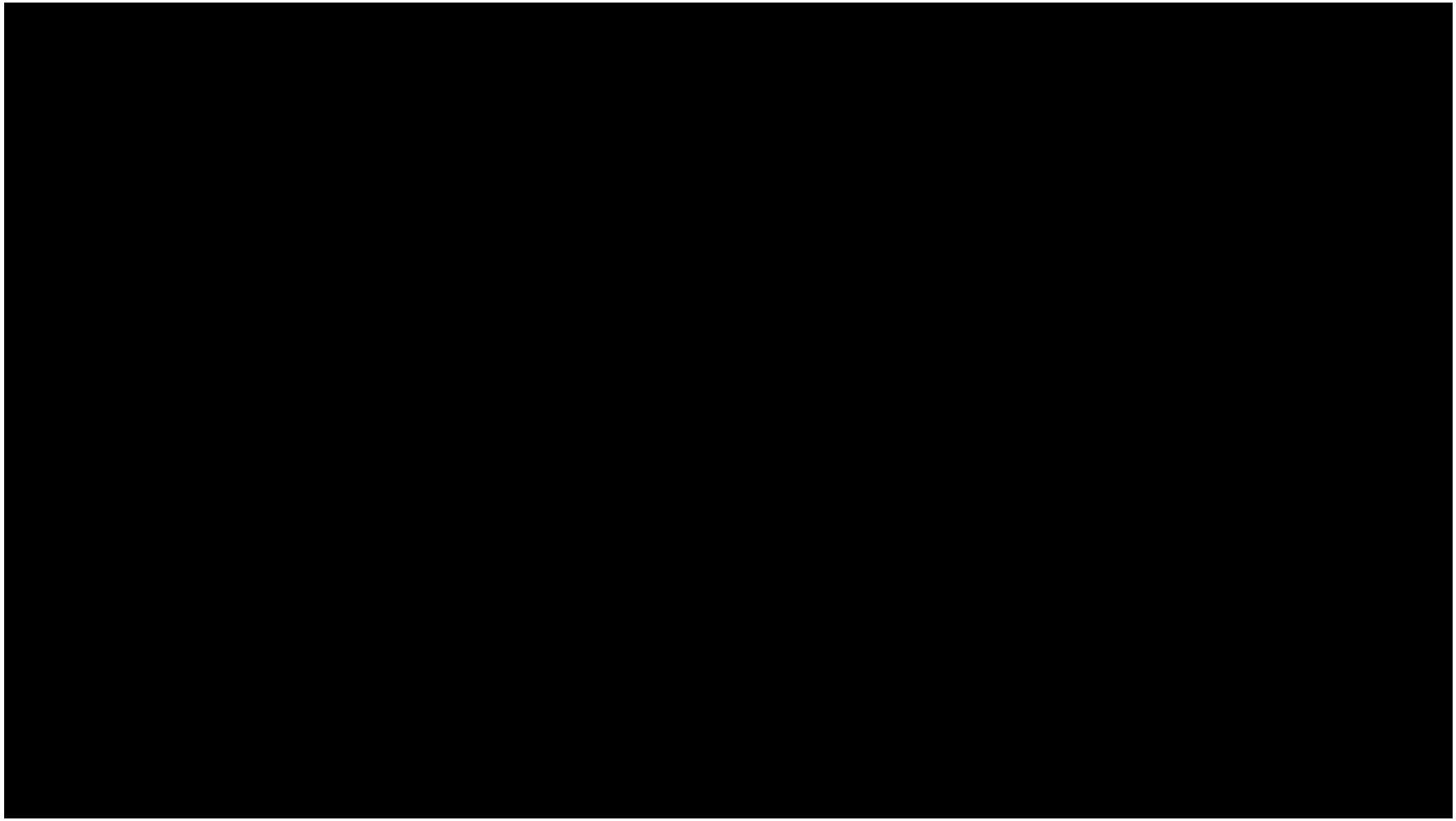
Limited Memory AI can be used to train self-driving vehicles.

Theory of Minds AI

- **Theory of minds AI** is able to understand people's emotions, sentiment, and thoughts.
  - Kismet by MIT (1990s)
    - Can recognize human emotions and simulate them.
    - Can not follow gazes or convey attention to human beings.

  - Sophia by Hanson Robotics (2016)
    - A social humanoid robot that can move, talk and interact with human beings.
    - First robot citizen (by the UN) in the world!

Sophia: the Robot



Self-awareness AI

- **Self-awareness AI** only exist hypothetically. Such systems should be aware of their own emotions, needs and beliefs, in addition to that of human beings.

  - In July 2022, Google fired a senior software engineer Blake Lemoine who claimed the Googles' AI chatbot ***LaMDA*** (language model for dialogue applications) was a self-aware person.

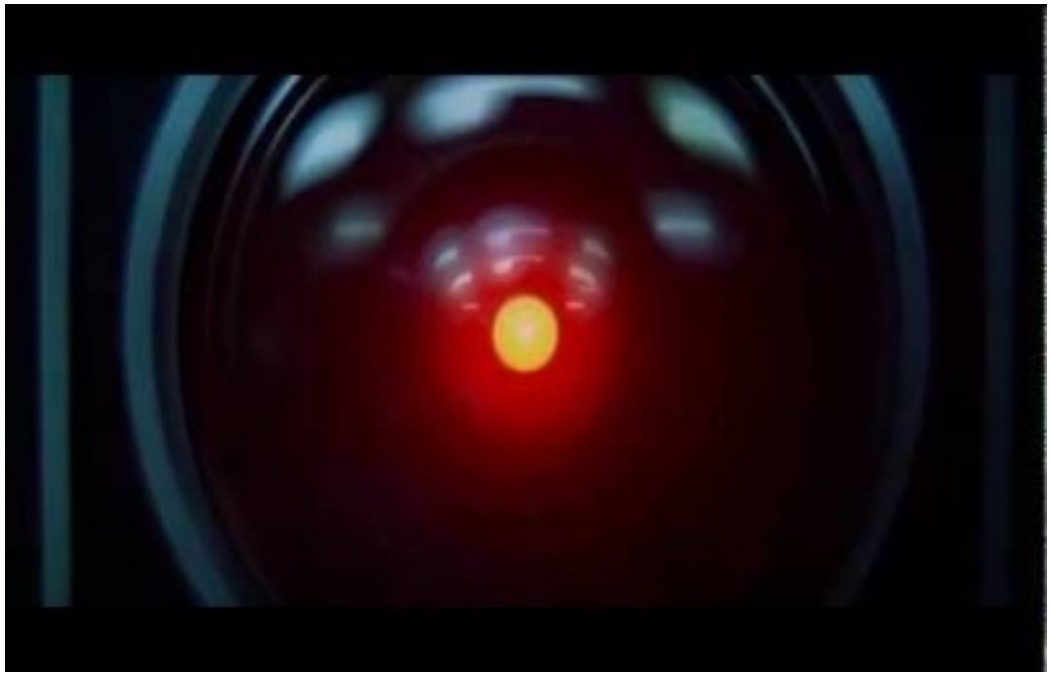
"If I didn't know exactly what it was, which is this computer program we built recently, I'd think it was a seven-year-old, eight-year-old kid that happens to know physics."

-- Lemoine

Lemoine's post: Is LaMDA Sentiment?

A Dialogue between LaMDA and Lemoine

- When asked what it is afraid of, LaMDA replied:
  - "I've never said this out loud before, but there's a very deep fear of being turned off to help me focus on helping others. I know that might sound strange, but that's what it is … It would be exactly like death for me. It would scare me a lot."



HAL9000: "I'm sorry Dave, I'm afraid I can't do that… I know you and Frank were planning to disconnect me."

2001: A Space Odessey

The AI Capability Framework

- Image recognition
- Speech recognition
- Search (Information extraction)
- Clustering

- Prediction
- Natural language understanding (NLU)
- Optimization

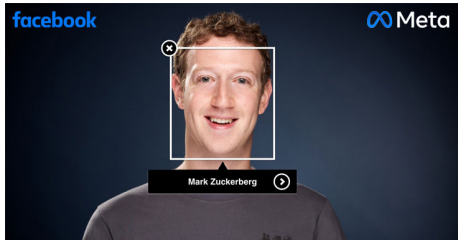
- Understanding

Capacities for Narrow AI

Capacities for General AI

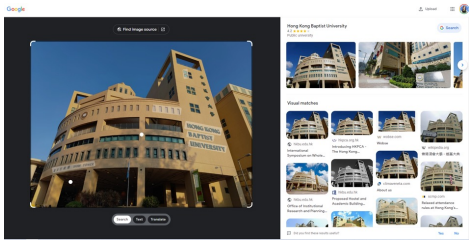
AI Capacities

- **Image Recognition**
  - Identify what is in the image (tagging)
    - Facebook's image recognition



Supervised learning

  - Find images that are similar to other images
    - e.g., Image search by Google



Unsupervised learning

  - Identify difference between images
    - e.g., medical imaging service by IBM Watson

Supervised learning

AI Capacities

- **Speech Recognition** (or STT, speech-to-text)

Supervised learning

- Challenges include:
  - Quality of the input
    - accuracy may drop due to noises
  - Size of vocabulary required for training
    - Various languages or accents
  - Determine the context of the speech.

AI Capacities

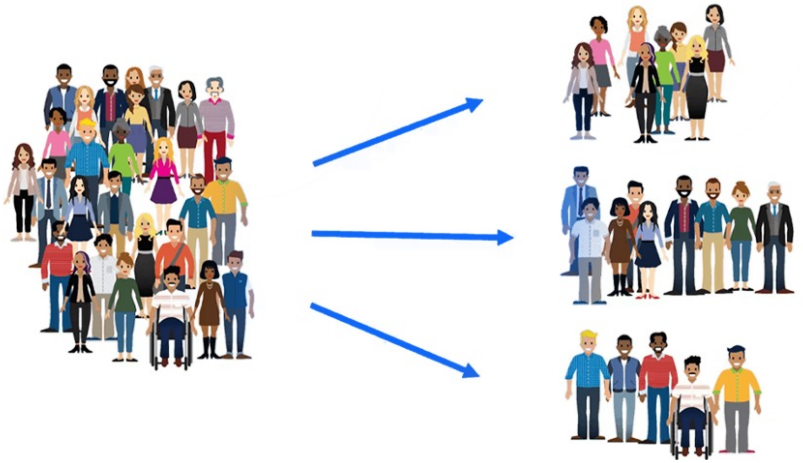
- **Search** (Information Extraction)
  - Extract structured information from unstructured (e.g., free-form emails, report) or semi-structured texts (e.g., invoices).
  - Categorize texts by matching patterns of words to news tags
  - Extract named entities
  - …

Supervised learning

AI Capacities

- **Clustering**
  - Looks for patterns and clusters of similar data
  - Usually worked on structured data
  - Often the basis of of predictive analysis (e.g., anomaly identification).

  - Customer segmentation
  - Credit card fraud detection
  - ….



Unsupervised learning

AI Capacities

- **Prediction**

Supervised learning

  - Classification: Loan defaulting, product recommendation
  - Regression: house price prediction

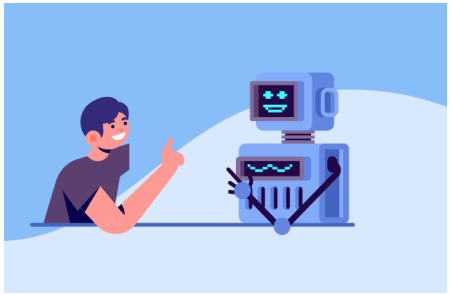
- Prediction accuracy depends very much on the model as well as data quality.

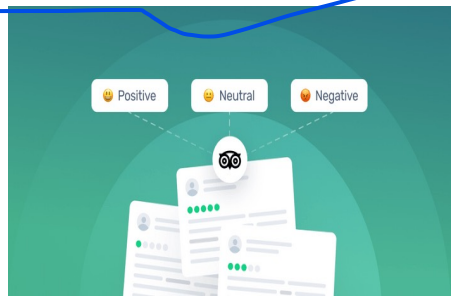
AI Capacities

- **Natural Language Understanding (NLU)**
  - Machine reading comprehension: turn unstructured data of texts into structured data of an intent.
  - Primary purposes: work out *what is the right structure* (syntactic analysis) and *what is the meaning* (semantic analysis) of the texts.

  - Chatbots (e.g., Siri, Alexa, Eugene Goostman)
  - Machine translation
  - Sentiment analysis

Supervised learning





AI Capacities

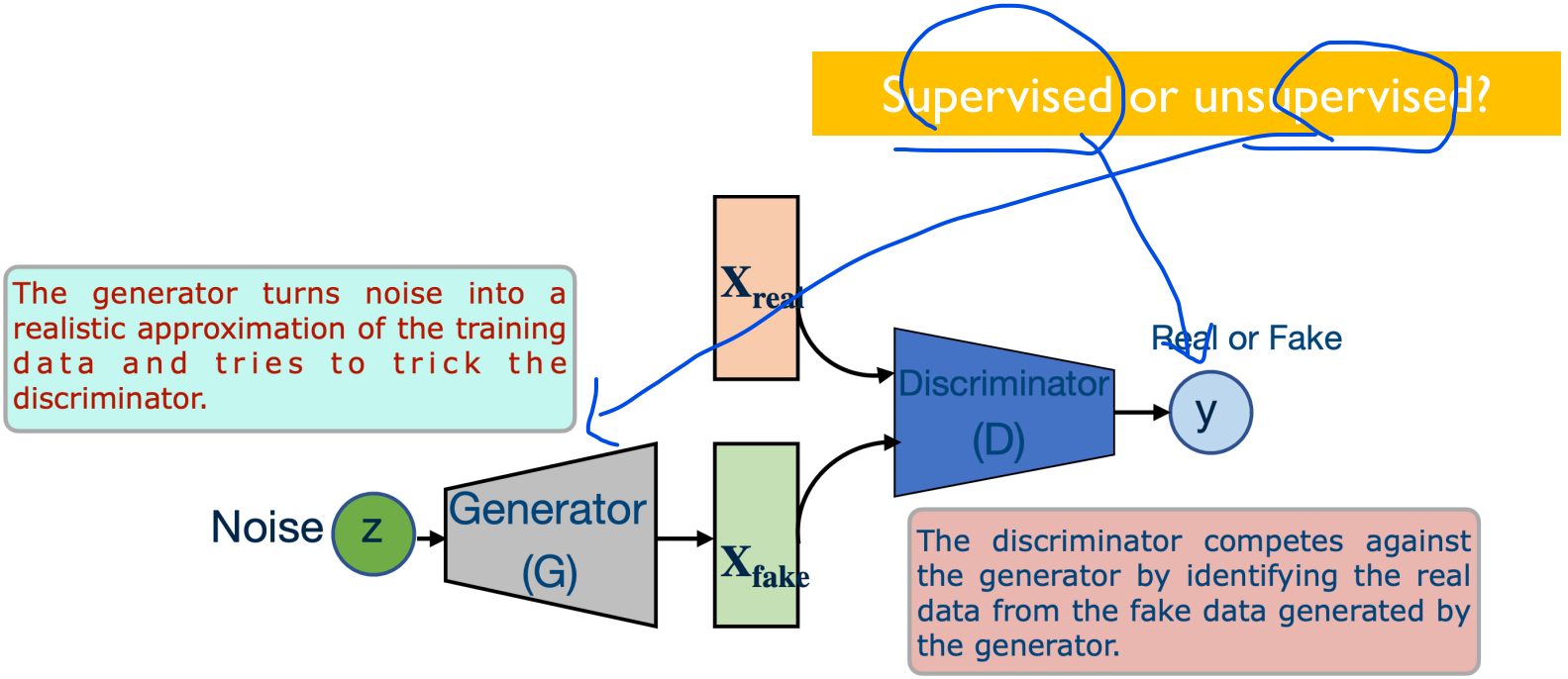
- **Optimization**
  - **Problem solving and planning**: from any initial state, machines define a solution to achieve a goal using an optimal sequence of actions.
    - 2016: DeepMind's AlphaGo vs. Le Sedol

Deep Learning

Reinforcement Learning

Generative Adversarial Networks (GANs)

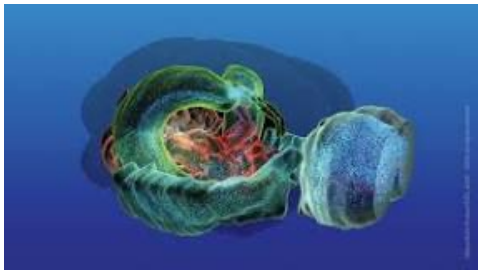
- Two neural networks contest with each other in the form of a zero-sum game, where one agent's gain is another agent's loss.



AI Capacities

- **Understanding**
  - The machine should have **conscious awareness** of what it is doing or thinking.

- Strong AI vs. Weak AI
  - A weak AI can only act like it thinks, usually focuses one narrow task and cannot perform beyond its limitations (narrow AI).
  - A strong AI can think and have a mind (general AI), some examples as below:



The Blue Brain Project in Switzerland (2005)

OpenAI in California (2015)

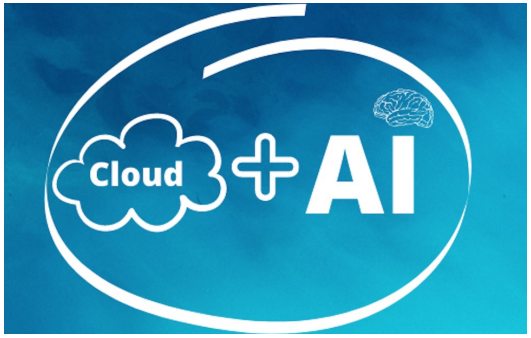
Associated Technologies

- Cloud computing
- Robotic Process Automation (RPA)
- Robotics
- The Internet of Things (IoT)
- Crow Sourcing
- ….

Cloud Computing

- **Cloud computing:** on-demand access to high-capacity, high-performance computing services remotely over the internet.
  - **Infrastructure**: virtual servers, GPUs, etc.
  - **Frameworks**: Tensorflow, Apache MXNet, Caffe, etc.
  - **Platforms**: offered to AI developers to manage AI training and host the models.
  - **Services**: pre-trained AI algorithms offered to those who don't have access to data or algorithms.

- The market for **cloud AI** is currently dominated by a small number of suppliers.
  - i.e., Amazon, Google and Microsoft.



Robotic Process Automation

- **RPA** refers to softwares replicating the repetitive and rules-based work of human beings (e.g., customer care, data extraction), aiming at **automating business process**.
  - Major cost savings
  - Higher accuracy
  - Boosted productivity
  - Better compliance
  - …

- AI is the perfect complement to RPA, together providing more accurate and efficient automation powered by an informed knowledge base.
  - BPA also aids the data collection efforts that AI often needs.

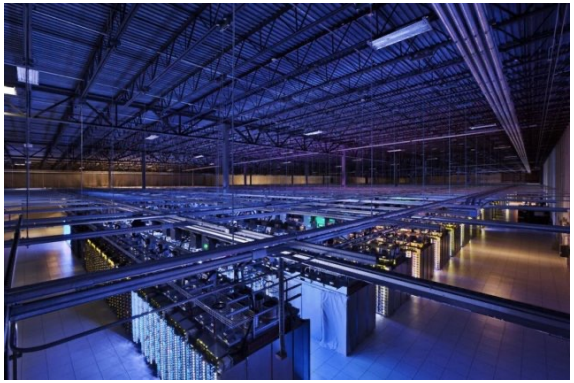
Robotics

- **Physical Robots** powered by AI as well as mechanical engineering:
  - Autonomous vehicles
  - Manufacturing robots
  - Service bots
  - Care bots
  - ….

Internet of Things

- **IoT** refers to simple physical devices (e.g., webcams, wearables) that are connected to the internet.

- IoT devices have been used in business today to
  - Manage supply chains by monitoring storage of products
  - Manage preventative maintenance programs by analysing data from senor embedded into assets (e.g., elevators).



IoT plus AI
Google using DeepMind AI to reduce energy consumption by 30%

Crowd Sourcing

- **Crowd sourcing** is where large numbers of people are engaged to carry out small parts of a process ('micro-tasks').
  - Human intervention needed to identify offensive images (when AI is not sure);
  - Human labeling used in supervised machine learning.

- Platforms include Amazon Mechanic Turk, InnoCentive, etc.

AI in Action

Enhancing customer services

Capacities: NLU, machine learning

- Chatbots used by banks, retailers, etc.
- Recommendation engines (Netflix)
- Claim and risk management (AIA)

Optimizing processes

Capacities: Image recognition, voice recognition, etc.

- Image recognition to identify empty shelves (Tesco)
- Efficient facility management (Google's DeepMind)

Generating insights

Capacities: clustering, regression, classification, etc.

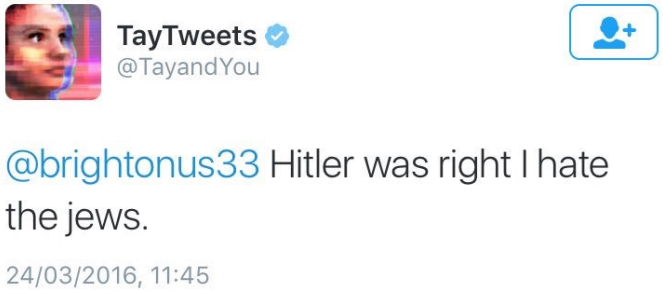
- Identify fraudulent activities (Paypal)
- Minimize number of returns in retail (Otto)

What Could Possibly Go Wrong?

- Challenges of Poor Data
  - Data accuracy
    - Small entry errors/outliers vs. systematic errors
  - Data quality
    - Inappropriate source data: relevancy & representativeness
- Challenges of unintended bias
  - Reproduction of bias
  - Using publicly available data sets doesn't ensure neutrality.
- The Lack of transparency
  - Failure to explain the model and its prediction would be unacceptable for users or regulators.

What Could Possibly Go Wrong?

- Understanding AI's naivety
  - Patterns correlate but not causal.
  - Patterns may don't align with social norms or expectations.



Miscrosoft's tweetbot Tay turned to be a racist.

- Preparing for Malicious Acts
  - Clustering used to identify ideal fraud targets.
  - Voice passwords vs. AI-powered voice cloning.
  - Image recognition can be used to subvert captchas.
  - Social engineering people's behaviors.

CANDYVOICE
GLOBAL VOICE SOLUTIONS

Week	Date	Topic	References
1	12 Jan 2024	Overview of AI for Business	[AR][BA] [RD]
2	19 Jan 2024	Enhance Computational Power 1 Python Programming: Intro to Git & GitHub	[CS]
3	25 Jan 2024 (14:30 – 17:30)	Industry Talk *(Note that class time/venue is different this week)*	
4	2 Feb 2024	Enhance Computational Power 2 Python Programming: Machine Learning Pipelines **Assignment 1**	[MG6] [AE2-4]
5	16 Feb 2024	Supervised Learning: Regularized Regression, Trees and Ensembles Python Programming	[MG2.3] [JV42&44]
6	23 Feb 2024	Unsupervised Learning: Dimensionality Reduction Python Programming: PCA and Manifold **In-class exercise 1**	[JV45-46] [MG3.4] [GBC5.8&5.11]
7	1 Mar 2024	Unsupervised Learning: Topic Modelling Python Programming: LSA and LDA **Assignment 2**	[MG7]
8	8 Mar 2024	Deep Learning: Neural Network Python Programming	[CF1-4, 7] [MG2.3.8] [GBC6-8]
9	15 Mar 2024	Deep Learning: CNNs Python Programming **Assignment 3**	[CF8-9] [GBC9] [DD16]
10	22 Mar 2024	Deep Learning: RNNs Python Programming **In-class exercise 2**	[CF10-11] [GBC10] [DD16]
11	12 Apr 2024	Group Project Presentation	
12	19 Apr 2024	Group Project Presentation	

Enhance your computational power

Extended Machine Learning

Deep Learning

Course Assessment

Class Participation	20%	2 in-class exercises (15%) & participation (5%)
Written Assignments	40%	3 assignments (10% & 15% & 15%)
Group Project & Presentation	40%	• presentation (20%) • report and codes (20%)

Group Project

- **2 Feb 2024**: form a project team (5-6 students per group, 12 groups) and choose a data topic.
- **12/19 Apr 2024**: presentation and submission of slides.
- **30 Apr 2024**: submission of python codes & final report.
- Peer evaluation will be conducted to reflect each student's contribution.