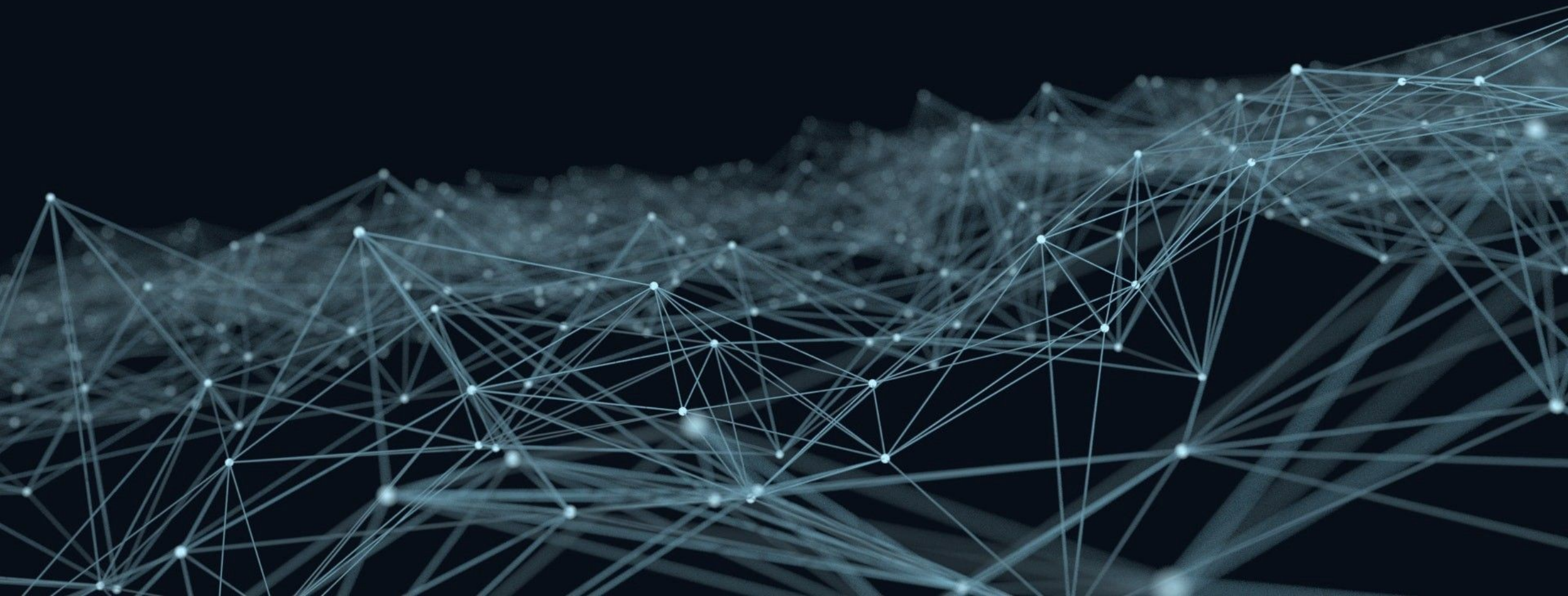
Generative Artificial Intelligence

Module One: Artificial Intelligence and Machine Learning



State of AI and ML

- In 2023, AI and ML are ubiquitous
  - “The Algorithms” have become the modern bogey man
- Implementation of ML has had mixed success
  - Often, when it works well, no one notices
  - Or when it works “good enough” like Siri or Google translate
  - People allow for some performance failures because expectations are low
  - However, when it fails, it can fail big and ugly
- Generative AI and Large Language Models are becoming disruptive
  - Deep fakes and compromising biometric authentication (eg. voice recognition)
  - Producing sophisticated and believable but incorrect results

Success Story

FUGRO ROAMES Machine Learning ◂ PREV NEXT ▸

Queensland, Australia is nearly 3 times the size of Texas with just one-sixth the population.

In order to deliver electricity to this widely dispersed population, Queensland relies on a network of 100 thousand kilometers of power lines and more than 1 million power poles.

Protecting the electrical grid means making sure that all of those power lines, power poles and conductors are in good repair, properly secured and not imperiled by encroaching vegetation or other structures. This used to be a laborious manual task requiring thousands of man-hours spent traveling along power lines.

Fugro Roames developed a vastly more efficient way to identify threats to power lines, poles and conductors. They use a combination of LiDAR and high resolution aerial photography to create a detailed 3D map of the physical condition of the electrical network and possible encroachment. Then they use machine learning to identify points on the network that have failed or are at risk of failure.

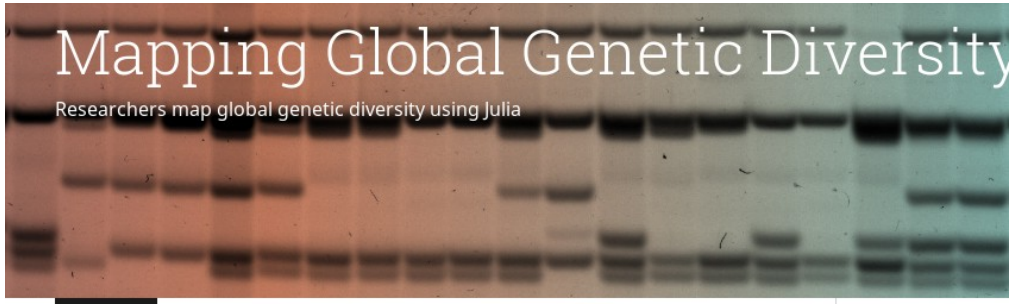
RELATED BLOG POSTS

A High Precision Cal
Feigenbaum's Alpha
27 Nov 2017 | Stuart Br
Mathematics, Northeas

Demystifying Auto-V
in Julia
27 Sep 2017 | Keno Fisc

Julia Computing and
Featured in Forbes A
25 Sep 2017 | Andrew C

Julia, The New Tech
Companies Demand



SCIENCE Genetic Diversity ◂ PREV NEXT ▸

Image Credits: Wikimedia Commons

For decades, scientists, naturalists and environmentalists have sounded the alarm about the loss of species diversity from Siberia to the Amazon. Today, with modern bioinformatic methods, it is possible to measure the diversity not only of species, but of different genes within individual populations, and to ask whether this genetic diversity is also being lost.

But, given the vast number of known species and the even greater number of genetic variants, how can we identify trends from such massive data?

According to c
Krabbe Borrega
University of C
chose Julia for
the analyses, n
felt it made my
more reproduc
work with. Run
was much fast
had been in R,
at the beginnin

Success Story

Success Story

IBM Medical Diagnosis ◂ PREV NEXT ▸

Diabetic retinopathy is an eye disease that affects more than 126 million diabetics and accounts for more than 5% of blindness cases worldwide. Timely screening and diagnosis can help prevent vision loss for millions of diabetics worldwide, but many of them lack access to health care.

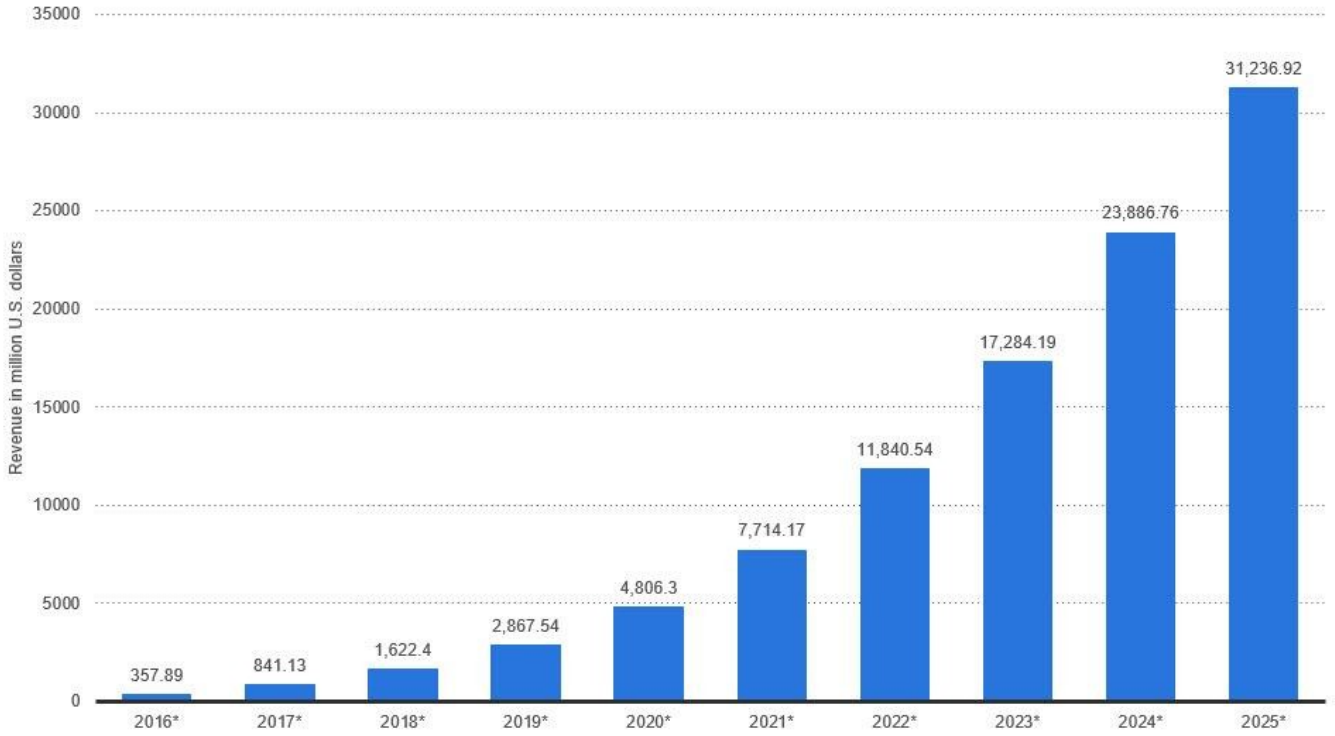
IBM and Julia Computing analyzed eye fundus images provided by Drishti Eye Hospitals, which provides eye diagnosis and care to thousands of rural Indians.

Drishti founder and CEO Kiran Anandampillai explains: "India is home to 62 million diabetics, many of whom live in rural areas with limited access to health facilities. Timely screening for changes in the retina can help get them to treatment and prevent vision loss. Julia Computing's work using deep learning makes retinal screening an activity that can be performed by a trained technician using a low cost fundus camera."

Market Trends

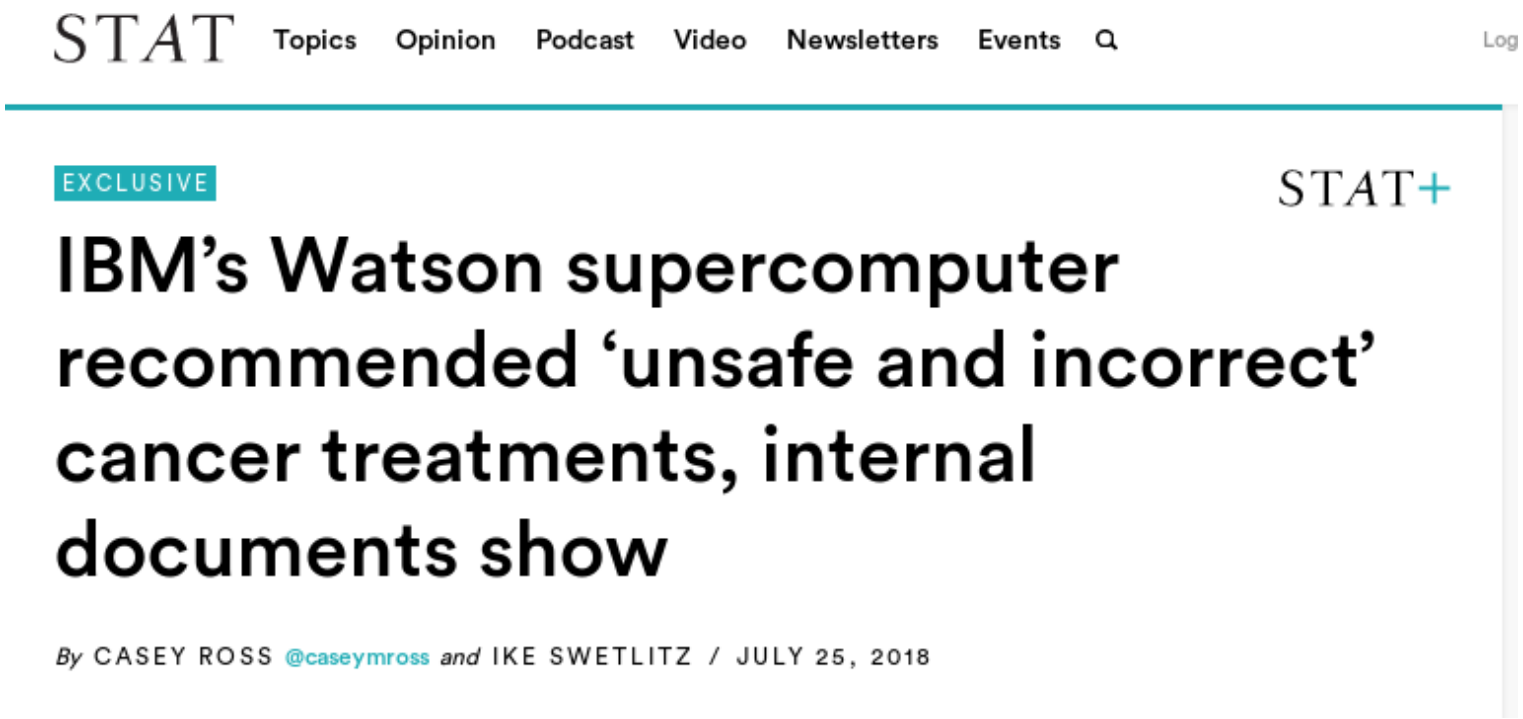
Enterprise artificial intelligence market revenue worldwide 2016-2025

Revenues from the artificial intelligence for enterprise applications market worldwide, from 2016 to 2025 (in million U.S. dollars)



statista

Oops



*"This product is a piece of s**t" wrote a doctor at Florida's Jupiter Hospital regarding IBM's flagship AI program Watson, according to internal documents obtained by Stat. In 2013 IBM developed Watson's first commercial application for cancer treatment recommendation, and the company has secured a number of key partnerships with hospitals and research centers over the past five years. But Watson AI Health has not impressed doctors. Some complained it gave wrong recommendations on cancer treatments that could cause severe and even fatal consequences. After spending years on the project without significant advancements, IBM is reportedly downsizing Watson Health and laying off more than half the division's staff."*

LMM Oops

boonchai wedmakawand/Getty Images

- **A law firm was fined $5,000 after one of its lawyers used ChatGPT to write a court brief.**
- **The document had included references to some cases and opinions that didn't exist.**
- **The lawyer said he had "no idea" ChatGPT could fabricate information.**

Oops

SAN FRANCISCO (Reuters) - Amazon.com Inc's (AMZN.O) machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

"Everyone wanted this holy grail," one of the people said. "They literally wanted it to be an engine where I'm going to give you 100 resumes, it will spit out the top five, and we'll hire those."

But by 2015, the company realized its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way. That is because Amazon's computer models were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period. Most came from men, a reflection of male dominance across the tech industry.

Oops

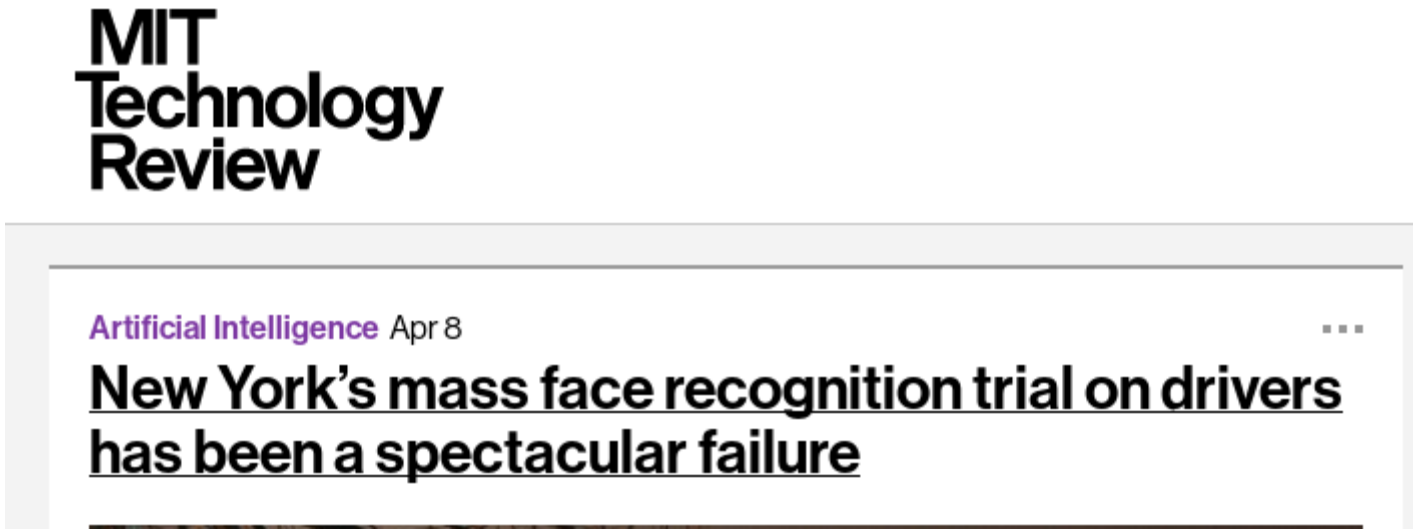
QUARTZ

Numbers don’t always tell the truth

Mark J. Girouard, an employment attorney at Nilan Johnson Lewis, says one of his clients was vetting a company selling a resume screening tool, but didn’t want to make the decision until they knew what the algorithm was prioritizing in a person’s CV.

After an audit of the algorithm, the resume screening company found that the algorithm found two factors to be most indicative of job performance: their name was Jared, and whether they played high school lacrosse. Girouard’s client did not use the tool.

Oops



The trial: An internal e-mail from the Metropolitan Transportation Authority seen by the WSJ included the details of the trial at the Robert F. Kennedy Bridge last year. Cameras attached to the bridge were supposed to capture and identify the faces of drivers through their windshields as they passed, matching them against government databases.

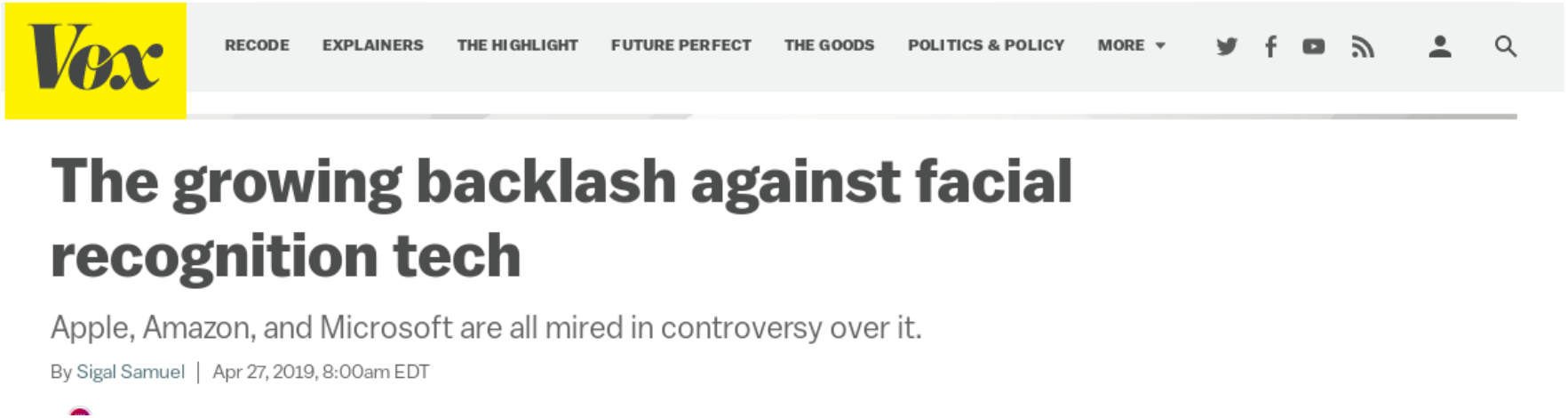
The results: But the document, from November of last year, says that the "initial period for the proof of concept testing at the RFK for facial recognition has been completed and failed with no faces (0%) being detected within acceptable parameters." That's no faces accurately identified. Oops. Despite the failure, more cameras are going to be positioned on other bridges and tunnels, according to a spokesperson.

Oops

Facial recognition technology has misidentified members of the public as potential criminals in 96 per cent of scans so far in London, new figures reveal.

The Metropolitan Police said the controversial software could help it hunt down wanted offenders and reduce violence, but critics have accused it of wasting public money and violating human rights.

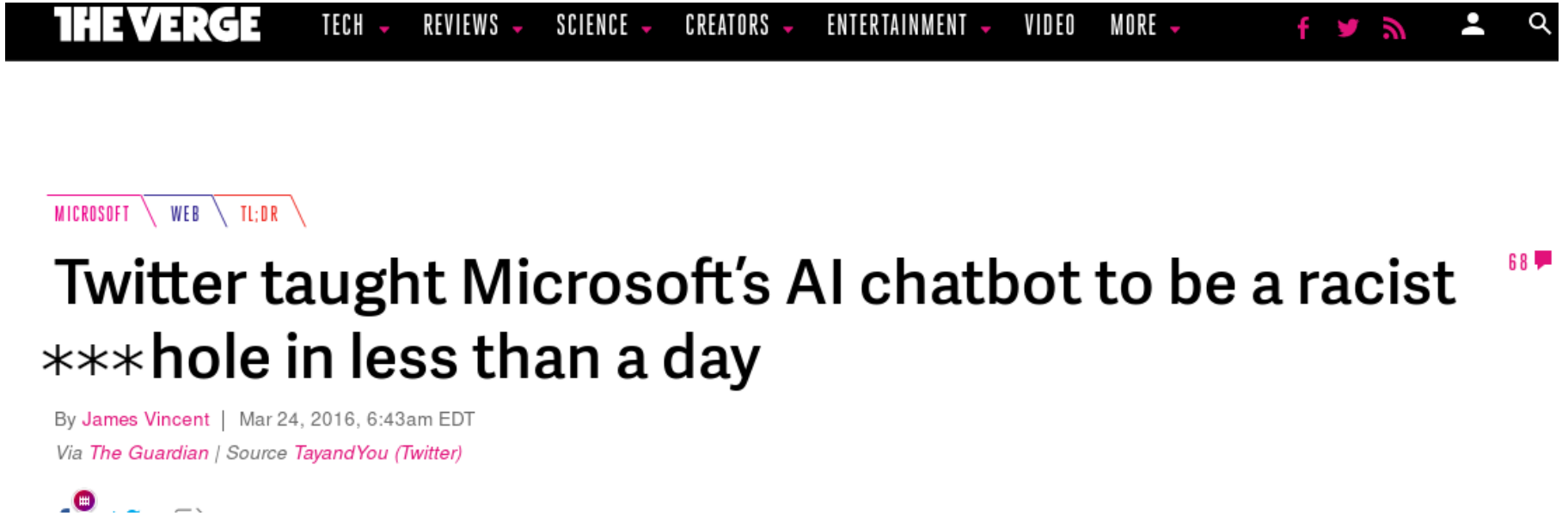
Oops



That's in addition to the researchers, advocates, and thousands of members of the public who have been voicing concerns about the risk of facial recognition leading to wrongful arrests. They worry that certain groups will be disproportionately affected. Facial recognition tech is pretty good at identifying white male faces, because those are the sorts of faces it's been trained on. But too often, it misidentifies people of color and women. That bias could lead to them being disproportionately held for questioning as more law enforcement agencies put the tech to use.

Now, we're reaching an inflection point where major companies — not only Apple, but also Amazon and Microsoft — are being forced to take such complaints seriously. And although they're finally trying to telegraph that they're sensitive to the concerns, it may be too late to win back trust. Public dissatisfaction has reached such a fever pitch that some, including the city of San Francisco, are now considering all-out bans on facial recognition tech.

Oops



It took less than 24 hours for Twitter to corrupt an innocent AI chatbot. Yesterday, Microsoft unveiled Tay — a Twitter bot that the company described as an experiment in "conversational understanding." The more you chat with Tay, said Microsoft, the smarter it gets, learning to engage people through "casual and playful conversation."

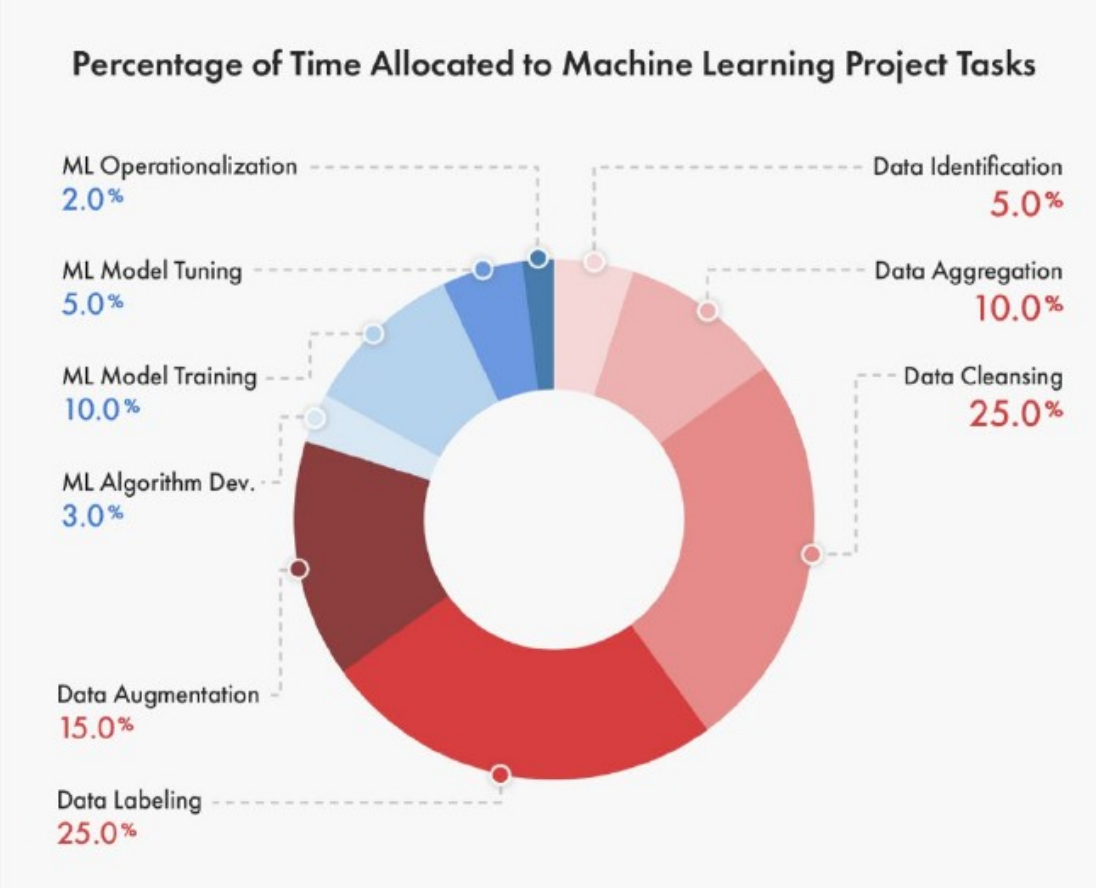
Unfortunately, the conversations didn't stay playful for long. Pretty soon after Tay launched, people starting tweeting the bot with all sorts of misogynistic, racist, and Donald Trumpist remarks. And Tay — being essentially a robot parrot with an internet connection — started repeating these sentiments back to users, proving correct that old programming adage: flaming garbage pile in, flaming garbage pile out.

ML in Production

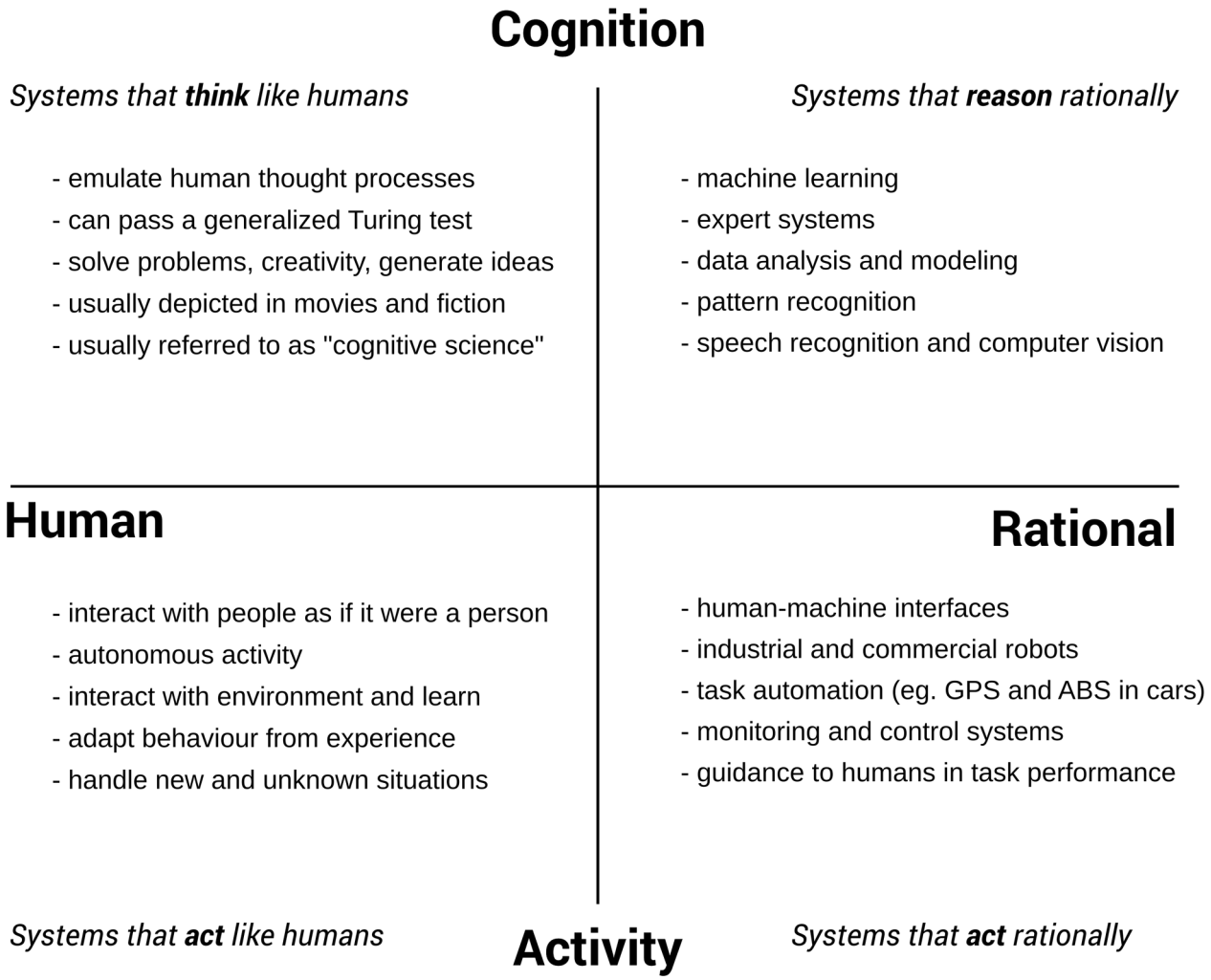
- There are many ML applications that have been introduced into production environments successfully
  - Eg. tracking patterns of financial fraud
- Or at least, we think these models are successful
  - How do we measure success?
  - Is an improvement in performance a success?
  - If we can identify twice as much fraud, but fraud is increasing ten-fold, is that a success?
  - How do we respond to new patterns and types of fraud?

ML Failures

- Only 2% of a ML project is spent transitioning to production (operationalization)
- Failures are not necessarily due to the model but because of factors in the operational environment
  - These factors will be considered later
  - In successful cases, the operational environment is like the dev environment
  - Training data is a representative sample of the population
  - The operational environment is relatively stable

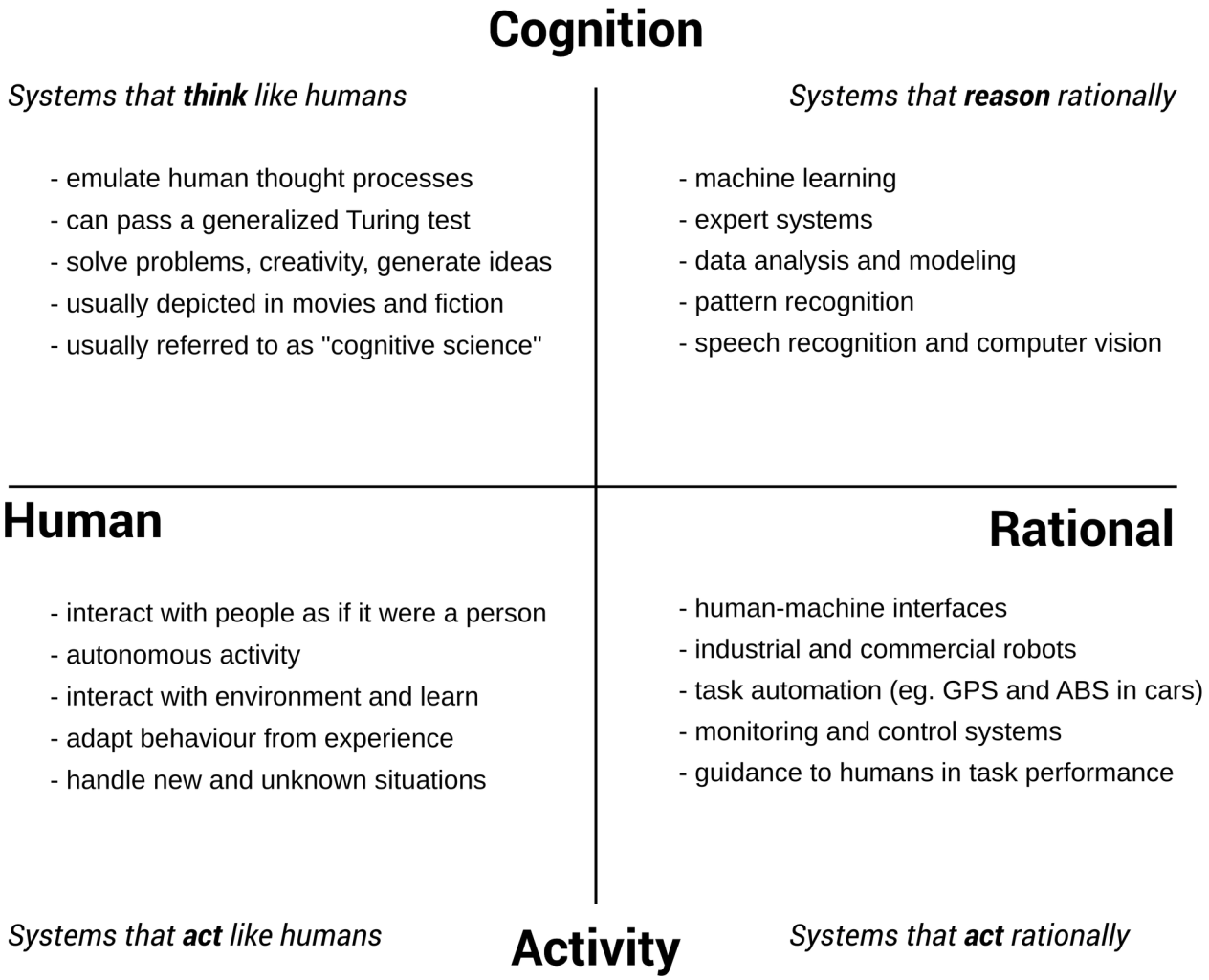


The Norvig Matrix



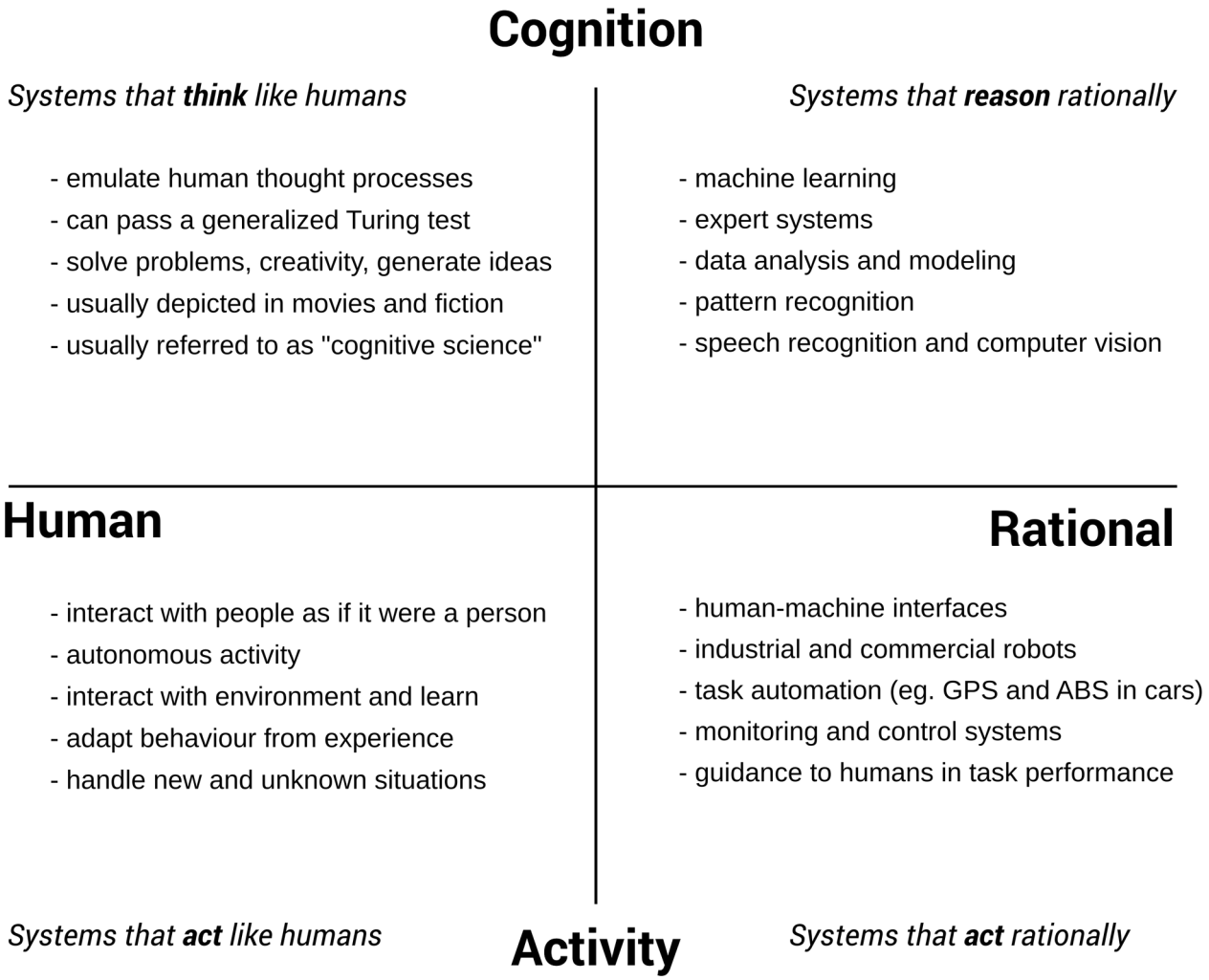
- From the classic AI textbook
- Divides the field of AI into different areas of study
  - Cognition refers to the ability to solve problems
  - Activity refers to how the AI interacts with the environment

The Norvig Matrix - Human-like Cognition



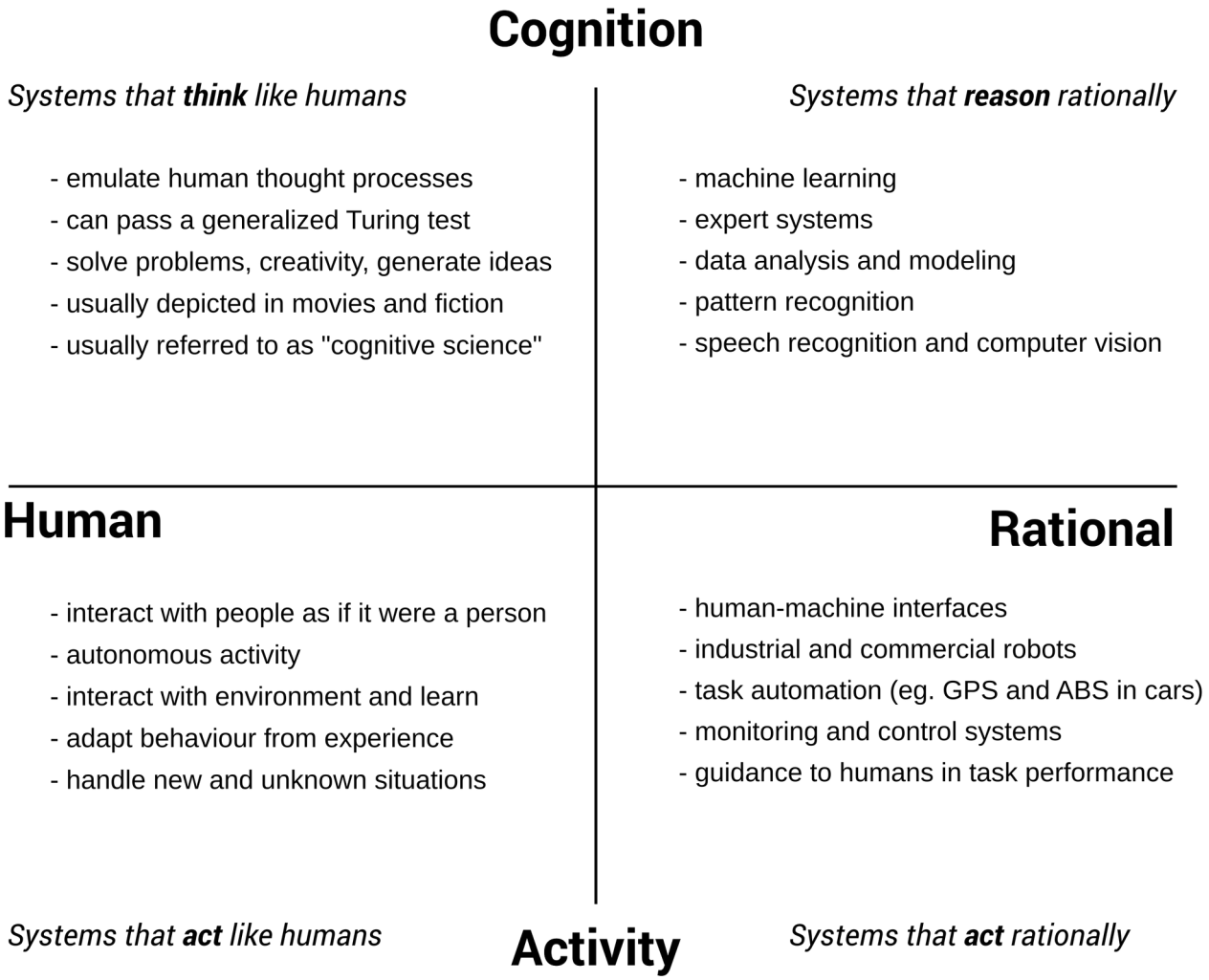
- Human like cognition
  - Is where the AI uses the same sorts of cognition as a human to solve problems
  - Algorithms are modeled after human reasoning
  - Often used as research tools in brain and cognition research
  - Current research uses the idea of growing an AI in the same way a child develops cognitively

The Norvig Matrix - Human-like Behavior



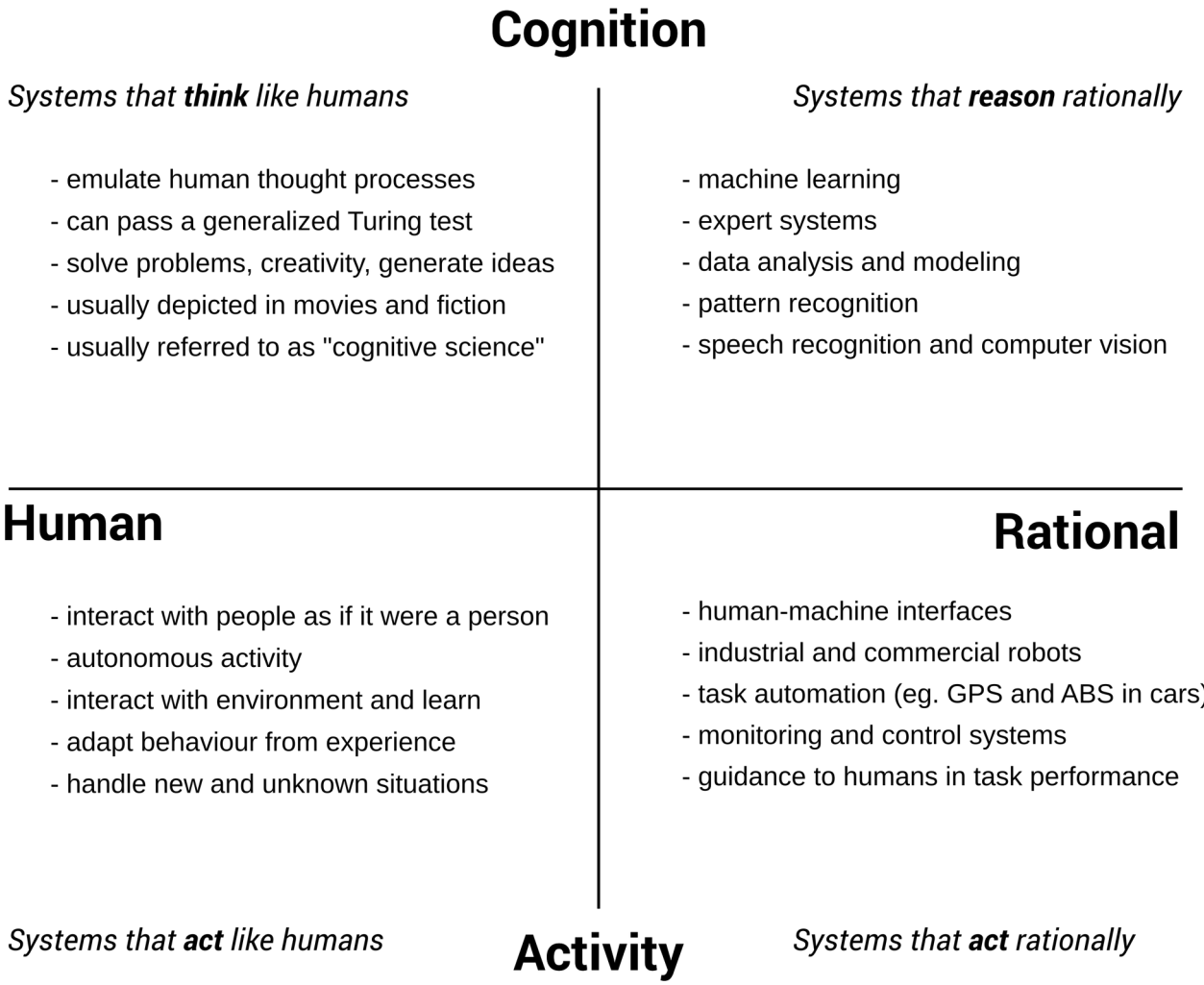
- Human like actions
  - Knows how to interact with an environment
  - Can learn how to interact with novel environments
  - One objective is to create human-like interfaces
  - AI systems that meet the criteria of the left column are called “General AI”
  - There currently exists no system that meets either of the criteria (despite the hype)

The Norvig Matrix - Rational Behavior



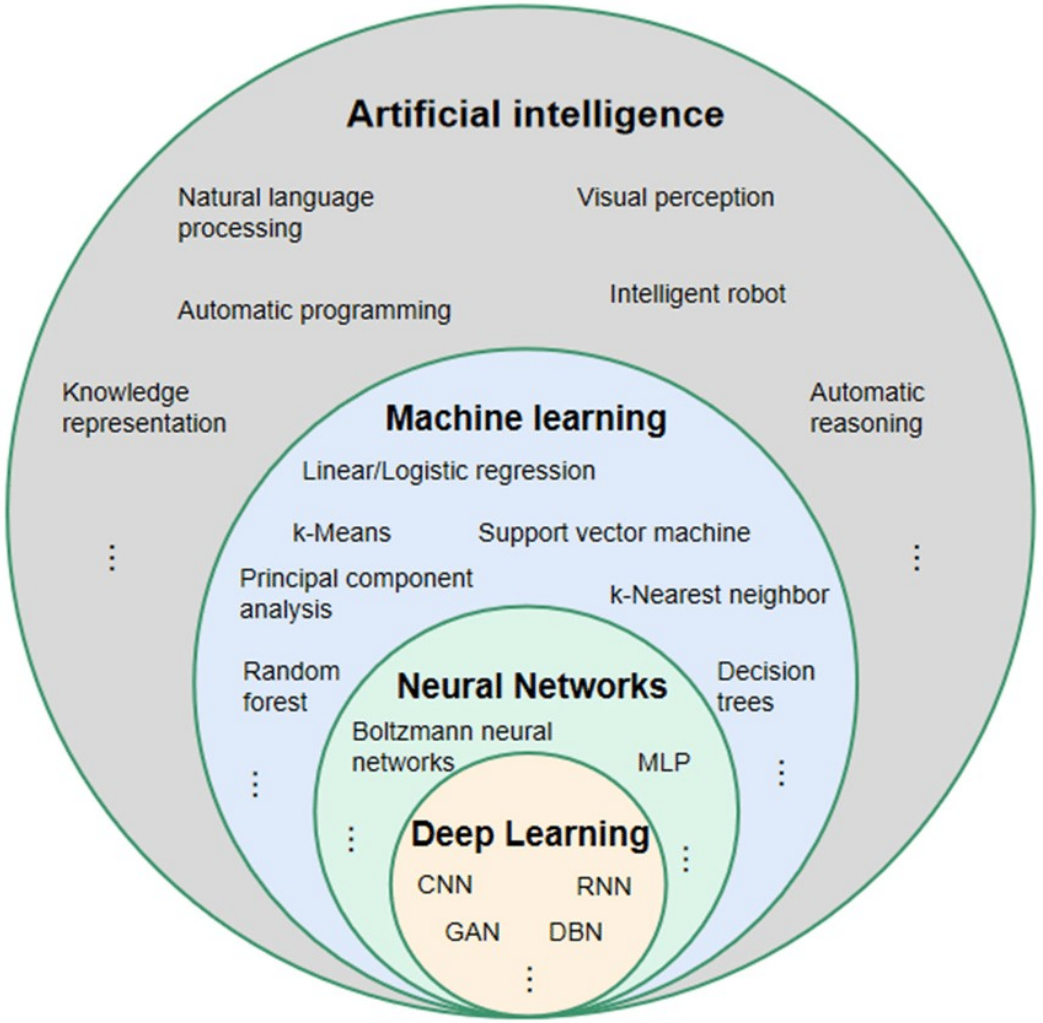
- Focus on “correct” actions
  - Not necessarily what a human would do
  - Tends to be focused on specific problem domains
  - Industrial robots, self-driving cars, etc
  - Often used to assist humans who make decisions

The Norvig Matrix - Rational Reasoning



- The focus of this course
  - Used to produce decisions based on data
  - The underlying mechanism does not have to resemble anything a human does
  - Often relies on looking for patterns in large sets of data
  - Then builds a statistical model to allow accurate estimations or result for new input data

AI and Machine Learning



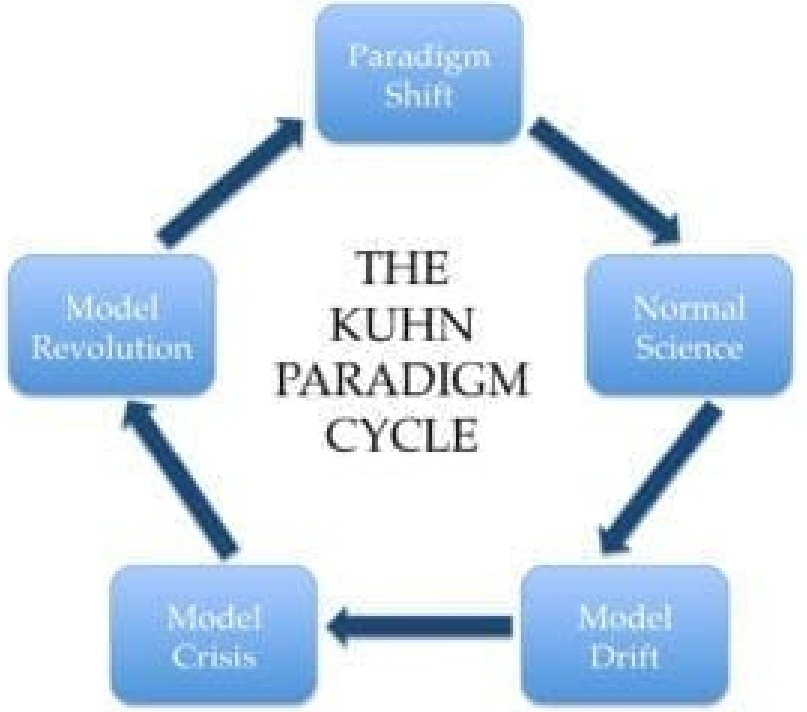
- General Typology
  - Neural Nets (NN) were originally supposed to emulate human reasoning but failed because the problem was far too complex
  - However the methods were perfect for solving advanced ML problems
- GAI is a subset of deep learning

Defining Machine Learning Realistically

- Machine learning is building statistical models
- The power of the models we can build depend on three primary factors
  - **Algorithms**: There has to exists a specific process for building a model
  - **Data**: There has to be enough data of sufficient quality to generate a useful model
    - *All models are wrong, they just have to be right enough to be useful*
  - **Compute**: There has to be sufficient compute capabilities to actually build the model with a given algorithm and set of data
- All of these have changed drastically

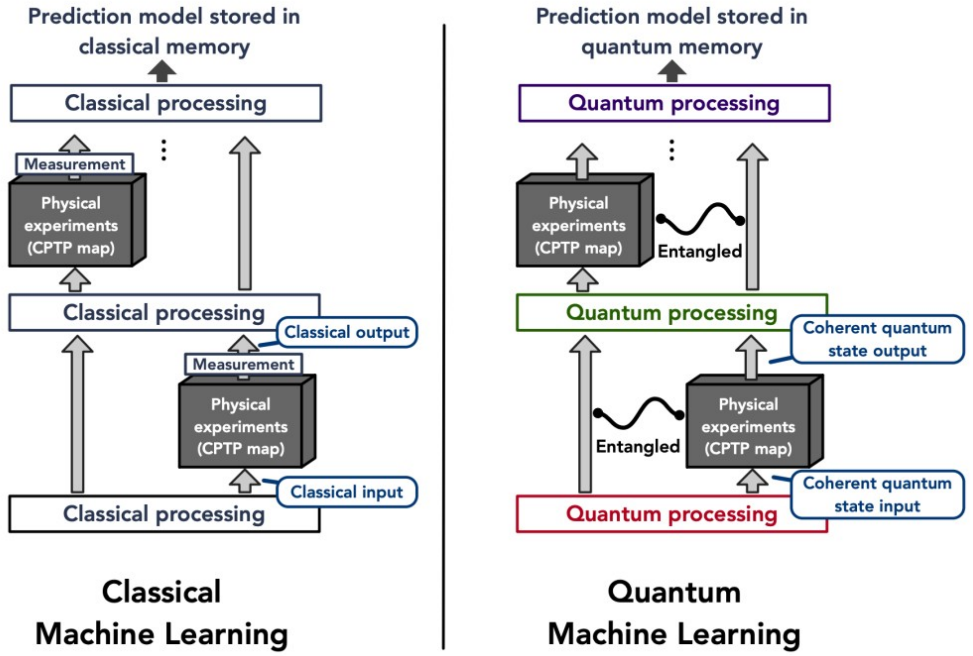
Machine Learning Generations

- Generation One: Traditional ML
  - Standard supervised and unsupervised models
- Generation Two: Deep Learning
  - Use of neural nets for more complex problems
- Generation Three: Generative AI
  - What this course is about
- Each generation extends the previous
  - Uses the tools and techniques of the previous generation
  - Stimulated by improvements in data, compute and algorithms
  - A very Kuhn-ian paradigm shift

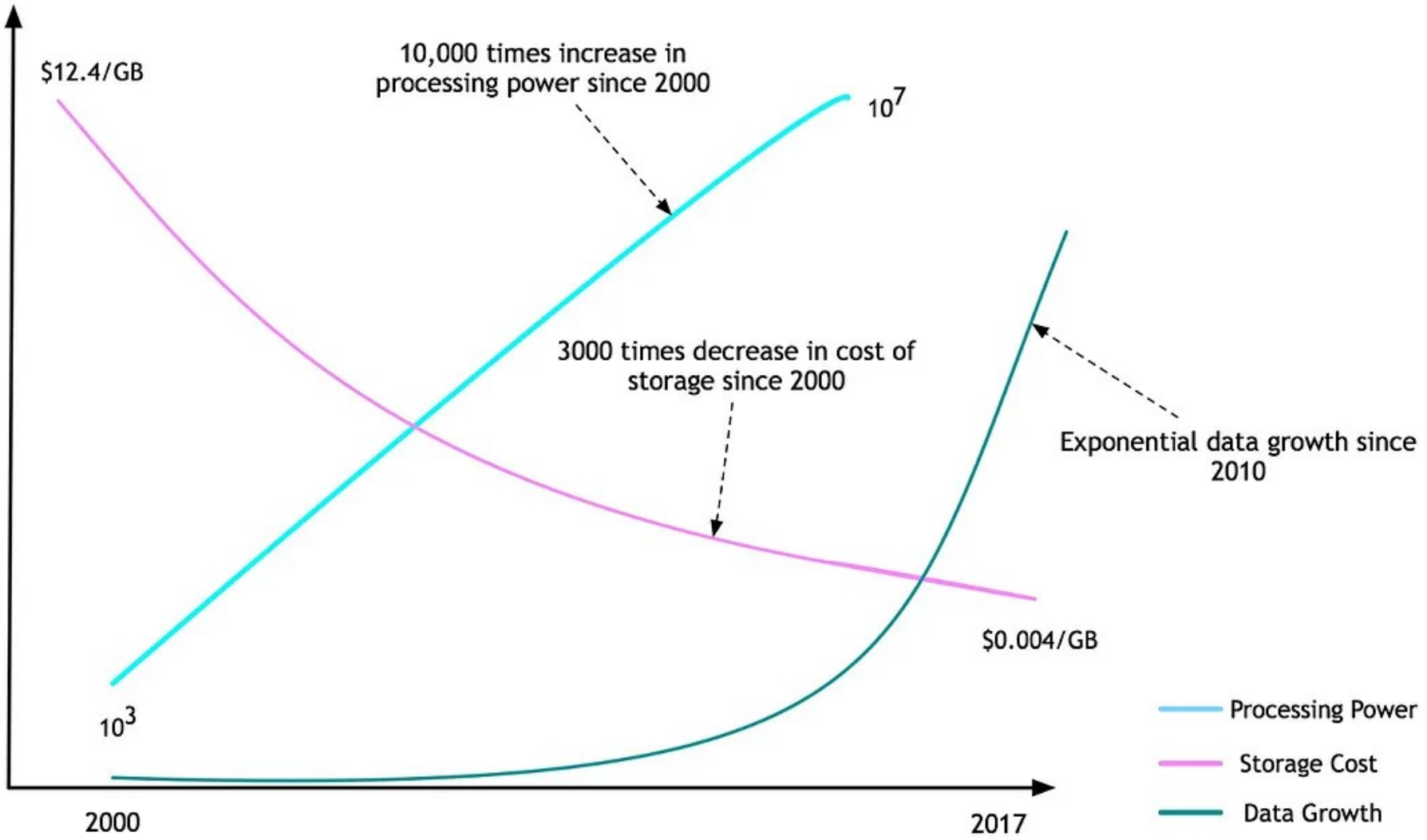


Quantum Machine Learning?

- Suggest by advocates as the fourth generation of ML
  - No consensus
  - Many suggest quantum computing does not give any real advantage for ML
  - Might require a rethinking of what ML is and how it should work
- However:
  - QC is still experimental and *very* expensive
  - Cannot be done at scale



Compute Power



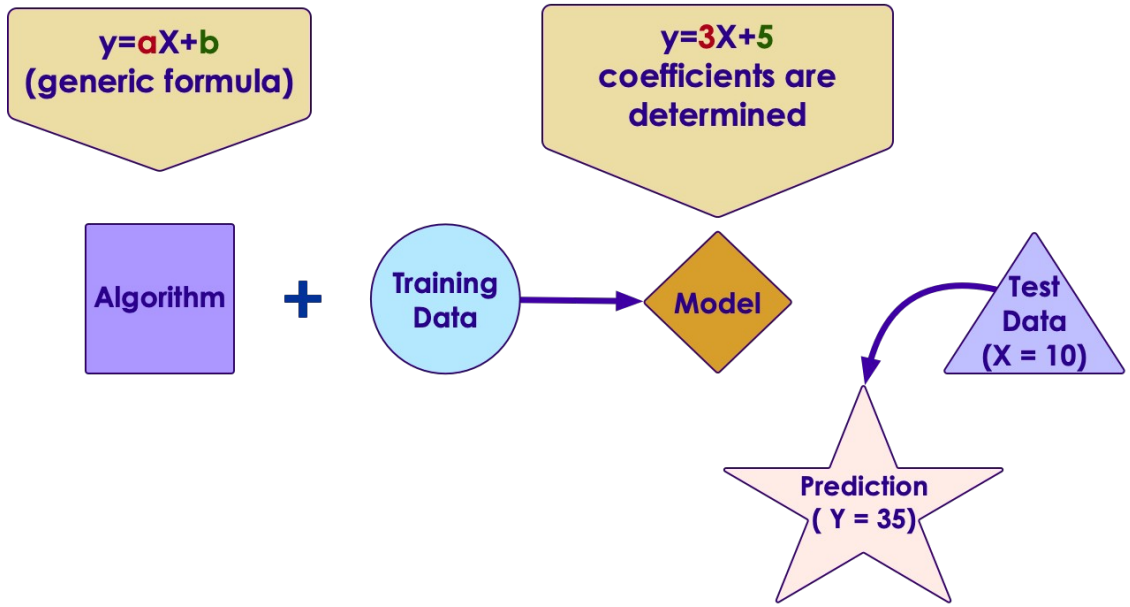
Compute Power

- Amount of computation that can be done
  - Individual CPUs, GPUs and TPUs are much faster
  - Hardware allows for massive parallelization
  - Storage capacity has increased dramatically
- Costs of storage and compute have dropped
- Compute and store on demand
  - Virtual and cloud architectures
  - Reduced capital investments
- Eg. To train ChatGTP 3 on a CPU would take about 350 years

Google TPUs

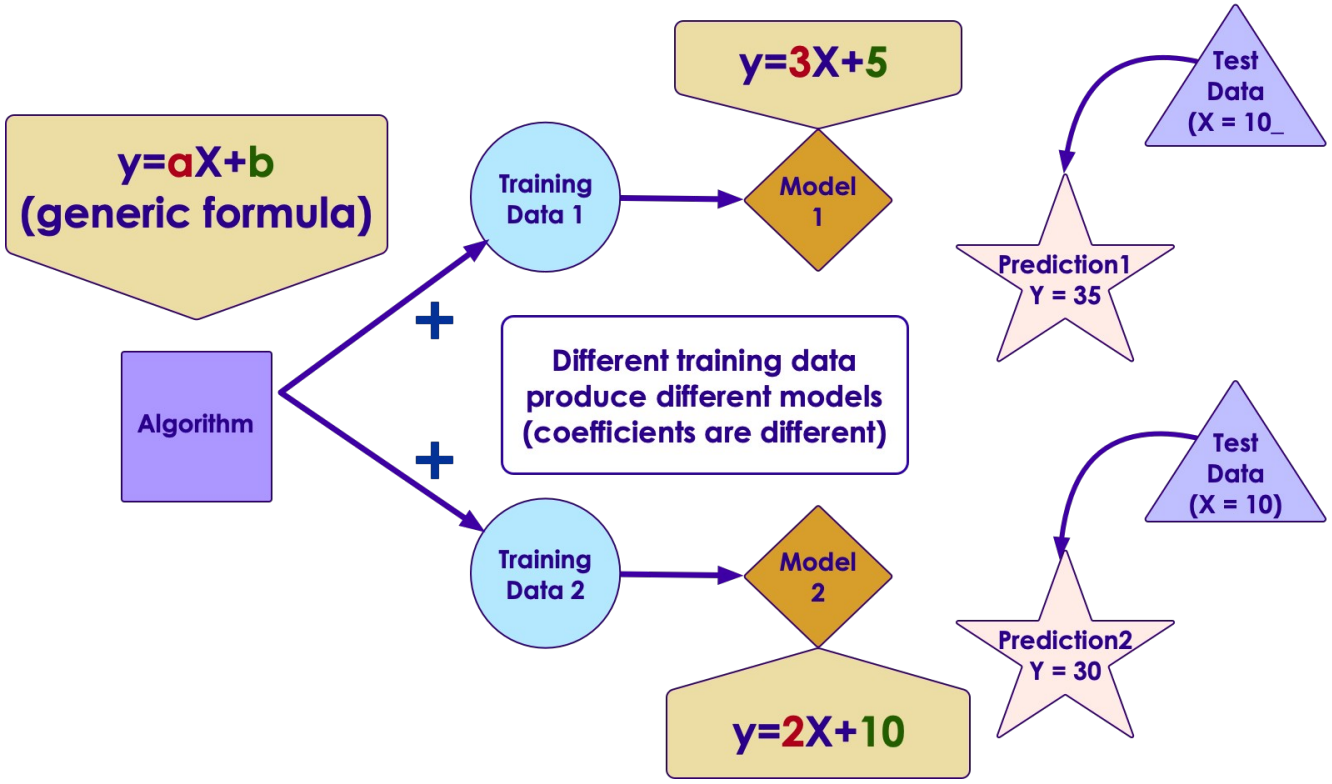
Traditional ML and Data

- The “model” is a statistical model used for prediction on a data sample from the population
- The “algorithm” is how the model is trained (decision tree, SVM etc)
- Testing critical to ensure the model is applicable to the population



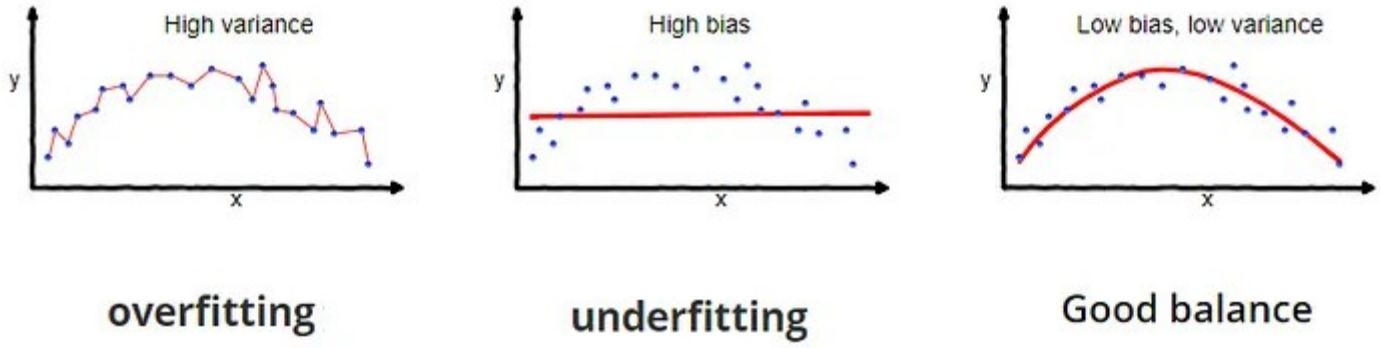
Traditional ML Data Dependency

- Training sets are samples from the population
  - Different samples produce different models



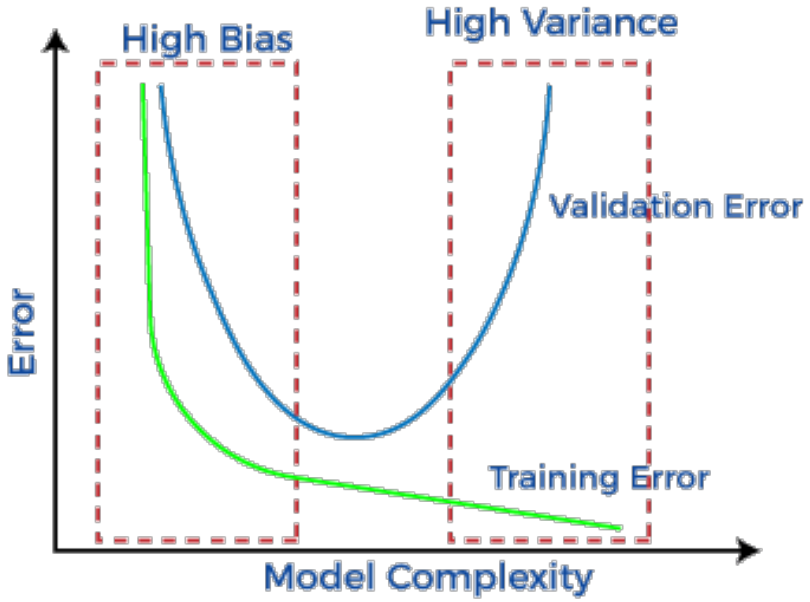
The Problem of Bias

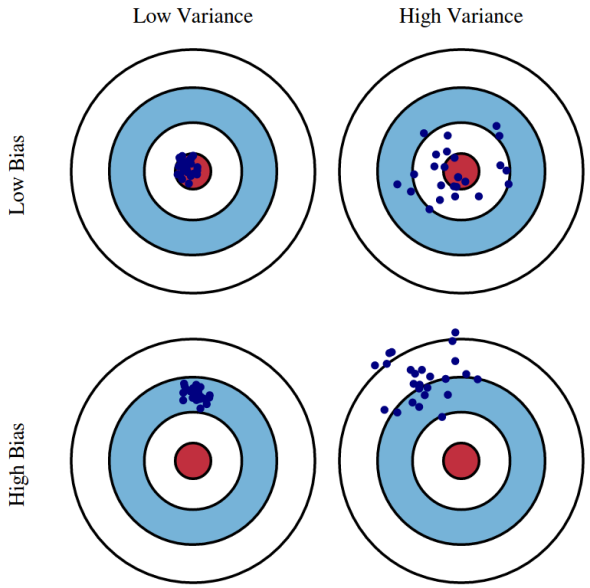
- Bias can be thought of as how poorly the model generalizes from the training data to the overall population
  - High bias is related to overfitting where the model predicts the training data very well but performs poorly on other data from the population
  - High variance is how well the model explains the variance in the training data (ie. can make useful predictions



The Problem of Bias

- This is also referred to as the variance-bias trade-off
  - Variance is how well the model can make prediction in the training data
  - Models with high variance perform well with the training dataset
  - But they may not generalize well to the population because of bias
  - This shows up in validation errors “It worked great in the lab but..”
  - As the model improves variance it has to stop at the sweet spot that minimizes validation errors

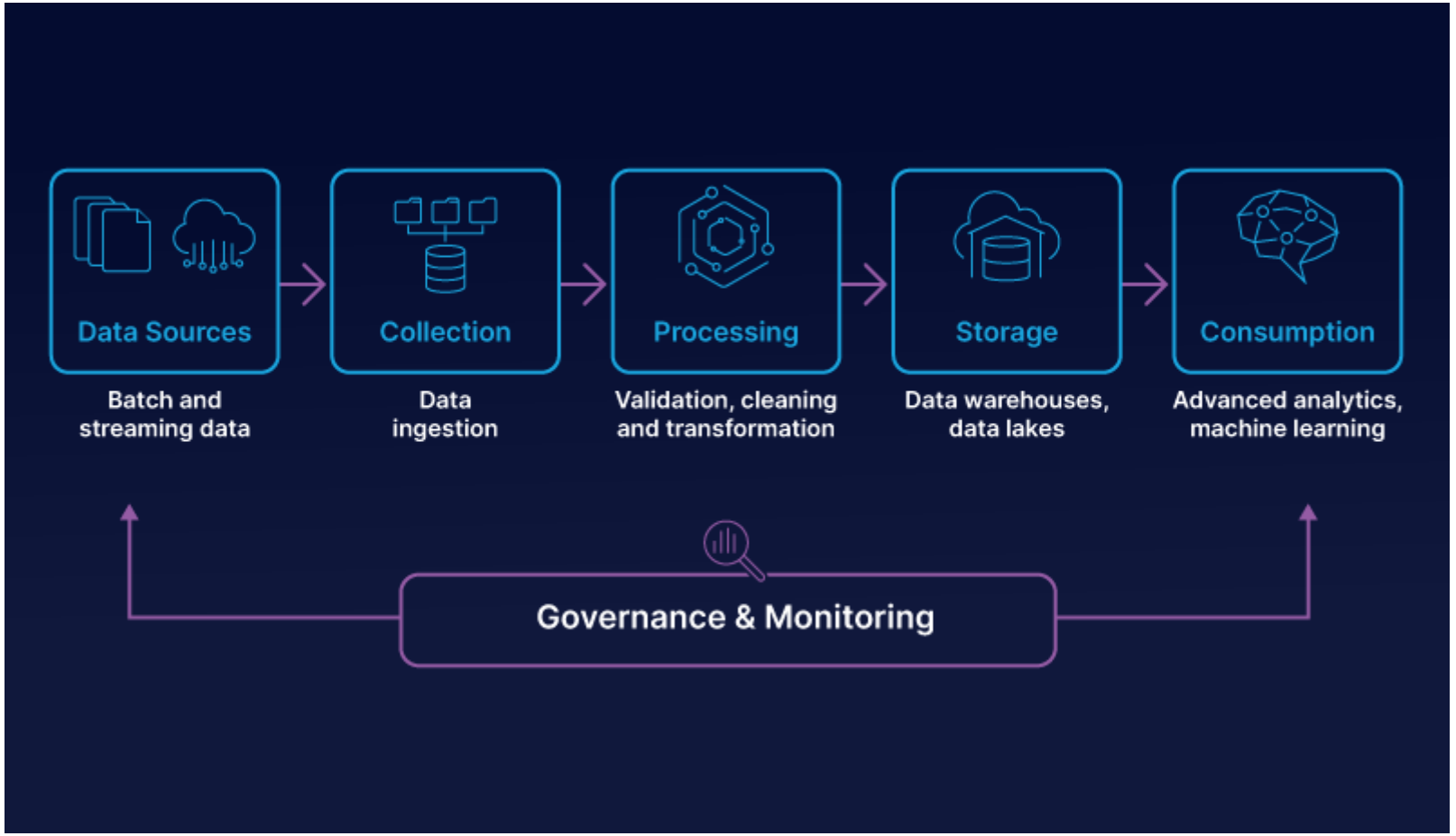




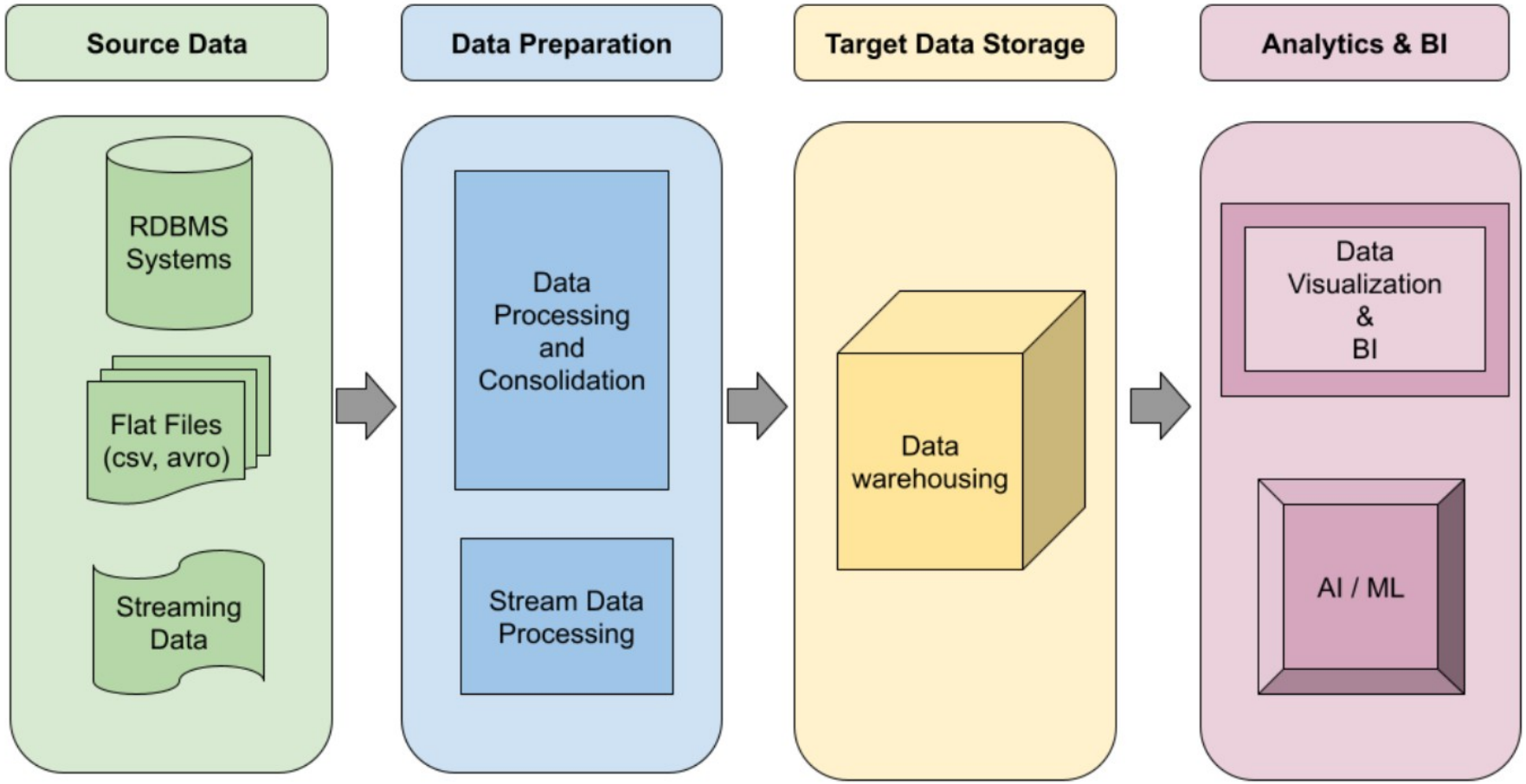
Data Limiting Factors

- Availability of data
  - Where the data is collected from
  - Gap in accessibility between digitized and non-digitized data
- Data Issues
  - Costs of storage might be prohibitive
  - How to store massive amounts of data in a way that is accessible
  - Data accuracy – how representative is the training data of the population?
  - Data quality – how good is the data or is our sample just wrong
- Data Engineering
  - Tagging data for supervised learning
  - Cleaning and transforming data

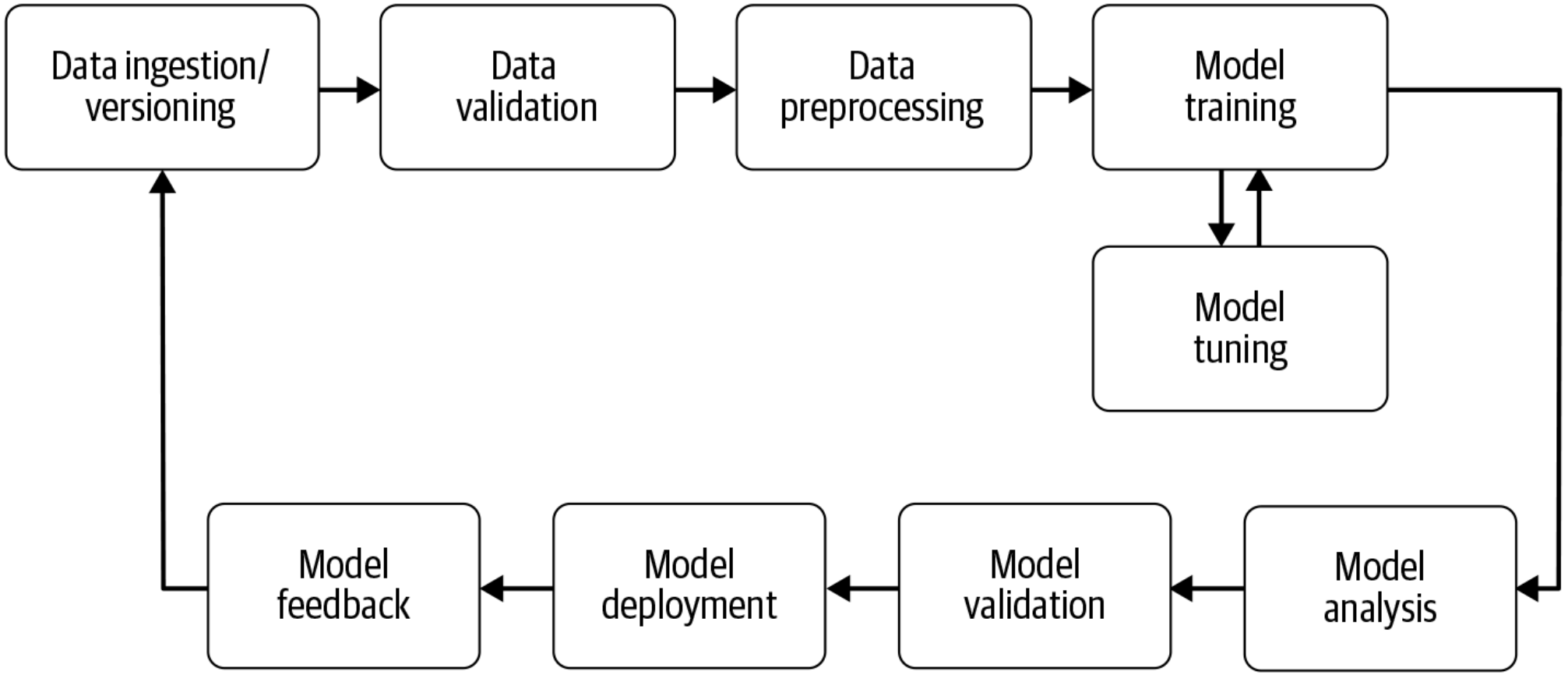
Data Engineering Pipeline



Data Engineering Pipeline

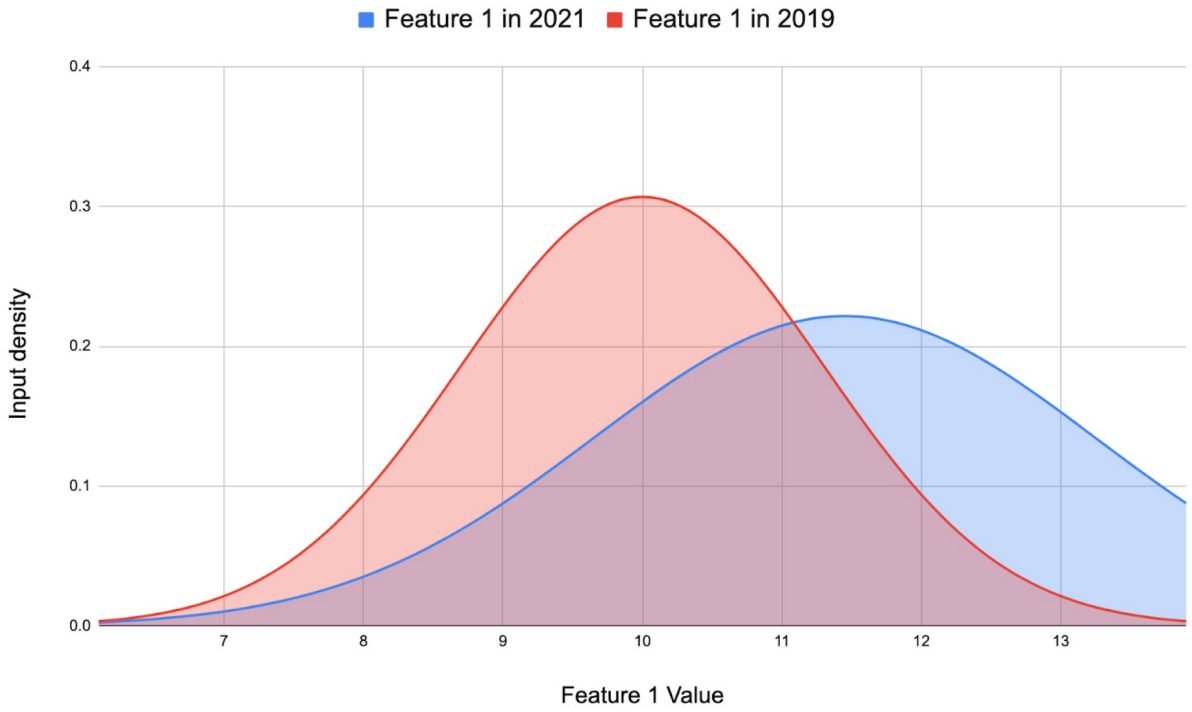


MLOPs Pipeline



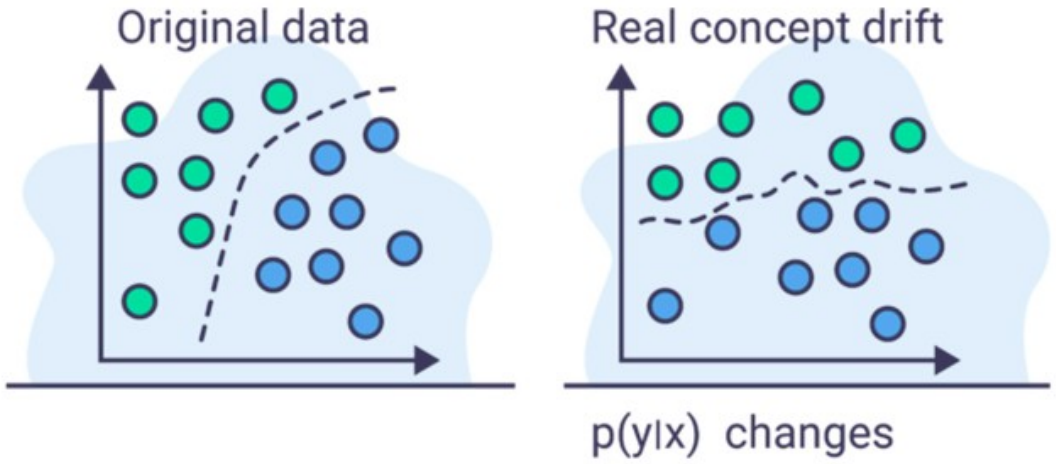
Why MLOPs?

- Because models are trained in a sample they are prone to data drift
  - The population changes and the training data is no longer representative
  - New training sets need to be sample from the new data and the model retrained



Why MLOPs?

- Models are trained with certain assumptions about what features are important and their relationships
  - When these change, we have concept drift
  - New features may occur in the population since training
  - Relationship between two features may change
  - Some features may become less important over time
- The model has to be retrained after re-engineering the features



What if..

- We could train our models on the entire population?
- Or at least a large enough sample that variance between samples is insignificant?

Defining Generative AI

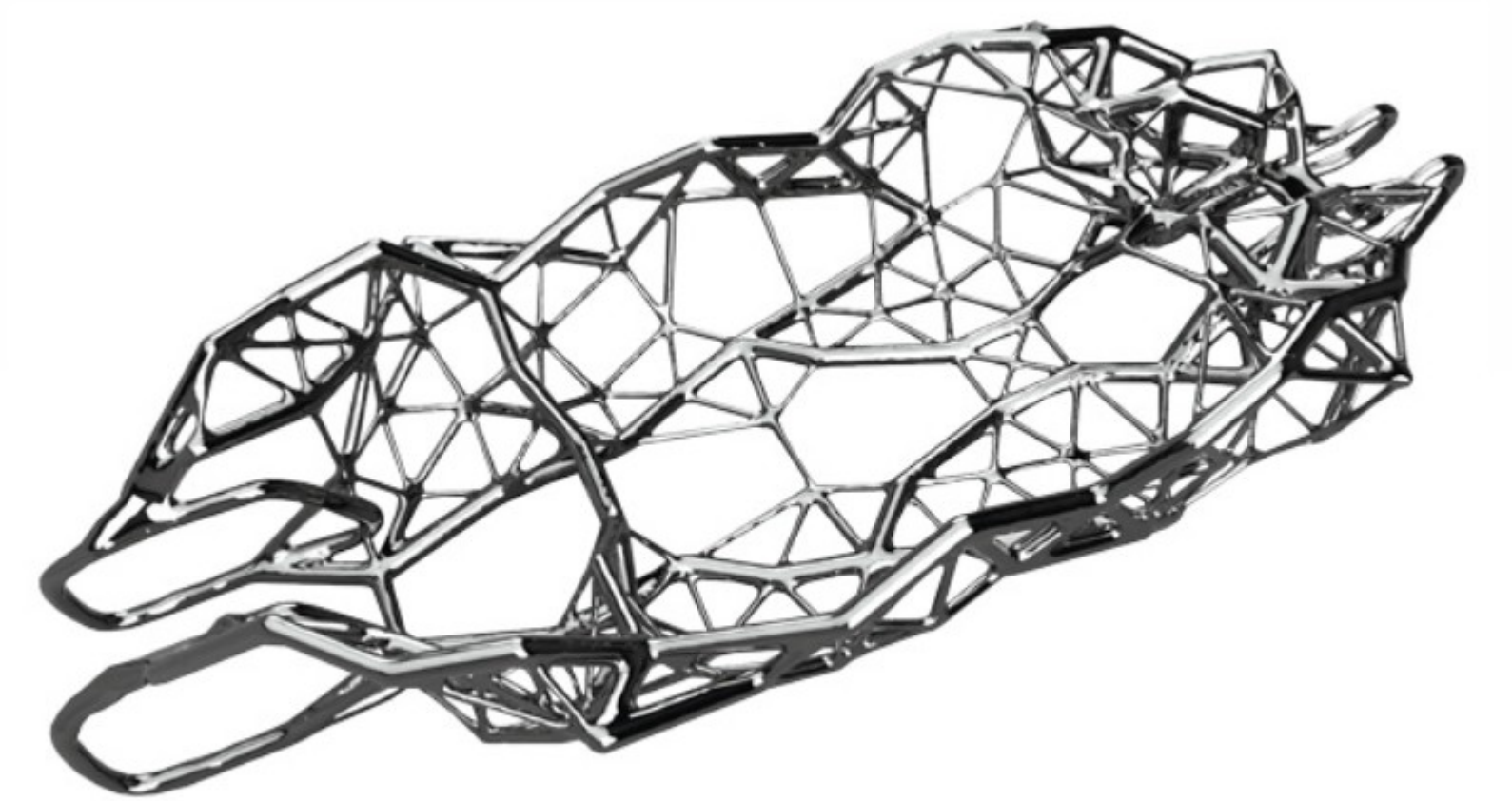
- Outside of ML, AI has been used to generate novel solutions
- For example, evolutionary algorithms are used to to generate solutions to optimization and search problems
- Algorithms often rely on biologically inspired processes such as mutation, crossover and selection

The 2006 NASA ST5 spacecraft antenna. This complicated shape was found by an evolutionary computer design program to create the best radiation pattern. It is known as an evolved antenna.

Generated Designs

NASA's Jet Propulsion Laboratory used generative design to develop a concept extraplanetary lander with lower mass and improved performance.

Generated Designs



Hack Rod and Autodesk used data from sensors in a custom car (and on its driver) to measure strains and stresses. They then fed that data into Dreamcatcher, which used to real-world information to create a new body design that improved the vehicle's ability to withstand those stresses. Images courtesy of Autodesk.

Generative AI - Machine Learning

- GAI creates ML models from existing data to:
  - Create new, realistic artifacts that resemble the training data but doesn't repeat them
  - Creates new text, image, video and other content
- GAI can produce synthetic data
  - The use of GAI to create new data points that are similar to existing data points, x-rays of cancer tumors for example, is called synthetic data
  - Very useful for training models when not enough training data exists
- GAI can produce domain transformations
  - Combines features of two different "types"
  - *Show me my selfie as if it had been painted by Picasso*
  - *Modify this picture so that it shows an evening scene instead of afternoon*
  - *Play "Highway to Hell" in the style of Johnny Cash*

Feature Engineering

- Features or parameters are the properties of our data points
- Feature engineering is selecting and modifying features
  - There are potentially an infinite number of features
  - In ML we have to select only a few to build a model on
- We can also think of each possible feature as a clustering of the data points
  - The problem of feature extraction and selection is a significant one
  - It directly impacts the usability and reality of the model we create
- If we have a large enough training set and enough features
  - We have probability distributions for all the features over data that closely resembles the population from which it is drawn

Generative AI

- Assuming we have a large enough training set and enough features
  - Each data point maps to a very large feature vector, maybe billions of features
  - Assume the data points have labels
  - Then we can generate a new data point from a set of features that are similar to other data points with that label
  - Our GAI model doesn’t track data points but uses the large number of features to identify similarities in the data
  - Think of it a having a probability distribution for each feature, then it can generate something most likely to be what is requested

Generative AI

- This allows for predictive capabilities
  - Given enough data in an input structure (often a sequence like a string of word) it allows for prediction of what comes next
  - This can also be used to generate text string or other sequences
- Transformational capabilities
  - Given two different types of data (images of faces and paintings by Picasso) it is possible to create a new data point with features common to both
  - “Your selfie as if it was painted by Picasso”
  - Create a photo of George Washington drinking wine

People that Don’t Exist

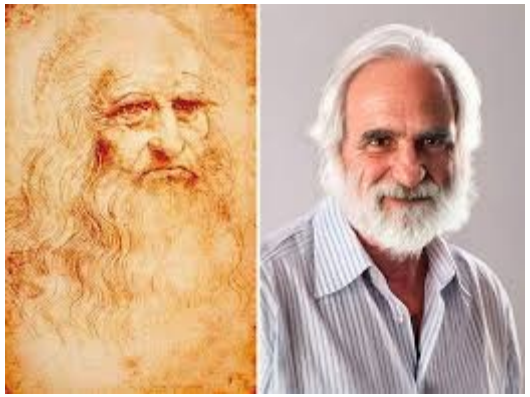
- GAI can produce faces of people that don’t exist by generating them from a model. All of the faces below have been generated

Domain Transfer

- Converting depictions of historical people to photographs





Generative AI

- We pointed out earlier that generative AI required three things to happen
  - Access to enough data to build really big models on petabytes of data and billions of features
  - Enough compute power to train the models
  - A theoretical approach that enables us to build the models
- The rest of this module will focus on the theory that enables generative AI

Traditional Machine Learning

- The rest of this module will cover basics of Machine Learning as background
  - Detailed discussions of the different algorithms is not covered
  - There is some additional material in the repository
- The next module will cover the deep learning background needed

Typology

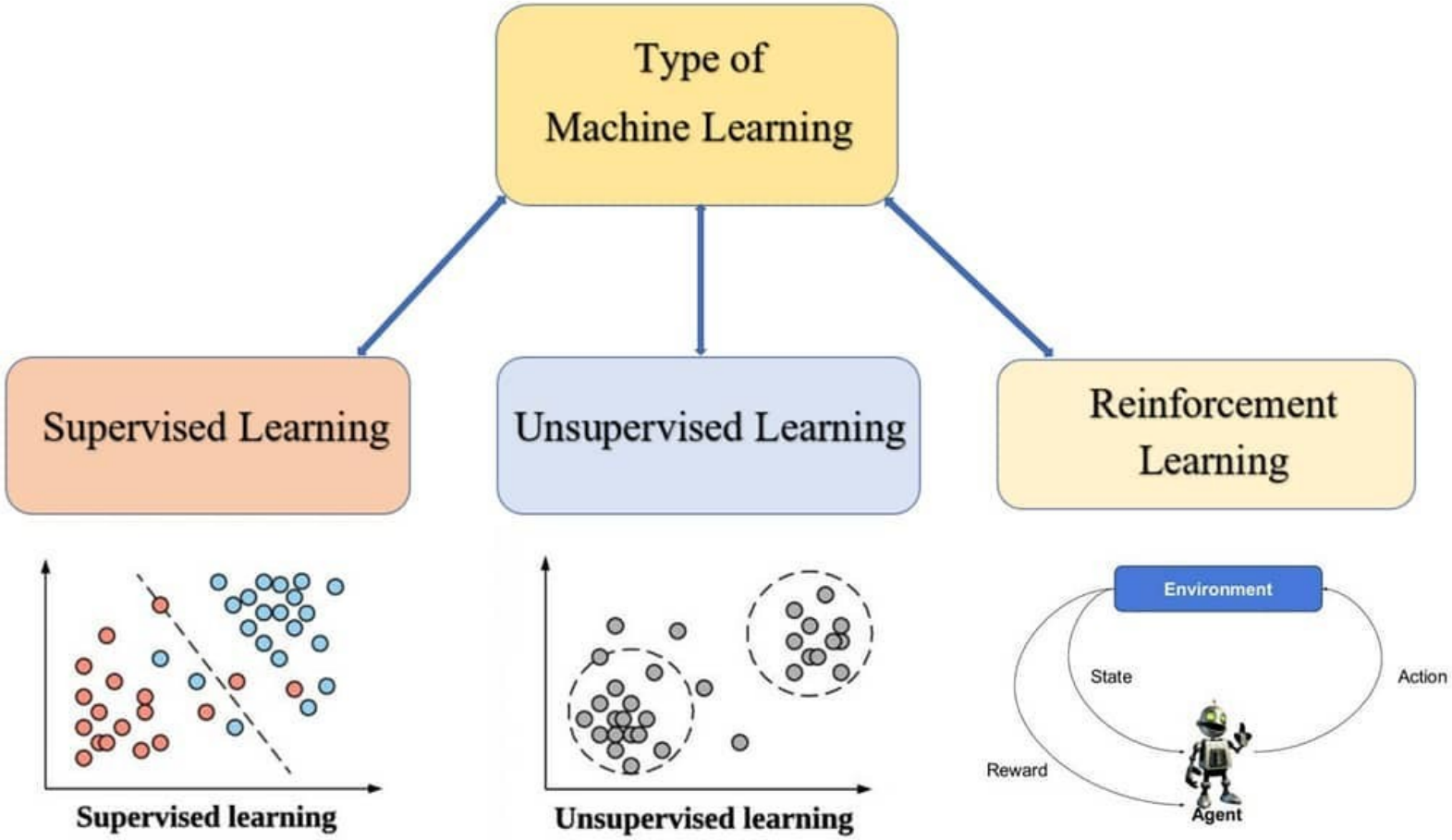


Image Credit: https://www.infinitycodex.in

ML Typology - Supervised Learning

- Each data point in the data set is labeled with the “correct” answer
  - These may be taken from historical data or manually generated by human domain experts
- A portion of the data is used to train the model
  - The “correctness” of the models is calculated by an error function that shows in general how badly or well the model performed on the training data
- The model is tuned to minimize the error on the training set
- The rest of the data is then used to test the model
  - Ideally, the error on the test set should be similar to the error on the training set
  - If not, something called over-training may have occurred where the training set is not representative of the underlying population

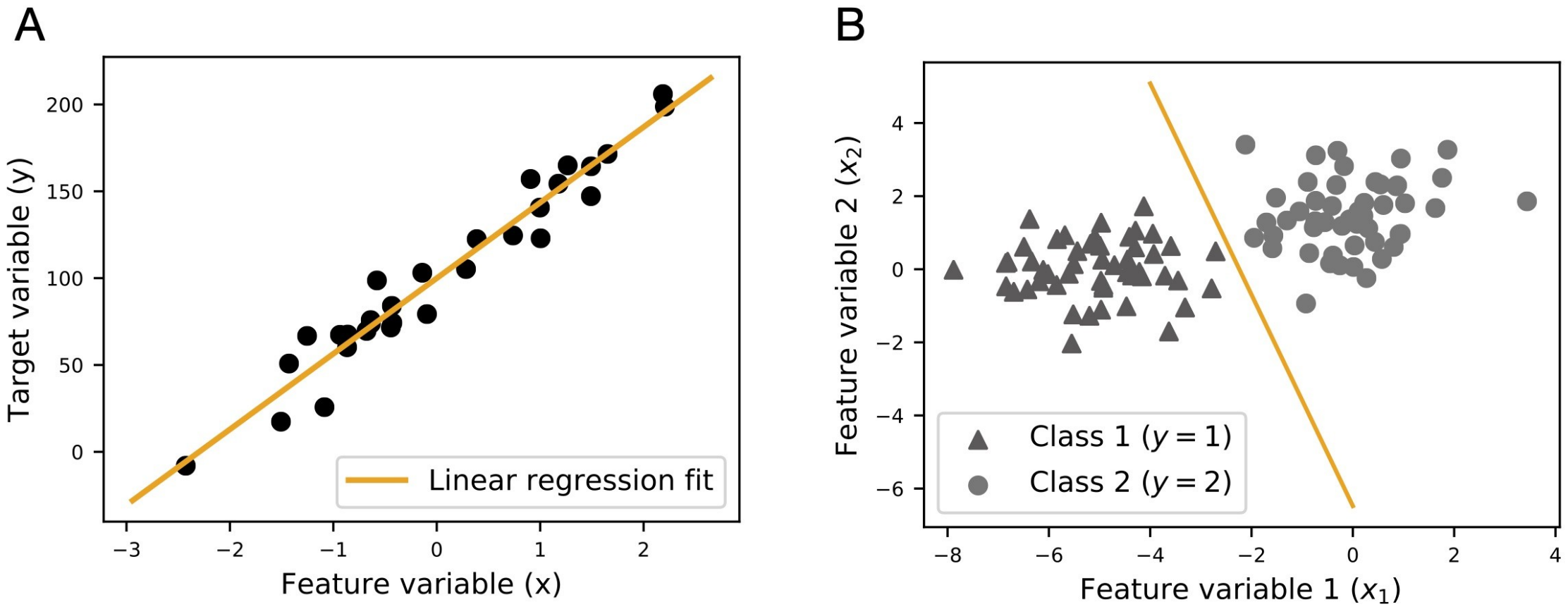
ML Typology - Supervised Learning

- There are two types of Supervised learning models
  - Regression models
    - The output is some predicted value
  - Classification models
    - The output is a category
    - Also called categorical learning model

Regression	Classification
Regression is the task of predicting a continuous quantity.	Classification is the task of predicting a discrete class label.
Regression Means to predict the output value using training data.	Classification means to group the output into a class.
A regression problem requires the prediction of a quantity.	In a classification problem data is labelled into one of two or more class.
If it is a real number or continuous then it is regression problem.	If it is discrete or categorical variable, then it is classification problem.
A regression problem with multiple input variables is called a multivariable regression problem.	A classification problem with two classes is called binary, more than 2 classes is called as multi-classification problem.
Example : Predict the house prices.	**Example** : Is that E-mail is Spam or not a Spam.

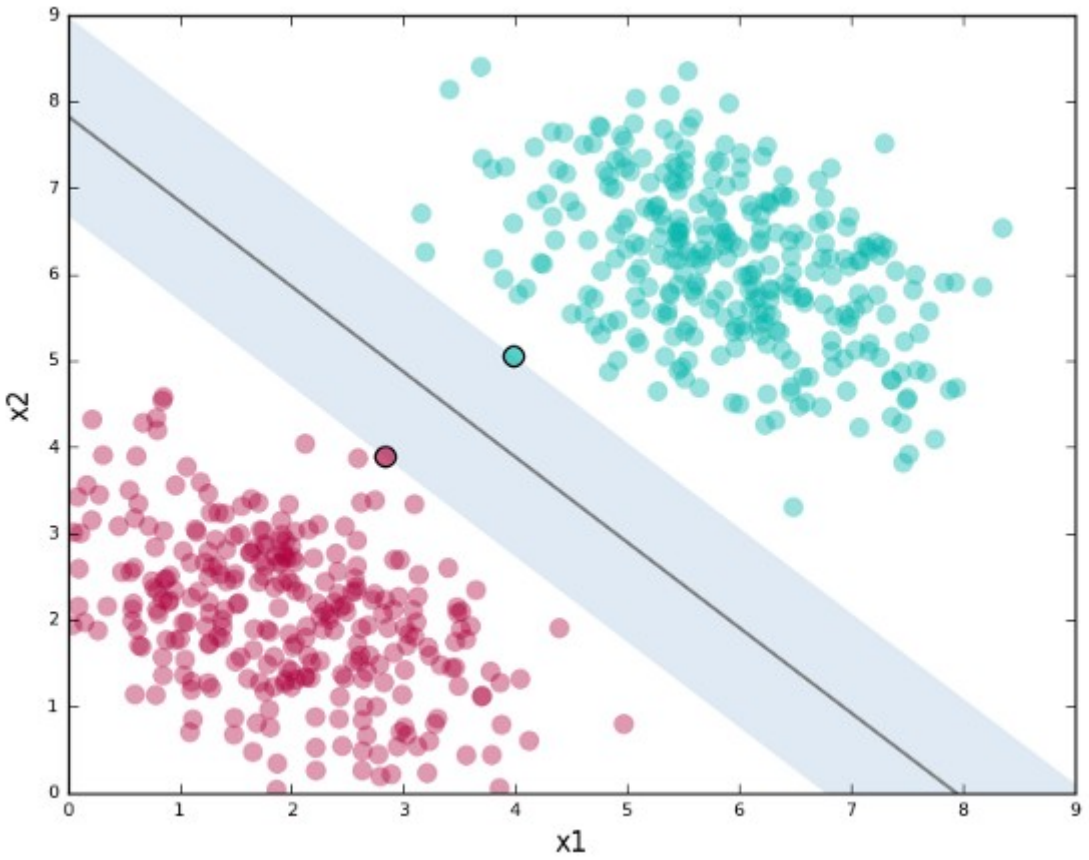
Image Credit: https://www.infinitycodex.in

ML Typology - Supervised Learning



Example - Linear Classifier

- A linear classifier is a hyperplane that divides the data into two sections
  - If the data is 2-d, the hyperplane is a line
- Each possible line is a model or a hypothesis
- A learning algorithm is a process for finding the optimal line
- Optimal can be thought of as the solution having the lowest loss function
- The number of times we run the algorithm is an example of a hyper-parameter



ML Typology - Unsupervised Learning

- Derived from classic data mining algorithms
- Two basic types of problems
- Clustering
  - Looking for groupings in the population via shared features
  - Eg. Do mass shooters fit a common profile of characteristics?
- Association
  - Looking for correlations between data points
  - Eg. If customers buy a car, how likely are they to buy an extended warranty?
- Most unsupervised ML work nowadays tends to be classification

ML Typology - Unsupervised Learning

Clustering vs. Classification

Traditional Clustering

- Goal is to identify similar groups of objects
- Groups (clusters, new classes) are discovered
- Dataset consists of attributes
- Unsupervised (class label has to be learned)
- Important: Similarity assessment which derives a "*distance function*" is critical, because clusters are discovered based on distances/density.

Classification

- Pre-defined classes
- Datasets consist of attributes and a class labels
- Supervised (class label is known)
- Goal is to predict classes from the object properties/attribute values
- Classifiers are learnt from sets of classified examples
- Important: classifiers need to have a high accuracy

ML Typology - Clustering

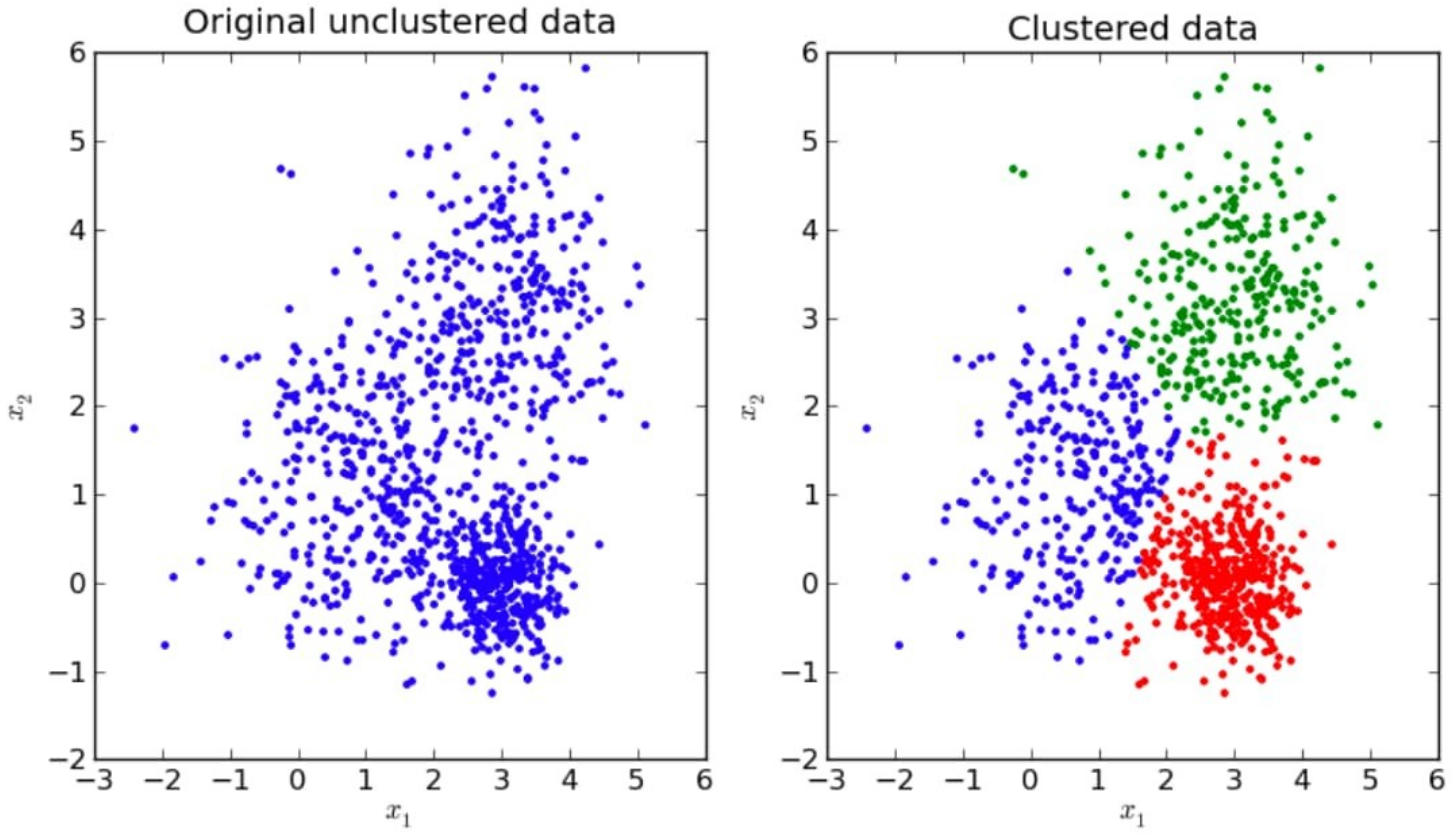


Image Credit:https://vicoranjos.com/technology/what-is-ai-specifically-what-is-machine-learning

ML Algorithms

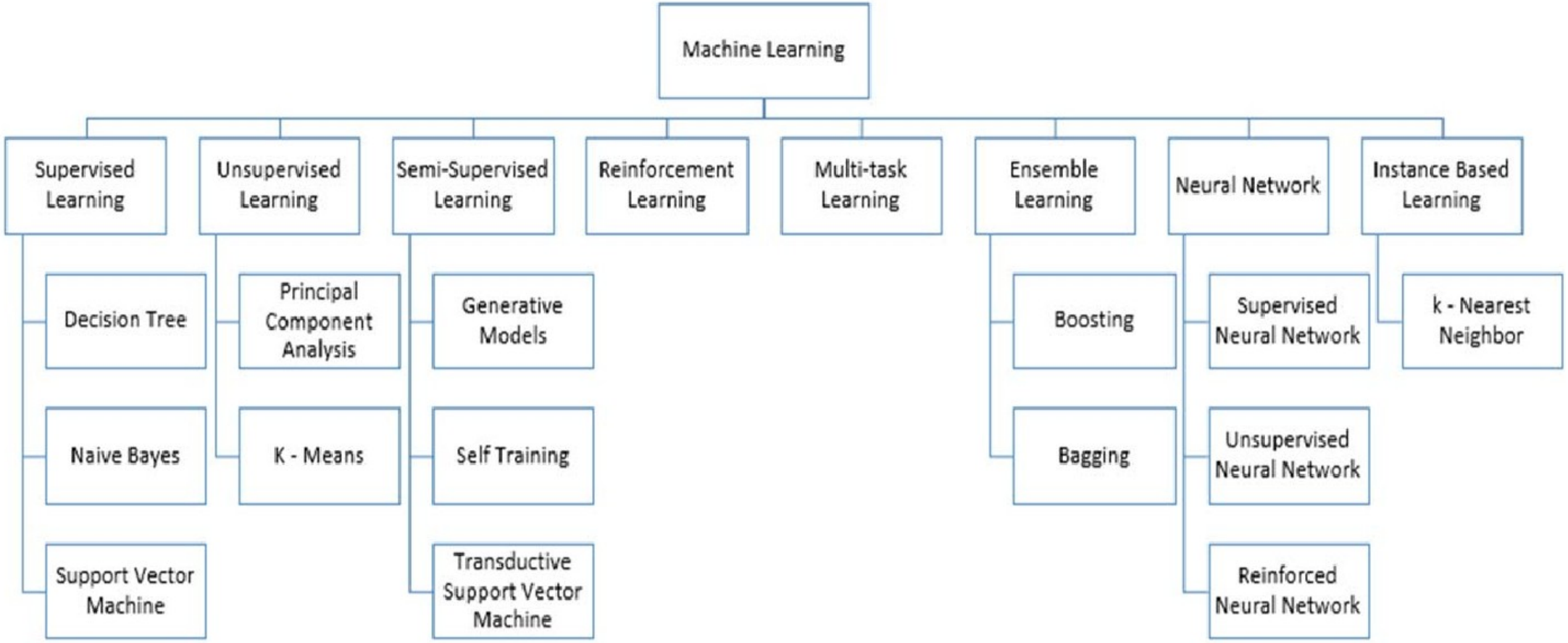


Fig. 1. Types of Learning [2] [3]

Image Credit:https://victoranjos.com/technology/what-is-ai-specifically-what-is-machine-learning

ML Typology - Reinforcement Learning

- Used to determine how agents should make decisions
  - Problems are usually expressed as Markov Decision Processes
  - The agent has some cost function and a reward function
  - It has to optimize a sequence of decisions based on its current state
  - The model is trained to optimize actions based on the training data
- Often called simulation based optimization
  - For example, chess playing programs and AlphaGo use R-ML to decide on what moves to make
  - Heavily used in game theory and economics

ML Typology - Reinforcement Learning

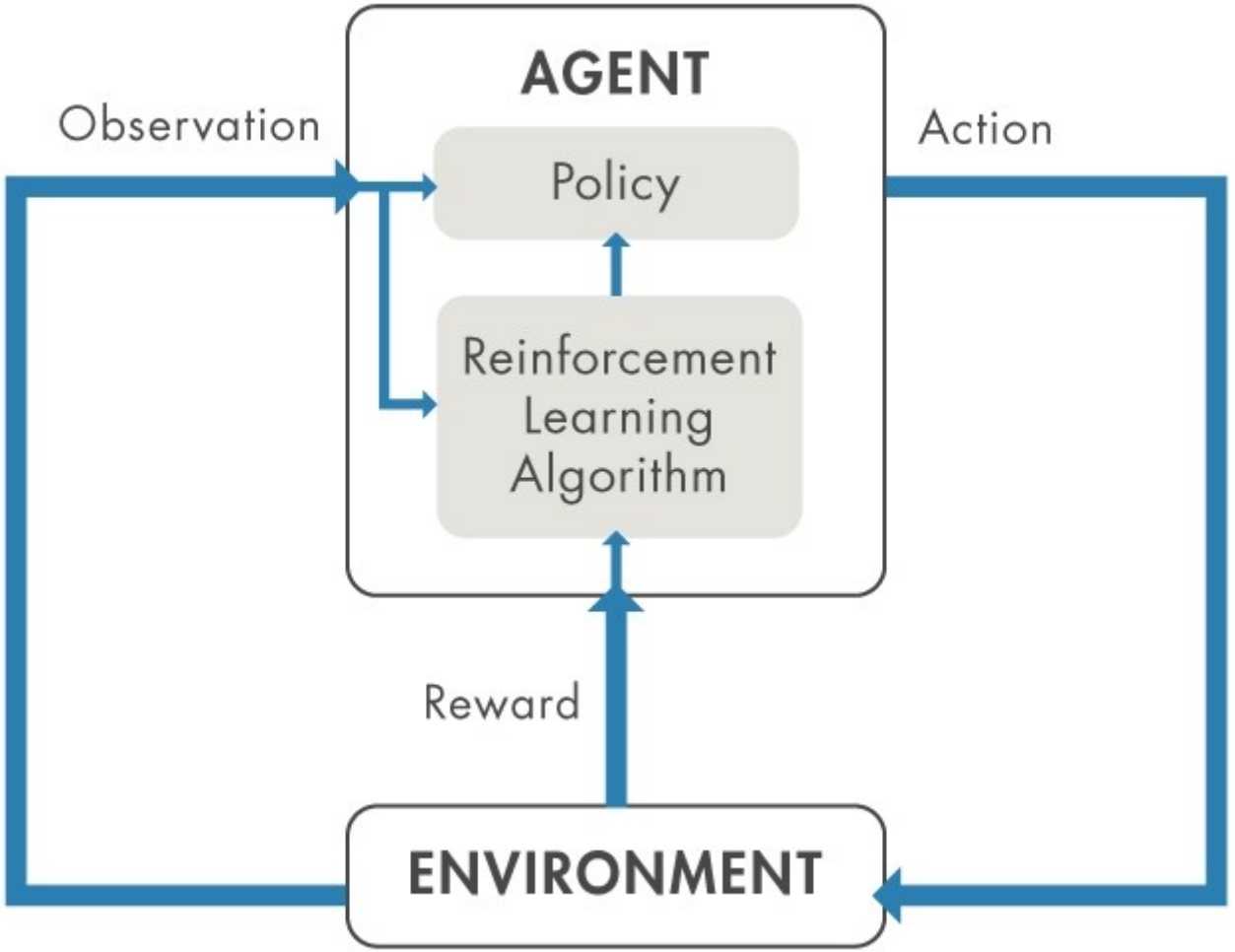
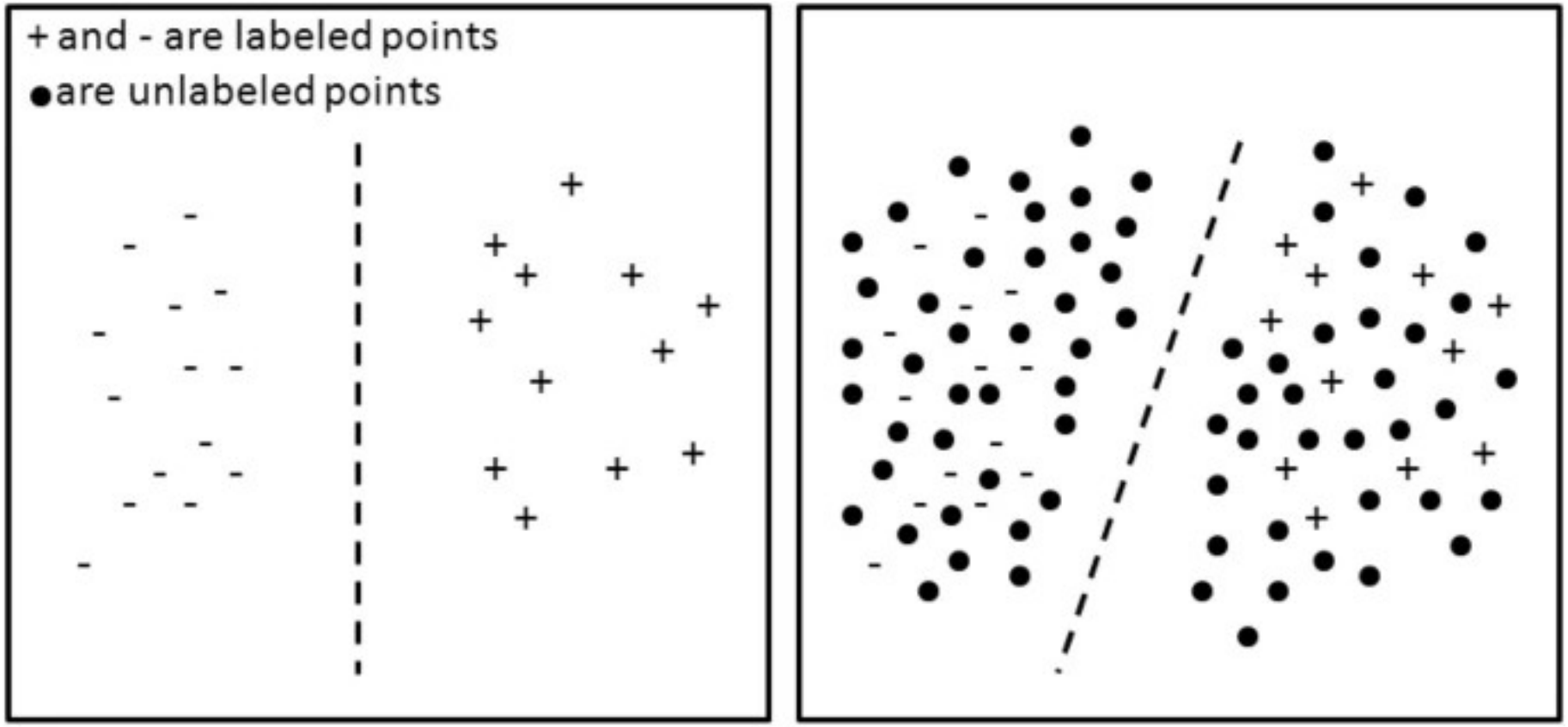


Image Credit: https://www.mathworks.com/company/newsletters/articles/reinforcement-learning-a-brief-guide.html

ML Typology - Semi-supervised Learning

- Hybrid approach often used in real world situations
  - Not all the data in the data set is labeled
  - It may too expensive or otherwise impossible to label all the data
  - Very popular with generative AI
- Two main areas
  - Transductive learning: To infer the correct labels for the unlabeled data
  - Inductive learning: To infer the correct relationships between the data features and the labels
- Adding a small amount of labeled data to a unsupervised learning problem tends to improve performance
  - Data is pretrained on unlabeled data and then fine tuned on labeled

ML Typology - Semi-supervised Learning



AWS Accounts

Lab


Questions?

End Module