



**University of Idaho**

Department of Computer Science

# **CS 4622/5622**

## **Applied Data Science with Python**

*Dr. Alex Vakanski*



# Lecture 1

## A Short History and Current State of Artificial Intelligence

(not required for quizzes or assignments)



# Lecture Overview

---

- Artificial Intelligence vs. Machine Learning vs. Deep Learning vs. Data Science
- How to develop intelligent machines?
- AI timeline
  - DL success in Computer Vision
  - DL success in Natural Language Processing
  - Generative text-to-image models
  - Foundation models
  - Reasoning models
- AI limitations and challenges
- Prospective trends in AI



# Artificial Intelligence

---

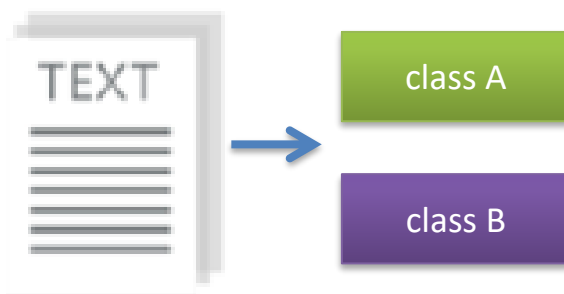
*AI vs. Machine Learning vs. Deep Learning vs. Data Science*

- *Artificial Intelligence (AI)* is a scientific field concerned with the development of algorithms that allow computers to reason or learn without being explicitly programmed
  - AI is opposite to **natural (biological) intelligence** displayed by humans and animals
- AI as an academic discipline was founded in 1956
- AI studies theories and technologies related to:
  - Planning and reasoning
  - Knowledge representation
  - Machine learning
  - Natural language processing
  - Perception
  - Motion and manipulation

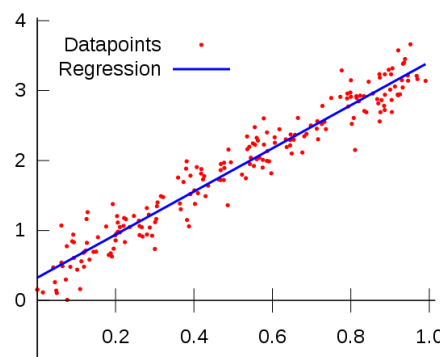
# Machine Learning

*AI vs. Machine Learning vs. Deep Learning vs. Data Science*

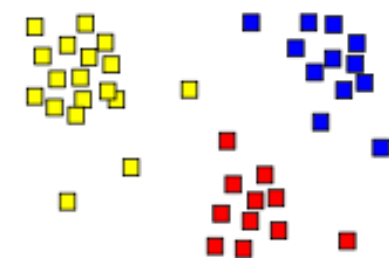
- **Machine Learning (ML)** is a subfield of Artificial Intelligence, that studies methods that learn from data and make predictions on unseen data
- Categories of ML approaches
  - **Supervised learning**: learning with **labeled data**
    - Example: image classification, email classification
    - Example: regression for predicting real-valued outputs
  - **Unsupervised learning**: discover patterns in **unlabeled data**
    - Example: cluster similar data points
  - **Reinforcement learning**: learn to act based on **feedback/reward**
    - Example: learn to play Go or Minecraft



Classification



Regression

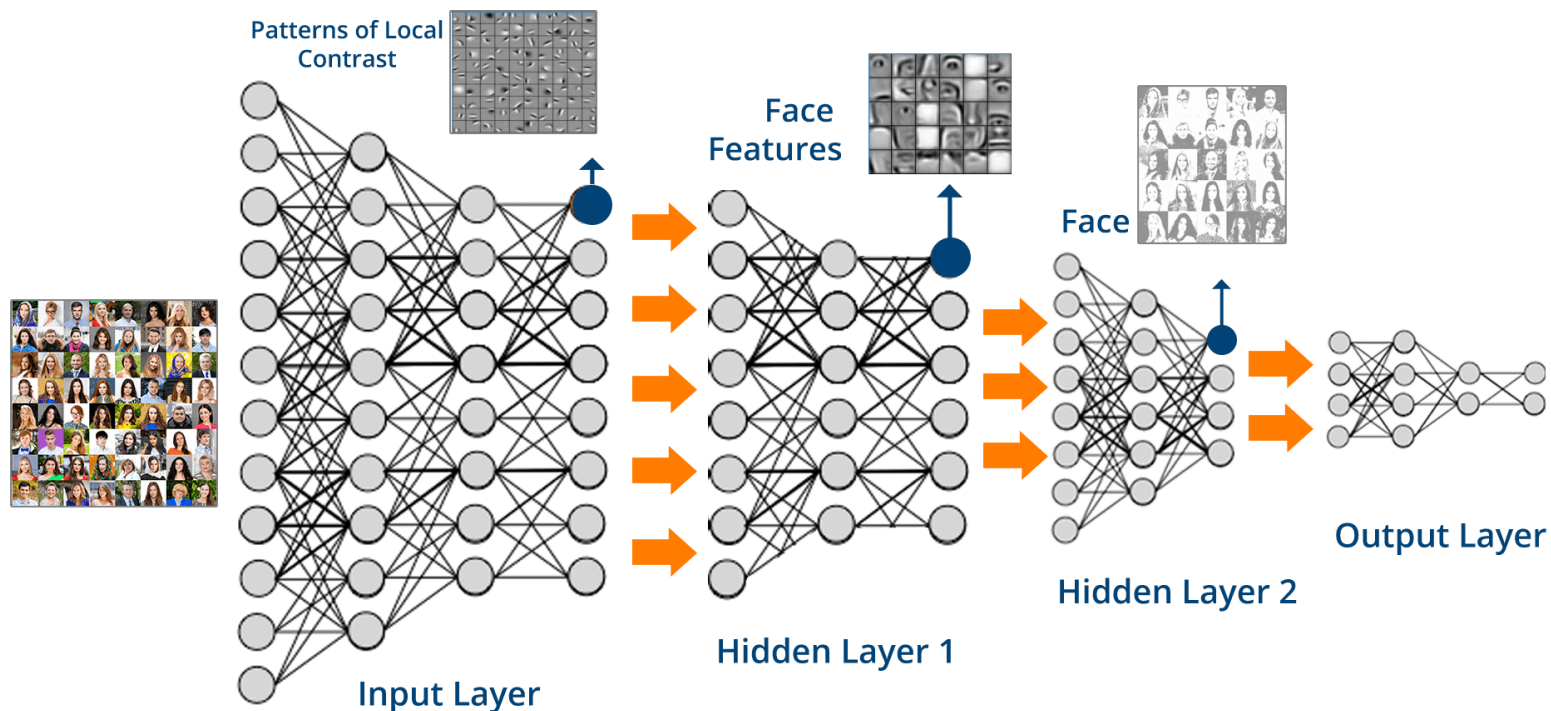


Clustering

# Deep Learning

*AI vs. Machine Learning vs. Deep Learning vs. Data Science*

- **Deep Learning (DL)** is a sub-area in Machine Learning that uses **artificial neural networks** (ANNs) with multiple layers for learning data representations
  - Advantages of DL: ability to automatically extract features in data, processing complex high-dimensional data, scalable with data, model size, and computational power
  - The most common architectures in deep ANNs are: multi-layer perceptron NNs, convolutional NNs, recurrent NNs, graph NNs, transformer NNs

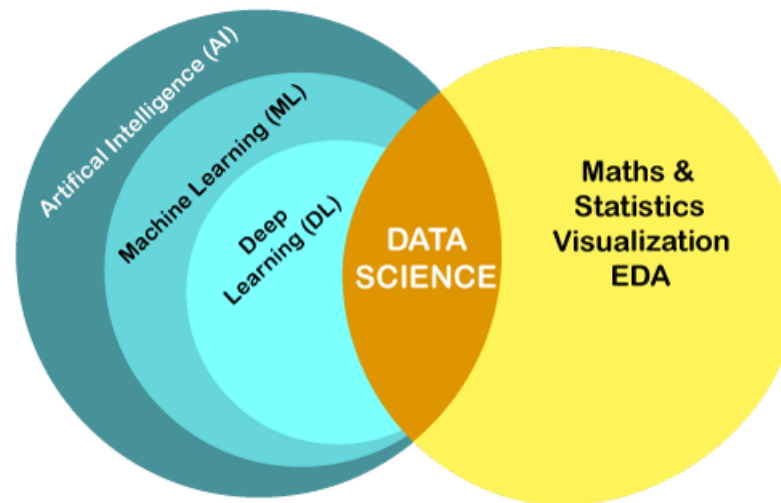


# Data Science

*AI vs. Machine Learning vs. Deep Learning vs. Data Science*

- **Data Science (DS)** is an interdisciplinary field that uses scientific methods and algorithms to extract knowledge from data, and applies the insights to application domains (such as to make business decisions)
- Data Science versus Machine Learning
  - DS has overlaps with ML (as well as with AI and DL)
  - DS can rely on ML approaches, but it can also obtain insights from data via mathematical and statistical analysis, data visualization techniques, exploratory data analysis (EDA), or other approaches that don't necessarily require training an ML model

## AI vs. ML vs. DL vs. DS



# What is Intelligence?

---

## *How to Develop Intelligent Machines?*

- An **intelligent agent** is any system that perceives the environment and takes actions to maximize the chances of achieving its goals
  - Goals can vary, e.g., human goals can be to make a coffee, build a wall, solve a math problem, drive a car, cook a meal, etc.
- **Definition:** *Intelligence* is an agent's ability to achieve goals in a wide range of environments
- Intelligent agents should be able to acquire and retain knowledge, and use it to respond effectively to new tasks or act in new situations and environments
  - E.g., more intelligent humans should be able to solve many physics problems that they haven't seen before (e.g., think of Einstein)
- Intelligence encompasses many related abilities for:
  - Reasoning and rational thinking, comprehending ideas, applying planning, problem-solving
  - Learning and adaptation, dealing with unexpected situations and uncertainties
  - Interacting with the real world to perceive, understand, and act



# How to Develop Intelligent Machines?

---

## *How to Develop Intelligent Machines?*

- AI scientists in 1950s believed that machines with human-level intelligence can be developed within 10 to 20 years
- *Initial AI approaches* included:
  - Imitate step-by-step reasoning that humans use to solve a problem
  - Create a knowledge database based on human domain knowledge about a task, and develop an inference engine to process the states and make decisions
- Challenges: handling uncertainties, combinatorial explosion (the space of solutions quickly becomes too large for most problems)
  - These approaches failed to deliver, as the scientists underestimated the complexity of human intelligence
- Various **misconceptions** about intelligence has perpetuated in the AI field
  - E.g., computers can process information -> human thinking is similar to logic processing -> encoding human thinking into a program can lead to intelligent machines
  - E.g., chess is a game of intellect and chess players are very intelligent people -> developing computers that can reason and play chess at a human expert level can lead to machines with human-level intelligence

# Weak vs. Strong AI

---

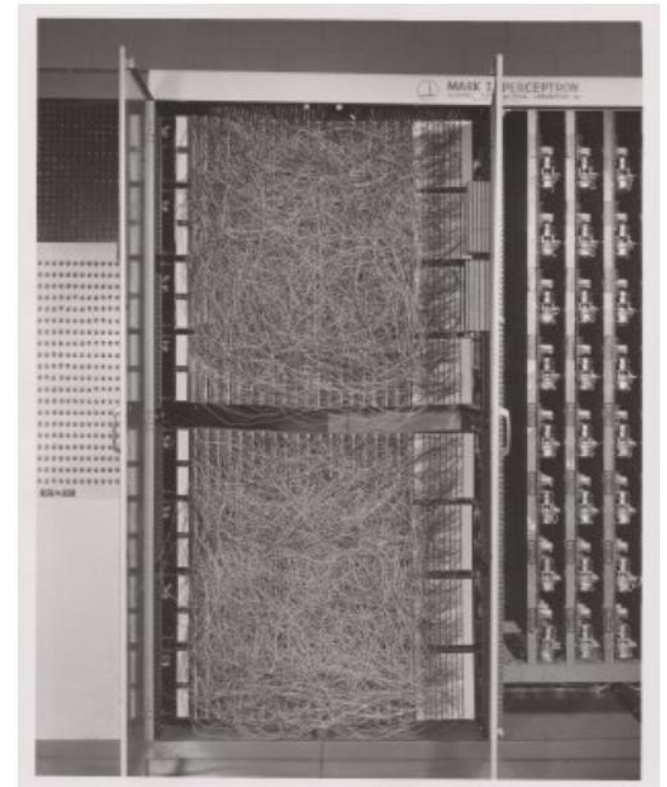
*How to Develop Intelligent Machines?*

- AI systems can be classified into weak AI and strong AI systems
- **Weak AI**, or **narrow AI**: can solve one specific task
  - E.g., image classification ML models
  - E.g., Deep Blue computer that defeated the world chess champion
- **Strong AI**, or **artificial general intelligence (AGI)**: can solve a variety of tasks
  - AGI is the ability to understand or learn any intellectual task that a human being can
    - AGI performance would be indistinguishable from that of humans
  - At present, AGI systems do not exist

# AI Timeline

## AI Timeline

- 1943 – The first model of a simple artificial neuron proposed
- 1950 – Alan Turing introduced the **Turing test**
- 1955 – The **term Artificial Intelligence** used for the first time
- **1956 – Workshop on AI held in Dartmouth College**, New Hampshire, organized by John McCarthy, Marvin Minsky, Nathaniel Rochester, Claude Shannon
  - Official beginning of AI as academic discipline
  - A statement from the workshop proposal: “Every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.”
- 1958 – **Perceptron** algorithm proposed by Rosenblatt
  - Shown is the Mark I Perceptron computer, used for implementing the algorithm



# AI Timeline

## *AI Timeline*

- 1958 – The term **Machine Learning** was used for the first time
- 1961 – The first industrial **robot** Unimate was installed on an assembly line at General Motors in New Jersey
- 1966 – **Eliza**, a chatbot that simulates conversations with a psychotherapist
- 1970-1980 – First **AI winter**, agencies reduced funding for AI projects due to unsatisfactory progress
- 1982 – An expert systems deployed for configuring computer orders
- 1987-1992 – Second **AI winter**, DARPA cut AI funding for expert systems
- 1995 – The advent of machine learning and statistical methods
- 1997 – IBM's supercomputer **Deep Blue** won against world chess champion Gary Kasparov



# AI Timeline

## AI Timeline

- 2002 – Vacuum robots Roomba released
- 2006 – Facebook, Netflix, Twitter started using AI-based recommender systems
- 2011 – IBM's supercomputer **Watson** won against two human rivals in the quiz show Jeopardy
- 2012 – **Deep NN model AlexNet** won image classification contest - *beginning of the era of deep learning*
- 2015 – **GAN** (Generative Adversarial Network) introduced
- 2016 – Google's DeepMind program **AlphaGo** defeated the Go grandmaster Lee Sedol
  - The game of Go is more difficult than chess, because the number of possible moves is much greater



# AI Timeline

---

## *AI Timeline*

- 2017 – **Transformer** network architecture was introduced in the paper by Vaswani et al. “Attention Is All You Need”
- 2020 – OpenAI’s **GPT-3** is the first large language model with 175B parameters, performed well on many NLP tasks
- 2021 – DeepMind’s **AlphaFold** achieved high accuracy in predicting the 3-dimensional shape of proteins
- 2022 – OpenAI’s **DALL·E 2** generated photorealistic images with remarkable quality
- 2022 – Facebook’s **NLLB** (No Language Left Behind) model for machine translation between 200 languages
- 2022 – OpenAI released **ChatGPT**, a large language model with human-like abilities in answering questions and chatting
- 2023 – Meta AI’ **Llama 2** is the first open-source large language model that is freely available for commercial use





# AI Timeline

---

## *AI Timeline*

- 2023 – Mistral released Mixtral LLM, a **mixture-of-experts model** that integrates 8 LLMs, and outperformed larger models on standard benchmarks
- 2023 – Google launched **Gemini**, Anthropic launched **Claude 3**: both reached the top spot on standards benchmarks at the time of launching
- 2024 – **Vision-Language models** (GPT-4 omni, LlaVA, Claude) for image interpretation and analysis
- 2024 – **Multi-Agent frameworks** (LangChain, AutoGPT, AutoGen) connect to other services and provide assistance in making reservations, planning a trip, etc.
- 2025 – **Turing test** passed by GPT-4.5, it was mistaken for human 73% of the time
- 2025 – GPT-o3 and Gemini Deep Think won **gold medal** at the International Mathematic Olympiad (IMO)

# DL Success in Computer Vision

## *DL Success in Computer Vision*

- **Computer Vision** tasks
  - Image and video recognition/classification, segmentation, object detection, image synthesis
- Important architectures in CV
  - AlexNet – 2012
    - Convolutional NNs for image recognition, 5 layers, GPU for parallel processing
    - ImageNet Large Scale Visual Recognition Challenge (ILSVRC): AlexNet reduced the error on ImageNet from 26% by traditional ML approaches to 15%
  - VGG – 2014
    - 16 layers CNN architecture
  - Inception – 2015
    - Stacked 1x1 convolutions, 22 convolutional layers
  - ResNet – 2015
    - Introduced residual connections, it is a family of networks with 18, 34, 50, 101, and 152 layers
    - Several related models were proposed afterwards, e.g., ResNeXt (2017), EfficientNet (2019)
  - Vision Transformers (ViT) – 2020
    - Employ attention layers, inspired by the transformer models used in NLP





# DL Success in Natural Language Processing

---

## *DL Success in Natural Language Processing*

- *Natural Language Processing* (NLP) tasks
  - Text classification, text summarization, speech recognition, machine translation, dialog generation, part-of-speech tagging
- In the last 8 years, *Large Language Models (LLMs)* powered by transformer NNs achieved unprecedented success in NLP tasks
  - The quality of generated text by recent LLMs is often undistinguishable from human-written text
- Examples of LLMs include:
  - GPT-4: OpenAI, 1.76T (trillion) parameters
  - Gemini 2.5 Pro: Google, 1.5T parameters
  - Claude 4 Opus: Anthropic, 2T parameters
  - Llama 3.1: Meta AI, 405B parameters
- Note that compared to the human brain having between 100 and 500 trillion synaptic connections, current LLM models are still fairly small

# Large Language Models

*DL Success in Natural Language Processing*

- *Training data* for LLMs
  - LLMs are typically trained on diverse sets of text data gathered from the web
    - E.g., text collected from Wikipedia, e-books, news articles, and many other sources
- *LLMs training*
  - Data preprocessing: LLMs take as inputs words projected into an embeddings space, where each word is replaced with a numerical **token**
  - Given a sequence of words (tokens) from a dictionary, the training objective is to predict the next word (i.e., assign the probability of the next token)

Input: A quick brown	Output: <b>fox</b>
Input: Marry had a little	Output: <b>lamb</b>
Input: Nothing is	Output: <b>impossible</b>
  - This is a form of **unsupervised learning**, since there is no need to label the data
- *Fine-tuning*
  - To adapt LLMs for specific tasks, the trained models are typically fine-tuned on smaller, specific datasets
  - Recent LLMs are often fine-tuned via Reinforcement Learning from Human Feedback, where humans rank the generated text, and the feedback is used to fine-tune the model

# Large Language Models

*DL Success in Natural Language Processing*

- *LLM network architecture*

- The architecture of all LLMS is based on the **transformer** neural networks
- Transformers employ the **attention mechanism** to identify the words in a sentence that impact the meaning of other words
- I.e., an important characteristic is the ability for modeling words based on the context

- Challenges

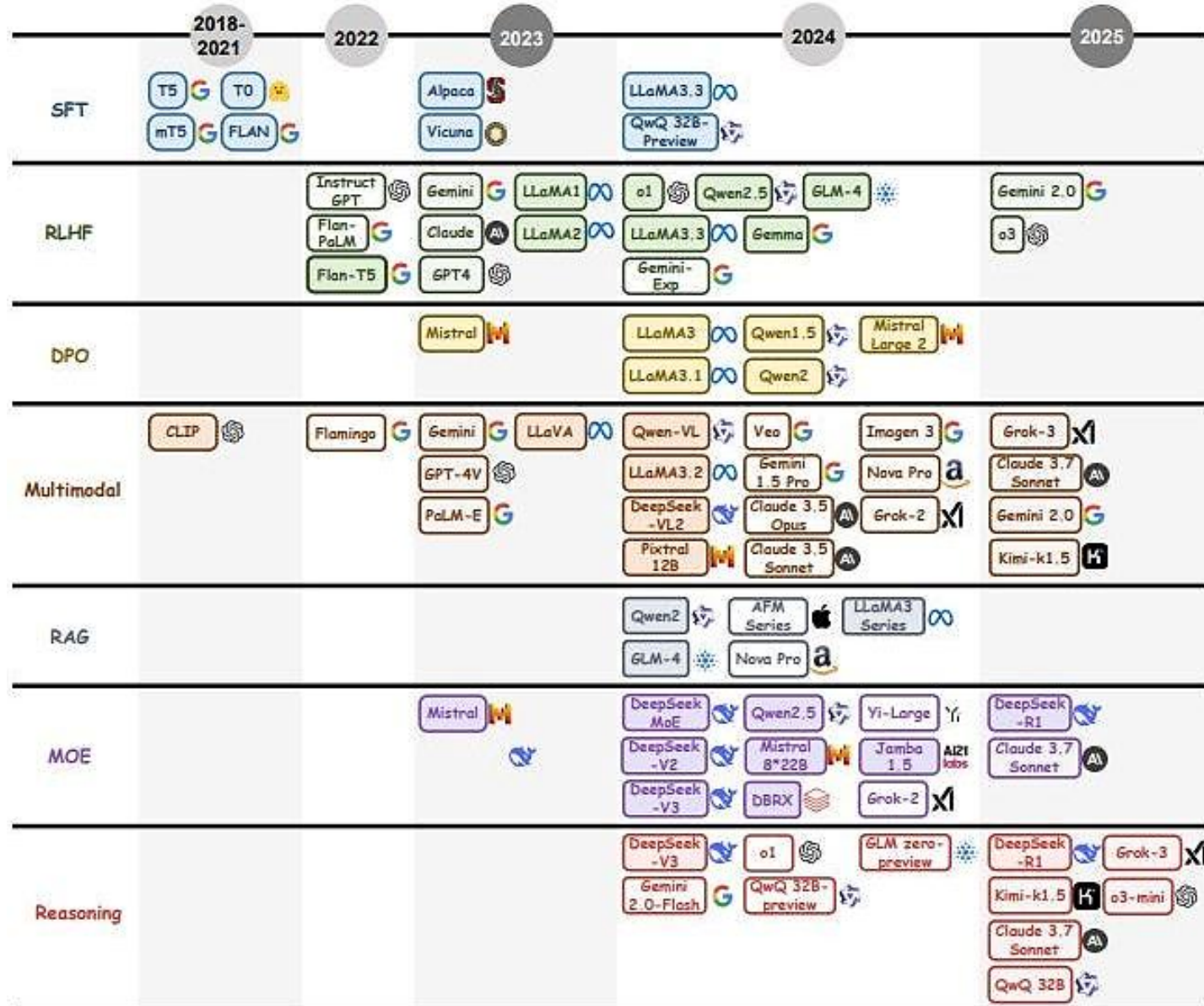
- Training LLMs requires substantial computational resources and time
  - E.g., GPT-3 was trained for 36 days with 1,024 NVIDIA A100 GPUs, resulting in an estimated training cost of \$12M
  - GPT-4 was probably trained on between 10,000 and 20,000 A100 GPUs
  - Currently, Meta AI has about 20,000 A100 GPUs, Microsoft has about 40,000 H100 GPUs, Stability.ai has about 5,000 A100 GPUs, Inflection AI has 22,000 H100 GPUs
    - E.g., purchasing cost of A100 GPU is about \$15K -> cost of 10,000 A100 GPUs is about \$150M
    - E.g., purchasing cost of H100 GPU is about \$40K -> cost of 20,000 H100 GPUs is about \$800M

- Concerns regarding LLMs

- Misuse and unethical use of AI, amplifying disinformation, environmental impact (high carbon emissions), increasing economic inequalities, centralization of power (e.g., affordable only by the largest corporations)

# Timeline of Large Language Models

*DL Success in Natural Language Processing*





# LLMs Leader Board by LMSYS

*DL Success in Natural Language Processing*

Rank (UB) ↑	Model ↓	Score ↓	95% CI (±) ↓	Votes ↓	Organization ↓	License ↓
1	 gpt-5-high	1481	±11	3,181	OpenAI	Proprietary
2	 gemini-2.5-pro	1458	±5	28,091	Google	Proprietary
2	 o3-2025-04-16	1451	±5	34,027	OpenAI	Proprietary
2	 claude-opus-4-1-20250805	1446	±9	5,187	Anthropic	Proprietary
4	 chatgpt-4o-latest-20250326	1440	±5	32,125	OpenAI	Proprietary
4	 gpt-4.5-preview-2025-02-27	1438	±6	15,271	OpenAI	Proprietary
5	 grok-4-0709	1430	±6	14,078	xAI	Proprietary
5	 qwen3-235b-a22b-instruct-2507	1428	±8	6,097	Alibaba	Apache 2.0
7	 kimi-k2-0711-preview	1420	±6	13,578	Moonshot	Modified MIT
7	 claude-opus-4-20250514-thinking-16k	1420	±6	19,330	Anthropic	Proprietary
8	 deepseek-r1-0528	1418	±6	19,389	DeepSeek	MIT
8	 glm-4.5	1414	±8	5,907	Z.ai	MIT
9	 claude-opus-4-20250514	1412	±5	27,428	Anthropic	Proprietary

# Generative Text-to-Image Models

## *Generative Text-to-Image Models*

- *Generative models* learn to generate new data instances, given a training set
- **Text-to-image models**
  - [DALL·E 2](#) by OpenAI
  - [Imagen](#) by Google
  - [Stable Diffusion](#) by Stability.ai
- These text-to-image models employ text embeddings from pretrained LLMs (e.g., GPT used with DALL·E 2)
  - Produce images with remarkable photorealism, accurate fine details, compositionally, spatial relations of the objects in images, and even with creativity in image synthesis
  - They employ **diffusion probabilistic models**, which use NNs to learn the steps of adding and removing noise to images
  - Can create new images which are unlikely to have been seen in the training data



# Images Generated by DALL·E 2

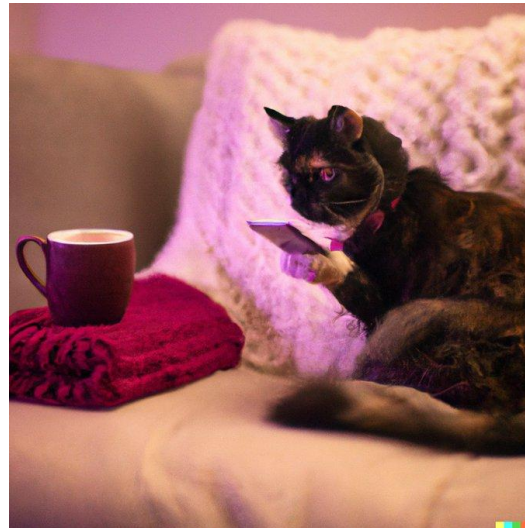
## *Generative Text-to-Image Models*

- These are a few (cherry-picked) examples of images generated by DALL·E 2

A photo of a quaint flower shop storefront with a pastel green and clean white facade and open door and big window



Cat sipping tea and posting to twitter while sitting on a couch



A rabbit detective sitting on a park bench and reading a newspaper in a victorian setting



A lion in a hoodie hacking on a laptop



Teddy bears shopping for groceries in ancient Egypt



Teddy bears working on new AI research on the moon in the 1980s



# Foundation Models

---

## *Foundation Models*

- **Foundation models** are large NN models trained at **scale** with high capabilities for **transfer learning** to many other applications
  - Early examples of foundation models are LLMs, such as GPT-4 and PaLM
- The scale of these models results in new **emergent capabilities** – e.g., they perform well on tasks on which they were not explicitly trained to do
  - “**Emergence** is when quantitative changes in a system result in qualitative changes in behavior”
  - This allow fine-tuning to new tasks with small number of training data instances
    - E.g., **few-shot learning** refers to fine-tuning with only a few instances
- Notable applications of pretrained LLMs include:
  - Programming code completion models: CoPilot, AlphaCode, Codex, Codegen
  - Text-to-image generative models: DALL·E 2, Imagen, Stable Diffusion
  - Protein sequence prediction, solving math problems, preparing legal documents (other task examples are listed on the next page)
- Transfer learning is what makes foundation models possible, but scale is what makes them powerful



# Foundation Models

## Foundation Models

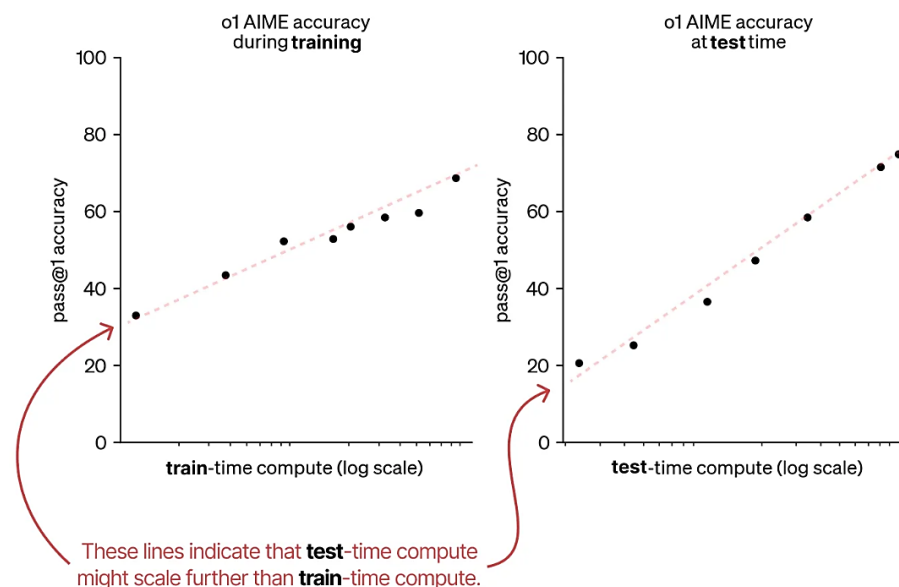
- Examples of applications and downstream tasks in which foundations models are being used

<b>Program writing</b>	<b>Image captioning</b>	<b>Generate images</b>	<b>Parse data</b>	<b>Classify text</b>
Use natural language to generate SQL/Python/Java code	Describe and classify images	Create images based on natural language	Extract data from images	Identify entities, parts-of-speech, and other text categories
<b>Q&amp;A</b>	<b>Writing assistant</b>	<b>Summarize</b>	<b>Solve homework</b>	<b>Translate</b>
Answer natural language questions based on knowledge base	Correct your writing	Summarize text to key concepts	Solve basic math and programming problems	Translate text from one language to another
<b>Code explanation</b>	<b>Copywriting</b>	<b>Sentiment rating</b>	<b>Recipe creation</b>	<b>Chat</b>
Writes the description of code functionality in natural language	Generate ad/product/job descriptions based on short prompts	Rates the sentiment, toxicity, warmth, etc. of text	Use at your own risk	Talks like a human

# LLM Scaling Laws

## LLMs Scaling Laws

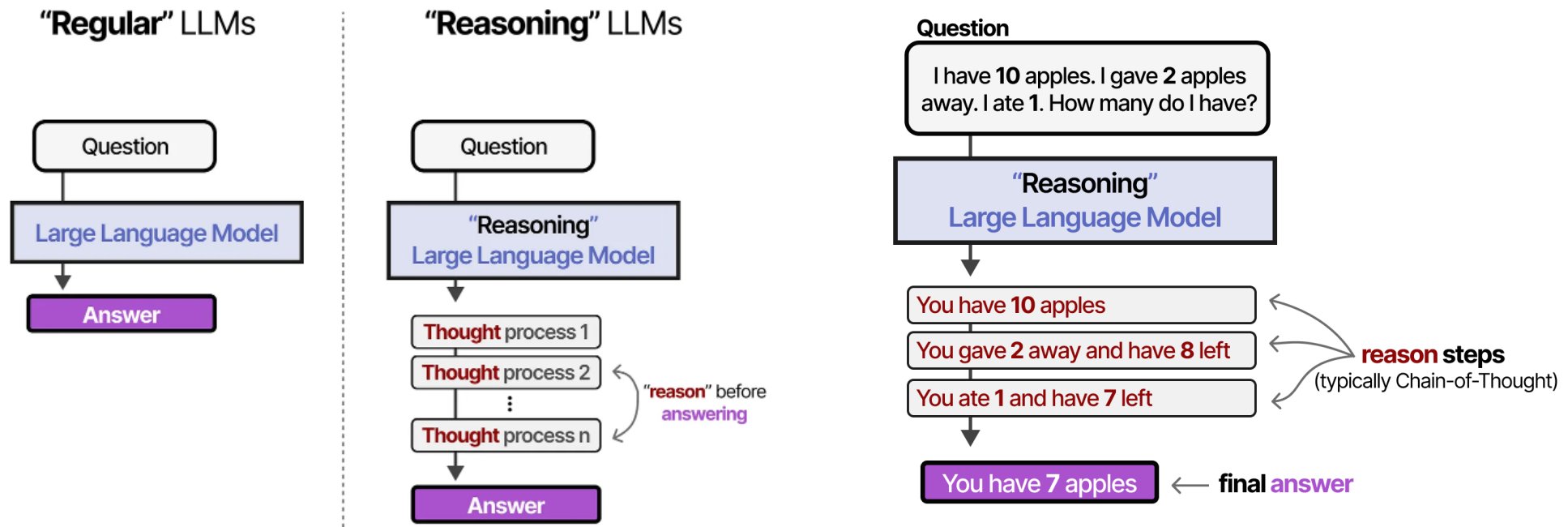
- LLM *scaling laws* provide a relationship between the model's performance and model's scale (typically shown on a log scale)
  - Well known **train-time compute scaling laws** include Chinchilla and Kaplan laws (see left figure below)
    - They indicate that performance increases with more compute, tokens, and parameters
  - OpenAI's **test-time compute scaling law** (right figure below) suggests that test-time compute follows the same trend as train-time compute
    - Performance improves by allowing LLMs to “think longer” during inference



# Reasoning LLMs

## Reasoning LLMs

- **Reasoning LLMs** perform multiple reasoning steps before providing an answer at test time
  - The **reasoning steps** or **thought process** break down the inference process into smaller, structured inferences (**Chain-of-Thought**)
  - Reasoning LLMs: OpenAI o1 and o3, DeepSeek-R1, Google Gemini 2.0 Flash Thinking, and actually most of the latest LLMs have reasoning abilities





# AI Agents

---

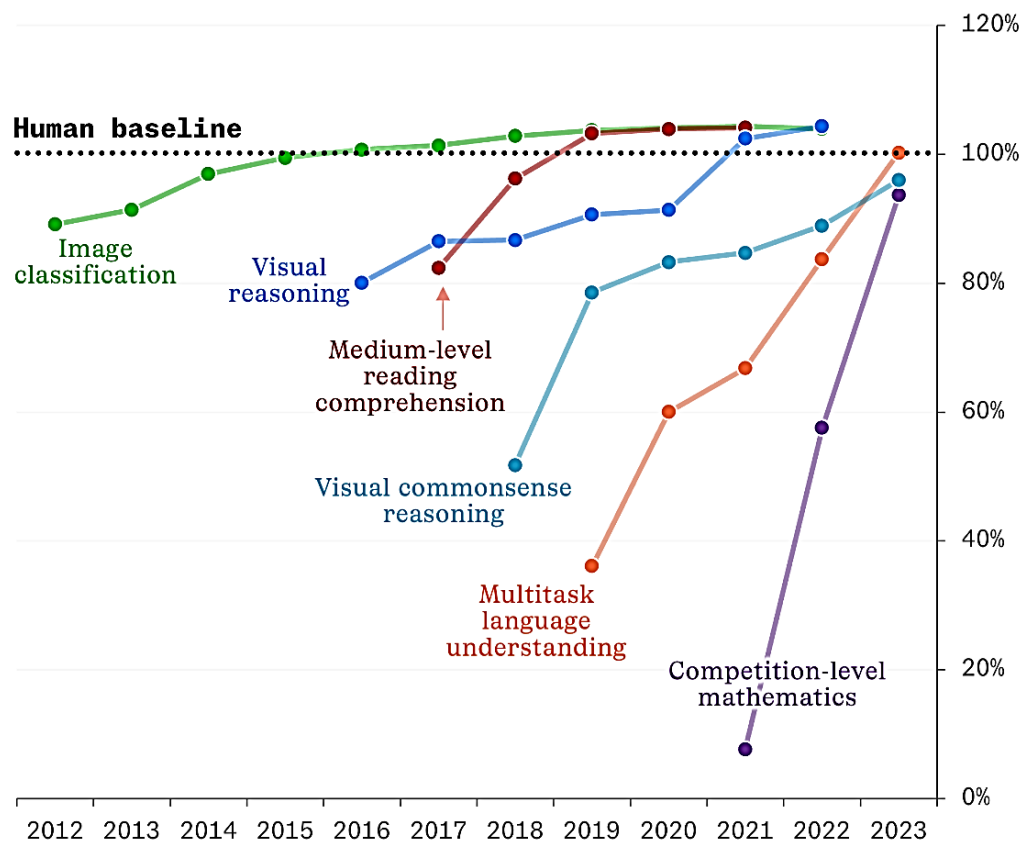
## *AI Agents*

- *AI Agents* use LLMs to understand instructions, reason through tasks, and take actions across digital tools or environments
- Abilities
  - Interpret natural language commands
  - Plan multi-step solutions
  - Call external tools (e.g., web search, code execution)
  - Adapt behavior based on feedback
- Examples of use
  - Automating document analysis
  - Running complex simulations
  - Managing workflows (e.g., email sorting, report writing)
  - Scientific discovery and literature review

# Progress in AI

## *Progress in AI*

- The graph shows a comparison between AI performance and human baseline performance (100%) on benchmarks dataset for several tasks
  - E.g., handwritten recognition is evaluated on MNIST dataset, image recognition is based on ImageNet dataset, etc.





# Engineering vs Science Phase of Technology

## *AI Limitations and Challenges*

- Theoretical guarantees about the AI performance are lacking at present time
  - Currently, AI is in *Engineering phase*: models are designed to solve tasks, are integrated into new products, add value to companies, have economic impact
  - *Science phase* of AI is to follow: theory is developed to guarantee convergence, prove stability, interpret the decisions, explain successes and failures of models
- Various technologies historically began with an engineering phase (inventions made, products built) to be later followed by a science phase (theory developed)
  - Steam engines were used in paper mills and factories since 1776; the theory of Thermodynamics was developed between 1820s and 1850s
  - Airplanes were constructed and flown since 1904-1905; the modern theory of Aerodynamics was developed in 1930s
  - Electric circuits were discovered around 1800; the theory of Electromagnetism was founded between 1820s and 1830s

# Trustworthy AI

## *AI Limitations and Challenges*

- **Trustworthy AI** – efforts to address the limitations to ensure that end-users can trust the predictions by AI models
- Topics in trustworthy AI include:
  - **Robustness**
    - Even unnoticeably small perturbations can impact the model predictions
  - **Generalization**
    - OOD (out-of-distribution) inputs; e.g., a model trained on medical images in one hospital performs poorly on images in another hospital (due to different equipment or settings used)
  - **Explainability**
    - The decision-making process of large models is non-transparent and difficult to understand
  - **Fairness**
    - Predictions can show bias against demographic groups, based on gender, age, culture
  - **Privacy protection**
    - Models can memorize and reveal input data; e.g., a model can reveal sensitive private information in medical records used for training
  - **Ethics**
    - The models should produce ethical decisions that are aligned with our human values (also referred to as **AI Alignment**)

# Moravec's Paradox

---

## *AI Limitations and Challenges*

- The paradox is based on observations by the researcher **Hans Moravec**: the hard problems for humans are easy for computers, and the easy problems for humans are hard for computers
  - E.g., it is easier for computers to play chess or solve logic problems, than to make a coffee or plant a tree
  - Robotic tasks that involve sensorimotor and perception skills are more difficult than planning and reasoning tasks
- One possible explanation of Moravec's paradox is because sensorimotor skills are older and developed earlier in the evolution than reasoning skills
  - We can perform skills like recognizing a face, moving in space, or catching a ball unconsciously and effortlessly, because they have been optimized over millions of years
  - Abstract thinking, reasoning, or solving math problems are thousands of years old skills that we haven't mastered completely, and we need to put more effort
- We should expect that the difficulty to reverse-engineer a skill is proportional to the amount of time it took for the skill to develop in animals



# The Bitter Lesson

---

## *AI Limitations and Challenges*

- *The Bitter Lesson* (2019) is a short paper by Rich Sutton
  - <http://www.incompleteideas.net/IncIdeas/BitterLesson.html>
- The Bitter Lesson is based on his observations regarding the historical development of AI methods, which can be characterized with three phases:
  - Phase 1 - AI researchers incorporate human domain knowledge into their AI methods, which helps in short term
  - Phase 2 - In the long term, the performance of such models plateaus without further progress
  - Phase 3 - Progress is eventually achieved by general methods that scale computation with search and learning
- In conclusion:
  - AI methods that **leverage computation and search at scale** are the most effective
  - Human-centric approaches complicate methods and make them less suited to leveraging computation and search at scale
  - The search for solutions should be done by our methods, not by us
  - We need AI methods that can discover like us, and not based on our discoveries

# Prospective Trends in AI

---

## *Prospective Trends in AI*

- *Unsupervised/self-supervised learning*
  - Increased reliance of methods that learn from raw data without annotations or labels
- *Training/testing at scale*
  - Further scaling along the three main factors: amount of computation, number of model parameters, and training dataset size
  - Test-time compute scaling offers additional potential for performance improvement
- *Multi-modal learning*
  - Capacity to learn from multiple sources of information: text, audio, video, sensor data
  - Task-specific models replaced with general models capable of solving multiple tasks
- *Agentic frameworks*
  - Development of domain-specialized AI agents that use external tools, apply multi-step reasoning, and perform actions
- *New algorithms (e.g., reinforcement learning, neuro-symbolic learning)*
  - Advances in reinforcement learning for autonomous exploration and adaptation, methods that combine neural and symbolic reasoning, etc.