

Applied Machine Learning (COMP0081)

Matt Kusner & Brooks Paige
Computer Science



Administrative Stuff



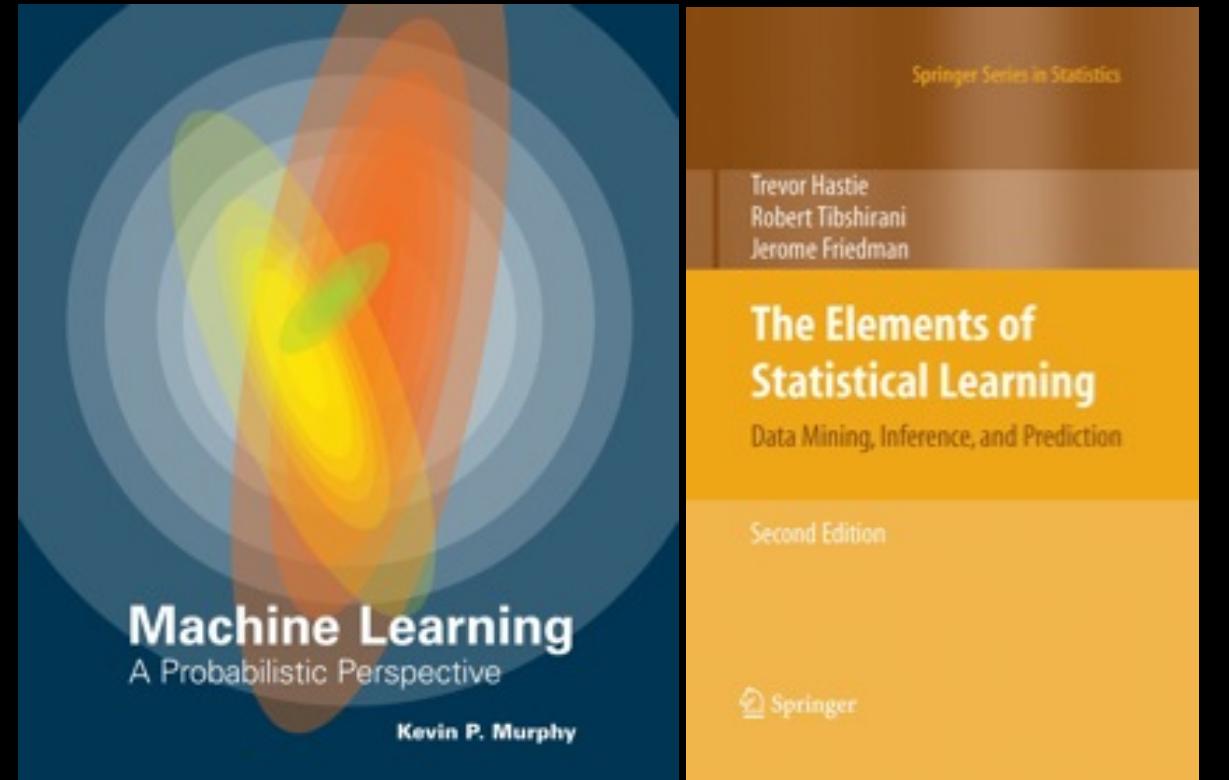
Course Overview

- Instructors: Matt Kusner and Brooks Paige
- Homepages:
 - Moodle: <https://moodle.ucl.ac.uk/course/view.php?id=30005>
 - Autograder: <https://tinyurl.com/COMP0081CourseworkWorkflow>
- TAs:
 - Muhammad Ali Chaudhry
 - Xuyao Feng
- Lectures / Q&A Sessions / Guest Talks:
 - Lectures: **Pre-recorded online**
 - Q&A Sessions + Guest Talks: **Tuesday 1pm, Wednesday 10am, In-Person**
- TA Office Hours: (Details will be posted on Moodle.)
 - TODO Leave Feedback: <https://tinyurl.com/COMP0081OfficeHourFeedback>
- Questions:
 - Post all questions on Moodle (you can make them private)
 - **Do not email directly (except in an emergency)**



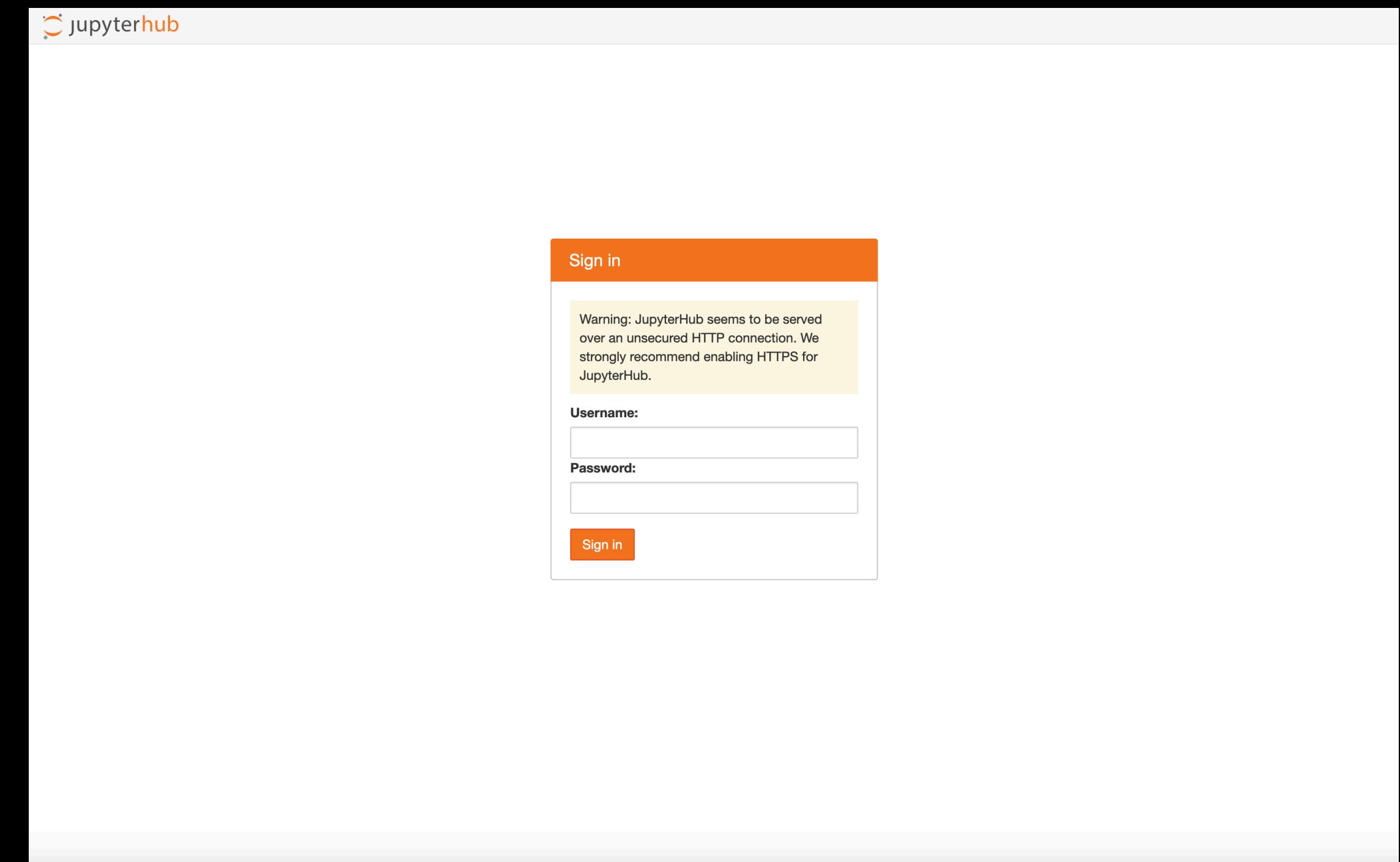
Course resources

- Primary texts
 - Machine Learning a Probabilistic Perspective (K.P. Murphy)
 - The Elements of Statistical Learning (Hastie, Tibshirani, Friedman)
- Additional texts
 - An Introduction to Statistical Learning by James, Witten, Hastie, and Tibshirani
 - Patterns, Predictions, and Actions by Hardt and Recht
 - Fairness and Machine Learning by Barocas, Hardt, and Narayanan
- Background resources on the website



Courseworks

- There will be 2. No exam!
- You have (roughly) **2 weeks** for each
- You will submit to a custom autograder
- Unlimited submits until deadline
- We will run the autograder every Monday, Wednesday, and Friday until the deadline
- Details at: <https://tinyurl.com/COMP0081CourseworkWorkflow> (will finalise dates and Moodle links (in bullet 1) soon!)



Course Topics

- We will cover:
 - Gaussian processes
 - Gradient-based optimization
 - Unsupervised Learning
 - Bias/Variance Trade-off
 - Boosting
 - Support Vector Machines
 - Deep Learning
 - Causal Inference
 - (and more!)
- We will **not** cover:
 - Reinforcement Learning
 - Genetic Programming

Academic Integrity

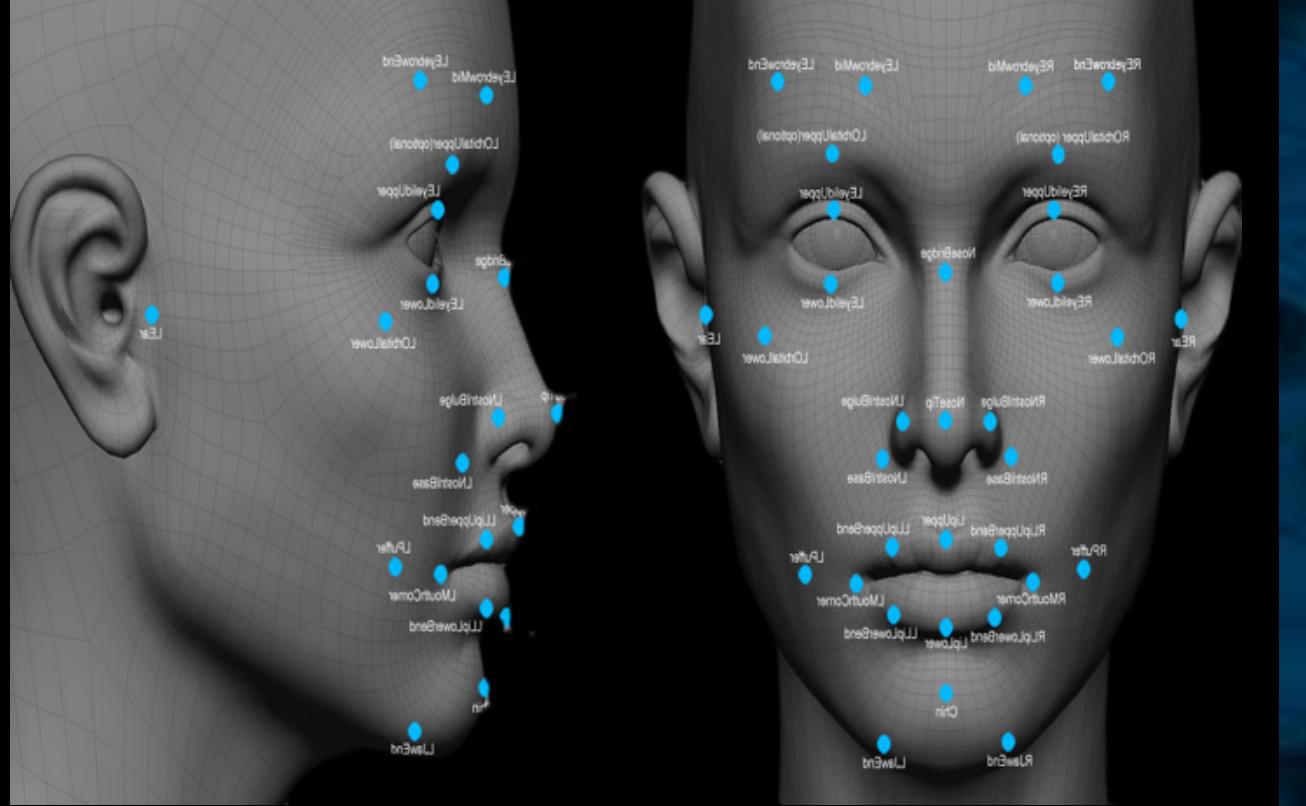
- Zero tolerance policy: all occurrences will be reported
- We **actively** look for academic conduct violations
- The autograder checks for plagiarism

Academic Integrity

- *Examples:*

- Most common: Students steal from same source
- Students post to RentACoder.com or other page
- Students post solutions on the web
- Students use solutions from last year's course



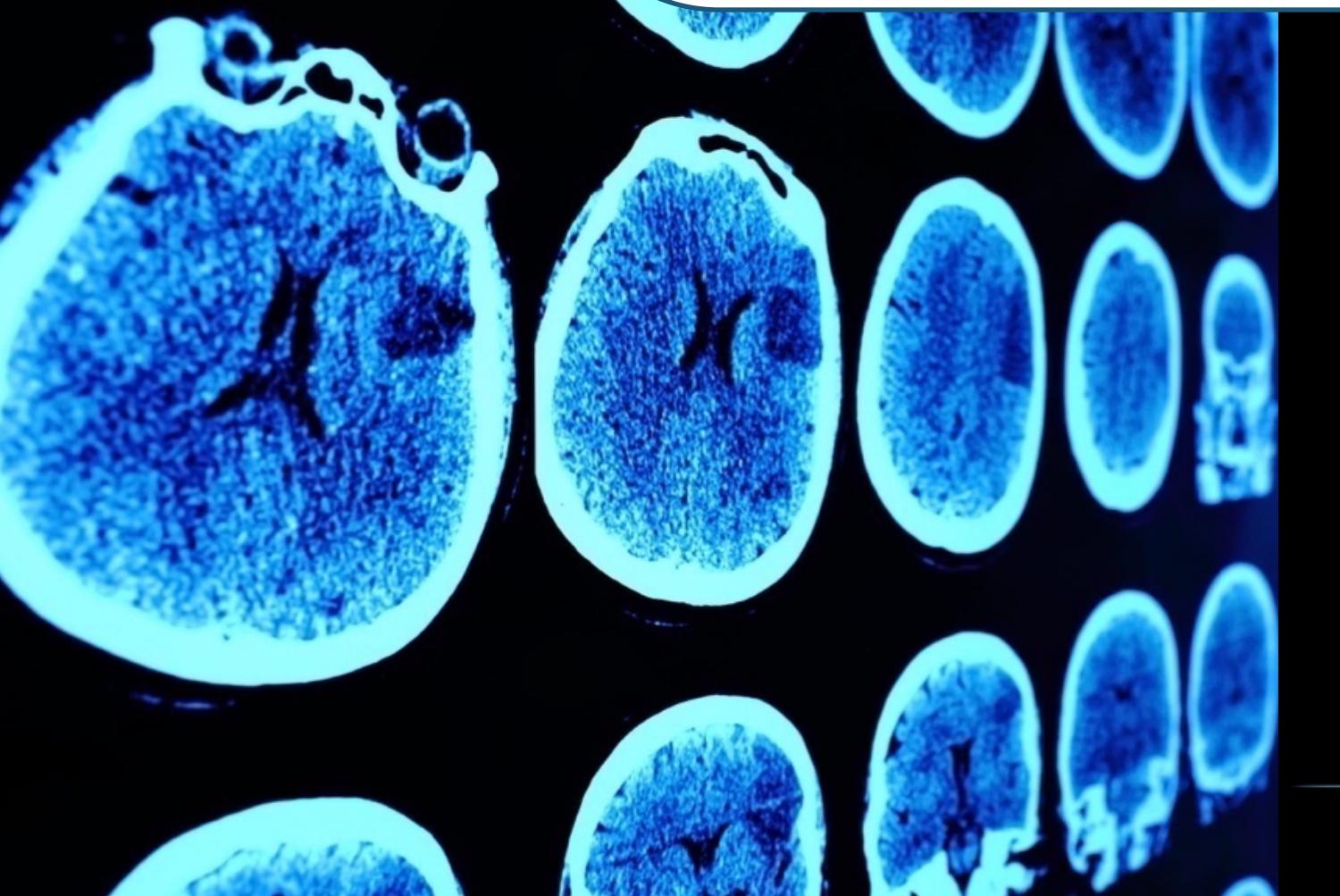


Machine Learning (ML)

Programs that improve with **experience**.

Text Mining

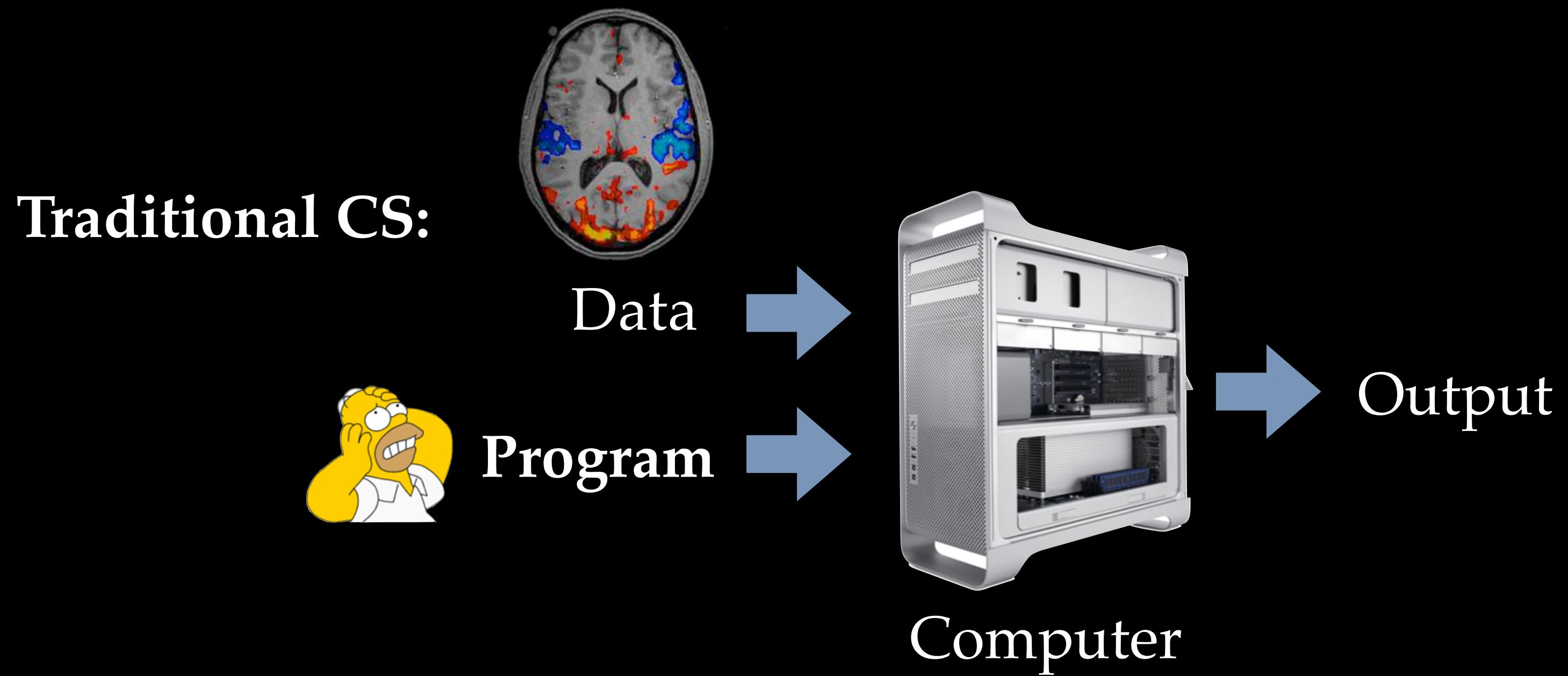
Applications and Theory



Siri

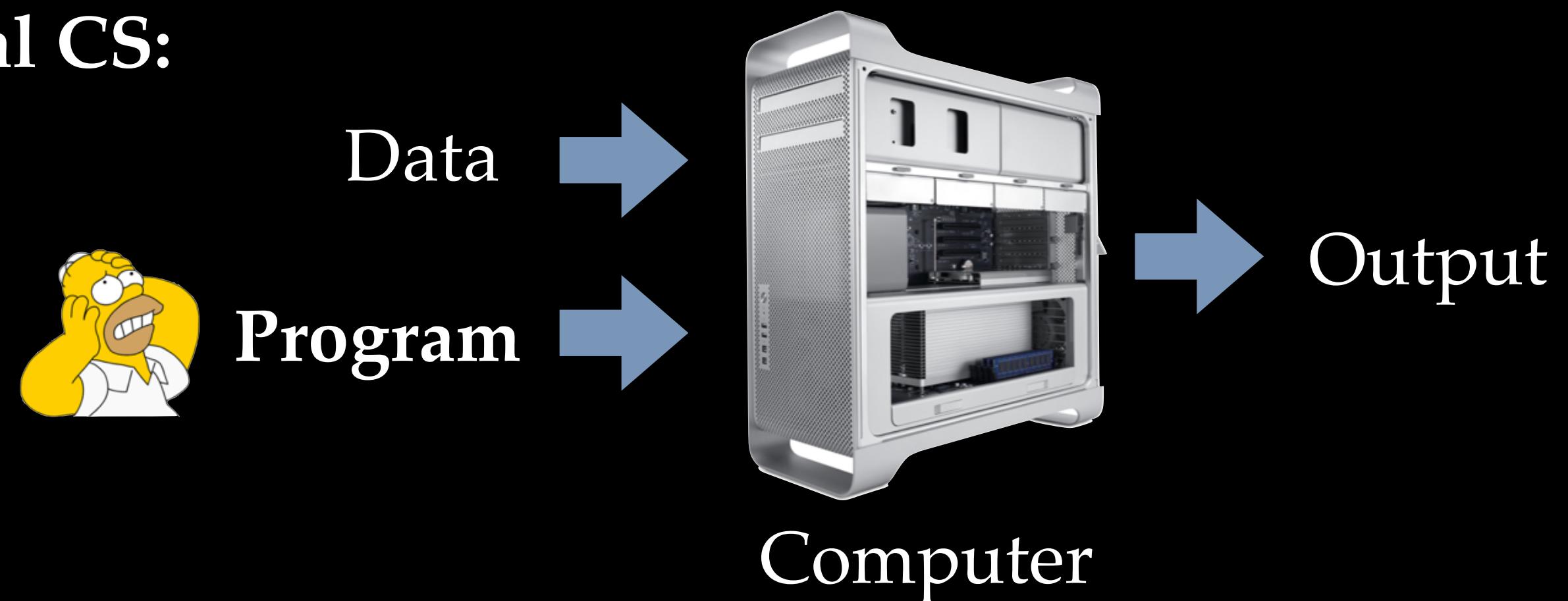


Traditional Computer Science

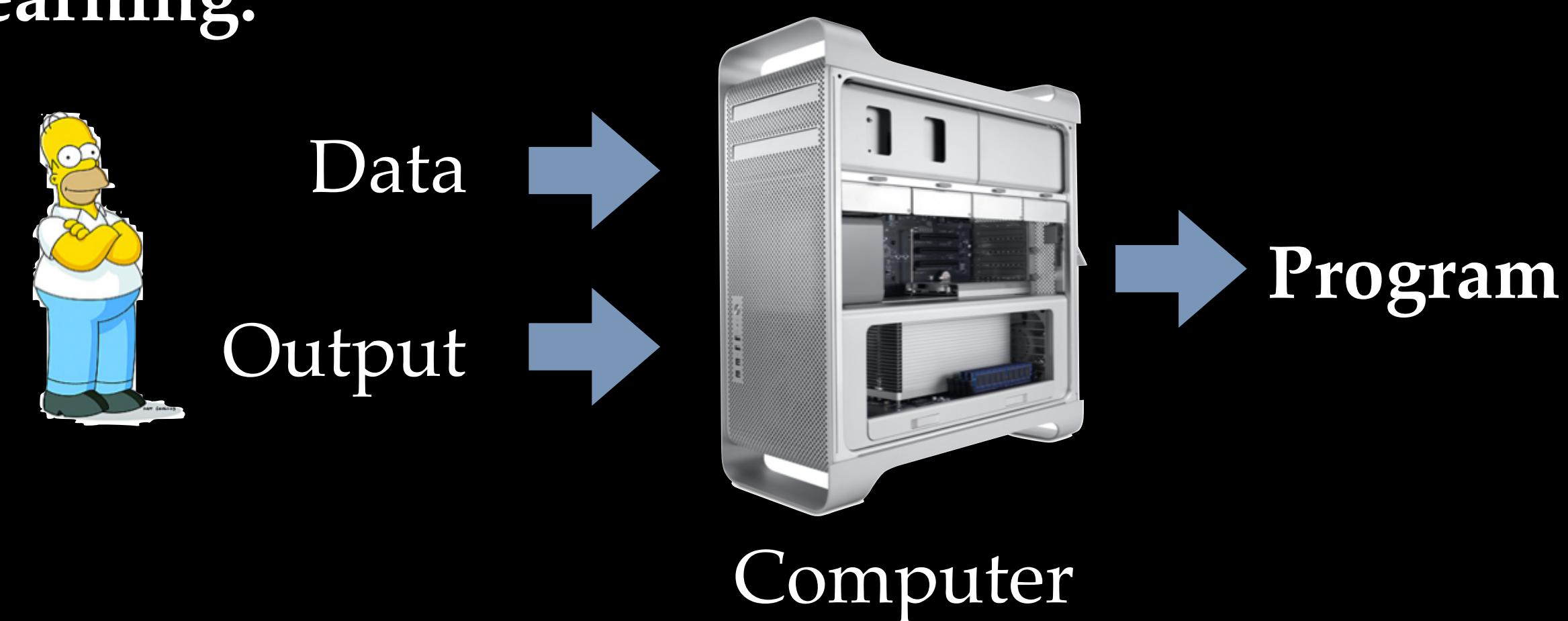


Machine Learning

Traditional CS:

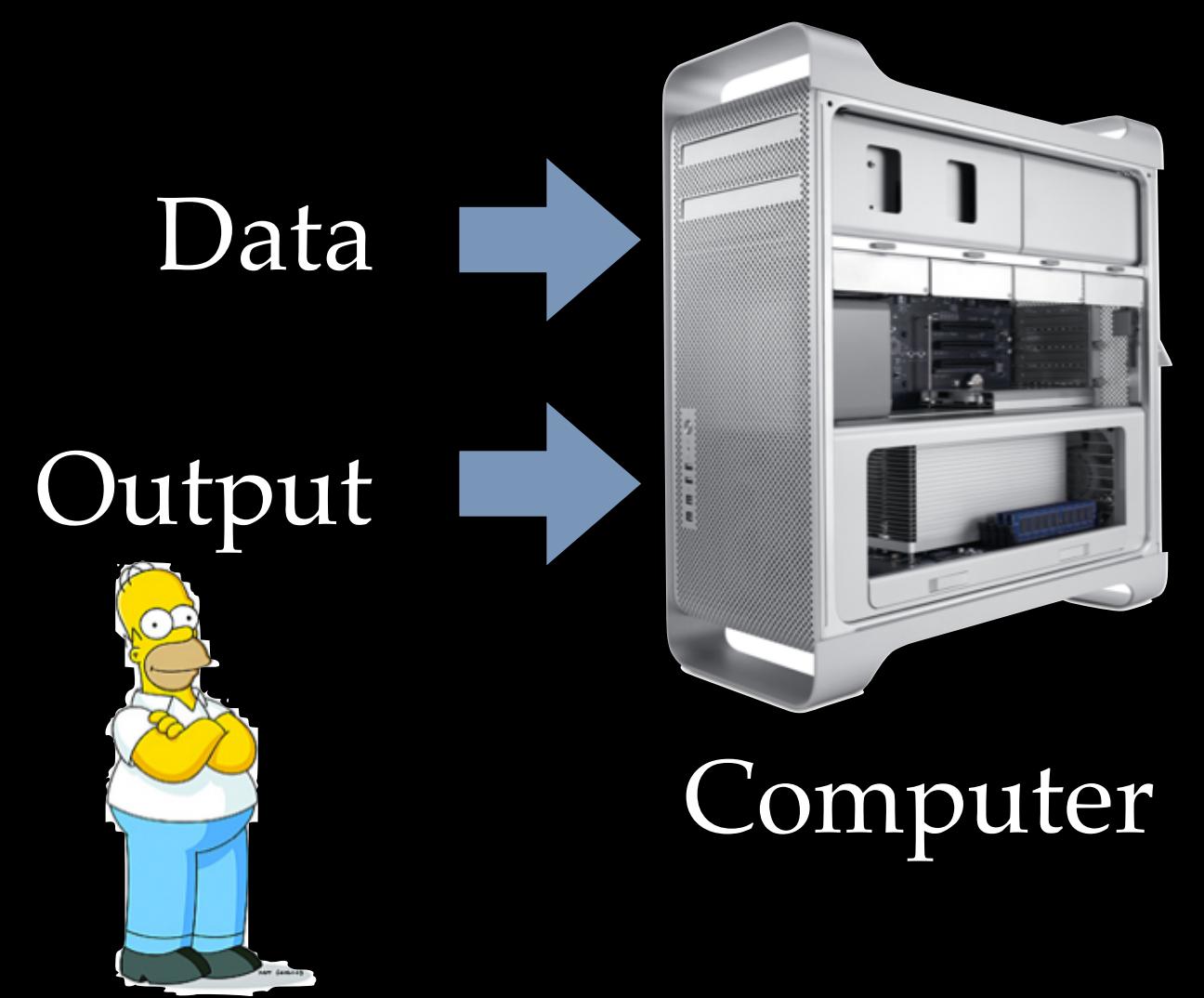


Machine Learning:

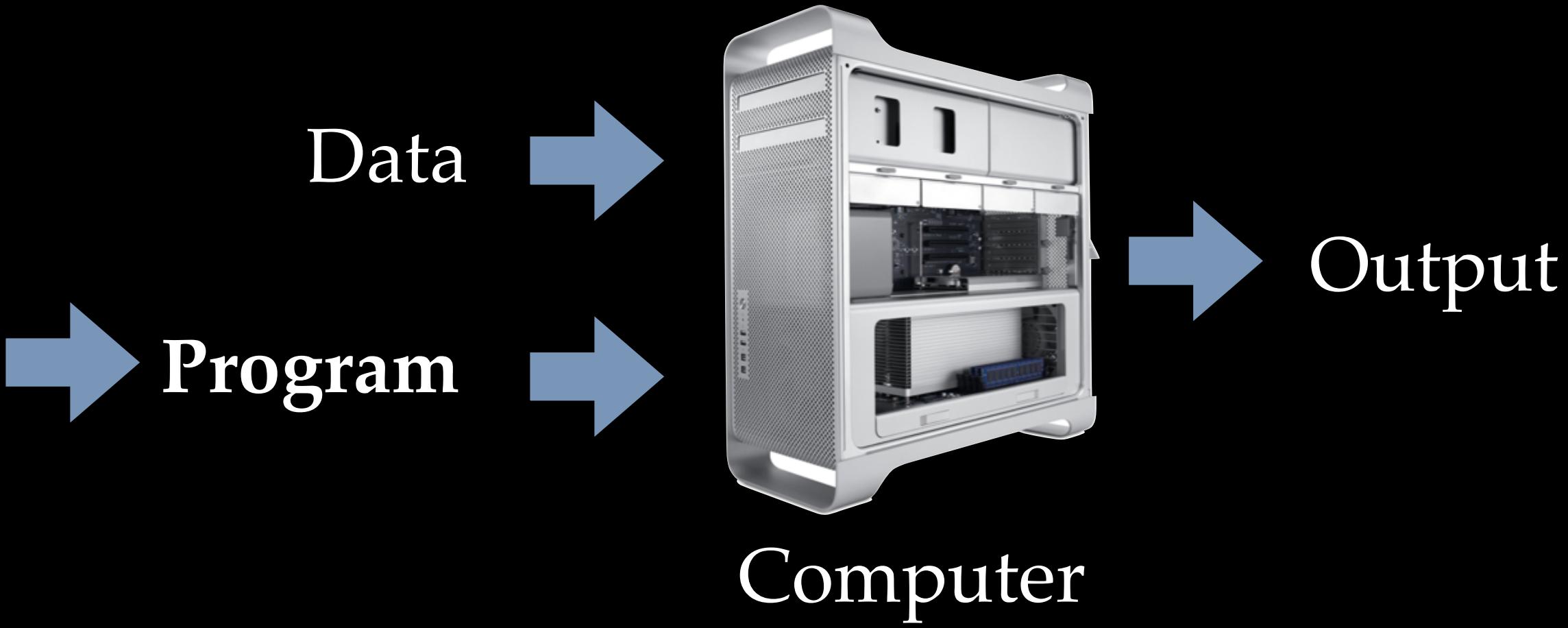


Machine Learning

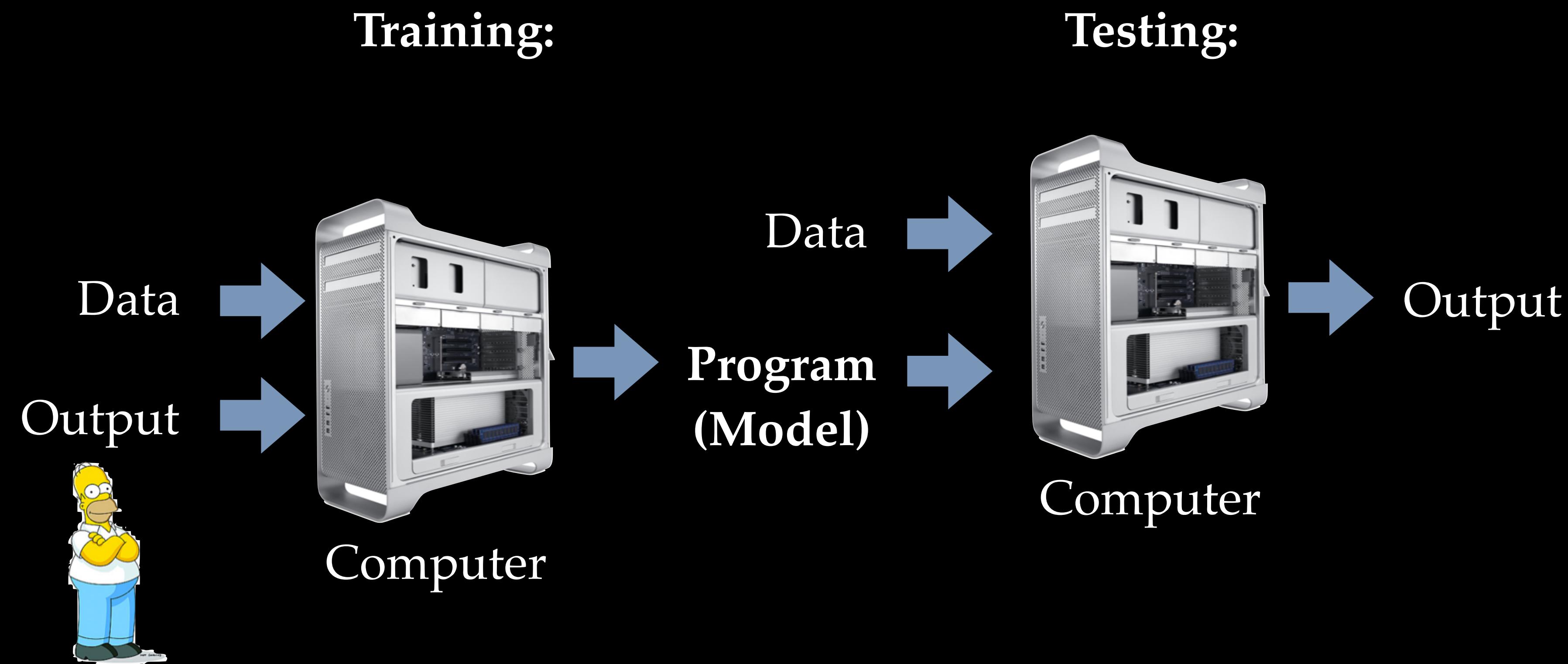
Machine Learning:

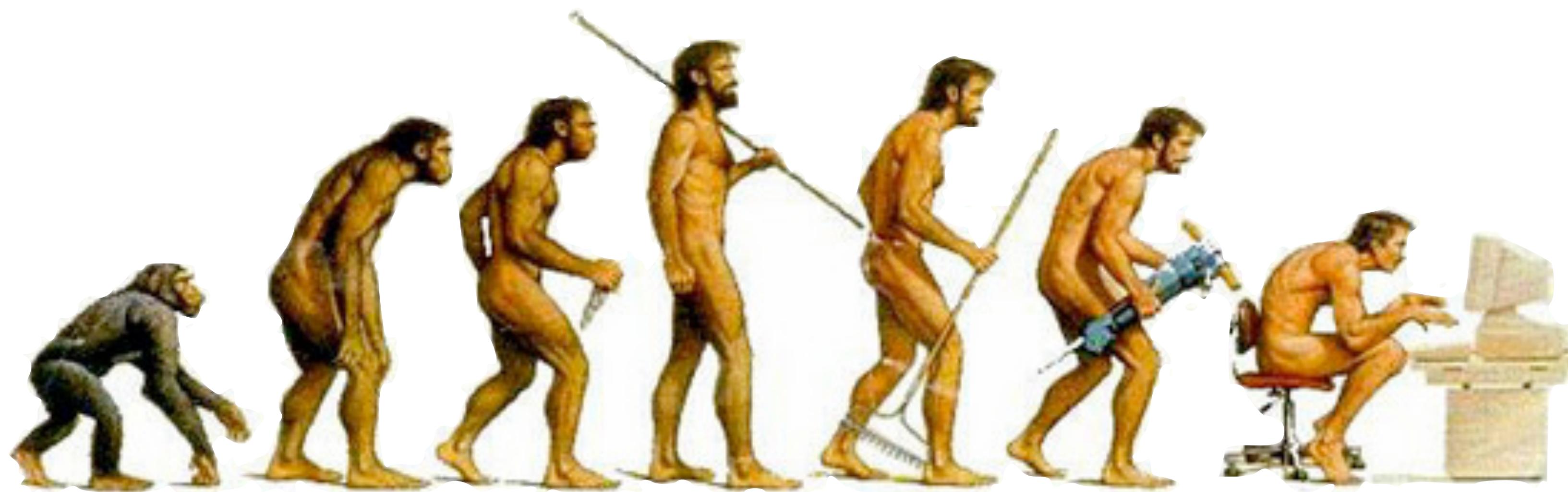


Traditional CS:



Machine Learning





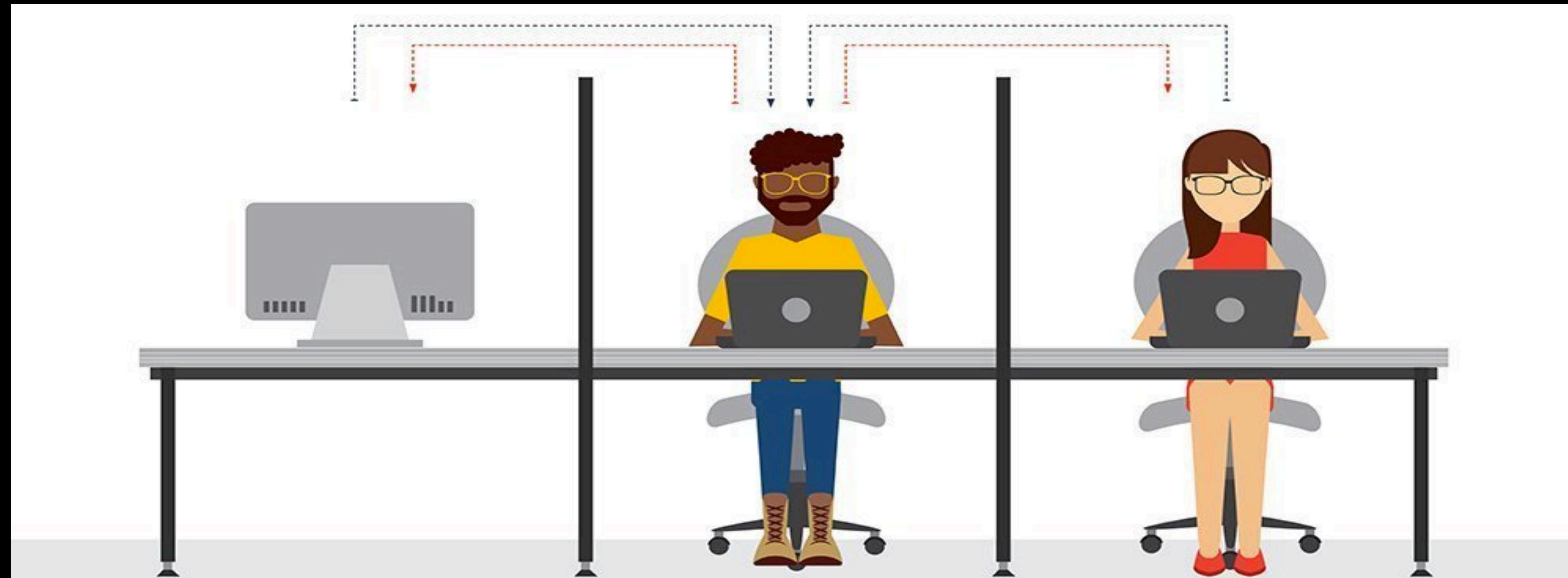
A (very brief) History of ML



Alan Turing

The Turing Test, 1950

A machine is intelligent if its answers
are indistinguishable from a human's





Arthur Samuel

Checkers Program, 1952

Created a Checkers-playing program
that got better overtime.

Also introduced the term
“Machine Learning.”



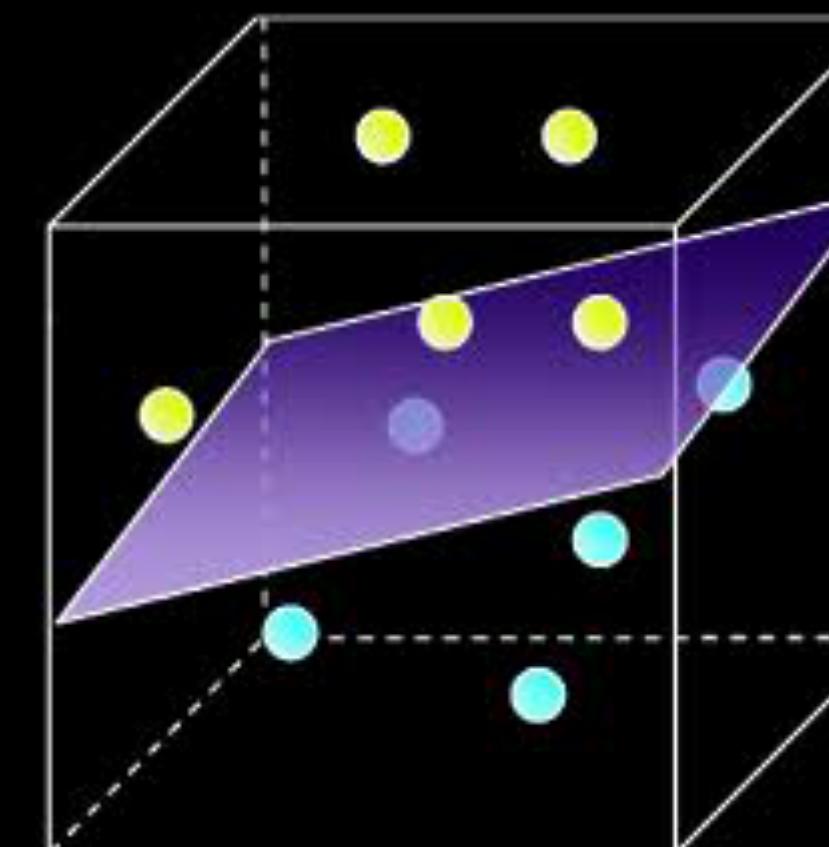
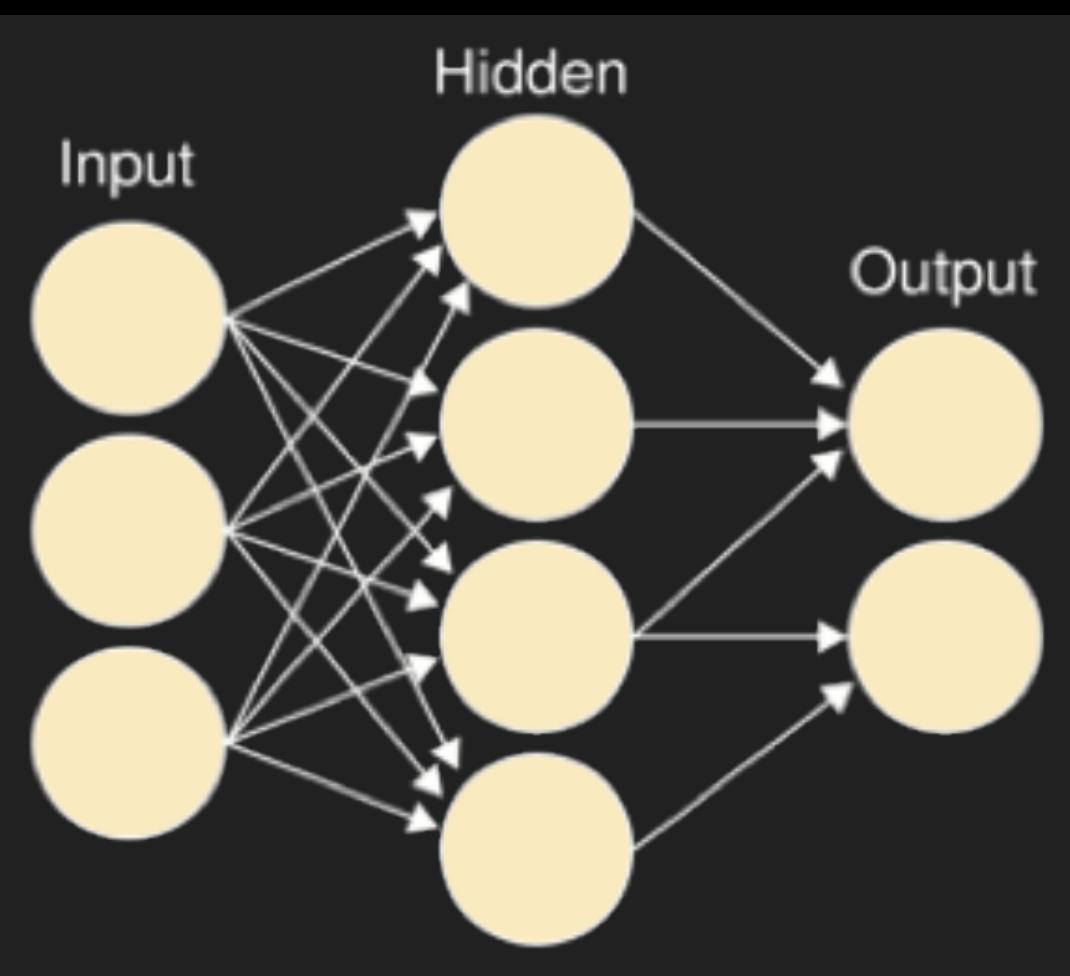


Perceptron, 1957

Predecessor of deep networks.

Frank Rosenblatt

Separating two classes of objects using a linear threshold classifier.





Frank Rosenblatt
@ Cornell!

NEW NAVY DEVICE LEARNS BY DOING

Psychologist Shows Embryo of Computer Designed to Read and Grow Wiser

WASHINGTON, July 7 (UPI) — The Navy revealed the embryo of an electronic computer today that it expects will be able to walk, talk, see, write, reproduce itself and be conscious of its existence.

The embryo—the Weather Bureau's \$2,000,000 "704" computer—learned to differentiate between right and left after fifty attempts in the Navy's demonstration for newsmen.

The service said it would use this principle to build the first of its Perceptron thinking machines that will be able to read and write. It is expected to be finished in about a year at a cost of \$100,000.

Dr. Frank Rosenblatt, designer of the Perceptron, conducted the demonstration. He said the machine would be the first device to think as the human brain. As do human beings, Perceptrons will make mistakes at first, but will grow wiser as it gains experience, he said.

Dr. Rosenblatt, a research psychologist at the Cornell Aeronautical Laboratory, Buffalo, said Perceptrons might be fired to the planets as mechanical space explorers.

Without Human Controls

The Navy said the perceptron would be the first non-living mechanism "capable of receiving, recognizing and identifying its surroundings without any human training or control."

The "brain" is designed to remember images and information it has perceived itself. Ordinary computers remember only what is fed into them on punch cards or magnetic tape.

Later Perceptrons will be able to recognize people and call out their names and instantly translate speech in one language to speech or writing in another language, it was predicted.

Mr. Rosenblatt said in principle it would be possible to build brains that could reproduce themselves on an assembly line and which would be conscious of their existence.

In today's demonstration, the "704" was fed two cards, one with squares marked on the left side and the other with squares on the right side.

Learns by Doing

In the first fifty trials, the machine made no distinction between them. It then started registering a "Q" for the left squares and "O" for the right squares.

Dr. Rosenblatt said he could explain why the machine learned only in highly technical terms. But he said the computer had undergone a "self-induced change in the wiring diagram."

The first Perceptron will have about 1,000 electronic "association cells" receiving electrical impulses from an eye-like scanning device with 400 photo-cells. The human brain has 10,000,000,000 responsive cells, including 100,000,000 connections with the eyes.

Perceptron, 1957

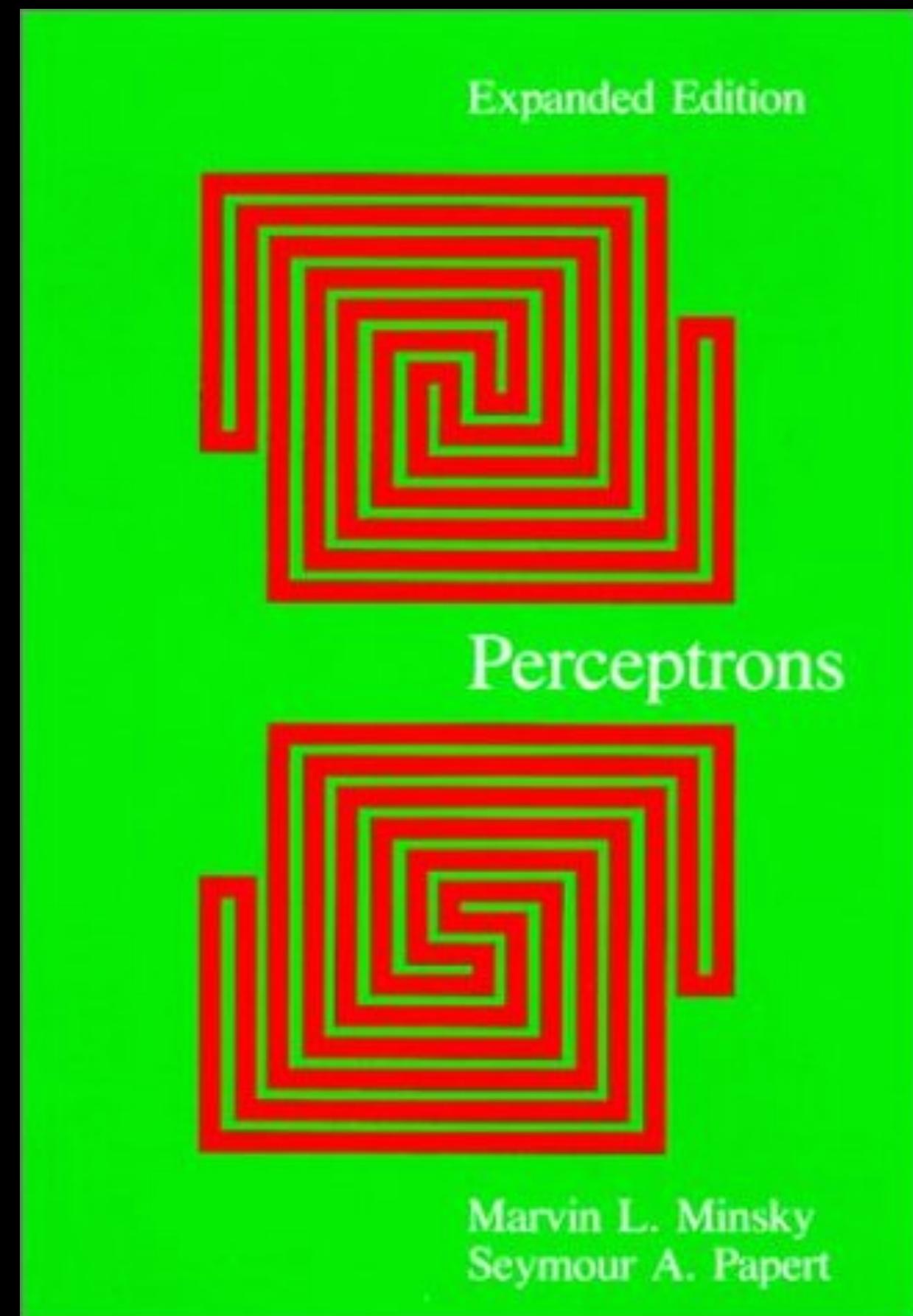
New Navy Device Learns by Doing

- The New York Times (July 8, 1958)

"Later perceptrons will be able to recognize people and call out their names and instantly translate speech in one language to speech or writing in another language, it was predicted."

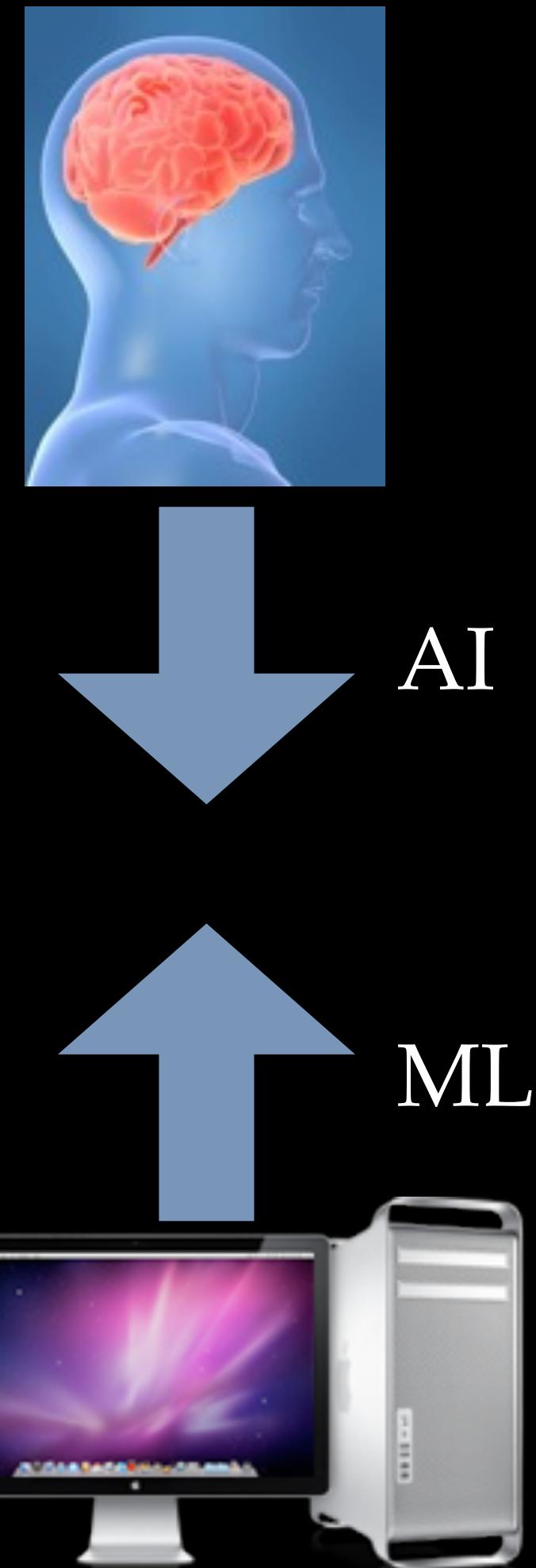
AI Winter (1974-1980)

- (1969) Minsky & Papert “killed” AI
- Burst huge expectation bubble
- Speech understanding / translation fails
- UK and US stop funding AI research



Rebirth as Machine Learning

- Machine Learning:
 - Originally: Mostly a name game to get funding.
- Profound difference:
 - ML: Bottom up, AI: Top down
 - ML: More practical smaller goals
 - Based on **Statistics and Optimization, not Logic**



TD-Gammon (1994)

- Gerry Tesauro (IBM) teaches a neural network to play Backgammon. The net plays 100K+ games **against itself** and beats world champion [Neurocomputation 1994]
- Algorithm teaches **itself** how to play so well!!!
- Algorithm found new techniques that people had erroneously ruled out.



Deep Blue (1997)

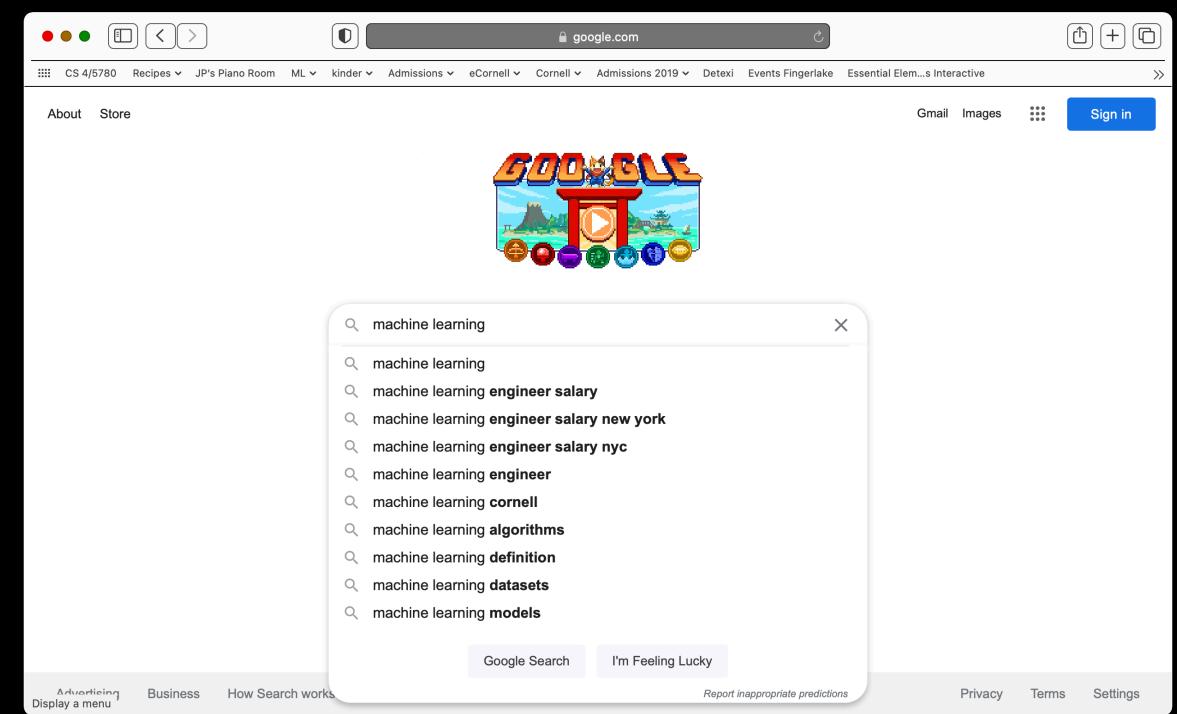
- IBM's Deep Blue wins against Kasparov in chess. Crucial winning move is made due to Machine Learning (G. Tesauro).
- (Mostly a more classical AI system)



Expanding the reach, 2000s

Learning to rank

- Powering search engines: Google, Bing, ...



Topic Modeling:

- Detecting and organizing documents by subject matter.
- Making sense of the unstructured data on the web.

Online economy:

- Ad placement and pricing.
- Product recommendation.

Machine learning became profitable!

Return of Neural Networks, 2010s

Neural networks return and excel at image recognition, speech recognition, ...



The 2018 Turing award was given to Yoshua Bengio, Geoff Hinton, and Yann LeCun.

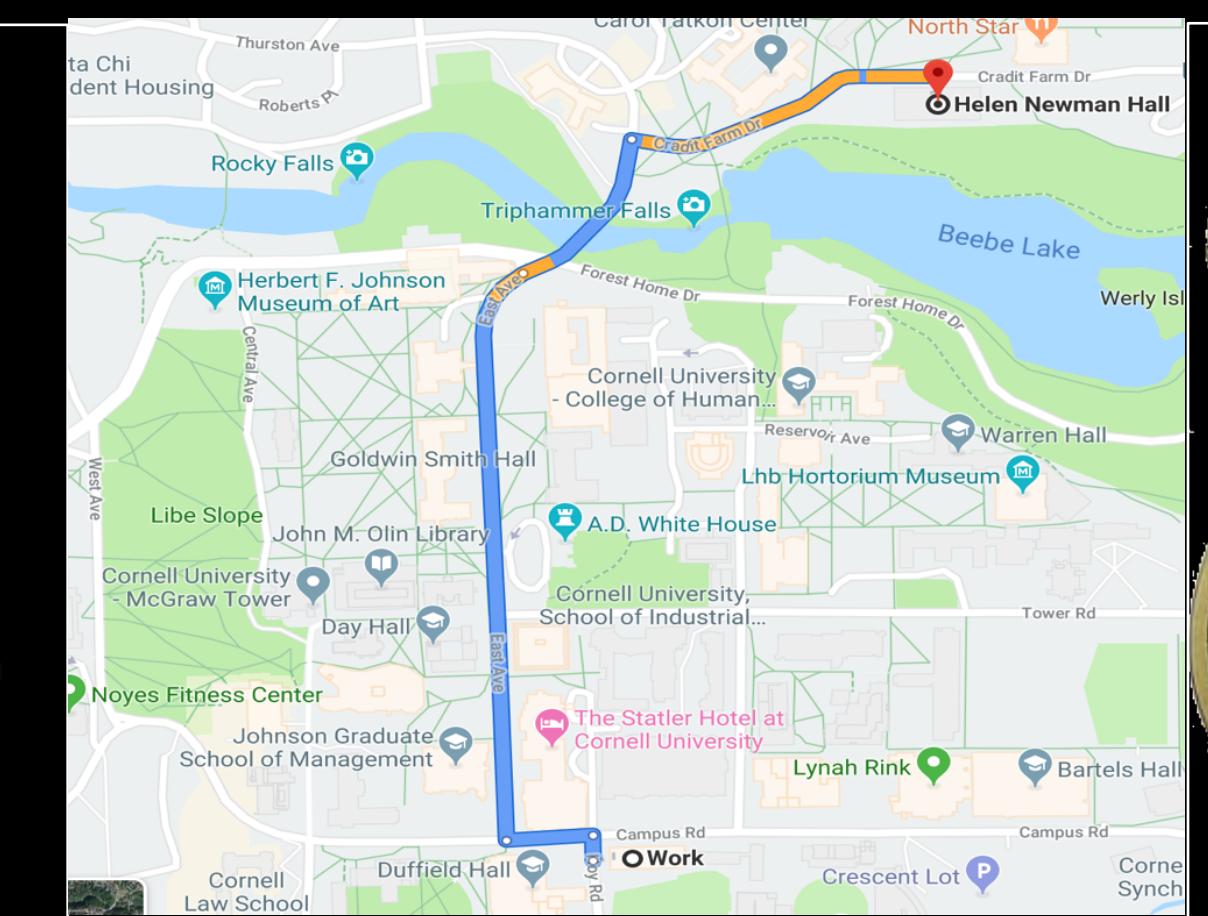
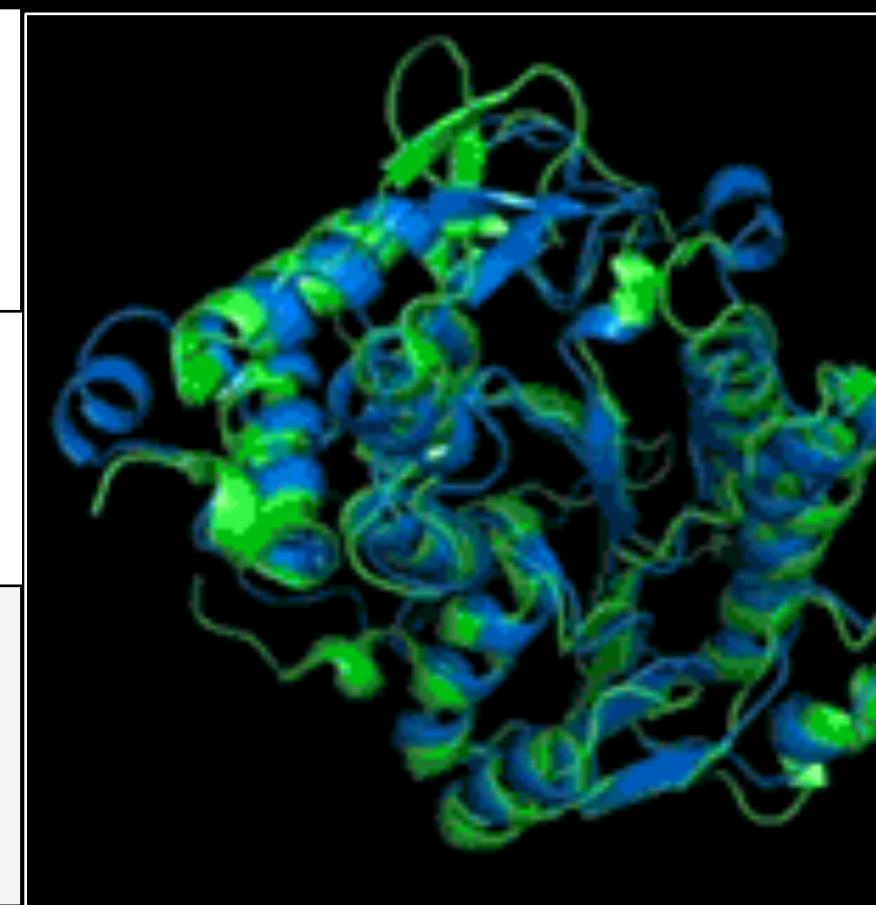
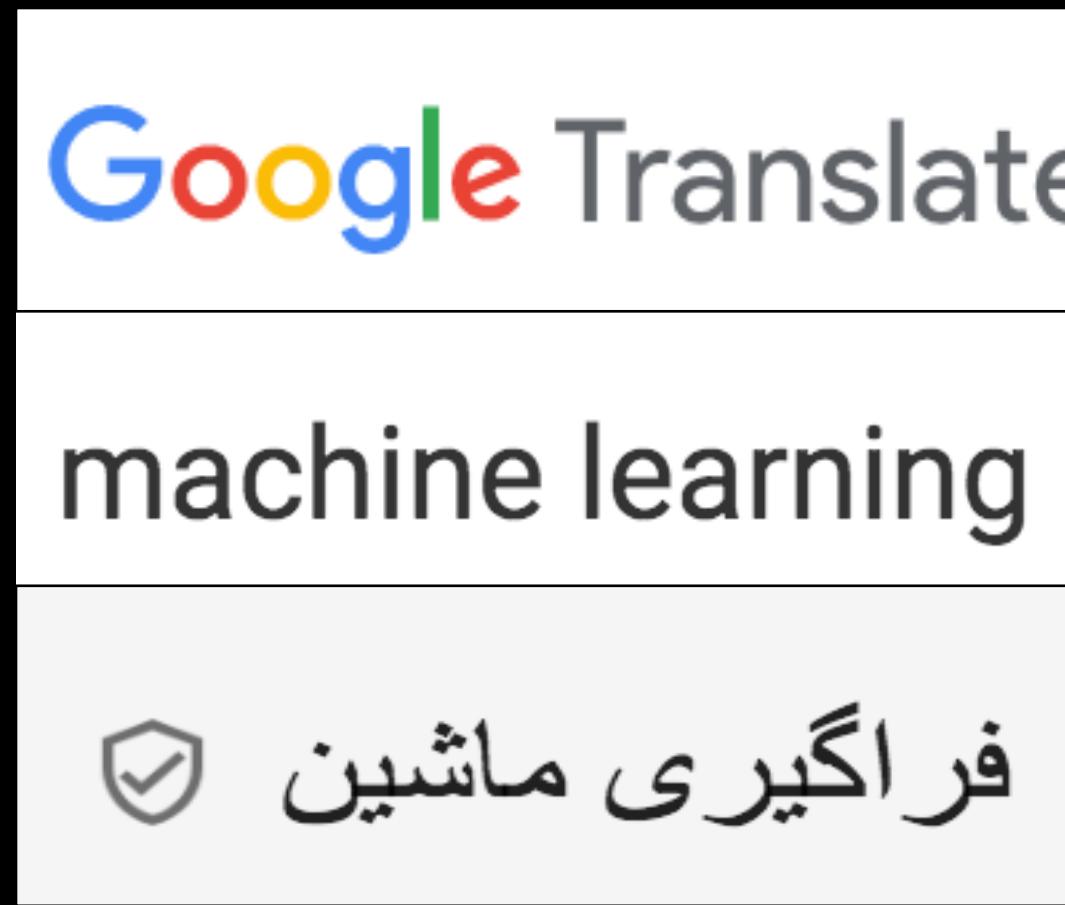


2016 Alpha Go

- 1920 CPUs and 280 GPUs
- Deep Mind's Alpha Go wins against Lee Sedol 5:1
- Big shock
 - China invests heavily in AI research
- Beginning of “AI arms race”



Surrounded by Machine Learning



Azure Machine Learning | Create Your Free Account Today

Ad azure.microsoft.com/Services/MachineLearning ▾



When will it stop?

- Humans learn really well!
 - So, we know that we can still do a lot better!
- However, it is hard. Very few people can design new ML algorithms.
- But many people can use them!



What types of ML are there?

As far as this course is concerned:

- **supervised learning:** Given labeled examples, find the right prediction of an unlabeled example. (e.g. *Given annotated images learn to detect faces.*)
- **unsupervised learning:** Given data try to discover similar patterns, structure, sub-spaces (e.g. *automatically cluster news articles by topic*)
- **reinforcement learning:** Try to learn from delayed feedback (e.g. *robot learns to walk, fly, play chess*)



Outlook



“A breakthrough in machine learning would be worth ten Microsofts.” (Bill Gates, Microsoft)



“It will be the basis and fundamentals of every successful huge IPO win in 5 years.” (Eric Schmidt, Google / Alphabet)



“AI and machine learning are going to change the world and we really have not begun to scratch the surface.”
(Jennifer Chayes, UC Berkeley)



“ML is transforming sector after sector of the economy, and the rate of progress only seems to be accelerating.” (Daphne Koller, Stanford / Coursera/ Insitro)



“Machine learning is the next Internet” (Tony Tether, DARPA)



Data privacy / misuse

Learning models leak training data
(Fredrickson et al. '15)



Leaked data



Real image

Learning algorithms detect sexual orientation better than people
(Wang & Kosinski'17)



Formal definitions of data privacy:

- K- anonymity (Sweeney)
- Differential Privacy (Dwork, McSherry, Nissim, Smith).



Latanya Sweeney



Cynthia Dwork



Frank McSherry



Kobbi Nissim



Adam Smith

Robust and Secure ML

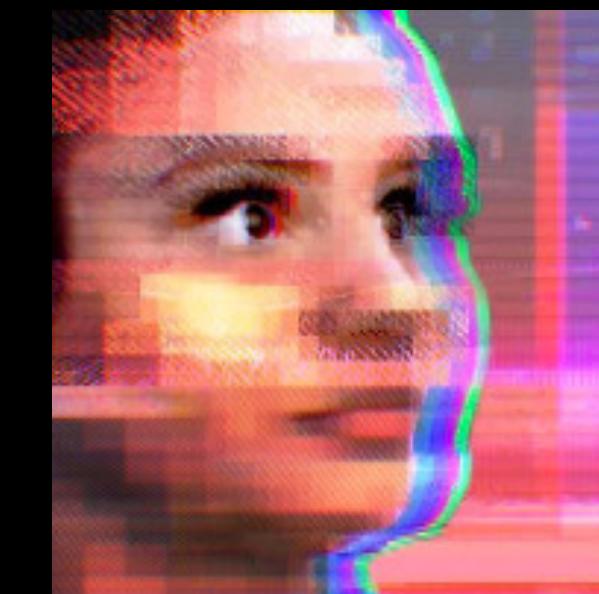
Image Recognition
Misreading traffic
signs
(Eykholt et al)



Speech recognition
Hide commands in
noise (Carlini & Wagner)



Poisoning Attacks
Tay (chat bot) became
inflammatory in 16 hr.



How to create robust and secure machine learning algorithms?

Learning and the Society

- Bad dynamics, perpetuating and worsening stereotypes and biases.
- Who carries the burden of bad prediction?
- How to design good dynamics?

The Best Algorithms Struggle to Recognize Black Faces Equally

Google's algorithm shows prestigious job ads to men, but not to women. Here's why that should worry you.

Gender and racial bias found in Amazon's facial recognition technology (again)

Do Google's 'unprofessional hair' results show it is racist?

lock unprofessional hairstyles for work



How Amazon Accidentally Invented a Sexist Hiring Algorithm

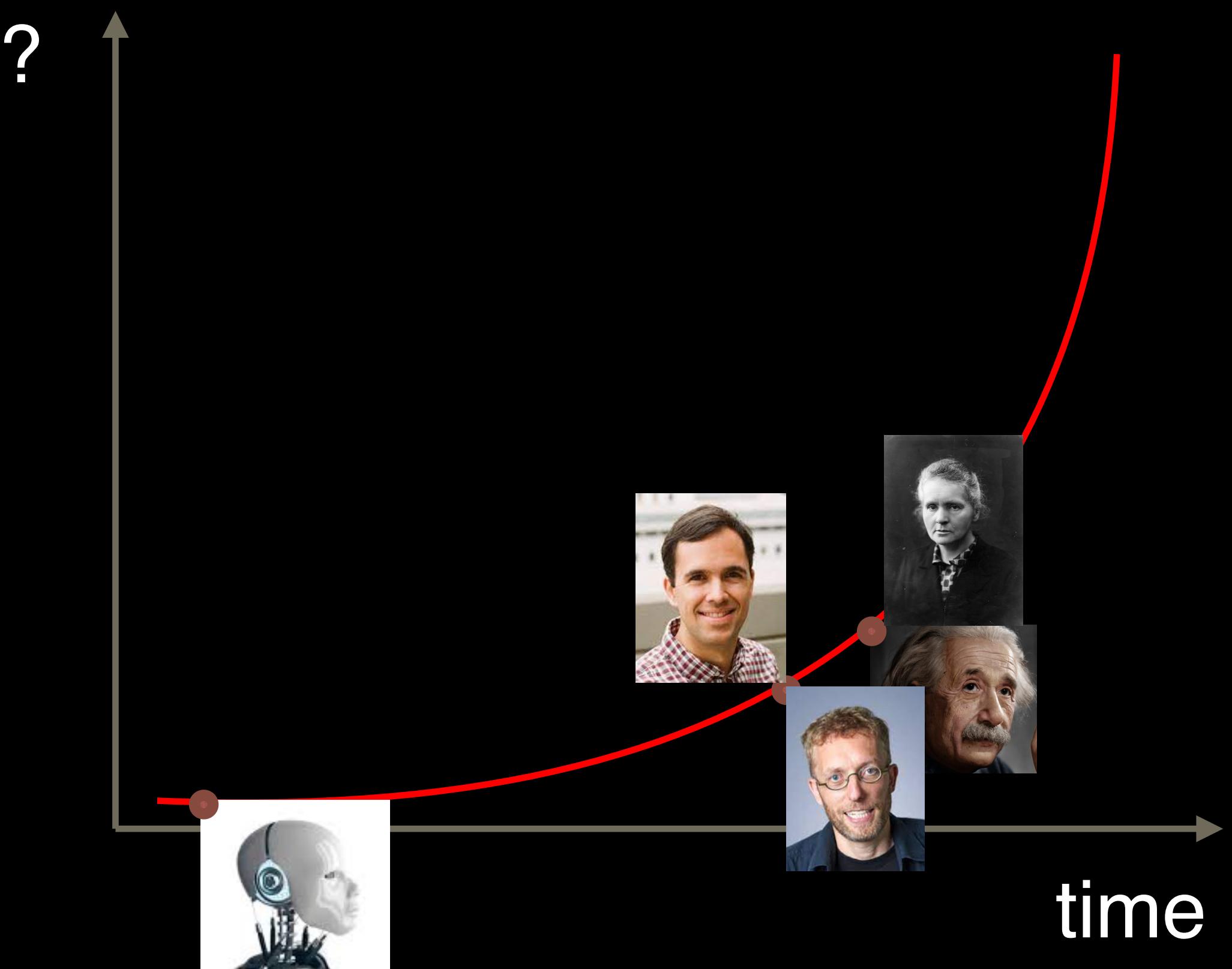
A company experiment to use artificial intelligence in hiring inadvertently favored male candidates.

When an Algorithm Helps Send You to Prison

By Ellora Thadaney Israni



Will AI take over the world?



Will AI take over the world?

Good news:

AI is nowhere near to general Intelligence (no real progress)

Bad news:

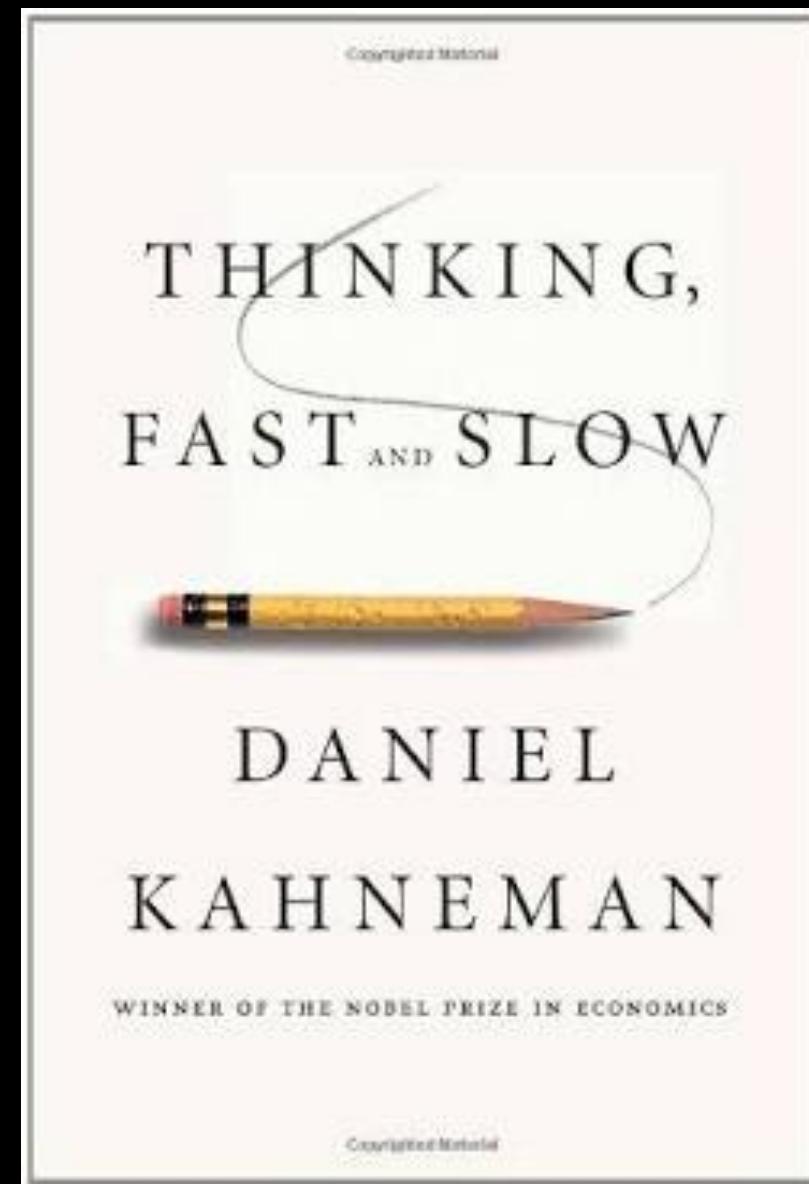
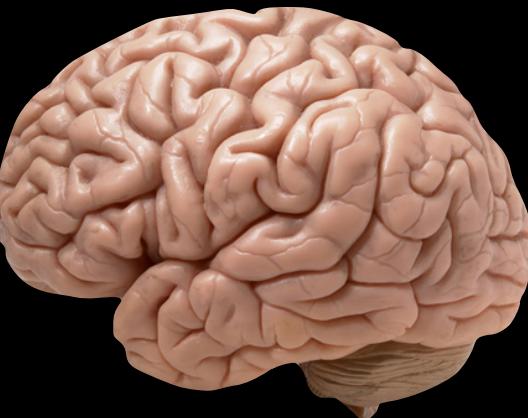
AI doesn't have to be smarter than us to be harmful



time

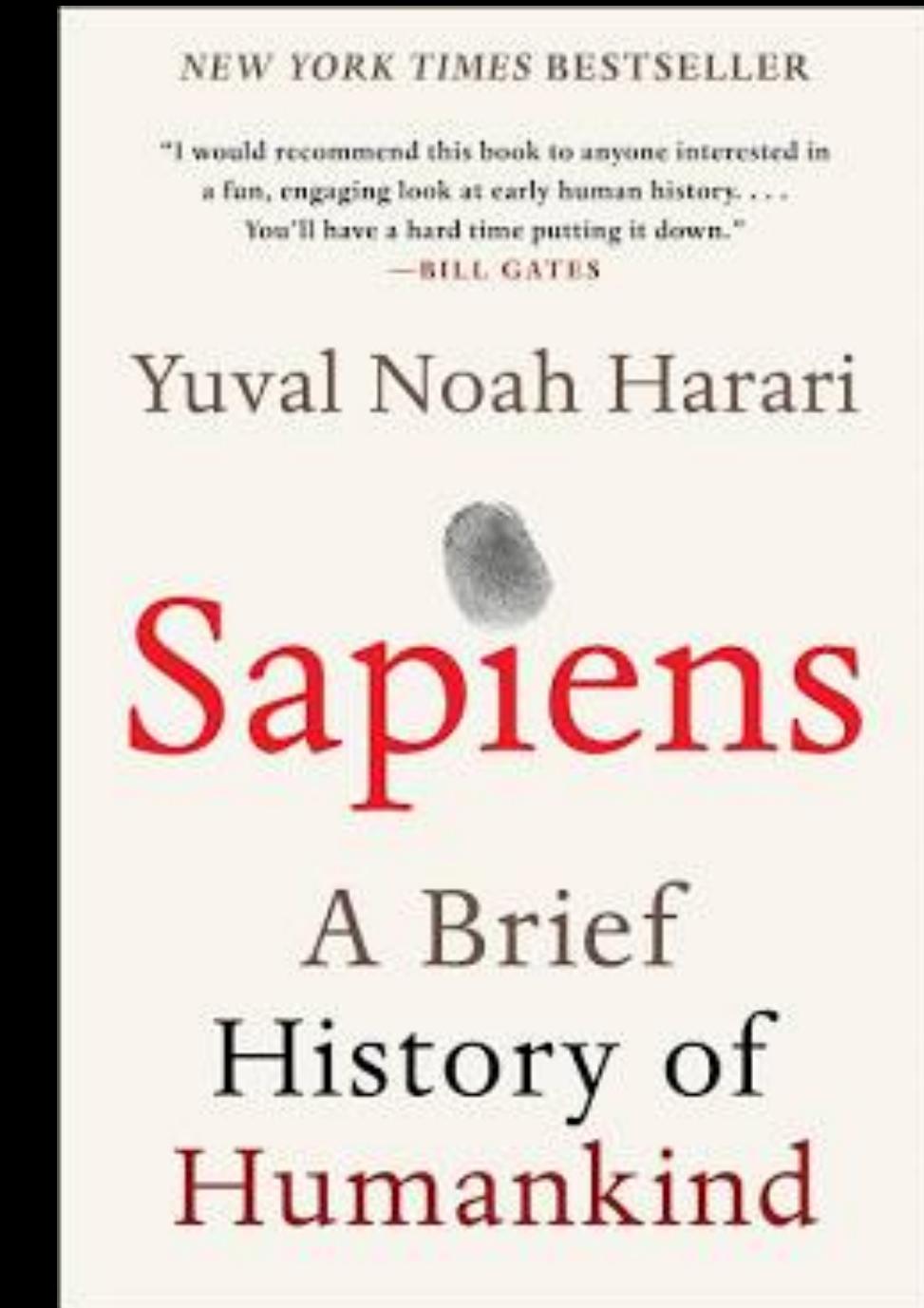
One brain, two systems

- System 1:
 - Subconscious
 - Fast
 - Requires low energy
 - Involuntary
 - Triggers surprise
- System 2:
 - Conscious
 - Slow
 - Expensive
 - Voluntary
 - Requires concentration



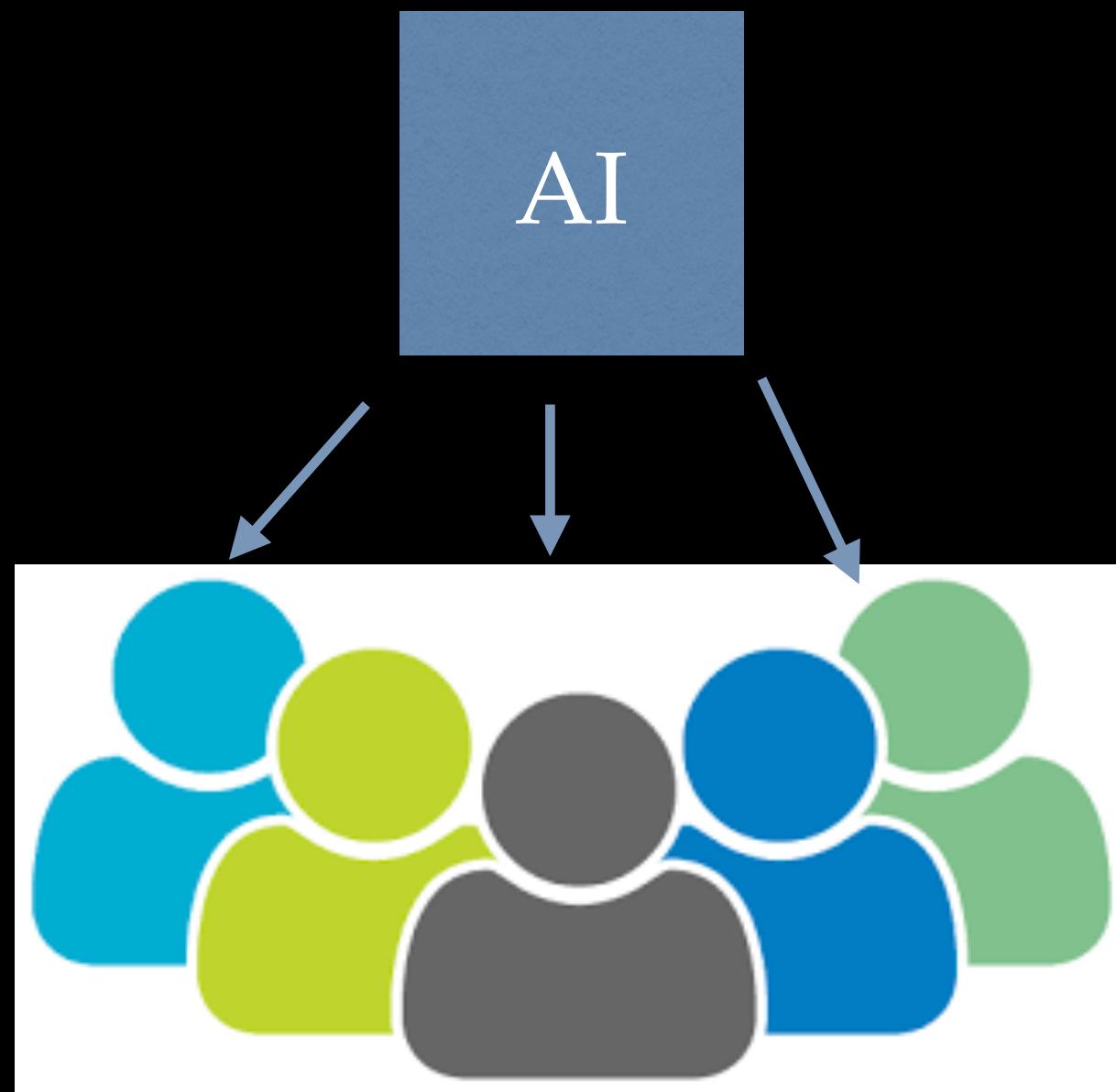
Our brain: strength and weakness

- Weakness:
 - “Unarmed human” was not on the top of the food chain
 - Our system 1 reacts instantly to rudimentary fears / dangers / drives (flight, fight, feeding, sexual function)
 - Homo sapiens had no time to adapt to its new position as APEX predator



AI and Online advertising

- Advertisers pay AI companies to induce change in people's behaviors
 - AI learns to interact with System 1
 - (e.g. Displays sensational / alarming headlines)
 - Leads to fast clicks/ prolonged engagement (more advertising time)
 - Causes (social) anxiety, fear, undesired behavior, elevates misinformation



AI/ML is different from humans

- Where and how we (choose to) deploy AI/ML systems matters
- Good at some things humans are not
- Can have extensive “unforeseen” consequences (both in development and deployment)
- Not a drop in for humans; inappropriate to use in certain settings
- Important to understand what is going on “under the hood” to understand what problems are AI/ML problems and where use is appropriate

Now let's get crack'n