



CS60050: Machine Learning

Autumn 2024

Sudeshna Sarkar

Introduction to ML

24 July 2024



Course Website

<https://machine-learning-2024-cs60050.netlify.app/>

Course Timings

- Wed 11-12 PM, Thu 12-1 PM, Fri 8-9 AM
- **Section 1 (Sudeshna Sarkar, NC 243)**
 - All PG students. UG students of EC, EE, MA
- **Section 2 (Dr. Somak Aditya, NC442)**
 - All UG students except EC, EE, MA


Contact

Email: sudeshna@cse.iitkgp.ac.in Subject “CS60050 ML24”



Course Evaluation Plan

Tentative

- Mid Term - 25%
 - Final Exam - 40%
 - Assignments (3-4) - 20%
 - Class-Tests (Two) - 15%
- 

A decorative graphic in the top-left corner consisting of a network of interconnected nodes and lines, rendered in light gray. The nodes are represented by circles of varying sizes, some with concentric rings, and the lines are thin and gray, creating a web-like structure.

Attendance Policy

Students must attend all classes.
Enter the class on time.

Attendance Policy: Attendance record will be maintained and
uploaded on the website.

All students must maintain 75% attendance to continue the
course.

A decorative graphic in the bottom-right corner, similar to the one in the top-left, featuring a network of interconnected nodes and lines in light gray. The nodes are circles of varying sizes, some with concentric rings, connected by thin gray lines.

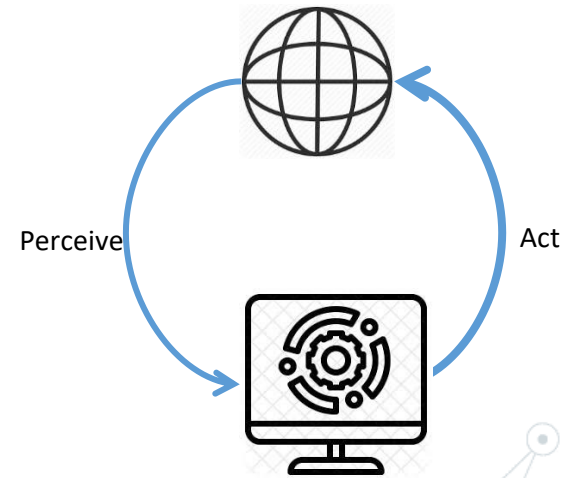
A decorative network diagram in the top-left corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow with a grey outline. The connections form a complex, branching structure.

What is Machine Learning?

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It features a cluster of nodes connected by lines, with some nodes being solid grey and others hollow with grey outlines.

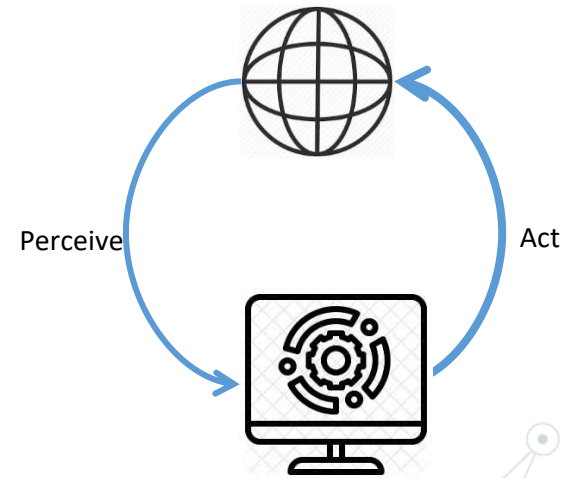
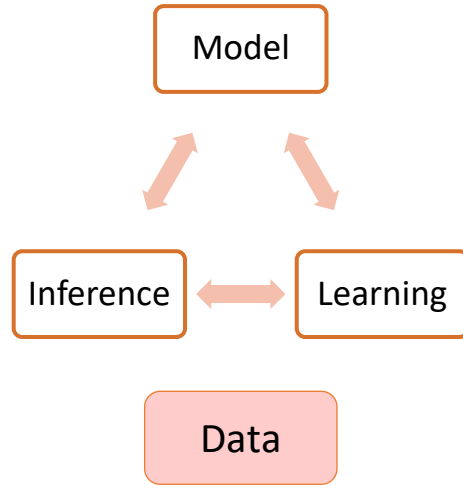
Artificial Intelligence

- The quest for building Intelligent Agents that can think and act rationally (or humanlike)
- Aspects of intelligent behaviour
 - **Learn (from experience)**
 - **Adapt to new situations**
 - **Reason**
 - **Act intelligently**

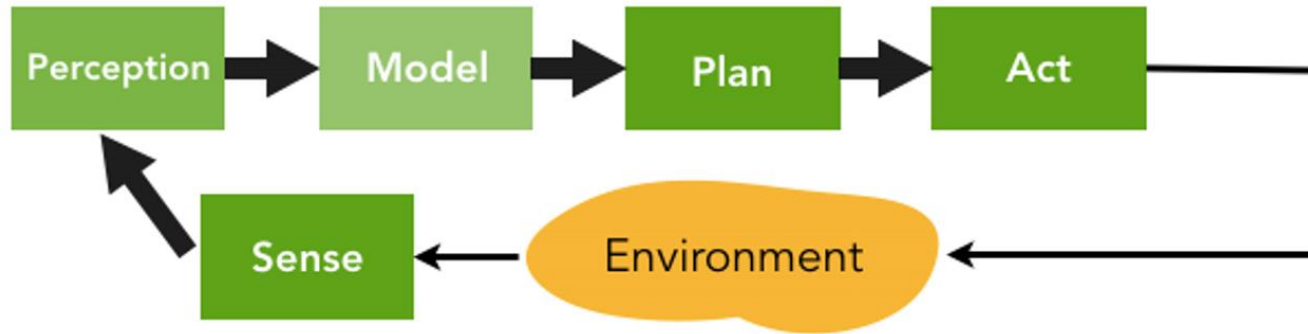


Artificial Intelligence

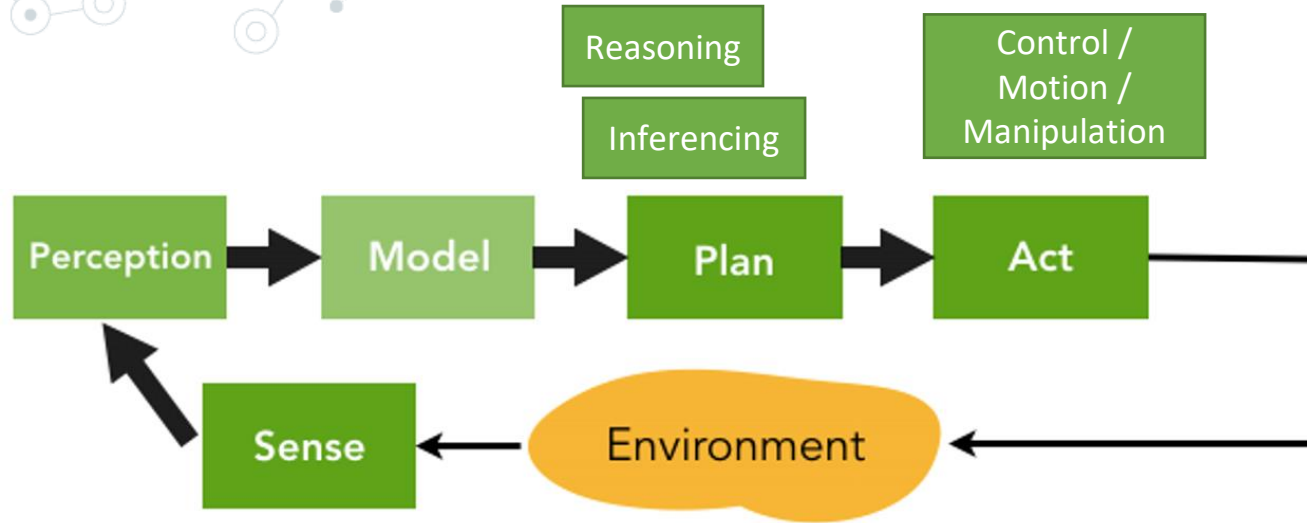
- The quest for building Intelligent Agents that can think and act rationally (or humanlike)



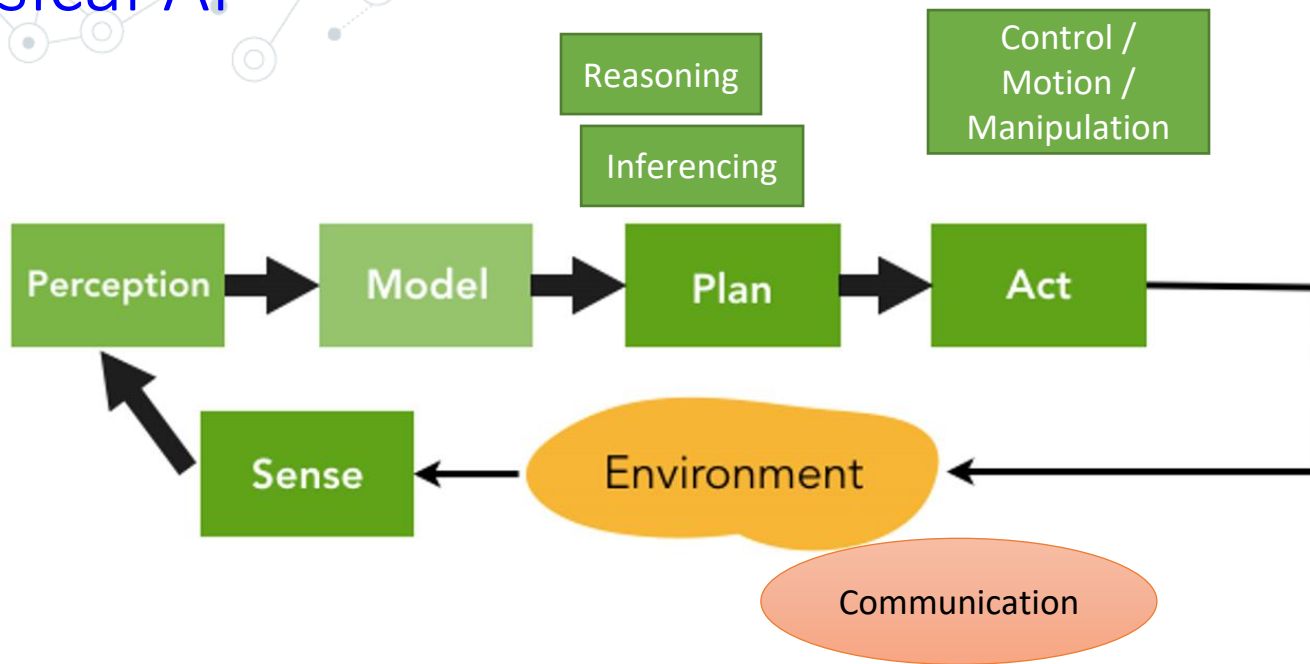
Classical AI



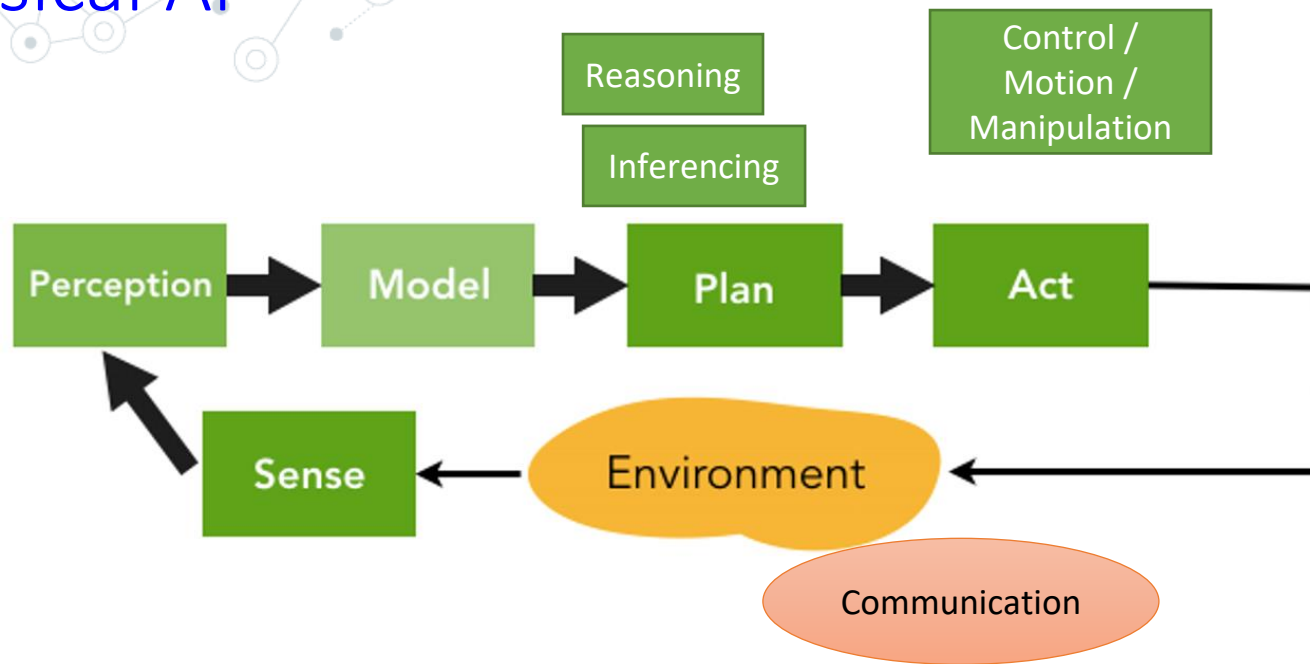
Classical AI



Classical AI



Classical AI



Learning

Data

Machine Learning Toolbox

- Machine Learning
- Statistics
- Probability
- Computer Science
- Optimization

What is ML?

Speech Recognition

1. Learning to recognize spoken words

THEN

"...the SPHINX system (e.g., Lee 1989) learns speaker-specific strategies for recognizing the primitive sounds (phonemes) and words from the observed speech signal...neural network methods...hidden Markov models..."

(Mitchell, 1997)

NOW

vs vs vs

Red vs Blue vs Green

Figure from <https://botpenguin.com/alexa-vs-siri-vs-google-assistant/>

Robotics

2. Learning to drive an autonomous vehicle

THEN

"...the ALVINN system (Pomerleau 1989) has used its learned strategies to drive unassisted at 70 miles per hour for 90 miles on public highways among other cars..."

(Mitchell, 1997)

NOW

waymo.com

Games / Reasoning

3. Learning to beat the masters at board games

THEN

"...the world's top computer program for backgammon, TD-GAMMON (Tesauro, 1992, 1995), learned its strategy by playing over one million practice games against itself..."

(Mitchell, 1997)

NOW

Computer Vision

4. Learning to recognize images

THEN

"...The recognizer is a convolution network that can be spatially replicated. From the network output, a hidden Markov model produces word scores. The entire system is globally trained to minimize word-level errors..."

(LeCun et al., 1995)

NOW

Figure from <https://proceedings.neurips.cc/paper/2015/file/c39863d3b9d6b764c36e9a4a8c45b-Paper.pdf>

Learning Theory

5. In what cases and how well can we learn?

Sample Complexity Results

Definition 4.1. The sample complexity of a learning algorithm is the number of examples required to achieve arbitrarily small error (with respect to the optimal hypothesis) with high probability (i.e., close to 1).

Four Cases we care about:

- Realizable**

$$n \geq \frac{1}{\epsilon^2} \left(\frac{1}{\eta} \log \frac{1}{\delta} + \frac{1}{\eta^2} \log \frac{1}{\delta} \right)$$
- Agnostic**

$$n \geq \frac{1}{\epsilon^2} \left(\frac{1}{\eta} \log \frac{1}{\delta} + \frac{1}{\eta^2} \log \frac{1}{\delta} \right)$$
- Finite**

$$n \geq \frac{1}{\epsilon^2} \left(\frac{1}{\eta} \log \frac{1}{\delta} + \frac{1}{\eta^2} \log \frac{1}{\delta} \right)$$
- Infinitely**

$$n \geq \frac{1}{\epsilon^2} \left(\frac{1}{\eta} \log \frac{1}{\delta} + \frac{1}{\eta^2} \log \frac{1}{\delta} \right)$$

PK Learning

Can we learn $R(x)$ in form of $R(x)$?

PK can be learned if PK is linearly separable, which is approximately correct if $R(x) \approx 0$ and $R(x) \approx 1$ with high probability. $R(x) \approx 0$ and $R(x) \approx 1$ are not linearly separable.

1. How many examples do we need to learn?

2. How do we quantify our ability to generalize to unseen data?

3. Which algorithms are better suited to specific learning settings?

Learning

Data



Model

- Requires a leap of faith: generalization

ML Big Picture

Learning Paradigms:

What data is available and when? What form of prediction?

- supervised learning
- unsupervised learning
- semi-supervised learning
- reinforcement learning
- active learning
- imitation learning
- domain adaptation
- online learning
- density estimation
- recommender systems
- feature learning
- manifold learning
- dimensionality reduction
- ensemble learning
- distant supervision
- hyperparameter optimization

Theoretical Foundations:

What principles guide learning?

- ☐ probabilistic
- ☐ information theoretic
- ☐ evolutionary search
- ☐ ML as optimization

Problem Formulation:

What is the structure of our output prediction?

boolean	Binary Classification
categorical	Multiclass Classification
ordinal	Ordinal Classification
real	Regression
ordering	Ranking
multiple discrete	Structured Prediction
multiple continuous	(e.g. dynamical systems)
both discrete & cont.	(e.g. mixed graphical models)

Facets of Building ML Systems:

How to build systems that are robust, efficient, adaptive, effective?

1. Data prep
2. Model selection
3. Training (optimization / search)
4. Hyperparameter tuning on validation data
5. (Blind) Assessment on test data

Big Ideas in ML:

Which are the ideas driving development of the field?

- inductive bias
- generalization / overfitting
- bias-variance decomposition
- generative vs. discriminative
- deep nets, graphical models
- PAC learning
- distant rewards

Application Areas

Key challenges?

NLP, Speech, Computer Vision, Robotics, Medicine, Search



CS60050: Machine Learning

Autumn 2024

Sudeshna Sarkar

Introduction to ML

25 July 2024



Well-Posed Learning Problem

Three components $\langle T, P, E \rangle$:

1. Task, T
2. Experience, E
3. Performance measure, P

Definition of learning:

A computer program **learns** if its performance at task T , as measured by P , improves with experience E .

Well-Posed Learning Problem

Three components $\langle T, P, E \rangle$:

1. *Task, T* The behaviour or task being improved
2. *Experience, E* The experiences that are being used to improve performance in the task
3. *Performance measure, P* For example: increasing accuracy in prediction, acquiring new, improved speed and efficiency

Definition of learning:

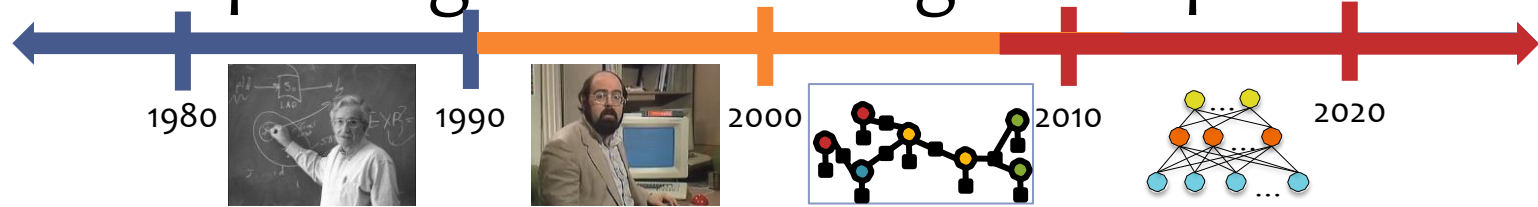
A computer program **learns** if its performance at task T , as measured by P , improves with experience E .

Example Learning Problem(s)

Learning to respond to voice commands (Siri)

- 1. *Task, T:*
- 2. *Performance measure, P:*
- 3. *Experience, E:*

Capturing the Knowledge of Experts



Solution #1: Expert Systems

- Over 20 years ago, we had rule-based systems:
 - Put a bunch of linguists in a room
 - Have them think about the structure of their native language and write down the rules they devise

Introspection...

x = "Give me directions to Starbucks"

x = "How do I get to Starbucks?"

x = "Where is the nearest Starbucks?"

x = "I need directions to Starbucks"

x = "Is there a Starbucks nearby?"

x = "Starbucks now!"

Rules...

if x matches "give me directions to Z": cmd = DIRECTIONS(here, nearest(Z))

if x matches "how do i get to Z": cmd = DIRECTIONS(here, nearest(Z))

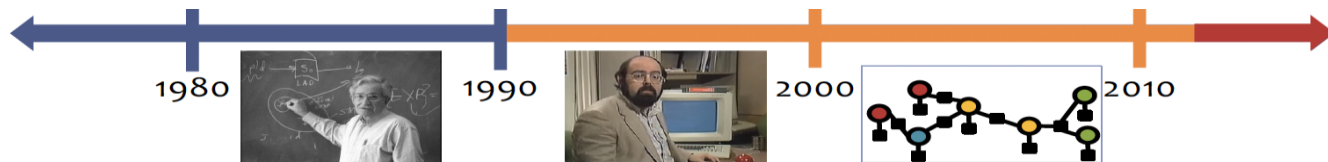
if x matches "where is the nearest Z": cmd = DIRECTIONS(here, nearest(Z))

if x matches "I need directions to Z": cmd = DIRECTIONS(here, nearest(Z))

if x matches "Is there a Z nearby": cmd = DIRECTIONS(here, nearest(Z))

if x matches "Z now!": cmd = DIRECTIONS(here, nearest(Z))

Capturing the Knowledge of Experts



Solution #2: Annotate Data and Learn

- Experts:
 - **Very good** at answering questions about specific cases
 - **Not very good** at telling **HOW** they do it
- 1990s: So why not just have them tell you what they do on **SPECIFIC CASES** and then let **MACHINE LEARNING** tell you how to come to the same decisions that they did

Capturing the Knowledge of Experts



Solution #2: Annotate Data and Learn

1. Collect raw sentences $\{x^{(1)}, \dots, x^{(n)}\}$
2. Experts annotate their meaning $\{y^{(1)}, \dots, y^{(n)}\}$

$x^{(1)}$: How do I get to Starbucks?

$y^{(1)}$: `directions(here,
nearest(Starbucks))`

$x^{(2)}$: Show me the closest Starbucks

$y^{(2)}$: `map(nearest(Starbucks))`

$x^{(3)}$: Send a text to John that I'll be late

$y^{(3)}$: `txtmsg(John, I'll be late)`

$x^{(4)}$: Set an alarm for seven in the morning

$y^{(4)}$: `setalarm(7:00AM)`

Learning to respond to voice commands

1. Task, T: predicting action from speech
2. Performance measure, P: percent of correct actions taken in user pilot study
3. Experience, E: examples of (speech, action) pairs



Learning to approve loans

1. Task, T :
2. Performance measure, P :
3. Experience, E :

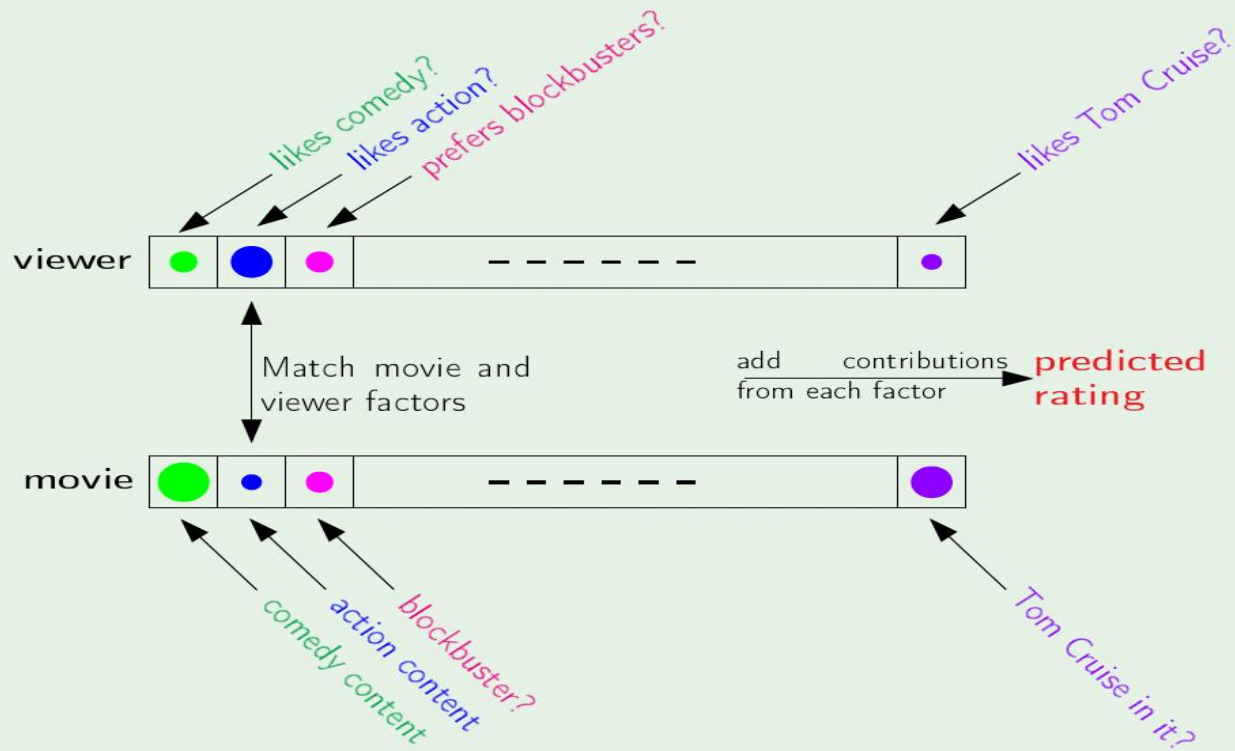
Learning to approve loans

1. Task, T: **decide whether to extend a loan to someone**
2. Performance measure, P: **minimize number of defaulters**
3. Experience, E: **Data from past loans, interview with loan officers**

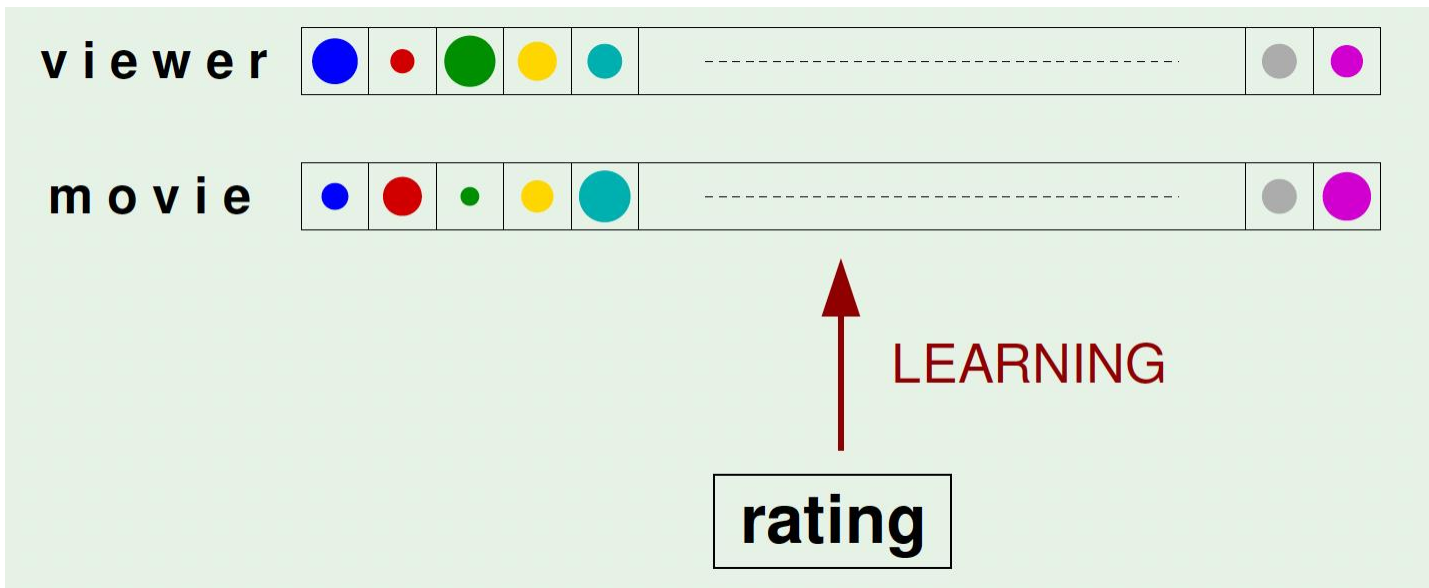
Learning to approve loans

1. Task, T: **predict the probability of someone defaulting on a loan**
2. Performance measure, P: **Amount of interest earned over 10 years**
3. Experience, E: **Data from past loan applications and defaults**

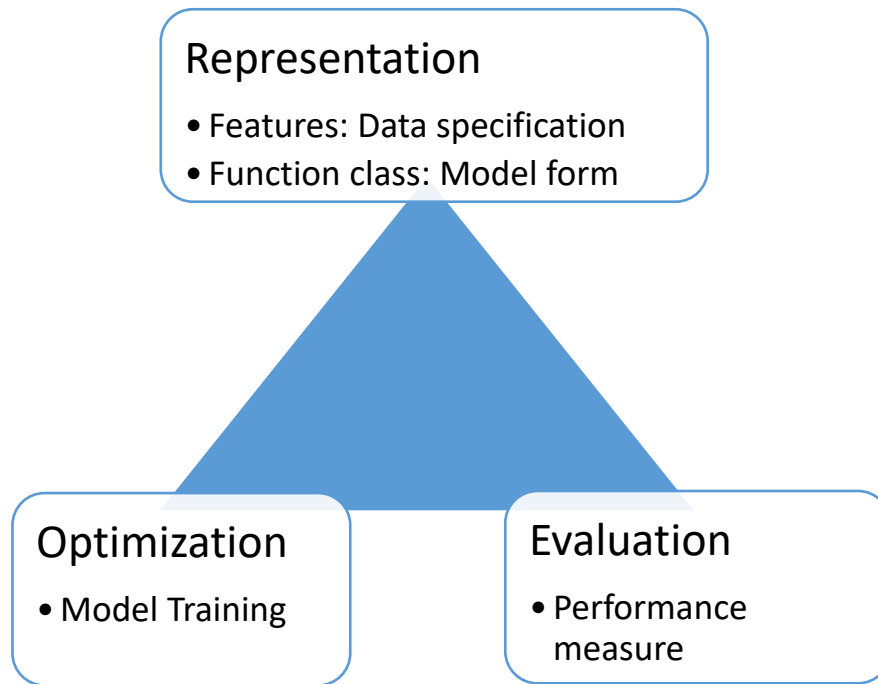
Movie Rating – A Solution



The Learning approach



Components of a ML application



A. Representation of Data

How is the data specified?

A. Features

- Feature vector of n features

$$\bar{x} = (x_1, x_2, \dots, x_n)$$

B. Convert input to a vector of basis functions

$$(\phi_0(\bar{x}), \phi_1(\bar{x}), \dots, \phi_p(\bar{x}))$$

A microwave



Attributes:

- Volume: 17 l, 23 l, ...
- Functions: Micro, Convection, ...
- Power level
- Accessories
- Type of dial
- Brand
- Warranty
- Price

Image of shirt

- Collar style
- Sleeve type
- Colour
- ...



Features

Image classification

- Raw pixels
- Histograms
- GIST descriptors



Product Rating (Webcam)

- Frame rate
- Resolution
- Autofocus
- Microphone
- Lens
- Brand

Bank Marketing Dataset

<http://archive.ics.uci.edu/ml/datasets/Bank+Marketing>

Predict if the client will subscribe (yes/no) a term deposit (variable y).

Input variables:

bank client data:

1. age
2. type of job
3. marital status
4. education
5. has credit in default?
6. has housing loan?
7. has personal loan?

related with the last contact of the current campaign:

8. contact communication type ('cellular','telephone')
9. last contact date and duration

other attributes:

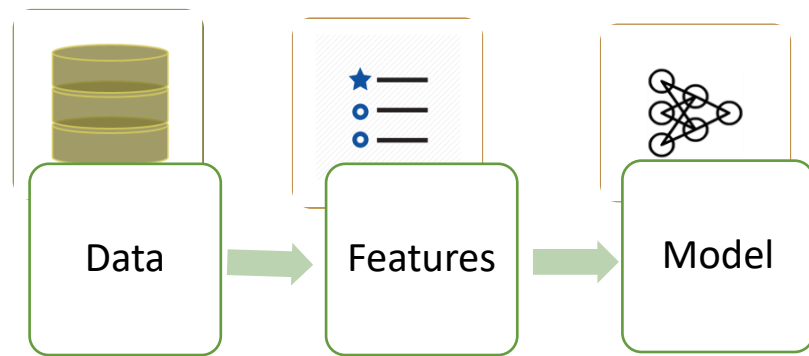
12. No of contacts performed for this client
13. No of days after client last contacted
14. No of contacts performed before this campaign and for this client
15. outcome of prev marketing campaign

social and economic context attributes

16. employment variation rate - quarterly indicator
17. consumer price index - monthly indicator
18. consumer confidence index - monthly indicator
19. euribor 3 month rate - daily indicator
20. number of employees - quarterly indicator

Feature Choice

- Input Data comprise features
 - Structured features (numerical or categorical values)
 - Unstructured (text, speech, image, video, etc)
- Use only relevant features
- Too many features?
 - Select feature subset (reduction)
 - Extract features: Transform features



B. Model Representation

- The richer the representation, the more useful it is for subsequent problem solving.
- The richer the representation, the more difficult it is to learn.

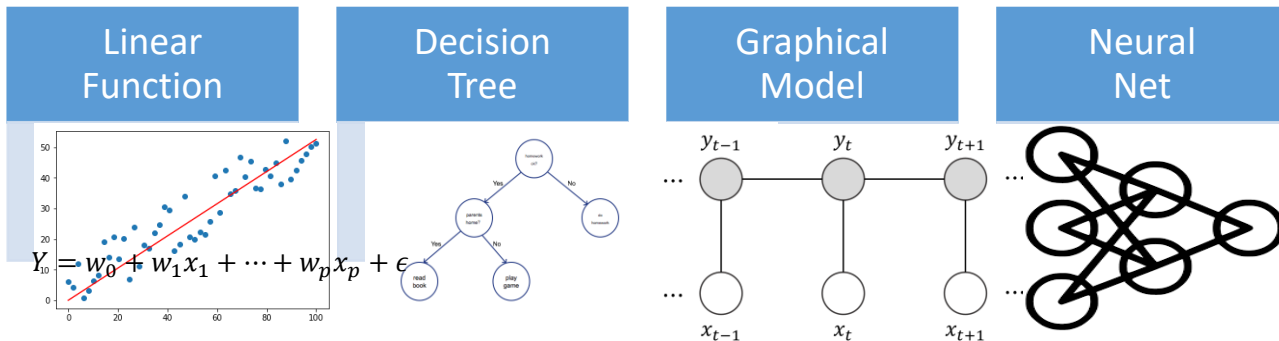
$$y = f(\bar{x})$$

$$y = g(\bar{\phi}(\bar{x}))$$

- Linear function
- Decision Tree
- Graphical Model
- Neural Network

B. Model Representation Hypothesis space

$$y = f(\bar{x})$$



2. Evaluation

1. Accuracy = $\frac{\text{\# correctly classified}}{\text{\# all test examples}}$
2. Logarithmic Loss:

$$L_i = -\log(P(Y = y_i|X = x_i))$$

$$L = \sum_{c=1}^M y_{oc} \log(p_{oc})$$

3. Mean Squared error

$$MSE = \frac{1}{m} \sum (y_{pred} - y_{true})^2$$

3. Optimization

- Define loss function
- Optimize loss function
- Stochastic Gradient Descent (Convex functions)
- Combinatorial optimization
 - E.g.: Greedy search
- Constrained optimization
 - E.g.: Linear programming

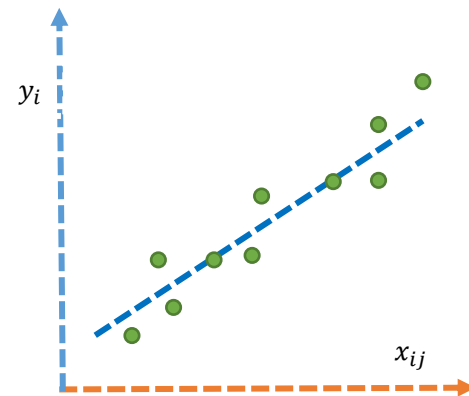
Elements of Optimization

1. Variables
2. Constraints
3. Objective Function

Simple Linear Regression

1. Variables: w_0, w_1, \dots, w_n
2. Constraints: none
3. Objective Function: Minimize

$$\sum_{i=1}^m \left(y_i \left(w_0 + \sum_{j=1}^n w_j x_{ij} \right) \right)^2$$



- m data points, n features
 - x_{ij} : j th attribute of i th instance
 - y_i : output of i th instance

Find coefficients w_0, w_1, \dots, w_n to best fit data

- **Task:** Credit approval
- Applicant information:

Age	23 years
Gender	male
Annual salary	\$30000
Years in residence	1 year
Years in job	1 year
Current debt	\$15000
...	...

- Approve Credit?

Components of Learning

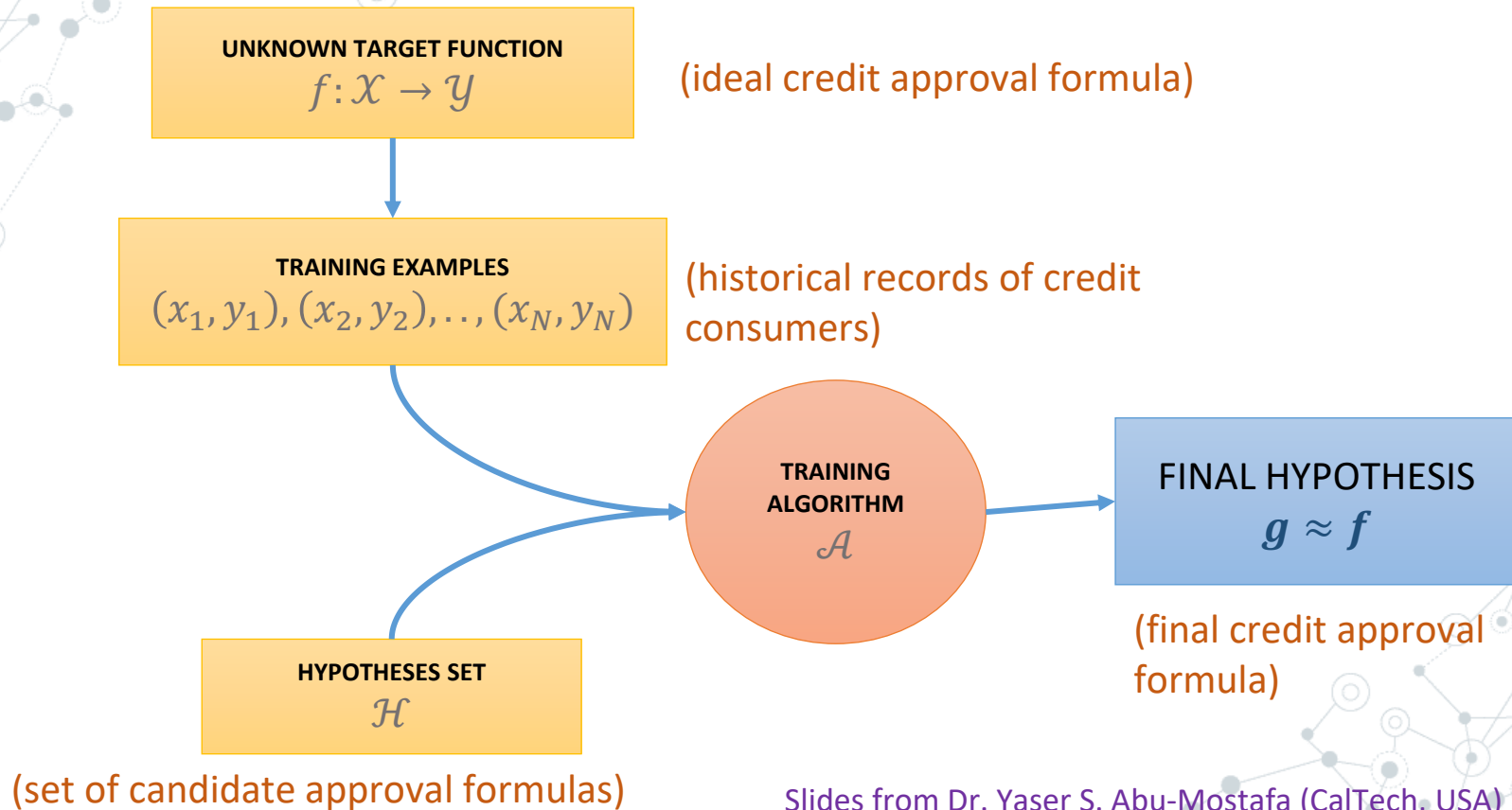
Formalization

- Input x (customer application)
- Output y (good/bad customer?)
- Target function $f: \mathcal{X} \rightarrow \mathcal{Y}$ (ideal credit approval formula)
- Data $(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)$ (historical records)



- Hypothesis $g: \mathcal{X} \rightarrow \mathcal{Y}$ (formula to be used)

Components of Learning





CS60050: Machine Learning

Autumn 2024

Sudeshna Sarkar

Introduction to ML

26 July 2024



Course Website

<https://machine-learning-2024-cs60050.netlify.app/>

1st Lab Session

Monday , 29 July

Tentative time: 6:30 pm

Exact Venue and Time To be announced

Contact

Email: sudeshna@cse.iitkgp.ac.in Subject “CS60050 ML24”

- **Task:** Credit approval
- Applicant information:

Age	23 years
Gender	male
Annual salary	\$30000
Years in residence	1 year
Years in job	1 year
Current debt	\$15000
...	...

- Approve Credit?

Components of Learning

Formalization

- Input x (customer application)
- Output y (good/bad customer?)
- Target function $f: \mathcal{X} \rightarrow \mathcal{Y}$ (ideal credit approval formula)
- Data $(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)$ (historical records)



- Hypothesis $g: \mathcal{X} \rightarrow \mathcal{Y}$ (formula to be used)

Solution Components

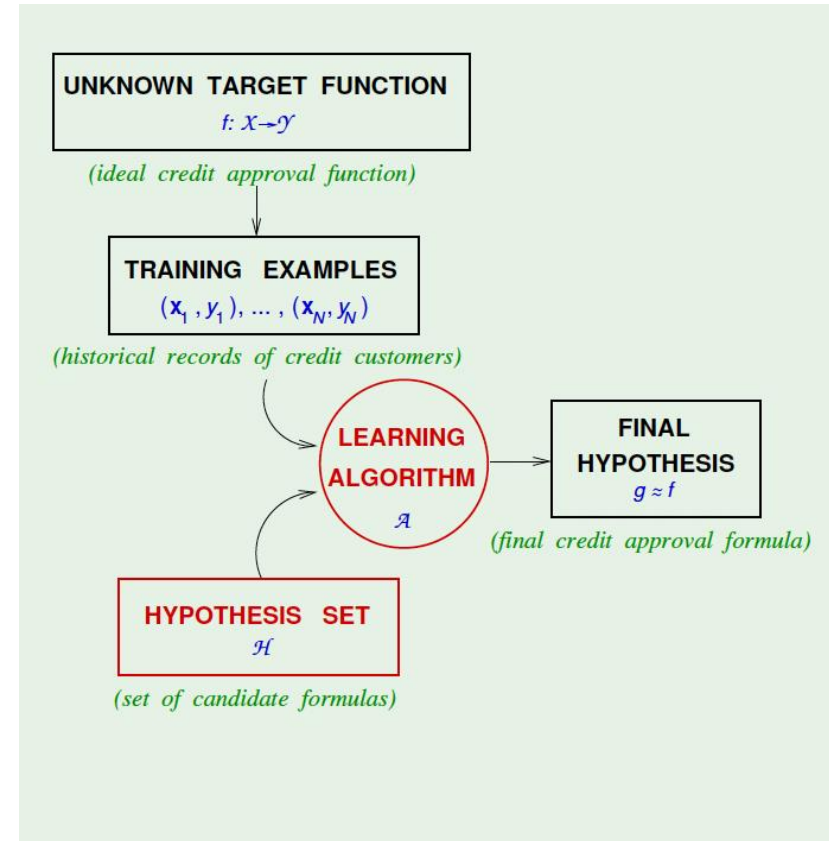
2 solution components of the learning problem

- The Hypothesis Set

$$\mathcal{H} = \{h\}, g \in \mathcal{H}$$

- The Learning Algorithm

Together, they are referred to as the *learning model*.



A simple hypothesis set – the ‘perceptron’

For input $x = (x_1, \dots, x_d)$ ‘attributes of a customer’

Approve credit if $\sum_{i=1}^d w_i x_i > \text{threshold}$,

Deny credit if $\sum_{i=1}^d w_i x_i < \text{threshold}$,

Linear formula $h \in \mathcal{H}$ can be written as

$$h(x) = \text{sign}(\sum_{i=1}^d w_i x_i - \text{threshold})$$

Separability

The perceptron implements

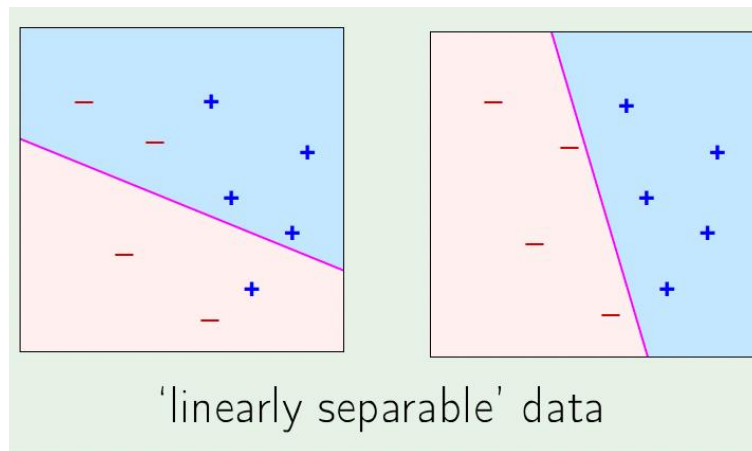
$$h(x) = \text{sign}(\sum_{i=1}^d w_i x_i + w_0)$$

Introducing an artificial coordinate $x_0 = 1$

$$h(x) = \text{sign}(\sum_{i=0}^d w_i x_i)$$

In vector form, the perceptron implements

$$h(x) = \text{sign}(w^T x)$$



A simple Learning Algo - PLA

The perceptron implements

$$h(\mathbf{x}) = \text{sign}(\mathbf{w}^T \mathbf{x})$$

Given the training set:

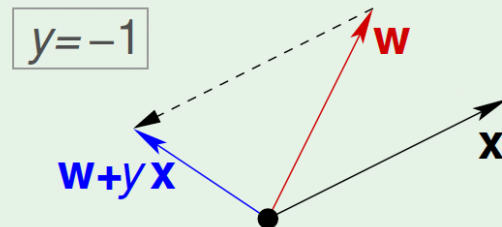
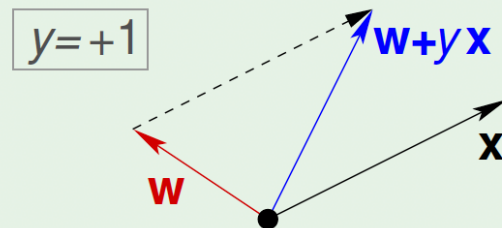
$$(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)$$

pick a **misclassified** point:

$$\text{sign}(\mathbf{w}^T \mathbf{x}_n) \neq y_n$$

and update the weight vector:

$$\mathbf{w} \leftarrow \mathbf{w} + y_n \mathbf{x}_n$$



Iterations of PLA

- One iteration of the PLA:

$$\mathbf{w} \leftarrow \mathbf{w} + y\mathbf{x}$$

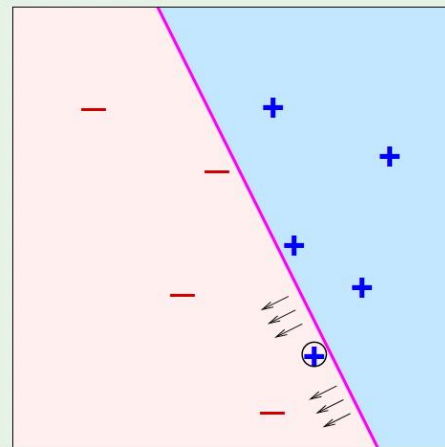
where (\mathbf{x}, y) is a misclassified training point.

- At iteration $t = 1, 2, 3, \dots$, pick a misclassified point from

$$(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)$$

and run a PLA iteration on it.

- That's it!



Broad types of machine learning

- Supervised Learning
 - Training Data with labels: X, y (pre-classified)
 - Given an observation x , what is the best label for y ?
- Unsupervised learning
 - Training Data without labels: X
 - Given a set of x 's, find hidden structure
- Semi-supervised Learning
 - Training Data + some Labels
- Reinforcement Learning
 - Given: observations and periodic rewards as the agent takes sequential action in an environment
 - Determine optimum policy

Supervised Learning

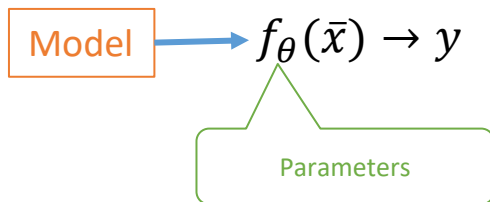
- Given data containing the inputs and outputs:

Training Data:

$$\{(\bar{x}_1, y_1), (\bar{x}_2, y_2), \dots, (\bar{x}_m, y_m)\}$$

- Learn a function $f(x)$ to predict y given x

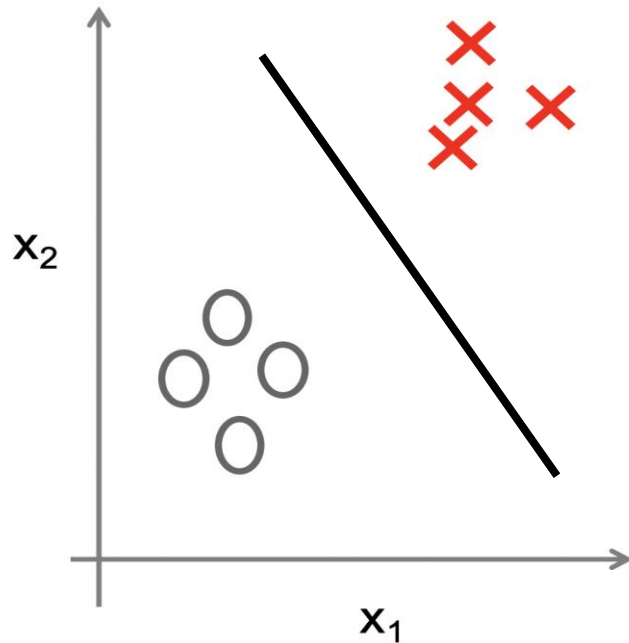
\bar{X}	Y
\bar{x}_1	y_1
\bar{x}_2	y_2
...	..
\bar{x}_m	y_m



Training: Learn the model from the Training Data

Given Test instance \bar{x}' , predict $y' = f_{\theta}(\bar{x}')$

Supervised Learning

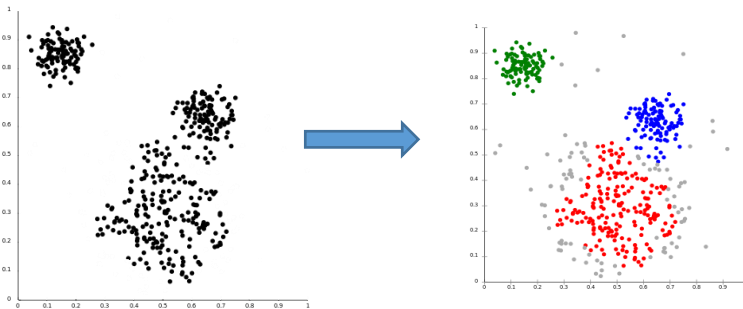


Classification (one example)

- Input: (input-features, correct output)
 - $\langle \text{size, \#rooms} \rangle, \langle \text{cheap/costly} \rangle$
- Output of learning algorithm
 - Function maps features to output
 - $F(\langle \text{size, \#rooms} \rangle) = \text{cheap/costly}$

Unsupervised Learning (Clustering)

- Given $\{\overline{x_1}, \overline{x_2}, \dots \overline{x_m}, \}$ without labels
- Find hidden structure in the data
 - Clustering
 - Dimensionality Reduction
- Clustering: Grouping similar objects

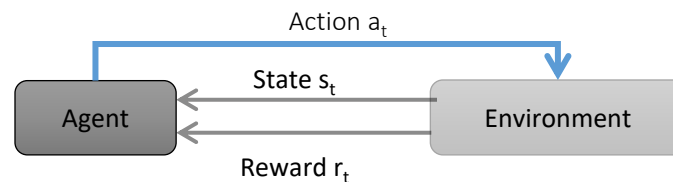


Reinforcement Learning

- Given a sequence of states and actions with (delayed) rewards, output a policy.

- Receive feedback in the form of **rewards**
- Agent's utility is defined by the reward function
- Must (learn to) act so as to **maximize expected rewards**

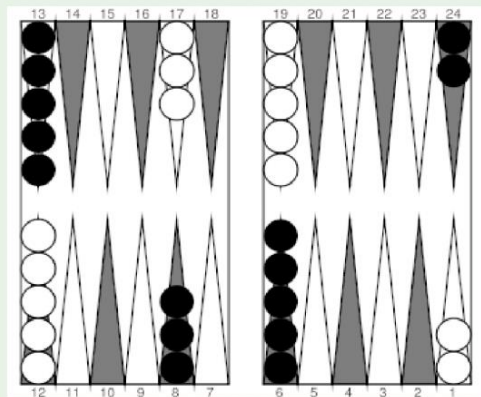
Goal: Constantly learn to make 'optimal' predictions based on real-time feedback from past predictions



- Examples:
 - Game playing (Go)
 - Robot grasping
 - Controlling aircraft and robotic motion

Reinforcement Learning

Instead of (input, correct output),
we get (input, some output, grade for this output)



The world champion was
a neural network!