Chapter-6

Machine Learning

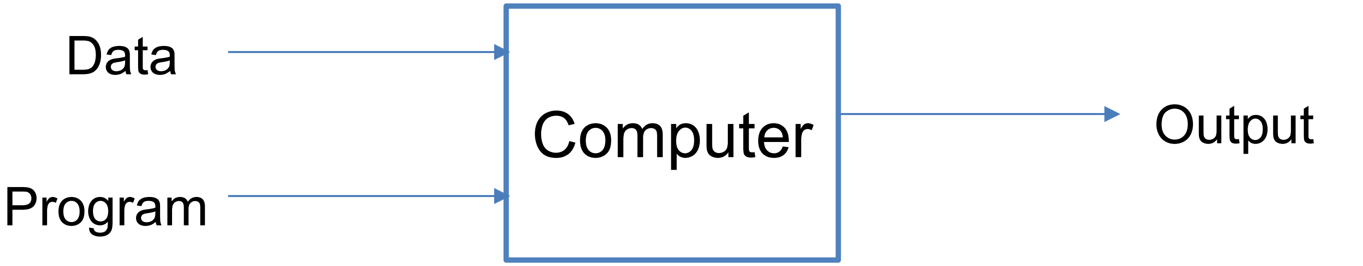
What is Machine Learning?

- “Learning is any process by which a system improves performance from experience.”
  - Herbert Simon

- Definition by Tom Mitchell (1998):
  - Machine Learning is the study of algorithms that
    - improve their performance P
    - at some task T
    - with experience E.

    A well-defined learning task is given by <P, T, E>.

Traditional Programming

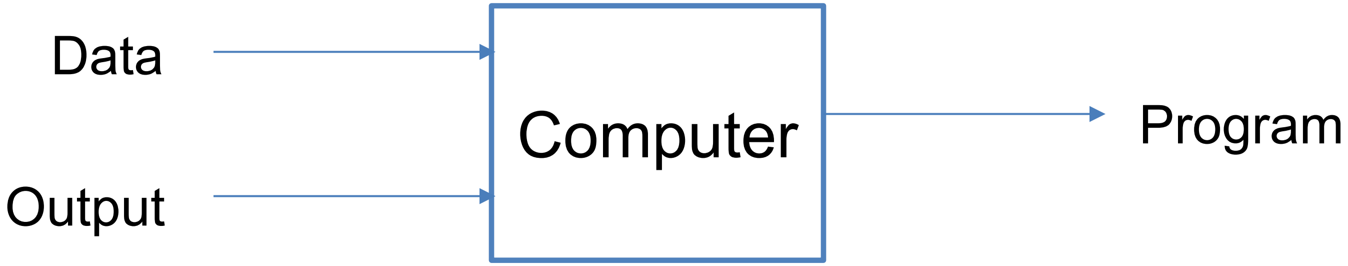

Data

Program

Computer

Output

Machine Learning


Data

Output

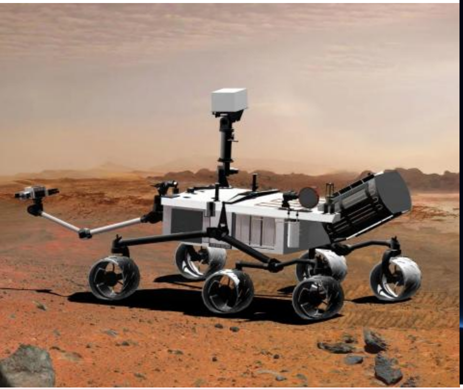
Computer

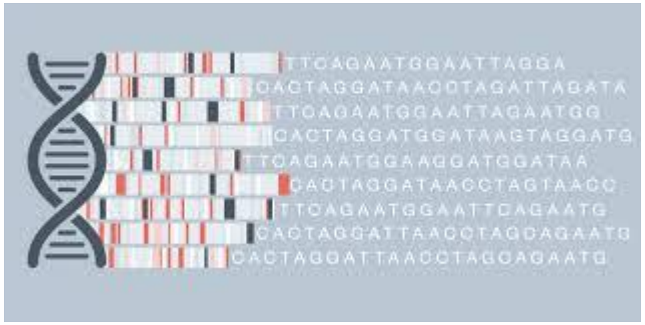
Program

When do we use machine learning?

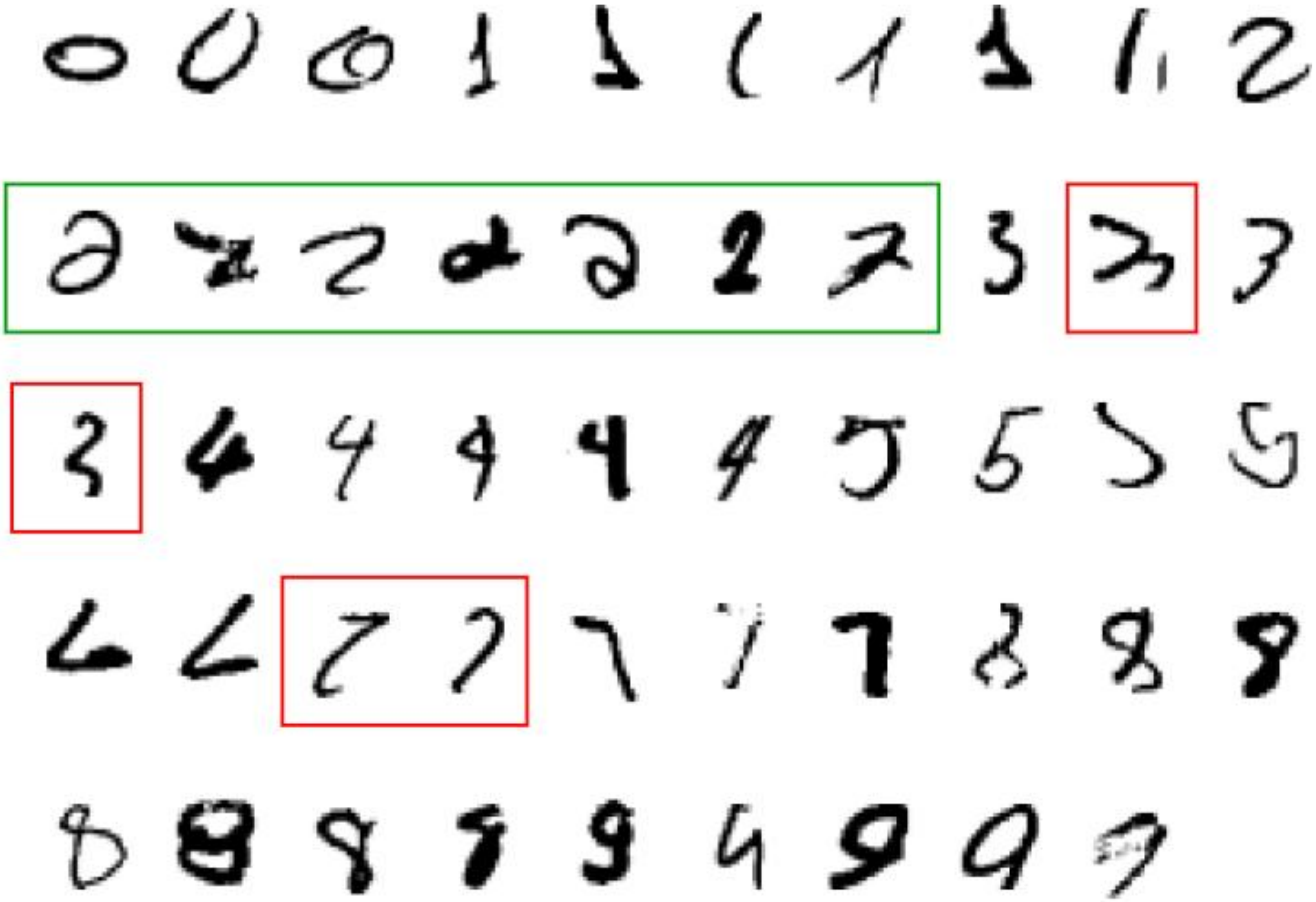
ML is used when:

- Human expertise does not exist (navigating on Mars)
- Humans can’t explain their expertise (speech recognition)
- Models must be customized (personalized medicine)
- Models are based on huge amounts of data (genomics)





A classic example of a task that requires machine learning: It is very hard to say what makes a 2



Some more examples of tasks that are best solved by using a learning algorithm

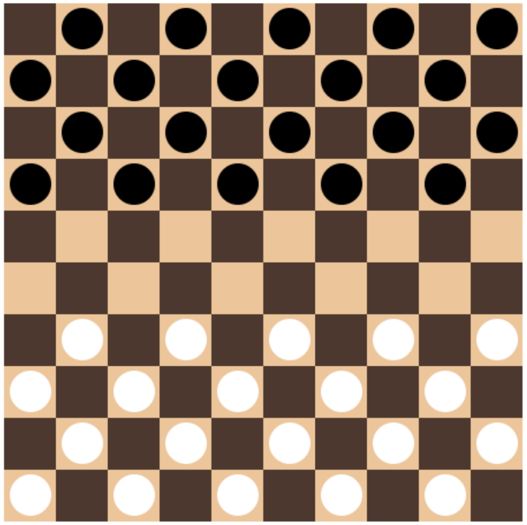
- Recognizing patterns:
  - Facial identities or facial expressions
  - Handwritten or spoken words
  - Medical images
- Generating patterns:
  - Generating images or motion sequences
- Recognizing anomalies:
  - Unusual credit card transactions
  - Unusual patterns of sensor readings in a nuclear power plant
- Prediction:
  - Future stock prices or currency exchange rates

Sample Applications

- Web search
- Computational biology
- Finance
- E-commerce
- Space exploration
- Robotics
- Information extraction
- Social networks
- Debugging software

Samuel’s Checkers-Player

“Machine Learning: Field of study that gives computers the ability to learn without being explicitly programmed.” -Arthur Samuel (1959)



Defining the Learning Task

Improve on task T, with respect to
performance metric P, based on experience E

T: Playing checkers
P: Percentage of games won against an arbitrary opponent
E: Playing practice games against itself

T: Recognizing hand-written words
P: Percentage of words correctly classified
E: Database of human-labeled images of handwritten words

T: Driving on four-lane highways using vision sensors
P: Average distance traveled before a human-judged error
E: A sequence of images and steering commands recorded while observing a human driver.

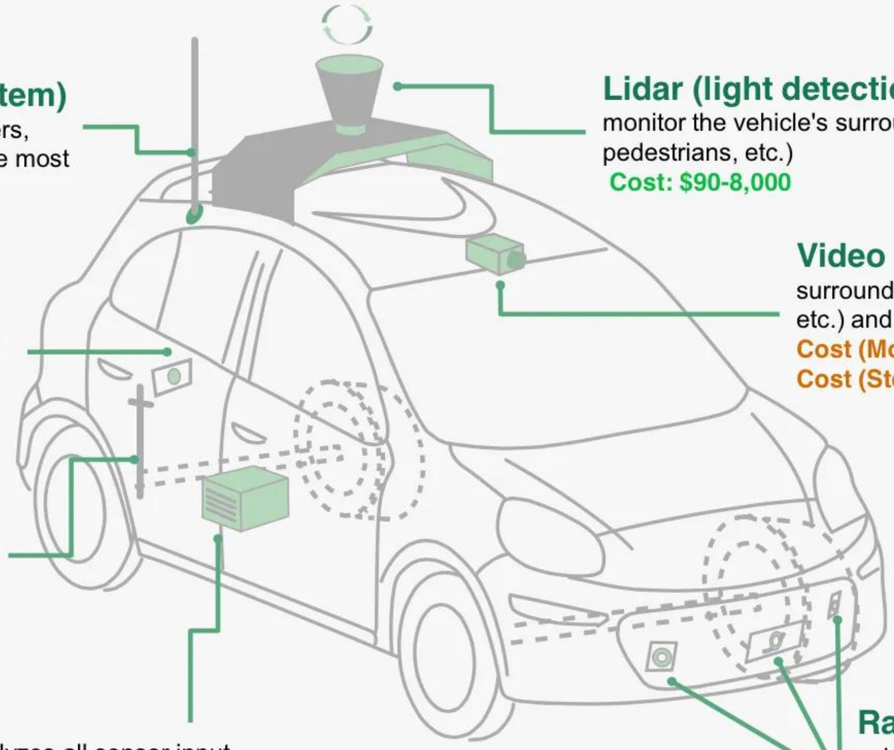
T: Categorize email messages as spam or legitimate.
P: Percentage of email messages correctly classified.
E: Database of emails, some with human-given labels

State of the Art Applications of Machine Learning

Autonomous Cars

SELF DRIVING MODE
40

Autonomous Cars



GPS (global positioning system) combined with readings from tachometers, altimeters and gyroscopes to provide the most accurate positioning
Cost: $80-$6,000

Ultrasonic sensors to measure the position of objects very close to the vehicle
Cost: $15-$20

Odometry sensors to complement and improve GPS information
Cost: $80-$120

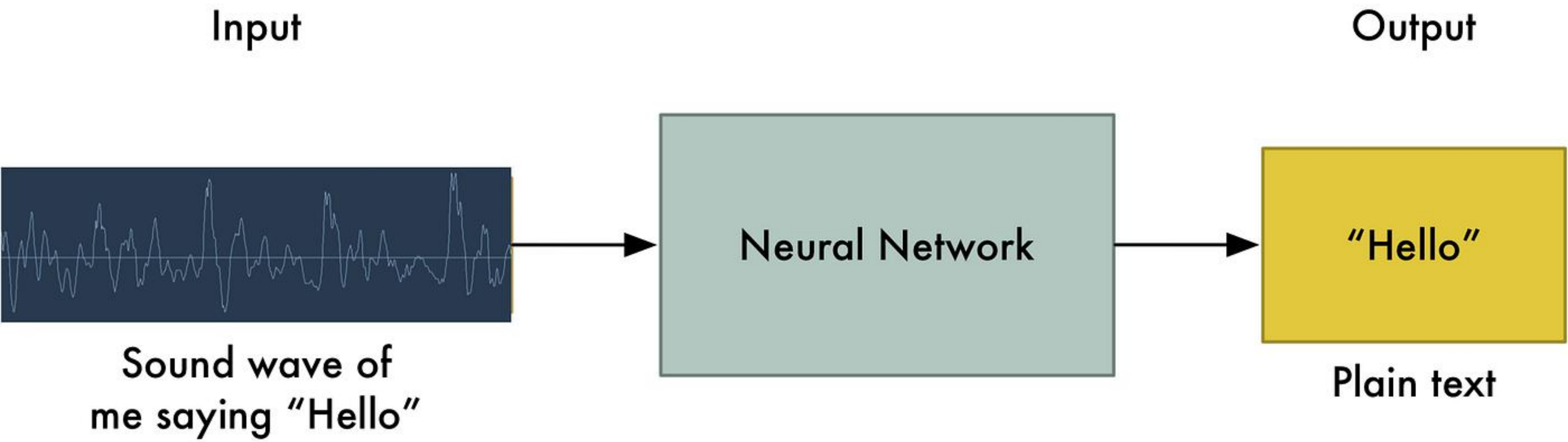
Central computer analyzes all sensor input, applies rules of the road and operates the steering, accelerator and brakes
Cost: ~50-200% of sensor costs

Lidar (light detection and ranging) monitor the vehicle's surroundings (road, vehicles, pedestrians, etc.)
Cost: $90-8,000

Video cameras monitor the vehicle's surroundings (road, vehicles, pedestrians, etc.) and read traffic lights
Cost (Mono): $125-$150
Cost (Stereo): $150-$200

Radar sensors monitor the vehicle's surroundings (road, vehicles, pedestrians, etc.)
Cost (Long Range): $125-$150
Cost (Short Range): $50-$100

Speech Recognition


Input

Output

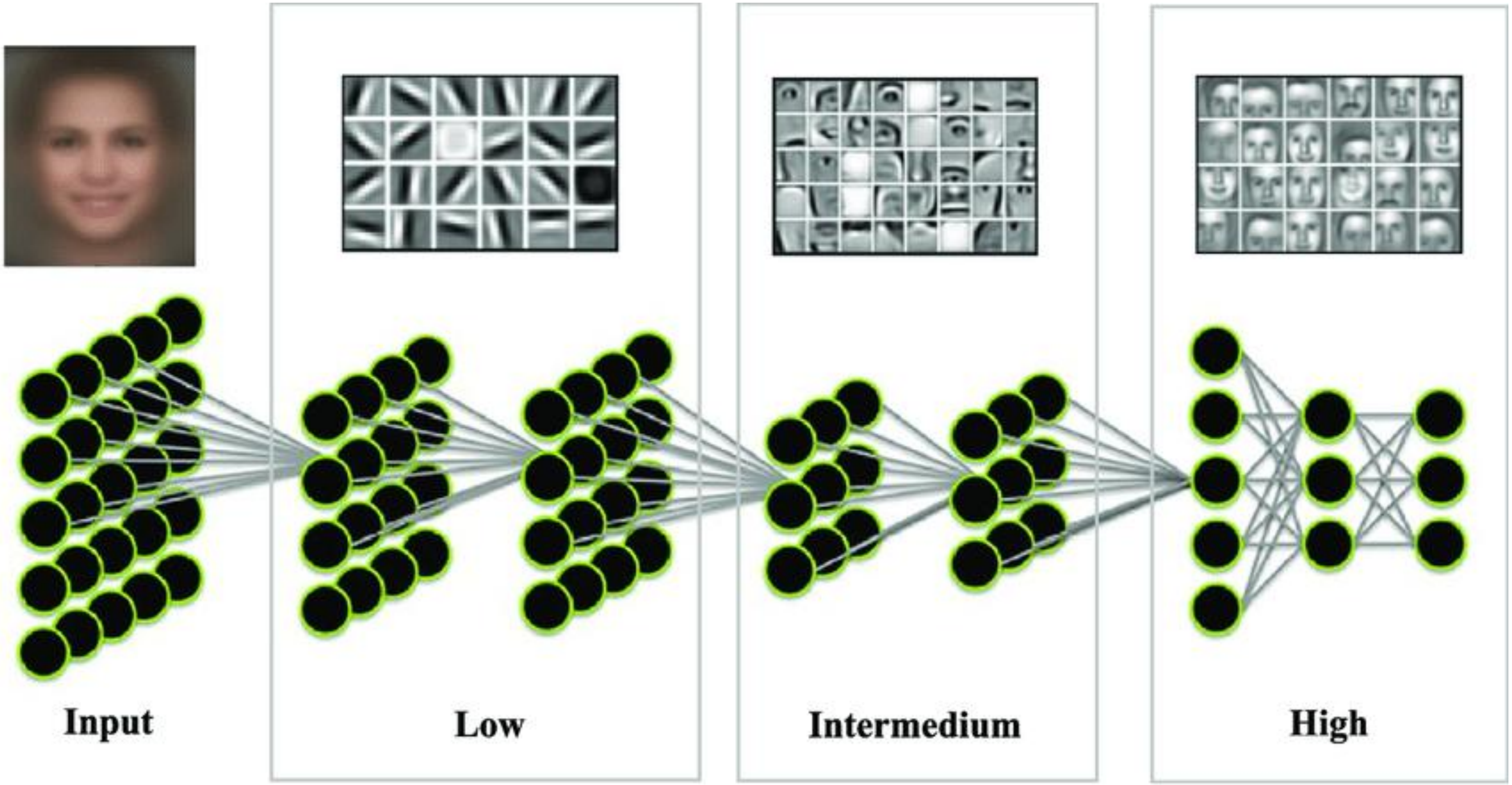
Neural Network

"Hello"

Sound wave of
me saying "Hello"

Plain text

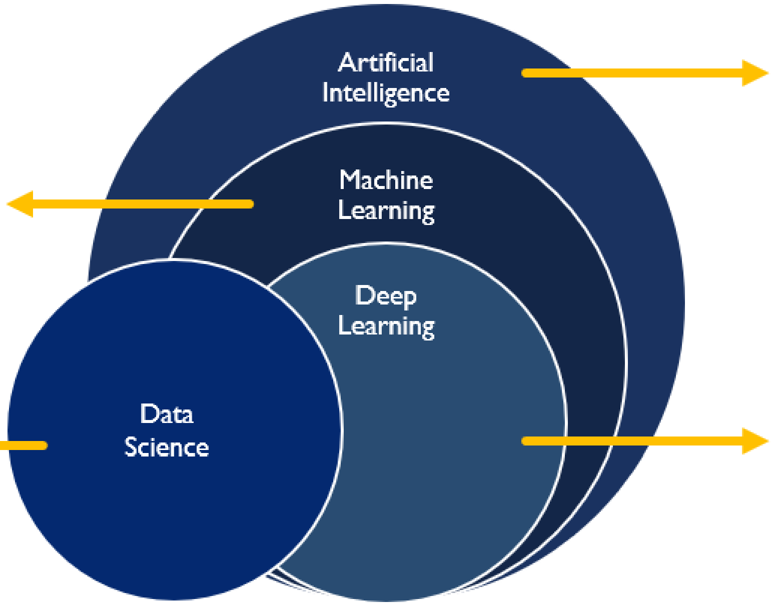
Face Recognition



DS vs AI vs ML vs DL

Machine Learning is a subset of AI, and builds a model based on training data to make predictions

Data Science is a subset of AI. It is an area of statistics, scientific methods, etc. to extract meaning and insights from data..



Artificial Intelligence means creating smart machines to mimic human behavior

Deep learning is a subset of ML, a class of ML algorithms to solve complex problems.

Forms of Learning

Any component of an agent can be improved by learning from data. The improvements, and the techniques used to make them, depend on four major factors:

- Which *component* is to be improved.
- What *prior knowledge* the agent already has.
- What *representation* is used for the data and the component.
- What *feedback* is available to learn from.

Forms of Learning: Components to be learned

The components of these agents include:

1. A direct mapping from conditions on the current state to actions.
2. A means to infer relevant properties of the world from the percept sequence.
3. Information about the way the world evolves and about the results of possible actions the agent can take.
4. Utility information indicating the desirability of world states.
5. Action-value information indicating the desirability of actions.
6. Goals that describe the most desirable states.
7. A problem generator, critic, and learning element that enable the system to improve.

Forms of Learning: Components to be learned

For example, an agent training to become a taxi driver.

- Every time the instructor shouts “Brake!” the agent might learn a condition action rule for when to brake (component 1);
- the agent also learns every time the instructor does not shout. By seeing many camera images that it is told contain buses, it can learn to recognize them (2).
- By trying actions and observing the results—for example, braking hard on a wet road—it can learn the effects of its actions (3).
- Then, when it receives no tip from passengers who have been thoroughly shaken up during the trip, it can learn a useful component of its overall utility function (4)

Forms of Learning: Representation and prior knowledge

- We have seen several examples of **representations** for agent components: propositional and first-order logical sentences for the components in a logical agent; Bayesian networks for the inferential components of a decision-theoretic agent, and so on.
- Effective learning algorithms have been devised for all of these representations.
- This chapter (and most of current machine learning research) covers inputs that form a **factored representation**—a vector of attribute values—and outputs that can be either a continuous numerical value or a discrete value.

Forms of Learning: Types of feedback

- Supervised Learning
- Unsupervised Learning
- Semi-Supervise Learning
- Reinforcement Learning

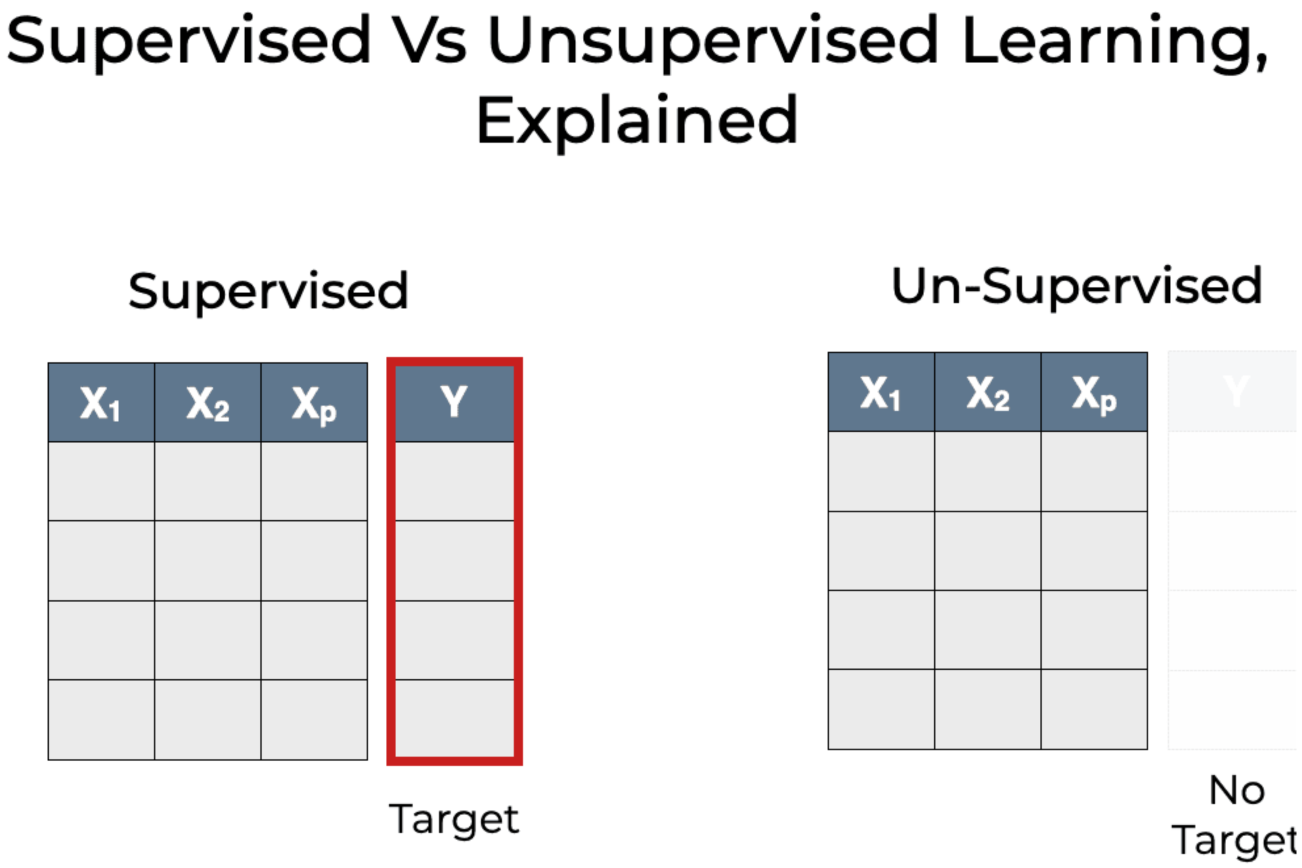
Forms of Learning: Types of feedback

- Supervised Learning
  - In supervised learning the agent observes some example input–output pairs and learns a function that maps from input to output.
  - Learning with labeled data.
  - Goal: Predict outcomes based on input data.
  - Examples: Classification and regression tasks.
  - In component 1 above, the inputs are percepts, and the output are provided by a teacher who says “Brake!” or “Turn left.” In component 2, the inputs are camera images, and the outputs again come from a teacher who says, “that’s a bus.” In 3, the theory of braking is a function from states and braking actions to stopping distance in feet. In this case the output value is available directly from the agent’s percepts (after the fact); the environment is the teacher.

Forms of Learning: Types of feedback

- Unsupervised Learning
  - In unsupervised learning the agent learns patterns in the input even though no explicit feedback is supplied.
  - Learning without labeled data.
  - Goal: Find hidden patterns or intrinsic structures in input data.
  - The most common unsupervised learning task is dimensionality reduction, clustering (detecting potentially useful clusters of input examples).
  - For example, a taxi agent might gradually develop a concept of “good traffic days” and “bad traffic days” without ever being given labeled examples of each by a teacher.
  - Machine Learning algorithm: **K-means clustering** (Basic knowledge required)

Forms of Learning: Types of feedback



Supervised Vs Unsupervised Learning, Explained

Supervised

X_1	X_2	X_p	Y

Target

Un-Supervised

X_1	X_2	X_p	Y

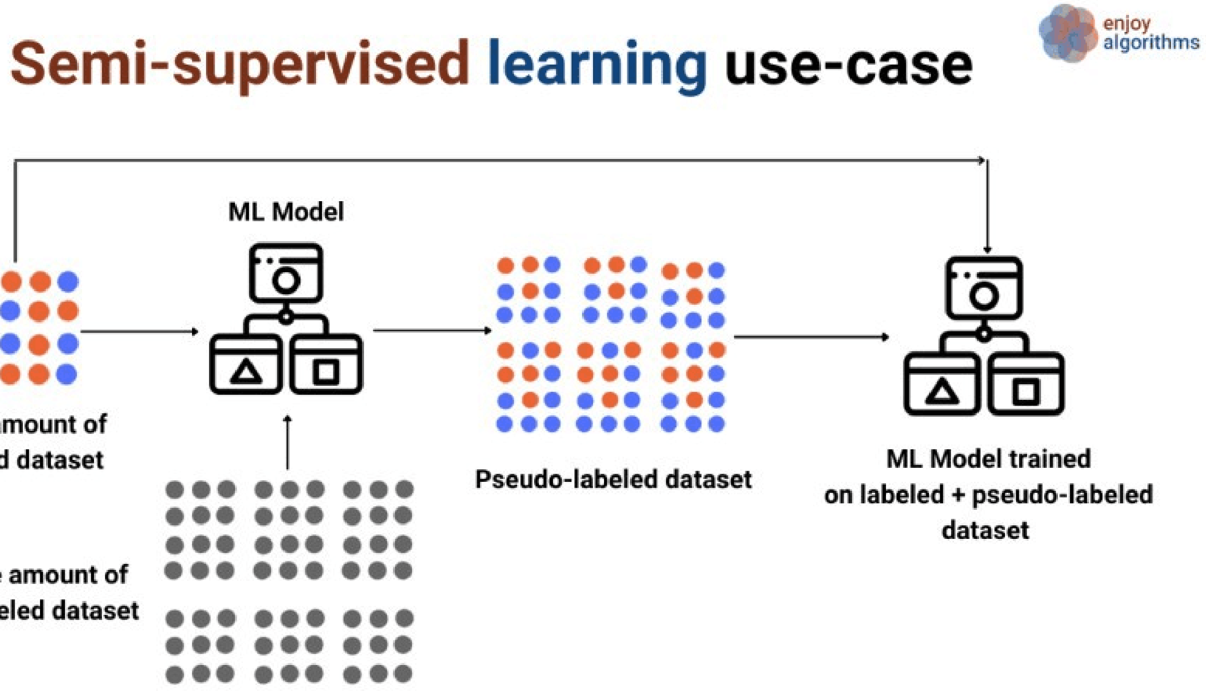
No Target

Forms of Learning: Types of feedback

- Semi-Supervised Learning
  - In semi-supervised learning we are given a few labeled examples and must make what we can of a large collection of unlabeled examples. Even the labels themselves may not be the oracular truths that we hope for.
  - Combination of a small amount of labeled data with a large amount of unlabeled data.
  - Goal: Improve learning accuracy when labeled data is scarce.

Forms of Learning: Types of feedback

- Semi-Supervised Learning


Semi-supervised learning use-case
enjoy algorithms
ML Model
Small amount of labeled dataset
Large amount of unlabeled dataset
Pseudo-labeled dataset
ML Model trained on labeled + pseudo-labeled dataset

Forms of Learning: Types of feedback

- Reinforcement Learning
  - In reinforcement learning the agent learns from a series of reinforcements—rewards or punishments.
  - Learning through interactions with the environment.
  - Goal: Maximize cumulative rewards.
  - Examples: Game playing, robotics.
  - For example, the lack of a tip at the end of the journey gives the taxi agent an indication that it did something wrong. The two points for a win at the end of a chess game tells the agent it did something right.

Supervised Learning

- The task of supervised learning is this:
  - Given a training set of N example input–output pairs

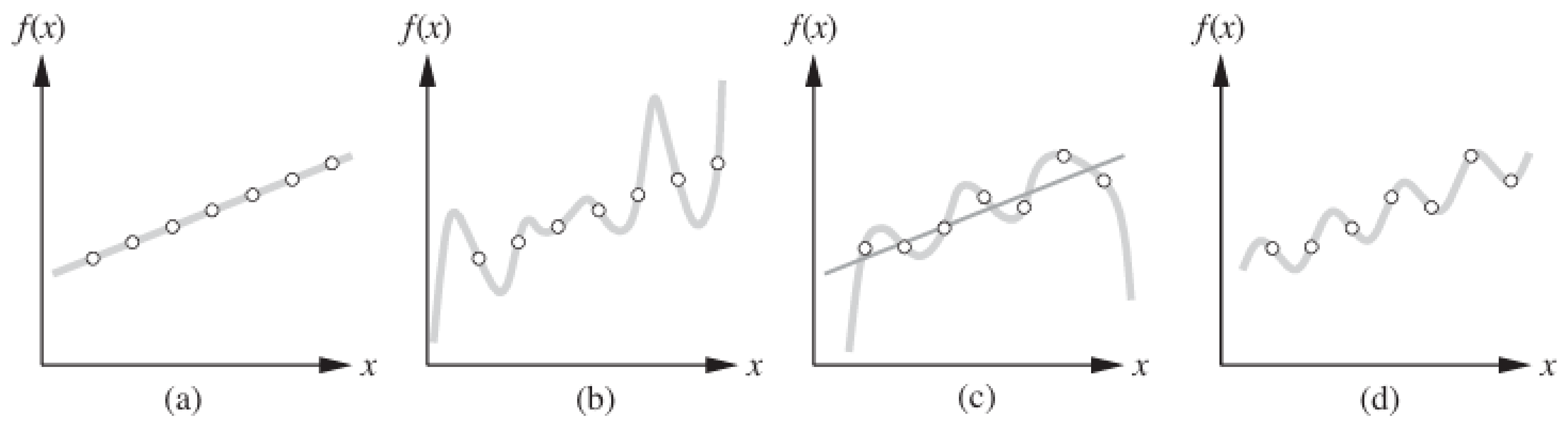
    $(x_1,y_1),(x_2,y_2),\ldots(x_N,y_N)$,

    where each y_j was generated by an unknown function y = ***f***(x), discover a function ***h*** that approximates the true function ***f***.
  - Here *x* and *y* can be any value; they need not be numbers.
  - The function ***h*** is a hypothesis.

Supervised Learning

- Learning is a search through the space of possible hypotheses for one that will perform well, even on new examples beyond the training set.
- To measure the accuracy of a hypothesis we give it a **test set** of examples that are distinct from the training set.

Supervised Learning



(a) (b) (c) (d)

Figure 18.1 (a) Example $(x, f(x))$ pairs and a consistent, linear hypothesis. (b) A consistent, degree-7 polynomial hypothesis for the same data set. (c) A different data set, which admits an exact degree-6 polynomial fit or an approximate linear fit. (d) A simple, exact sinusoidal fit to the same data set.

Types of Supervised Learning

- Supervised learning can be separated into two types of problems when data mining:
  - **Classification**:
    - Predicting a categorical outcome.
    - Examples: Spam detection, image classification.
  - **Regression**:
    - Predicting a continuous outcome.
    - Examples: House price prediction, stock price forecasting.

Algorithms in Machine Learning

- Classification: Logistic Regression, support vector machines (SVM), decision trees, k-nearest neighbor, random forest, and Naïve Bayes
- Regression: Linear Regression, Decision Tree Regressor, K Nearest Neighbor Regressor, and Random Forest Regressor.

The Theory of Learning

The Theory of Learning

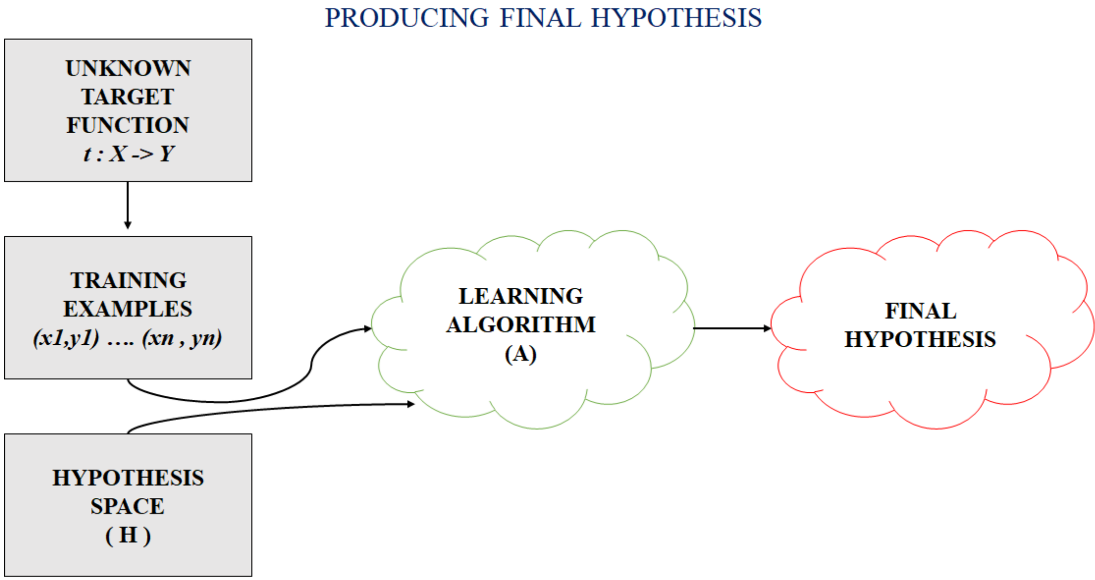
- How can we be sure that our learned hypothesis will predict well for previously unseen inputs? That is, how do we know that the hypothesis ***h*** is close to the target function ***f*** if we don't know what ***f*** is? These questions have been pondered for centuries, by Ockham, Hume, and others.
- In recent decades, other questions have emerged: how many examples do we need to get a good ***h***?
- What hypothesis space should we use? If the hypothesis space is very complex, can we even find the best ***h***, or do we have to settle for a local maximum?
- How complex should ***h*** be? How do we avoid overfitting?

Hypothesis (***h***)

- A hypothesis in machine learning is the model’s presumption regarding the connection between the input features and the result.
- It is an illustration of the mapping function that the algorithm is attempting to discover using the training set.
- To minimize the discrepancy between the expected and actual outputs, the learning process involves modifying the weights that parameterize the hypothesis.
- The objective is to optimize the model’s parameters to achieve the best predictive performance on new, unseen data, and a cost function is used to assess the hypothesis’ accuracy.

Hypothesis (*h*)

- In most supervised machine learning algorithms, our main goal is to find a possible hypothesis from the hypothesis space that could map out the inputs to the proper outputs.
- The following figure shows the common method to find out the possible hypothesis from the Hypothesis space:

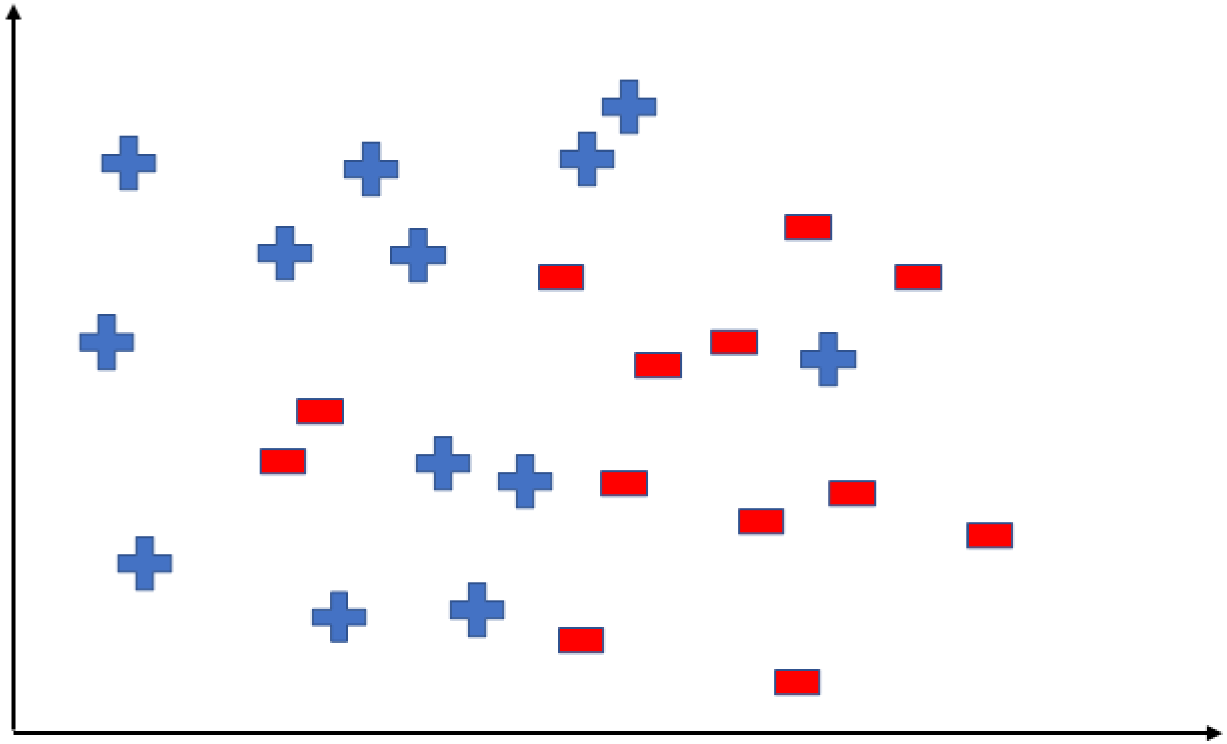


PRODUCING FINAL HYPOTHESIS
UNKNOWN TARGET FUNCTION $t : X \to Y$
TRAINING EXAMPLES $(x1,y1) \ldots (xn , yn)$
HYPOTHESIS SPACE (H)
LEARNING ALGORITHM (A)
FINAL HYPOTHESIS

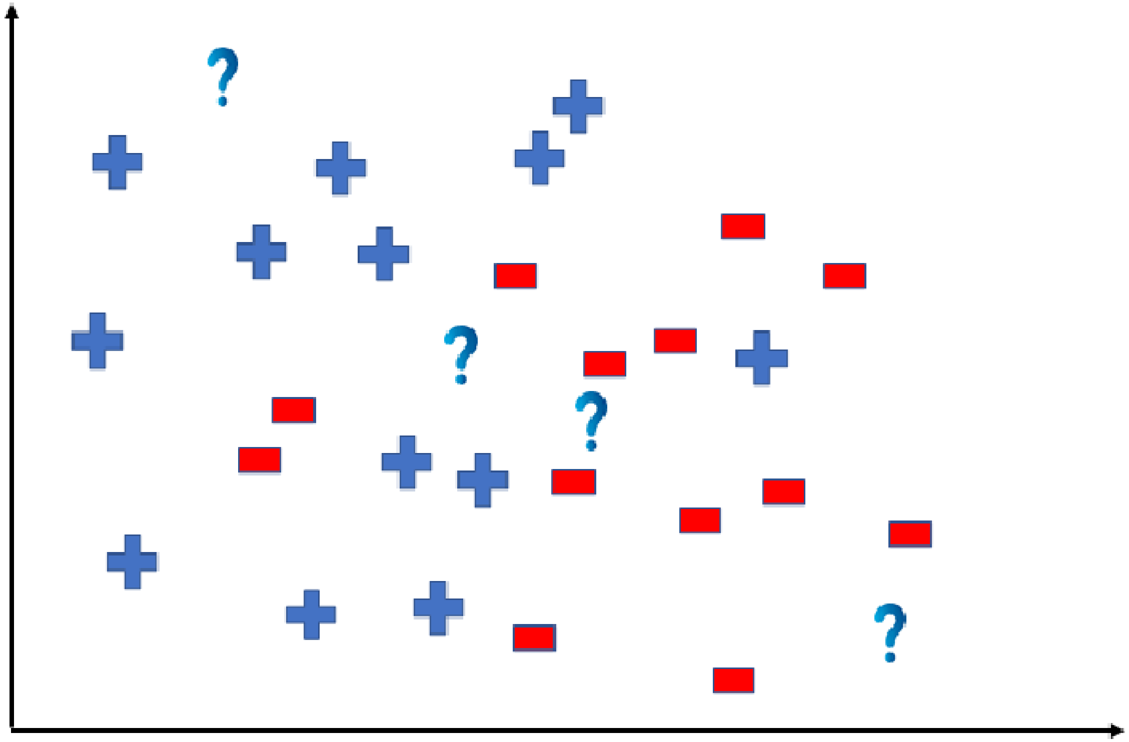
Hypothesis Space (H)

- Hypothesis space is the set of all the possible legal hypothesis. This is the set from which the machine learning algorithm would determine the best possible (only one) which would best describe the target function or the outputs.

Hypothesis & Hypothesis Space

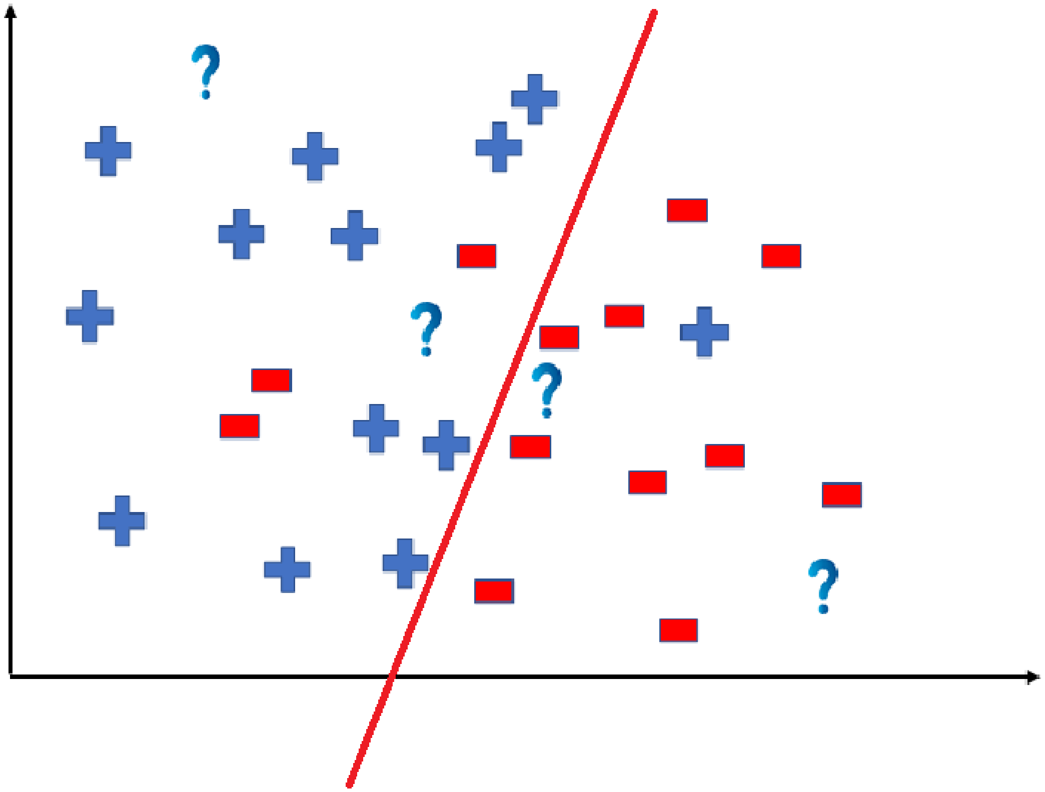


Hypothesis & Hypothesis Space



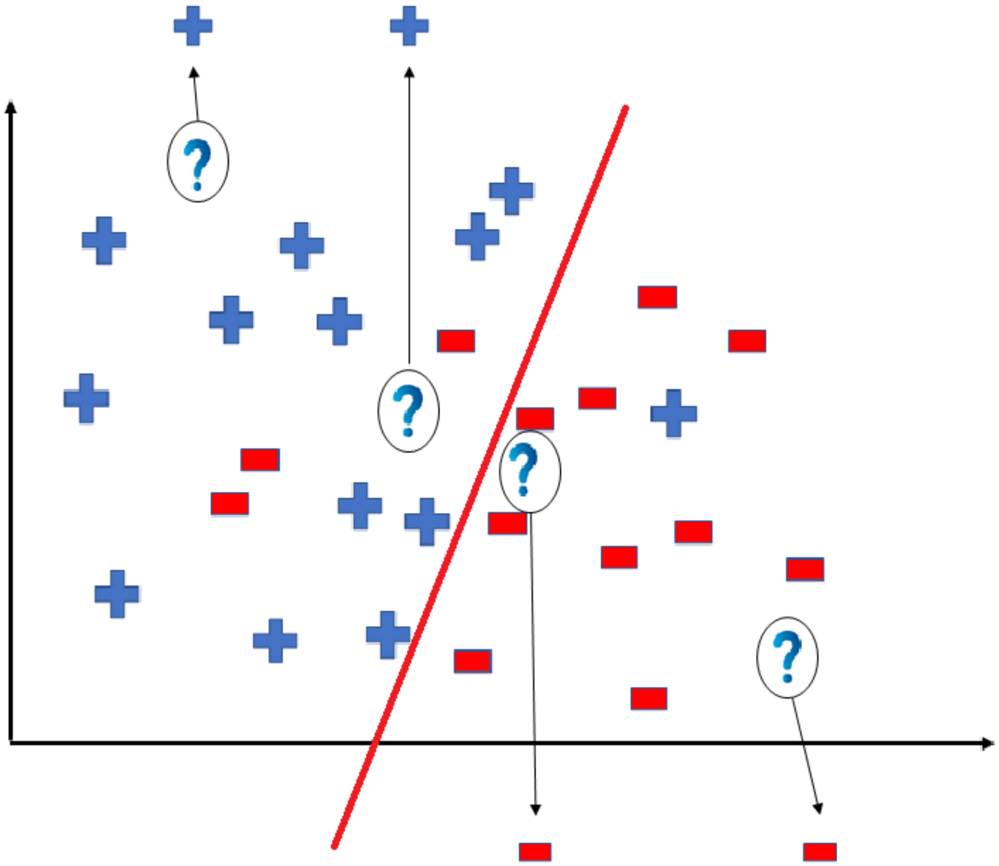
Test Data

Hypothesis & Hypothesis Space



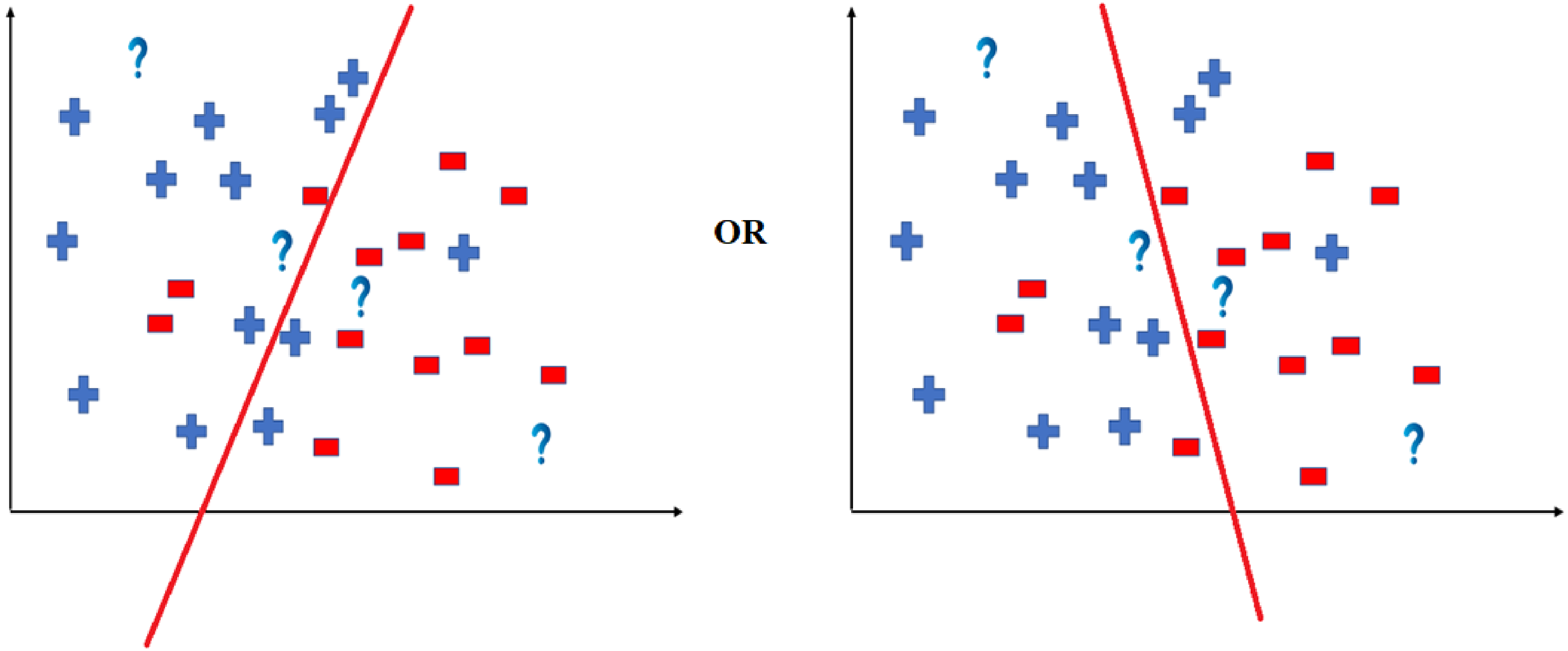
Dividing the coordinate to predict the outcomes

Hypothesis & Hypothesis Space



Result yielded

Hypothesis & Hypothesis Space

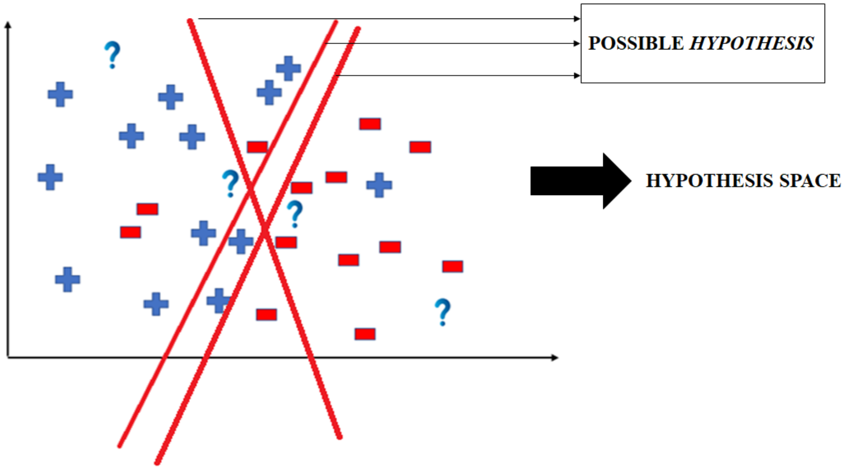


Possible Coordinate plane division

Hypothesis & Hypothesis Space

The way in which the coordinate would be divided depends on the data, algorithm and constraints.

- All these legal possible ways in which we can divide the coordinate plane to predict the outcome of the test data composes of the Hypothesis Space.
- Each individual possible way is known as the hypothesis.



Hypothesis representation in ML

Hypotheses in machine learning are formulated based on various algorithms and techniques, each with its representation. For example:

- Linear Regression: $\boldsymbol{h}(X)=\theta_0+\theta_1 X_1+\theta_2 X_2+\ldots+\theta_n X_n$
- Decision Trees: $\boldsymbol{h}(X)=\text{Tree}(X)$
- Neural Networks: $\boldsymbol{h}(X)=\text{NN}(X)$

Inductive Bias

- Inductive bias can be defined as the set of assumptions or biases that a learning algorithm employs to make predictions on unseen data based on its training data.
- These assumptions are inherent in the algorithm's design and serve as a foundation for learning and generalization.
- The inductive bias of an algorithm influences how it selects a hypothesis (a possible explanation or model) from the hypothesis space (the set of all possible hypotheses) that best fits the training data.
- It helps the algorithm navigate the trade-off between fitting the training data perfectly (overfitting) and generalizing well to unseen data (underfitting).

Types of Inductive Bias

- **Bias towards simpler explanations**:
  - Many machine learning algorithms, such as decision trees and linear models, have a bias towards simpler hypotheses. They prefer explanations that are more parsimonious and less complex, as these are often more likely to generalize well to unseen data.

Types of Inductive Bias

- **Bias towards smoother functions**:
  - Algorithms like kernel methods or Gaussian processes have a bias towards smoother functions. They assume that neighboring points in the input space should have similar outputs, leading to smooth decision boundaries.

Types of Inductive Bias

- **Bias towards specific types of functions**:
  - Neural networks, for example, have a bias towards learning complex, nonlinear functions. This bias allows them to capture intricate patterns in the data but can also lead to overfitting if not regularized properly.

Types of Inductive Bias

- **Bias towards sparsity**:
  - Some algorithms, like Lasso regression, have a bias towards sparsity. They prefer solutions where only a few features are relevant, which can improve interpretability and generalization.

Bias-Variance Tradeoff

What is bias?

- Bias is the difference between the average prediction of our model and the correct value which we are trying to predict.
- Model with high bias pays very little attention to the training data and oversimplifies the model. It always leads to high error on training and test data.

Bias-Variance Tradeoff

What is variance?

- Variance is the variability of model prediction for a given data point or a value which tells us spread of our data.
- Model with high variance pays a lot of attention to training data and does not generalize on the data which it hasn’t seen before. As a result, such models perform very well on training data but has high error rates on test data.

Bias-Variance Tradeoff

Underfitting

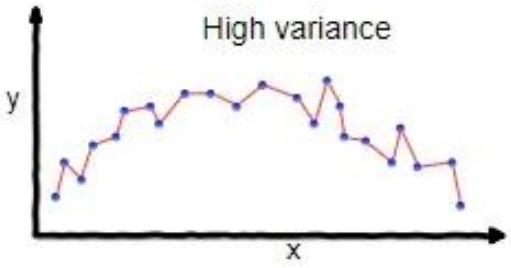
- In supervised learning, **underfitting** happens when a model unable to capture the underlying pattern of the data.
- These models usually have high bias and low variance.
- It happens when we have very less amount of data to build an accurate model or when we try to build a linear model with a nonlinear data.
- Also, these kind of models are very simple to capture the complex patterns in data like Linear and logistic regression.

Bias-Variance Tradeoff

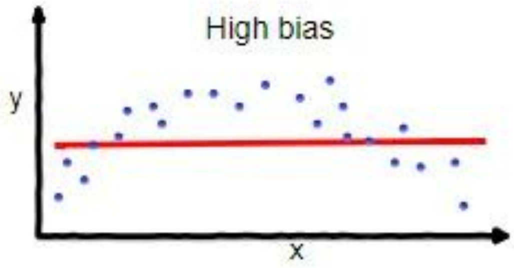
Overfitting

- In supervised learning, **overfitting** happens when our model captures the noise along with the underlying pattern in data.
- It happens when we train our model a lot over noisy dataset.
- These models have low bias and high variance.
- These models are very complex like Decision trees which are prone to overfitting.

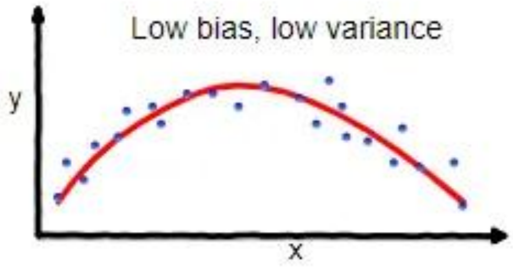
Bias-Variance Tradeoff



overfitting



underfitting



Good balance