

Machine Learning *Theory*

Christian Rossi

Academic Year 2023-2024

Abstract

The course topics are:

- Introduction: basic concepts.
- Learning theory:
 - Bias/variance tradeoff. Union and Chernoff/Hoeffding bounds.
 - VC dimension. Worst case (online) learning.
 - Practical advice on how to use learning algorithms.
- Supervised learning:
 - Supervised learning setup. LMS.
 - Logistic regression. Perceptron. Exponential family.
 - Kernel methods: Radial Basis Networks, Gaussian Processes, and Support Vector Machines.
 - Model selection and feature selection.
 - Ensemble methods: Bagging, boosting.
 - Evaluating and debugging learning algorithms.
- Reinforcement learning and control:
 - MDPs. Bellman equations.
 - Value iteration and policy iteration.
 - TD, SARSA, Q-learning.
 - Value function approximation.
 - Policy search. Reinforce. POMDPs.
 - Multi-Armed Bandit.

Contents

| | | |
|----------|----------------------------------|----------|
| 1 | Introduction | 1 |
| 1.1 | Machine learning | 1 |
| 1.1.1 | Supervised learning | 2 |
| 1.1.2 | Unsupervised learning | 2 |
| 1.1.3 | Reinforcement learning | 2 |
| 2 | Supervised learning | 4 |
| 2.1 | Introduction | 4 |
| 2.1.1 | Function approximation | 4 |
| 2.1.2 | Taxonomy | 5 |

CHAPTER 1

Introduction

1.1 Machine learning

Definition (*Learning*). A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P , improves with experience E .

Machine learning, a subset of artificial intelligence, derives knowledge from experience and induction.

In machine learning, we depend on computers to make informed decisions using new, unfamiliar data. Designing a comprehensive set of meaningful rules can prove to be exceedingly difficult. Machine learning facilitates the automatic extraction of relevant insights from historical data and effectively applies them to new datasets.

The objective is to automate the programming process for computers, acknowledging the bottleneck presented by writing software. Instead, our aim is to utilize the data itself to accomplish the required tasks.

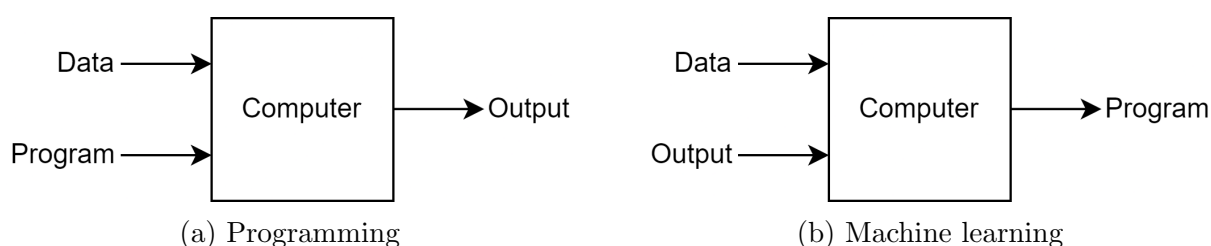


Figure 1.1: Difference between programming and machine learning

Machine learning paradigms can be categorized into three main types:

- *Supervised learning*: involves labeled data and direct feedback, aiming to predict outcomes or future events.
- *Unsupervised learning*: operates without labeled data or feedback, focusing on discovering hidden structures within the data.
- *Reinforcement learning*: centers around a decision-making process, incorporating a reward system to learn sequences of actions.

1.1.1 Supervised learning

Supervised learning encompasses several distinct tasks:

- *Classification*: this involves assigning predefined categories or labels to data points based on their features. The model is trained on labeled data, learning patterns to predict the class labels of new data points.
- *Regression*: the goal here is to predict continuous numerical values based on input features, as opposed to discrete class labels in classification. The model learns a function mapping input features to output values.
- *Probability estimation*: this task predicts the likelihood of certain events or outcomes occurring, often used to gauge the confidence of model predictions.

Formally, in supervised learning, a model learns from data to map known inputs to known outputs. The training set is denoted as $\mathcal{D} = \{\langle x, t \rangle\}$, Where $t = f(x)$, with f representing the unknown function to be determined using supervised learning techniques.

Various techniques can be employed for supervised learning, including linear models, artificial neural networks, support vector machines, and decision trees.

1.1.2 Unsupervised learning

Unsupervised learning encompasses two main tasks:

- *Clustering*: in this task, the objective is to group similar data points together based on their features, without predefined labels. The goal is to uncover underlying patterns or structures within the data. Clustering algorithms segment the data into clusters or groups, where data points within the same cluster exhibit greater similarity compared to those in different clusters. Unlike supervised learning, where labeled data is provided, clustering algorithms explore data solely based on features to identify similarities.
- *Dimensionality reduction*: this task involves reducing the number of input variables or features in a dataset while retaining essential information. This is often done to address the curse of dimensionality, enhance computational efficiency, and mitigate overfitting risks in models. Dimensionality reduction techniques aim to transform high-dimensional data into a lower-dimensional representation while preserving most relevant information.

Formally, in unsupervised learning, computers learn previously unknown patterns and efficient data representations. The training set is defined as $\mathcal{D} = \{x\}$, where the goal is to find a function f that extracts a representation or grouping of the data.

Various techniques are used for unsupervised learning, including k-means clustering, self-organizing maps, and principal component analysis.

1.1.3 Reinforcement learning

Reinforcement learning encompasses several key approaches:

- *Markov decision process*: a mathematical framework for modeling decision-making, involving states, actions, transition probabilities, and rewards. The goal is to find a policy that maximizes cumulative rewards while considering uncertainty.

- *Partially observable MDP*: an extension of MDP where the current state is uncertain and must be inferred from observations. The objective remains the same, but the agent maintains a belief over possible states based on observations.
- *Stochastic games*: models for decision-making with multiple agents, where outcomes depend on actions and random factors. Players aim to optimize strategies considering other players' actions and uncertainties.

In reinforcement learning, the computer learns the optimal policy based on a training set \mathcal{D} containing tuples $\langle x, u, x', r \rangle$, where x is the input, u is the action, x' is the resulting state after the action, and r is the reward. The policy Q^* is defined to maximize $Q^*(x, u)$ over actions u for each state x in the training set.

Various techniques such as Q-learning, SARSA, and fitted Q-iteration are used to find this optimal policy.

CHAPTER 2

Supervised learning

2.1 Introduction

Supervised learning stands as the predominant and well-established learning approach. Its core objective is to enable a computer, given a training set $\mathcal{D} = \{\langle x, t \rangle\}$, to approximate a function f that maps an input x to an output t . The input variables x , often referred to as features or attributes, are paired with output variables t , also known as targets or labels. The tasks undertaken in supervised learning are as follows:

- *Classification*: when t is discrete.
- *Regression*: when t is continuous.
- *Probability estimation*: when t represents a probability.

Supervised learning finds application in scenarios where:

- Humans lack the capability to perform the task directly (e.g., DNA analysis).
- Humans can perform the task but lack the ability to articulate the process (e.g., medical image analysis).
- The task is subject to temporal variations (e.g., stock price prediction).
- The task demands personalization (e.g., movie recommendation).

2.1.1 Function approximation

The process of approximating a function f from a dataset \mathcal{D} involves several steps:

1. *Define a loss function \mathcal{L}* : this function calculates the discrepancy between f and h , a chosen approximation.
2. *Select a hypothesis space \mathcal{H}* : this space consists of a set of candidate functions from which to choose an approximation h .
3. *Minimize \mathcal{L} within \mathcal{H}* : the goal is to find an approximation h within the hypothesis space \mathcal{H} that minimizes the loss function \mathcal{L} .

The hypothesis space \mathcal{H} can be expanded to theoretically achieve a perfect approximation of the function f . However, a significant challenge arises because the loss function \mathcal{L} cannot be easily determined, primarily due to the absence of the actual function f .

2.1.2 Taxonomy

The taxonomy is as follows:

- *Parametric* or *nonparametric*: parametric methods are characterized by having a fixed and finite number of parameters, while nonparametric methods have a number of parameters that depend on the training set.
- *Frequentist* or *Bayesian*: frequentist approaches utilize probabilities to model the sampling process, whereas Bayesian methods use probability to represent uncertainty about the estimate.
- *Empirical risk minimization* or *structural risk minimization*: empirical risk refers to the error over the training set, while structural risk involves balancing the training error with model complexity.

The type of machine learning can be:

- *Direct*: This method involves learning an approximation of f directly from the dataset \mathcal{D} .
- *Generative*: in this approach, the model focuses on modeling the conditional density $P(t|x)$ and then marginalizing to find the conditional mean:

$$\mathbb{E}[t|x] = \int t \cdot P(t|x) dt$$

- *Discriminative*: This method models the joint density $P(x, t)$, infers the conditional density $P(t|x)$, and then marginalizes to find the conditional mean:

$$\mathbb{E}[t|x] = \int t \cdot P(t|x) dt$$