Machine Learning

Chao Ren

December 20, 2025

Contents

Chapter 1

Introduction to Machine Learning

1.1 What is machine learning?

"The goal of machine learning is to develop methods that can automatically detect patterns in data, and then to use the uncovered patterns to predict future data or other outcomes of interest."

> **Definition 1** (Mitchell, 1997)**.** A computer program is said to **learn** from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E.

> **Example.** In the case of face detection, E is input data containing faces marked clearly by bounding boxes, T is identifying faces by putting boxes around them in new images, and P could be the fraction of faces correctly identified.
>
> Thus by Mitchell's definition, a computer program *learns* "face detection" if its performance improves when provided with more experience, i.e. more images with faces marked by bounding boxes.

1.2 A brief history of machine learning

Machine learning as a modern discipline grew out of several disciplines, notably statistics, computer science, and neuroscience.

1.2.1 Fisher and the Iris Dataset

Arguably one of the first instances of an automatic classification was due to statistician/biologist Ronald A. Fisher in 1936. Given data about three kinds of iris flowers, he proposed to look at a linear function of the four measurements

that best discriminates the types (Fisher Linear Discrminant Analysis). 1936 is also at least a decade before the first computers were built.

1.2.2 Rosenblatt and the Perceptron

Frank Rosenblatt constructed the Perceptron, inspired by biological principals. In ML terms, a perceptron is viewed as taking multiple inputs, and if the weighted sum of these exceeds a threshold, the output is 1, otherwise 0. Rosenblatt also designed an algorithm that would adjust the weights if on a new input the prediction was incorrect. Under certain assumptions, it can be shown this algorithm converges to the correct classifier.

> **Note.** We will return to perceptrons in the form of more general artificial neurons, where the output will be a continuous function of the weighted sum of the inputs. A "deep neural network" is simply many artificial neurons stacked together in layers.

1.3 Machine Learning Paradigms through Applications

1.3.1 Supervised Learning

The training data consists of input and output pairs. The goal of the learning algorithm is to learn a map from input to output.

> **Example.** Boston Housing Dataset. The data consists of several attributes, some numerical (area) and some categorical (whether the house is on the river). The goal is to predict the house price.
> When the output of the algorithm is a real value, it is called *regression*.

> **Example.** Imagenet Object Detection. Data consists of images with bounding boxes around objects and labels for the objects. The task it to put bounding boxes around objects in certain categories and label them.
> When the output of the algorithm is a category, this is called *classification*. In this case there are multiple categories and is referred to as *multi-class* classification. When there are two categories it is *binary* classification. In the case of detecting objects in an image, there may be several objects appearing in the same image. This is referred to as *multi-label multi-class* classification.

1.3.2 Unsupervised Learning

The training data lacks outputs. The goal is usually to find some interesting structure in the dataset.

> **Example.** Clustering Genetic Data. Novembre et al. (2008) looked at genetic data of 3000 European individuals. They find this data can be clustered remarkably well in groups corresponding to geography. The learning algorithm was only given genetic data (not nationality) and asked to detect clusters. *Clustering* is a canonical example of unsupervised learning. Another on is *dimensionality reduction*, both useful for learning and for visualization.

1.3.3 Other Paradigms

These don't neatly fit into (un)supervised learning, but are important nevertheless.

Active Learning

Task is to predict outputs corresponding to individual instances (as in supervised learning). However, initially, all data is unlabelled. The goal is to design algorithms that try to identify the most useful data which can then be labelled by humans as needed.

Semi-Supervised Learning

Goal is to design learning algorithms that make use of large quantities of unlabelled data that may often be available in conjunction with some labelled data.

Collaborative Filtering

Best explained by recommender systems. A matrix with entries containing movie ratings by users is quite sparse. The goal is to complete this matrix accurately so that useful predictions can be made to users.

Reinforcement Learning

Differs from other paradigms in the sense that there is no need for explicit inputs/outputs. A key aspect of RL-applicable settings is the sequential nature of actions that must be taken. For example when designing systems for self-driving cars or automatically flying helicopters, whether an action was a mistake may only be known several steps after the action was taken. It is hard to generate examples of correct/incorrect behaviour, but it is often possible to define a reward function. It was an integral component of the system that beat the world Go champion.

1.4 Some Practical Concerns

Before applying ML techniques, it is important that the data has a useful representation (e.g. filtering specific words from spam email rather than the raw electronic format). We will work with the assumption that the data has already been cleaned up and put in a suitable format.