

## What is Machine Learning?

A useful way to introduce the machine learning methodology is by means of a comparison with the conventional engineering design flow. 6 1.1. What is Machine Learning? 7 This starts with an in-depth analysis of the problem domain, which culminates with the definition of a mathematical model. The mathematical model is meant to capture the key features of the problem under study, and is typically the result of the work of a number of experts. The mathematical model is finally leveraged to derive hand-crafted solutions to the problem. For instance, consider the problem of defining a chemical process to produce a given molecule. The conventional flow requires chemists to leverage their knowledge of models that predict the outcome of individual chemical reactions, in order to craft a sequence of suitable steps that synthesize the desired molecule. Another example is the design of speech translation or image/video compression algorithms. Both of these tasks involve the definition of models and algorithms by teams of experts, such as linguists, psychologists, and signal processing practitioners, not infrequently during the course of long standardization meetings. The engineering design flow outlined above may be too costly and inefficient for problems in which faster or less expensive solutions are desirable. The machine learning alternative is to collect large data sets, e.g., of labelled speech, images or videos, and to use this information to train general-purpose learning machines to carry out the desired task. While the standard engineering flow relies on domain knowledge and on design optimized for the problem at hand, machine learning lets large amounts of data dictate algorithms and solutions. To this end, rather than requiring a precise model of the set-up under study, machine learning requires the specification of an objective, of a model to be trained, and of an optimization technique. Returning to the first example above, a machine learning approach would proceed by training a general-purpose machine to predict the outcome of known chemical reactions based on a large data set, and by then using the trained algorithm to explore ways to produce more complex molecules. In a similar manner, large data sets of images or videos would be used to train a general-purpose algorithm with the aim of obtaining compressed representations from which the original input can be recovered with some distortion. 8 Introduction 1.2

## When to Use Machine Learning?

Based on the discussion above, machine learning can offer an efficient alternative to the conventional engineering flow when development cost and time are the main concerns, or when the problem appears to be too complex to be studied in its full generality. On the flip side, the approach has the key disadvantages of providing generally suboptimal performance, or hindering interpretability of the solution, and to apply only to a limited set of problems. In order to identify tasks for which machine learning methods may be useful, reference [31] suggests the following criteria: 1. the task involves a function that maps well-defined inputs to well-defined outputs; 2. large data sets exist or can be created containing input-output pairs; 3. the task provides clear feedback with clearly definable goals and metrics; 4. the task does not involve long chains of logic or reasoning that depend on diverse background knowledge or common sense; 5. the task does not require detailed explanations for how the decision was made; 6. the task has a tolerance for error and no need for provably correct or optimal solutions; 7. the phenomenon or function being learned should not change rapidly over time; and 8. no specialized dexterity, physical skills, or mobility is required. These criteria are useful guidelines for the decision of whether machine learning methods are suitable for a given task of interest. They also offer a convenient demarcation line between machine learning as is intended today, with its focus on training and computational statistics tools, and more general notions of

Artificial Intelligence (AI) based on knowledge and common sense [87] (see [126] for an overview on AI research)

**Learning Tasks** We can distinguish among three different main types of machine learning problems, which are briefly introduced below. The discussion reflects the focus of this monograph on parametric probabilistic models, as further elaborated on in the next section.

1. **Supervised learning:** We have  $N$  labelled training examples  $D = \{(x_n, t_n)\}_{n=1}^N$ , where  $x_n$  represents a covariate, or explanatory variable, while  $t_n$  is the corresponding label, or response. For instance, variable  $x_n$  may represent the text of an email, while the label  $t_n$  may be a binary variable indicating whether the email is spam or not. The goal of supervised learning is to predict the value of the label  $t$  for an input  $x$  that is not in the training set. In other words, supervised learning aims at generalizing the observations in the data set  $D$  to new inputs. For example, an algorithm trained on a set of emails should be able to classify a new email not present in the data set  $D$ . We can generally distinguish between classification problems, in which the label  $t$  is discrete, as in the example above, and regression problems, in which variable  $t$  is continuous. An example of a regression task is the prediction of tomorrow's temperature  $t$  based on today's meteorological observations  $x$ . An effective way to learn a predictor is to identify from the data set  $D$  a predictive distribution  $p(t|x)$  from a set of parametrized distributions. The conditional distribution  $p(t|x)$  defines a profile of beliefs over all possible of the label  $t$  given the input  $x$ . For instance, for temperature prediction, one could learn mean and variance of a Gaussian distribution  $p(t|x)$  as a function of the input  $x$ . As a special case, the output of a supervised learning algorithm may be in the form of a deterministic predictive function  $t = \hat{t}(x)$ .

2. **Unsupervised learning:** Suppose now that we have an unlabelled set of training examples  $D = \{x_n\}_{n=1}^N$ . Less well defined than supervised learning, unsupervised learning generally refers to the task of learning properties of the mechanism that generates this data set. Specific tasks and applications include clustering, which is the problem of grouping similar examples  $x_n$ ; dimensionality reduction, feature extraction, and representation learning, all related to the problem of representing the data in a smaller or more convenient space; and generative modelling, which is the problem of learning a generating mechanism to produce artificial examples that are similar to available data in the data set  $D$ . As a generalization of both supervised and unsupervised learning, semi-supervised learning refers to scenarios in which not all examples are labelled, with the unlabelled examples providing information about the distribution of the covariates  $x$ .

3. **Reinforcement learning:** Reinforcement learning refers to the problem of inferring optimal sequential decisions based on rewards or punishments received as a result of previous actions. Under supervised learning, the "label"  $t$  refers to an action to be taken when the learner is in an informational state about the environment given by a variable  $x$ . Upon taking an action  $t$  in a state  $x$ , the learner is provided with feedback on the immediate reward accrued via this decision, and the environment moves on to a different state. As an example, an agent can be trained to navigate a given environment in the presence of obstacles by penalizing decisions that result in collisions. Reinforcement learning is hence neither supervised, since the learner is not provided with the optimal actions  $t$  to select in a given state  $x$ ; nor is it fully unsupervised, given the availability of feedback on the quality of the chosen action. Reinforcement learning is also distinguished from supervised and unsupervised learning due to the influence of previous actions on future states and rewards. This monograph focuses on supervised and unsupervised learning. These general tasks can be further classified along the following dimensions.

- **Passive vs. active learning:** A passive learner is given the training examples, while an active learner can affect the choice of training examples

on the basis of prior observations. • Offline vs. online learning: Offline learning operates over a batch of training samples, while online learning processes samples in a streaming fashion. Note that reinforcement learning operates inherently in an online manner, while supervised and unsupervised learning can be carried out by following either offline or online formulations. 1.3. Goals and Outline 11 This monograph considers only passive and offline learning.