In this chapter, we give a general introduction to image classification, which is one of the basic machine learning problems and we also discuss some popular datasets: MNIST, CIFAR and ImageNet.

Introduction to machine learning Machine learning, a subset of the field of artificial intelligence (AI), is a field that uses the algorithms to explore the underlying patterns in the data. It is an interdisciplinary field involving many majors such as mathematics, statistics and computer science.

Mitchell mitchell1997machine gives a formal definition of learning "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." Here the experience E, task T and performance measure P can be chosen from a broad range.

The machine learning algorithms can be broadly categorized into three divisions based on the approach, the data type and the task to be solved: supervised learning algorithms, unsupervised learning algorithms and reinforcement learning algorithms. We will focus on the supervised learning algorithms here.

A typical supervised machine learning task consists of the dataset, the model and the learning algorithm. The data can be selected from a wide variety like digits, pictures, words, etc. The dataset includes the training set, validation set and test set. For the clarification problem, we call the dataset involved in training the model the training set, the dataset used for selecting the optimal model the validation set and the dataset to be applied with the optimal model to measure the corresponding generalization ability the test set. The data is used to help the algorithm to build a mathematical model to extract the patterns or learn the experience. This process is called training the model. The main task of the model is to extract the features and characteristics from the training set for learning and generalize it to the previously unseen test set for inferring. The generalization ability is defined as the performance of the model when making inferences on the previously unseen data.

Supervised learning algorithms try to build a mathematical model of a set of data that contains both the inputs and the desired outputs russell2010artificial. The inputs, which are also called the predictors or the independent variables, are used to predict the values of the outputs, which are also called the responses, the labels or the dependent variables friedman2001elements. If the the range of the outputs is categorical or has finite numbers, the supervised learning algorithm is used for classification. If there are infinite many numbers in the the range of the outputs, the supervised learning algorithm is used for regression.

The no free lunch theorem wolpert1996lack for machine learning states that, averaged over all possible data generating distributions, every classification algorithm has the same error rate when classifying previously unseen examples. It means no machine learning algorithm is universally any better than any other in some sense goodfellow2016deep. Therefore we need to select the optimal algorithm based on the specific problem, dataset and task since no model dominates all the time.

There are many classic supervised learning algorithms that are widely used in various fields. For example, linear regression, logistic regression, support vector machine (SVM), K nearest neighbor (KNN) and so on. For these supervised learning algorithms, the procedure includes 6 steps to be performed praveena2017literature. enumerate

- T he type of data to be used as the training set needs to be determined by the people. For instance, the data can be an image, a word or a vector.
- C ollect a training set and test set representative of the real-world use of the model.
- R esolve the input feature representation of the learned model. For example, the input obtained from measurements can be transformed to a feature vector while an image can be transformed to a matrix.
- C hoose the structure of the learned model and the corresponding learning algorithm. This is to determine which model to use and how to optimize the model.
- F inish the experiment design and execute the learning algorithm on the training set.
- E valuate the accuracy of the learned model on the test set.