Machine Learning Overview

MInDS @ Mines

Machine learning is a subset of Artificial Intelligence that focuses on learning rules from data. Machine learning has three primary types; supervised learning, unsupervised learning and reinforcement learning. An approach to applying machine learning that can be effective is deep learning. Deep learning uses neural networks to solve machine learning problems. In this document, we will give an overview of all the above.

Artificial Intelligence

Intelligence is anything that can think rationally; making decisions, predictions and detecting patterns. Artificial Intelligence (AI) [1] is the field of studying man-made intelligence. An entity is intelligent if we perceive it to act rationally, it does not need to have an actual understanding of why it acts the way it does. There are three main approaches to AI development that can be effective:

[1] a16z has provided a video primer on AI winters and the current state of AI

- Search and optimization

Determine the complete solution space to a problem, then enumerate over the possibilities that can occur to find the values that perform the best.

- Logic

Propositional logic and first-order logic can model a problem. When presented with a new problem using the same logic statement structures, the developed model can then determine if the problem statement aligns with the original model.

- Machine Learning

Machine learning uses data, and sometimes an answer to a question, to determine the underlying rules that result in an answer.

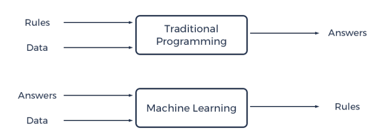


Figure 1: Machine learning flow diagram

Machine Learning

Machine learning uses a variety of approaches to learn underlying rules that govern data or systems. Many of these approaches involve statistics and so some often refer to the same field as statistical learning. In general, machine learning is the learning of a model that can accurately represent the reality it models.

Machine learning consists of three primary types:

- Supervised Learning (SL)

SL determines a model that can take an input set of features and predict a label for these features. We do so by training the model given a set of inputs with predetermined labels and learning the rules that result in that label. If the label to predict is a continuous value, then the problem is a *regression* problem. If the label to predict is a discrete value then the problem is a *classification* problem.

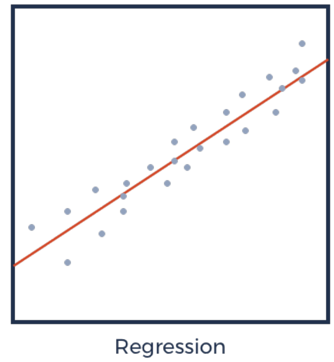


Figure 2: Example of regression

- **Unsupervised Learning** (UL)

UL does not use predetermined labels and instead detects patterns in data.

Patterns include finding similarities between some data points and differences with others. A simple example of unsupervised learning is clustering.

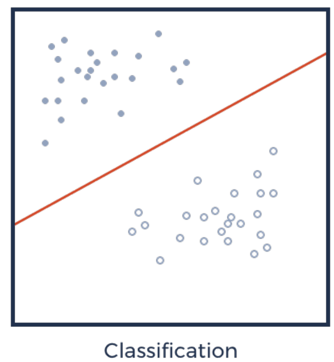


Figure 3: Example of classification

- **Reinforcement Learning** (RL)

RL trains a model to make decisions based on a reward or punishment. RL algorithms model as much as possible of the real world scenario and run a large number of simulations to account for variations to learn the appropriate decisions.

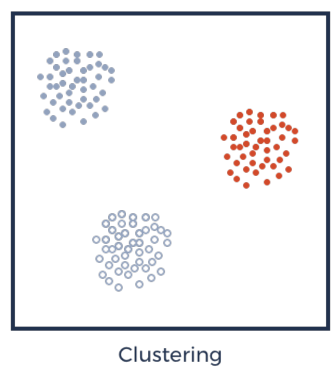


Figure 4: Example of clustering

Other popular types / subsets

1. **Semi-supervised learning** - When we have a small subset of data with labels and the remaining subset unlabeled, and train a model to predict labels.
2. **Multi-Label Learning** - SL where we have more than one target label to predict. Eg. Labeling all the objects in an image.
3. **Multi-View or Multi-Modal Learning** - Data representing an entity can come in different formats each presenting a potentially different perspective. Eg. brain image of a patient and genetic data of the patient can both represent the patient.
4. **Multi-Instance Learning** - Data contain pieces, called instances, that make up the whole data record. Eg. image made up of patches, each containing a desired item to identify.
5. **Zero Shot Learning** - SL where the model can classify an item as none of the classes that it trained on. Eg. training on images of cats and dogs and being able to tell that an image of a horse is neither of those.
6. **Transfer Learning** - Transfer learning is the study of problems where the distribution of training data and testing data are different. An example is when training a translation model on 2 languages but using it on a third language. Languages usually have different ways of expressing similar ideas.
7. **Active Learning** - Active learning is where a learning algorithm is able to interact with a user to obtain desired outputs for new data. In traditional engineering fields, it is also called experimental design.

Figure 5: Training process for reinforcement learning

Data representations

In all the different types of machine learning and AI, we can use different data representation for real world objects. We often also summarize our data so that we can effectively process it or have a more concise representation. This is to minimize any redundancy represented by two or more features. *Dimensionality reduction* is the field that studies this data summarization. When we represent data, each attribute of the data is a *dimension* or *feature*. Dimensionality reduction reduces the number of dimensions in data to achieve certain learning goals such as minimizing information loss.

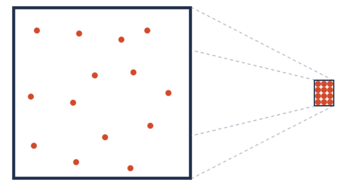


Figure 6: Illustration of dimensionality reduction

Deep Learning

Deep learning is the subset of machine learning that uses deep neural networks to solve machine learning problems. Deep learning is a set of tools that we can use to solve problems, it does not define a problem type.

A neural network (NN) is a graph or network made up of perceptrons or neurons organized in layers.

Each perceptron takes n inputs of data, combines them with allocated weights to each feature to create a weighted sum that gets passed to an *activation function* to produce an output. A feed forward neural network (FFNN) is one where the flow of data between perceptrons does not create a cycle. Layers organize the structure of a neural network; perceptrons on the same layer are not connected to each other, receive inputs from a previous layer, and output to the next in a FFNN. A deep neural network is a network that has a large number of layers between the input and output. Layers between the input and output are *hidden layers*.

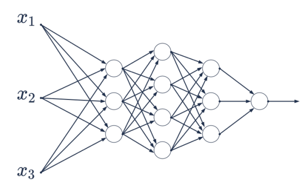
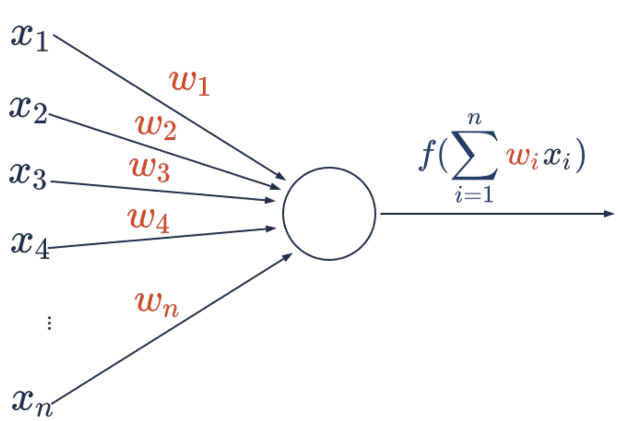


Figure 7: A neural network with hidden layers.

Figure 8: How a perceptron works.



Modifications to the simple feed forward neural network described above allow for specialized uses. This course will cover some popular variations on neural networks: [2]

[2] The neural network zoo covers a larger amount of neural networks and provides links to their original papers.

- **Convolutional Neural Nets** (CNNs)

CNNs work by encoding features into a lower dimension that is the input to a feed forward neural network or neural network of another type.

- **Recurrent Neural Nets** (RNNs)

RNNs can have cycles in the data flow between perceptrons. A popular example of RNNs is Long-Short Term Memory networks (LSTMs).

- **Generative Adversarial Networks** (GANs)

GANs work by creating two competing models; a *generator* or forger and a *discriminator* or detective. The end result is a model that can create fake data that is difficult to identify as fake and a model that can identify fakes.

Applications

Experts are applying machine learning models to almost every field. Common application areas of machine learning include:

- **Computer Vision** (CV)

We can use a matrix to represent an image where each pixel has a value for its color. Using this matrix representation, we can apply machine learning models. We can also lower the dimensionality of the image to be more manageable for high resolution images. When using images, CNNs are effective at compressing the data before performing the machine learning task.

- **Natural Language Processing** (NLP)

For text, we can use a term frequency matrix to represent a set of documents. Each feature represents a specific word, each sample represents one document, and each value represents the number of times that word appears in the document. We can also use learned embeddings to better represent text based on the relationships between the words in the documents. Both these approaches can work well with machine learning methods, the result is a vector representation for each document. For NLP, RNNs are effective because they interact with relationships between words based on the order in which they appear. This approach simulates understanding context in content.

- **Bioinformatics**

- **Medical Image Computing**