1. Introduction to Artificial Intelligence

1.1 Artificial Intelligence (AI)

Artificial intelligence is the intelligence acquired by a machine to solve problems usually solved by humans.

IBM Watson, MS Cortana, Apple Siri, Autonomous Vehicles are some of the examples of a large number of existing well-known AI applications.

1.1.1 Definition of Artificial Intelligence (AI)

AI is an art of creating machines that perform functions that require intelligence when performed by people. [KUR]Al is playing a leading role in healthcare, manufacturing, e-commerce, retail, social Media, logistics and other industry sectors. Some of the reasons for increasing use of AI are the rise in the processing power, availability of data, and new technologies. AI use cases span from monitoring one's home, determining which stock to invest in, helping to decide which recipe to make to helping in choosing your life partner!

AI is an umbrella term which covers the science of making machines intelligent, whether it is a robot, a refrigerator, a television, a car, a firmware or a software component. ML is the subset of AI. ML and AI are often used interchangeably, but they are not the same thing.

ML is explained in more details in 1.2 Machine Learning (ML)

1.1.2 Types of AI

AI can broadly be categorized as Narrow, General or Super AI.

● Narrow AI: Machines that are programmed for carrying out a specific task with limited context. For example, game playing machines, voice assistants and all AI currently.

● General AI: Machines with general cognitive abilities are popularly called as Strong AI cases. These AIs can reason and understand their environment as humans do, and act accordingly. For instance, common- sense reasoning. Currently, General AI has not been realized and nobody knows when or if it will become a reality at all.

● Super AI: Machines that are capable of replicating human thoughts, ideas and emotions. It is that super state of intelligence where machines will become smarter and wiser than humans. Considering the current state of AI developments, Super AI will not become a reality anytime soon.

1.2 Machine Learning (ML)

1.2.1 Definition of ML

Arthur Samuel defined ML as, “A field of study that gives computers the ability to learn without being explicitly programmed.” ML systems learn and improve with experience, and, with time, refine a model that can be used to predict the outcome of questions, based on the previous learning [JB1].

Beyond ML, AI uses concepts of knowledge representation and reasoning for handling diverse scenarios. Notion of searching, scheduling and optimizing fall under the scope of AI, but not necessarily ML.

Some of the technologies used to accomplish AI are:

- Machine Learning (ML)
- Natural Language Processing (NLP)
- Robotics
- Speech Processing
- Computer Vision

There are a few ways in which ML algorithms can be categorized:

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

1.2.2 Supervised Learning - Classification and Regression

Supervised Learning: In this kind of learning, the model learns from labeled data during the training phase. The labeled data acts as a trainer/supervisor for the mapping function which infers the relationship between input data and the output label during the training. During the testing phase, the mapping function is then applied to a new set of unseen data to predict the output which is also labeled. The model is deployed once the output accuracy level is satisfactory.

Problems solved by Supervised Learning are further divided into two categories:

Classification: When the problem requires classifying an input into one of a few pre-decided classes, supervised learning is used. This kind of model is used when the output data is discrete or when the output falls among the number of classes fed during training. Face recognition or object detection in an image are examples of problems that can use classification. Some other applications of classification are spam detection (spam or no spam), the diagnosis of a disease on the basis of the likes of an X-ray, correct identification of road signs by a driver assistance system, etc. Some of the

commonly used algorithms for classification are logistic regression, nearest neighbor, support vector machine, and neural nets.

Regression: When the output data is continuous or numeric in nature, e.g., predicting the age/weight of a person, predicting the future price of the stock, etc., regression learning is used. The most commonly used algorithm for this kind of problems is linear regression, a simple algorithm which explains the relation between inputs and the output and inputs as a linear equation. Some other algorithms are logistic regression, support vector machines, Lasso regression, etc.

1.2.3 Unsupervised Learning – Clustering and Association

Unsupervised Learning: Clean, labeled data are not readily available all the time, so that certain problems need to be solved without an explicitly labeled training set. This kind of ML where no labeled data is provided explicitly is called Unsupervised Learning. The objective in such problems is to learn the pattern and structure of input data without any associated labels.

Unsupervised Learning is further classified in the following two methods, based on the type of outputs:

Clustering: This Unsupervised Learning model groups the input data based on some common characteristics or attributes. Input data with similar attributes (not labeled) are grouped in one cluster. Thus, the outputs are clusters of input data. For instance, customer segmentation in market analysis.

Association: Association Rule Mining finds interesting relationships or dependencies among the data attributes. The discovery of interesting associations provides a source of information often used for decision making.

For example, market-basket data analysis, product recommendation system based on learnings derived from customer shopping behavior are good examples of association rule-based modeling.

1.2.4 Reinforcement Learning

It is a type of ML where an agent (algorithm) learns by interacting with the environment in an iterative manner and thereby learns from experience. The agent is rewarded when it makes a right decision and penalized when it makes a wrong one. This reward and penalty-based learning is thus defined as ‘reinforcement learning’ (RL). Setting up the proper environment, choosing the right strategy for the agent to meet the desired goal, and designing a reward function, are some of the key challenges in implementing RL. Robotics, Autonomous Vehicles, and Chatbots are examples of applications that can use RL.

1.3 Deep Learning (DL)

1.3.1 Deep Learning and the Types of Neural Networks

Deep Learning (DL) refers to the systems gaining experience from massive data sets. DL uses Artificial Neural Networks (ANN) to analyze large data sets, e.g. Autonomous Vehicles, Large Text Processing, and Computer Vision applications among others. DL is a subset of ML and ML is a subset of AI. DL uses the same types of learning (Supervised, Unsupervised and Reinforcement Learning) as ML.

Artificial Neural Networks: Artificial Neural Networks (ANN) are inspired by the architecture of the human brain. 'Neurons', as the basic unit of ANN, act upon the input stimulus and produce the output signal. The input goes through the layers of activation functions to generate the output. These layers form a mesh like network. Every ANN has at least two layers – input and output layers. All the layers between these two layers are called hidden layers. Some of the various types of neural networks are:

Deep Neural Network (DNN): Deep Neural Network (DNN) is an ANN with two or more hidden layers.

Convolutional Neural Network (CNN): Convolutional Neural Network (CNN) is an ANN that emerged from the study of the brain's visual cortex, and they have been used in image recognition since the 1980s. Unlike other neural networks, CNNs work directly on input images without serializing/ vectorizing an input image and extracting features by filters. CNNs power image search services, autonomous vehicles, automatic video classification systems, and more.

Recurrent Neural Network (RNN): These ANNs can predict the future of time series problems. They follow a sequential approach on series of input data of arbitrary length rather than inputs of fixed length as in other neural networks. Each input and output are independent of all the other layers. The feedback from the output layer is fed to the same network recurrently, till the right level of confidence is achieved. RNNs can analyze time series data such as stock prices, and tell you when to buy or sell. In autonomous vehicles, they can anticipate trajectories and help avoid accidents.

1.4 Stages of the ML Process

A typical ML project follows all the stages of the Cross Industry Standard Process for the Data Mining (CRISP-DM) framework – an industry standard, and a flexible framework.

1.4.1 Stages of the ML Process – CRISP-DM Process

CRISP-DM has traditionally six stages in the data mining life cycle. It has been customized to meet the requirements of ML projects, by adding a seventh stage.

The seven stages of the CRISP-DM framework for ML are: [DSC1] [SMU]

1. Data acquisition: Gather data from all internal and external sources (for example databases, CSV files, social media, etc.)

2. Data preparation: Clean the raw data and reshape it. New attributes are created with feature engineering, a process for creating new variables from existing data. Dimensionality reduction, data imputation, null value treatment for the missing values, etc., are some of the methods involved in data preparation.

3. Modeling: Select the model or algorithm, divide the available data into training set and testing set. Models are obtained by executing ML algorithms on the training data set. Use the testing data set to evaluate and enhance the performance of the model until satisfactory performance is achieved.

4. Evaluation: Evaluate the model on various metrics (discussed in 3.2 Metrics) and baseline it before it goes for final deployment.

5. Deployment: Deploy and monitor the baselined model for metrics in the production environment.

6. Operations: Carry out regular maintenance and operations. Regenerate and refine the model when the metrics fall below a certain threshold.

7. Optimization: The deployed solution may be replaced due to concept drift (see 6.1.3 Risk of Concept Drift (CD)), as better algorithms become available, or because of some major failures in performance.

Steps 1-4 can be classified as part of the offline phase, the output of which is the trained model. Steps 5-6 are a part of the online phase, where the model trained in the offline phase is integrated with the rest of the system and deployed in a production environment. The optimization step involves re-execution of steps 1-6.

1.4.2 Steps for the Identification of the ML Problem Type

It is important to understand the problems that we are trying to solve and the type of learning required to solve those problems. One way we can identify the ML problem type is discussed below:

1. If the problem involves the notion of multiple states, and involves moves at each state, then explore RL.
2. If there is an output variable it is supervised learning.
    2.1. In the case that the output is discrete and categorical, it is a classification problem.
    2.2. In the case that the output is numeric and continuous in nature, then it is a regression problem
3. If the output is not provided in the given data set, then explore the unsupervised learning.
    3.1. If the problem involves grouping similar data, then it is a clustering problem.
    3.2. If the problem involves finding co-occurring data items, then apply association rule mining
    3.3. If the raw data is unstructured, extracting features automatically can be explored with deep learning algorithms.

The prerequisite to the above steps is that there should be enough data available for the analysis of the appropriate ML problem type.