CHAPTER 8

Machine Learning

In earlier chapters, we discussed aspects of computer architecture and how to efficiently program and deploy software. Thus far, we've been successful getting computers to carry out what they have been programmed to accomplish. Beyond traditional programming, questions arise about whether or not computers can mimic humans in terms of intelligence and learning. In science fiction literature, there are many stories of machines taking over the world. Is this possible? Until relatively recently, these fictions have been given little credence because there are fundamental differences between how human intelligence and computing machines work. Machines act as obedient servants – working as they are explicitly programmed to accomplish a well-defined task. They did not learn and improve or develop intelligence. And that's where machine learning comes to play. Some of the most succinct descriptions of machine learning are from Stanford and McKinsey & Co. As per Stanford, "Machine learning is the science of getting computers to act without being explicitly programmed."[1] And, as per McKinsey & Co, "Machine learning is based on algorithms that can learn from data without relying on rules-based programming."[2]

[1]Andrew Ng, http://mlclass.stanford.edu/#:~:text=Machine%20learning%20is%20the%20science,understanding%20of%20the%20human%20genome.

[2]Jacques Bughin et al., "Artificial Intelligence the Next Digital Frontier?" McKinsey Global Institute, June 2017, www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.pdf.

P. D. Crutcher et al., *Essential Computer Science*,
https://doi.org/10.1007/978-1-4842-7107-0_8

Note Fundamentally, machine learning is the science of getting computers to learn as well as, or better than, humans.

The key difference between machine learning and conventional machine intelligence is the way machines acquire intelligence. With machine learning, machines gather intelligence based on examples (data, aka experience). In the conventional machine intelligence case, machines are explicitly programmed (instructed) to behave in a certain intelligent way. So machines may still behave like intelligent agents without applying machine learning, but they do not get better with experience.

By the way, machine learning is not a completely new thing; it has evolved and started to see more usage, proliferation, and success owing to advancement in compute resource and availability of data. In the following section, we talk about evolution of machine learning.

Brief History of Machine Learning

From the very beginning of computing devices, when we thought about learning and machines, we tried to draw parallels from the understanding of how human brains work and how computing machines/algorithms work. Neurons and their associated networks (neural networks) play the foundational role in human learning process, so researchers have tried to emulate these processes in machines. This field of study is broadly known as machine learning and artificial intelligence.

The first theory on neural networks was a paper published in 1943 where neurophysiologist Warren McCulloch and mathematician Walter Pitts talked about neurons and how they work. They decided to model these neurons using an electrical circuit, creating the underlying framework for future machine learning progress.

In 1950, Alan Turing created the "Turing Test," which is a method for determining whether a computer is capable of thinking like a human being. Turing proposed that a computer can be said to possess artificial intelligence if it can mimic human responses under specific conditions. This test is simple: for a computer to qualify as having artificial intelligence, it must be able to convince a human that it is a human and not a computer. The test was originally named "The Imitation Game."

Arthur Samuel in 1952 created the first computer program that could learn as it ran. It was a game that played checkers. Later in 1958, Frank Rosenblatt designed the first artificial neural network to recognize patterns and shapes. Then in 1959, Bernard Widrow and Marcian Hoff created two neural network models at Stanford University. The first was called ADALINE, and it could detect binary patterns. The other one (which was the next generation) was called MADALINE. MADALINE was used to eliminate echo on phone lines – so the first useful real-world application of machine learning, MADALINE, came into use and continues to be used today.

Despite the success of MADALINE, there was not much progress until the late 1970s for many reasons. Recently, both the amount of data available and exponential growth in processing capabilities, neural networks, and other ML technologies have become viable.

Artificial Intelligence, Machine Learning, and Deep Learning

We use the terms artificial intelligence, machine learning, and deep learning a lot. Is there a difference between them? At times, we seem to use these terms interchangeably, but it is important to understand that they are related and not interchangeable. We define each one in the following.

Artificial intelligence (AI) refers to intelligence demonstrated by machines. In other words, artificial intelligence refers to the simulation of intelligent behavior in computers or the capability of a machine to imitate intelligent human behavior. It is used broadly to refer to any algorithms, methods, or technologies that make a system act and behave like a human. It employs machine learning, computer vision, natural language processing, cognitive robotics, and other related technologies.

Machine learning is a subfield of artificial intelligence that uses algorithms that improve with experience or learn the rules without explicitly being programmed.

Deep learning is a technique of machine learning that uses multilevel (deep) neural networks for learning. Figure 8-1 represents the relationship between the three. It illustrates that deep learning is a subfield of machine learning that is a subfield of artificial intelligence.

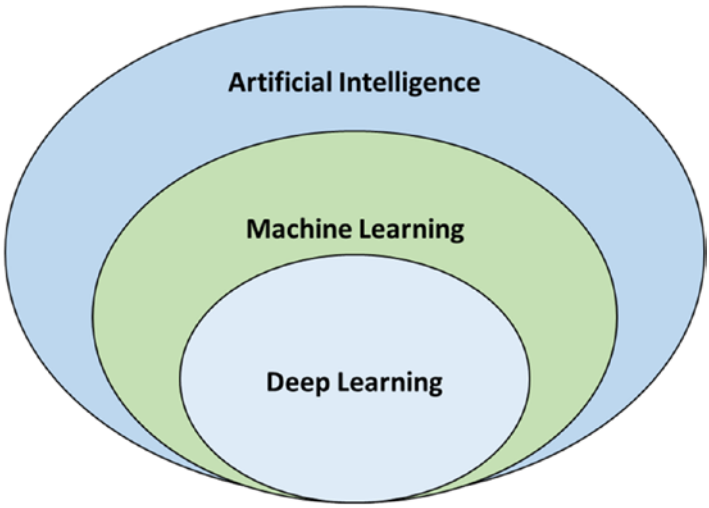

Figure 8-1. *Relationship Between Artificial Intelligence, Machine Learning, and Deep Learning*

Fundamental Tenets of Machine Learning

Having discussed machine learning and its evolution earlier, we now discuss the key tenets of machine learning. In machine learning, machines learn with data to detect patterns and rules to

- Categorize like objects.
- Predict likely outcomes based on identified (learned) rules.
- Identify patterns and relationships.
- Detect anomalous behaviors.

Essentially there are three parts of a machine learning system: model, training, and inference. Figure 8-2 illustrates the high-level flow. At first, a machine learning model is created, and then it is trained with the training data. After training, the model would have "learned," based on the data, and is ready to be used for making useful prediction for new data, which

is known as inference. It is worth mentioning that a large volume of data is required for the model to pick good rules and become reasonably accurate. In practice, the training of the model is a continuous process, bringing in new training data as we see more kinds of data from the real world, making the model predictions more accurate over time. Because of the iterations and amount of data that need to be processed, the training process is computationally intensive. The degree of computational requirement depends on the model (algorithm) being used and the size of the training database. The good news here is that once a model is trained, making an inference based on new data is fairly low cost.

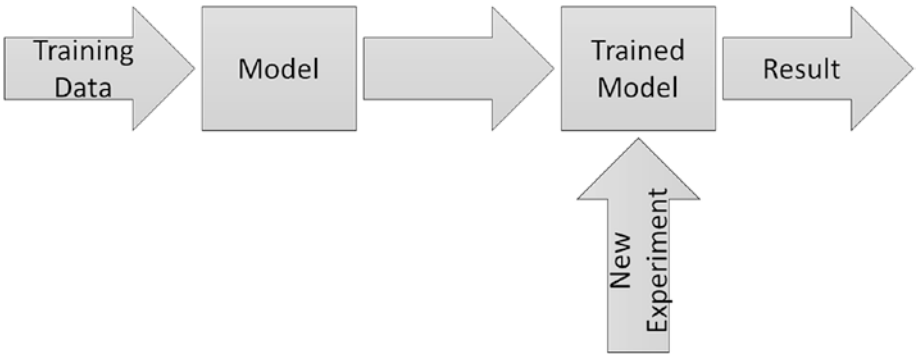

Figure 8-2. *Representation of a Machine Learning System*

Models

A machine learning (ML) model is fundamentally a recipe (i.e., statistical representation of the system) learned using examples (i.e., training data) with an ability to predict behavior given new data. In other words, a machine learning model is fundamentally the representation of a learning system that can be used to predict (i.e., infer) results for new data.

The processes machines use to learn are known as algorithms. Different algorithms learn in different ways. With the right model, as new

data is provided to the "machine," the algorithm's performance improves, thereby resulting in increasing "intelligence" over time.

Training

Training refers to the model being fed with the data such that it learns the rules or improves the model. The structure of the data will be different depending upon the type of machine learning and the chosen model. Data points are generally represented as a feature vector, or feature. Each feature represents one attribute of the data. A vector is just like an array data structure, discussed previously.

So, taking an example, let's say we are designing a machine learning system to predict the price of a car in resale. The actual prices of cars sold previously, along with the descriptions of cars, will be fed to the learning model. The car description will have multiple attributes (features) like maker of the car, age of the car, the distance the car has been driven, and so on. Each of these features can be represented using one of the following types of data:

1. Categorical Data: Data that takes one of the few values in a set, for example, color of a car
2. Binary Data: Data that has two values, for example, whether a car has valid insurance or not
3. Numerical Data: Data that is a number, for example, price of a car
4. Graphical Data: Data that is in graphical form, for example, picture of a car

As part of the training process, we usually divide the available data for training into parts: one part used for training and learning and the other part used for validation/checking accuracy of the model. Given a trained model, we're ready for inference. As mentioned in the preceding, we're

never really done training, as we need to constantly update our training data set to accurately reflect the real-world data we encounter using the model.

Prediction (Inference)

Now, once the model is ready and trained, the "trained model" is used for "prediction" or more formally "inference" with new data. The model is fed the new data and predicts the "result/output" for the same. From the computation resource perspective, inference is much faster than training because it can be done in real time or near real time in many cases.

Categories of Machine learning

In the context of machine learning, there are some well-known categories of learning problems. The key ones are (1) supervised, (2) unsupervised, (3) semi-supervised, and (4) reinforcement learning.

Supervised Learning

We know that in machine learning, we feed data to a model and the model learns using the data. In the case of supervised learning, the data is labeled with the right answer (we know what is good and what is bad, if you will). So, essentially, the model is being supervised while training. Another way to look at it is a person curating the data and creating the (good/bad) labels, essentially supervising the model. Supervised learning models the relationship between the output and the input data such that it can predict the output values for new data based on the derived (learned) relationships from the previous data sets. In other words, supervised learning can be considered a form of function approximation. Supervised learning is the most common machine learning technique applied in real-life use cases.

One example is when we are creating a spam detector engine. The model is fed with the description of the message along with the label (spam or "not a spam"). The learning is anchored around the label that is the correct answer (as per the supervisor). There are two major subcategories of supervised learning:

1. Regression: The simplest form of regression is linear regression where we attempt to fit a straight line to a given set of data. In more complex regression systems, the predicted value (output) will fall within a continuous spectrum (it won't be a binary value like true or false). An example of a regression system is a car/house price predictor that will be used to predict the price of a given car/house based on the description of the same.
2. Classification: In a classification system, the prediction falls in one of a few classes (also referred to as groupings or clusters). An example of a classification system would be a spam detector that will classify whether or not a given message is spam.

In supervised learning, there are many algorithms that can be used, some of the most common ones being

- Linear regression
- Logistic regression
- Nearest neighbor
- Naïve Bayes
- Decision trees
- Support vector machines

Unsupervised Learning

In contrast to supervised learning, with unsupervised learning, the model studies data to identify clusters, segmentation, and patterns. In this case, the data fed to the learning model is unlabeled. Essentially, that means there is no right or wrong answer key to the data set. The machine determines correlations and relationships by learning from the available data. This is pretty easy to do visually in two or even three dimensions, but as you can imagine, it is not intuitive with more dimensions, where each feature is a new dimension. A couple of applications of unsupervised learning are anomaly detection and categorizing similar objects. Again, there are many algorithms that can be used for unsupervised learning; however, the most common ones are

- K-means clustering
- Association rules

Semi-supervised Learning

Semi-supervised learning is used to address similar problems as supervised learning. It combines the techniques from both supervised and unsupervised learning. In semi-supervised learning, the machine is provided some labeled data, along with additional data that is not labeled. Typical use cases will be image and speech analysis, web content classification, protein sequence classification, and so on.

Reinforcement Learning

A reinforcement learning algorithm continuously learns from the environment in an iterative fashion. In the process, the model learns from the experiences of the environment. In other words, in reinforcement learning, the model is provided a set of allowed actions, rules, and

potential outcomes (rewards). Essentially, the rules of the game are defined. The model then applies the rules and takes one of many possible actions and earns a reward. Based on the reward (outcome), the model determines what series of actions will lead to an optimal or optimized result. Reinforcement learning is how we learn to play a game and get better. The rules and objectives are clearly defined. However, the outcome depends on the judgment of the player who must adjust the approach in response to the environment, skill, and actions of the other player.

Machine Learning in Practice

Machine learning is prevalent in all aspects of life today. For example, social media platforms use machine learning for face detection, image recognition, automatic friend suggestion, and so on. Ecommerce and other product/service providers use machine learning for personalized recommendations. Virtual personal assistants use machine learning for speech recognition, natural language processing, and conversations. Self-driving cars use machine learning for navigation and controls. In the financial world, banks, for example, use machine learning to predict loan defaults and accordingly approve/reject/limit loan applications. Also, financial institutions use machine learning to detect fraudulent transactions. These are just a few examples to illustrate the wide and growing usage in day-to-day life; there are many more.

Leading Machine Learning Frameworks

The rapid advancements in the machine learning world have led to proliferation of frameworks. One of the most common frameworks today is TensorFlow. TensorFlow is an open source platform for machine learning. Because of its comprehensive toolset, it enables the creation, training, and use of machine learning models easily. There are many other frameworks

like Microsoft Cognitive Toolkit (CNTK), Theano, Scikit Learn, Caffe, H2O, Amazon Machine Learning, Torch, Google Cloud ML Engine, Azure ML Studio, Spark MLlib, and MXNet, for instance. Some of these frameworks are better suited to specific areas or applications of machine learning than others. Interested readers can find more about any of these frameworks, but any further discussion of them is beyond the scope of this book.

To make it easy to use the machine learning frameworks, higher-level APIs are created, which support multiple frameworks and also abstract the framework differences. For example, Keras, developed by Google, is an open source software library that provides a Python interface for artificial neural networks. It works on Linux and OS X and supports multiple back ends including TensorFlow. Another parallel high-level API is PyTorch. PyTorch was developed by Facebook and works across Windows, Linux, and OS X.

Machine Learning and Cloud Computing

We often hear machine learning and "cloud" discussed together. A casual observer might think they are connected somehow. Theoretically speaking, they are not. Cloud computing is about computing resources being available at will, and machine learning is about making computers learn and make use of that learning. The reason we often talk about them together is because machine learning training usually requires a lot of computing resources. Therefore, it makes good sense to leverage cloud computing for procuring and using these resources. As machine learning assumes increase in importance in business applications, there is a strong possibility of this technology being offered as a cloud-based service known as Machine Learning as a Service (MLaaS).

The Way Forward

Artificial intelligence/machine learning (AI/ML) has the potential to touch literally all aspects of our lives. By the time we read or reread this section, any specific estimates on deployments and proliferation of AI and ML across solutions will be out of date. As per Gartner, "Artificial Intelligence and Machine Learning have reached a critical tipping point and will increasingly augment and extend virtually every technology enabled service, thing, or application."[3] One thing for sure, AI/ML is making inroads and making real impact. As it progresses and more businesses look to leverage the capabilities and benefits, ML will become an integral part of intelligent systems.

We have reached or maybe exceeded human-level performance at narrowly defined tasks such as strategy games, visual image detection, and parsing natural language.

There is a lot of debate around how things will shape up around machine learning. As we can imagine, with the continuous improvement in computation capability, data storage, processing, and learning, machines will continue to become more and more intelligent and powerful.

Extrapolating the advancements, some imagine that in the foreseeable future, machines could be capable of having "artificial general intelligence," a more recent term. Artificial general intelligence is the intelligence of a machine that has the capacity to understand/learn any intellectual task that a human can. Today, it is a primary goal of some focused AI research to gain the artificial general intelligence level where complete problems are modeled and solutions are hypothesized. Applications include computer vision, natural language understanding, and dealing with unexpected circumstances for solving real-world problems.

[3]Kasey Panetta, "Gartner's Top 10 Strategic Technology Trends for 2017," October 18, 2016, www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/.

Whether or not machines reach the "artificial general intelligence" level, machine learning is going to help solve problems that are intractable today. For instance, machine learning can help discover what genes are involved in specific disease pathways. Based on this, machine learning can be used to determine the most effective personalized treatment based on patient DNA and other related characteristics. Additionally, machine learning is enabling autonomous driving and will continue to improve safety. There are plenty of studies extrapolating the benefits of autonomous driving saving lives resulting from accident avoidance and so on.

Like any technology, there are potentially negative side effects of advancements in machine learning. Some worry about machines taking over humans. While that may sound futuristic, there are more immediate challenges or concerns. For instance, machine learning models may sound like black boxes. While a lot of time can be spent in validating the model, one can never be sure about the output of the machine learning model (especially deep learning). Incorrect results could be incredibly costly or even fatal.

There are potentially dire consequences of machine learning, some of which Elon Musk and Stephen Hawking present. For example, Musk has repeatedly warned that AI will soon become just as smart as humans and said that when it does, we should all be scared because humanity's very existence is at stake. Hawking said the emergence of artificial intelligence could be the "worst event in the history of our civilization."[4] And he followed up saying, "The development of full artificial intelligence could spell the end of the human race." And then there are others like James Barat who have termed machine learning as "our final invention" with his

[4] www.usatoday.com/story/tech/talkingtech/2017/11/07/hawking-ai-could-worst-event-history-our-civilization/839298001/.

book *Our Final Invention: Artificial Intelligence and the End of the Human Era*.[5] The book discusses the potential benefits and possible risks of human-level or superhuman artificial intelligence

A fundamental misunderstanding or maybe myth is that AI/ML is the solution for all the problems. Some of us feel like the AI/ML systems train themselves and become the solution for everything. The reality is that in order for a system to do something as simple as distinguish a cat from a dog, it must undergo supervised (deep) learning with volumes of data where its neural networks are trained to distinguish one from the other. So, while machine learning may sound like a potential replacement for an existing technology, we must be mindful of the time, effort, and resources it takes to model, train, and use a machine learning model. For example, machine learning may sound like the technology to replace traditional statistical analysis algorithms; however, knowing the time and resource penalty to build accurate models, we would be better off using the conventional statistical algorithms in most cases. As we've learned in previous chapters, we should be using "the" most appropriate tool for that specific use case.

Summary

In this chapter, we started with the fundamentals of machine learning, their benefits, and the evolution of machine learning. Then we talked about the various types of machine learning and the connection of machine learning with cloud computing. We followed that up with how machine learning is looking to shape up in the future.

[5]Thomas Dunne Books, 2013.

References

- Artificial Intelligence/Machine Learning Primer: www.actiac.org/system/files/Artificial%20Intelligence%20Machine%20Learning%20Primer.pdf
- Machine Learning for All: www.coursera.org/learn/uol-machine-learning-for-all
- Machine Learning: www.coursera.org/learn/machine-learning