

What is machine learning?

 bdtechtalks.com/2017/08/28/artificial-intelligence-machine-learning-deep-learning/

August 28, 2017

This article is part of Demystifying AI, a series of posts that (try) to disambiguate the jargon and myths surrounding AI.

I was nine years old when I had my first taste of programming, and fell in love with the art (yes, I believe programming is as much art as it is science). I quickly became fascinated with how I could control the flow of my programs by setting logical rules and conditions, *if...else* statements, switches, loops and more.

In later years, I learned to remove clutter from my code by creating modules and abstracting pieces of code into functions and classes. I enhanced my software development skills with object oriented analysis and design (OOA/D). I learned code reuse and design patterns. I learned to express my program in UML charts and diagrams. And I learned to apply those principles in nearly a dozen programming languages.

But the rule of thumb of programming remained the same: Defining the rules and logic. The rest were just tricks that helped facilitate the implementation and maintenance of those rules.

For decades, rule-based coding has dominated the way we create software. We analyze a problem or set of problems, specify the boundaries, the entities, the processes, the relations, and we turn those into rules that define the way a software is supposed to work.

While this approach has served us well, it has resulted in “dumb” software, programs that will never change their behavior unless a human programmer updates the logic in one way or another. Neither is it appropriate for scenarios where the rules aren’t clear cut, such as recognizing objects in images, or finding malicious activity in network traffic or navigating a robot across uneven terrain.

Machine learning, the cornerstone of modern artificial intelligence, is the science that has upended the traditional programming model. Machine learning helps create software that can modify and improve its performance without the need for humans to explain to it how to accomplish tasks. This is the technology that is behind a lot of the innovations we’re directly using today and are seeing on the horizon, including the creepily smart suggestions you see in websites, digital assistants, driverless cars, analytics software and more.

Machine learning is software that learn from examples. You don’t code machine learning algorithms. You train them with large sets of relevant data. For instance, instead of trying to explain how a cat looks like to an ML algorithm, you provide it with millions of pictures of cats. The algorithm finds recurring patterns in those images and figures out for itself how to define the appearance of a cat. Afterwards, when you show the program a new picture, it can distinguish whether it contains a cat or not.

Many people equate machine learning to artificial intelligence. However, AI is one of those loose terms, which can be applied to anything ranging from complex rule-based software to human-level intelligence that hasn't been invented yet. In reality, machine learning is a specialized subset of AI, which has to do with creating programs based on data as opposed to rules.

What are supervised, unsupervised and reinforcement learning?

There are several flavors of machine learning algorithms. One of the most prevalent is "supervised learning," in which you train the algorithm with labeled data and map a set of inputs to a set of outputs. The cat example from above is an example of supervised learning. Another example would be speech recognition, where you provide the algorithm with sound waveforms and their corresponding written words.

The more samples you provide a supervised learning algorithm, the more precise it becomes in classifying new data. And therein lies the main challenge of supervised learning. Creating large datasets of labeled samples is very time-consuming and requires extensive human effort. Some platforms such as Amazon's Mechanical Turk provide data labeling services.

In "unsupervised learning," another branch of machine learning, there's no reference data. Everything is unlabeled. In other words, you provide the input, but not the output. The algorithm ingests unlabeled data and draws inferences and finds patterns. Unsupervised learning is especially useful for cases where there are hidden patterns that humans can't define.

For instance, you let a machine learning algorithm monitor your network activity. It then sets a baseline for normal network activity based on the patterns it finds. From there, whenever it will probe for and flag outlier activity.

In comparison to supervised learning, unsupervised learning is a step closer to machines teaching themselves. However, the problem with unsupervised learning is that the outcome is often unpredictable. That's why it's usually combined with human intuition to steer it in the right direction as it learns on its own. For instance, in the network security example explained above, there are many reasons for network activity to deviate from the norm without the cause being malicious intentions. But a machine learning algorithm will not know that in the beginning and a human analyst will have to correct its decisions until it learns the exceptions and makes better decisions.

Another lesser-known field of machine learning is "reinforcement learning." In reinforcement learning, the programmer defines the state, the desired goal, allowed actions and constraints. The algorithm figures out how to achieve the goal by trying different combinations of allowed actions. This approach is especially efficient when you know what the goal is, but can't define the path to reach it.

Reinforcement learning is used in a number of settings. Among the more famous cases is Google DeepMind's AlphaGo, the machine learning program that mastered the complex board game Go. The company is now using the same approach to improve the efficiency of UK's power grid. Uber is using the same technique to teach AI agents to play Grand Theft Auto (or more precisely, let them learn by themselves).

What is deep learning?

Image converted using ifftoany

While machine learning is a subset of artificial intelligence, deep learning is a specialized subset of machine learning. Deep learning uses neural networks, an artificial replication of the structure and functionality of the brain.

Deep learning fixes one of the major problems present in older generations of learning algorithms. As datasets grow, the efficiency and performance of machine learning algorithms plateaus. However, deep learning algorithms continue to improve as they are fed more data.

Instead of directly mapping input to output, deep learning algorithms rely on several layers of processing units. Each layer passes on its output to the next layer, which processes it and passes it onto the next. In some models, the computations might flow back and forth between processing layers several times.

Deep learning has proven to be very efficient at various tasks, including image captioning, voice recognition, and language translation.

What are the challenges of machine learning?

While machine learning is extremely important and pivotal to the development of future applications, it is not without its own set of challenges.

For one thing, the development and deployment of machine learning algorithms rely heavily on huge amounts of computation and storage resources to perform their tasks. This very dependency makes their execution limited to cloud servers and large datasets. Consequently, performing them at the edge is considerably more challenging.

Another problem with machine learning—especially deep learning—is opacity. As algorithms become more complex, it becomes harder to explain the decisions they make. In many cases, this might not be a problem. But when you want to confer critical decisions to algorithms, it is important that they become transparent and self-explanatory.

And there's also the issue of bias. Machine learning algorithms tend to pick up the habits and tendencies that are embedded in the data they are trained with. While in some cases, finding and rooting out bias is easy, in others it's deeply embedded and hard to spot.

However, none of these challenges are likely to prevent AI and machine learning from becoming the general-purpose technology of our era, a term that has been previously used

for inventions such as steam engine and electricity. Where we are going, machine learning will be defining and disrupting things like never before.