AI For Everyone

Om Prabhu
19D170018
Undergraduate, Department of Energy Science and Engineering
Indian Institute of Technology Bombay

Last updated July 19, 2020

NOTE: This document is a brief compilation of my notes taken during the 'AI For Everyone' course by `deeplearning.ai`. You are free to read and modify it for personal use. You may check out the course here: `https://www.coursera.org/learn/ai-for-everyone`.

Contents

---

1 Introduction

1.1 About myself

Hello. I am Om Prabhu, currently an undergrad at the Department of Energy Science and Engineering, IIT Bombay. If you have gone through my website (`https://omprabhu31.github.io/`) earlier, which is probably where you found this document too, you will know that I am quite a bit into programming and tinkering with code to try and do cool stuff. Additionally, I love playing video games, listening to music and engaging in a little bit of creative writing as and when I get time. With this brief self-introduction, let us get into why I decided to pursue this course.

1.2 About this course

As you probably know, AI (artificial intelligence) is rapidly changing the way we work and live. It is difficult to name industries which are not likely to be impacted by AI in the near future (I initially thought of the textile industry as an example, but a simple Google search proved exactly how wrong I was). AI is generating huge amounts of industrial revenue per year and is likely to create 13 trillion US dollars per year by the time we reach 2030 (source: McKinsey Global Institute).

Hence, it is important to gain at least a general overview of the what makes AI such a powerful tool. Right off the bat, one of the major reasons why AI has taken off recently is due to the rise of neural networks and deep learning. But this is not all. One needs to learn what types of data are valuable to AI and how the type and amount of data influences the performance of a neural network. Further, it is also important to know how AI can be used to build personal as well as company projects. Lastly, it is also important to know how AI will affect society and jobs so that one is better able to understand AI technology and navigate this rise of AI.

With all this said, let us try to understand what AI really is and accomplish the above objectives.

---

2 What is AI?

AI is a very happening industry today and there is a lot of excitement among people as to how the rise of AI will map out. While this has boosted development of AI technologies even further, it has also lead to irrational fears among society. One of the major reasons for this is because not many people realize that AI can actually be put into 2 separate categories:

- ANI (artificial narrow intelligence): can do one thing (eg: smart speaker, self driving car, web search algorithms); incredibly valuable in specific industries due to narrow application
- AGI (artificial global intelligence): can do anything a human can do (perhaps even more things)

While the world has seen tremendous progress with ANIs, the same cannot be said for AGIs. This lack of distinction between ANIs and AGIs is what has led to fears of super-intelligent robots taking over the world.

In this section, we will be mainly looking at what ANIs can do and how to apply them to real-world problems.

2.1 Machine Learning

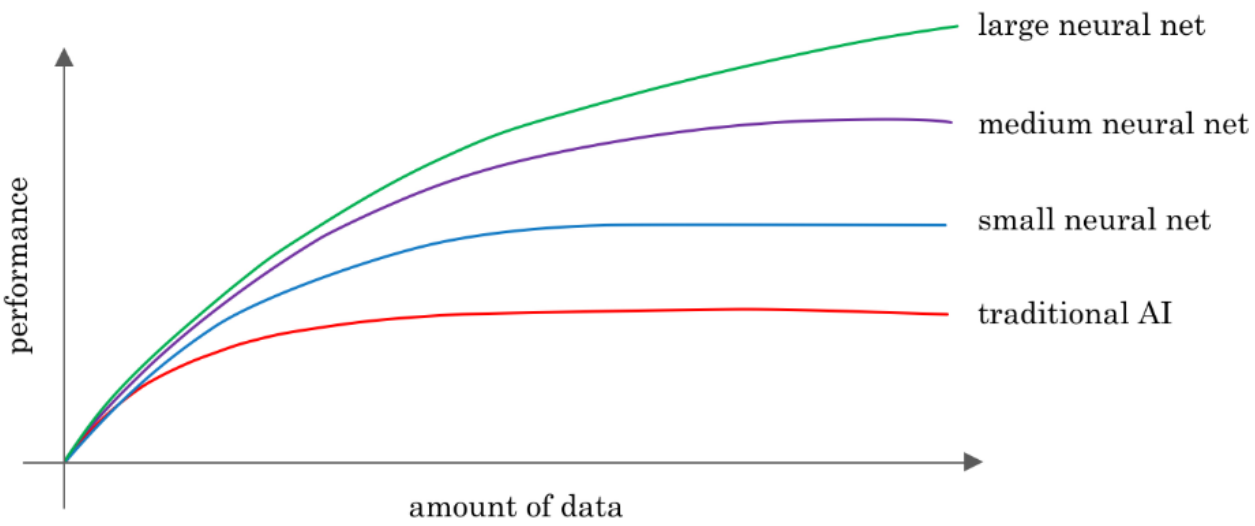
The rise of AI has been driven by one major tool known as Machine Learning. While the term might give a characteristic of omniscience to machines, this is far from true. In fact, the most used form of ML is what is known as Supervised Learning (or A $\rightarrow$ B mapping):

- learning a function that maps input to output based on a database of example I/O pairs
- learning algorithm analyses example training data to generate a function to map new examples
- eventually the algorithm can *learn* to predict the target output in previously unseen situations

One major application of this technology is in the online advertising industry. The input is in the form of advertisement details & some user info based on which the AI algorithm tries to figure out if the user will click on the ad or not. This is how users are shown only a certain set of advertisements online.

Another application of supervised learning lies in self driving cars. The input is a set of images & some radar info from sensors on the car. The AI uses this data to output the position of nearby cars and/or obstacles so that the self-driving car can avoid them.

Surely the concept of merely taking the input to construct an output seems limiting in the general sense of the scope of AI, however it can evidently be very valuable once a suitable application scenario is found. Now while the idea of supervised learning has been around for decades, it has taken off only in the recent years. This is mainly because of the limitation of technology to train large sets of neural networks to process huge amounts of data while also improving AI performance. This can be illustrated through a graph as follows:



- for traditional AI systems, the data vs performance graph maxes out pretty early
- on training increasingly complex neural networks with higher amounts of data, performance keeps on getting better for much longer

Hence to achieve the highest performance levels, we need two things. Firstly, it helps to have a lot of data - this is where terms like 'big data' come in. Additionally, we need the ability to train large sets of neural networks, which is made possible by specialized processors like advanced GPUs.

2.2 Data

Data is one of the 2 main things required to improve performance of AI systems. But simply having lots of data is not always helpful - we need to have the right type of data in the right format (structured or unstructured). Let's take a look at an example of a 'dataset' (or a table of data):

Size of house (sqft)	...	Price of house (1000$)
548		119
679		167
834		233
1209		342
1367		399

In practice, we will need a lot more than just 5 data entries to build an AI system, but let's work with this for now. The above dataset could work for an AI which checks whether houses are priced appropriately or not. In this case, the input would be the size of the house and the output would be the price. Going further, we might try to improve our AI by adding more input data fields such as the number of bedrooms, location, etc.

Another application of the same dataset would be figuring out the most appropriate house for a consumer on a fixed budget. In this case, our input and output fields will be exactly the opposite compared to the first application. What this means in essence is that, given a dataset, it is up to us to decide what is the input and what is the output, and how to choose these definitions to bring out the maximum value to our product.

2.2.1 Collection of data

So far, we have established that data is an important tool for AI systems and that there is a certain flexibility regarding the choice of input and output. But how do we get data? To discuss this, let us now switch to the more traditional example in machine learning of an algorithm designed to recognize images of cats:

- manual labelling: collect a set of pictures and manually label them as 'cat' or 'not cat'
  - tried and true way of obtaining a highly reliable dataset having both input and output fields
  - difficult, given the huge amount of data required (usually on the scale of several thousands of entries)
- observing behaviours
  - user behaviour: e-commerce websites keeping a tab on prices offered to users and whether they bought the product or not, something like this:

User ID	Time	Price ($)	Purchased
0156	Feb 22, 09:19:19	19.07	No
1548	Apr 01, 23:34:56	23.01	Yes
4898	May 23, 11:59:02	18.72	Yes
8896	Jul 10, 17:42:37	16.55	No

  - machine behaviour: fault prediction in machines based on operating conditions, something like this:

Machine ID	Temperature (K)	Pressure (atm)	Fault
55132	332	10.96	Yes
29475	378	8.22	Yes
00826	489	5.78	No
19475	653	2.99	No

- download from internet/partnerships: pre-compiled datasets that can be readily downloaded from the web (after obtaining required licenses if any), or obtained from partners (eg: a company obtaining fault analysis datasets from machine manufacturers)

2.2.2 Misconceptions about data

When thinking about the use of data, many people believe that they should have a lot of data on hand before feeding it into an AI system, and that having vast amounts of data will ensure the success of the AI system. Here's why this may not always work in practice:

- more data does NOT mean a perfect dataset
  - better to start relatively small and keep on continuously feeding data to the AI team
  - more often than not, the AI team provides dynamic feedback to the IT team regarding what data is useful and what type of IT infrastructure to invest in
- do NOT assume the success of an AI team just because it has a lot of data − garbage in, garbage out
  - not all data is valuable, 'bad' data will lead to AI learning inaccurate things
  - processing huge amounts of data needs appropriate infrastructure to complement it

There are many more data problems that may arise in practice, like:

- incorrect/missing values, or incomplete data: refer to the below example

Size of house (sqft)	No. of bedrooms	Price of house (1000$)
548	1	119
679	1	0.001
834	2	unknown
unknown	3	342
1367	54	399

- multiple types of data: AI algorithms work very well for all types of data, but techniques for dealing with them might vary
  - unstructured data: images, audio, video, text documents
  - structured data: tables, spreadsheets, databases

2.3 AI terminology

Up till now, we've been throwing around terms like AI, machine learning, neural networks, etc. Let's briefly explore what these terms actually mean.

2.3.1 Machine learning vs. data science

There is a thin line between what can be interpreted as machine learning and as data science. Let's say we have a dataset of houses like the one below:

Size of house (sqft)	No. of bedrooms	No. of bathrooms	Newly renovated	Price of house (1000$)
548	1	2	N	119
679	1	2	N	167
834	2	3	Y	233
1209	3	4	Y	342
1367	4	2	N	399

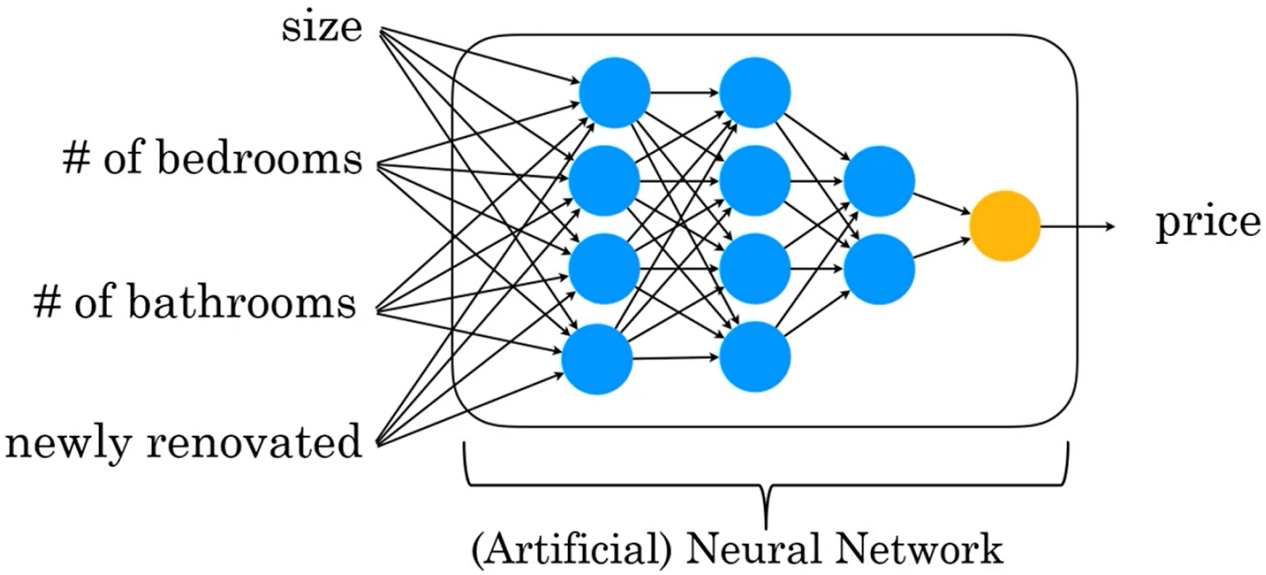
An application of this dataset to help construction companies price houses appropriately with the first 4 columns as input and the price as output would be a machine learning system, and particularly a supervised learning system. ML often results in running AI systems used on a mass scale.

In contrast, another application of the dataset is to actually let a team analyse the data in order to gain insights. They might come up with certain conclusions based on this, for example 'Houses with 3 bedrooms are pricier than 2 bedrooms of a similar size'. This can help companies take decisions on whether to build houses with 2 or 3 bedrooms, whether to renovate houses in order to sell them for a higher price, etc. This is an example of a data science project, where the output is a set of conclusions that helps companies take business decisions.

Let's take the online advertising industry as another example. Personalized ads powered by AI systems (that take ad info and user info as input and determine if the user will click on the ad or not) are machine learning systems. However when business teams analyse trends in the industry and come up with conclusions like 'the textile industry is not buying a lot of ads, but could be convinced otherwise with the right sales approach', it becomes a part of data science.

2.3.2 Deep learning

Let's take the same example of pricing houses. We take the 4 columns on the left as input. One of the most effective ways of generating the output would be to feed it into what are called neural networks.

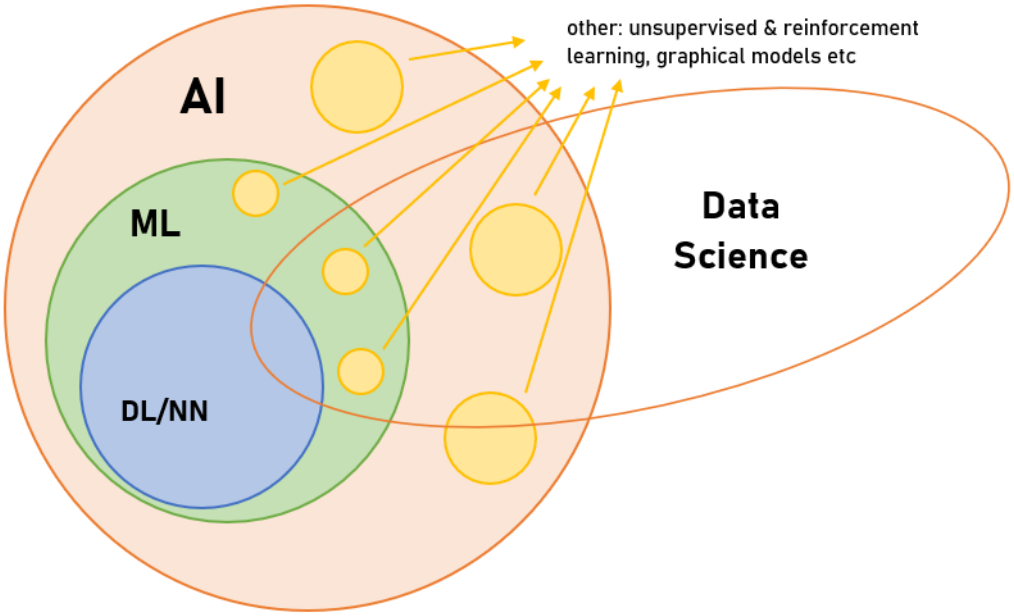


These are pretty similar to the network of neurons spread across the human body (which is also why they are referred to as artificial neural nets). This representation of ANNs bears some resemblance to the brain in that the blue circles are called artificial neurons which relay information across the network. And the resemblance ends right here. The details of how ANNs work are completely unrelated to how the human brain works.

At the end, what an ANN boils down to is nothing but a big mathematical equation that leads the system to reach the output based on a set of input parameters. This makes them very effective for learning A $\rightarrow$ B mappings. The terms 'deep learning' and 'neural networks' are used almost interchangeably today.

2.3.3 The larger picture

If we were to construct a Venn diagram showing all the concepts above, we would probably have something like this:



To date, there is a discrepancy about how data science fits into this picture. Some say AI is a subset of data science while others say the opposite. However, it is better seen as a cross-cutting subset that comprises of all these tools from AI and also other tools that drive business insights.

2.4 AI companies

In this era, it is possible for almost any company to employ a few deep learning algorithms. However, that by itself does not necessarily make it an AI company. AI companies specialize in the following:

- strategic data acquisition: many AI companies have free products solely for the purpose of acquiring data that can be better monetized elsewhere
- unified data warehouses: pre-emptive investments in bringing data together to a unified warehouse/a small set of connected warehouses
- pervasive automation: inserting AI algorithms to automate certain generic tasks in order to apply human labour & intelligence in more specialised work roles
- specialized roles: such as machine learning engineers (MLEs); allows for better division of labour and assigning specialized tasks to increase efficiency

It turns out that there is a systematic process using which companies can implement many of the above strategies to ensure that they use AI to their maximum benefit:

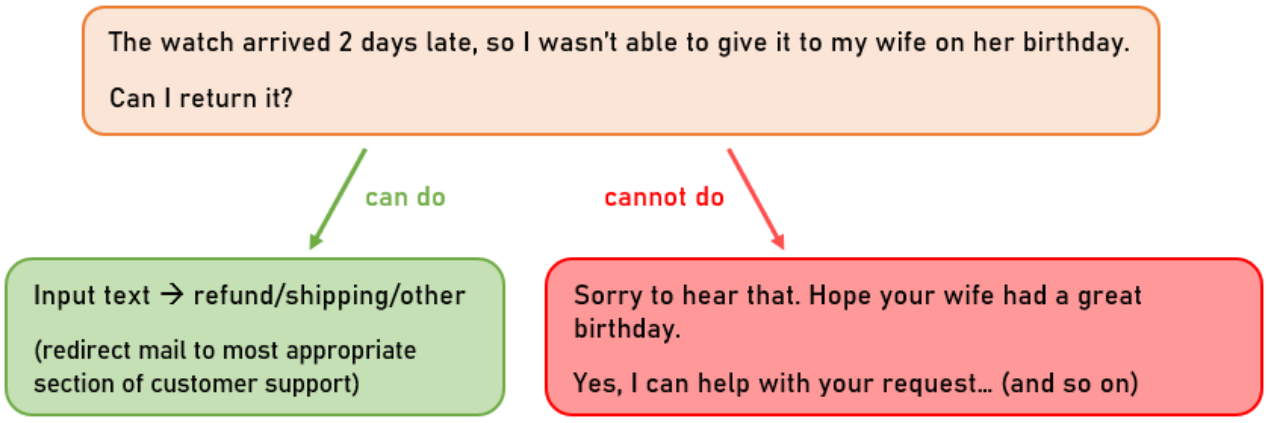
1. execute pilot projects to gain momentum and get a better sense of what AI can and cannot do, what types of data are useful, etc
2. bring together an AI team and provide extensive AI training to engineers as well as managers & executives
3. develop an AI strategy and build IT infrastructure based on dynamic feedback from the AI team
4. align internal and external communications so that others in the company hierarchy (shareholders, customers, etc) know how to navigate the rise of AI

2.5 Limitations of AI

Before committing to an AI project, it is important to check whether it is feasible. While the success stories we read in articles might make it sound like AI knows no bounds, this is far from reality. There are several limitations (currently, at least) as to what AI can and cannot do.

As an imperfect rule of thumb, anything that a human can do within a few seconds of thought can probably be automated using AI - for example, telling whether a phone is scratched/dented, looking around and determining positions of cars, deciphering audio, etc. In constrast, an AI probably cannot write a 50-page report based on in-depth analysis of the stock market. Let us take a look at some more examples:

- customer support automation: can sort incoming emails and redirect them to appropriate sections of customer support; cannot type out personalized responses

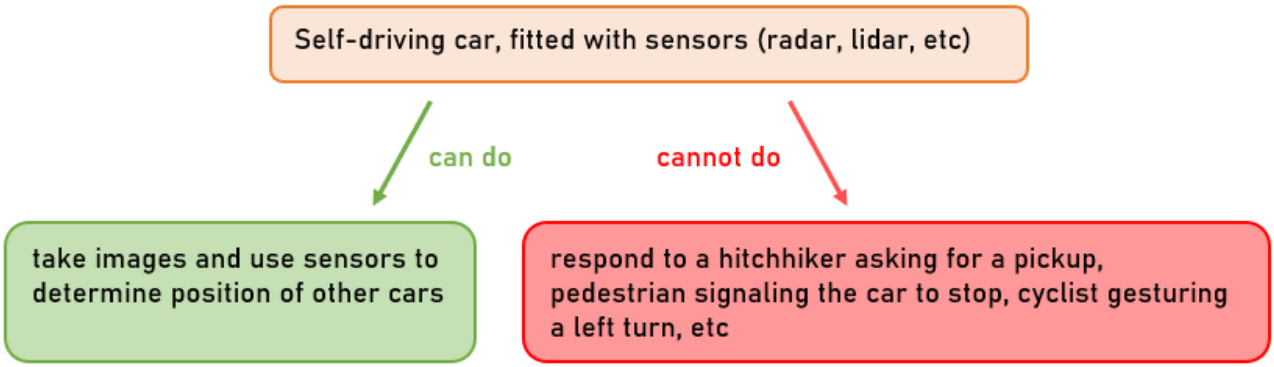


What if we try to do this anyway? Say we have a deep learning algorithm ready and a decent sized dataset of 1000 user emails and appropriate responses. We would get something like this:

"My product is damaged." → "Thank you for your email."
"Where can I write a review?" → "Thank you for your email."
"How do I send a product as a gift?" → "Thank you for your email."

It turns out that a sample size of 1000 (or even 100,000 as a matter of fact) is just not enough for an AI algorithm to write out appropriate and empathetic responses. In some cases, the AI may even generate gibberish which is clearly not desired.

- self-driving car: can use sensors and photographs to figure out relative positions of other cars; cannot respond appropriately to human gestures



One of the main reasons why this is so difficult to do is due to the sheer amount of possible hand gestures that could be made by humans. It is difficult to collect data of tens of thousands of people performing gestures. And again if we try to do it anyway, the consequences would be even harsher than in the scenario of customer support above.

- X-ray diagnosis: can diagnose diseases from around 10,000 labelled images (difficult to collect for rare diseases); cannot diagnose diseases based on a small set of images in a medical textbook (a human doctor can do this, however)

In the context of X-ray diagnosis, we can make out another weakness of AI, that is when it is asked to work with new types of data. Let's say the sample data contains high quality X-ray images. The AI algorithm will most likely fail when faced with poor-quality X-ray scans or images from even a slightly defective machine.

In the end, there are no hard and fast rules about the stuff that AI can or cannot do. Most of the times, AI projects require some weeks of technical diligence to figure out their feasibility. However, keeping the above points in mind, one should be able to get a fair judgement regarding the same.

2.6 Understanding deep learning

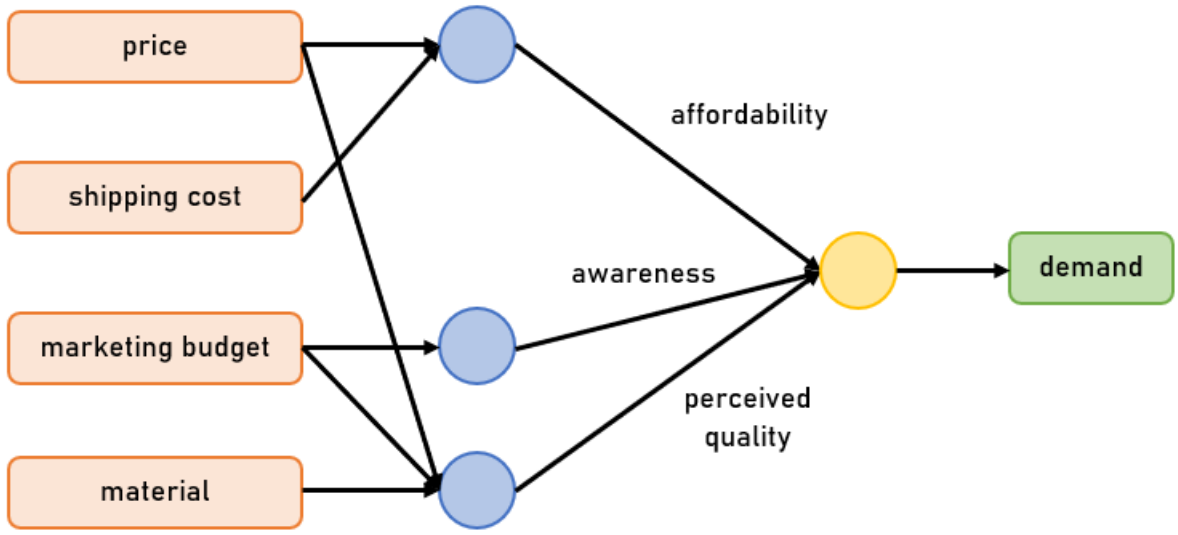
The terms deep learning and neural networks are used almost interchangeably in AI. Let us use an example of demand prediction to try and understand what neural networks really are.

Suppose a t-shirt company wants to know how many units they can expect to sell based on their selling price. The required dataset might be a in the form of a demand curve, where the higher the price the lesser the demand. This form of curve can be used to train what is perhaps the simplest possible neural network.

All this single-neuron network does is compute the curve shown and 'learn' it in order to map any value of price to the appropriate value of demand. A single neuron can be thought of as a Lego brick, and a neural network as a very complicated stack, often in multiple layers, of such bricks.

Let's look at a more complicated example. Suppose that instead of just the price, we have more variables like shipping cost, marketing cost and material. Then we will have multiple factors that influence demand like

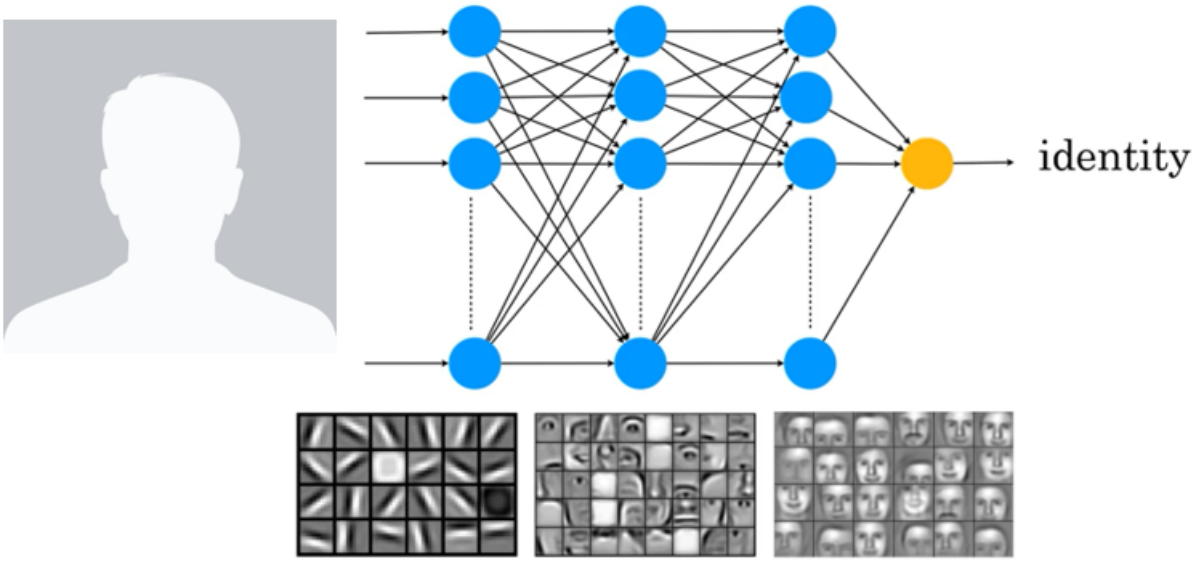
affordability, consumer awareness and perceived quality. We might then have a slightly more complicated neural net like the one below:



This slightly more complicated neural network maps the 4 input parameters to the output that is the demand.

From that the way in which we have discussed neural networks above, it appears as if we have to actually figure out the key factors as affordability, awareness and perceived quality. However, things do not work this way. One of the best things about neural networks is that we only have to provide it the input and the output – all of the stuff in the middle, it figures out by itself. It automatically 'learns' and completely trains itself to find the most accurate possible function that maps from the input to the output.

With this slightly advanced definition of neural networks, let us try to understand an actual practical application of neural networks in face recognition.



When we look at a face, we see certain features like eyes, expression, etc. What a neural network sees is millions of RGB values for each and every pixel in the image. Typically, when you give it an image, the neurons in the earlier parts of the network will learn to detect edges in pictures and later learn to detect parts of objects. After they learn to detect eyes and noses and the shape of cheeks and the shape of mouths, the neurons in later parts of the network will learn to detect different shapes of faces and finally, will put all this together to output the identity of the person in the image.

END OF WEEK 1

This is the end of the course documentation from Week 1. Keep on reading further for documentation from further weeks, or spend some time gaining further insight into the previously discussed topics.

---

3 Building AI Projects

So far we have covered the basics of AI and machine learning. But how do we put this technology to use in a project? Let's take a look.

3.1 Workflow of a machine learning project

There are 3 basic steps when building a machine learning project. Let us take speech recognition as an example, particularly Google speech recognition. How do you build a system that recognizes the words 'Ok Google'?

1. Collect data: involves collecting some audio clips of people saying the words 'Google' and 'Ok' (and lots of other words too - we want speech beyond 'Ok Google' to be recognized too)
2. Train the model: use a ML algorithm to learn input to output mappings
   - often the first attempt doesn't work very well
   - need to keep on iterating over the algorithm until it is good enough
3. Deploy the model: package the software into a product and ship it
   - may not work as well initially due to lot of new data (eg: if the sample dataset was from American users, the AI may not be able to recognize 'Ok Google' from Indian users as well initially)
   - get back user data (while maintaining privacy regulations) to maintain and update the model

Let us revisit this process in another example of self-driving cars:

1. Collect data: sample images and, for each of the images, position of nearby cars
2. Train the model: invariably the first model won't work well (eg: may detect trees or rocks as cars initially); need to reiterate until the model is good enough according to safety standards
3. Deploy the model: must be done in ways that preserve safety; get new data back (eg: new types of vehicles like tow trucks, auto rickshaws, etc) and update the model continually to the point that it can be released to the commercial market

3.2 Workflow of a data science project

Unlike a ML project, the output of a data science project is a set of insights that can be used to influence business decisions. Naturally it follows that they have a different workflow compared to ML projects. Let us take the example of an e-commerce platform that sells coffee mugs. There might be several steps a user has to perform to buy the product.

As a salesperson, it is our job to make sure that the majority of users get through all these steps. This analysis is done in a series of steps:

1. Collect data: gather user info (country, time, product they checked out, price they were offered, where they quit in the buy process)
2. Analyse data: get a data science team to work on the dataset
   - initially, the team might have a lot of ideas as to why users are not motivated to buy the product
   - need to iterate the analysis to get good insights and find out the major causes (eg: shipping costs are too high, so users quit at the checkout page)
3. Suggest hypothesis & actions: data science team presents the insights and suggests any suitable actions (eg: incorporate part of shipping costs into product cost)

– deploy changes to the product design and get new user data back (eg: users overseas may now buy more, but locals may not due to rise in base price)
– re-analyse new data continuously to possibly come up with even better hypothesis/suggestions

Again, let us briefly discuss this framework in another context of optimizing a manufacturing line for coffee mugs. We will want to make sure that as little defective mugs are produced as possible:

1. Collect data: data about different types of clay (suppliers, mixing times, moisture content, etc) and regarding different batches of mugs (temperature of kiln, duration in kiln, defects per batch, etc)
2. Analyse data: ask the data science team to analyse data to find the major source of defects (eg: too high temperature might lead to softening of clay and cause mugs to crack)
3. Suggest hypothesis & actions: change operations (eg: vary humidity and temperature based on time of day), get dynamic feedback from manufacturing output and take further actions if necessary

3.3 Impact of data on job functions

The digitization of society means that more and more data is being stored in digital formats. Due to this, almost all jobs have been or will be impacted by the advent of machine learning and data science. Let us see briefly how data science & ML have made or are making their way into different industries:

	Data Science	**Machine Learning**
Sales	optimising a sales tunnel (refer Section 3.2)	automated lead sorting - prioritize certain marketing leads over others (contact CEO of large company over an intern at small company)
Manufacturing	optimising a manufacturing line (refer Section 3.2)	visual product inspection (AI algorithms can learn to figure out if products are defective or not)
Recruiting	optimising the recruiting process (analysing why people are not making it to certain stages or why too many people are making it)	automated resume screening based on sample dataset of resumes and whether to select candidate or not (fair and ethical screening free of any bias)
Marketing	A/B testing - launching 2 versions of a website to find out what appeals to consumers	customized product recommendations to significantly increase sales
Agriculture	crop analytics (find out what to plant and when to plant based on market conditions, soil & weather conditions, etc)	precision agriculture (recognize presence of weeds through images/video and spray an appropriate amount of weed killers)

Of course, this list is not exhaustive and there are many more industries which have seen or will see the impact of AI soon enough.

3.4 Choosing an AI project

There are definitely a lot of things we can try to do with AI, but how to we choose an AI project? Let us discuss a general framework on how to choose an AI project. Many of these points have already been discussed, but let us revisit them in this context:

- feasibility and value addition:

  - must be feasible to do with AI and also add value to the business/application
  - brainstorming with cross-functional teams (comprising both AI experts as well as business domain experts) to narrow down projects
- brainstorming framework:
  - think about automating tasks rather than entire jobs (eg: for radiologists, AI might be useful in X-ray diagnosis but not as useful in consulting with other doctors or patients)
  - consider main drivers in business value and try to augment them using AI to increase the scale and productivity of the business
  - consider tasks which are particularly painstaking for humans and try to automate them if possible
- do not insist on acquisition of big data
  - try to make progress with small datasets and get dynamic feedback from the AI team as to what type of data to obtain further and what type of IT infrastructure to build

After brainstorming and narrowing down to a certain list of projects, it is time to pick one to work with. Committing to an AI project requires a lot of work to see it through and hence, it is important to conduct due diligence on it. Technical diligence is used to make sure the task is feasible to carry out using AI, while business diligence revolves more around deciding how much value it is going to add and if it is worth the effort.

Technical Diligence	Business Diligence
can an AI system meet the desired performance	will automation lower costs enough?
how much data is needed	how much revenue/efficiency it will increase
engineering timeline (how long and how many people it will take)	will launching this project bring enough value to the business?
	building spreadsheet financial models to estimate the value quantitatively

Another type of diligence one should try to perform is ethical diligence (i.e. is the society/environment being harmed). Any AI project should ideally add value to society and if not, it should not cause harm at least.

Another factor we need to consider is whether we want to build or buy (or maybe do a combination of both):

- outsourcing ML projects can lead to easier access to datasets
- data science projects are more commonly done in-house since they are highly tied to the business (it takes very deep insider knowledge about the business which is unlikely to occur through outsourcing)
- try and build things that will be specialized to the project
- avoid building things that are an industry standard (eg: storage servers, computer hardware, etc)

3.5 Working with an AI team

(This section is currently in the works. Expect it to be up within a week's time.)
