Understanding the jargon: AI Sub-fields

In this article, we'll be attempting to demystify all the jargon that is associated with artificial intelligence and data science. But first, we'll need to understand the very basics of how an AI algorithm works to be able to better gauge what all of the below means.
Here are the most general steps of how we train an AI model (this will be true for *almost* all AI models):

1. You have a set of paired inputs `(x, y)`
2. You, as a human, know that `y` is predictable with information given in `x`
3. Your model `M` is a black box that takes as input `x` and outputs a value `y'`
4. You compare the expected output `y` and the actual output `y'` and have a way to measure the error.
5. The error gives the model feedback on how wrong it is, based on which it self-corrects itself according to some predefined rules.
6. You keep repeating until the model `M` is accurate enough on the `(x, y)` pairs that it **hasn't yet seen during training.**

In pseudo code, this is how you train an ML model (*almost* always):

```
M = new Model()
for (x, y) in training_dataset:
    result = M(x)
    err = error(y, result)
    M.self_correct_according_to(err)
    if M.accuracy(unseen_data) > 0.95:
        print("We're done!")
        exit;
```

So, to do any sort of data science related work, you need:

1. Data (images, audio, excel sheets, EEG readings, signals, MRI Scans, or pretty much any information that can be represented digitally as numbers)
2. A Model (in code, this will be a (generally differentiable) function that takes an input, does some calculations, and returns an output)
3. A way to measure how bad the model is (so it can correct/train itself)
4. A way to measure how good the model is. (so it knows when to stop correcting/training itself)

With that you of the way, we can actually move on to understanding the differences between different areas in AI. There are two (or more) kinds of meanings each of these terms have.

- One is the actual, technical meaning.
- The other is what people mean when they actually say these words in every day language. This is similar to how Xerox is a company but people use the term interchangeably with photocopying.

If you haven't noticed already, I've been very liberal with using these terms even throughout this article up until now. Since the meanings of all these terms is very fluid, I'll try to be as general as possible in explaining them.

Let's start with some definitions from Wikipedia (please remember the acronyms, it'll make life easy)-

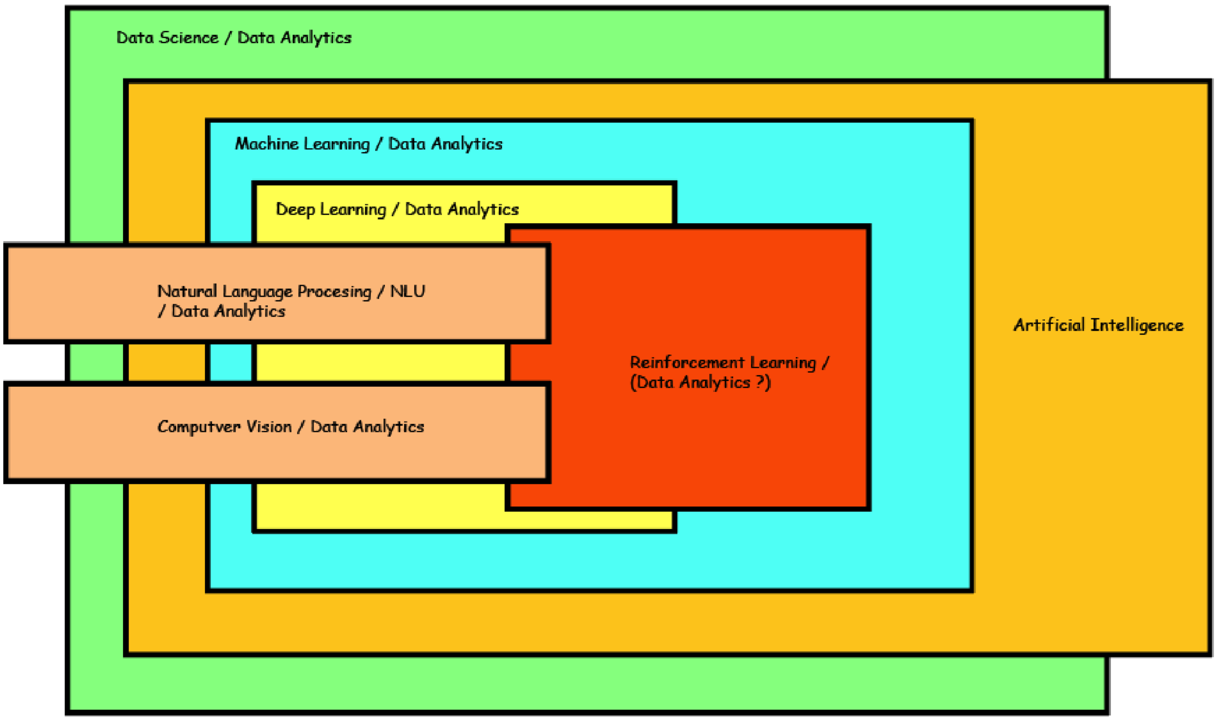
- Artificial intelligence (AI) : sometimes called **machine intelligence**, is intelligence demonstrated by machines, unlike the **natural intelligence**displayed by humans and animals.

- Machine Learning (ML): the study of computer algorithms that improve automatically through experience
- Deep Learning (DL): (also known as **deep structured learning**) is part of a broader family of machine learning methods based on artificial neural networkswith representation learning
- Reinforcement Learning (RL): is an area of machine learning concerned with how software agents ought to take actions in an environment in order to maximize the notion of cumulative reward. Reinforcement learning is one of three basic machine learning paradigms, alongside supervised learningand unsupervised learning.
- Data Science: is an inter-disciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from many structural and unstructured data.[1][2] Data science is related to data mining, machine learning and big data.
- Data Analytics: is the systematic computational analysis of data or statistics. It is used for the discovery, interpretation, and communication of meaningful patterns in data
- Computer vision (CV): is an interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos. From the perspective of engineering, it seeks to understand and automate tasks that the human visual system can do.
- Natural Language (NLP): is a subfield of linguistics, computer science, information engineering, and artificial intelligence concerned with the interactions between computers and human (natural) languages, in particular how to program computers to process and analyze large amounts of natural language data.

I'll try and give some popular and common-place examples for you to get an idea of all the places where fields directly affect your life (if you're not new to this, you'll find this almost cliche):

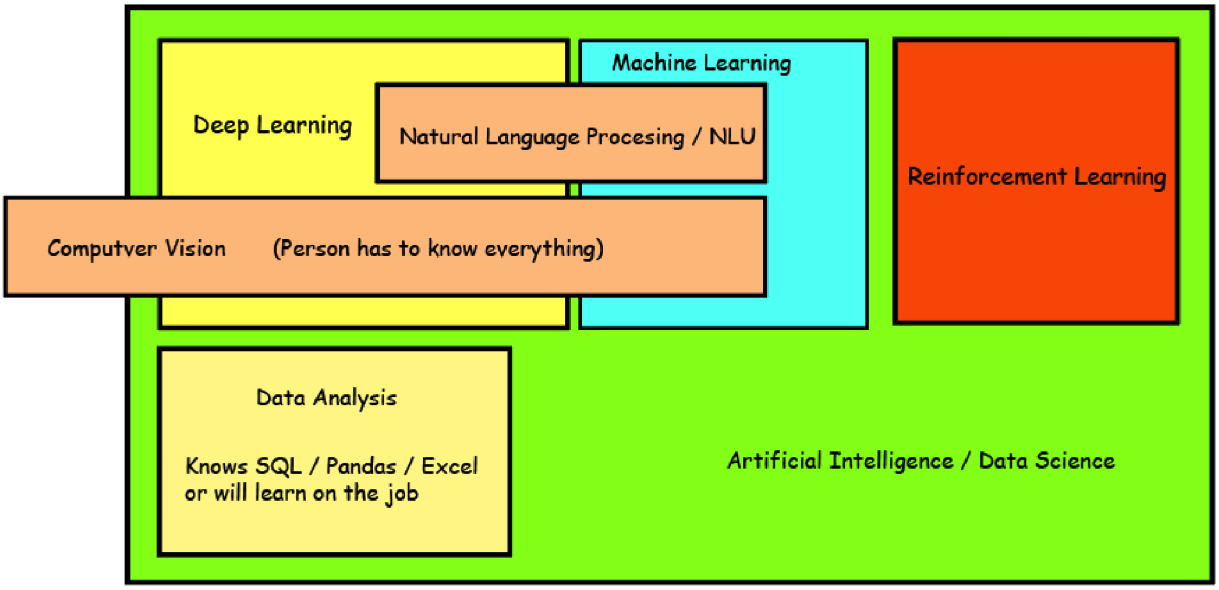
1. Instagram's Explore section is curated using something called a recommender system that is developed with DL algorithms
2. Google Photos recognizes your friend's faces using CV algorithms which are part of DL.
3. Google Now understands what you mean when you give it voice commands using NLP and NLU (Natural Language Understanding)
4. The AlphaGo algorithm that caught the news after beating the world's best Go players was created by DeepMind using RL algorithms.
5. Banks do credit scoring using ML algorithms.
6. Regular decision making in big (and some small) companies is done using data analytics by analyzing huge volumes of data to gather useful insights.
7. AI and Data Science are loose terms that people regularly use to talk about all of the above.

This figure is (mostly) a technically accurate overview of where everything overlaps and what is contained in what else, and where these terms differ:
(forgive my poor illustration skills and the use of Comic Sans)


Data Science / Data Analytics
Machine Learning / Data Analytics
Deep Learning / Data Analytics
Natural Language Procesing / NLU / Data Analytics
Reinforcement Learning / (Data Analytics ?)
Artificial Intelligence
Computver Vision / Data Analytics

Notice that AI has a portion that extends outward from everything else. This is because there are classic AI algorithms that don't fall in any of these categories. Further, notice how I've included "Data Analytics" in almost every bubble. The simple reason is that all these techniques allow you to analyze data in some way or the other. You'll see how this becomes a problem when companies put "Data Analyst" on their job descriptions and an applicant eventually realizes what they wanted was a guy who can perform SQL queries and not necessarily analyze huge amounts of glorious conversational data from Reddit. The opposite is also true.
Another thing to notice is how NLP and CV extend into different areas and even outside of everything else. This is because even applying a simply brightness filter constitutes what is called Computer Vision and that algorithm doesn't fall into any of these categories. The same logic applies for NLP too. Another important aspect is that the Data Science bubble seems to encompass pretty much everything because, well, all of these areas are variants of the **Science of Data**.

Here's the problem- this is what most people actually (incorrectly) mean when they talk about these areas:


Machine Learning
Deep Learning
Natural Language Procesing / NLU
Reinforcement Learning
Computver Vision
(Person has to know everything)
Data Analysis
Knows SQL / Pandas / Excel
or will learn on the job
Artificial Intelligence / Data Science

This is the categorization they use in industry, and sometimes even in Academia. Specifically, Machine Learning, Reinforcement Learning and Deep Learning are mostly talked about as three very separate areas of study.
This is why I originally said that all these terms are very fluid and depend a lot on context and organizations where they are used. It's best to infer what you need in the moment.

But then, how do I choose what to do ?

Here's a framework that will work for a majority of people:

If you already know what domain you want to apply your skills to, this part becomes much easier than otherwise. So, first I'll detail what career options you could have based on what you learn. If you have something in mind already, then this should help a lot.

There are two kinds of data: structured and unstructured.

- Structured Data: these are mostly CSV/Excel files with lots of rows and columns. Here, each entry has a very specific meaning to us humans.
- Unstructured Data: Images, audio, etc. This kind of data can be very chaotic and doesn't follow rules during creation. (can you lay out the formal rules for an image to contain a cat?)

You can apply both ML and DL to both structured and unstructured data. But, in practice, you'll use more ML algorithms for structured data and more DL algorithms for unstructured data.

- If you know you want to go into finance / banking / investment or other related fields where spreadsheets will be your best friends, you'll probably want to focus first on ML and data analysis.
- If you're looking to work in robotics, do things like face detection, identify objects in an image, tag audio samples by their genre, make intelligent voice-enabled applications, etc., then you should be looking more into DL.
- If you're fascinated by how virtual agents in games work and how to create intelligent agents in simulated environments, then RL is probably what you'll be focusing on.
- You should NOT try to learn everything. One would think it's obvious but too often a lot of people try and learn all of these things at the same time.

Now, if you're still confused like I was (and most people are. It's okay!), then the best way to go about this is do a course which gives you an introduction to all of these fields. By the time you complete it, you will have a much better idea of where to go next. In any case, you will have to learn the basics of ML before trying to get into DL or RL anyway. But don't fret, it's not more than a few hours of work if done the right way.

All of this sounds very fancy. Is it that hard?

Short answer: NO
Long answer: Probably, Yes.

At a conceptual level, almost all the time you'll be able to distill all the math down to matrix multiplications, basic calculus and introductory probability theory. If you're not planning to be a researcher in academia, then you won't be needing to get into the conceptually hard parts in AI. Everything you'll need to know to work in industry will generally have an associated blog on Medium explaining it in simple language. So **No**, at a conceptual level needed for industry, ML isn't hard.

But,

There is a huge, ever growing (daily) breadth (not depth) of concepts that constitute this field. For most people (like me), this is actually an advantage as it keeps things interesting. For some though, it can quickly get taxing to stay updated all the time with the latest papers and industry practices. In ML, it's not just the frameworks and software, but also the very foundational concepts the keep getting revisits and major modifications all the time as researchers discover new phenomena. But again, it highly depends on your career whether and to what degree you'll need to stay updated. For the most part, you'll just need to be current with how the popular ML/DL frameworks change over time and any *major* new techniques that show up. Following a few YouTube channels and some quality weekly newsletters should be enough (this will be covered in a later article)

Also,

If you're aiming to get an AI *Research* position at a big tech company (FAANG), or get a PhD/Postdoc at a reputed university abroad, then I'll be honest: you're in a for a few years (3-10 years based on your exact aims) of grueling hard work, disappointment, glory, and probably realizing you never wanted it in the first place after having consumed your 20s entirely in another rat race. I don't want to discourage anyone, but this is a very important thing to know. I will talk about this in detail later in the series.

Just give me the links to the online courses already!!

In the next article, we'll talk about how to *actually* learn all things things that I said you should. I'll also share some of what I believe to be the best resources on the internet. We'll talk about *how to choose* online courses / resources / books and things to stay away from (like Udemy). We'll also talk about choosing the right frameworks and languages (PyTorch vs Tensorflow, Sklearn vs NVIDIA RAPIDS, Python vs C++) based on your specific needs. In the same article, or in a follow up, I'll talk about the setting up the hardware you need for ML/DL work.