AI For Everyone

Labelling

1. Download from partners/websites labeled datasets
2. Manual labeling of data
3. Automate the way of receiving data (observing behaviors from users/machines)
    - product purchased/not purchased
    - ad clicked/not clicked
    - machine fault/not fault

Data misuses and solutions

a) e.g. Invest 3 years in feature engineering before starting building AI systems

Solution: Once we have collected some features we must start the ML cycle/iteration and improve either the data or the ML system

b) Assume that having much data will be valuable to built an AI system

Solution: Many AI systems can be start and make progress using also small datasets. Having more data never hurts. But having more data doesn't mean that data are valuable. AI experts can answer the question how much value there is in the data.

c) Messy data, garbage in – garbage out: missing values, wrong values

Solution: pre-processing, data imputation, filtering

Data science teams: provide insights, extract knowledge and report a powerpoint, excel from data to companies to take decisions

Machine learning teams: build software machine learning systems that make decisions automatically

Taxonomy of areas: Deep Learning/Neural Networks is a subset of Machine Learning, and ML is a subset of AI.

Workflow of a ML project:

1. Collect data to work with

The data to work with should have the same distribution as the data that will be tested in the production environment. In the workflow of a ML project we might revisit this step if we need to use more data in order to train a better model.

2. Train a candidate model to map input to output, y = f(x)

This is an iterative process in which we can always search for a better model/mapping. However, we start by building a dump model and continuously improve it by testing new ideas, hyperparams, etc.

3. Deploy the model

Test the model in the real world and monitor for any false positive / false negatives (we can reuse them to retrain/update the model) – get data back and update the model.

Workflow of a Data Science project:

1. Collect data to work with

e.g. for sales maximization we might need to collect user actions in an e-commerce website or for minimizing defective construction in a manufacturing line we might need to collection data from each processing step of the manufacturing line

2. Analyze the data and try to extract knowledge / insights

use statistics, clustering, distributions, optimization, iterate many ideas…

3. Suggest hypothesis/actions

Use A/B testing and apply an action suggested by the DS team. After the change we can retrieve new data periodically and analyze the side effects of the change suggested.

Some DS / ML cases in the industry: Sales optimization, Manufacturing (visual inspection), Recruiting, Marketing (recommendation systems), Agriculture.

Brainstorming AI projects: Synthesize a cross-functional team with domain experts / business people and AI experts that can brainstorm together to find AI projects that are VALUABLE for the company and also are FEASIBLE technologically.

Brainstorming framework that can be used by cross-functional teams:

1. Try to build ML systems that automate tasks, not jobs. A job position might perform daily 10 tasks. Try to identify the most fruitful and valuable tasks a job positions does and brainstorm on them to see if they are valuable and feasible to automate with ML. E.g. 1) In a call routing center you might try to automate the email routing task, 2) For a radiologist we might need to automate X-ray reading.

2. Try to identify the main pain points in a business and brainstorm on them. An ML system could solve a main pain problem so it is important to brainstorm on them.

3. What are the main drivers of business value? What brings value to the company? Some of them may be solved by AI, some other not.

Small datasets advice: Even if we haven’t much data we should not abandon the try. Of course, having more data almost never hurts. But, with small datasets we can still make progress on a problem.

Due diligence: If a project needs only 1 to be tested as a prototype go for it immediately and report the results. However, when a project needs many months to get results we can perform due diligence on the project: spend some time to assure that what is hope is true really is true.

A. Technical diligence: Is the AI system doable/feasible?

1. Can the AI system meet the desired performance? e.g. Business people might require 99% precision and 99% recall on imbalanced classes. However, this might not always be possible. We have to check if the desired performance can be met. It is useful also to check the literature to check what are the state-of-the-art limits on many well-known problems. E.g. it is not doable a speech recognition system with 100% accuracy.

2. How much data is required for the AI system to be built and meet the desired performance?

3. How much time and people do we need to build / deploy the AI system?

B. Business diligence: Will the AI system with desired performance achieve your business goals?

The AI system might help to lower the costs, increase the revenue, or launch a new product or business. Business people have to do their analysis and be sure that their AI strategic will help the company. The company specifies an acceptance criteria: might be the lowest performance for which the company benefits and ML team tries to achieve it progressively. The measure has to be on test/hold-out data for which the model will not be trained.

C. Ethical diligence: Do we make the society better? Do we help the world? Do we use AI to make a better world?

Build vs Buy the AI technology: ML projects can be in-house and outsourced. DS projects are usually in-house because they are very tied in the domain and business.

“Never sprint in front of a train” If there is a standard industry solution (software, standard, open-source), do not try to reinvent it in-house. It is a massive force with large velocity that will probably overpass your progress. Embrace the industry solution and try to invest your limited resources time/money/HR on things that YOU can make unique and good. Try to find your innovation.

Some reasons why we might not be able to achieve 100% accuracy:

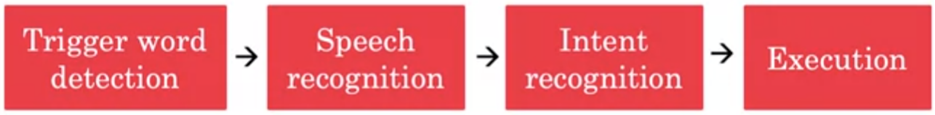
1. Limitations of ML
2. Insufficient training data
3. Mislabeled data
4. Ambiguous data

2-3 years are need for a company to be great at AI

Complex AI projects: They have usually multiple components mapping A→B in a sequence, usually called: AI pipeline.

Examples (case studies):

1. A smart speaker (voice-activated device) might have the following components: **a**) trigger word/wakeword detection, **b**) speech recognition, **c**) intent recognition, **d**) command execution. Each of the components might be developed by different teams in an AI project.



Example A: “Hey device, tell me a joke”

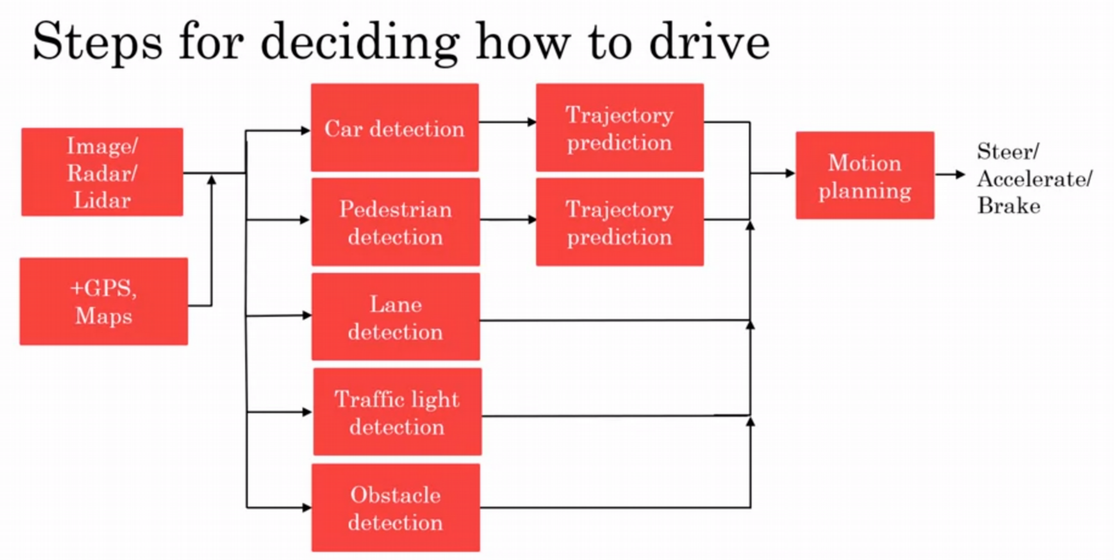
Input: “Hey device” (audio) → **a** → Output: 0/1 (trigger word or not)
Input: “tell me a joke” (audio) → **b** → Output: “tell me a joke” (transcript)
Input: “tell me a joke” (transcript) → **c** → Output: “joke” (command)
Input: “joke” (command) → **d** → Output: a random joke is generated

Example B: “Hey device, set a timer in 10 minutes”

Input: “Hey device” (audio) → **a** → Output: 0/1 (trigger word or not)
Input: “set a timer in 10 minutes” (audio) → **b** → Output: “set a timer in 10 minutes” (transcript)
Input: “set a timer in 10 minutes” (transcript) → **c** → Output: “timer” (command)
Input: “timer” (command), **“10 minutes” (arguments)** → **d** → Output: a timer is set in 10 minutes

The “10 minutes” needs to be extracted from the “set a timer in 10 minutes” and used as extra parameter in the last **d** step.

2. A self-driving car might have the following components: a) sensors that input images/radar/lidar/GPS/maps, b) car/pedestrian/lane/traffic-light/obstacle detection (computer vision supervised learning problems), c) trajectory detection of cars/pedestrians (how they are moving), d) motion planning (what path to follow to arrive to the destination and avoid obstacles/collisions), e) translate motion planning path to specific steering/acceleration/break appropriately. Each of the components might be developed by different teams in an AI project.



Roles/responsibilities in an AI team:

AI roles are not clearly defined in AI industry yet because AI is evolving so fast.

1. Software Engineer (software engineering tasks, code infrastructure, software libraries, design patterns/principles)

2. Machine Learning Engineer (gathers data, learning models that map A-B, improves a model in ML using various iterations/cycles)

3. Machine Learning Researcher (extends state-of-the-art ML, publishes papers)

4. Applied ML Scientist (combines both 2 and 3 – finds and adapts paper solutions in the company's problems/projects)

5. Data Scientist (not very well defined role, examine data and provide insights, make presentations to executives, teams)

6. Data Engineer (when managing big data volumes we need this role to save, organize and make data easily accessible, secure in a cost effective way)

7. AI Product/Project Manager (help to decide what to build, what is feasible and valuable)

AI transmission playbook: A roadmap of 5 steps of how to help a company to become great at AI

URL: https://landing.ai/ai-transformation-playbook/

1) Execute pilot projects to gain momentum

Run AI projects for some months and check the results.

It is not necessary for these projects to give value to the company immediately. However, it is important for the results to be interesting and promising.

We run multiple AI projects to gain momentum and learn how things are done in AI.

An AI solution might need time to be embedded to an existing system and prove its value.

For the initial AI project we should think something that has good change of success rather than to give value for the company.

The pilot AI projects can be in-house or outsourced.

2) Build an in-house AI team

In the beginning might be OK to outsource you AI projects. This can really help you gain momentum on the field. However, to be more expertise on AI or to execute long-term sequence of AI projects you need to build an in-house AI team.

An in-house AI team that is centralized in a company can help various Business Units (BU). The AI engineers of the in-house team can collaborate with domain experts from BUs and together within the brainstorming framework can find feasible and valuable AI projects that can give value to the company.

3) Provide broad AI training

AI engineers need to be trained on AI techniques, technology, science. However, multiple people on multiple levels need also to understand how AI can affect their roles. For example:

- Executives / Business leaders (~4/5 hours training)

  What AI can do for your business?
  Think how to build AI strategies
  Resource allocation

- Leaders working on AI projects (~12 hours training)

  Set project directions (technical and business diligence)
  Resource allocation
  Track and monitor progress of AI projects

- AI engineers (~100 hours training for a SE to become ML/DS engineer)

  Build and ship AI software
  Gather data
  Execute on specific AI projects

4) Develop an AI strategy

Although it sounds more naturally for the AI strategy to be the 1st step, Andrew Ng thinks that it should be the 4th step. So, only after we have run some pilot AI projects to gain some momentum, built an in-house AI team with some engineers and have some training (1,2 and 3 steps) we will be truly ready to understand how AI can help the company. It also need some time for the executives and business leaders to adopt AI and design an AI strategy that can give a long-term advantage to an industry sector.

There is an AI strategy defined as **“Virtuous Cycle of AI”** (self-reinforcing positive loop): We build a better product and because it is better we gain more users. Then we can get more data from the their usage and use their data in an AI system to build an even better product (and the loop continues).

Data strategy:

Strategy data acquisition (e.g. ways of collecting data about your users: free email service, free photo-sharing service).

Build a unified data warehouse (unify information/data from multiple data sources to help AI engineers to connect the dots and spot the patterns in data).

5) Develop internal/external communications

AI Pitfalls

1. Don’t expect that AI can solve everything

   Be realistic about what AI can/cannot do given limitations, technology, data, engineering resources. Do business/technical diligence to select feasible and valuable AI projects.

2. Don’t just hire 2/3 ML engineers and count solely on them

   Although ML engineers are scarce job roles you need mostly cross-functional teams with both AI and business talent people to find feasible and valuable projects.

3. Don’t expect the AI project to work the first time

The development of an AI project is an iterative cycle/process with multiple attempts needed to succeed.

4. Don’t expect traditional planning processes to apply without changes

   Work with AI team to establish timeline estimates, milestones, KPIS metrics that make sense.

5. Don’t think that you need superstar AI engineers to start developing anything

   As long as you have some AI engineers try to get start the ML cycle and improve your AI project later on.

Your first steps

Ask your colleagues to start learning AI, learn books an online ML courses

Start some brainstorming projects (start with a small AI project and try to succeed)

Hire a few DA/ML people to help

Hire an AI leader to manage the team and the production

Discuss with CEO for possibilities of AI transformation

Limitations in AI

1. Explainability is hard but sometimes doable (many AI systems are black boxes)

2. Adversarial attacks: Either artificial (e.g. adversarial examples attacking a computer vision model) or physical (e.g. wearing adversarial glasses and fooling a face recognition system). **Solution:** Adversarial Training, Adversarial Defense Methods.

3. Biased AI through biased data (discriminate, unfairly against minorities)

   ○ Example 1: NLP systems learn mappings from A → B and use textual information. After learning the embeddings of words (e.g. with word2vec) if we do analogy reasoning we might find that unhealthy stereotypes exist in our text data. The AI system will become bias because it is trained on biased data. **Solution:** “zero-out” bias in words and train on less biased text.

   ○ Example 2: Face recognition systems that are trained mostly on lighter-skinned individuals will perform poorly on dark-skinned individuals. **Solution:** Train on various types of faces.

Bad use of AI: Fake data, fake video/image/speech/text.

AI is the new Electricity.