11-785 Deep Learning Projects

Fall 2018
Projects

• Teams of at most (whenever possible exactly) 4 students. Submit your teams by the deadline, if some need teammates at this point we will complete them manually.

• Projects are expected to demonstrate significant expertise in ability to deal with neural networks
Project Schedule

• Proposal:
  - Must include:
    ◦ Problem definition
    ◦ Objective
    ◦ Some suggestion for an approach

• HW5: Mid-term report, due in November (temp date is Nov 10th)
  - Must include
    ◦ Problem description
    ◦ Approach and definition of intermediate waypoints
    ◦ Evaluation metrics on intermediate waypoints

• Final poster presentation (December)

• Final report (December)
  - Must include
    ◦ Full problem description in paper format
    ◦ Proposed approach
    ◦ Results and conclusions
Proposal

• Should be about one page
• Don’t stress too much on this, we will let you change later if needed
• Especially, on the approach suggestion, we know you don’t have all the tools for complex problems at this point. This proposal is mainly for you to have a better idea of what you want to do.
Ideas

- These are only suggestions
- You may also come up with your own idea
- It's OK for multiple teams to work on the proposed ideas
  - Provided they work independently

- Most suggested ideas have scope for publication
  - But only if attempted approach is novel

- The slides only mention barebones outlines or topics
  - You will have to do your background review prior to proposing a project on these topics
Category

• Speech and audio
The Airbus Challenge

• Airbus is releasing a collection of ATC voice recordings

• Challenge: Beat everyone in the world at recognizing these commands

• Resources: We have a couple of hundred thousand ATC recordings from the FAA to practice on, before Airbus releases their data

• Much bragging rights, if you end up near the top..
  - Name, fame, glory and pubs..
Large-scale audio content analysis

• Audio information retrieval

• The YFCC corpus has nearly a million audio recordings

• Objective:
  - Analyze their content
  - Retrieve recordings in response to natural-language queries
  - Run this over all million recordings!

• Will be the first large-scale analysis of this kind (except, perhaps, within Google)
  - Publications highly likely
Category

• Images/video
Medical Imaging

• Learn to recognize lung disease in Xrays

• Data
  - 100k lung Xrays (from India)
  - Only 10k of them have “healthy/unhealthy” labels
  - But all of them have pathologist report (which is not a doctor’s label) in English

• Approach will ideally learn to also take advantage of reports as weak labels
  - Combines image and text processing
  - Multiple problems possible, e.g. recognizing health problems from pathologist report (rather than Xrays)

• Data are from a company; algorithms may end up being employed in hospitals
  - Also, this is the largest real Xray data set of this kind
  - Potential for impactful publication
  - Your work is likely to be reported on by media sites, if you’re successful
Video summarization

• How to key in on the most important segments of a video recording
  - E.g. how do you key in on the most important segments of a game.

• One could work directly on the video stream, or alternately transcribe the images or speech and work off the text.

• Significant scope for contributions to state of art
  - but will be challenging
Video question answering

• Information retrieval and question answering from video data

• Significant prior art on the topic, but also significant scope for advancement of the state of the art
  - And publication
Category

• Adversarial modelling, model forensics
Generating Adversarial Examples

- Generate images / speech recordings that are unaltered to human perception but will fool Google voice / Alexa / Google Images
  - Some fun recent work: How to edit a malware-infected program so that the malware is not detected

- Both “whitebox”
  - You build the classifier

- And “blackbox”
  - You have no access to the classifier, e.g. alexa or google

- “Hot” area, scope for publication
  - Will require significant lit review
Resisting Adversarial Examples

• Training networks to *resist* adversarial examples

• At least somewhat theoretical

• Scope for publication
Identifying Adversarial Examples

• “Is this instance adversarially modified?”

• Scope for publication
Peering into a classifier

- Determine if a specific data instance has been used to train a network
  - “You used my photo to train your classifier”
Backdooring into a network

• Use “backdoor” training instances
  - Data poisoning

• Will permit fooling of network, but only if data provided in a specific way
  - E.g if the user wears a specific pair of glasses

• But will perform normally otherwise

• Some very interesting new work in this area by Dawn Song
Watermarking

• How to watermark your model
  - So that you can identify it if someone “steals” it
  - Even if they have modified it..

• Two variants:
  - Owner wants to know if it is indeed their model
  - A customer who has bought it needs to verify it

• Currently a “hot” area of research
Category

• Reinforcement learning
Multi-Agent Deep Reinforcement Learning for Co-operative and Competitive games

• Train multiple independent agents (policy networks) on simple mixed co-operative and competitive games.

• Challenge:
  - Flexibly allow for separate reward functions among agents to incorporate co-operative and competitive game aspects.
  - Overcome non-stationarity introduced by co-adapting independent policies in the multi-agent setting.

• Example game, *Physical deception*
  - $N$ agents cooperate to reach a single target landmark from a total of $N$ landmarks. They are rewarded based on the minimum distance of any agent to the target (so only one agent needs to reach the target landmark).
  - However, a lone adversary also desires to reach the target landmark; the catch is that the adversary does not know which of the landmarks is the correct one.
  - Thus the cooperating agents, who are penalized based on the adversary distance to the target, learn to spread out and cover all landmarks so as to deceive the adversary.
Deep Reinforcement Learning in Partially Observable Environments

• Train a deep RL agent under partial observability. May be limited access to the environment (e.g. constrained field of view) or noisy observations (e.g. cheap sensor).

• Challenge:
  - In most interesting sequential decision tasks, we usually don’t have access to the entire environment state at any given time.
  - Practical deep RL agents need to be able to estimate some “belief state” given a series of observations (think POMDP) to solve a task under partial observability.
  - Need to incorporate some form of “memory” in the belief state estimation (maybe an RNN or differentiable memory unit).

• Example:
  - First-person navigation of a maze environment. The task is to visit a number of landmarks hidden in different locations around the maze as quickly as possible.
Category

- Return to basics: Newer models
Alternative to current models

• E.g. can LSTMs replace Resnets?

• Can Attention replace every recurrent structure?