CS839 Special Topics in Deep Learning
Course Overview

Sharon Yixuan Li
University of Wisconsin-Madison

September 3, 2020
Part I: Logistics
Instructor

• Prof. Sharon Li

    Email: sharonli@cs.wisc.edu

    Office: 5393 Computer Sciences

    Virtual office hours: TBD

Use piazza for questions:

piazza.com/wisc/fall2020/cs839/home

For emails, please include [CS839] in the subject title!
Teaching Assistant

• Yiyou Sun

  Email: sunyiyou@cs.wisc.edu

  Virtual office hours: Tuesday 3-4pm (BB Collab)

  Piazza: piazza.com/wisc/fall2020/cs839/home
Course Enrollment

Course capacity: ~40 students due to
• Limited computing resources & first offering

Waiting list has >60 students
• Enroll on a first come first serve if registered students drop the course.
• This class will be offered again next fall!
This course will allow you to:

• **Advance** your knowledge in deep learning
  • In-depth read papers on cutting-edge topics of AI and deep learning

• **Project**
  • Explore new research directions and applications of deep learning
  • Ability to start original research in a collaborative team

• **Practice**
  • Write code in Python / Jupyter
  • Solve real problems
Course Schedule

- Time: **Tuesday** and **Thursday** 4:00-5:15pm CT
- Location: **BlackBoard Collaborate** for Fall 2020
- Schedule is available on the course website:
  
- Slides online on website
Prerequisites

• This course assumes that you already have a basic understanding of deep learning.

• Prerequisites
  • CS760: Machine Learning
  • (preferred) CS761: Mathematical Foundations of Machine Learning

• Familiarity with linear algebra, statistics, optimization is expected.
Textbooks


  https://www.deeplearningbook.org/front_matter.pdf

• *Dive into Deep Learning*. Aston Zhang and Zachary C. Lipton and Mu Li and Alexander J. Smola.

Course readings

- Most readings will be recent papers, articles and book chapters
- Available on course website (will be updated from time to time)

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Thursday, September 3</td>
<td>Course overview and introduction [Slides]</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tuesday, September 8</td>
<td>Neural Architecture Design I (lecture) [Slides]</td>
<td>Goodfellow-Bengio-Courville Chapter 6</td>
</tr>
</tbody>
</table>
| 2    | Thursday, September 10| Neural Architecture Design II (paper presentation) | Deep Residual Learning for Image Recognition  
Densely Connected Convolutional Networks (to present)  
Mask R-CNN                                             |
| 3    | Tuesday, September 15 | Neural Architecture Design III (paper presentation) | Neural Architecture Search with Reinforcement Learning  
Efficient Neural Architecture Search via Parameter Sharing |
| 3    | Thursday, September 17| Trustworthy Deep Learning I (lecture)       | Goodfellow-Bengio-Courville Chapter 7.5, 7.13                                    |
| 4    | Tuesday, September 22 | Trustworthy Deep Learning II (paper presentation) | Out-of-distribution Reliability  
Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images  
On Calibration of Modern Neural Networks  
Enhancing The Reliability of Out-of-distribution Image Detection in Neural Networks  
A Simple Unified Framework for Detecting Out-of-Distribution Samples and Adversarial Attacks  
Robust Out-of-distribution Detection via Informative Outlier Mining (to present) |
Grading scheme

- In-class quizzes: **10%** (you can skip up to 2 of them)
- Paper presentation: **20%**
- Project proposal: **10%** (2 pages, due end of September)
- Final project presentation: **15%**
- Final project report (written): **45%**
- No final exam
Paper presentation (20%)

- **Sign up today:** 2-3 students each presentation

[https://docs.google.com/spreadsheets/d/18hCfFDD3ahPJfed_nkk4nWtzzFnc_ynRqr10000RgX4](https://docs.google.com/spreadsheets/d/18hCfFDD3ahPJfed_nkk4nWtzzFnc_ynRqr10000RgX4)

---

**Course schedule:** [http://pages.cs.wisc.edu/~sharonl/courses/cs839_fall2019/schedule.html](http://pages.cs.wisc.edu/~sharonl/courses/cs839_fall2019/schedule.html)

* Each presentation group can have a maximum of 3 students. As a team, every student in the same group will receive the same score for the presentation.
* It’s up to the presentation team to arrange the presentation & scribes in a way that maximizes the outcome.

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Presenter 1 Name</th>
<th>Presenter 1 Email</th>
<th>Scribe person name</th>
<th>Scribe person email</th>
<th>Presenter 2 Name (optional)</th>
<th>Presenter 2 Email (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 10</td>
<td>Neural Architecture Design (+10% bonus in final grade)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 15</td>
<td>Neural Architecture Design (+5% bonus in final grade)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 22</td>
<td>Trustworthy Deep Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 24</td>
<td>Trustworthy Deep Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 29</td>
<td>Trustworthy Deep Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 13</td>
<td>Interpretable Deep Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 15</td>
<td>Interpretable Deep Learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 22</td>
<td>Deep Learning Generalization and Theory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 27</td>
<td>Deep Learning Generalization and Theory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 3</td>
<td>Learning with less supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 5</td>
<td>Learning with less supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 10</td>
<td>Learning with less supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 17</td>
<td>Lifelong learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 19</td>
<td>Lifelong learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>December 1</td>
<td>Deep generative modeling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>December 3</td>
<td>Deep generative modeling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Paper presentation (20%)

- Sign up **today:** 2-3 students each presentation
  - 1-2 persons will present and lead the discussion
  - Interactive discussion (everyone should do the reading ahead of class)
  - One person will take notes and synthesize the discussion
  - Compile three quiz questions for in-class testing (send to TA, who will upload to Canvas)
- First presentation (September 10) gets extra **10%** in final grade.

*Densely Connected Convolutional Networks by Gao et al. 2017*

- A great guide by Prof. Kayvon Fatahalian on giving clear talks:
  
  https://graphics.stanford.edu/~kayvonf/misc/cleartalktips.pdf

- Deadlines:
  - **Day before presentation:** email TA the slides + quiz questions by 6pm
  - **Day following the presentation:** email TA the notes by 6pm (10% per-day late penalty)
During class

- Start with quiz questions on Canvas (10-15mins)
  - You may skip up to 2 quizzes throughout the semester
- Presenter(s):
  - Time the presentation to last 1 hour, including QA
- All:
  - Ask questions during the presentation
Presentation rubric

• Technical:
  • Depth of content
  • Accuracy of content
  • Paper criticism
  • Discussion lead

• Soft presentation skills
  • Time management
  • Responsiveness to audience
  • Organization
  • Presentation aids (slides etc)
Project (70%)

- **Original work** in deep learning
  - Existing tools applied to novel problem
  - Novel algorithms/theory/tools
  - Choose research topic covered by this course.

- **Academic research process**
  - Research in a team (2-4 students)
  - End result is a paper/report (ICML template) + academic presentation
  - Ask instructor & TA for advice if you are stuck - we are here to help
Project (70%)

- 9/17 Register team (names, working title)
- 9/29 Project proposal (2 pages, excluding references)
- 10/1 or 10/6 Talk to instructor to discuss (5-min talk with 10-min discussion)
- 12/8-12/17 Final presentation & report

Start early (last minute projects often fail)!
Integrity

Any instance of sharing or plagiarism, copying, cheating, or other disallowed behavior will constitute a breach of ethics. Students are responsible for reporting any violation of these rules by other students, and failure to constitutes an ethical violation that carries with it similar penalties.
GPU access

- Every student enrolled will be granted access to instructional GPU servers.
- 4 servers (8 GPUs each) for ALL.
- Job submitted through SLURM to ensure fair resource usage.
- Recommend using 1 GPU at a time.
- Ask TA on Piazza for GPU related questions.
- Account will be deleted after the end of semester.
Part II: Topic Overview
Topics covered in this course

1. Neural architecture design
2. Trustworthy deep learning
3. Interpretable deep learning
4. Deep learning generalization and theory
5. Learning with less supervision
6. Lifelong learning
7. Deep generative modeling

Each topic will be covered by Lecture + Paper presentations (Overview & deep dive)
1. Evolution of neural net architectures

- **LeNet**
- **AlexNet**
- **Inception Net**
- **ResNet**
- **DenseNet**
1. Evolution of neural net architectures
1. Evolution of neural net architectures

- DenseNet
- NasNet

AutoML

[Zoph et al. 2017]
2. Trustworthy Deep Learning

Out-of-distribution reliability

**Closed-world:** Training and testing distributions match

**Open-world:** Training and testing distributions differ
2. Trustworthy Deep Learning
Out-of-distribution reliability

Food Image Classifier

This is “out of distribution”!
2. Trustworthy Deep Learning
Out-of-distribution reliability for safety-critical applications
2. Trustworthy Deep Learning
Adversarial Robustness

$x$

“panda”
57.7% confidence

[Goodfellow et al. 2015]
2. Trustworthy Deep Learning
Fairness / Group Robustness

Common training examples

Waterbirds
- y: waterbird
- a: water background

Test examples

- y: waterbird
- a: land background

CelebA
- y: blond hair
- a: female

MultiNLI
- y: contradiction
- a: has negation
  (P) The economy could be still better.
  (H) The economy has never been better.

- y: entailment
  a: no negation
  (P) Read for Slate’s take on Jackson’s findings.
  (H) Slate had an opinion on Jackson’s findings.

- y: entailment
  a: has negation
  (P) There was silence for a moment.
  (H) There was a short period of time where no one spoke.

[Sagawa et al. 2020]
THIS IS YOUR MACHINE LEARNING SYSTEM?

YUP! YOU POUR THE DATA INTO THIS BIG PILE OF LINEAR ALGEBRA, THEN COLLECT THE ANSWERS ON THE OTHER SIDE.

WHAT IF THE ANSWERS ARE WRONG?

JUST STIR THE PILE UNTIL THEY START LOOKING RIGHT.
3. Interpretable Deep Learning

The big picture

3. Interpretable Deep Learning

What

Why
3. Interpretable Deep Learning

[Selvaraju et al. 2016]
3. Interpretable Deep Learning

(a) Original Image  
(b) Guided Backprop ‘Cat’  
(c) Grad-CAM ‘Cat’  
(d) Guided Grad-CAM ‘Cat’  
(e) Occlusion map ‘Cat’  
(f) ResNet Grad-CAM ‘Cat’  

(g) Original Image  
(h) Guided Backprop ‘Dog’  
(i) Grad-CAM ‘Dog’  
(j) Guided Grad-CAM ‘Dog’  
(k) Occlusion map ‘Dog’  
(l) ResNet Grad-CAM ‘Dog’  

[Selvaraju et al. 2016]
4. Deep Learning Generalization and Theory

[Belkin et al. 2018]
5. Learning with less supervision

- **Fully Supervised**
  - CAT, DOG, FLOOR
  - ImageNet

- **Weakly Supervised**
  - A CUTE CAT COUPLE
  - #CAT
  - Instagram/Search

- **Self-supervised**
  - Images in the wild
6. Lifelong Learning

Machines that improve with experience and become “smarter” over time.

https://www.darpa.mil/news-events/2017-03-16
7. Deep Generative Modeling

4.5 years of face generation

2014
2015
2016
2017
2018

http://www.whichfaceisreal.com/methods.html
7. Deep Generative Modeling

Synthesize the images

http://www.whichfaceisreal.com/methods.html
7. Deep Generative Modeling

Style transfers

https://github.com/StacyYang/MXNet-Gluon-Style-Transfer
Part III: Get to know EVERYONE
Remember to sign up the paper presentation TODAY!
Thanks!