DSC190: Machine Learning with Few Labels



Zhiting Hu Lecture 1, September 27, 2024



HALICIOĞLU DATA SCIENCE INSTITUTE

Logistics

• Class webpage: http://zhiting.ucsd.edu/teaching/dsc190fall2024

DSC190-Fall2024

Logistics Lectures Homework Project



Machine Learning with Few Labels

Machine learning is about computational methods that enable machines to learn concepts from experience. Many of the successful results of machine learning rely on learning with massive amounts of data labels. However, in many real problems we do not have enough labeled data, but instead have access to other forms of experience, such as structured knowledge, constraints, feedback signals from the environment, auxiliary models from related tasks, etc. This course focuses on those learning settings with few labels. This course is designed to give students a holistic understanding of related problems and methodologies (such as **large language/multi-modal models, world models, self/weakly/un-supervised learning, transfer learning, meta-learning, reinforcement learning, adversarial learning, knowledge constrained learning, panoramic learning), different possible perspectives of formulating the same problems, the underlying connections between the diversity of algorithms, and open questions in the field. Students will read, present, and discuss papers, and complete course projects.**

Logistics



Instructor: Zhiting Hu Email: zhh019@ucsd.edu Office hours: Mon 3:30-4:30pm Location: HDSI 442



TA: Yuheng Zha Email: yzha@ucsd.edu Office hours: Thu 3:30-4:30pm Location: HDSI 437

- Discussion forum: Piazza
- Homework & writeup submission: Gradescope

- 2 Homework assignments (30% of grade)
- Paper presentation (20%)
- Course project (46%)
- Participation (4%)

- 2 Homework assignments (30% of grade)
 - Theory exercises, implementation exercises
 - 3 total late days without penalty
- Paper presentation (20%)
- Course project (46%)
- Participation (4%)

- 2 Homework assignments (30% of grade)
- Paper presentation (20%)
 - Each individual student will give an oral presentation on a research paper
 - 10 mins = 8 mins presentation + 2 mins QA (tentative)
 - Timing -- hard time constraint: if you run over the expected time limit (8min), there will be no QA session for your presentation, and thus no credits for the QA component
 - Critical thinking: discuss both strengths and limitations of the paper
 - Sign up in a google sheet (TBA)
 - Design quiz questions for audience
 - Peer grading: other students will rate and give feedback (5% of grade)
 - Starting later part of the quarter, after the class size is stabilized
- Course project (46%)
- Participation (4%)

- 2 Homework assignments (30% of grade)
- Paper presentation (20%)
- Course project (46%)
 - 3 or 4-member **team** to be formed and sign up in a google sheet (TBA)
 - Designed to be as similar as possible to researching and writing a conference-style paper:
 - Due to tight timeline, fine to use synthetic/toy data for proof-of-concept experiments + explanation of theory/intuition of why your approach is likely to work
 - **Proposal** : 2 pages excluding references (10%) -- due in 2 or 3 weeks (TBA)
 - Overview of project idea, literature review, potential datasets and evaluation, milestones
 - Midway Report : 4-5 pages excluding references (20%)
 - **Presentation** : oral presentation, 15-20mins (20%)
 - Peer grading (5%)
 - **Final Report :** 6-8 pages excluding references (50%)

- 2 Homework assignments (30% of grade)
- Paper presentation (20%)
- Course project (46%)
- Participation (4%)
 - Submission of quiz answers and feedback on paper/project presentations
 - Contribution to discussion on Piazza
 - Completion of mid-quarter and final course evaluation
 - Any constructive suggestions

Have Large Language Models (LLMs) Solved ML/AI?



What are a couple of meals I can make with this?

Based on the items visible in the fridge, here are a couple of meal ideas:

 Yogurt parfait: Layer yogurt, strawberries, and blueberries in a bowl or jar. Top with honey or nuts for added texture and flavor.
Carrot and hummus wrap: Spread hummus on a tortilla or wrap. Top with shredded carrots and any other desired veggies. Roll up and enjoy!



Sora

Have Large Language Models (LLMs) Solved ML/AI?



2) Carrot and hummus wrap: Spread hummus on a tortilla or wrap. Top shredded carrots and any other desired veggies. Roll up and enjoy!

ÖpenAl ol

Sora

GPT-4

Have Large Language Models (LLMs) Solved ML/AI?

A year ago

Blog

Introducing ChatGPT

We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests.

Try ChatGPT 7 Read about ChatGPT Plus

AI doomsday imagined by ChatGPT + DALL-E3



LLMs are great... but fundamentally limited



Language Reasoning Embodied Reasoning

Social Reasoning

• Language reasoning (e.g., math, logics, common sense, ...)



Language Reasoning Embodied Reasoning

Social Reasoning

• Language reasoning (e.g., math, logics, common sense, ...)

Here is a plan for surveying the mental health of Problem: Track the same undergraduate students on our campus. This year, we will group of students over time ask freshmen; next year, sophomores; the year after, juniors; and the year after that, seniors. Are there any problems with this plan?

GPT-4

 Longitudinal Data and Cohort Effects: This approach doesn't track the same group of students over time...
...

Language Reasoning Embodied Reasoning

Social Reasoning

• Language reasoning (e.g., math, logics, common sense, ...)

Human: Internal world model

- Physical common sense
- Object permanence
- Spatial relation (e.g., support)

GPT-4

Emily found a desk and place the cell phone on top of it. [Irrelevant Actions] ... putting the lime down next to the cell phone. [Irrelevant Actions] ... She final finally put an apple on the desk. How many items are there on the desk?

There are two items

(correct answer: three)

[Xiang et al., 2023. Language Models Meet World Models: Embodied Experiences Enhance Language Models]

Language Reasoning Embodied Reasoning

Social Reasoning

• Building embodied agents requires embodied reasoning





LLMs: Autoregressive plan generation



Language Reasoning Embodied Reasoning Social Reasoning

Human: strategic planning

- Internal world model to predict states
- Simulation of alternative plans
- Assess outcomes to refine/pick the best



• Building socially intelligent systems requires social reasoning



AI Coworkers



Al Assistants

Language

Reasoning





Embodied

Reasoning





Al Companions

🔵 Replika

How are you feeling?

7º -

• Social reasoning: understanding humans

Explain why this is funny

GPT-4V

... The final panel reveals the punchline: the robot has merely produced a pile of crumpled paper, just like the human did, suggesting that the robot also suffers from writer's block ... highlighting a situation where the human and the AI are equally challenged



Social Reasoning

• Social reasoning: understanding humans



Language Reasoning

Embodied Reasoning Social Reasoning

Does this person need help?

• Social reasoning: understanding humans

Social reasoning also requires a world model: Humans' actions are constrained by physics



Language

Reasoning

Does this person need help?



. . .

It looks like the person in the image is carrying a heavy load of boxes, which might suggest they are in the process of moving. While I can't determine the actual need for help without context or the ability to interact with the situation, Social Reasoning

Embodied

Reasoning

LanguageEmbodiedReasoningReasoning

Social Reasoning

• Social reasoning: understanding humans



Is the person on the right helping?

GPT-4V

• Social reasoning: understanding humans

Understanding humans ≠ understanding actions

Is the person on the right helping?

Language

Reasoning

The person on the right appears to be helping by holding the chair, probably to steady it or to move it into place. The way they are reaching out and positioning themselves suggests they are assisting the person who is reaching across the table.

Correct action: Holding the chair Wrong intent: Helping



Embodied Reasoning

Social Reasoning

• Social reasoning: Theory of Mind

Reasoning about hidden mental variables that drive observable actions





Social

Reasoning

Embodied

Reasoning

Goal: Sit down Belief: The chair was not moved

False belief

Language

Reasoning

caused by the person on the right

Towards A Holistic Landscape of QUESTION ANSWERING Situated Theory of Mind in Large Language Models Chuanyang Jin^{1,2} Yutong Wu³ Jing Cao² Jiannan Xiang⁴ Yen-Ling Kuo^{2,5} Jovce Chai Zigiao Ma Jacob Sansom **Run Peng** Zhiting Hu⁴ Tomer Ullman³ Antonio Torralba² Joshua B. Tenenbaum² Tianmin Shu^{2,6} Computer Science and Engineering Division, University of Michigan {marstin, jhsansom, roihn, chaijy}@umich.edu ¹New York University ²Massachusetts Institute of Technology ³Harvard University ⁴UC San Diego ⁵University of Virginia ⁶Johns Hopkins University

Theory of Mind Might Have Sponta

Authors: Michal Kosinski^{*1}

Affiliations:

¹Stanford University, Stanford, CA94305, USA

Social reasoning: Theory of Mind

Limitations in LLMs



Language

Reasoning

Social Reasoning

Embodied

Reasoning

Summary so far

 LLMs have limited language, embodied, and social reasoning abilities; not human-level yet

Language	Embodied	Social
Reasoning	Reasoning	Reasoning

Humans conduct model-based reasoning based on models of the world and agents



• Perceiving physical properties (e.g., materials, viscosity)





Stimuli from Vivian Paulun



• Predicting dynamics



Kubricht et al. (2017)



• Predicting dynamics



Kubricht et al. (2017)



• Predicting dynamics



Kubricht et al. (2017)



Model-based control/planning





Bates et al. (2015)



Model-based control/planning

Human tool use

Unlike model-free RL, humans can learn to use tools through just a few trials

Get the red ball into the green goal



Allen et al. (2020)



Model-based control/planning

Too use via model-based planning

Key is to use a world model to simulate the outcomes of possible plans

In the mind	
Sample	

Allen et al. (2020)



World models in robotics and embodied AI

- Model-based planning
- Model-based reinforcement learning



LeCun (2022)

World models in robotics and embodied AI



- World model as state transition probabilities
- Causal relationship between action and state change



Agent models

• An agent is more than just an object and actions


Agent models

• An agent is more than just an object and actions

Strengths

strong, weak

Goals

helping, hurting, escaping

Relationships

friends, enemies

Moral judgment

good guy, bully

Beliefs

he is locked, i am safe



(size / velocity / angle...) A big triangle moves back and forth, while a small triangle and a small circle rotate 360° ...

The minimum definition of an agent model







Formulation

Partially observable Markov decision process (POMDP)



Level-0 agent models for embodied reasoning







Goal: Office or coffee shop?

An observer





Model-based Theory of Mind

 $P(\text{mind}|\text{state, actions}) \propto \frac{P(\text{actions}|\text{state, mind})}{P(\text{mind})}$

Level-0 agent model



Model-based Theory of Mind

 $P(\text{mind}|\text{state, actions}) \propto \frac{P(\text{actions}|\text{state, mind})}{P(\text{mind})}$

Level-0 agent model

Human Behavior Prediction P(future actions|state, mind)

Human-Al Interaction

 $\pi(\operatorname{action}_{AI}|\operatorname{state},\operatorname{mind}_{AI},\operatorname{mind}_{\operatorname{human}})$

Higher-order agent models for *recursive* social reasoning





Summary so far: world models and agent models



Summary so far: world models and agent models



What is Machine Learning?

• Computational methods that enable machines to learn concepts and improve performance from **experience**.

Experience of all kinds



Type-2 diabetes is 90% more common than type-1







Data examples

Rules/Constraints

Knowledge graphs

Rewards

. . .

Auxiliary agents



Adversaries



Master classes

And all combinations thereof

Experience of all kinds



Adversaries

Master classes

Experience of all kinds



Type-2 diabetes is 90% more common than type-1







Data examples

Rules/Constraints

Knowledge graphs

Rewards

. . .

Auxiliary agents



Adversaries



Master classes

And all combinations thereof

Experience: (massive) data examples



Image classification



Machine translation



Language modeling (BERT, GPT-2, **GPT-3**, ...)

45TB of text data: CommonCrawl, WebText, Wikipedia, corpus of books, ...

Experience: (massive) data examples

TECH \ ARTIFICIAL INTELLIGENCE \

OpenAl's text-generating system GPT-3 is now spewing out 4.5 billion words a day

Robot-generated writing looks set to be the next big thing

By James Vincent | Mar 29, 2021, 8:24am EDT



Speak easy

Human scorers' rating* of Google Translate and human translation





Neural-network[†]

For the former secretary of state, this is to forget a month of bungling and convince the audience that Mr Trump has not the makings of a president

Phrase-based[†]

Source: Google

For the former secretary of state, it is a question of forgetting a month of muddles and convincing the audience that Mr Trump does not have the stuff of a president

The former secretary of state has to put behind her a month of setbacks and convince the audience that Mr Trump does not have what it takes to be a president

[The Economist]

*0=completely nonsense translation, 6=perfect translation [†]Machine translation

Privacy, security issues

Assistive diagnosis



Abnormal findings

• Expensive to collect/annotate

Controllable content generation



	Controlling writing style
Plain	LeBron James contributed 26 points, 8 rebounds, 7 assists.
	•
Elaborate	LeBron James rounded out the box score with an all around impressive performance, scoring 26 points, grabbing 8 rebounds and dishing out 7 assists.

Applications: personalized chatbot, live sports commentary production

• Expensive to collect/annotate

Controllable content generation



Source image

Generated images under different poses

Applications: virtual clothing try-on system

• Expensive to collect/annotate

Robotic control



• Difficult / expertise-demanding to annotate



Applications: test model robustness

• Difficult / expertise-demanding to annotate

Prompt generation: automatically generating prompts to steer pretrained LMs



• Specific domain Low-resource languages

~7K languages in the world



• Specific domain Low-resource languages

Written languages	All languages
(3.5K)	(7K)
Languages with	
NER Annotation	
(30?)	

[Figure courtesy: Dan Roth, CIS620]

• Specific domain Low-resource languages



• Specific domain Low-resource languages

	Written languages (3.5K)	All langua	ages (7K)
Languages with parallel text (100?) Languages with NER Annotation (30?)	Wikipedia languages (300)	Can we use the multilingual links in Wikipedia?	

• Specific domain

Question answering





QA based on car manual?



- Privacy, security issues
- Expensive to collect/annotate
- Difficult / expertise-demanding to annotate
- Specific domain

Machine learning solutions given few data (labels)

- How can we make more efficient use of data?
 - Clean but small-size
 - Noisy
 - Out-of-domain
- Can we incorporate other types of experience in learning?





Data examples

Rules/Constraints Knowledge graphs



Rewards

S.KS

Auxiliary agents





And all combinations thereof

Adversaries

Master classes

- Loss
- Experience
- Optimization solver
- Model architecture

 $\min_{\theta} \mathcal{L}$ (θ, \mathcal{E}) Ľ **Optimization** Loss Experience Model solver architecture

• Loss

This course does **not** discuss model architecture

- Experience
- Optimization solver
- Model architecture



- Loss
- Experience
- Optimization solver
- Model architecture

This course does not discuss model architecture

Model of certain architecture whose parameters are the subject to be learned, $p_{\theta}(x, y)$ or $p_{\theta}(y|x)$

- Neural networks
- Graphical models
- Compositional architectures

- Loss
- Experience
- Optimization solver
- Model architecture



This course does not discuss model architecture

Model of certain architecture whose parameters are the subject to be learned, $p_{\theta}(x, y)$ or $p_{\theta}(y|x)$

- Neural networks
- Graphical models
- Compositional architectures



Transformers

- Loss
- Experience
- Optimization solver
- Model architecture

This course does **not** discuss model architecture

Model of certain architecture whose parameters are the subject to be learned, $p_{\theta}(x, y)$ or $p_{\theta}(y|x)$

- Neural networks
- Graphical models
- Compositional architectures





Generative directed models



General CRFs

• Loss

This course discusses a little about optimization

- Experience
- Optimization solver
- Model architecture

Assuming you know basic procedures:

- (Stochastic) gradient descent
- Backpropagation
- Lagrange multiplier


Components of a ML solution (roughly)

- Loss This course discusses a lot of loss & experience
- Experience
- Optimization solver
- Model architecture

Core of most learning algorithms



Machine learning solutions given few data (labels)

- (1) How can we make more efficient use of data?
 - Clean but small-size, Noisy, Out-of-domain Ο
- (2) Can we incorporate other types of experience in learning?



diabetes is 90% more common than type-1

Type-2



Rules/Constraints Knowledge graphs



Auxiliary agents



Adversaries



And all combinations thereof

Rewards

Machine learning solutions given few data (labels)

- (1) How can we make more efficient use of data?
 - Clean but small-size, Noisy, Out-of-domain, ...
- Algorithms
 - **Supervised learning:** MLE, maximum entropy principle
 - **Unsupervised learning**: EM, variational inference, VAEs
 - **Self-supervised learning**: successful instances, e.g., BERT, GPT-3, contrastive learning, applications to downstream tasks
 - **Distant/weakly supervised learning:** successful instances
 - **Data manipulation:** augmentation, re-weighting, curriculum learning, ...
 - Meta-learning

Mostly first half of the course

Machine learning solutions given few data (labels)

- (2) Can we incorporate other types of experience in learning?
 - Learning from auxiliary models, e.g., adversarial models:
 - Generative adversarial learning (GANs and variants), co-training, ...
 - Learning from structured knowledge
 - Posterior regularization, constraint-driven learning, ...
 - Learning from rewards
 - Reinforcement learning: model-free vs model-based, policy-based vs valuebased, on-policy vs off-policy, extrinsic reward vs intrinsic reward, ...
 - Learning in dynamic environment (not covered)
 - Online learning, lifelong/continual learning, ...





... And all combinations thereof



Master cl



Second half of the course

Algorithm marketplace

Designs driven by: experience, task, loss function, training procedure ...



maximum likelihood estimation reinforcement learning as inference inverse RL data re-weighting active learning policy optimization reward-augmented maximum likelihood data augmentation softmax policy gradient label smoothing imitation learning actor-critic adversarial domain adaptation posterior regularization GANS knowledge distillation intrinsic reward constraint-driven learning generalized expectation prediction minimization regularized Bayes learning from measurements energy-based GANs weak/distant supervision

Where we are now? Where we want to be?

Та

• Alchemy vs chemistry





FI

Uup Lv

maximum likelihood estimation reinforcement learning as inference

Quest for more standardized, unified ML principles

Machine Learning 3: 253–259, 1989 © 1989 Kluwer Academic Publishers – Manufactured in The Netherlands

EDITORIAL

Toward a Unified Science of Machine Learning

[P. Langley, 1989]





REVIEW _____ Communicated by Steven Nowlan

A Unifying Review of Linear Gaussian Models

Sam Roweis*

Computation and Neural Systems, California Institute of Technology, Pasadena, CA 91125, U.S.A.

Zoubin Ghahramani*

. . .

Department of Computer Science, University of Toronto, Toronto, Canada

Physics in the 1800's

- Electricity & magnetism:
 - Coulomb's law, Ampère, Faraday, ...
- Theory of light beams:
 - Particle theory: Isaac Newton, Laplace, Plank
 - Wave theory: Grimaldi, Chris Huygens, Thomas Young, Maxwell
- Law of gravity
 - Aristotle, Galileo, Newton, ...









"Standard equations" in Physics



A "standardized formalism" of ML



Data examples

Type-2 diabetes is 90% more common than type-1

Constraints



Rewards A



Auxiliary agents



Adversaries



Imitation



- Panoramically learn from all types of experience
- Subsumes many existing algorithms as special cases

Will discuss in later in the class

Questions?