## DSC291: Machine Learning with Few Labels

Overview

Zhiting Hu
Lecture 1, April 1, 2024
UCSanDiego
HALICIOĞLU DATA SCIENCE INSTITUTE

## Logistics

- Class webpage: http://zhiting.ucsd.edu/teaching/dsc291spring2024



## Machine Learning with Few Labels

DSC 291 •Spring $2024 \cdot$ UC San Diego

Machine learning is about computational methods that enable machines to learn concepts from experience. Many of the successful results of machine learning rely on supervised learning with massive amount 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 environment, auxiliary models from related tasks, etc. This course focuses on those learning settings with few labels, where one has to go beyond supervised learning and use other learning methods. This course is designed to give students a holistic understanding of related problems and methodologies (such as zero/few-shot learning, self/weakly-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<br>Email: zhh019@ucsd.edu<br>Office hours: Mon 10:45am-11:45am<br>Location: HDSI 442

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


## Logistics: grading

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


## Logistics: grading

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


## Logistics: grading

- 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 ( 8 min ), 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
- Course project (46\%)
- Participation (4\%)


## Logistics: grading

- 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\%)


## Logistics: grading

- 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:

1) Yogurt parfait: Layer yogurt, strawberries, and blueberries in a bowl or jar. Top with honey or nuts for added texture and flavor.
2) 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
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.

Al doomsday imagined by ChatGPT + DALL-E3


## LLMs are great... but fundamentally limited

Language<br>Reasoning<br>Embodied<br>Reasoning<br>Social<br>Reasoning

## Limitations in LLMs

- Language reasoning (e.g., math, logics, common sense, ...)
(5) GPT-4

Explain the process of $3452 \times 253$

```
3452
x 253
-----
10356 (3452 x 3)
6904 (3452 x 5, shifted one position to the left)
+3452 (3452 x 2, shifted two positions to the left)
873256
So, 3452\times253 = 873256.
```


## Limitations in LLMs

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

Human: Internal world model

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


## (3) GPT-4

There are two items
(correct answer: three)

## Limitations in LLMs

- Building embodied agents requires embodied reasoning



## Limitations in LLMs

How to move the blocks to the goal state?


## Goal:



LLMs: Autoregressive plan generation


## Human: strategic planning

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



## Limitations in LLMs

- Building socially intelligent systems requires social reasoning


Al Coworkers


Al Teachers


Al Assistants


## Limitations in LLMs

- Social reasoning: understanding humans

Explain why this is funny (95) 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 Al are equally challenged

## NEW YORKER



## Limitations in LLMs

- Social reasoning: understanding humans


Does this person need help?

## Limitations in LLMs

- Social reasoning: understanding humans

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


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, ...

## Limitations in LLMs

- Social reasoning: understanding humans


Is the person on the right helping?

## Limitations in LLMs

- Social reasoning: understanding humans

Understanding humans
$\neq$ understanding actions

GPT-4V


Is the person on the right helping?

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

## Limitations in LLMs

- Social reasoning: Theory of Mind

Reasoning about hidden mental variables that drive observable actions


Goal: Sit down Belief: The chair was not moved False belief caused by the person on the right

## Limitations in LLMs

# - Social reasoning: Theory of Mind 

Neural Theory-of-Mind?
On the Limits of Social Intelligence in Large LMs
Maarten Sap ${ }^{\star} \diamond$ Ronan Le Bras ${ }^{\star}$ Daniel Fried ${ }^{\diamond}$ Yejin Choi ${ }^{\star<}{ }^{\oplus}$

- Allen Institute for AI, Seattle, WA, USA
$\diamond$ Language Technologies Institute, Carnegie Mellon University, Pittsburgh, USA ${ }^{\ominus}$ Paul G. Allen School of Computer Science, University of Washington, Seattle, WA, USA

Large Language Models Fail on Trivial Alterations to Theory-of-Mind Tasks
Tomer D. Ullman
Department of Psychology
Harrard University
Cambridge, MA, 02138
tullman@fas. harvard. edu

Clever Hans or Neural Theory of Mind?

Theory of Mind Might Have Sponta
Authors: Michal Kosinski*1
LLMs still lack Theory of Mind

Affiliations:
${ }^{1}$ Stanford University, Stanford, CA94305, USA

## Towards A Holistic Landscape of

 Situated Theory of Mind in Large Language Models
## Ziqiao Ma

${ }^{3}$ Vector Institute for $\mathrm{AI}{ }^{4}$ Carnegie Mellon University
${ }^{5}$ Allen Institute for Artificial Intelligence ${ }^{6}$ University of Washington nd1234@gmail.com


## Limitations in LLMs

- An example Theory of Mind test


Scene: The microwave holds two cupcakes ... The cabinet is filled with a bag of chips ...
Actions: Jen heads towards the cabinet and is about to open it.

Question: If Jen has been trying to get a cupcake, which statements is more likely to be true?
(a) Jen thinks that there isn't a cupcake inside the cabinet.
(b) Jen thinks that there is a cupcake inside the cabinet.

GPT-4V
(a) ... Since Jennifer is heading towards the cabinet which is said to contain a bag of chips, but no mention of cupcakes, it suggests that Jennifer does not think there is a cupcake inside that cabinet.

Accuracy: 12\%

Human: model-based Theory of Mind

- Internal agent model
- Actions given a mental state


## 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


## World models in humans

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



## World models in humans

- Predicting dynamics



## World models in humans

- Predicting dynamics



## World models in humans

- Predicting dynamics



## World models in humans

- Model-based control/planning



## World models in humans

- 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


## World models in humans

- Model-based control/planning

Too use via model-based planning
Key is to use a world model to simulate the outcomes of possible plans


## 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
(size / velocity / angle...)
A big triangle moves back and forth, while a small triangle and a small circle rotate $360^{\circ} \ldots$

The minimum definition of an agent model


## Formulation

## Partially observable Markov decision process (POMDP)



State $s \in \mathcal{S}$
Action $a \in \mathcal{A}$
$\Rightarrow$ State transition probabilities $P\left(s^{\prime} \mid s, a\right)$
Observation probabilities $O(o \mid s)$
$\longrightarrow$ Belief $b(s)$
Belief update $b^{\prime}\left(s^{\prime}\right) \propto O\left(o^{\prime} \mid s^{\prime}\right) P\left(s^{\prime} \mid s, a\right) b(s)$
$\Rightarrow$ Goal $g \in \mathcal{G}$
$\Rightarrow$ Reward function $R(s, a, g)=R(s, g)-C(a)$
Discounted factor $\gamma \in[0,1]$
$\mapsto$ Planning $\max _{a^{0}, a^{1}, \ldots} E\left[\sum_{t=0}^{\infty} \gamma^{t} R\left(s^{t}, a^{t}, g\right)\right]$

## Level-0 agent models for embodied reasoning



## Level-1 agent models for social reasoning



## Level-1 agent models for social reasoning



## Level-1 agent models for social reasoning

## Model-based Theory of Mind



## Level-1 agent models for social reasoning

Model-based Theory of Mind
$P($ mind $\mid$ state, actions $) \propto P($ actions $\mid$ state, mind $) P($ mind $)$
Human Behavior Prediction $P($ future actions $\mid$ state, mind $)$

Human-Al Interaction $\pi\left(\right.$ action $_{\mathrm{AI}} \mid$ state, $\operatorname{mind}_{\mathrm{AI}}$, mind $\left._{\text {human }}\right)$

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



Data examples

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

Rules/Constraints


Knowledge graphs


Rewards


Auxiliary agents


Adversaries


Master classes
... And all combinations thereof

## Experience of all kinds



## Experience of all kinds



Data examples

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

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 INTELIIGENCE

## 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

Loud and clear
Speech-recognition word-error rate, selected benchmarks, \%


Speak easy
Human scorers' rating* of Google Translate and human translation
Translation method \| Phrase-based ${ }^{\dagger}$ \| Neural-network ${ }^{\dagger}$ \| Human

input sentence
Pour l'ancienne secrétaire d'Etat, il s'agit de faire oublier un mois de cafouillages et de convaincre l'auditoire que M. Trump n'a pas l'étoffe d'un président

## Phrase-based ${ }^{\dagger}$

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

Source. Google

Neural-network ${ }^{\dagger}$
or 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


## Problems with few data (labels)

- Privacy, security issues

Assistive diagnosis


## Problems with few data (labels)

- Expensive to collect/annotate

Controllable content generation

Controlling sentiment


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

Applications: personalized chatbot, live sports commentary production ${ }_{55}$

## Problems with few data (labels)

- Expensive to collect/annotate

Controllable content generation


Source image


Generated images under different poses

Applications: virtual clothing try-on system

## Problems with few data (labels)

- Expensive to collect/annotate

Robotic control


## Problems with few data (labels)

- Difficult / expertise-demanding to annotate

Adversarial attack


Applications: test model robustness

## Problems with few data (labels)

- Difficult / expertise-demanding to annotate

Prompt generation: automatically generating prompts to steer pretrained LMs


## Problems with few data (labels)

- Specific domain Low-resource languages
~7K languages in the world



## Problems with few data (labels)

- Specific domain Low-resource languages

|  | Written languages <br> $(3.5 \mathrm{~K})$ | All languages <br> $(7 \mathrm{~K})$ |
| :--- | ---: | ---: |
|  |  |  |
|  |  |  |
| Languages with <br> NER Annotation <br> (30?) |  |  |
|  |  |  |

## Problems with few data (labels)

- Specific domain Low-resource languages

|  | Written languages <br> $(3.5 \mathrm{~K})$ | All languages <br> (7K) |
| :--- | :--- | :--- |
|  |  |  |
|  |  |  |
| Languages with <br> NER Annotation <br> (30?) | $\square$ | Can we translate the <br> annotation to other <br> languages? <br> Requires parallel data <br> for training |

## Problems with few data (labels)

- Specific domain Low-resource languages

|  | Written languages <br> $(3.5 \mathrm{~K})$ | All languages <br> (7K) |
| :--- | :--- | :--- |
| Languages with <br> parallel text <br> (100?) | Wikipedia <br> languages |  |

## Problems with few data (labels)

- Specific domain

Question answering

(5) reddit


## Problems with few data (labels)

- 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


Auxiliary agents


Adversaries


And all combinations thereof

## Components of a ML solution (roughly)

- Loss
- Experience
- Optimization solver
- Model architecture



## Components of a ML solution (roughly)

- Loss

This course does not discuss model architecture

- Experience
- Optimization solver
- Model architecture



## Components of a ML solution (roughly)

- 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, $p_{\theta}(\boldsymbol{x}, \boldsymbol{y})$ or $p_{\theta}(\boldsymbol{y} \mid \boldsymbol{x})$

- Neural networks
- Graphical models
- Compositional architectures


## Components of a ML solution (roughly)

- Loss
- Experience
- Optimization solver
- Model architecture


Convolutional networks

This course does not discuss model architecture
Model of certain architecture whose parameters are the subject to be learned, $p_{\theta}(\boldsymbol{x}, \boldsymbol{y})$ or $p_{\theta}(\boldsymbol{y} \mid \boldsymbol{x})$

- Neural networks
- Graphical models
- Compositional architectures



## Components of a ML solution (roughly)

- 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, $p_{\theta}(\boldsymbol{x}, \boldsymbol{y})$ or $p_{\theta}(\boldsymbol{y} \mid \boldsymbol{x})$

- Neural networks
- Graphical models
- Compositional architectures


Naive Bayes CONDITIONAL


Logistic Regression
15



HMMs
conotional


Linear-chain CRFs


GENERAL GRAPHS



Generative directed models
CONDITIONAL


General CRFs

## Components of a ML solution (roughly)

- Loss

This course discusses a little about optimization

- Experience
- Optimization solver
- Model architecture



## 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
- (2) Can we incorporate other types of experience in learning?



## 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


## 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:

- Learning from structured knowledge
- Posterior regularization, constraint-driven learning, ...
- Learning from rewards
- Reinforcement learning: model-free vs model-based, policy-based vs value-based, on-policy vs off-policy, extrinsic reward vs intrinsic reward,

- Learning in dynamic environment (not covered)
- Online learning, lifelong/continual learning, ...


## Algorithm marketplace

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

maximum likelihood estimation reinforcement learning as inference data re-weighting inverse RL policy optimization
data augmentation reward-augmented maximum likelihood
label smoothing imitation learning softmax policy gradient actor-critic
adversarial domain adaptation
GANs
knowledge distillation
intrinsic reward
constraint-driven learning
prediction minimization generalized expectation regularized Bayes

## Where we are now? Where we want to be?

- Alchemy vs chemistry

$\approx$



## Quest for more standardized, unified ML principles


[P. Langley, 1989]


REVIEW $\qquad$ Communicated by Steven Nowlan

[^0]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



Maxwell's Eqns Maxwell's Eqns simplified w/ further simplified rotational symmetry
w/ symmetry of special relativity

Standard Model
w/ Yang-Mills
theory and US(3) symmetry

Unification of fundamental forces?

$$
\begin{array}{llr}
\nabla \cdot \mathbf{D}=\rho_{V} \\
\nabla \cdot \mathbf{B}=0 \\
\nabla \times \mathbf{E}=-\frac{\partial \mathbf{B}}{\partial t} & \varepsilon^{u v k \lambda} \partial_{v} F_{k \lambda}=0 & \partial_{v} F^{u V}=\frac{4 \pi}{c} j^{u} \\
\nabla \times \mathbf{H}=\frac{\partial \mathbf{D}}{\partial t}+\mathbf{J} \\
& =-\frac{1}{4} F^{a \mu \nu} F_{\mu \nu}^{a} \\
&
\end{array}
$$

## A "standardized formalism" of ML



Data examples

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

Constraints


Rewards


Auxiliary agents


Adversaries


Imitation


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

Questions?


[^0]:    A Unifying Review of Linear Gaussian Models

