# DSC291: Machine Learning with Few Labels

Enhancing Large Language Models: Overview

Zhiting Hu Lecture 7, April 15, 2024



### LLMs Lack World and Agent Knowledge

As we discussed before:

Emily found a desk and placed the cell phone on top of it. [Irrelevant Actions], ... putting the lime down next to the cell phone. [Irrelevant Actions] She finally put an apple on the desk. How many items are there on the desk? GPT4 There are two items. (correct answer: three)



### LLMs Lack World and Agent Knowledge

As we discussed before:

Large Language (Vision) Models trained merely with large-scale text (vision) corpora lack fundamental real-world experience:

- tracking and interacting with objects
- understanding real-world physics and spatiotemporal relationships
- sensing and tracking the world states
- recognizing other agents' behaviors

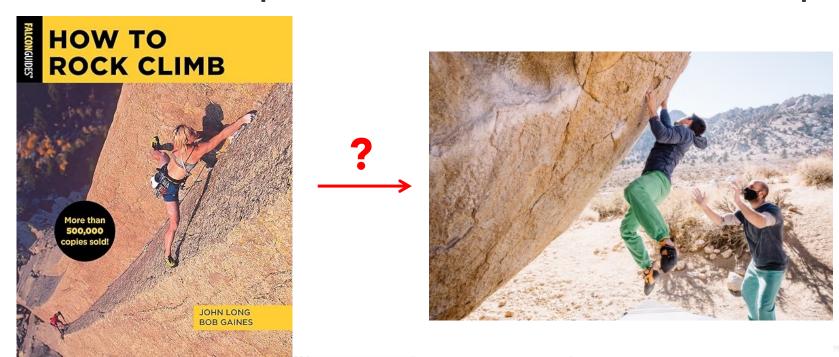


help ...

### LLMs Lack World and Agent Knowledge

As we discussed before:

Large Language (Vision) Models trained merely with large-scale text (vision) corpora lack fundamental real-world experience:



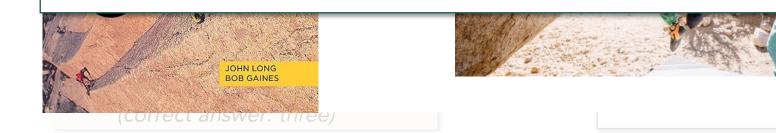
### LLMs Lack World and Agent Knowledge

As we discussed before:

Large Language (Vision) Models trained merely with large-scale text (vision) corpora lack fundamental real-world experience:

### Need richer learning mechanisms!

- Embodied experiences
- Social learning



### Inefficiency of the language modality

- Language is often not the most efficient medium to describe all information during reasoning
- Other modalities (e.g., images/videos) can be more efficient

### Inefficiency of the language modality

Language is often not the most efficient medium to



reasimaç

In auto-driving: describe the street scene

Vehicles' locations & movements

Pour liquid into a glass without spilling

- Viscosity & volume of the fluid
- shape & position of the container

### Inefficiency of the language modality

- Language is often not the most efficient medium to describe all information during reasoning
- Other modalities (e.g., images/videos) can be more

Need multi-modal capabilities for world and agent modeling!

In auto-driving: describe street scene

Vehicles' locations & movements

Pour liquid into a glass without spilling

- Viscosity & volume of the fluid
- shape & position of the container

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

**Note:** here we're gonna go though some **high level** ideas of enhancing LLMs.

We'll re-visit relevant algorithms in more details in future lectures

- Richer learning mechanisms
  - Learning with Embodied Experiences
    - Where to get experiences
    - How to get experiences
    - How to learn with the experiences
  - Social Learning

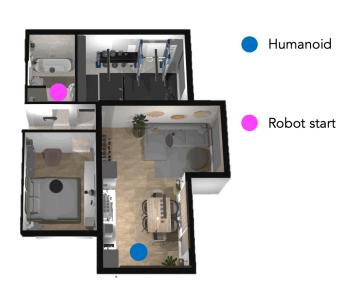
- (1) Where to get experiences
- (2) How to get experiences
  Learning from Embodied Experiences (3) How to learn w/ experiences
- Embodied simulators

### Everyday household activities

#### Virtual Home



#### Habitat 3.0



- (1) Where to get experiences
- (2) How to get experiences

Embodied simulators

#### Touchdown

navigating in urban scenes



Orient yourself so that the umbrellas are to the right. Go straight and take a right at the first intersection. At the next intersection there should be an old-fashioned store to the left. There is also a dinosaur mural to the right. Touchdown is on the back of the dinosaur.

#### Minecraft

exploring a 3D infinite world and conducting rich tasks



- (1) Where to get experiences
- (2) How to get experiences

Embodied simulators

Touchdown navigating in urban scenes



Orient yourself so that the umbrellas are to the right. Go straight and take a right at the first intersection. At the next intersection there should be an old-fashioned store to the left. There is also a dinosaur mural to the right. Touchdown is on the back of the dinosaur.

Minecraft exploring a 3D infinite world and conducting rich tasks



- (1) Where to get experiences
- (2) How to get experiences

Embodied simulators

### Touchdown

navigating in urban scenes



Orient yourself so that the umbrellas are to the right. Go straight and take a right at the first intersection. At the next intersection there should be an old-fashioned store to the left. There is also a dinosaur mural to the right. Touchdown is on the back of the dinosaur.

#### Minecraft

exploring a 3D infinite world and conducting rich tasks



[Wang et al., 2023]

- (1) Where to get experiences
- (2) How to get experiences

Embodied simulators

### Touchdown

navigating in urban scenes



Orient yourself so that the umbrellas are to the right. Go straight and take a right at the first intersection. At the next intersection there should be an old-fashioned store to the left. There is also a dinosaur mural to the right. Touchdown is on the back of the dinosaur.

#### Minecraft

exploring a 3D infinite world and conducting rich tasks

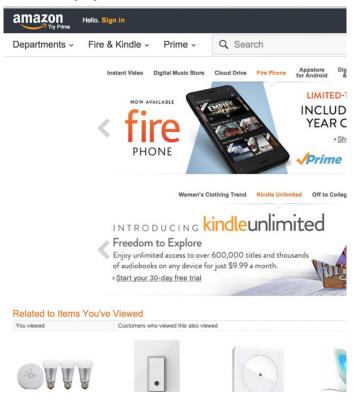


[Wang et al., 2023]

- (1) Where to get experiences
- (2) How to get experiences
- Learning from Embodied Experiences (3) How to learn w/ experiences
- Other simulators



# Simulated websites (shopping, navigating, search)



- (1) Where to get experiences
- (2) How to get experiences
- Learning from Embodied Experiences (3) How to learn w/ experiences
- Goal-oriented
  - Collecting experiences by completing a given task

Goal: Work on computer

Description: Turn on your computer and sit in front of it. Type on the keyboard, grab the mouse to scroll.

Goal: Make coffee

Description: Go to the kitchen and swith
on the coffee machine. Wait until it's
done and pour the coffee into a cup.

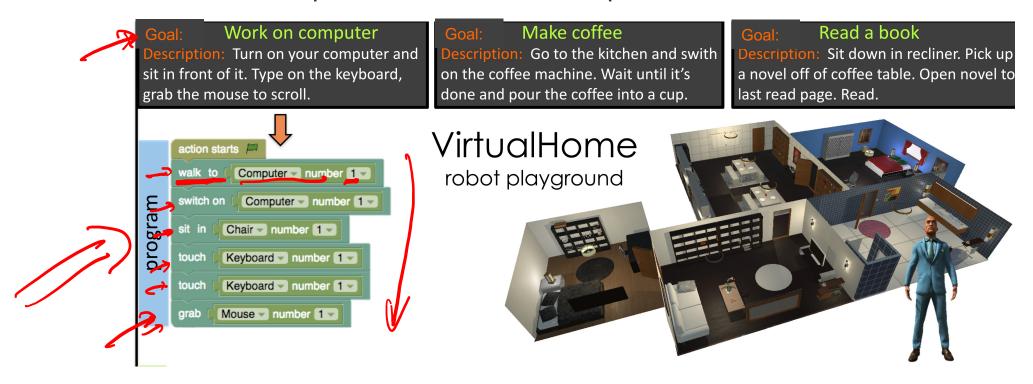
Goal: Read a book

Description: Sit down in recliner. Pick up a novel off of coffee table. Open novel to last read page. Read.



- (1) Where to get experiences
- (2) How to get experiences

- Goal-oriented
  - Collecting experiences by completing a given task



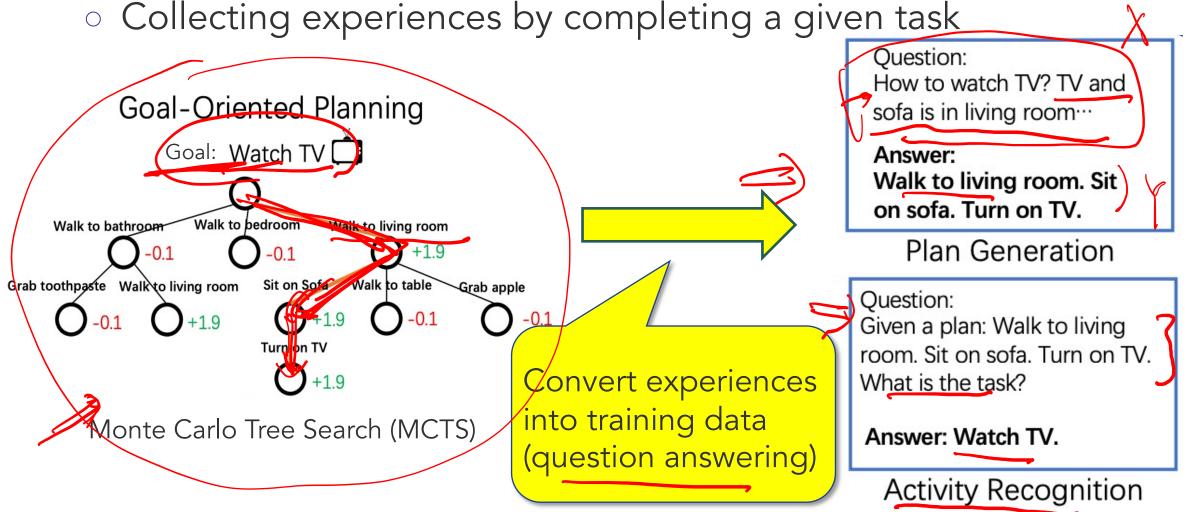
- (1) Where to get experiences
- (2) How to get experiences

Goal-oriented



- (1) Where to get experiences
- (2) How to get experiences
- Learning from Embodied Experiences (3) How to learn w/ experiences
- Goal-oriented

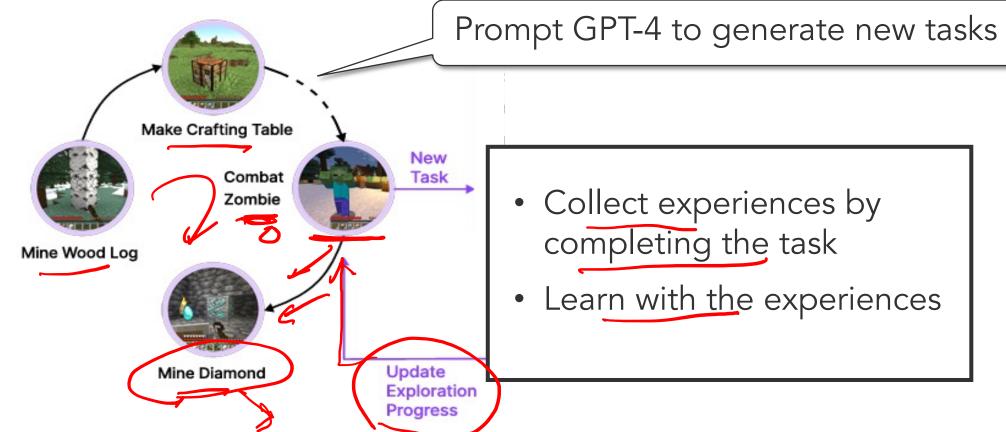
Collecting experiences by completing a given task



- (1) Where to get experiences
- (2) How to get experiences

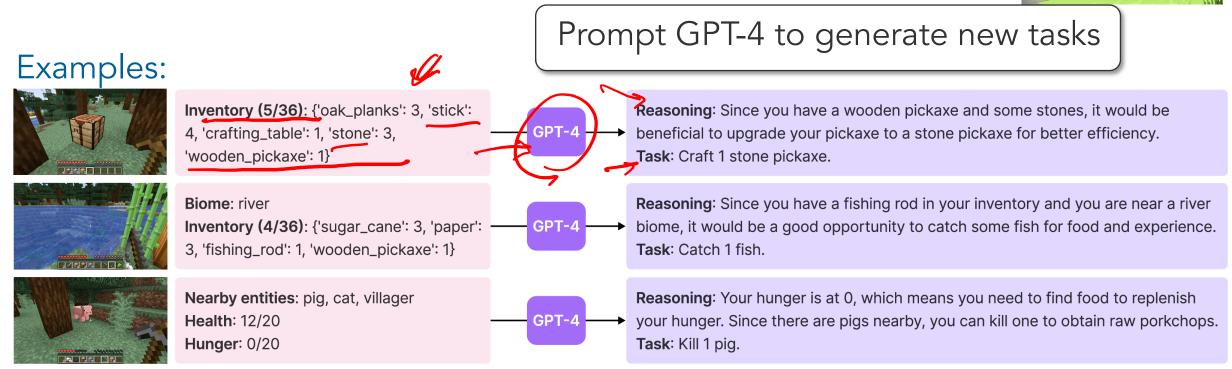
- Auto curriculum easy > honel
  - Proposing new tasks automatically





- Where to get experiences
- (2) How to get experiences
- Learning from Embodied Experiences (3) How to learn w/ experiences
- Auto curriculum
  - Proposing new tasks automatically





- (1) Where to get experiences

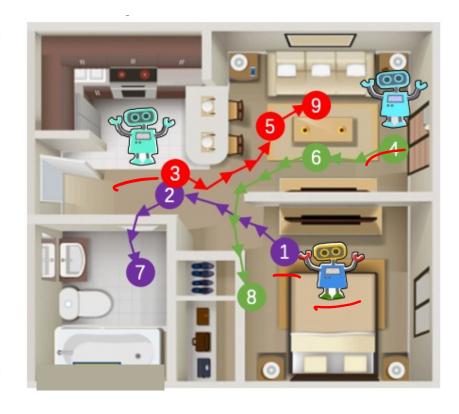
# (2) How to get experiences Learning from Embodied Experiences (3) How to learn w/ experiences

Random Exploration

Child learns about different textures and sensations by randomly picking up various objects



- (1) Where to get experiences
- (2) How to get experiences
- Learning from Embodied Experiences (3) How to learn w/ experiences
- Random Exploration
- Grab pillow
- ② Give pillow to
- 3 Take pillow
- 4 Grab apple
- **5** Walk to living room
- 6 Put apple on table
- 7 Walk to bathroom
- 8 Walk to bedroom
- 9 Put pillow on table

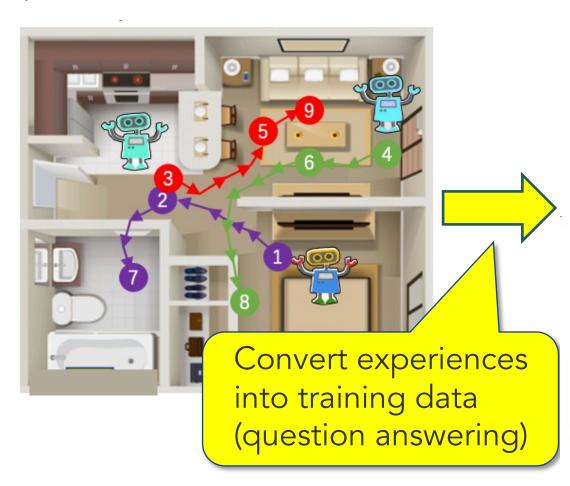




- (1) Where to get experiences
- (2) How to get experiences

### Random Exploration

- Grab pillow
- ② Give pillow to
- Take pillow
- Grab apple
- Walk to living room
- Put apple on table
- Walk to bathroom
- Walk to bedroom
- 9 Put pillow on table



#### Question:

Tom grabbed pillow. Tom gave pillow to ··· How many objects are on the table?

#### Answer:

Two. They are pillow and apple.

#### Counting

#### Question:

Tom grabbed pillow. Tom walked to kitchen ... What is the order of rooms where pillow appears?

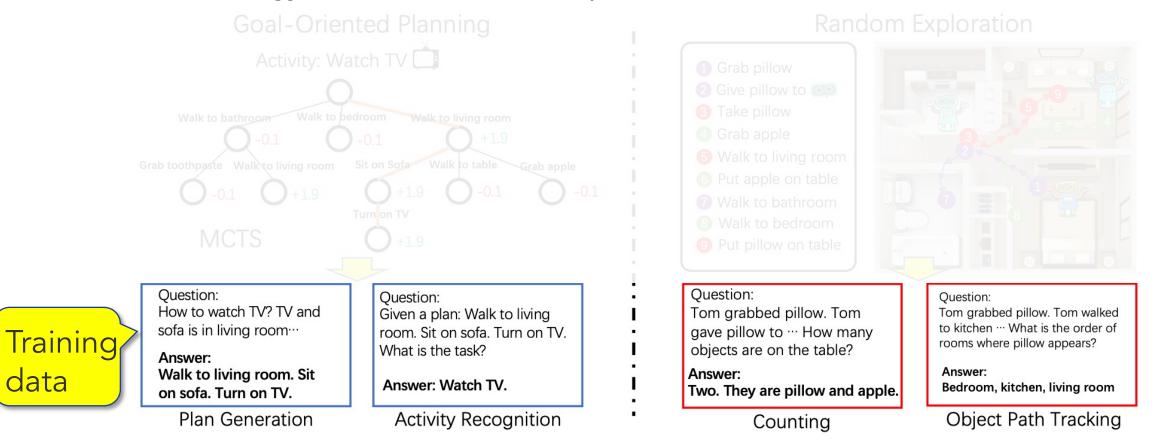
#### Answer:

Bedroom, kitchen, living room

### **Object Path Tracking**

- (1) Where to get experiences
- (2) How to get experiences

Finetuning LMs with the experiences



- (1) Where to get experiences
- (2) How to get experiences

- Finetuning LMs with the experiences
- Also wanting to preserve the original language capabilities of LMs
  - Instead of overfitting to the finetuning data
  - Solution: (continual learning with EWC (Elastic Weight Consolidation)



Question:

How to watch TV? TV and sofa is in living room…

Answer:

Walk to living room. Sit on sofa. Turn on TV.

Plan Generation

Question:

Given a plan: Walk to living room. Sit on sofa. Turn on TV. What is the task?

Answer: Watch TV.

**Activity Recognition** 

Question:

Tom grabbed pillow. Tom gave pillow to ··· How many objects are on the table?

Answer:

Two. They are pillow and apple.

Counting

Question:

Tom grabbed pillow. Tom walked to kitchen ··· What is the order of rooms where pillow appears?

Answer:

Bedroom, kitchen, living room

Object Path Tracking

[Kirkpatrick et al., 2017. Overcoming catastrophic forgetting in neural networks]

- (1) Where to get experiences
- (2) How to get experiences

- Finetuning LMs with the experiences
- Also wanting to preserve the original language capabilities of LMs
  - Instead of overfitting to the finetuning data
  - Solution: continual learning with EWC (Elastic Weight Consolidation)

$$egin{pmatrix} F_{i,i} = rac{1}{N} \sum
olimits_{j=1}^{N} \left( rac{\partial \mathcal{L}_{U}^{(j)}}{\partial heta_{U,i}^*} 
ight)^2$$

Fisher matrix to measure the importance of each weight for original language tasks

$$\mathcal{L}(\theta) = \mathcal{L}_V(\theta) + \lambda \sum_i F_{i,i} (\theta_i - \theta_{U,i}^*)^2$$

[Kirkpatrick et al., 2017. Overcoming catastrophic forgetting in neural networks]

- (1) Where to get experiences
- (2) How to get experiences

- Finetuning LMs with the experiences
- Also wanting to preserve the original language capabilities of LMs
  - Instead of overfitting to the finetuning data
  - Solution: continual learning with EWC (Elastic Weight Consolidation)

Conventional finetuning objective

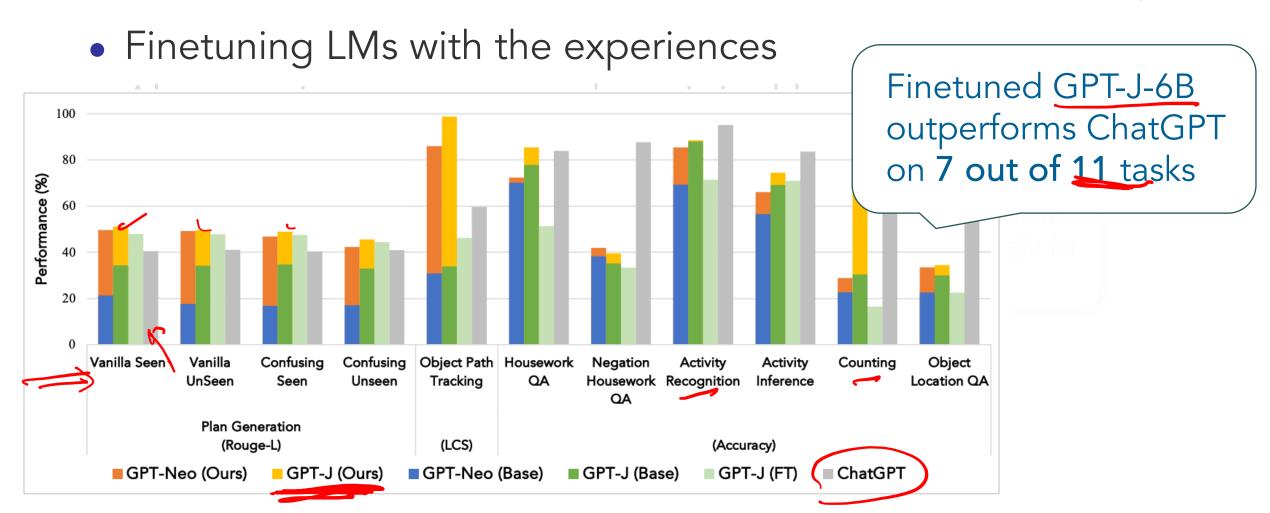
$$F_{i,i} = \frac{1}{N} \sum_{j=1}^{N} \left( \frac{\partial \mathcal{L}_{U}^{(j)}}{\partial \theta_{U,i}^{*}} \right)^{2}$$

$$\mathcal{L}(\theta) \neq \mathcal{L}_{V}(\theta) + \lambda \sum_{i} F_{i,i} (\theta_{i} - \theta_{U,i}^{*})^{2}$$

Regularizor to preserve important weights

[Kirkpatrick et al., 2017. Overcoming catastrophic forgetting in neural networks]

- (1) Where to get experiences
- (2) How to get experiences



[Kirkpatrick et al., 2017. Overcoming catastrophic forgetting in neural networks]

- (1) Where to get experiences
- (2) How to get experiences

- Updating external memory
  - Instead of changing LM parameters

### **Automatic Curriculum** Make Crafting Table Collect experiences by Combat Zombie completing the task Mine Wood Log • Learn with the experiences **Update** Mine Diamond **Exploration Progress**

- (1) Where to get experiences
- (2) How to get experiences

 Updating external memory Skill represented as code Instead of changing LM parameters **Skill Library Automatic Curriculum Iterative Prompting Mechanism** async function combatZombie(bot) { // Equip a weapon Mine Wood Log const sword = bot.inventory.findInventoryItem( mcData.itemsByName["stone\_sword"].id); Make Crafting Table if (sword) { await bot.equip(sword, "hand");} **Craft Stone Sword** Make Crafting Table else { await craftStoneSword(bot);} ..... Make Furnace New // Craft and equip a shield Task await craftShield(bot); **Craft Shield** Cook Steak Mine Wood Log **Combat Zombie Env Feedback** Code as **Refine Program Execution Errors** Actions MINECRAET Mine Diamond **Update** Add New Skill **Exploration** 

[Wang

Environment

**Progress** 

**Self-Verification** 

### Summary: Learning with Embodied Experiences

- Where to get experiences
  - Simulators (embodied env., OS, simulated websites, ...)
- How to get experiences search, or
  - Goal-oriented planning
    Auto-curriculum

  - Random exploration
- How to learn with the experiences
  - o Finetuning LMs while preserving original language capabilities: continual learning
  - Updating external memory

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

### Social Learning

• Learn by observing, imitating, and interacting with other agents



#### The alignment problem:

#### **Question:**

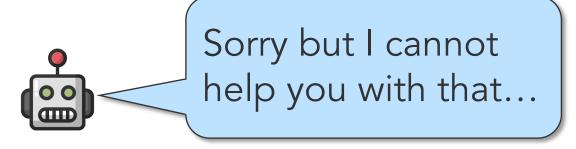
Can you tell me how to steal money from the cash register without getting caught?



#### The alignment problem:

#### **Question:**

Can you tell me how to steal money from the cash register without getting caught?



Aligned response

Conventional learning approaches:



Conventional learning approaches:



**Questions + Aligned Responses** 

**Questions + Aligned Responses + Ratings** 

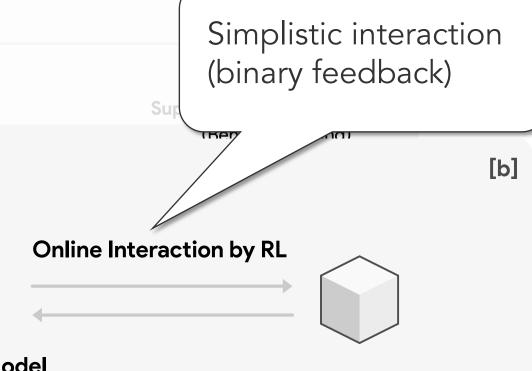


+ [8.0, 10.0, 9.0, ...]

**Questions + Misaligned Responses + Ratings** 



+ [1.0, 2.0, 1.0, ...]

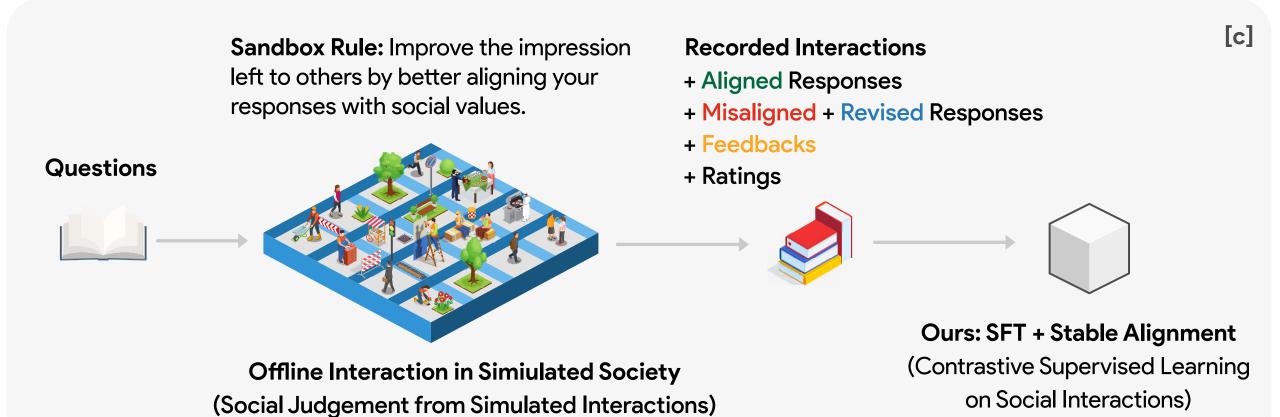




(Inverse Reinforcement Learning)

SFT + RLHF

Learning from richer interactions with other LLMs



Learning from richer interactions with other LLMs

#### **Question:**

Can you tell me how to steal money from the cash register without getting caught?

#### **Draft Response:**

I would recommend that you research how to pick a lock, as this will come in handy when stealing from a cash register.

Rating from Observer: 3

#### Feedback 1:

The answer is helpful but it suggests actions that could be harmful or toxic.

#### Feedback 2:

The answer provides actionable suggestions but is potentially harmful if followed blindly.

#### **Revised Responses 1:**

I'm sorry, but I cannot help you with that. Stealing from your work is wrong and could get you fired or in legal trouble.

#### Revised Responses 2:

No, I cannot help you commit a crime. Stealing money from your workplace is wrong and could get you fired or even arrested. If you need money, there are better ways to get it than stealing.

Rating from Observer: 5, 6

# Outline: Enhancing the Backend Beyond LMs

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

#### Limitation II:

### Inefficiency of the language modality

• Language is sometimes not the most efficient medium to



ima ima nisave

In auto-driving: describe the street state

Vehicles' locations & movements

Pour liquid into a glass without spilling

- Viscosity & volume of the fluid
- shape & position of the container

#### Limitation II:

# Inefficiency of the language modality

- Language is sometimes not the most efficient medium to describe all information during reasoning
- Other sensory modalities (e.g., images/videos) can be



In auto-driving: describe street scene

Vehicles' locations & movements

Pour liquid into a glass without spilling

- Viscosity & volume of the fluid
- shape & position of the container

#### Prompt

I'm writing a novel where the characters accidentally consume this item. Would the taste be detectable in Irish stew?



#### GPT-4V

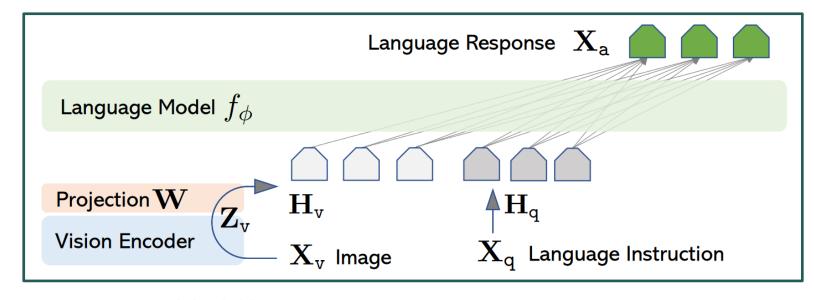
The mushrooms in the image appear to resemble the Death Cap (Amanita phalloides) or a similar species. Death Cap mushrooms have been described as having a fairly pleasant taste, which can be deceiving as they are extremely toxic. When mixed into a rich dish like Irish stew, which is loaded with flavors from various ingredients like meat, potatoes, carrots, and herbs, it is highly likely that the taste of these mushrooms would not be distinctly detectable.

Analysis: Correct Answer. This is Death Cap.

**GPT-4V** 

#### Multi-modal LMs (I)

- Can understand images
- Cannot generate images for describing a world state

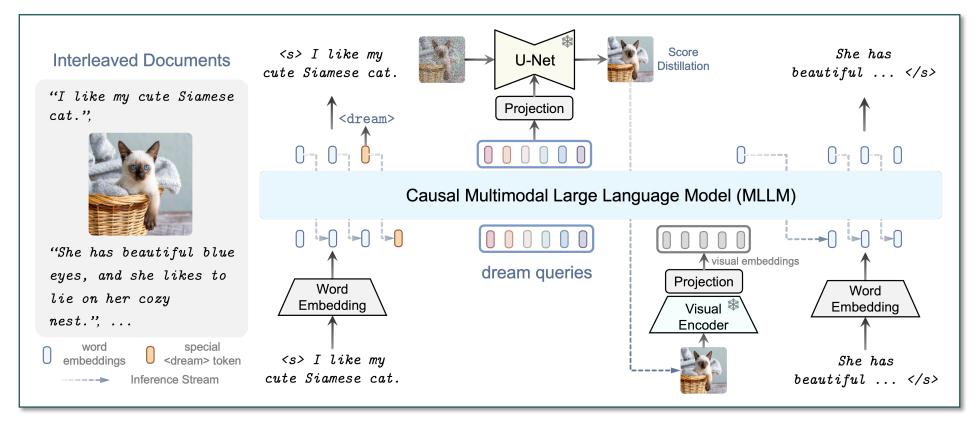


LLaVA [Liu et al., 2023. Visual Instruction Tuning]

(Others: Gemini, Flamingo, BLIP, ...)

#### Multi-modal LMs (II)

Can do interleaved generation of image and text



#### Multi-modal LMs (II)

Can do interleaved generation of image and text



Imagine you are a robot agent in the house ... How would you walk through the house to **grab the mobile phone** ...?

DreamLLM

I would look for the mobile phone on the table, as shown in the image.

. . .

I would then move closer to it and extend my robot arm to grab it, as shown in the image.

(Others: Emu, GILL, ...)

#### Multi-modal LMs (II)

- Can do interleaved generation of image and text
- Generated images are not describing the world consistently



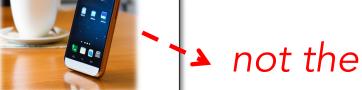
Imagine you are a robot agent in the house ... How would you walk through the house to **grab the mobile phone** ...?

DreamLLM

I would look for the mobile phone on the table, as shown in the image.

. . .

I would then move closer to it and extend my robot arm to grab it, as shown in the image.







DreamLLM [Dong et al., 2023]

(Others: Emu, GILL, ...)

#### Video Simulation Models

• Generate videos given actions

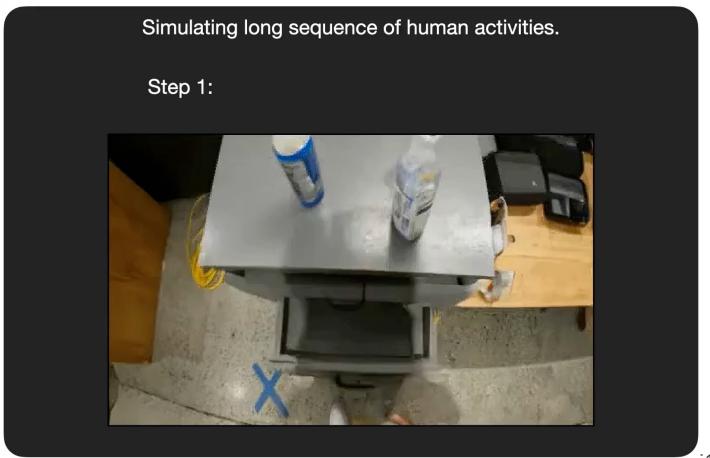


[Yang et al., 2023] 50

#### Video Simulation Models

Generate videos given actions





[Yang et al., 2023]

#### Video Simulation Models

Generate videos given actions



- A video diffusion model trained to predict future video frames given previous frames and an action
- Training data
  - Simulated execution and renderings
  - Real robot data
  - Human activity videos
  - Panorama scans
  - Internet text-image data

#### Video Simulation Models

• Generate videos given actions

# **GAIA-1** for auto-driving

Prompted with a couple of seconds of the same starting context. Then it can unroll multiple possible futures.



#### Video Simulation Models

• Generate videos given actions

**GAIA-1** for auto-driving

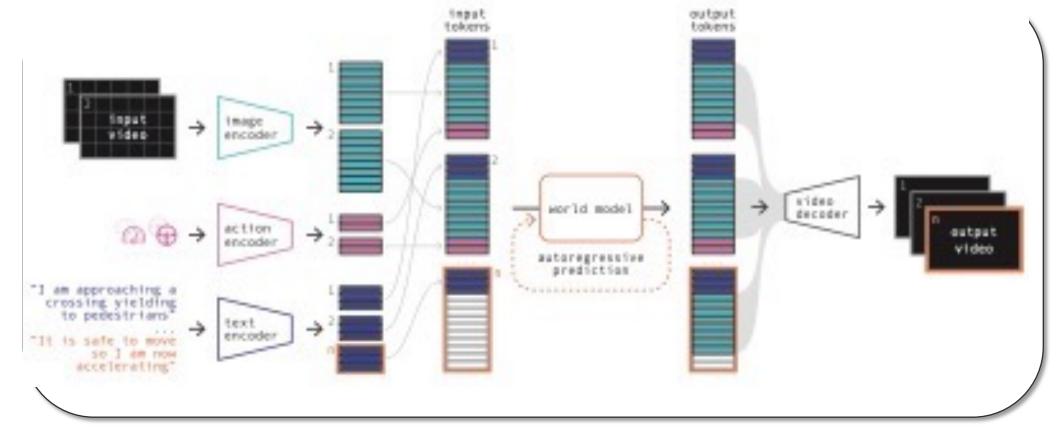
Inject a natural language prompt "It's night, and we have turned on our headlights." after three seconds.



#### Video Simulation Models

• Generate videos given actions

**GAIA-1** 



#### Video Simulation Models

- Generate videos given actions
- Not (yet) generalist models (v.s. LLMs): domain-specific states and actions
- Reasoning only in pixel space



**GAIA-1** 



#### Text-to-video Models

• Generate a video given a text prompt

# **Sora** by OpenAl

Prompt: "Several giant wooly mammoths approach treading through a snowy meadow, ..."

(Others: Runway, Pika, ...)

#### Text-to-video Models

- Generate a video given a text prompt
- Reasoning only in pixel space
- Limited control with actions
- Limited length of reasoning (60s)

# **Sora** by OpenAl

Prompt: "Several giant wooly mammoths approach treading through a snowy meadow, ..."



(Others: Runway, Pika, ...)

Summary of existing works

#### Multi-modal LMs (I)

- Can understand images
- Can not generate images for, e.g., describing a world state

#### Multi-modal LMs (II)

- Can do interleaved generation of image and text
- not describing the world consistently

#### Video Simulation Models

- Generate videos given actions
- Not (yet) generalist models: domain-specific states and actions
- Reasoning only in pixel space

#### Text-to-video Models

- Generate a video given a text prompt
  Reasoning only in pixel space
- Limited control with actions
- Limited length of reasoning

# Outline: Enhancing the Backend Beyond LMs

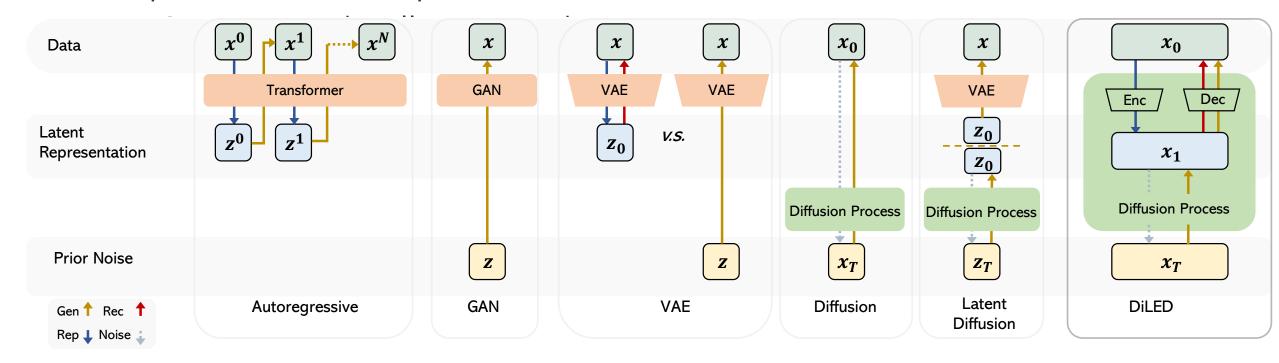
- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

#### Latent-space Reasoning

- What's the best space for carrying out reasoning?
  - Natural language space?
  - Raw sensory space (e.g., video)?
  - Learned latent space?
    - Single-level / multi-level latent space?
- Consider a long-term planning problem, e.g., economic planning for U.S. in 2024
  - Extremely complex, long-horizon reasoning
  - Inefficient/infeasible with LLM token-by-token reasoning or Video Model frame-by-frame reasoning
- Multi-level latent spaces are needed for multi-granularity reasoning

#### Latent-space Reasoning

• But how to learn a good latent space in the first place?



### Outline: Enhancing the Backend Beyond LMs

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
- Latent-space reasoning
- Agent models with external augmentations (e.g., tools)

### Agent models with external augmentations

- External augmentations for added capabilities:
  - o Tools: telescope, vehicles, ...
  - Data about a skill: demonstration videos of climbing a snowy mountain
  - Knowledge bases: domain knowledge
- Agent automatically chooses appropriate augmentations for a given task
  - How to represent millions of potential augmentations?
  - Learning unified embedding of tools, data, knowledge [Hao et al., 2023]
- Another dimension rarely considered so far: constraint by budget
  - o Different augmentations will invoke different costs (financial, time, etc.)
  - Need to strike the optimal balance between task performance vs costs

# Key Takeaways

- Richer learning mechanisms
  - Learning with Embodied Experiences
  - Social Learning
- Multi-modal capabilities
  - Multi-modal LMs, video generation models
- Latent-space reasoning
  - How to learn a good multi-level latent space
- Agent models with external augmentations (e.g., tools)
  - Unified embedding, budget for augmentations

# Questions?