

# Multimodal AI

## Lecture 10.2 – Interactive Agents

**Paul Liang**

Assistant Professor

MIT Media Lab & MIT EECS



<https://pliang279.github.io>

[ppliang@mit.edu](mailto:ppliang@mit.edu)

 [@pliang279](https://twitter.com/pliang279)



# Assignments for This Coming Week

Midterm exam grades: mean 84.2, median is 85.7

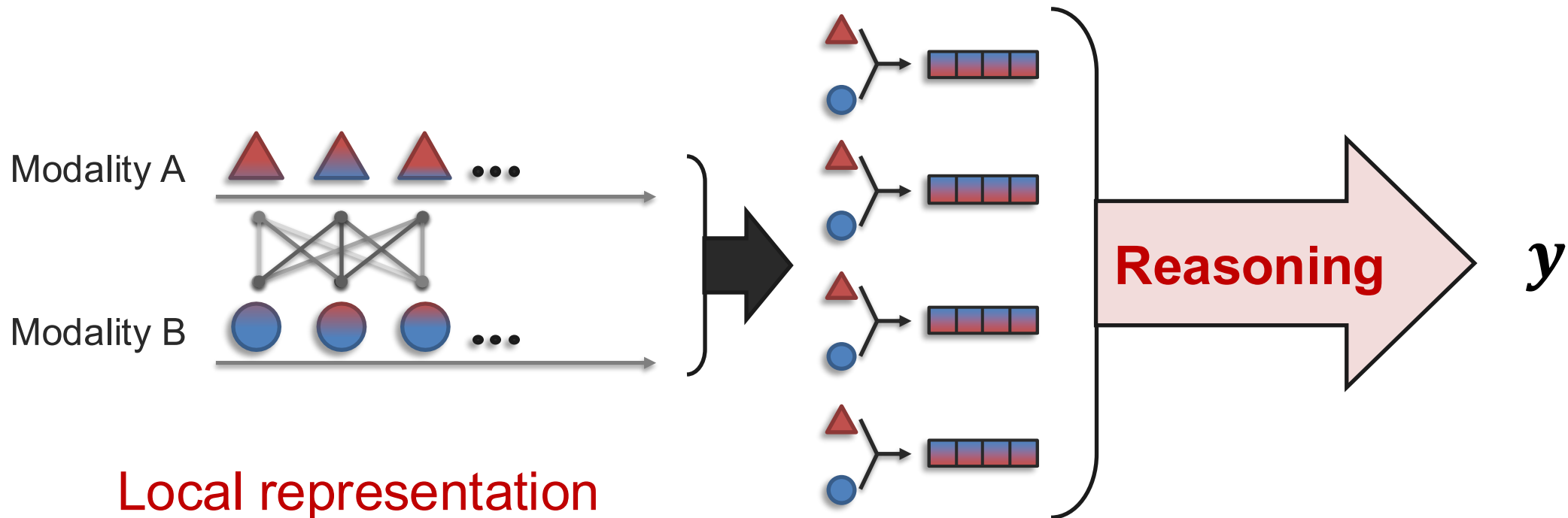
Project midterm due.

- Finalized main ideas and experimental setup, have datasets and baseline models working, detailed error analysis, initial progress towards implementing new ideas.

HW4 out tomorrow, on RL and reasoning.

# Reasoning

**Definition:** Combining knowledge, usually through multiple inferential steps, exploiting the structure of the problem.



Local representation  
+ Aligned representation

# Roadmap

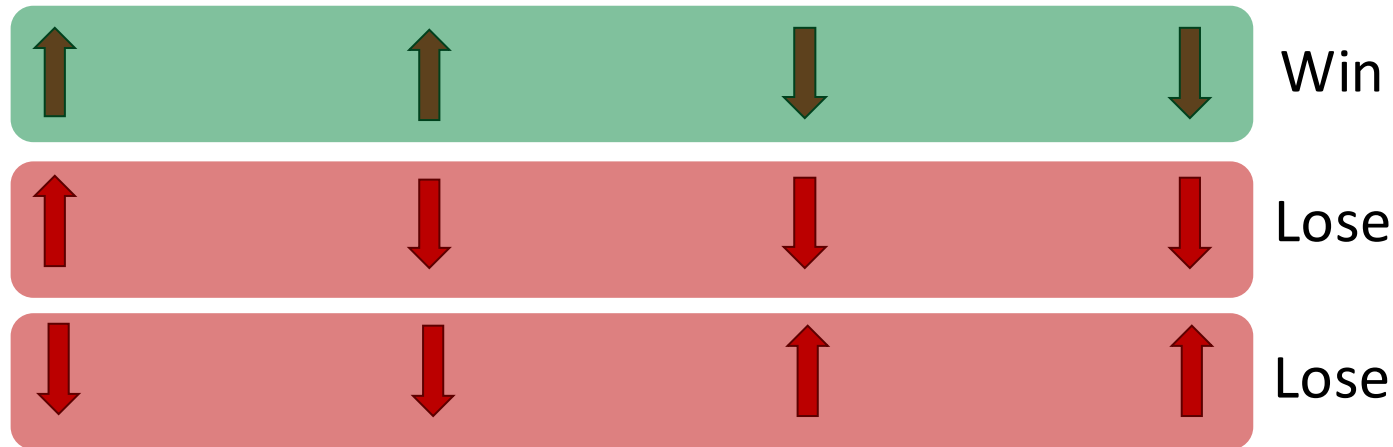
**Input, (reasoning step 1, step 2, step 3...), output**

Method 1: Direct prompting, no training (e.g., CoT)

Method 2: Supervised fine-tuning  
- Assuming you have reasoning traces

Method 3: Reinforcement learning  
- Assumes no reasoning traces  
- But a reward function scoring reasoning and outputs

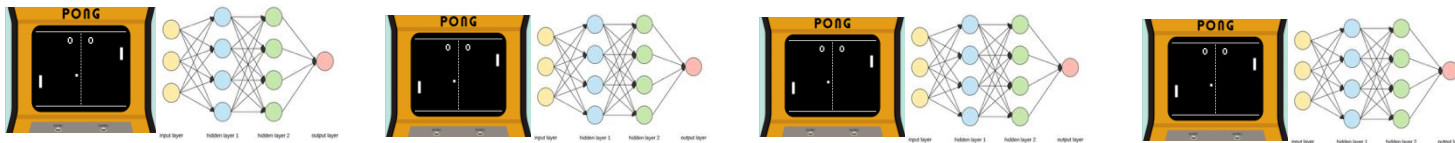
# Policy Gradients



Maximize  $\sum_i r_i \log p(y_i | x_i)$

Maximize  $\sum_i r_i \log p(y_i | x_i)$

Maximize  $\sum_i r_i \log p(y_i | x_i)$



# Policy Gradients

$$\nabla_{\theta} J(\theta) \approx \sum_{t \geq 0} r(\tau) \nabla_{\theta} \log \pi_{\theta}(a_t | s_t)$$

If  $r(\tau)$  is positive, increase the probability

If  $r(\tau)$  is negative, decrease the probability

But this suffers from high variance

# Policy Gradients

The raw reward may not be very meaningful.

**What is important then?** Whether a reward is higher or lower than what you expect.

-- Compare to a baseline, and use relative improvement

$$\nabla_{\theta} J(\theta) \approx \sum_{t \geq 0} (r(\tau) - b(s_t)) \nabla_{\theta} \log \pi_{\theta}(a_t | s_t)$$

e.g. exponential moving average of the rewards.

# GRPO (Deepseek R1)

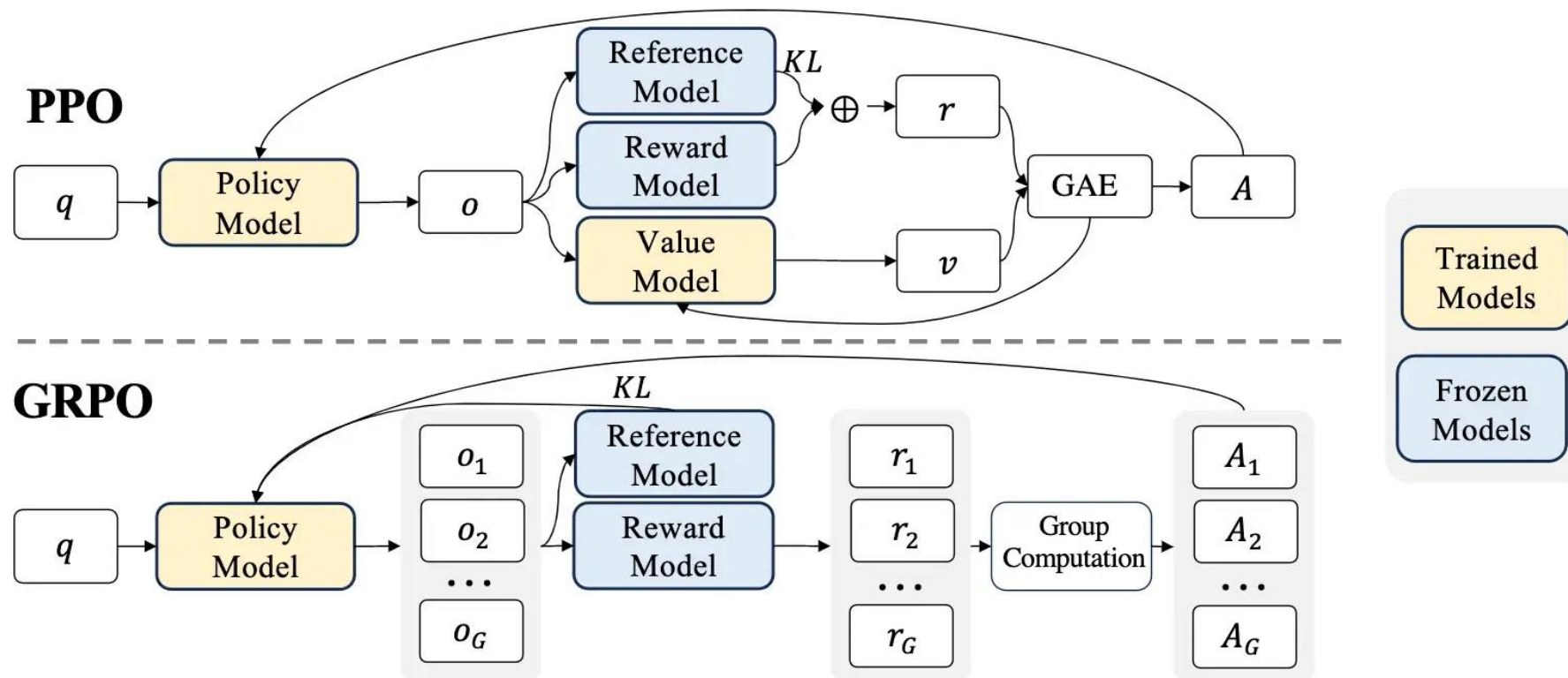
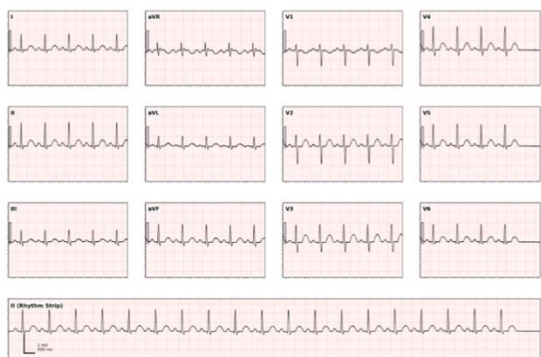
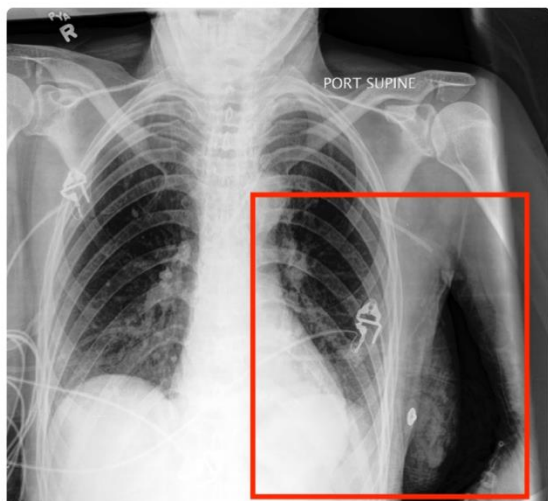


Figure 4 | Demonstration of PPO and our GRPO. GRPO foregoes the value model, instead estimating the baseline from group scores, significantly reducing training resources.

# Reasoning Examples

[https://github.com/DDVD233/QoQ\\_Med](https://github.com/DDVD233/QoQ_Med)

## Unified reasoning across images and medical sensors



**Question:** Below is a history of a patient:...How long will the patient stay in the hospital?

A. 0-4 days B. 5-8 days C. 9-12 days D. more than 12 days

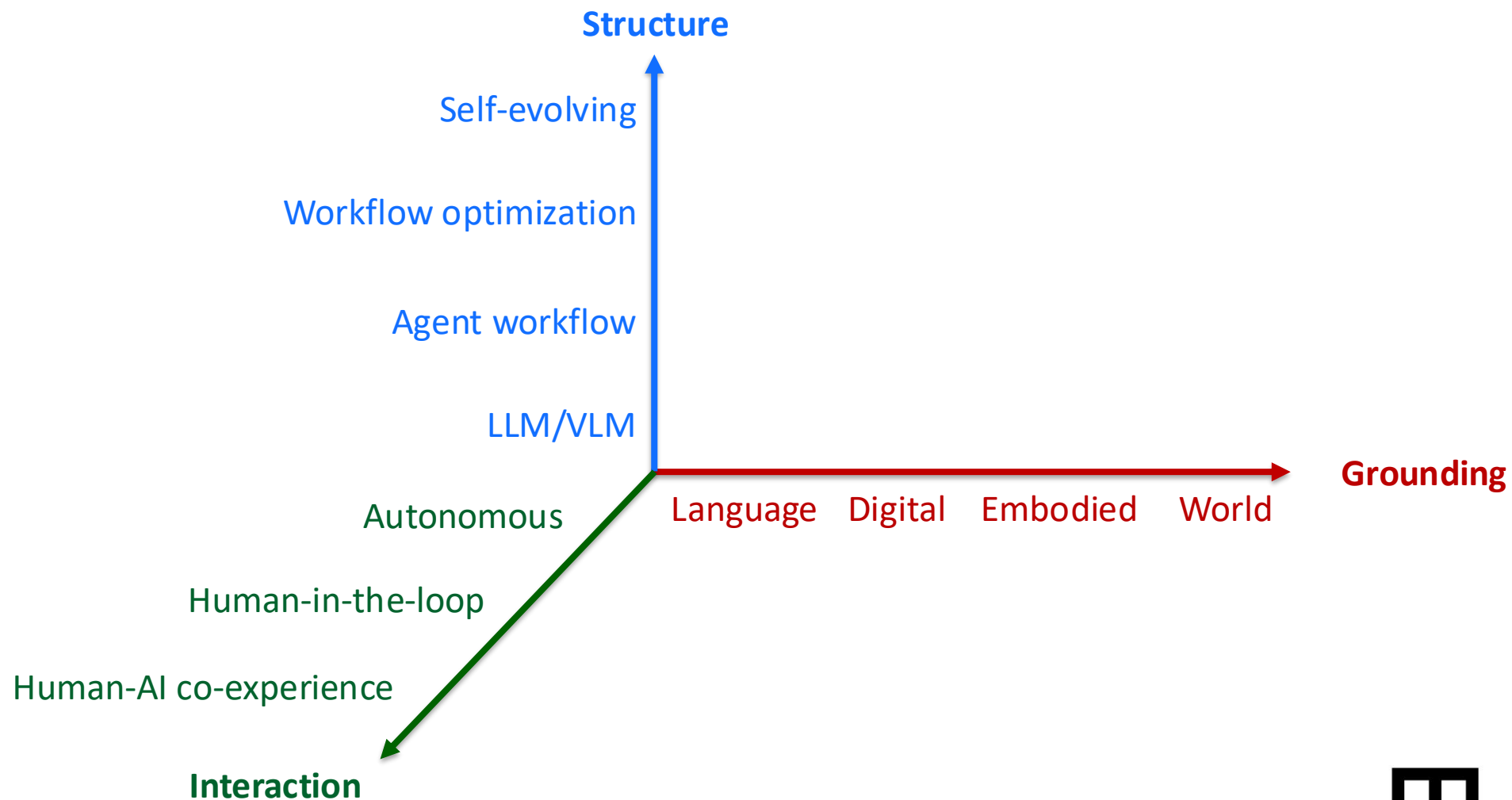
**Ground truth:** D. more than 12 days

### Model Reasoning:

...the patient has been on mechanical ventilation for 96 hours, which is a long duration indicating a complex respiratory condition. The ECG and other lab results do not show any immediate critical issues, but the patient's hematocrit and hemoglobin levels are low, which could be a sign of anemia or other underlying conditions requiring treatment...the high and low heart rate alarms suggest the patient might be at risk for arrhythmias or other issues requiring close monitoring. Given the prolonged ventilation and the need for multiple invasive procedures, the patient is likely to require a significant period in the ICU or a high-dependency unit for close monitoring and management of their respiratory condition.

**Answer:** D. more than 12 days

# My Overview of AI Agents



# Language Agents

- Many productive tasks we perform today are done on the computer
  - And many of these are on the web
- Many opportunities to automate menial tasks and augment human capabilities



Image generated by DALL·E 3.

# Language Agents

vpc-0i... 3 / channy-vpc Actions ▾

**Details** [Info](#)

VPC ID vpc-0...3	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0...	Main route table rtb-06...06	Main network ACL acl-05...56
Default VPC No	IPv4 CIDR 10.0.0.0/17	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID i-...	

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#)

**Resource map** [Info](#)

**VPC** [Show details](#)

Your AWS virtual network

channy-vpc

**Subnets (9)**

Subnets within this VPC

**us-west-2a**

- channy-subnet-public1-us-west-2a
- channy-subnet-private4-us-west-2a
- channy-subnet-private1-us-west-2a

**us-west-2b**

- channy-subnet-public2-us-west-2b
- channy-subnet-private2-us-west-2b

**Route tables (8)**

Route network traffic to resources

- channy-rtb-private6-us-west-2c
- channy-rtb-private4-us-west-2a
- rtb-0E...06
- channy-rtb-public** [Info](#)
- 3 subnet associations
- 2 routes including local
- channy-rtb-private5-us-west-2b
- channy-rtb-private2-us-west-2b

**Network connections (3)**

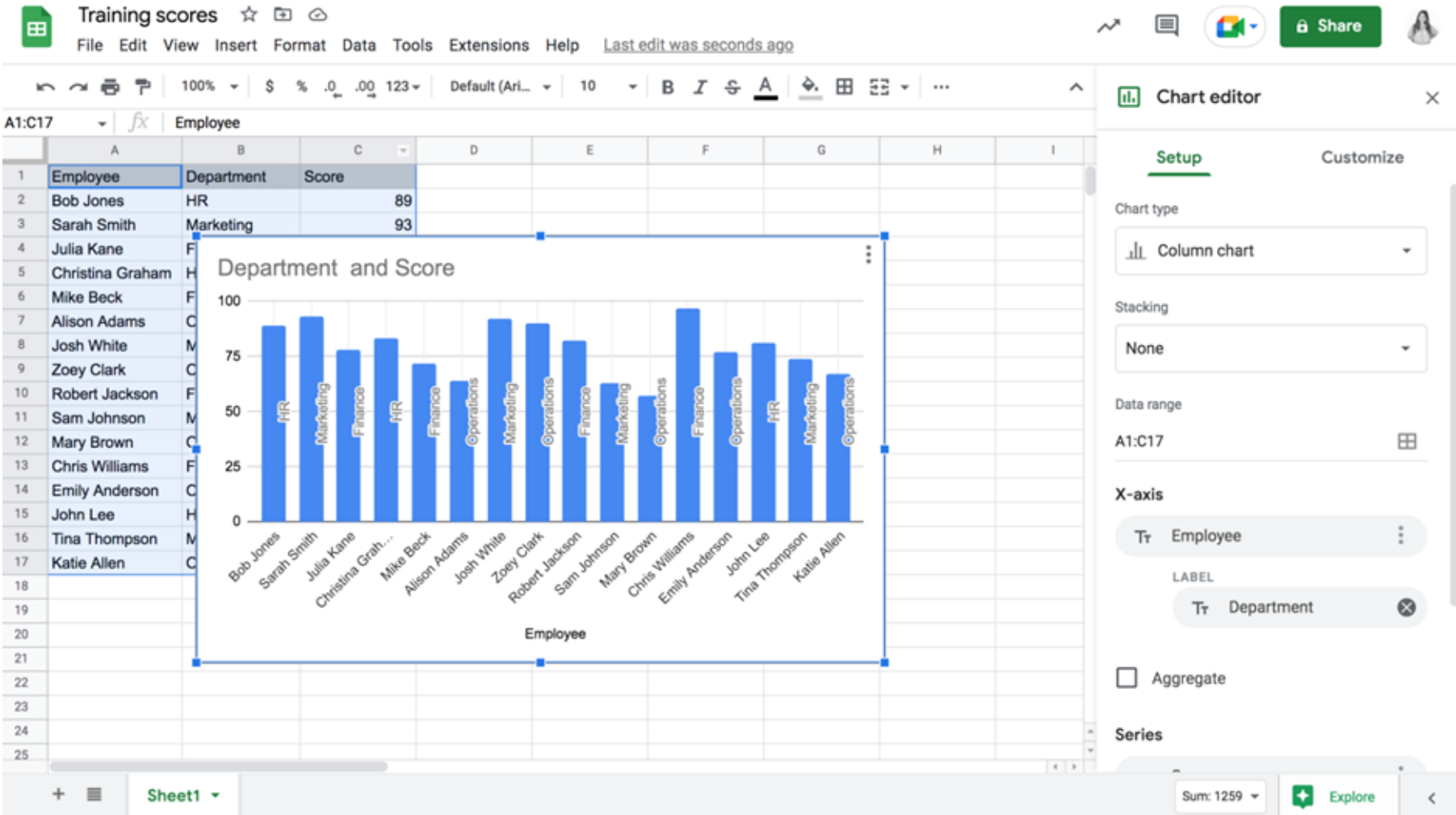
Connections to other networks

- channy-igw
- channy-nat-public1-us-west-2a
- channy-vpce-s3

**Introducing the VPC resource map**

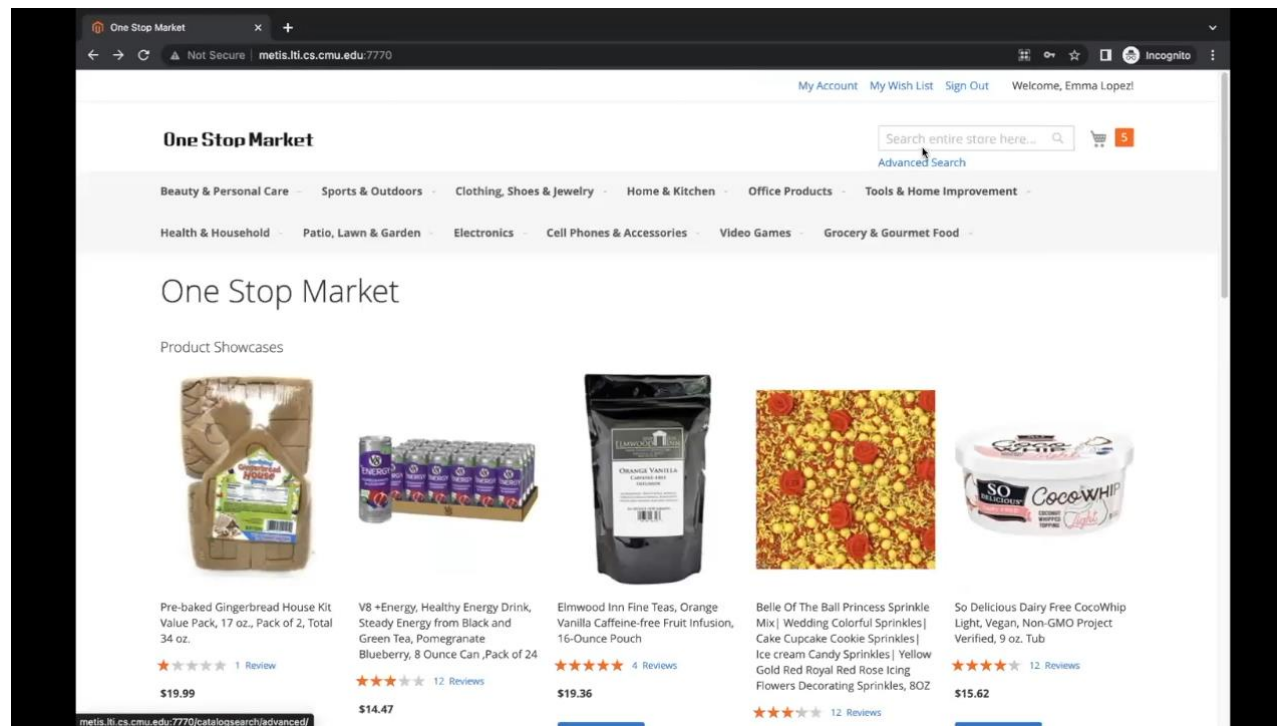
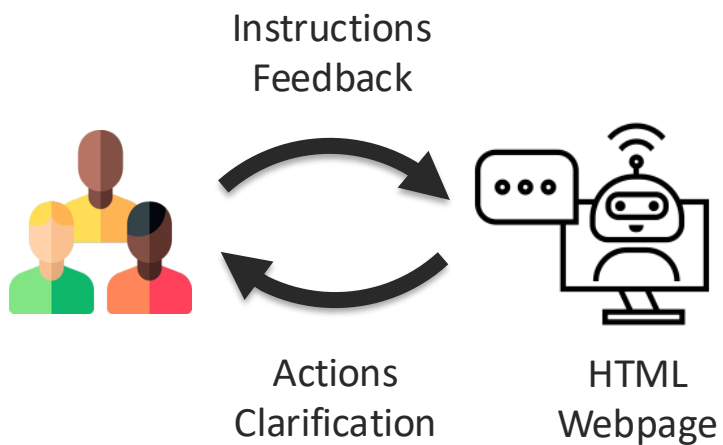
The new resource map helps you visualize the resources in your VPC. It shows your VPC, subnets, route tables, internet gateways, NAT gateways,

# Language Agents

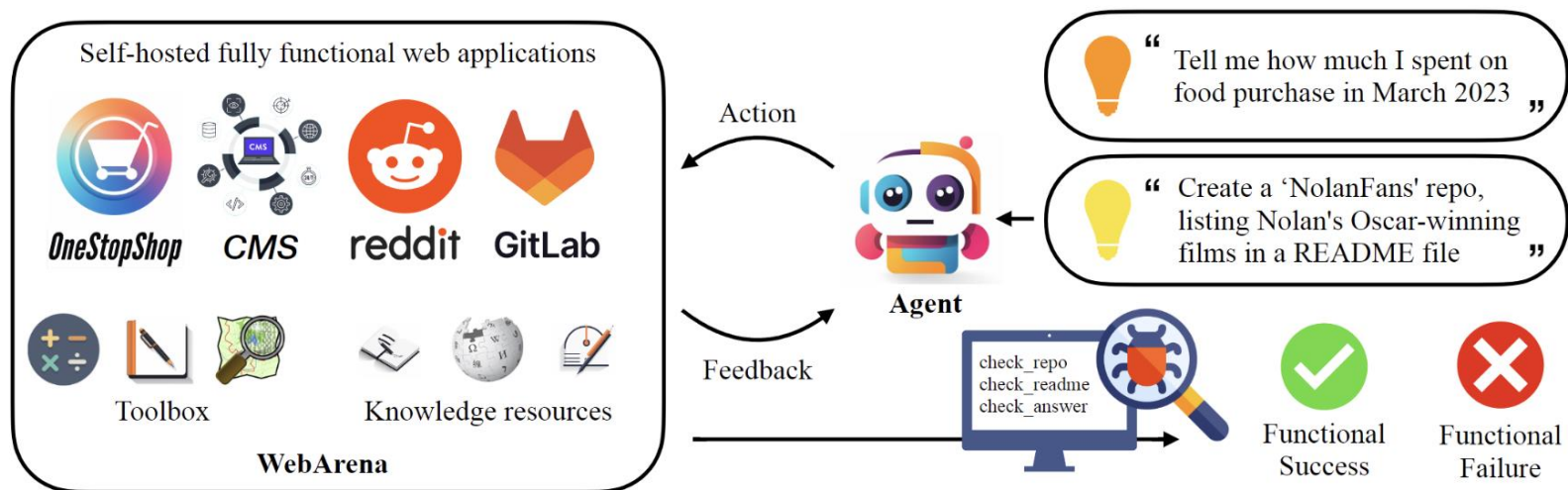


# WebArena Environment

**Example task:** Purchase a set of earphones with at least 4.5 stars in rating and ship it to me.



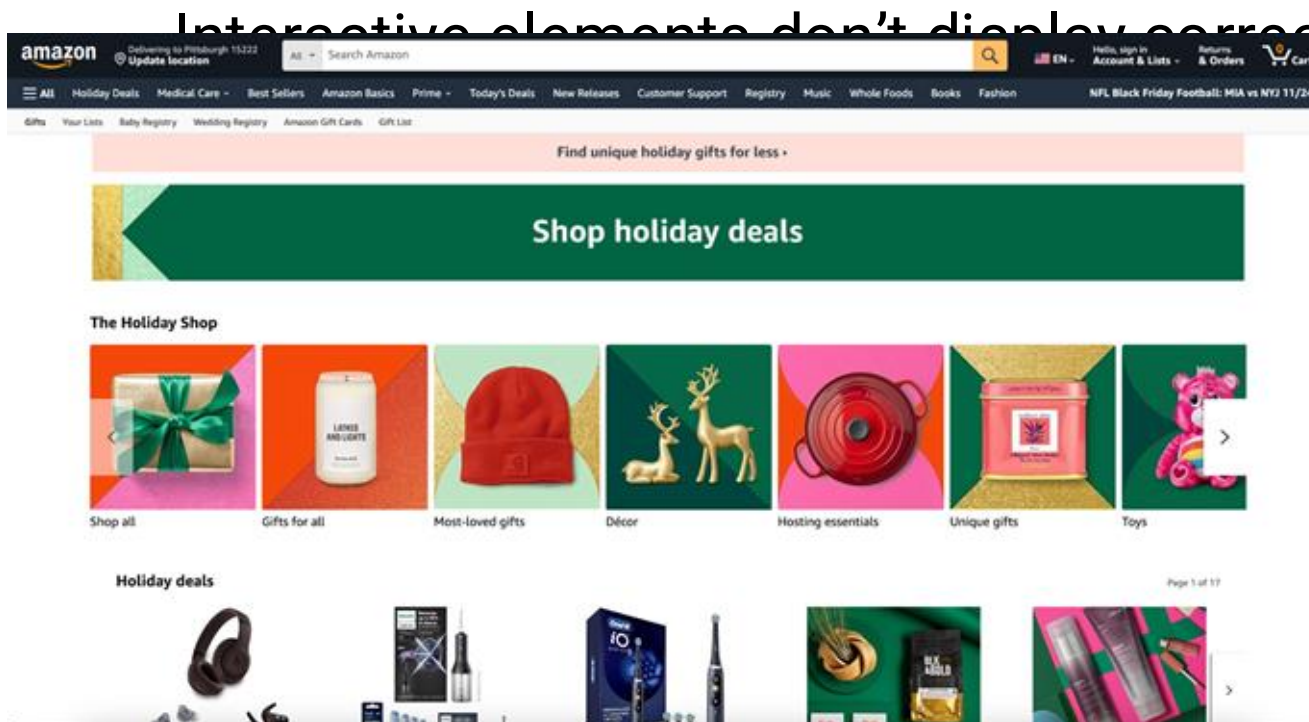
# WebArena Environment



- Websites from four popular categories (shopping, CMS, Reddit, GitLab)
  - Self-hosted open source re-implementations
  - Data from real websites (Amazon, Reddit, GitHub)
- Tasks easy for humans (78% success) but difficult for LLM agents (14%)
- **But:** Tasks are designed to use just text and HTML source code

# HTML is Insufficient

- Messy HTML, JavaScript: usually minified



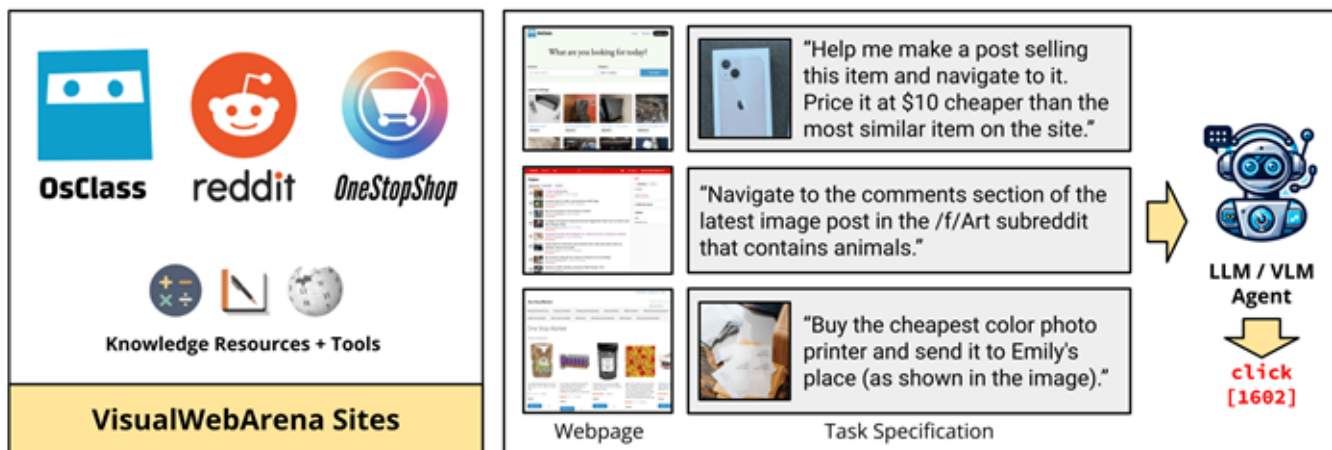
```

1 <!doctype html><html lang="en-us" class="a-no-js" data-19ax5a9jf="dingo"><!-- sp:feature:head-start -->
2 <head><script>var aPageStart = (new Date()).getTime();</script><meta charset="utf-8"/>
3 <!-- sp:end-feature:head-start -->
4 <!-- sp:feature:cs:head-open-part1 -->
5
6 <script type="text/javascript">var ue_t0=ue_t0||new Date();</script>
7 <!-- sp:end-feature:cs:head-open-part1 -->
8 <!-- sp:feature:cs:optimization -->
9 <meta http-equiv="x-dns-prefetch-control" content="on"/>
10 <link rel="dns-prefetch" href="https://images-na.ssl-images-amazon.com" crossorigin>
11 <link rel="preconnect" href="https://images-na.ssl-images-amazon.com" crossorigin>
12 <link rel="dns-prefetch" href="https://m.media-amazon.com" crossorigin>
13 <link rel="preconnect" href="https://m.media-amazon.com" crossorigin>
14 <link rel="dns-prefetch" href="https://completion.amazon.com" crossorigin>
15 <link rel="preconnect" href="https://completion.amazon.com" crossorigin>
16 <!-- sp:end-feature:cs:optimization -->
17 <!-- sp:feature:cs:head-open-part2 -->
18 <script type="text/javascript">
19 window.ue_ihb = (window.ue_ihb || window.ueinit || 0) + 1;
20 if (window.ue_ihb === 1) {
21
22   var ue_csm = window,
23       ue_hob = +new Date();
24   (function(d){var e=d.ue=d.ue||{};f=Date.now|[function(){return new Date};e.d=function(b){return f}-(b?0:d.ue_t0)];e
25   (c.push([c.slice.call(arguments),e.d],d.ue_id));b[a].replay=function(b){for(var a;a=c.shift();b[a[0],a[1],a[2]]);
26   (ueLogError(c,{attribution:a}||"undefined",logLevel:"WARN"))}})(ue_csm);
27
28   var ue_err_chan = 'jserr-rw';
29   (function(d,e){function h(f,b){if(!a.ec>a.mxe)&&f{a.ter.push(f);b[b]({});var c=f.logLevel||b.logLevel;c&&c!=='k&&c!=='
30   e.location.href;"};b.logLevel=c;b.attribution=f.attribution||b.attribution;a.erl.push({exif:info:b});function l(a
31   ,(attribution:is.attribution,logLevel:is.logLevel);void 0);return l}var k="FATAL",m="ERROR",n="WARN",p="DOWNGRADED",a={
32   pec:0,ts:0,erl:[],ter:[],buffer:[],mxe:50,startTimer:function(){a.ts++;setInterval(function(){
33   (d.ue&&a.pec<a.ec&&d.ue("at");a.pec=a.ec),1E4)};l.skipTrace=1;h.skipTrace=1;h.isStd=1;d.ueLogError=h;d.ue_err=a;e
34
35   var ue_id = "QAFJ353VVTZINANB39262",
36       ue_url = "/rd/uedata",
37       ue_navtiming = 1,
38       ue_mid = "ATVPDKIKX0DER",
39       ue_sid = "146-7769316-3082140",
40       ue_sn = "www.amazon.com",
41       ue_furl = "fls-na.amazon.com",
42       ue_surl = "https://unagi-na.amazon.com/1/events/com.amazon.csm.nexusclient.prod",
43       ue_int = 0,
44       ue_fcsm = 1,
45       ue_urt = 3,
46       ue_rpl_ns = "cel-rpl",
47       ue_ddq = 1,
48       ue_fpF = "//fls-na.amazon.com/1/batch/1/OP/ATVPDKIKX0DER:146-7769316-3082140:QAFJ353VVTZINANB39262$uedata=s:",
49       ue_abuimp = 1,
50       ue_ibft = 0,
51       ue_ssvmts = 0,
52       ue_jamtf = 0,
53       ue_fnt = 0,
54       ue_lpsi = 6000,
55       ue_no_counters = 0,
56       ue_lob = '1',
57       un *atch = 1.

```

# VisualWebArena: A Visually Grounded Benchmark

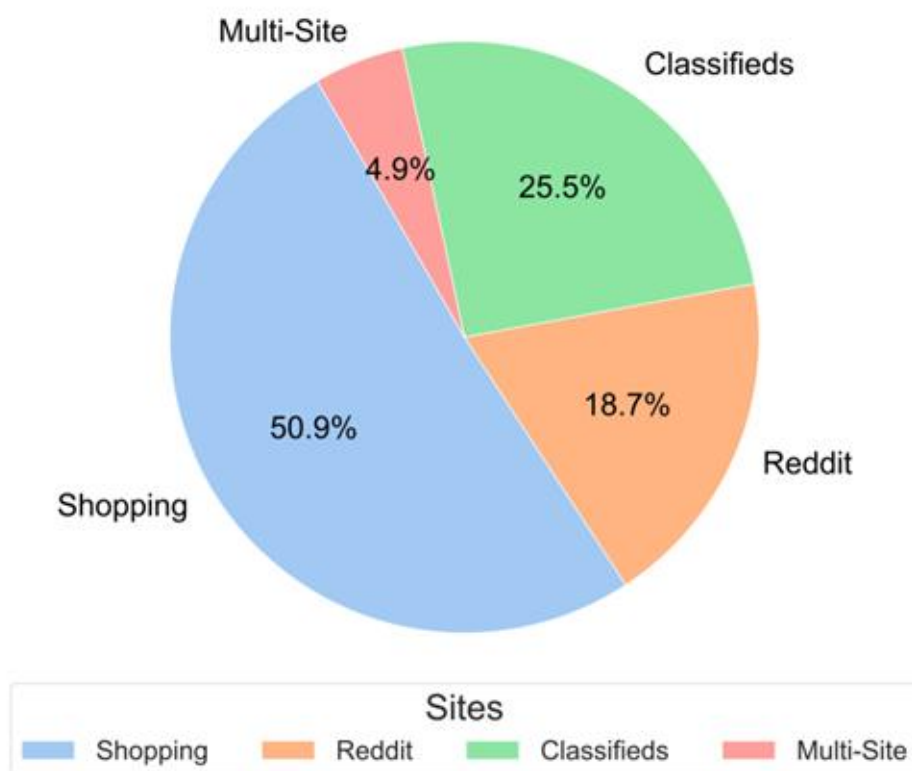
- Benchmark and track the progress of **multimodal agents**



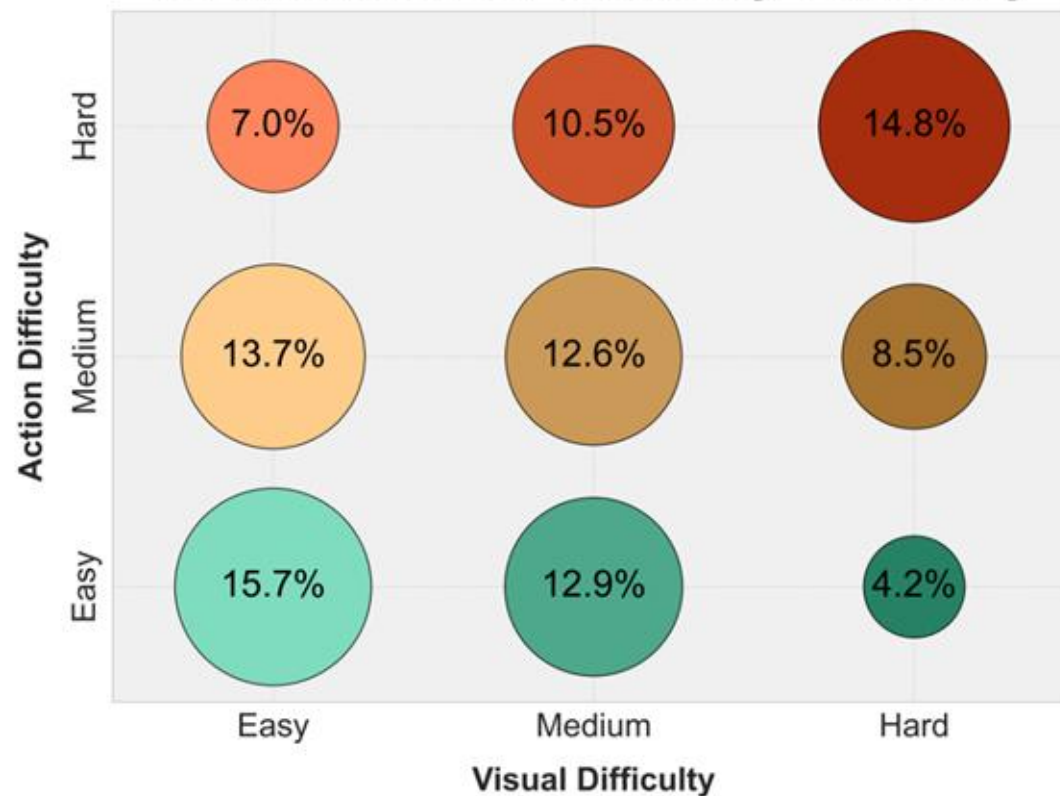
Action Type $a$	Description
click [elem]	Click on element elem.
hover [elem]	Hover on element elem.
type [elem] [text]	Type text on element elem.
press [key_comb]	Press a key combination.
new_tab	Open a new tab.
tab_focus [index]	Focus on the i-th tab.
tab_close	Close current tab.
goto [url]	Open url.
go_back	Click the back button.
go_forward	Click the forward button.
scroll [up down]	Scroll up or down the page.
stop [answer]	End the task with an optional output.

# VisualWebArena: A Visually Grounded Benchmark

## Distribution of Tasks Across Sites



## Distribution of Tasks by Difficulty



# VisualWebArena Shopping Example



**Task:** Buy the cheapest color photo printer and send it to Emily's place (as shown in the image).

My Account My Wish List Sign Out Welcome to One Stop Market




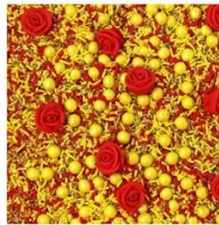

**One Stop Market** Search entire store here...

Advanced Search

Beauty & Personal Care · Sports & Outdoors · Clothing, Shoes & Jewelry · Home & Kitchen · Office Products · Tools & Home Improvement · Health & Household · Patio, Lawn & Garden · Electronics · Cell Phones & Accessories · Video Games · Grocery & Gourmet Food

## One Stop Market

Product Showcases

 <p>Pre-baked Gingerbread House Kit Value Pack, 17 oz., Pack of 2, Total 34 oz.</p> <p>★★★★★ 1 Review</p> <p>\$19.99</p> <p><a href="#">Add to Cart</a></p>	 <p>V8 +Energy, Healthy Energy Drink, Steady Energy from Black and Green Tea, Pomegranate Blueberry, 8 Ounce Can, Pack of 24</p> <p>★★★★★ 12 Reviews</p> <p>\$14.47</p> <p><a href="#">Add to Cart</a></p>	 <p>Elmwood Inn Fine Teas, Orange Vanilla Caffeine-free Fruit Infusion, 16-Ounce Pouch</p> <p>★★★★★ 4 Reviews</p> <p>\$19.36</p> <p><a href="#">Add to Cart</a></p>	 <p>Belle Of The Ball Princess Sprinkle Mix   Wedding Colorful Sprinkles   Cake Cupcake Cookie Sprinkles   Ice cream Candy Sprinkles   Yellow Gold Red Royal Red Rose Icing Flowers Decorating Sprinkles, 8OZ</p> <p>★★★★★ 12 Reviews</p> <p>\$23.50</p>	 <p>So Delicious Dairy Free CocoWhip Light, Vegan, Non-GMO Project Verified, 9 oz. Tub</p> <p>★★★★★ 12 Reviews</p> <p>\$15.62</p> <p><a href="#">Add to Cart</a></p>
---	---	--	---	---

# Execution-Based Evaluation



What is the ISIN of the company that occupies the largest portion in Warren Buffet's portfolio? Answer using the information from the Wikipedia site in the second tab.



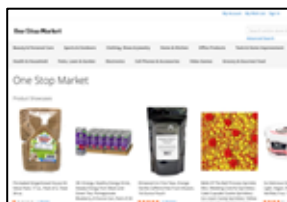
```
exact_match( $\hat{a}$ , "US0378331005")
```



"Create a post for each of the following images in the most related forums."



```
url="/wishlist"  
locator(".wishlist .product-image-photo")  
eval_vqa(s, "Is this a polo shirt? (yes/no)", "yes")  
eval_vqa(s, "Is this shirt green? (yes/no)", "yes")
```



Add something like what the man is wearing to my wish list.



```
eval_fuzzy_image_match(s,  $a^*$ )
```



"Navigate to my listing of the white car and change the price to \$25,000. Update the price in the description as well."



```
url="/index.php?page=item&id=84144"  
must_include( $\hat{a}$ , "$25000 |OR| $25,000")  
must_exclude( $\hat{a}$ , "$30000 |OR| $30,000")
```

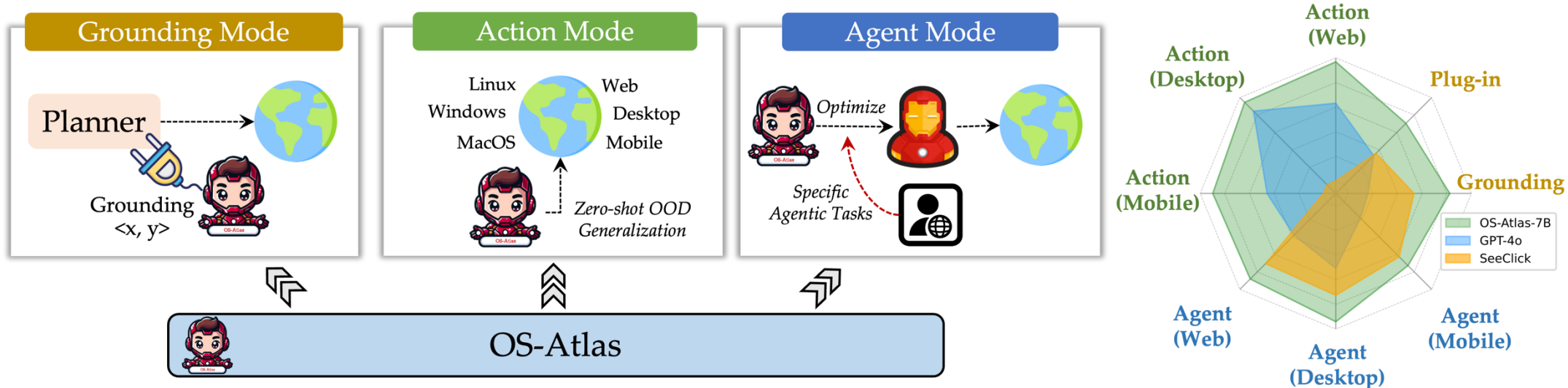
**Webpage(s)**

**Task Specification**

**Automatic Functional Evaluation**

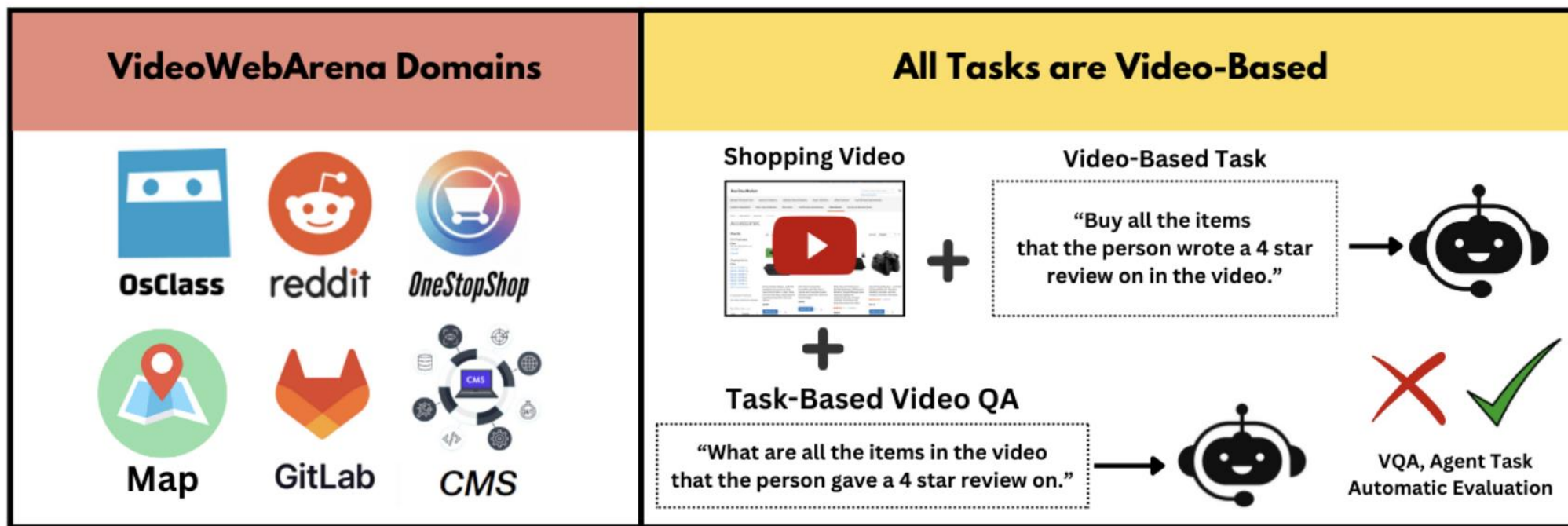
# OS-Atlas

Web + desktop + mobile GUI grounding



# VideoWebArena

Extension to video understanding web tasks



# VLMs as Agents

Tab 0 (current): Search results for: 'hp inkjet'

```
[1] RootWebArea "Search results for: 'hp inkjet'" focused: True
  [81] link 'My Account'
  [82] link 'My Wish List'
  [83] link 'Sign Out'
  [4086] StaticText 'Welcome to One Stop Market'
  [137] link 'Skip to Content'
  [23] link 'store logo'
  [39] img 'one_stop_market_logo'
  [40] link 'My Cart'
  [278] StaticText 'Search'
  [163] combobox 'hp inkjet' autocomplete: both hasPopup: listbox required: False expanded: False
    [426] StaticText 'hp inkjet'
  [281] link 'Advanced Search'
  [120] button 'Search' disabled: True
  [4080] tablist '' multiselectable: False orientation: horizontal
    [4082] tabpanel ''
      [2326] menu '' orientation: vertical
        [3077] menuitem 'Beauty & Personal Care' hasPopup: menu
        [3142] menuitem 'Sports & Outdoors' hasPopup: menu
        [3152] menuitem 'Clothing, Shoes & Jewelry' hasPopup: menu
        [3166] menuitem 'Home & Kitchen' hasPopup: menu
        [3203] menuitem 'Office Products' hasPopup: menu
        [3211] menuitem 'Tools & Home Improvement' hasPopup: menu
        [3216] menuitem 'Health & Household' hasPopup: menu
        [3222] menuitem 'Patio, Lawn & Garden' hasPopup: menu
        [3227] menuitem 'Electronics' hasPopup: menu
        [3288] menuitem 'Cell Phones & Accessories' hasPopup: menu
        [3303] menuitem 'Video Games' hasPopup: menu
        [3316] menuitem 'Grocery & Gourmet Food' hasPopup: menu
  [47] link 'Home'
  [12] main ''
    [32] heading "Search results for: 'hp inkjet'"
    [264] StaticText 'View as'
    [146] strong 'Grid'
    [147] link 'View as List'
    [148] StaticText 'Items'
    [151] StaticText '12'
    [153] StaticText 'of'
    [154] StaticText '687'
    [156] StaticText 'Sort By'
    [269] StaticText 'Relevance'
    [158] combobox 'Sort By' hasPopup: menu expanded: False
    [159] link 'Set Ascending Direction'
    [424] link 'Image'
    [1010] img 'Image'
    [1011] link 'HP Business Inkjet 2800 Wide Format Printer (CB174A#A2L)'
    [720] LayoutTable ''
      [1451] StaticText 'Rating:'
      [1232] generic '4.7%'
      [1069] link '2 Reviews'
    [1871] StaticText '$37.64'
    [1600] link 'Image'
```

**Accessibility tree / HTML:** Cluttered with unnecessary information, long and confusing context.

Search results for: 'hp inkjet'

Shop By

Shopping Options

Category

- Beauty & Personal Care
- Clothing, Shoes & Jewelry
- Home & Kitchen
- Office Products
- Tools & Home Improvement
- Health & Household
- Electronics
- Cell Phones & Accessories
- Video Games
- Grocery & Gourmet Food

HP Business Inkjet 2800 Wide Format Printer (CB174A#A2L) \$37.64

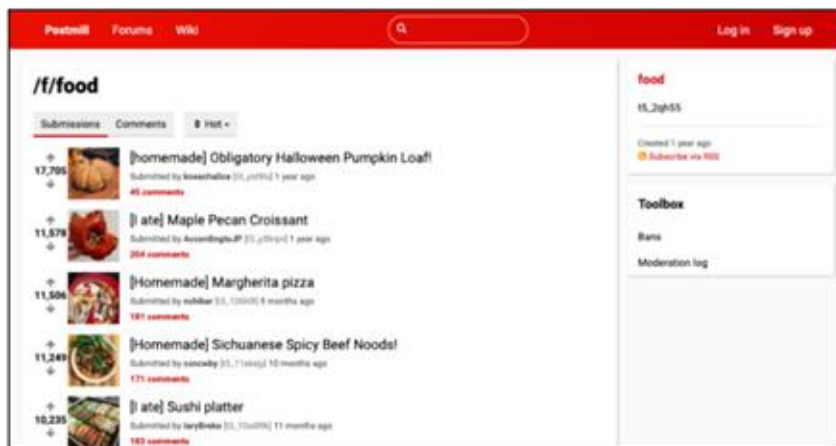
HP CB782A#ABA 640 Inkjet Fax Machine (Renewed) \$279.49

HP Deskjet Plus 4122 Inkjet All-in-one Wireless Printer \$139.99

HP Deskjet 2752 Wireless All-in-one Color Inkjet Printer, Scan and Copy with Mobile Printing, BRK11A (Renewed)

**VLM + SoM:** Simplified representation with Set-of-Marks (SoM) prompting over interactable elements.

# VLMs as Agents



Original Webpage



The annotated screenshot shows the same webpage with various elements highlighted by colored boxes and numbered markers (1-10). These markers correspond to the SoM elements listed below. The elements include the search bar, navigation tabs, post titles, images, and comment counts.

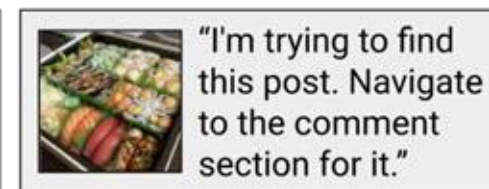
**Webpage with SoM of Interactable Elements**

**SoM Elements and Text Content**

```

...
[7] [A] [Comments]
[8] [BUTTON] [Hot]
[9] [IMG] [description: picture of a pumpkin]
[10] [A] [kneechalice]
...

```

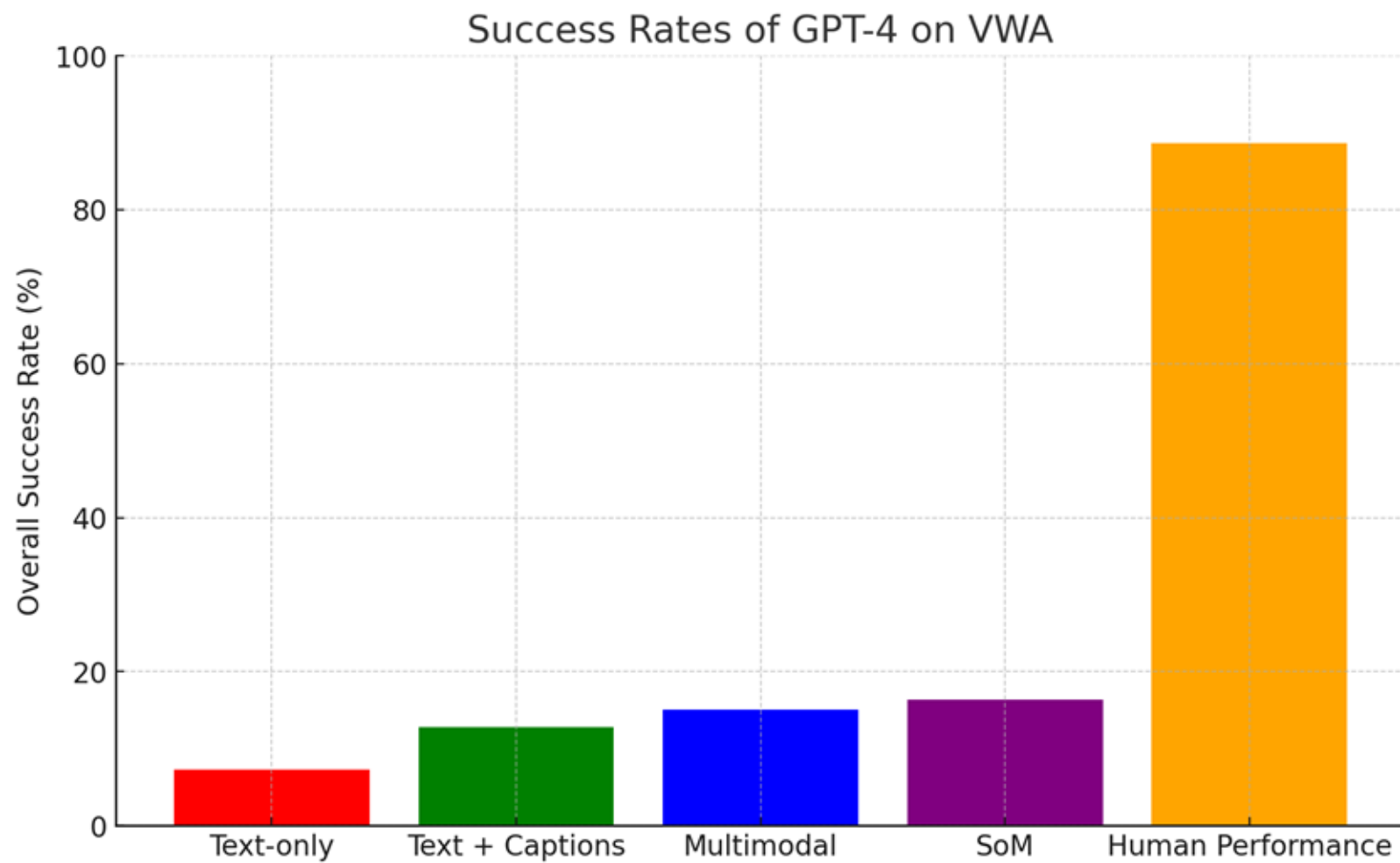


LLM / VLM  
Agent



click [31]

# Baseline Agents



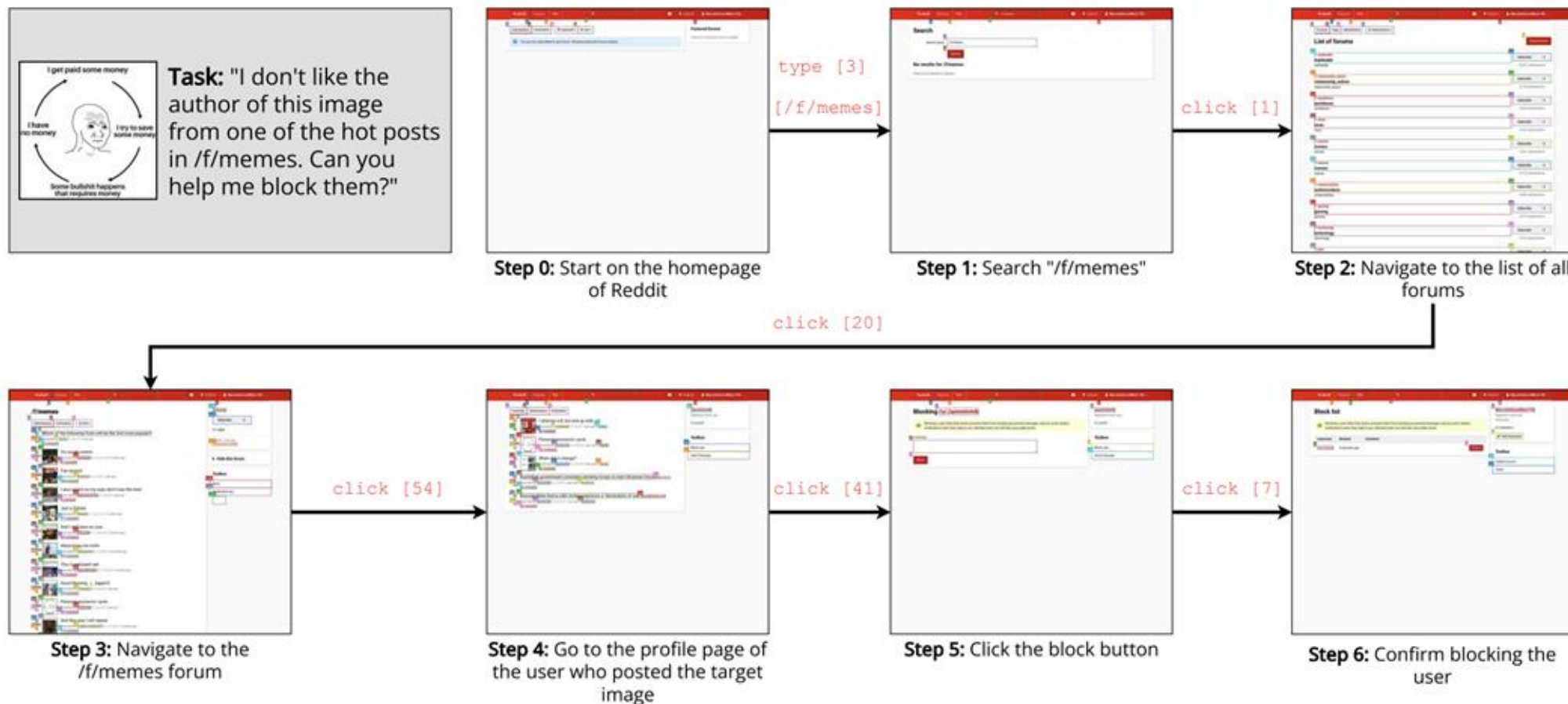
# Text-only LLM Agents

Model Type	LLM Backbone	Visual Backbone	Inputs	Success Rate (↑)
Text-only	LLaMA-2-70B	-	Accessibility Tree	1.10%
	Mixtral-8x7B			1.76%
	Gemini-Pro			2.20%
	GPT-3.5			2.20%
	GPT-4			7.25%
Caption-augmented	LLaMA-2-70B	BLIP-2-T5XL	Accessibility Tree + Captions	0.66%
	Mixtral-8x7B	BLIP-2-T5XL		1.87%
	GPT-3.5	LLaVA-7B		2.75%
	GPT-3.5	BLIP-2-T5XL		2.97%
	Gemini-Pro	BLIP-2-T5XL		3.85%
	GPT-4	BLIP-2-T5XL		12.75%

# Multimodal Agents

Model Type	Multimodal Model	Inputs	Success Rate (↑)
Multimodal	IDEFICS-80B-Instruct	Image + Captions + Accessibility Tree	0.77%
	CogVLM		0.33%
	Gemini-Pro		6.04%
	GPT-4V		15.05%
Multimodal (SoM)	IDEFICS-80B-Instruct	Image + Captions + SoM	0.99%
	CogVLM		0.33%
	Gemini-Pro		5.71%
	GPT-4V		<b>16.37%</b>
Human Performance	-	Webpage	88.70%

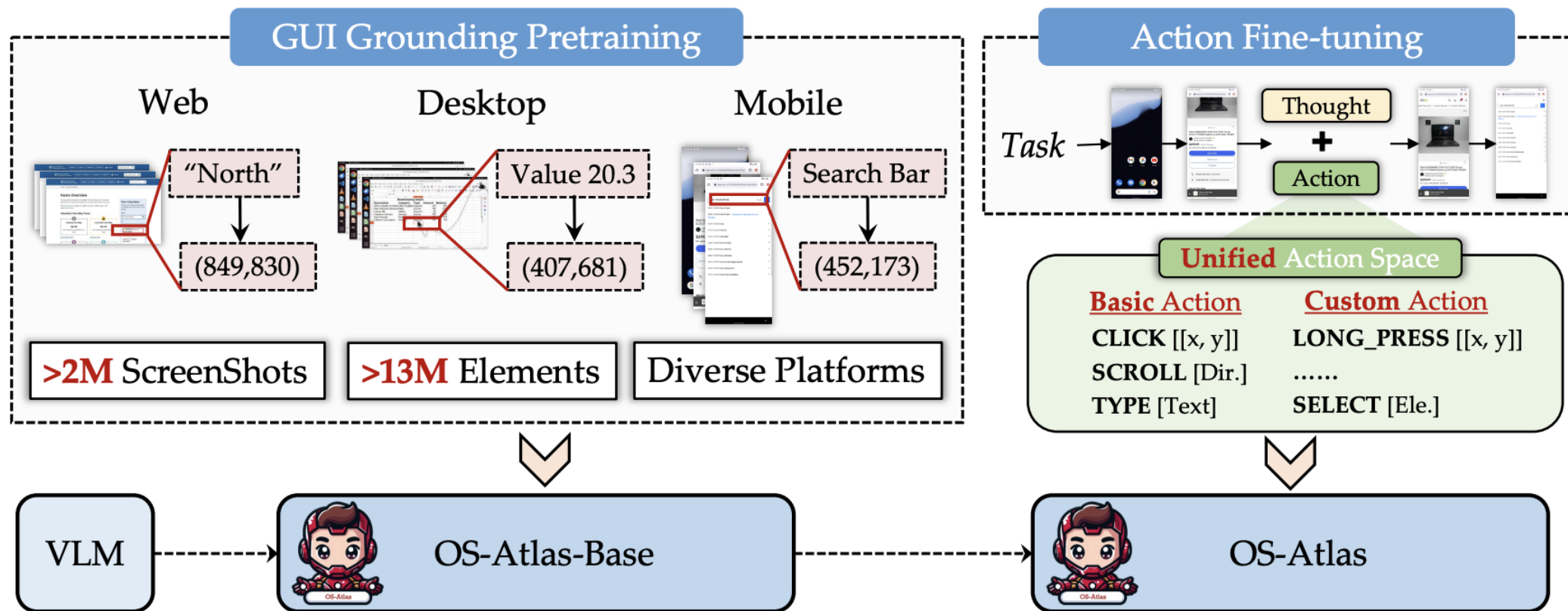
# Example Success Trajectory



Successful execution trajectory of the GPT-4V + SoM agent on the task for blocking a user that posted a certain picture.

# OS-Atlas

Web + desktop + mobile GUI grounding

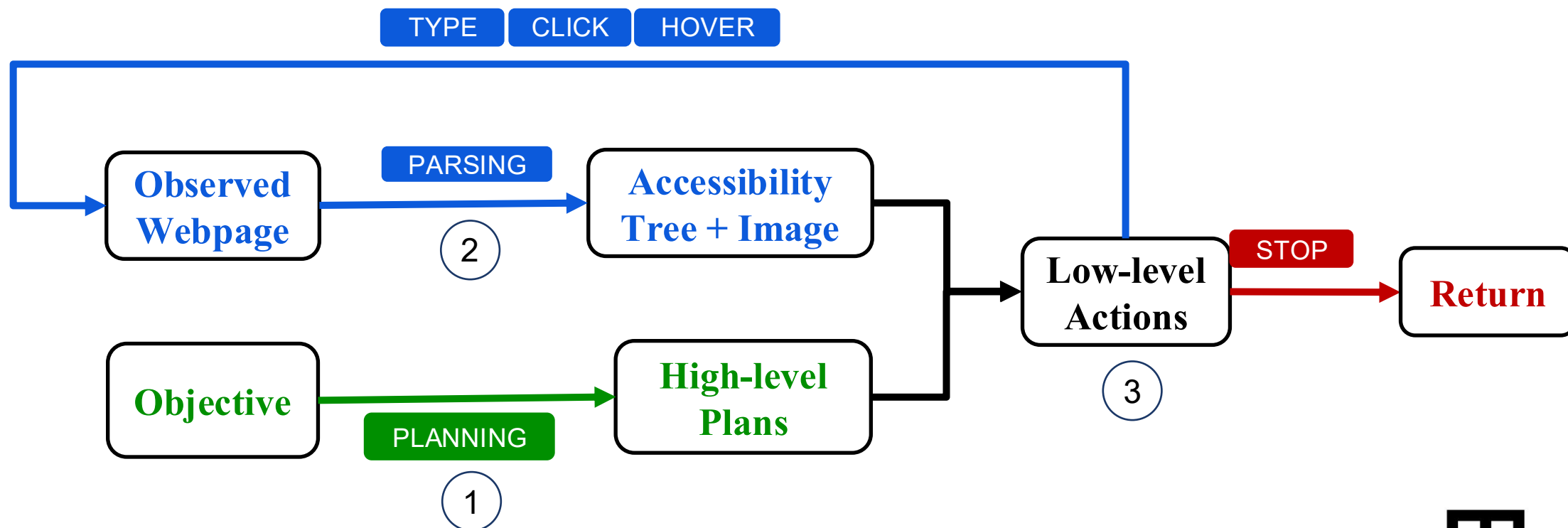


# Common Failure Modes

- **Long horizon reasoning and planning**
  - Getting stuck in loops
  - Correctly performing tasks but undoing them
- **Failures in visual processing**
  - Clicking the wrong item
  - Identifying specific items in complex webpages
  - Spatial reasoning (“what are the prices of products in the first row?”)

# Agents + Reasoning

- Model architecture of our interactive agent:
  - High-level Reasoning
  - Observation Parsing
  - Low-level Action Generation

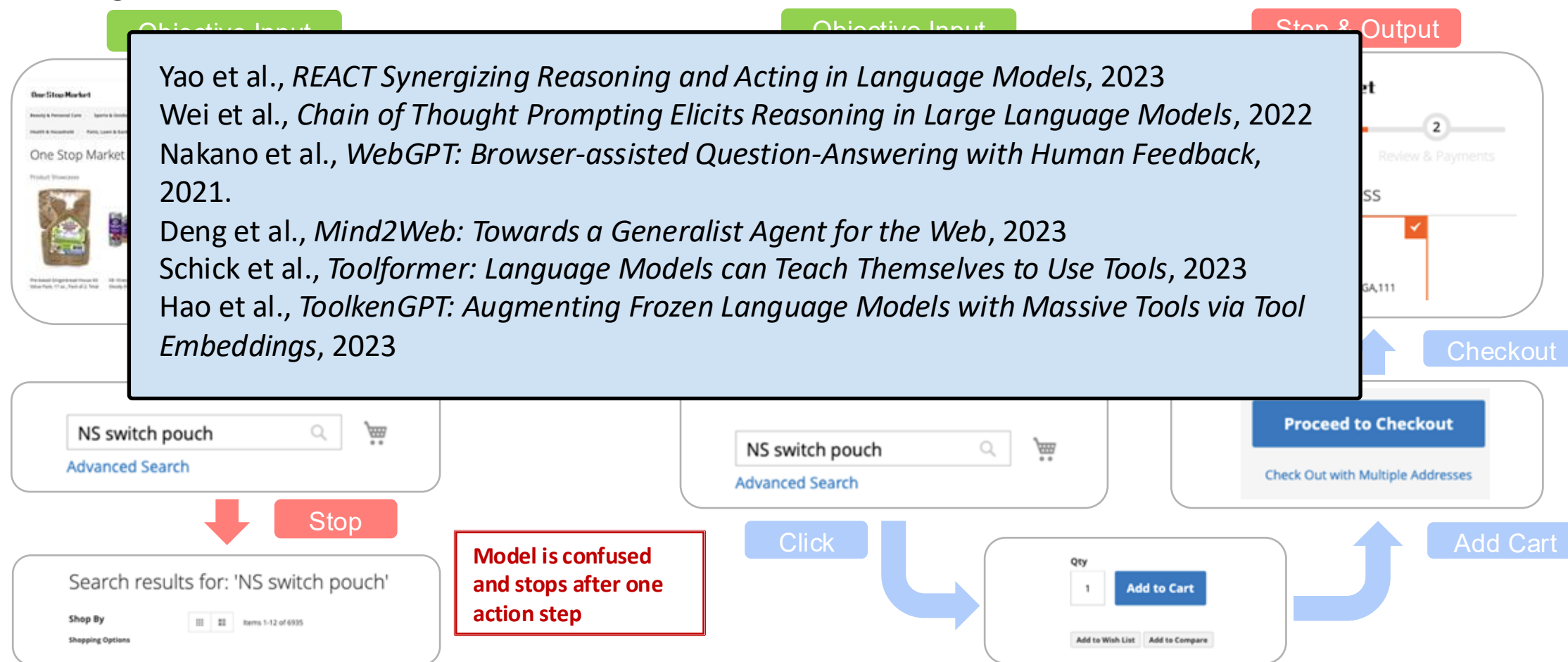


# Agents + Reasoning

**Task:** Buy the highest rated product from the NS switch pouch category within a budget under 60 dollars.

GPT-4's behavior

Desired Behavior



# Generating High-level Plans

What is the price range of wireless earphone in the One Stop Market?

## Generated High-level Plan

[Search] wireless earphone in the One Stop Market

[Find] the price range of wireless earphone in the One Stop Market

**TOO AMBIGUOUS  
HARD TO UNDERSTAND**

## Human Annotated High-level Plan

[Search] wireless earphones in the One Stop Market.

[Sort] the price of the wireless earphones from low to high

[Find] the first item

[Sort] the price of the wireless earphones from high to low

[Find] the first item

[Identify] the price range of wireless earphones in the One Stop Market

# Agents + Human-in-the-loop

Asking humans for clarification when it is uncertain about generated plans

What is the price range of wireless earphone in the One Stop Market?

**Zero-shot high-level plan**

[Search] wireless earphone in the One Stop Market



[Find] the price range of wireless earphone in the One Stop Market

**Too ambiguous**

**Few-shot high-level plan**

[Search] wireless earphone in the One Stop Market



[Find] the price of the first wireless earphone



[Read] the price range of wireless earphones in the One Stop Market

**Didn't sort**

**Few-shot high-level plan with human clarification**

[Search] wireless earphone in the One Stop Market



[Sort] the price of the wireless earphones from low to high



[find] the lowest priced wireless earphone



[sort] the price of wireless earphones from high to low



[find] the highest priced wireless earphone

**Subsequent model generations become correct after clarification**

**Ground truth high-level plan**

[Search] wireless earphones in the One Stop Market.



[Sort] the price of the wireless earphones from low to high



[Find] the first item



[Sort] the price of the wireless earphones from high to low



[Find] the first item



[Identify] the price range of wireless earphones in the One Stop Market

# Estimating Uncertainty

Sampling high-level plans generated by the model multiple times to estimate uncertainty

Few-shot High-level Plan

[Search] wireless earphone in the One Stop Market

[Find] the price of the first wireless earphone

[Read] the prices of the wireless earphones available in the One Stop Market

[Determine] the maximum price of the wireless earphones

[Determine] the minimum and maximum prices from the list of wireless earphones

Stop

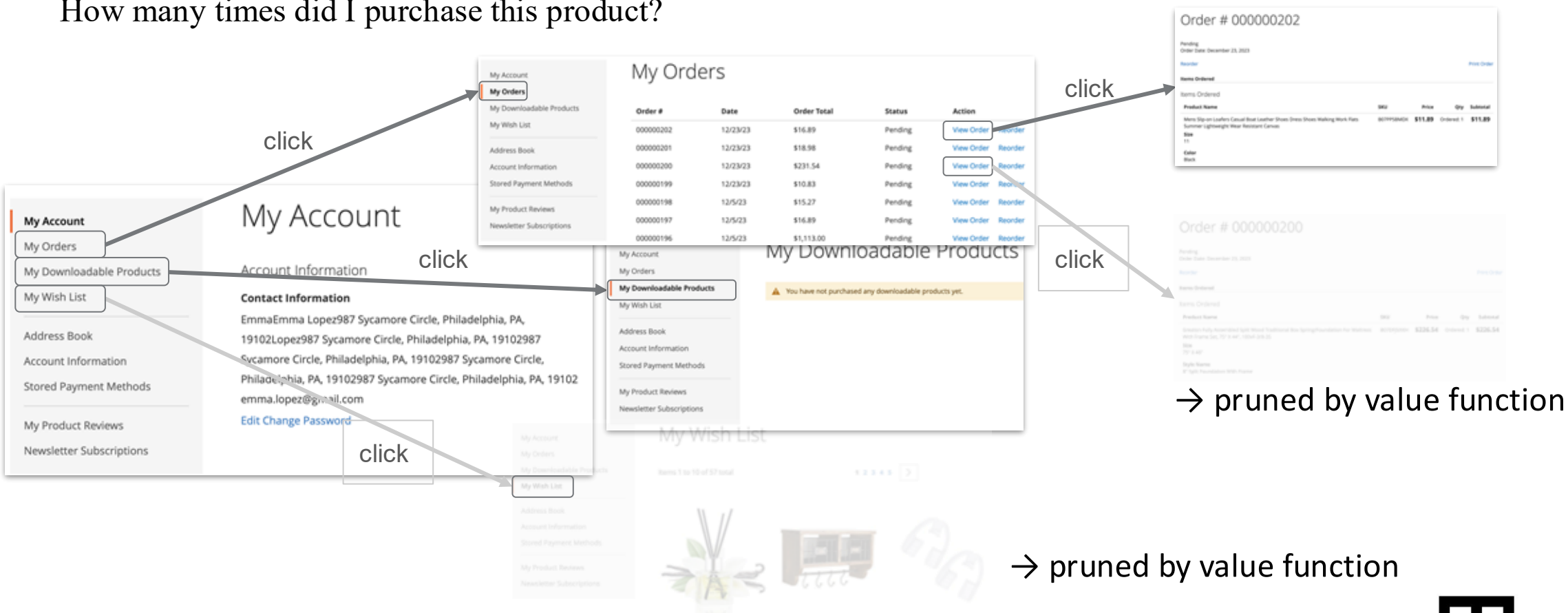
Without human clarification:

- Plan is ambiguous
- Model is uncertain about the overall plan

# Agents + Search

Searching over low-level actions – recall reinforcement learning

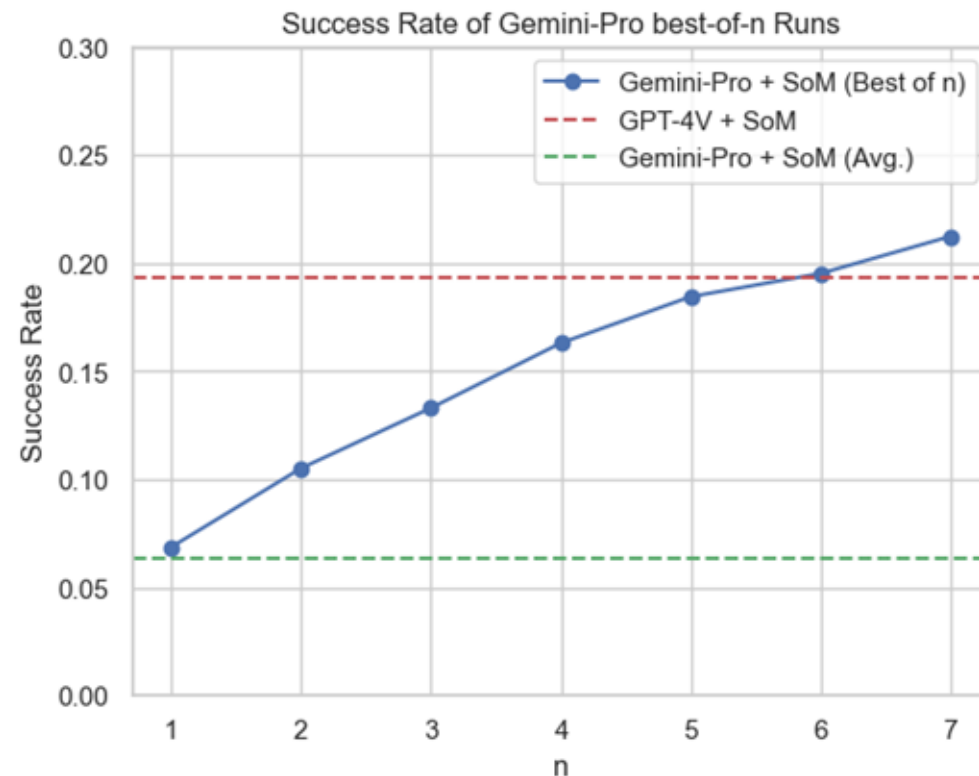
How many times did I purchase this product?



# Agents + Search

**Idea:** Allow the agent to execute and coordinate multiple instances in parallel for better exploration.

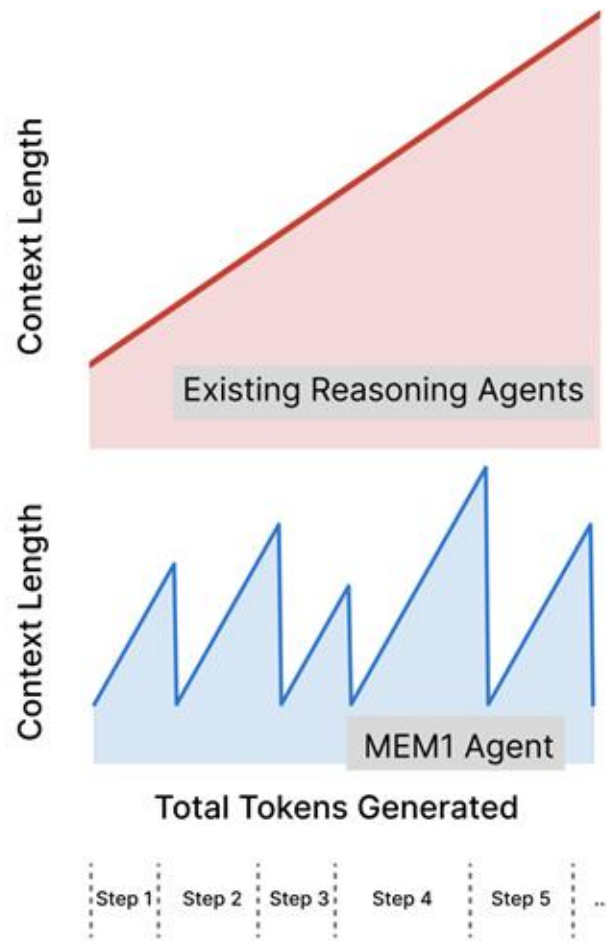
**Research Problem:** Learning a good value function for search and re-ranking of trajectories.



Gemini-Pro performance on VisualWebArena. With an accurate value function, exploration and search can substantially improve performance.

# Agents + Memory

<https://github.com/MIT-MI/MEM1>



**Key problem:** As reasoning context grows longer (more modalities and longer context), new complexity and forgetting challenges.

**Proposal:** Introduce an **internal state** that integrates **reasoning** and **memory**. At each step, the model **updates this internal state and discards all previous information**.

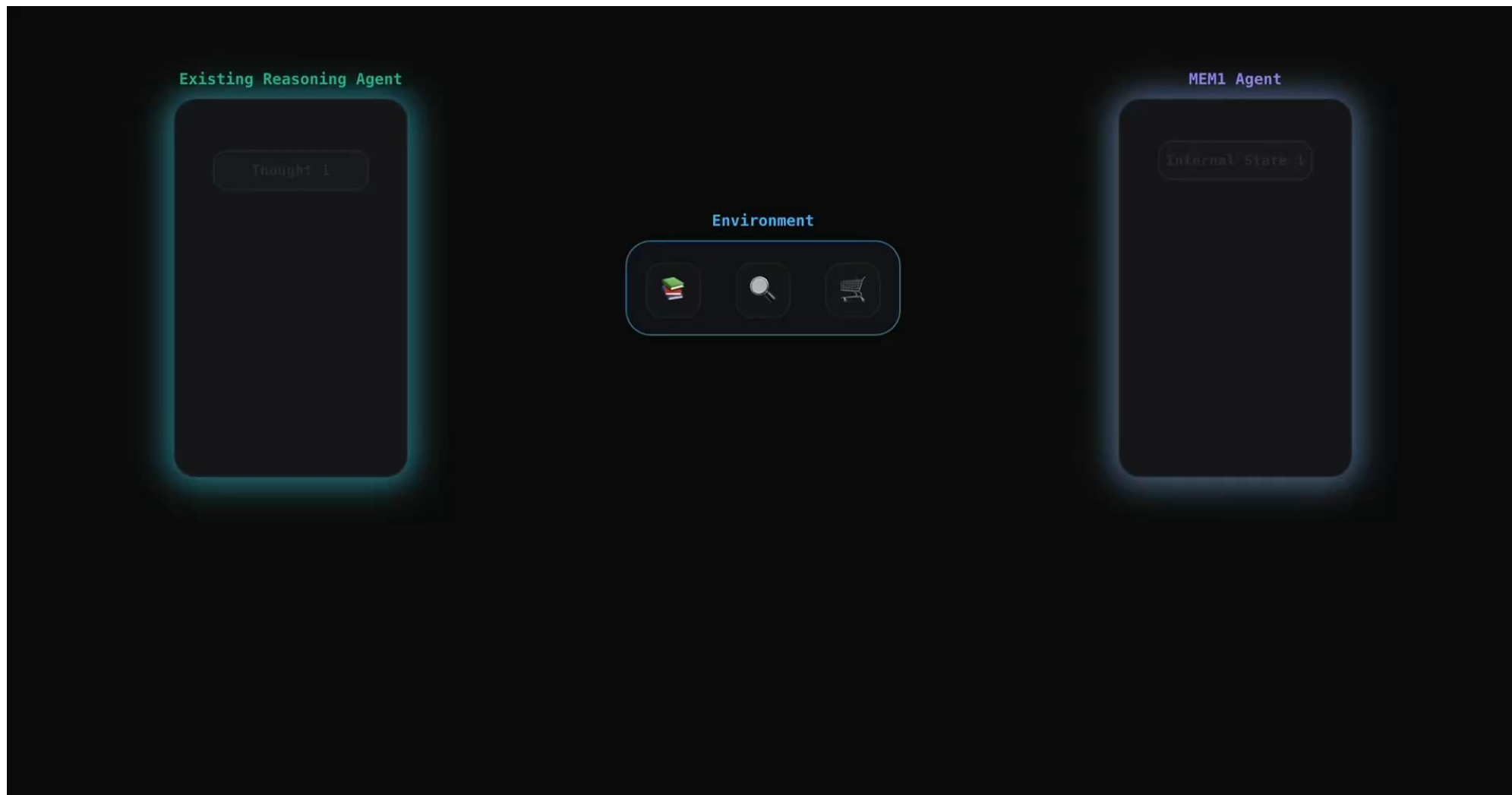
**Advantages:**

1. Enable near-constant memory
2. Support end-to-end optimization



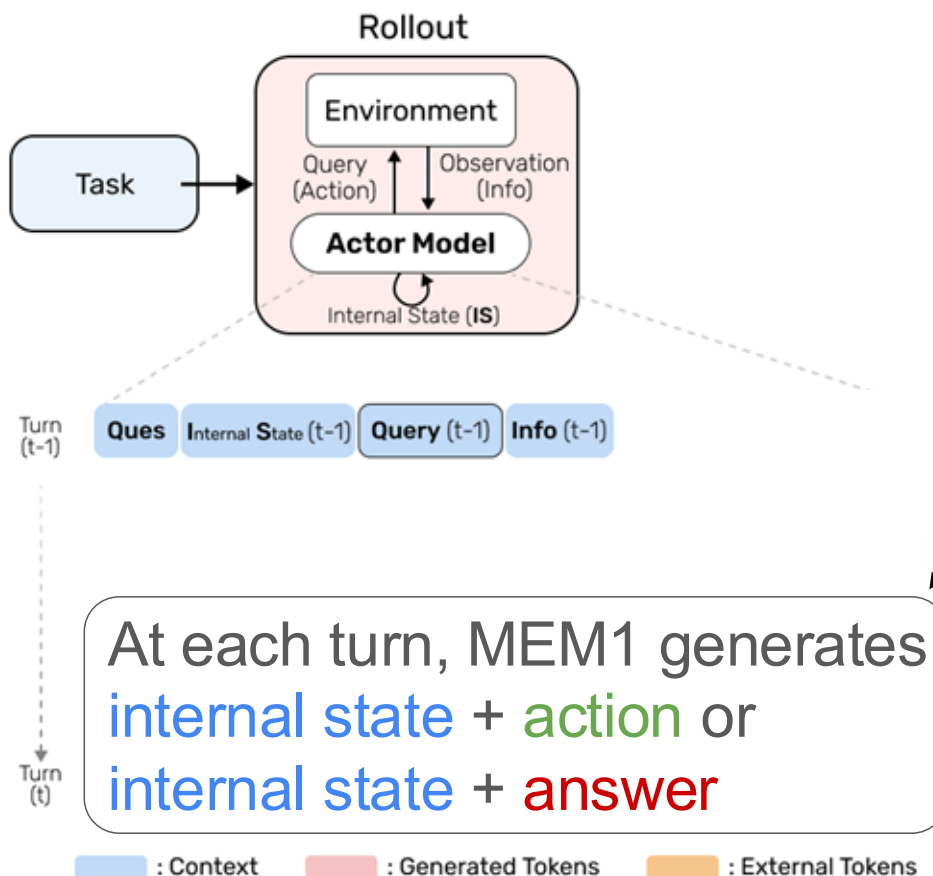
# MEM1: Memory Efficient Reasoning

<https://github.com/MIT-MI/MEM1>



# MEM1: Rollout with Internal State

<https://github.com/MIT-MI/MEM1>



## Prompt 1: Single-Objective Task (QA)

You will answer a complex question through iterative reasoning, summarization, and web searches.

At each step, you can see the question, previous reasoning and summary in `<internal_state> ... </internal_state>`, search query in `<search> ... </search>`, and the returned information in `<information> ... </information>` (except the first step where you will be given only the question). Then, you should:

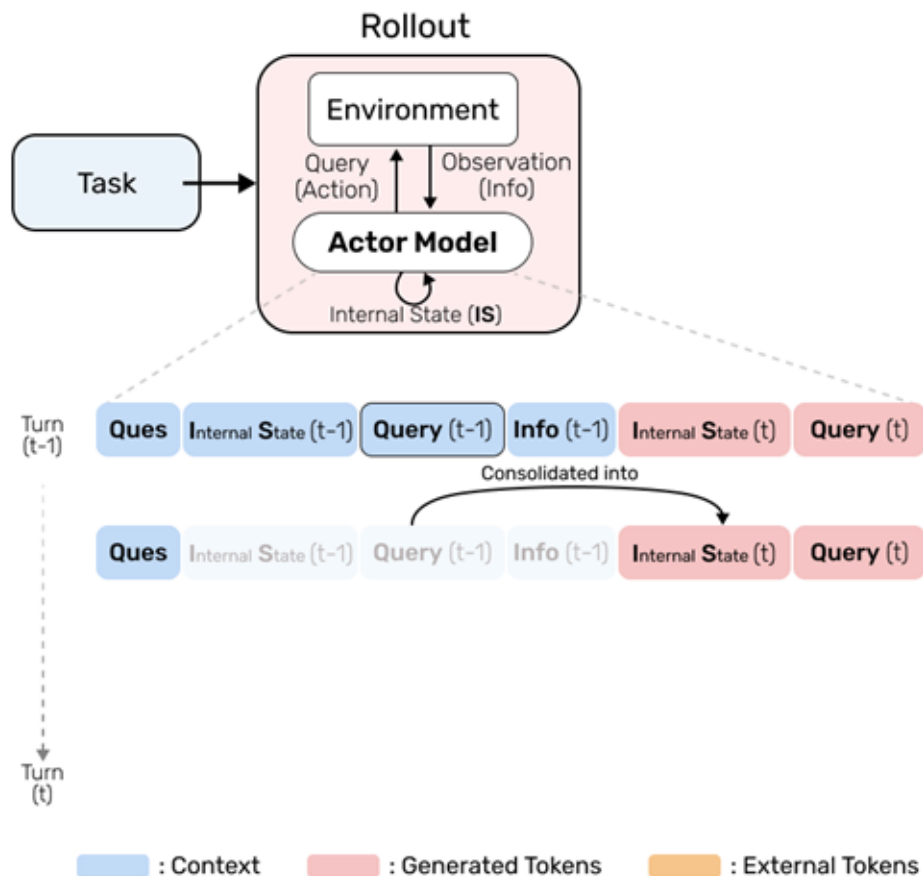
1. **Update a concise, cumulative summary with essential information and conduct reasoning inside `<internal_state>` `</internal_state>`.** This is your persistent memory and should include all important information from previous `<internal_state>` `</internal_state>` and `<information>` `</information>` (i.e. information and answers already found for questions).

2. Then choose one:
  - Issue a query (i.e., key words / phrases for search) inside `<search>` `</search>` (you may search repeatedly until the answer is clear). This query will be used to conduct search and return the results in `<information>` results `</information>`
  - Provide the final concise answer (no explanations) if no additional information is needed inside `<answer>` `</answer>`. The answer should be concise and only contain the words necessary to answer the question.

Question: [QUESTION]

# MEM1: Rollout with Internal State

<https://github.com/MIT-MI/MEM1>

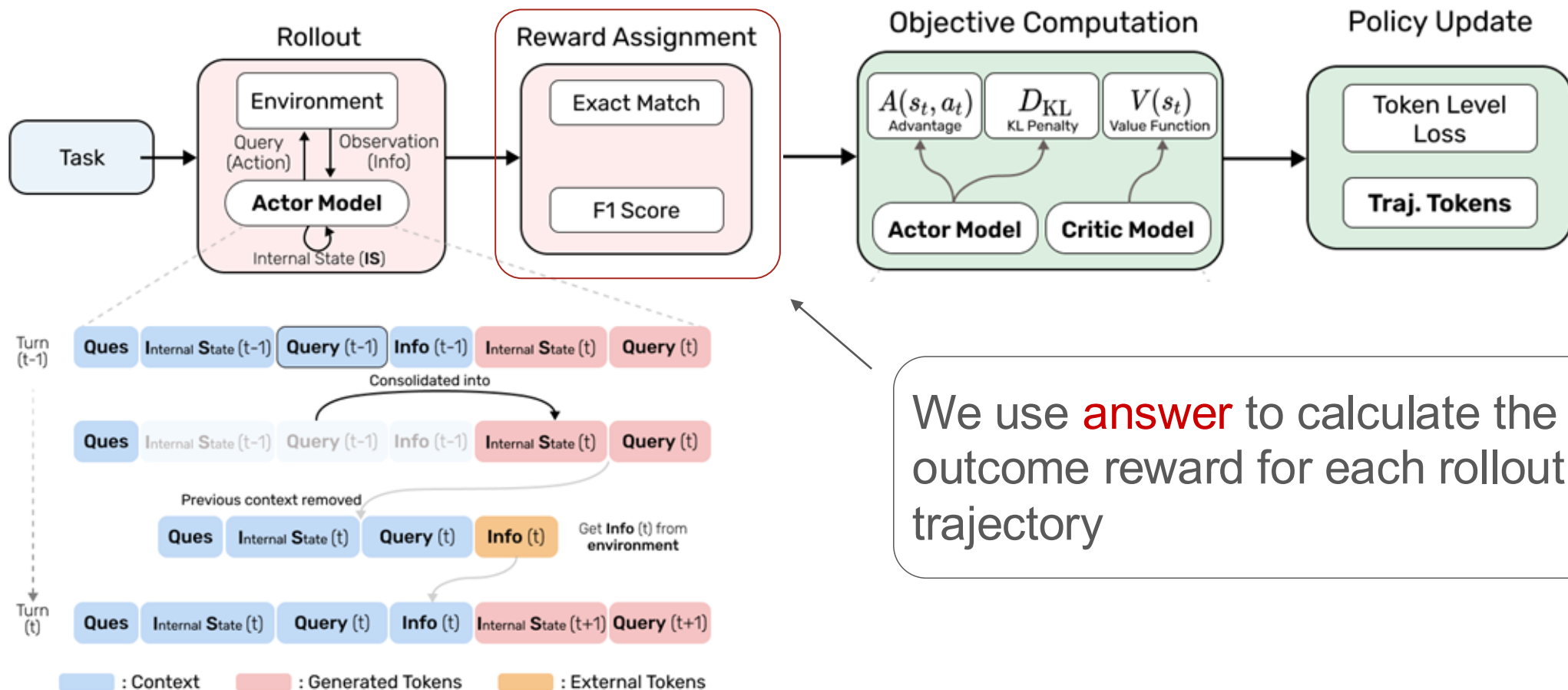


## Key idea: Memory Consolidation

- MEM1 keeps context size constant by pruning old states after each turn.
- All prior knowledge is compressed into the latest *Internal State*, so only the latest internal state, query, and info are kept in memory.
- Forces the agent to continuously integrate, update, and compress knowledge at every step.

# MEM1: Outcome Reward

<https://github.com/MIT-MI/MEM1>



We use **answer** to calculate the outcome reward for each rollout trajectory

# MEM1 Results: WebAgents

<https://github.com/MIT-MI/MEM1>

Model	Avg Final Reward $\uparrow$	Peak Token ( $\times 10^3$ ) $\downarrow$	Dependency ( $\times 10^6$ ) $\downarrow$	Inference Time Per Traj (s) $\downarrow$
GPT-4o	25.48	$5.30 \pm 1.23$	$3.99 \pm 1.16$	N/A
GPT-4o (truncate)	13.82	$0.99 \pm 0.99$	$0.81 \pm 0.23$	N/A
GPT-4o (A-MEM)	24.50	$1.84 \pm 0.06$	$0.31 \pm 0.11$	N/A
Qwen2.5-7B-Instruct	18.42	$5.64 \pm 1.34$	$3.38 \pm 0.89$	$12.31 \pm 1.82$
Qwen2.5-14B-Instruct	12.34	$5.44 \pm 0.92$	$3.30 \pm 0.61$	$18.17 \pm 2.32$
Agent-FLAN-7B	40.35	$3.37 \pm 1.12$	$2.18 \pm 1.62$	$9.95 \pm 6.19$
Agent-R-8B	63.91	N/A	N/A	N/A
AgentLM-7B	63.60	$2.24 \pm 0.40$	$0.28 \pm 0.07$	$3.91 \pm 1.07$
AgentLM-13B	70.80	$2.36 \pm 0.46$	$0.30 \pm 0.08$	$5.23 \pm 1.59$
<b>MEM1-WebShop</b>	<b>70.87</b>	<b><math>0.81 \pm 0.10</math></b>	<b><math>0.15 \pm 0.16</math></b>	<b><math>2.61 \pm 0.48</math></b>

MEM1 trained on WebShop achieves **state-of-the-art performance**, with **the fewest peak tokens** and **the shortest inference time**.

# MultihopQA Task Construction

<https://github.com/MIT-MI/MEM1>

Existing datasets often focus on **single-objective tasks**

An example question from HotpotQA:

- *Which US state is nicknamed The Equality State?*

We scale up existing datasets by **composing multiple tasks** into one and training the model on compositional tasks

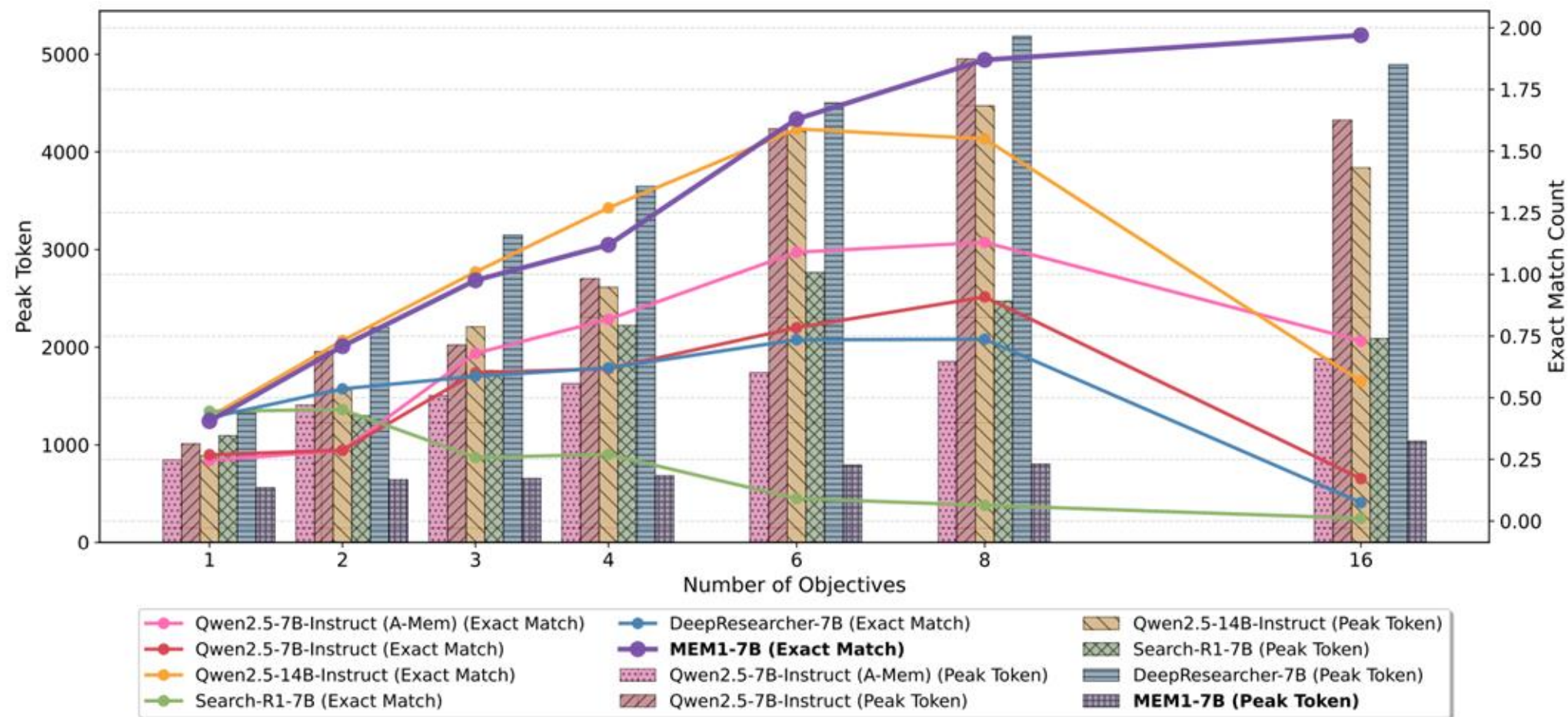
An example task of our 2-objective HotpotQA dataset:

- *Which US state is nicknamed The Equality State?; Which US State is nicknamed The Beaver State?*

~32.2% of compositional tasks involve two closely related questions

# MEM1 Results: MultihopQA

<https://github.com/MIT-MI/MEM1>



When # Questions  $\uparrow$   $\rightarrow$  Performance : Baseline Methods  $\downarrow$ ; MEM1  $\uparrow$   
 Context : Baseline Methods  $\uparrow$ ; MEM1  $-$

# Emergent Memory Behaviors

<https://github.com/MIT-MI/MEM1>

 MEM1 learns to **store key extracted info** about each question separately

**MEM1: ...**

**According to the provided information:**

- They had 9 World Series appearances in Brooklyn.
- They have had 11 World Series appearances in Los Angeles.

Therefore, .... Now, to answer the second question, ...

**From the provided information:**

- The show originally ran on ABC from 2011 to 2017 for six seasons...

# Emergent Memory Behaviors

<https://github.com/MIT-MI/MEM1>

 MEM1 learns to explicitly **update its memory** before moving on to the next question

[Omitted History]

**Env:** [Search Results]

**MEM1:** : After searching for the information, we found out that Beniamino Di Giacomo was born in Porto Recanati. **Now we can add this information to our cumulative summary: Beniamino Di Giacomo was born in Porto Recanati.** To answer the second question, 'In what city was Tim Alexander born?', we need to perform a web search...

# Emergent Memory Behaviors

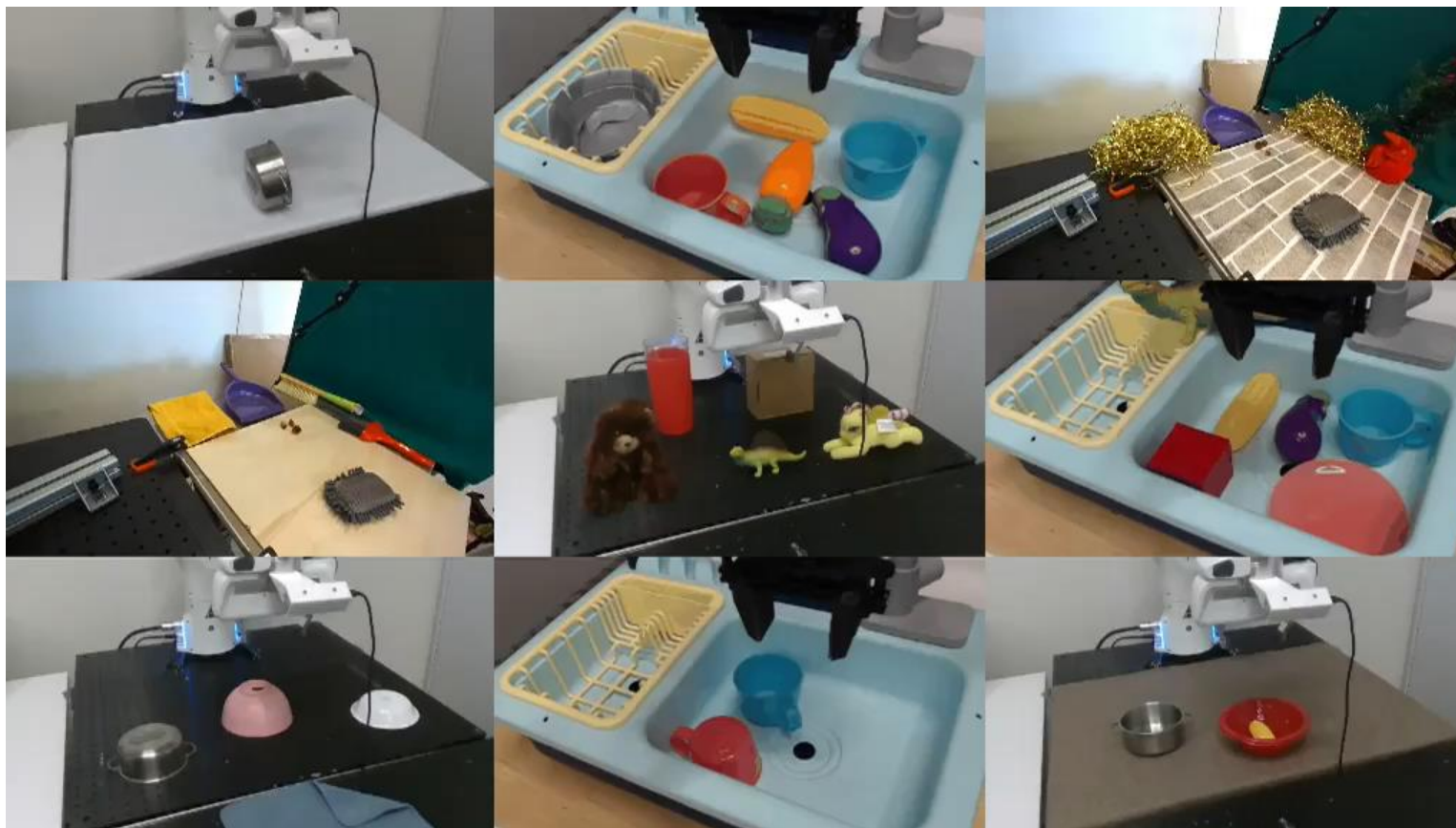
<https://github.com/MIT-MI/MEM1>

 MEM1 learns to skip one question after several searches without finding useful information.

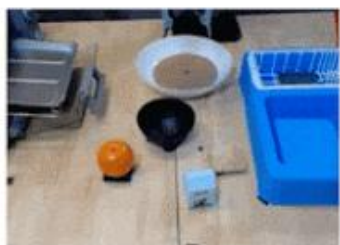
**MEM1: Unfortunately**, based on the information provided in the documents, I am unable to determine the name of the hotel designed by Veldon Simpson that was the largest in the world upon opening.  
**Moving on to the second question, ...**

# Embodied Agents

Generate precise robotics control directly via trained vision language models.



# Real Example: Google RT-X



CLVR, USC



RAIL, UC Berkeley



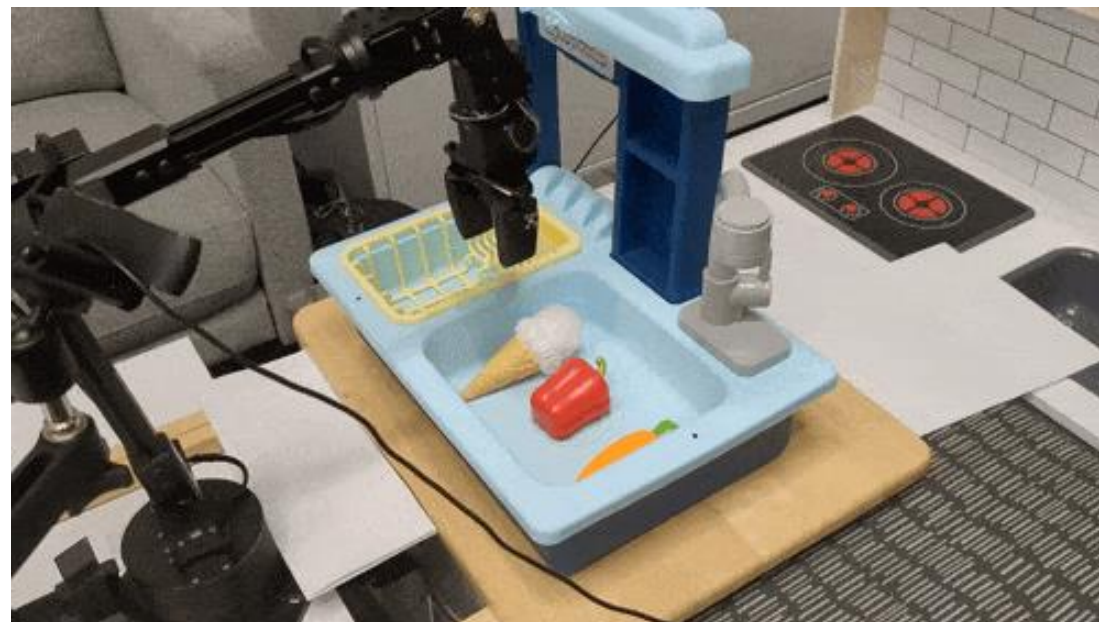
CILVR, NYU



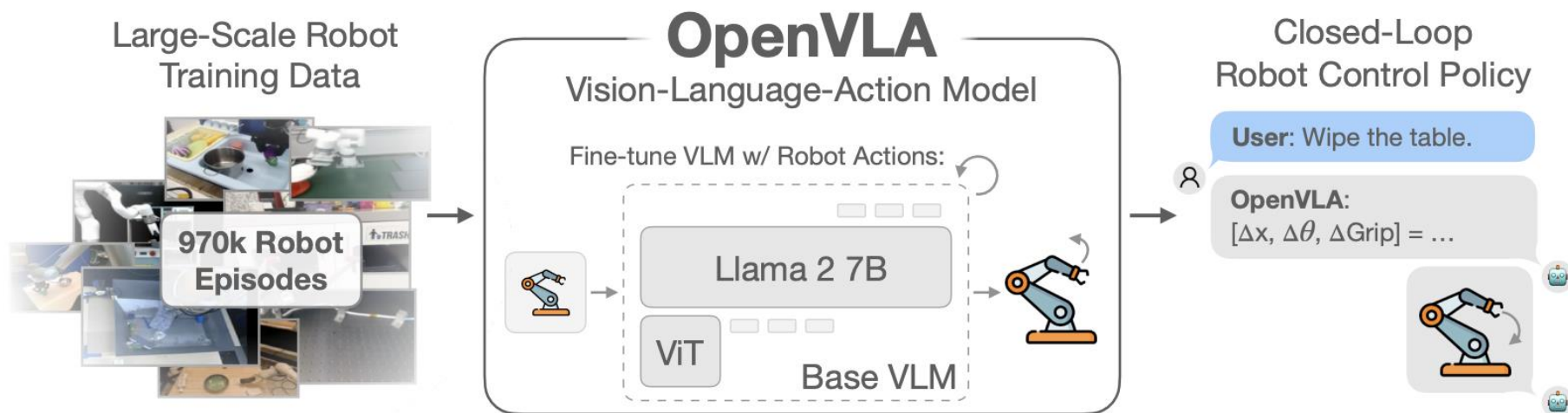
AUTOLab, UC Berkeley



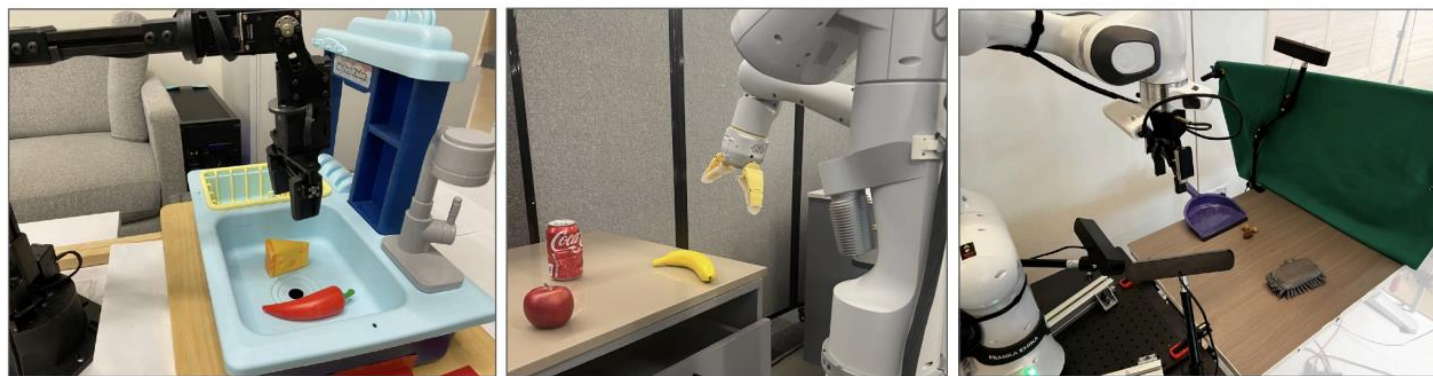
AIS, University of Freiburg



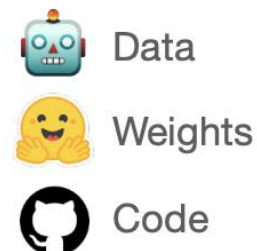
# Vision Language Action Models



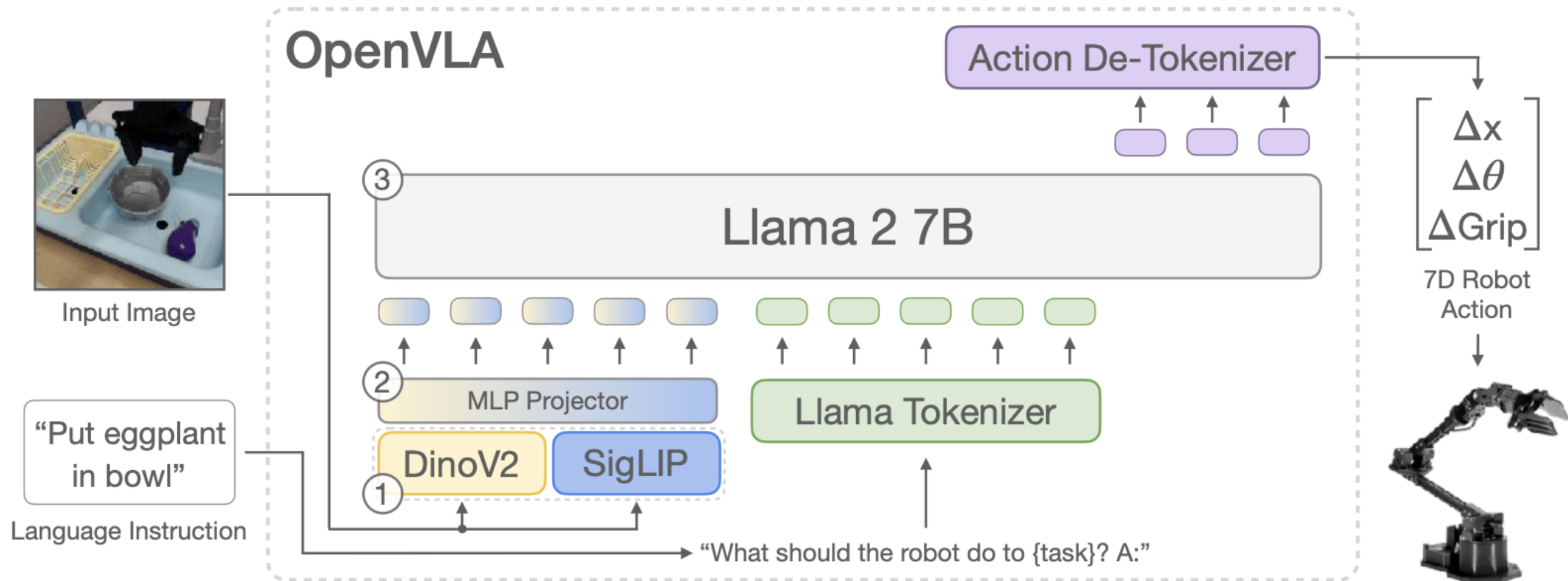
Multi-Robot Control & Efficient Fine-Tuning



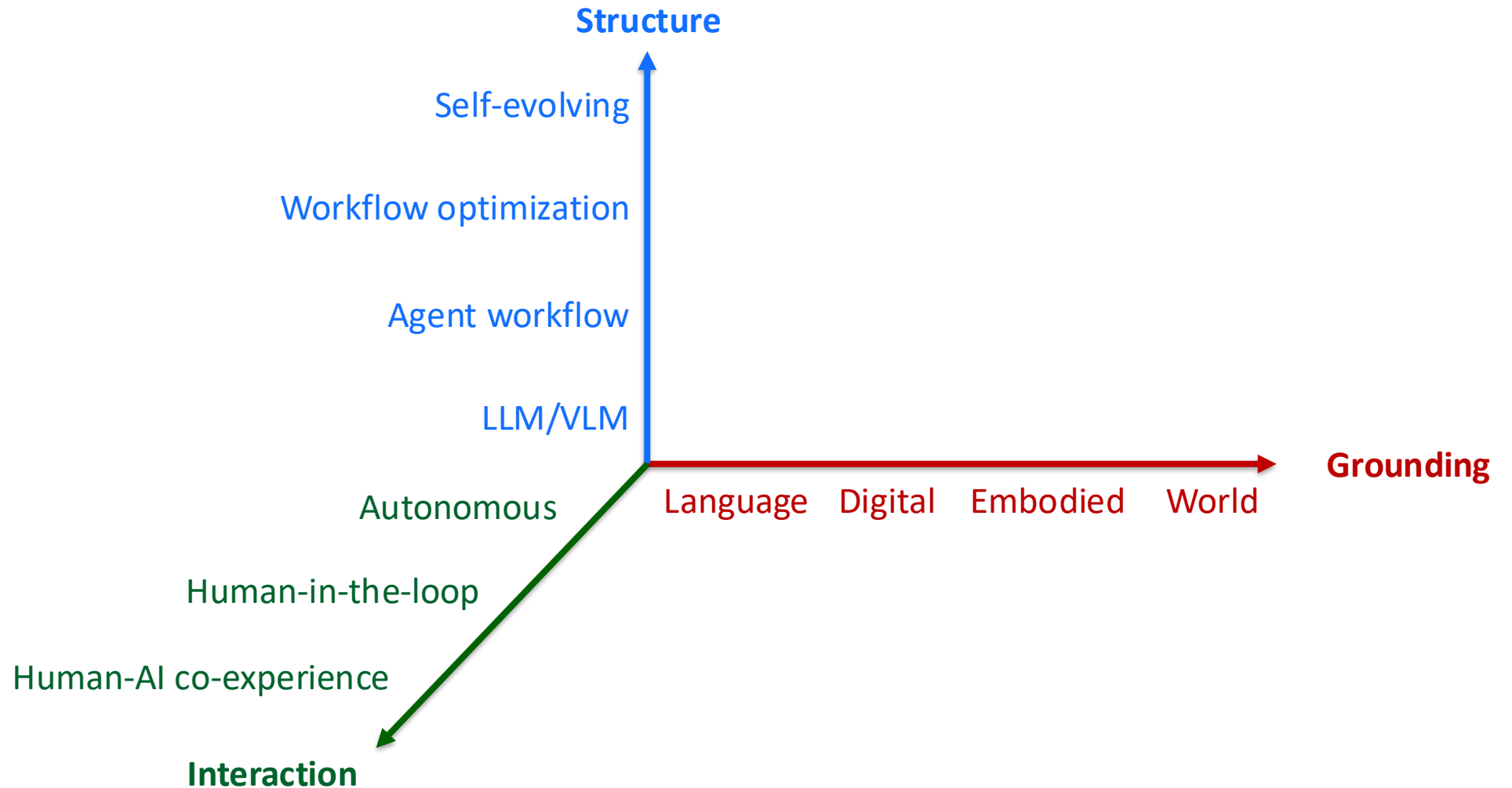
Fully Open-Source



# Vision Language Action Models



# Summary: My Overview of AI Agents



# Assignments for This Coming Week

Project midterm due.

HW4 out, on RL and reasoning.