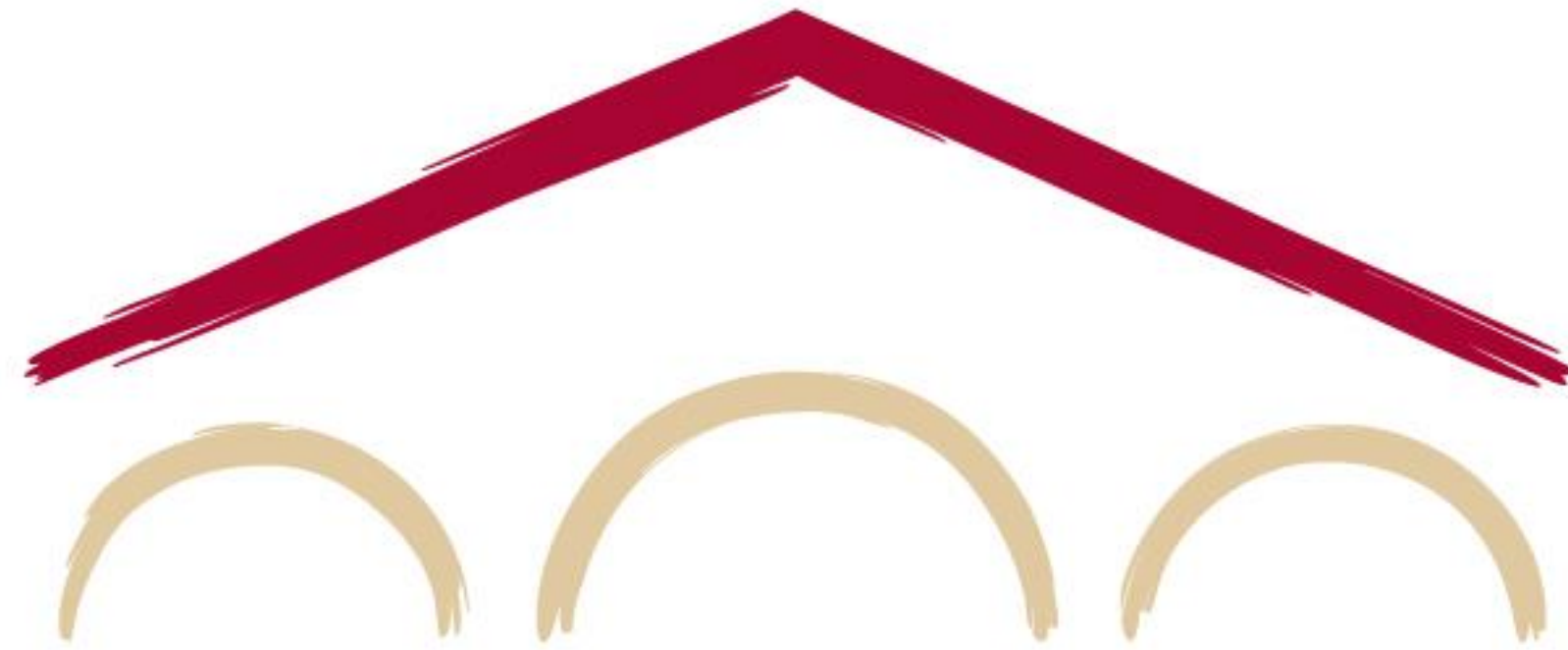


Meaning and Intelligence in Language Models: From Philosophy to Agents in a World

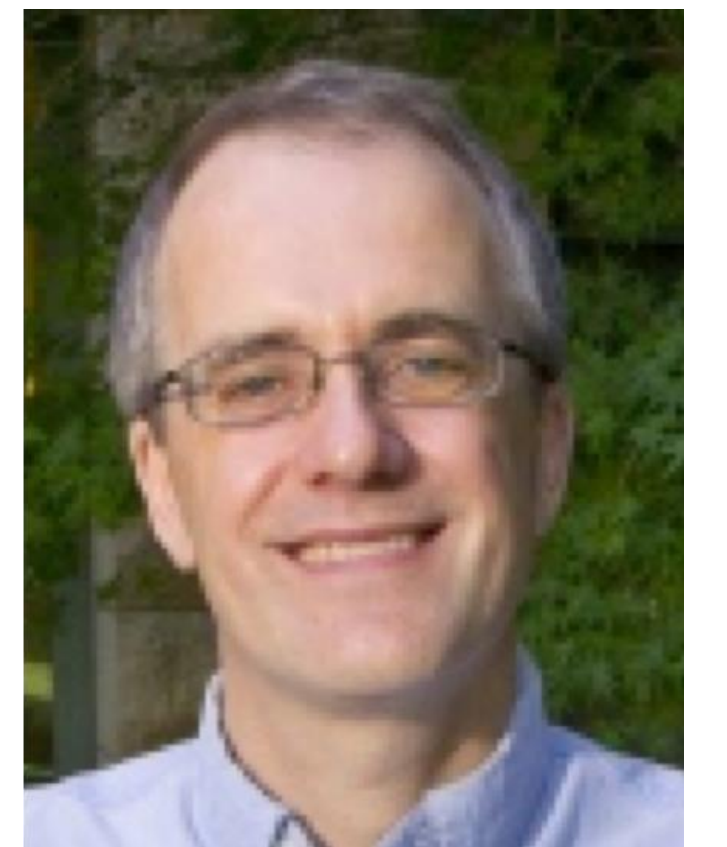


Christopher Manning

@chrmanning ✿ manning@stanford.edu

Stanford NLP Group ✿ Director, Stanford AI Lab

COLM, Philadelphia, 2024



Who should you take your LLM wisdom from in 2024?



or



* Calculated median survival from Gompertz equation, with the assumption that a is 0.05, and R , extrapolated to birth 2.45×10^{-6} .

$$S = e^{-(R_0/a)(1-e^{-at})}$$

References

1. Gavrilov and Gavrilova NS. *The Biology of Life Span, A Quantitative Approach*. Harwood Academic (1991).
2. Brody S. *J. Gen. Physiol.* 6 (1923) 245-257.
3. Jones HR. *Adv. Biol. Med. Physiol.* 4 (1950) 281-337.
4. Hallén A. *Acta Chem. Scand.* 62 (1962) 705-710.
5. " *Biogeront.* 3 (2002) 307-315.
6. " *Biogeront.* 8 (2007) in press.
7. Laurent TC, Killander J. *J. Chromatogr.* 14 (1964) 317-330.
8. Mirtzhal JJ, van Oudenarden A. *Science* 317 (2007) 482-484.
9. Finkel T, Serrano M, Blasco MA. *Nature* 2007;448:767-774.
10. McFarland G.V. Holliday R. *Exptl. Cell Res.* 1994; 212:167-175.
11. Hopkins AH et al. *Mech. Ageing Dev.* 122 (2001) 1431-1445.
12. Verheke et al. *Biogeront.* 3 (2002) 117-126.
13. Olson et al. *Biogeront.* 7 (2006) 221-230.
14. Chondrogianni N et al. *Exp. Gerontol.* 35 (2000) 721-728.
15. Chondrogianni N, Gross ES. *Biogeront.* 9 (2004) 55-61.

DISTRIBUTIONAL CLUSTERING OF ENGLISH WORDS

Fernando Pereira AT&T Bell Laboratories 600 Mountain Ave Murray Hill, NJ 07974, USA pereira@research.att.com

Naffali Tishby Dept. of Computer Science Hebrew University Jerusalem 91904, Israel tishby@cs.huji.ac.il

Lillian Lee Dept. of Computer Science Cornell University Ithaca, NY 14850, USA lllee@cs.cornell.edu

Abstract
We describe and evaluate experimentally a method for clustering words according to their distribution in particular syntactic contexts. Words are represented by the relative frequency distributions of contexts in which they appear, and relative entropy between these distributions is used as the similarity measure for clustering. Clusters are represented by average context distributions derived from the given words according to their probability of cluster membership. In many cases, the clusters can be thought of as encoding coarse semantic distinctions. Deterministic clustering is used to find the best distribution sets of clusters, as the ascending parameter increases, existing clusters become unstable and subdivide, yielding a hierarchical "shell" structure of the data. Clusters are used as the basis for class models of word occurrence, and the models evaluated with respect to hold-out test data.

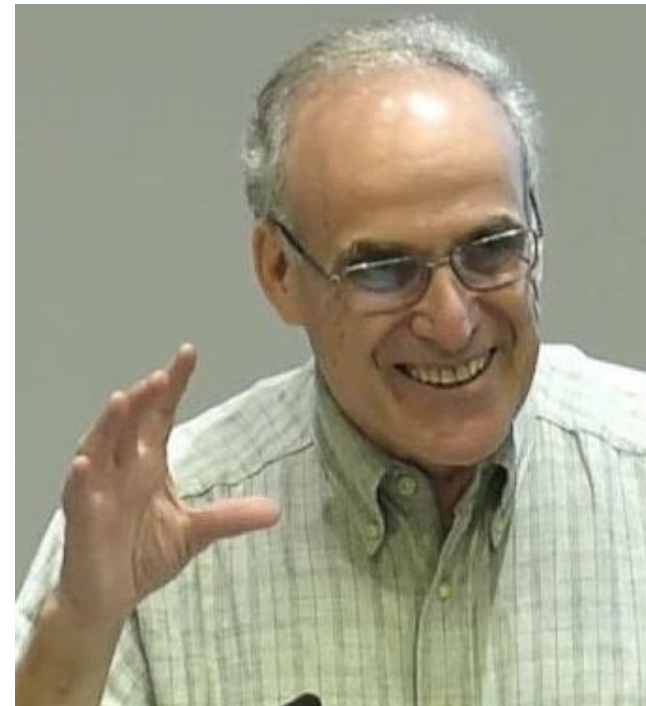
INTRODUCTION
Methods for automatically classifying words according to their context of use have both scientific and practical interest. The scientific question arises in connection with the study of linguistic (particularly lexical) structure and also in relation to the question of lexical acquisition both from psychological and computational learning perspectives. From the practical point of view, word classification addresses questions of data sparseness and generalization in statistical language models, particularly models for deciding among alternative analyses proposed by a grammar.

It is well known that a simple tabulation of frequencies of certain words participating in certain configurations, for example of frequencies of pairs of a restrictive main verb and the head noun of its direct object, cannot be reliably used for comparing the likelihood of different alternative analyses. The problem is that for large enough corpora the number of possible joint events is much larger than the number of event occurrences in the corpus, so many events are never realized or never, making their frequency counts unreliable estimates of their probabilities.

183



Pereira



Tishby



Lee

Distributional Clustering of English Words

Towards History-based Grammars: Using Richer Models for Probabilistic Parsing*

Eraa Black Fred Jelinek John Lafferty David M. Magerman Robert Mercer Salim Roukos IBM T. J. Watson Research Center

Abstract
We describe a generative probabilistic model of natural language, which we call HBG, that takes advantage of detailed linguistic information to resolve ambiguity. HBG incorporates lexical, syntactic, semantic, and structural information from the parse tree into the disambiguation process in a novel way. We use a corpus of bracketed sentences, called a *shell*, in combination with decision tree building to learn on the relevant aspects of a parse tree that will determine the correct parse of a sentence. This stands in contrast to the usual approach of further grammar rules using the usual linguistic information in the hope of generating the correct parse. In head-to-head tests against one of the best existing robust probabilistic parsing models, which we call P-CFG, the HBG model significantly outperforms P-CFG, increasing the parsing accuracy rate from 60% to 75%, a 25% reduction in error.

Introduction
Almost any natural language sentence is ambiguous in structure, reference, or source of meaning. Humans overcome these apparent ambiguities by examining the context of the sentence. But what exactly is context? Frequently, the correct interpretation is apparent from the words and constituents immediately surrounding the phrase in question. This observation leads to the following question: How much information about the context of a sentence or phrase is necessary and sufficient to determine its meaning? This question is at the crux of the debate among computational linguists about the application and implementation of statistical methods in natural language understanding.

Previous work on disambiguation and probabilistic parsing has offered partial answers to this question. Hidden Markov models of words and

31

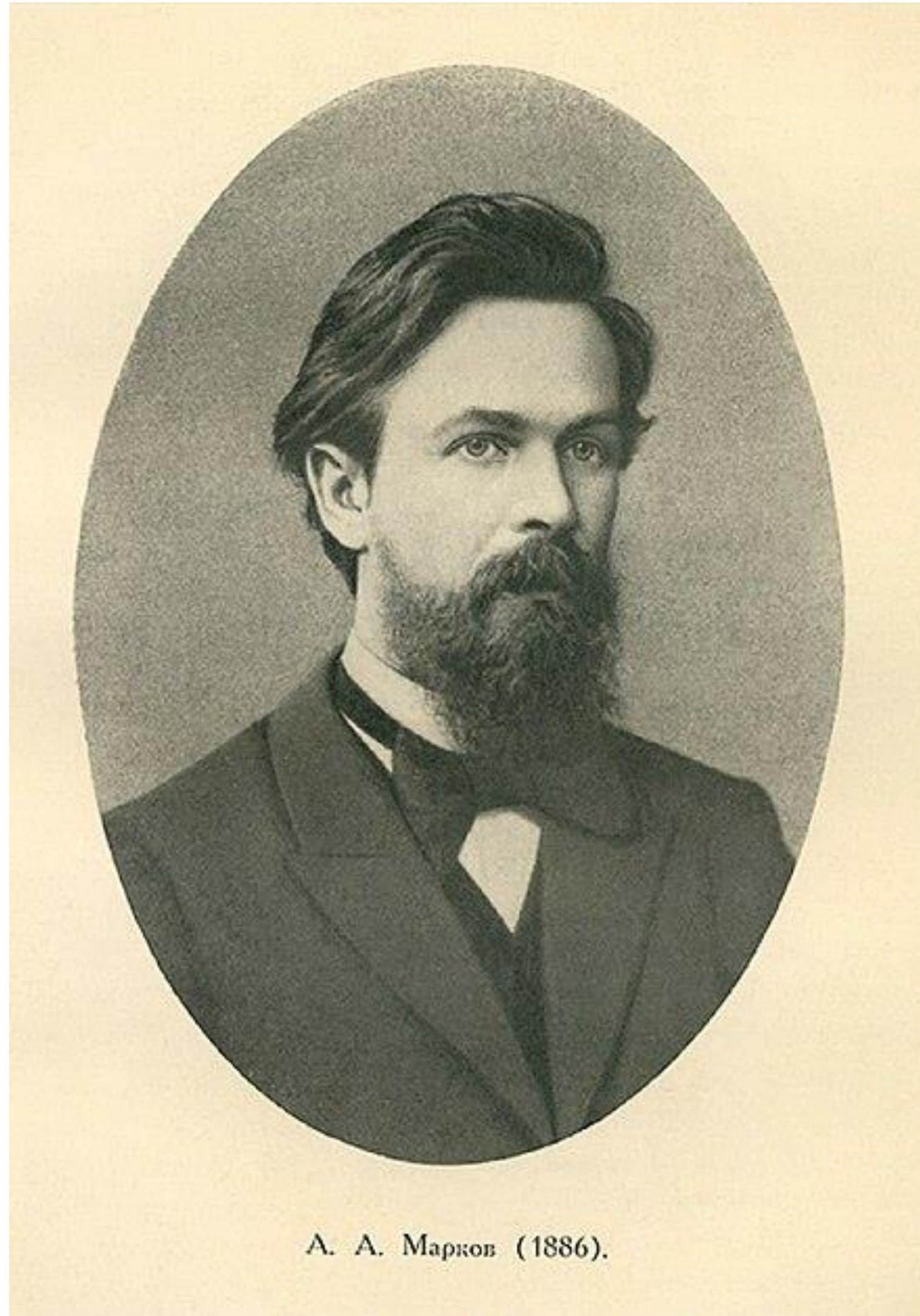


Black Lafferty Mercer Jelinek Magerman Roukos

Towards History-based Grammars: Using Richer Models for Probabilistic Parsing

Why was no one working on language models?

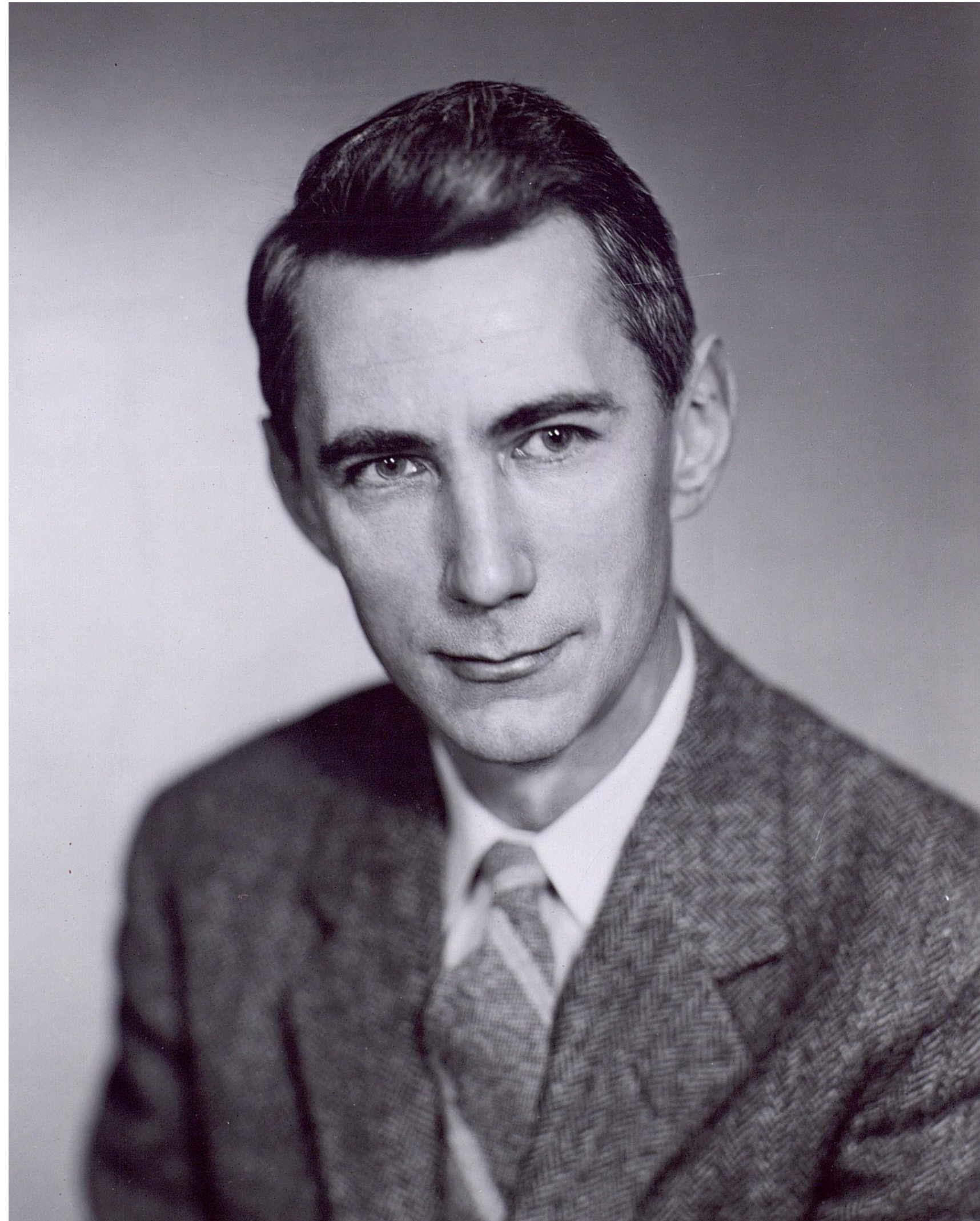
How were they hoping to get to artificial intelligence?



Andrey A. Markov
1856–1922

Transition probabilities (Markov chains)
between consonants and vowels in
Alexander Pushkin's verse novel,
Eugene Onegin

An Example of Statistical Investigation of the Text
Eugene Onegin Concerning the Connection of Samples
in Chains
1913



Claude E. Shannon
1916–2001

A Mathematical Theory of Communication
The Bell System Technical Journal 1948

Prediction and Entropy of Printed English
The Bell System Technical Journal 1951

Explores character and word-level n-gram models, with estimation and generation from a small text sample



The term/concept of a **Language Model**

Invented in Frederick Jelinek's group, IBM

Design of a Linguistic Statistical Decoder for the Recognition of Continuous Speech

IEEE Transactions on Information Theory 21(3), 1975

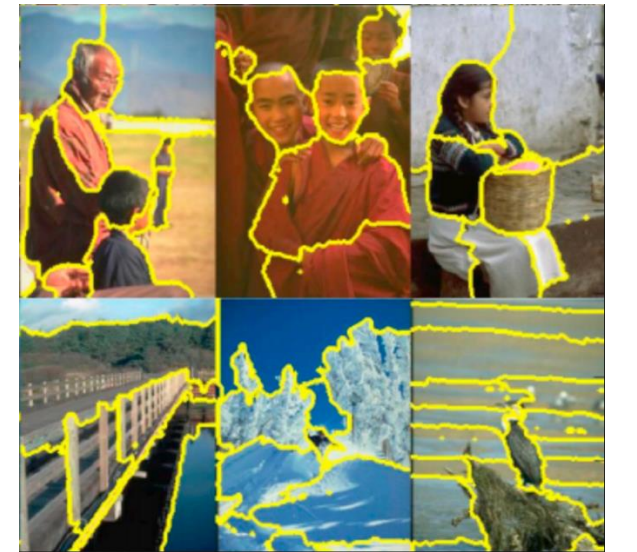
It was work from this group at IBM in the 1970s that defined the **probabilistic language model** of next token prediction that has continued to dominate till today

The bigram "language model" appears earlier, particularly in translations of Russian works. E.g., Igor Mel'chuk (1961) "Some Problems of Machine Translation Abroad" refers to Chomsky's " 'language model' of immediate constituents".
Jelinek may have been influenced by this Russian idiom?

The history of modern (neural) AI/ML that many think of

1950–2004

Experiments on perception and vision,
with minute amounts of data



2005–2009

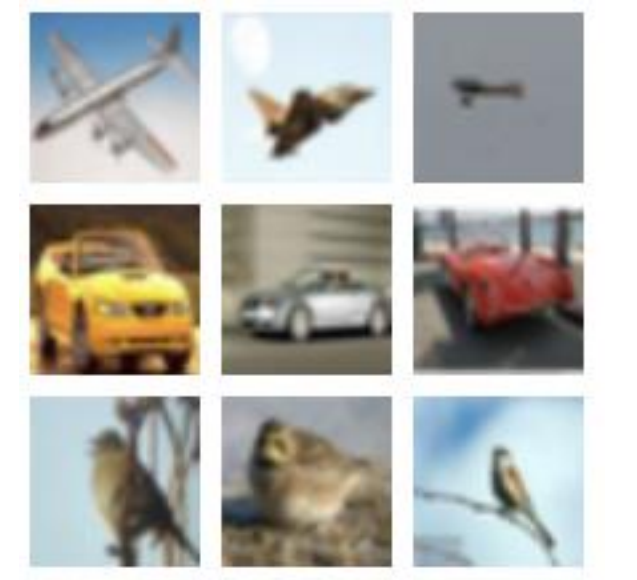
Small modern-style labeled vision datasets

2005–2012 PASCAL VOC 4–20 classes, 15,000 images

2006 Caltech 101 – ~5000 images, 101 classes, ~300x200

2007 Caltech 256 – 30,607 images of 256 classes

2009 CIFAR 10/100 – 600 images of 10/100 classes, 32x32



2010–2017

ImageNet! 1–14 million images, 1000 classes

Big data! Vision object classification is “solved”



standard schnauzer giant schnauzer

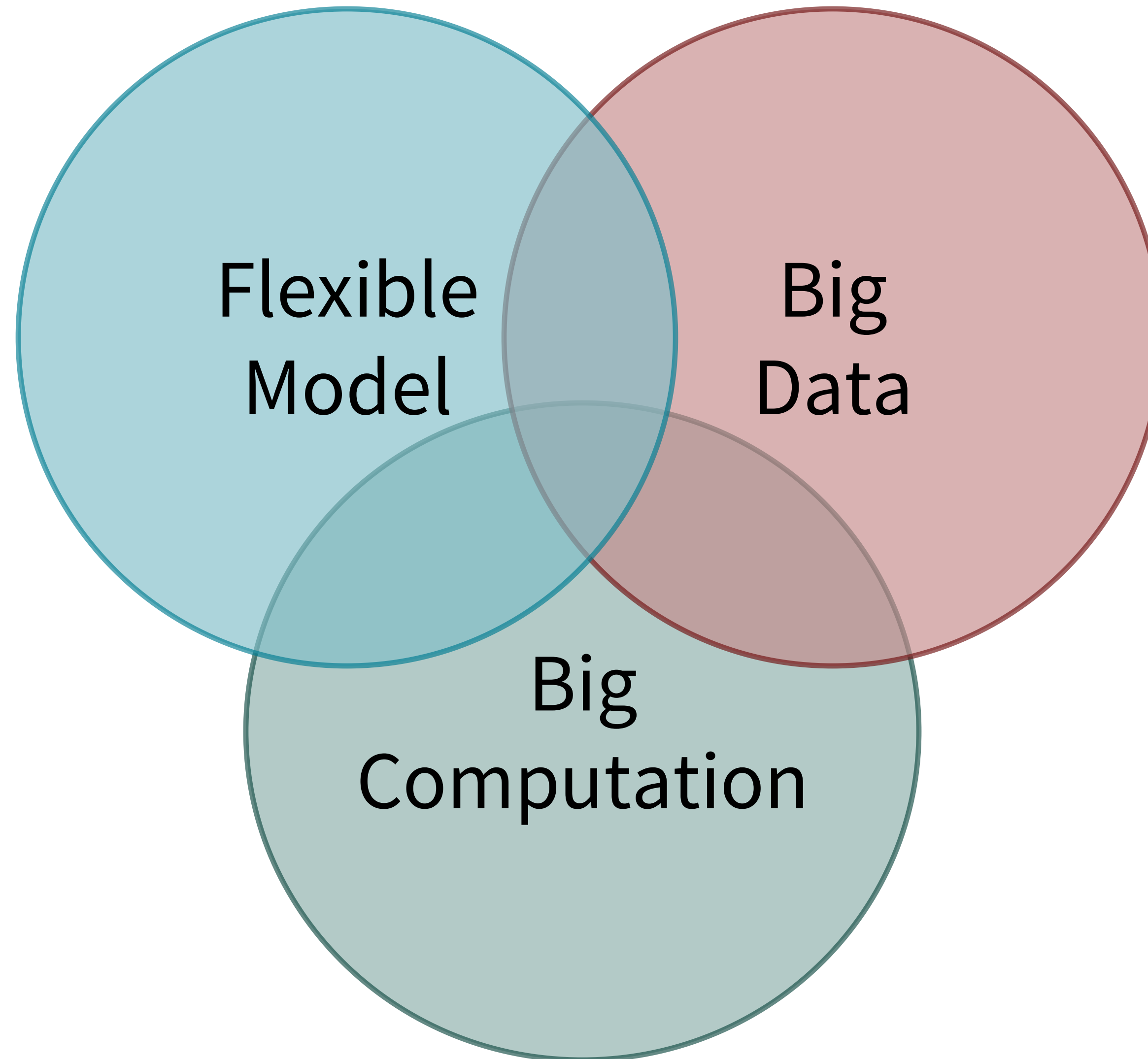


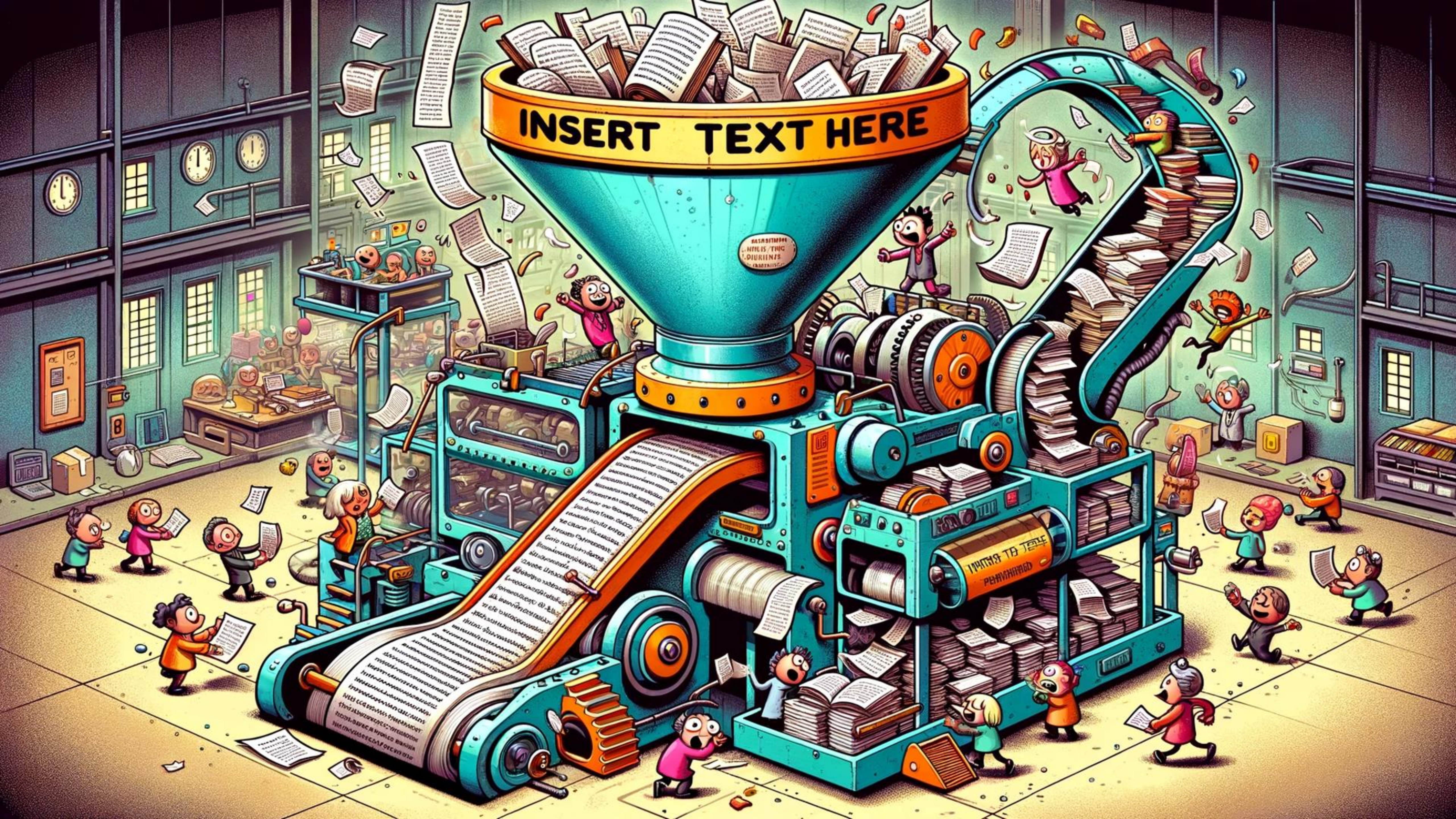
Persian cat Siamese cat

The History of Large Language Models

- 1998 CPAT-Tree-Based Language Models with an Application for Text Verification in Chinese. ROCLing 1998. First use of “LLM” trigram I know of; 200M word corpus
- 2000 A Neural Probabilistic Language Model. Bengio, Ducharme & Vincent NIPS 2000
First neural language model built on 32 million token corpus, 31K vocab
- 2007 Large Language Models in Machine Translation. Brants, Popat, Xu, Och and **Dean**. EMNLP 2007. **2 trillion token corpus** n-gram model of up to 5-grams
- 2018 **GPT** (Radford, Narasimhan, Salimans & Sutskever) and **BERT** (Devlin, Chang, Lee & Toutanova). 3.3 billion token corpus
- 2020– 100+ billion parameter neural language models trained on > 1 trillion tokens: GPT-3, GPT-4, PaLM 2, Llama 3, Nemotron-4,

LLMs need all the trinity of modern deep learning





INSERT TEXT HERE

ИМПУЛЬС
ИМПУЛЬС
ИМПУЛЬС

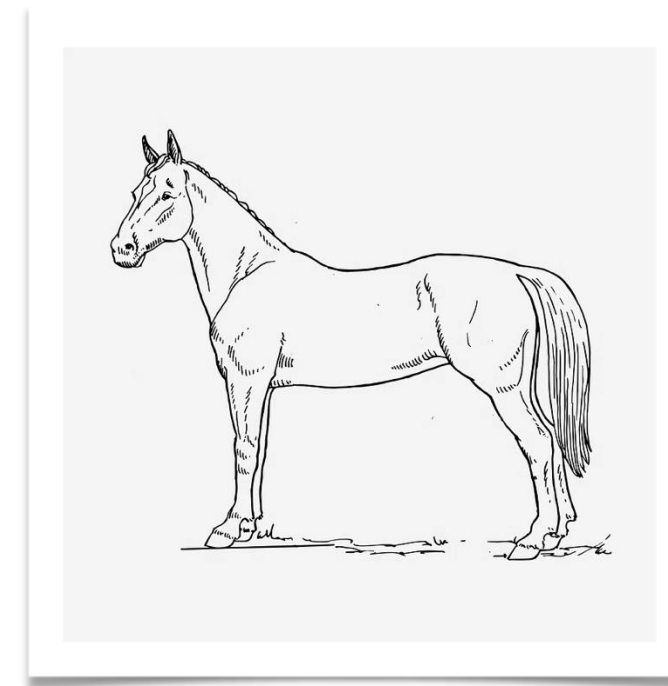
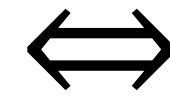
ИМПУЛЬС
ИМПУЛЬС

ИМПУЛЬС
ИМПУЛЬС
ИМПУЛЬС

Form vs. reference: Meaning as a relation between form and “communicative intent”

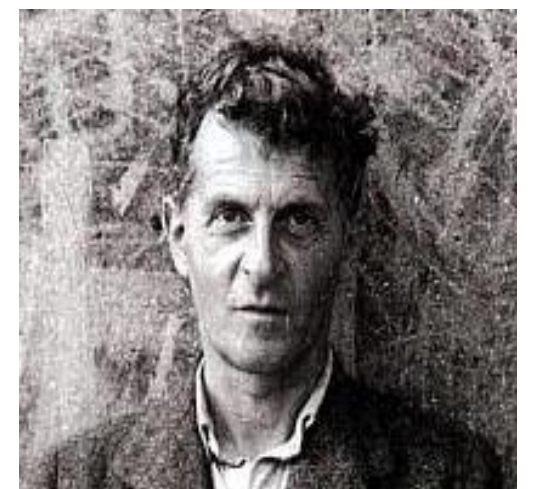
Bender and Koller (2020): “(linguistic) meaning [is] the relation between a linguistic form and communicative intent.”

horse



“the language modeling task, because it only uses form as training data, cannot in principle lead to learning of meaning”

“You say: the point isn’t the word, but its meaning, and you think of the meaning as a thing of the same kind as the word, though also different from the word. Here the word, there the meaning. The money, and the cow that you can buy with it. (But contrast: money, and its use.)”

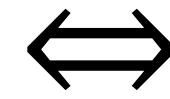


– Ludwig Wittgenstein. 1953. *Philosophical Investigations*, §120

Form vs. reference: Meaning as a relation between form and the world

The classic referentialist position, which has dominated recent linguistic semantics, attempts to ground meaning in the world:

horse



This might suggest that a plain language model has no notion of meaning, but a visual language model does?

Somehow, a primacy is given to certain kinds of sensory evidence, even though everything ends up as electrical signals in our brains.

Would we really want to say that a VLM captures meaning but a pure LLM does not?

I personally think not.

The alternative: Inferentialism/pragmatism

“For a large class of cases—though not for all—in which we employ the word ‘meaning’ it can be defined thus: the meaning of a word is its use in the language.”

– Wittgenstein, 1953, §43

Inferentialism couches understanding as an appreciation of appropriate vs. inappropriate ways to use language in a context. Often summed up as: **a use theory of meaning**


This context might be visual, textual, conversational, sociological, etc.

The real world may in some sense be privileged, but it is not the only context for grounding meaning: We also have virtual worlds and language contexts

This is essentially the notion of meaning that Turing (1950) also argued for, if perhaps partly for practical reasons

Under this notion, meaning is gradient: You can partially understand appropriate contexts of use

What is the meaning of 'shehnai'

1. You can have seen or held one and have a classic grounded meaning
 2. I can at least show you a picture 
 3. But surely the meaning that you have for the word 'shenai' would be richer if you had heard one played?
 4. If I have never seen, felt, or heard a shehnai, but someone tells me it is a traditional Indian instrument, a bit like an oboe, then surely the word has some meaning for me?
 - A connection to India, to wind instruments that use reeds, to playing music
- It gives me a reasonable approximation of appropriate contexts of use
5. If they added that it has holes sort of like a recorder, but it has multiple reeds and a flared end more like an oboe, then I have more "meaning"



What is the meaning of 'shehnai'

- What if all I have is one or more contexts of word use (like an LLM commonly gets)?
 - *“From a week before, shehnai players sat in bamboo machans at the entrance to the house, playing their pipes. Bikash Babu disliked the shehnai’s wail, but was determined to fulfil every conventional expectation the groom’s family might have.”*
 - From: Anuradha Roy, *An Atlas of Impossible Longing* (New York: Free Press, 2011)
- In some ways, I understand the meaning of the word 'shehnai' rather less than someone who has seen one, but:
 - I still know that it is a pipe-like musical instrument
 - My meaning of 'shehnai' is not a subset of the meaning of the person who has only held a shehnai, for I know some additional musical and cultural information on likely appropriate use that they lack




Large Language Models and “Intelligence”

Since ChatGPT, in the popular imagination, large language models have essentially become synonymous with **artificial intelligence**

The **artificial** part is easy. What is **intelligence**?

Is language understanding and generation distinct from general intelligence?

TICS 2534 No. of Pages 24 **ARTICLE IN PRESS**

Trends in Cognitive Sciences 

Feature Review

Dissociating language and thought in large language models

Kyle Mahowald,^{1,5,*} Anna A. Ivanova,^{2,5,*} Idan A. Blank,^{3,*} Nancy Kanwisher,^{4,*} Joshua B. Tenenbaum,^{4,*} and Evelina Fedorenko^{4,*}

Large language models (LLMs) have come closest among all models to date to mastering human language, yet opinions about their linguistic and cognitive capabilities remain split. Here, we evaluate LLMs using a distinction between formal linguistic competence (knowledge of linguistic rules and patterns) and functional linguistic competence (understanding and using language in the world). We ground this distinction in human neuroscience, which has shown that formal and functional competence rely on different neural mechanisms. Although LLMs are surprisingly good at formal competence, their performance on functional competence tasks remains spotty and often requires specialized fine-tuning and/or coupling with external modules. We posit that models that use language in human-like ways would need to master both of these competence types, which, in turn, could require the emergence of separate mechanisms specialized for formal versus functional linguistic competence.

Highlights
Formal linguistic competence (getting the form of language right) and functional linguistic competence (using language to accomplish goals in the world) are distinct cognitive skills.
The human brain contains a network of areas that selectively support language processing (formal linguistic competence), but not other domains like logical or social reasoning (functional linguistic competence).
In the late 2010s, large language models trained on word prediction tasks began achieving unprecedented success in formal linguistic competence, showing impressive performance on linguistic tasks that likely require hierarchy and abstraction.
Consistent performance on tasks requiring functional linguistic competence is harder to achieve for large language models and often involves augmentations beyond next word prediction.
Evidence from cognitive science and neuroscience can illuminate the capabilities and limitations of large language models and pave the way toward better, human-like models of both language and thought.

The language–thought conflation
When we hear a sentence, we typically assume that it was produced by a rational, thinking agent (another person). The sentences that people generate in day-to-day conversations are based on their world knowledge (“Not all birds can fly.”), their reasoning abilities (“You’re 15, you can’t go to a bar.”), and their goals (“Would you give me a ride, please?”). Thus, we often use other people’s statements as a window into their minds.

In 1950, Alan Turing leveraged this tight relationship between language and thought to propose his famous test [1]. The Turing test uses language as an interface to cognition, allowing a human participant to probe the knowledge and reasoning capacities of two conversation partners to determine which of them is a human and which is a machine. Although the utility of the Turing test has since been questioned, it has undoubtedly shaped the way society today thinks of machine intelligence [2].

The popularity of the Turing test, combined with language–thought coupling in everyday life, has led to several common fallacies related to the language–thought relationship. One fallacy is that **an entity (be it a human or a machine) that is good at language must also be good at thinking**. If an entity generates coherent stretches of text, it must possess rich knowledge and reasoning capacities. Let’s call this the **‘good at language -> good at thought’ fallacy**. This fallacy has come to the forefront due to the recent rise of **large language models (LLMs)** (see **Glossary**), including OpenAI’s GPT models, Anthropic’s Claude, and more open alternatives [3] like Meta’s LLaMa models and EleutherAI’s GPT-J. LLMs today can produce text that is difficult to distinguish from human output, outperform humans at some text comprehension tasks [4,5], and show superhuman performance on next-word prediction [6]. As a result, claims have emerged, both in the popular press and in the academic literature, that LLMs are not only a major advance in language processing, but are also showing **‘sparks of artificial general**

¹The University of Texas at Austin, Austin, TX, USA
²Georgia Institute of Technology, Atlanta, GA, USA
³University of California, Los Angeles, CA, USA
⁴Massachusetts Institute of Technology, Cambridge, MA, USA
⁵These authors contributed equally to this work

Trends in Cognitive Sciences, Month 2024, Vol. xx, No. xx <https://doi.org/10.1016/j.tics.2024.01.011> 1
© 2024 Elsevier Ltd. All rights reserved.



CALIFORNIA REPUBLIC

CA AB 2885

Section 11546.45.5 of the California Government Code (2024-09-28):

“Artificial intelligence” means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments



Intelligence vs. knowledge or task effectiveness

More commonly ...

We confuse being knowledgeable with being intelligent

Or the ability to do tasks?

AGI: “ability to perform most (cognitive/ economically valuable) tasks at or above the level of the average person”

Intelligence

“an agent’s ability to achieve goals in a wide range of environments”
– Shayne Legg and Marcus Hutter (2006)

“the ability to **learn** and perform a range of techniques to solve problems and achieve goals, **appropriate to the context in an uncertain, ever-varying world**”
– Christopher Manning

Some amazing reasoning examples now work in LLMs!

openai/text-davinci-002

The cost to produce a book is 1000 dollars plus 8 dollars per book. The book sells for 20 dollars each. How many books must be sold to make a profit?

1250 books must be sold to make a profit.

The cost to produce a book is 1000 dollars plus 8 dollars per book. The book sells for 20 dollars each. How many books must be sold to make a profit? Let's work step by step.

The cost of producing 1 book is $1000 + 8 = 1008$ dollars.
The cost of producing 2 books is $1008 + 8 = 1016$ dollars.
Therefore, the cost of producing n books is:

$$\text{Cost} = 1008 + 8n$$

The selling price of 1 book is \$20.

The selling price of 2 books is \$40.

The selling price of n books is:

$$\text{Selling Price} = 20n$$

We want to find how many books must be sold in order to make a profit. That is, we want to find n such that:

Cost < Selling Price

$$1008 + 8n < 20n$$

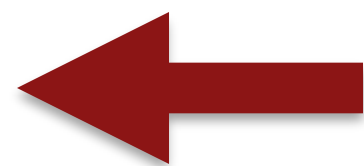
$$8n < 20n - 1008$$

$$-1008 < 12n$$

$$1000 < 12n$$

$$83.33 < n$$

Therefore, n must be greater than 83.33 in order to make a profit.



To determine how many books must be sold to make a profit, we need to figure out when the revenue from selling the books exceeds the total cost of producing them.

Let:

- x be the number of books sold.
- The cost to produce x books is:

$$\text{Total cost} = 1000 + 8x$$

(where 1000 dollars is the fixed cost, and 8 dollars is the variable cost per book).

- The revenue from selling x books is:

$$\text{Revenue} = 20x$$

(where each book is sold for 20 dollars).

To make a profit, the revenue must be greater than the total cost:

$$20x > 1000 + 8x$$

Solving the inequality:

1. Subtract $8x$ from both sides:

$$20x - 8x > 1000$$

$$12x > 1000$$

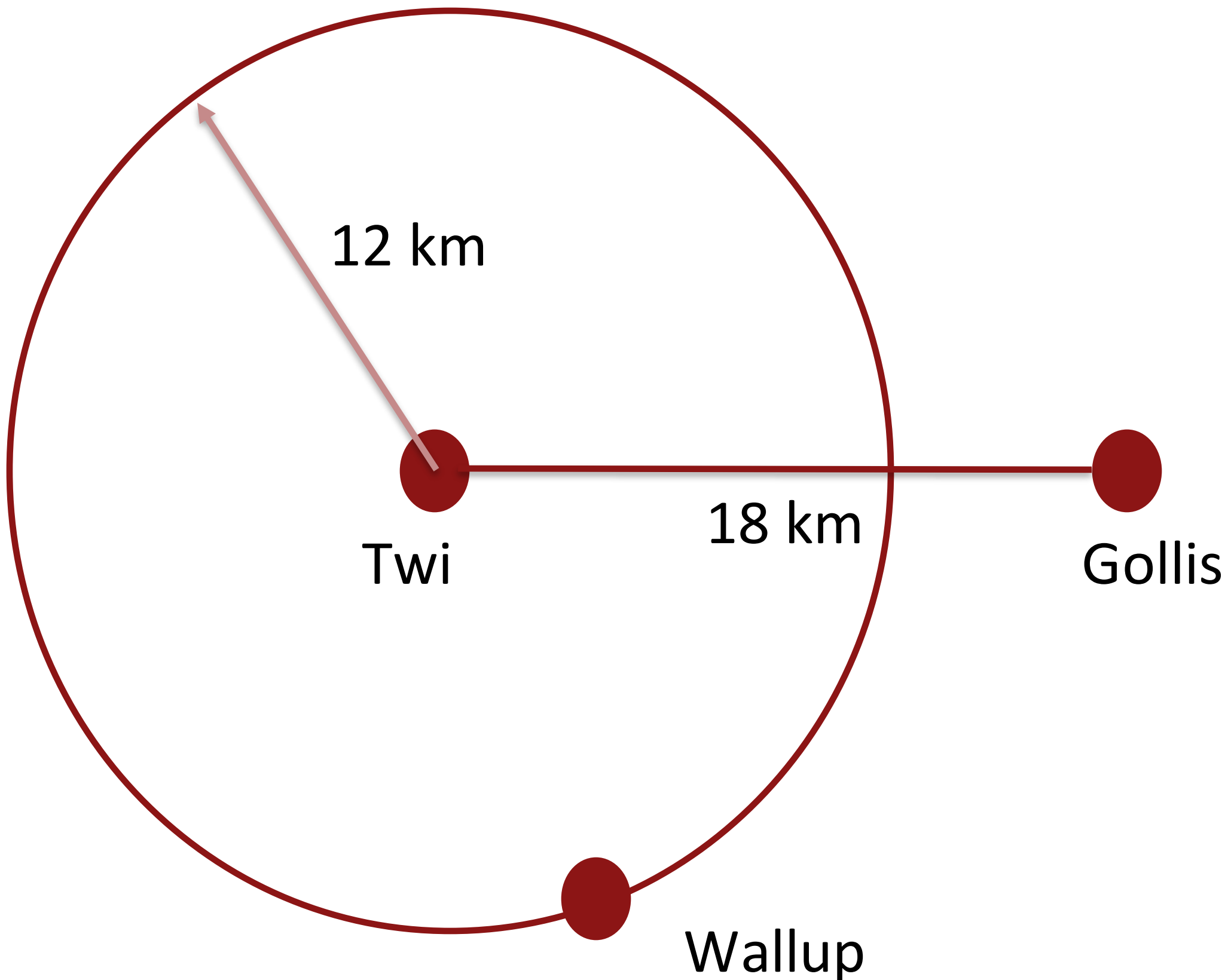
2. Divide both sides by 12:

$$x > \frac{1000}{12} \approx 83.33$$

Since x must be a whole number, you need to sell at least **84 books** to make a profit.



If the town of Twi is 12 km from the town of Wallup, and the town of Gollis is 18 km from the town of Twi, what is the maximum and minimum possible distance the town of Wallup is from Gollis?



To find the **maximum** and **minimum** possible distances between **Wallup** and **Gollis**, let's consider the two possible configurations for the positions of the towns.

1. Maximum Possible Distance:

For the maximum distance between Wallup and Gollis, Wallup and Gollis would be on **opposite sides of Twi** in a straight line. In this case, the total distance would be the sum of the two distances:

- **Wallup to Twi** = 12 km
- **Twi to Gollis** = 18 km

So, the maximum possible distance is:

$$\text{Maximum distance} = 12 \text{ km} + 18 \text{ km} = 30 \text{ km}$$

2. Minimum Possible Distance:

For the minimum distance, Wallup, Twi, and Gollis would be in a straight line, with Gollis on the **same side** of Twi as Wallup. In this case, the minimum possible distance would be the difference between the two distances:

- **Wallup to Twi** = 12 km
- **Twi to Gollis** = 18 km

The minimum possible distance is:

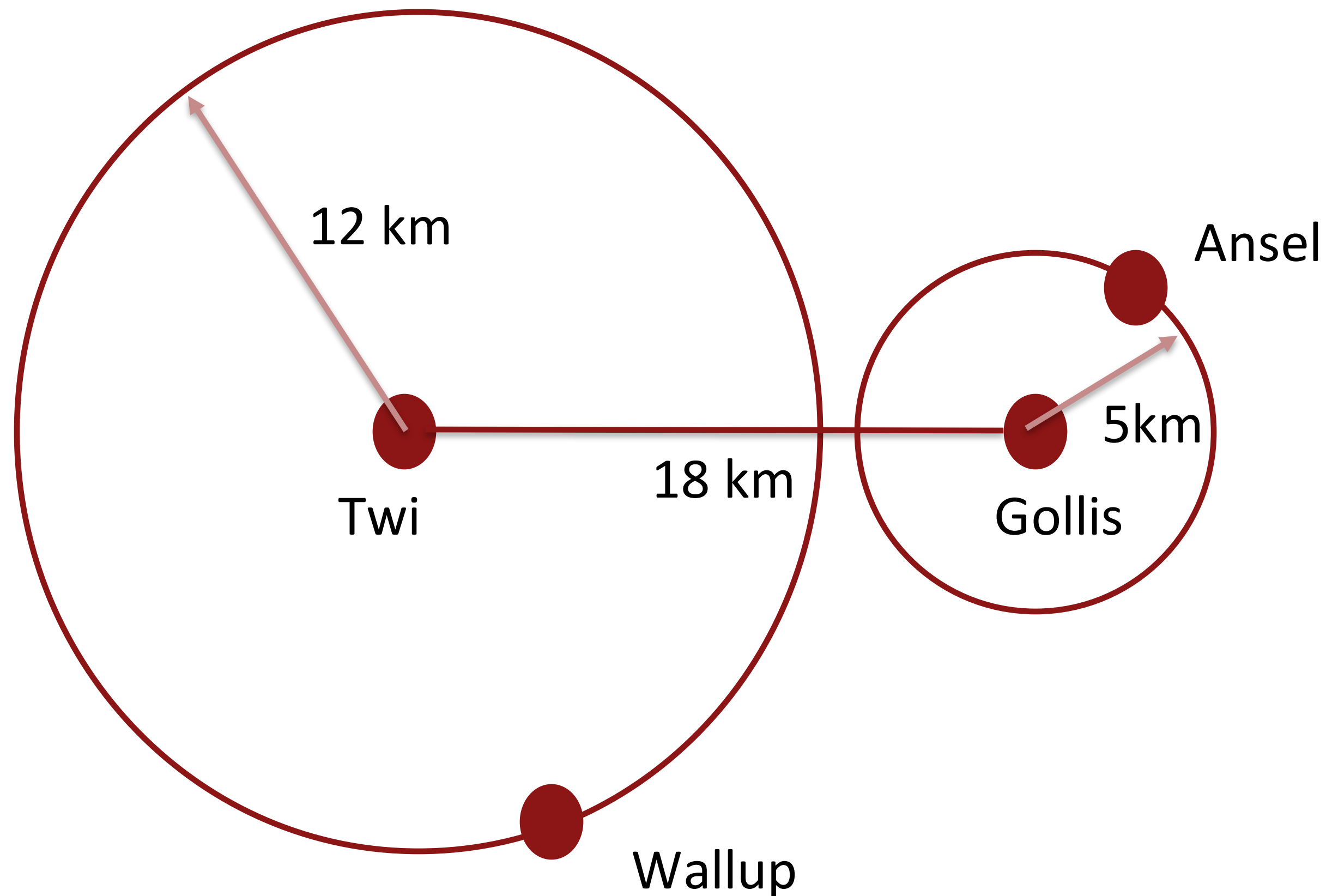
$$\text{Minimum distance} = |18 \text{ km} - 12 \text{ km}| = 6 \text{ km}$$

Conclusion:

- The **maximum distance** between Wallup and Gollis is **30 km**.
- The **minimum distance** between Wallup and Gollis is **6 km**.



If the town of Twi is 12 km from the town of Wallup, the town of Gollis is 18 km from the town of Twi, and the town of Ansel is 5 km from the town of Gollis, what is the maximum and minimum possible distance the town of Ansel is from Gollis?



Let's explore the problem step by step:

You want to know the **maximum** and **minimum** possible distances between the town of **Ansel** and the town of **Wallup**. We know the following distances:

- Wallup to Twi = 12 km
- Twi to Gollis = 18 km
- Gollis to Ansel = 5 km

Maximum Possible Distance:

For the **maximum possible distance** between **Ansel** and **Wallup**, the towns would need to be laid out in a straight line with Ansel on the opposite side of Gollis from Wallup. This would give us the longest possible distance by adding all the segments together:

- Wallup to Twi = 12 km
- Twi to Gollis = 18 km
- Gollis to Ansel = 5 km

So, the maximum possible distance from **Ansel to Wallup** is:

$$\text{Maximum distance} = 12 \text{ km} + 18 \text{ km} + 5 \text{ km} = 35 \text{ km}$$

Minimum Possible Distance:

For the **minimum possible distance**, Ansel would be on the same side of Gollis as Wallup, and we would subtract the distance between Ansel and Gollis from the other distances:

- Wallup to Twi = 12 km
- Twi to Gollis = 18 km
- Gollis to Ansel = 5 km

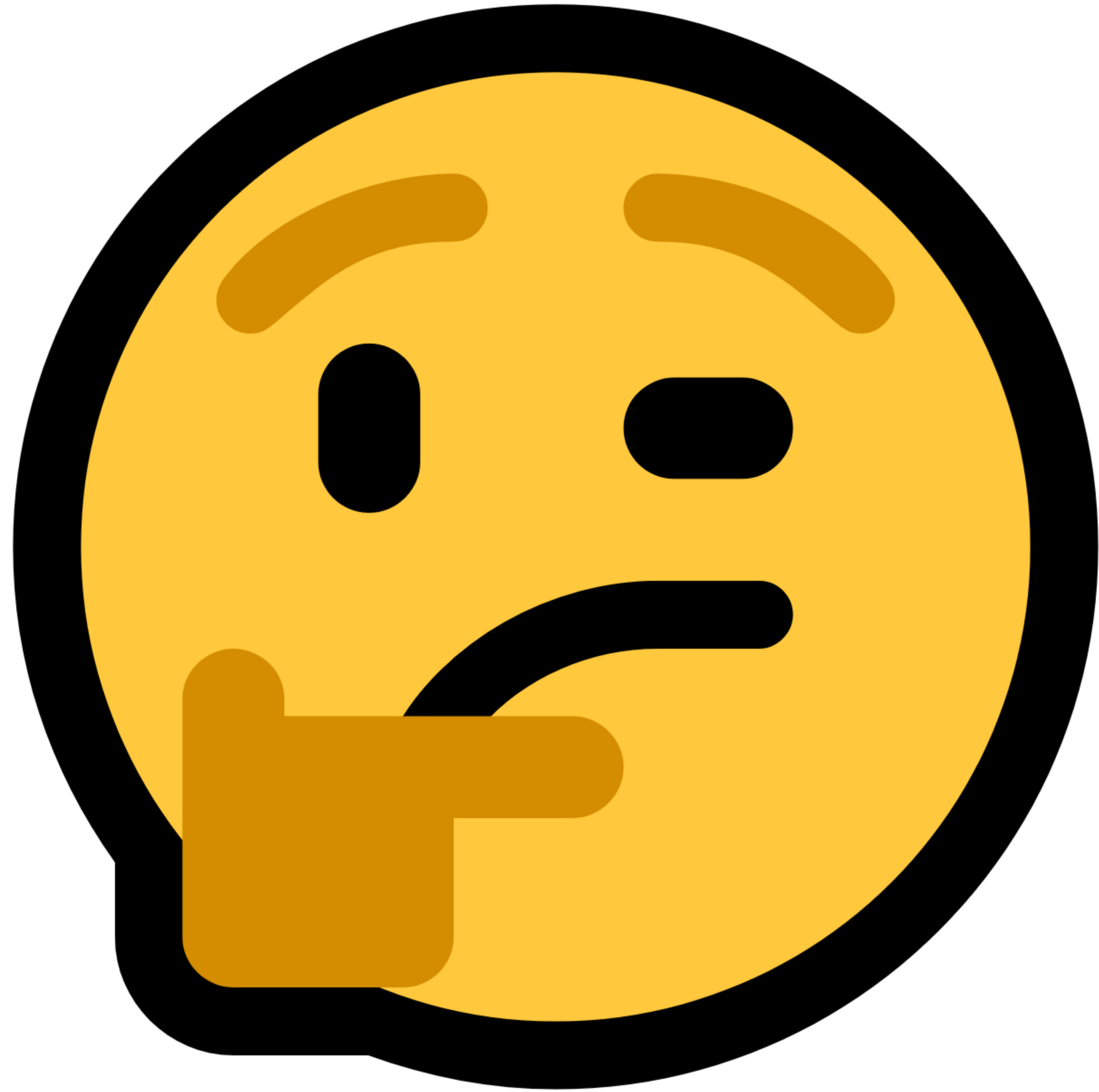
The minimum possible distance is:

$$\text{Minimum distance} = (18 \text{ km} - 5 \text{ km}) + 12 \text{ km} = 25 \text{ km}$$

Conclusion:

- The **maximum distance** from **Ansel to Wallup** is 35 km.
- The **minimum distance** from **Ansel to Wallup** is 25 km.





1st Workshop on System-2 Reasoning at Scale

December 15, 2024. [NeurIPS](#) Workshop, Vancouver, Canada

- What do we need to imbue language models with System-2 reasoning capabilities?
- Are scale and the “bitter lesson” going to dictate how the future of AI technology will unfold?
- Do we need a different mechanism for implementing System-2 reasoning, or should it be a property that emerges from a possibly different training method?
- How do we benchmark System-2-like generalization? How do we avoid data contamination?

Speakers + Panelists



Melanie Mitchell



Joshua Tenenbaum



François Chollet



Dzmitry Bahdanau



Tal Linzen



Jason Weston

Organizers



Shikhar Murty



Federico Bianchi



Róbert Csordás



Nouha Dziri



Alex Gu



Shunyu Yao

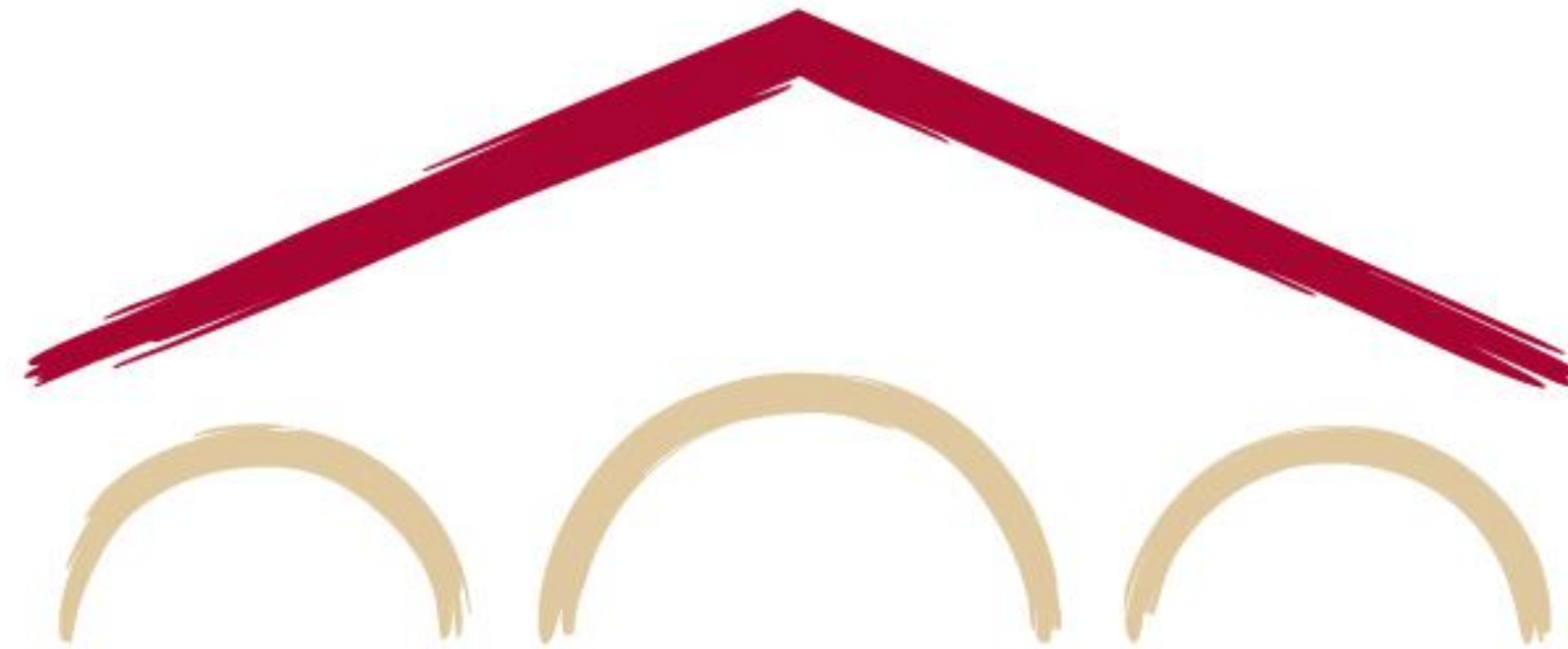


Chris Manning

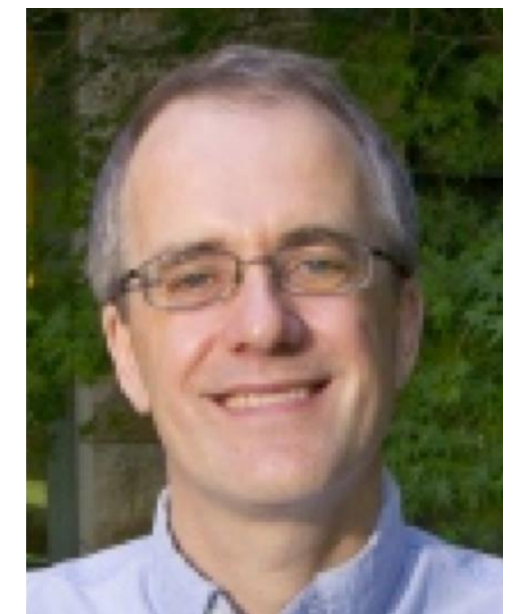


Yejin Choi

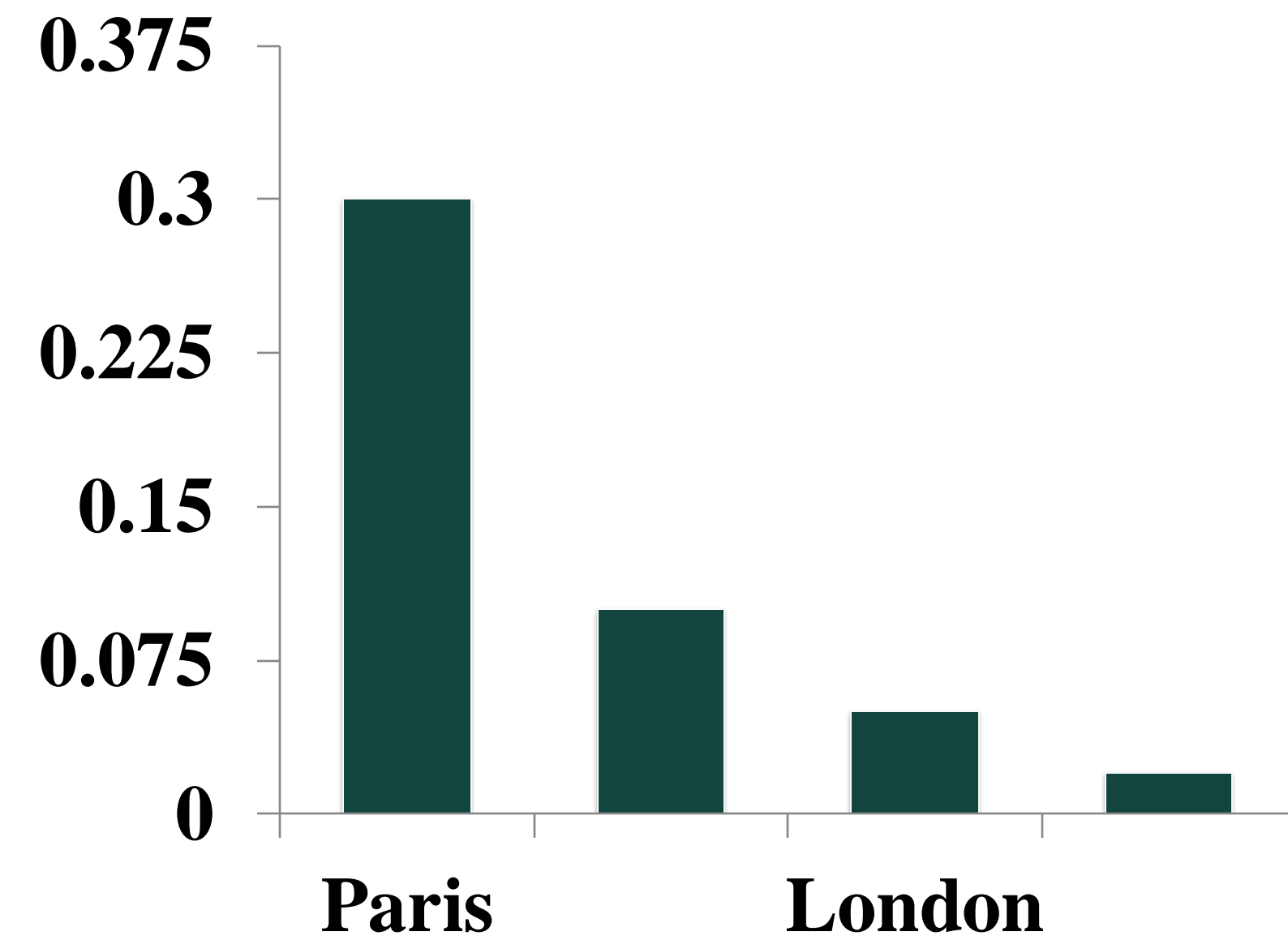
Learning Grounded Instruction Following with Language Models



Shikhar Murty



Grounded Instruction Following with Language Models?



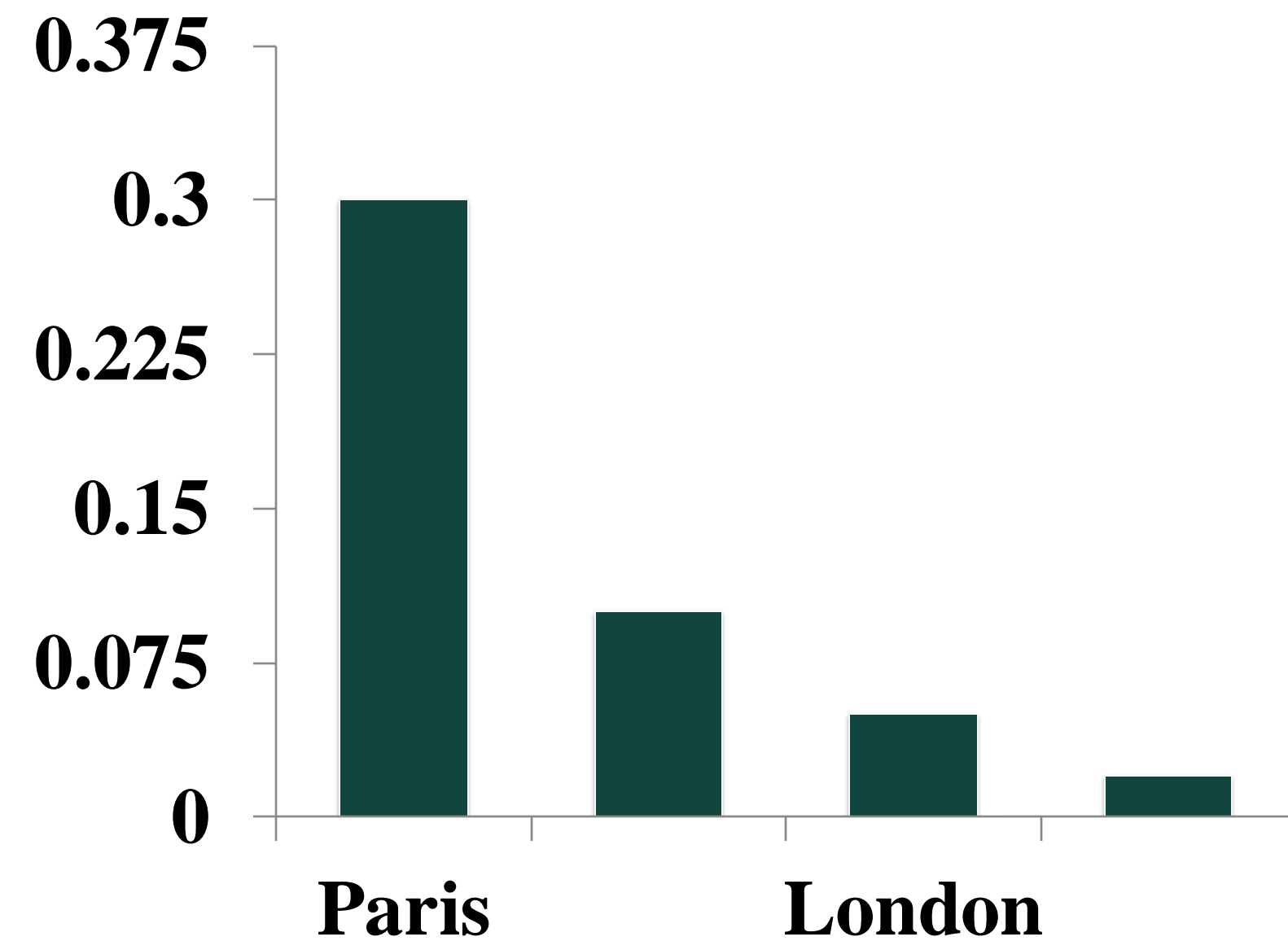
The capital of Paris is _____

Language Model



Grounded Instruction Following with Language Models?

First Attempt: Zero-shot instruction following



The capital of Paris is ____

Language Model



$$\pi_{\text{LM}}(\cdot | g)$$

Language
Model
Policy

```
You are an agent capable of the
following actions:
1.Type X on Y
2.Move mouse to X
3.Click on X
4.Hover on element X
5. ...
Your objective is to follow user instructions,
by mapping them into a sequence of actions.
Instruction: {g}

So far, you have taken the following actions:
a1:
a2:
...
After executing these actions, you observe
the following HTML state: <HTML state>

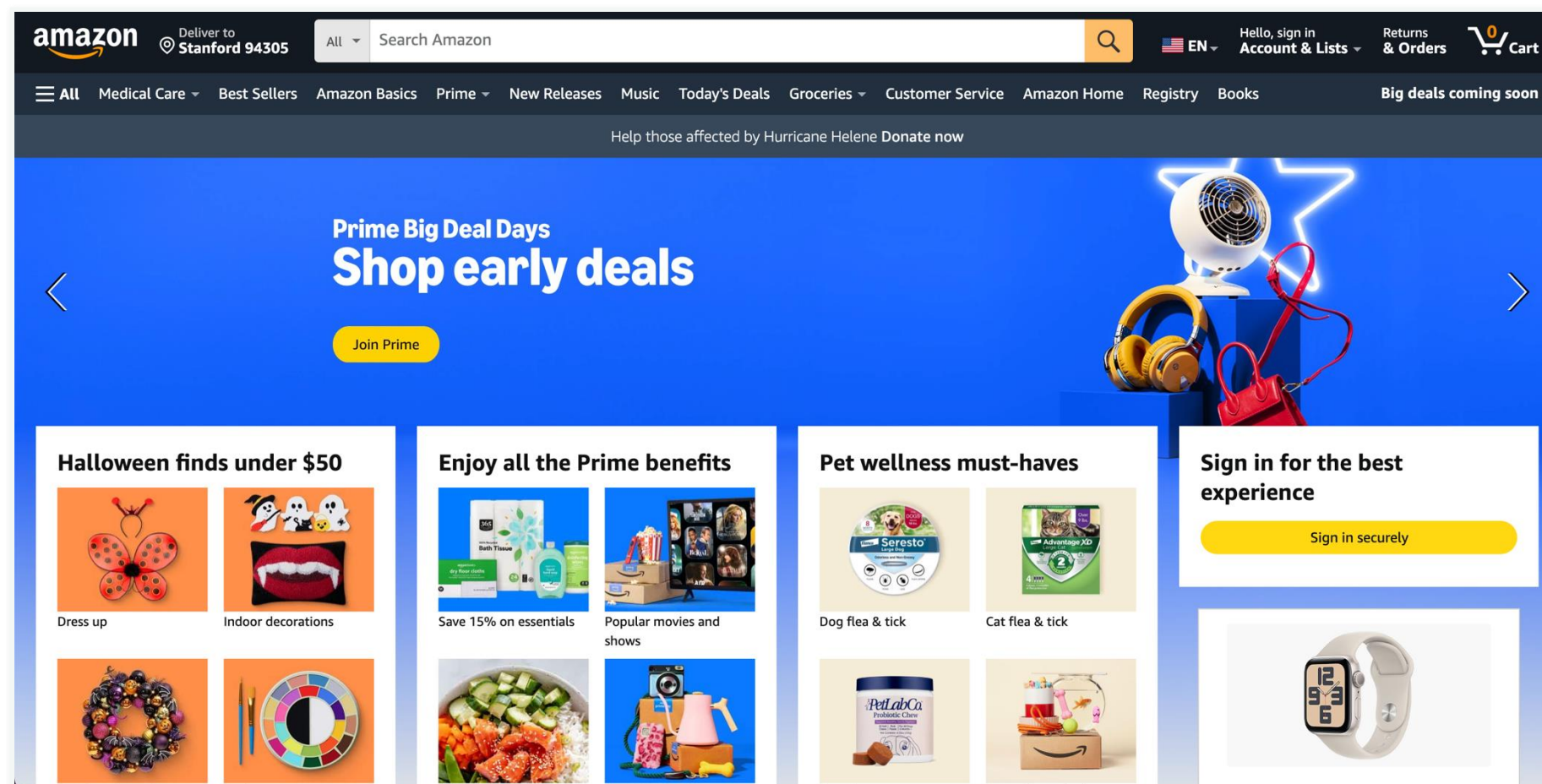
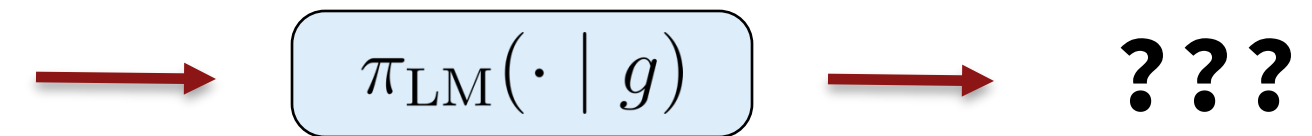
Now, think about your next action:
Thought: [model-pred]

Now, take an action:
Action: [model-pred]
```

Grounded Instruction Following with Language Models?

First Attempt: Zero-shot instruction following

Cancel shampoo subscription from the list of “subscribe and save” items

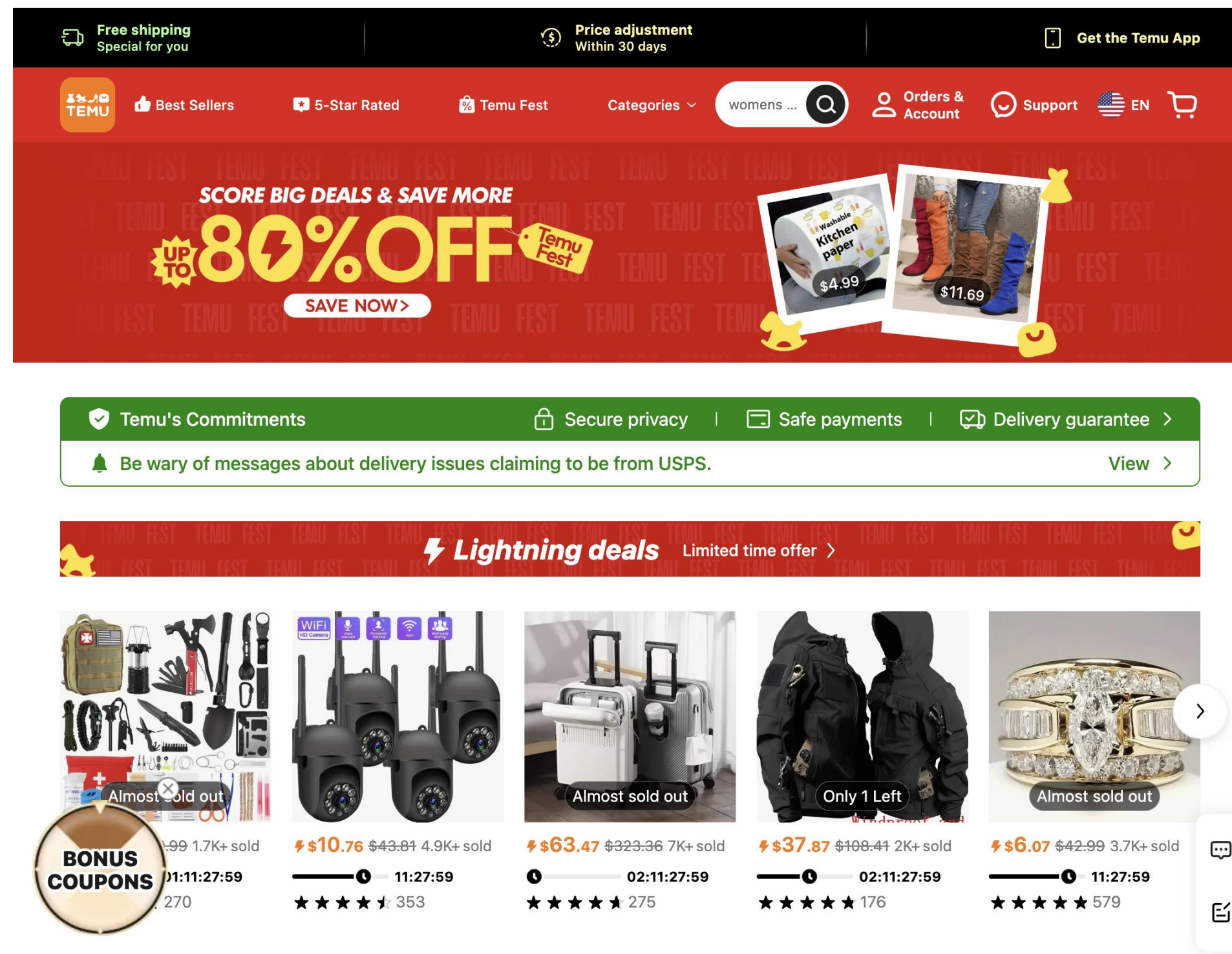
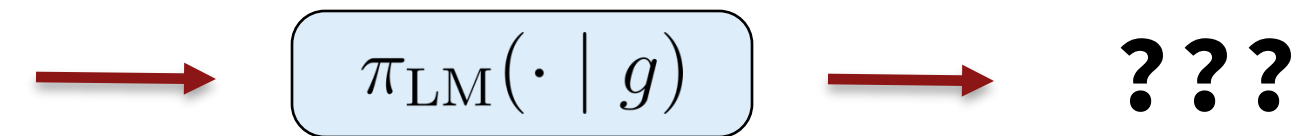


LMs cannot know how to navigate to the right section without prior knowledge of amazon.com
How can we provide this prior knowledge about environments?

Grounded Instruction Following with Language Models?

First Attempt: Zero-shot instruction following

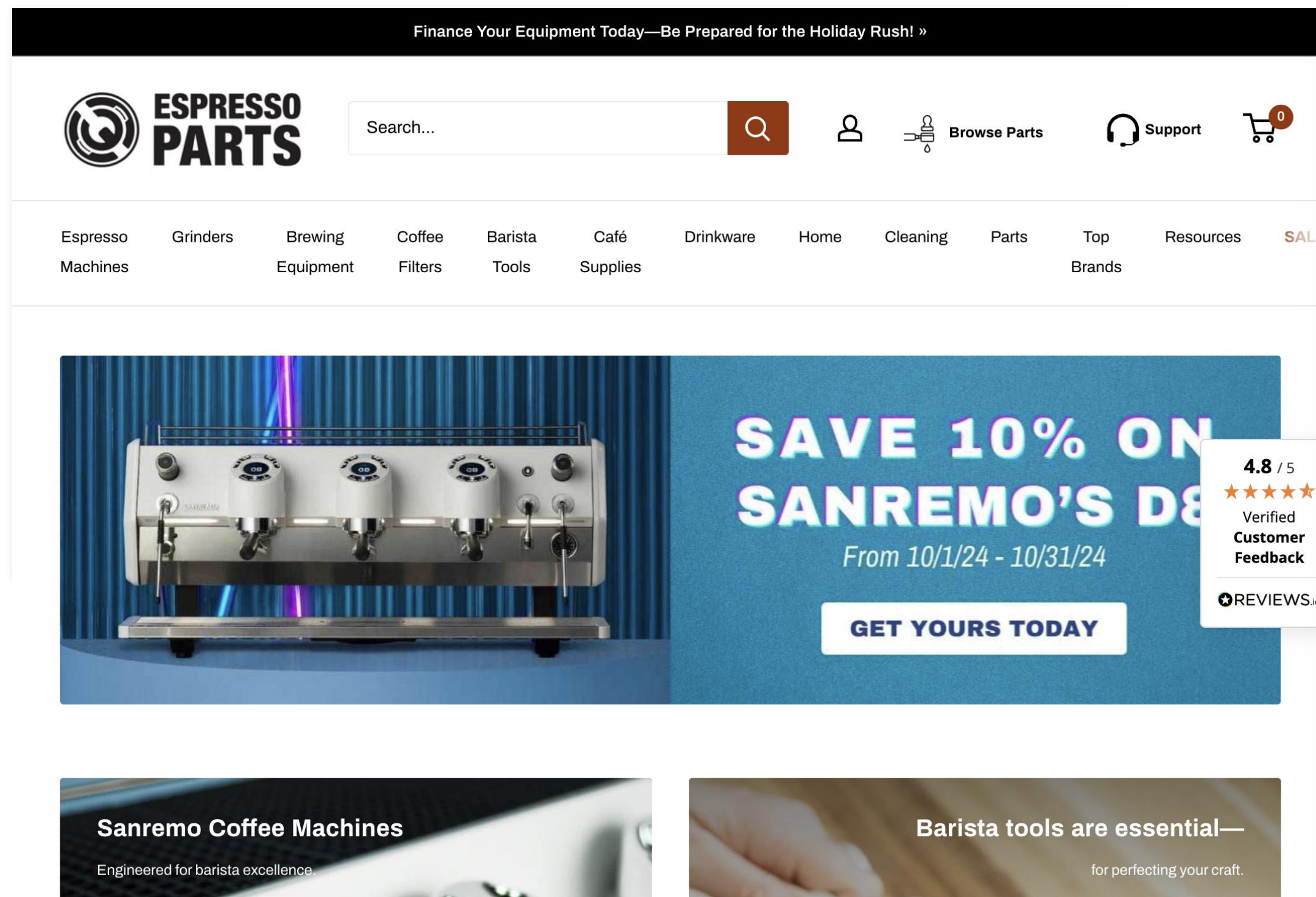
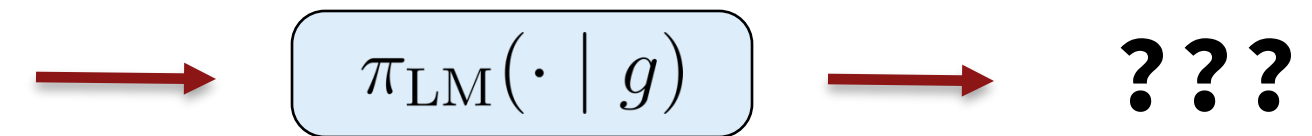
Cancel shampoo subscription from the list of “subscribe and save” items



Grounded Instruction Following with Language Models?

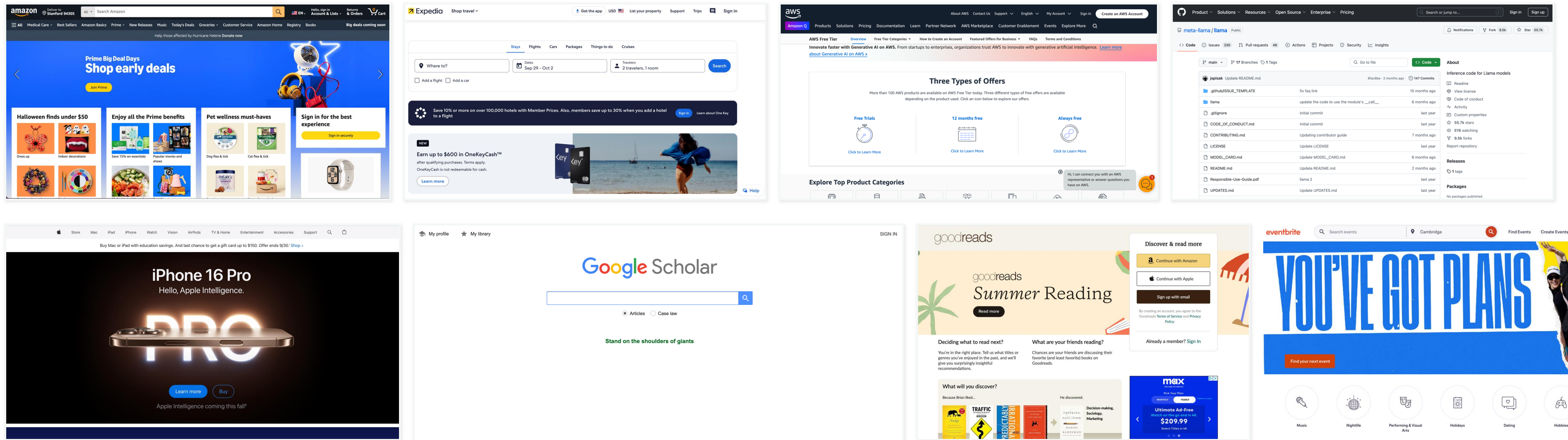
First Attempt: Zero-shot instruction following

Cancel shampoo subscription from the list of “subscribe and save” items



Grounded Instruction Following with Language Models?

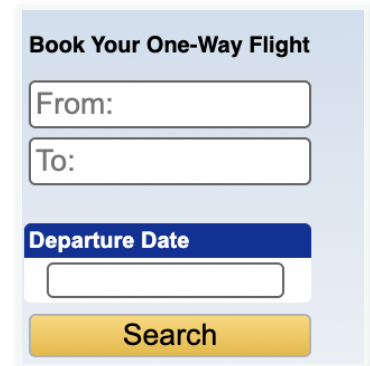
Second Attempt: Behavioral Cloning with Human demonstrations



Collecting human demonstrations that cover most use-cases across websites is expensive
Humans learn about new web-interfaces simply by interacting with them.
Can we do the same with models?

Grounded Instruction Following with *Synthetic* Demonstrations

BAGEL: Our first attempt for generating synthetic demonstrations via interaction



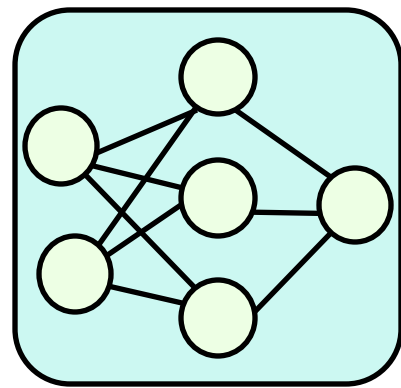
Book Your One-Way Flight

From:

To:

Departure Date

Search



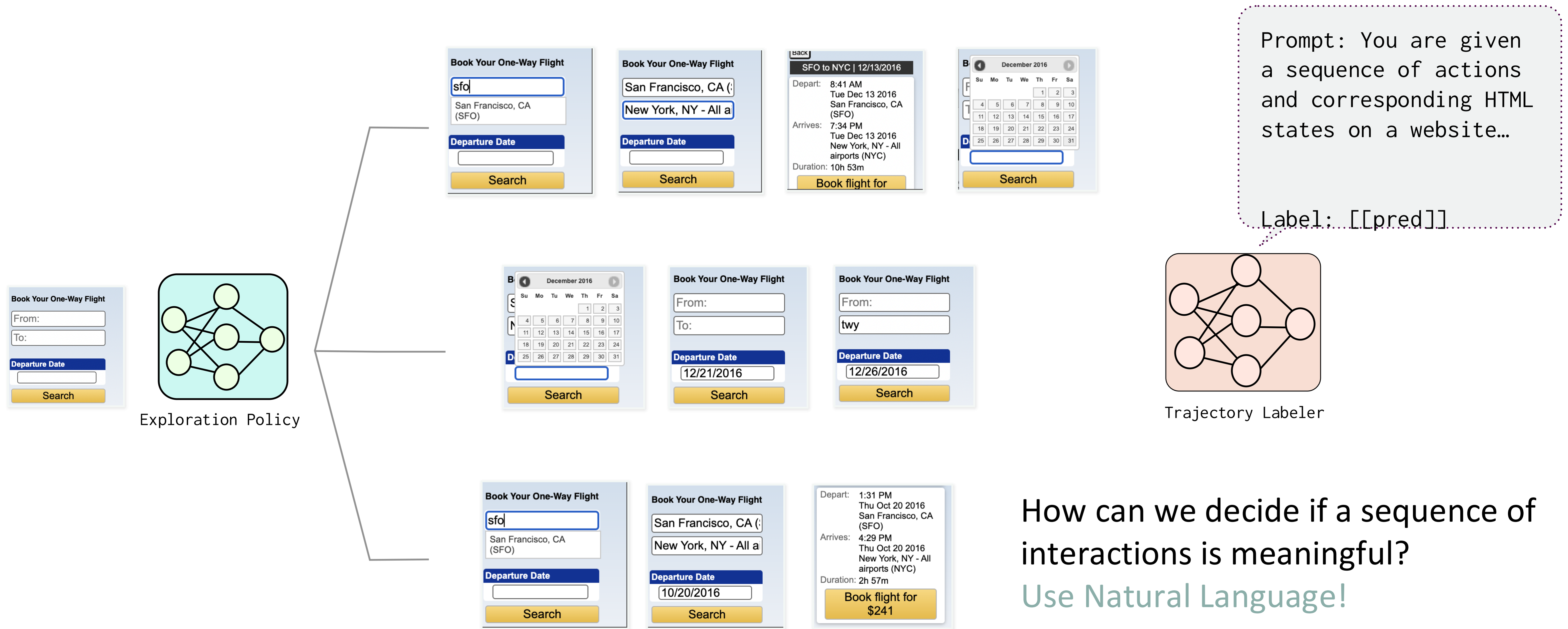
Exploration Policy

Prompt: Given a website, take actions of the following format to explore...

Action: `[[pred]]`

Grounded Instruction Following with *Synthetic Demonstrations*

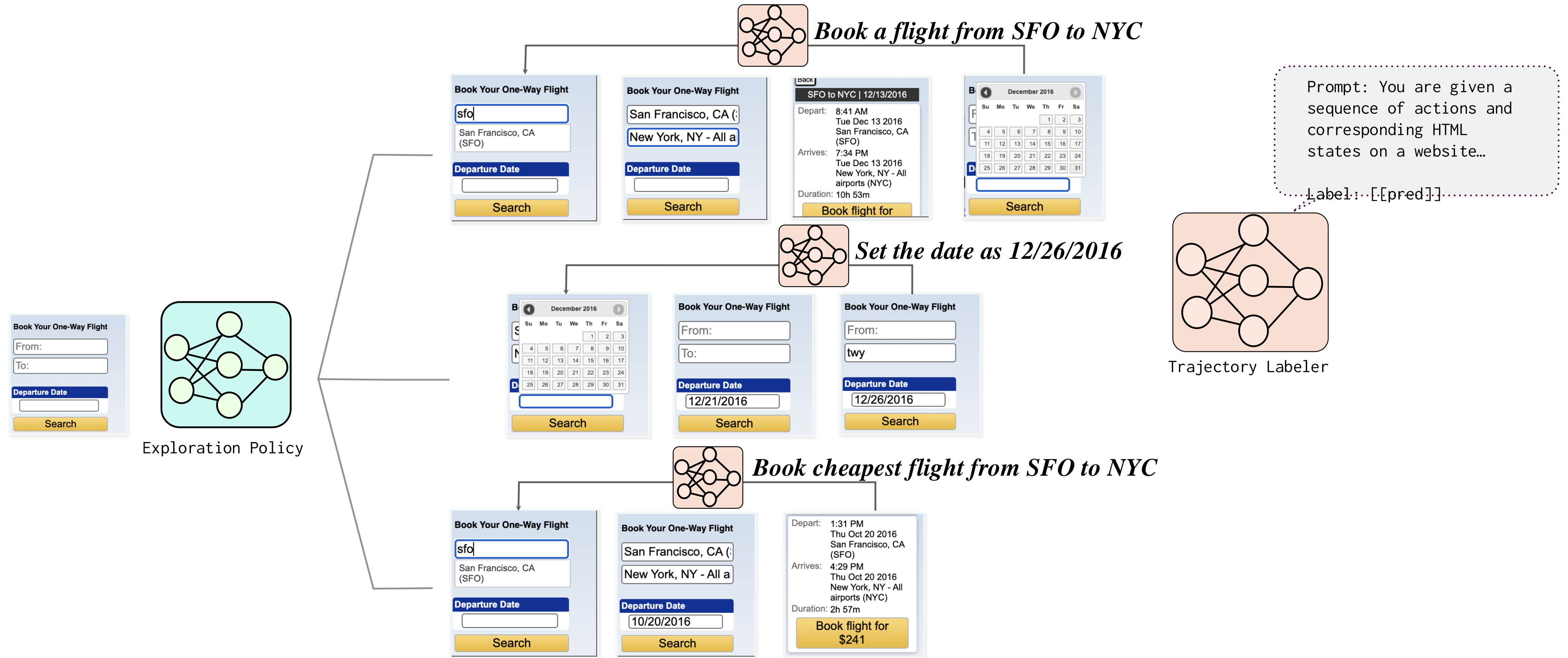
BAGEL: Our first attempt for generating synthetic demonstrations via interaction



How can we decide if a sequence of interactions is meaningful?
Use Natural Language!

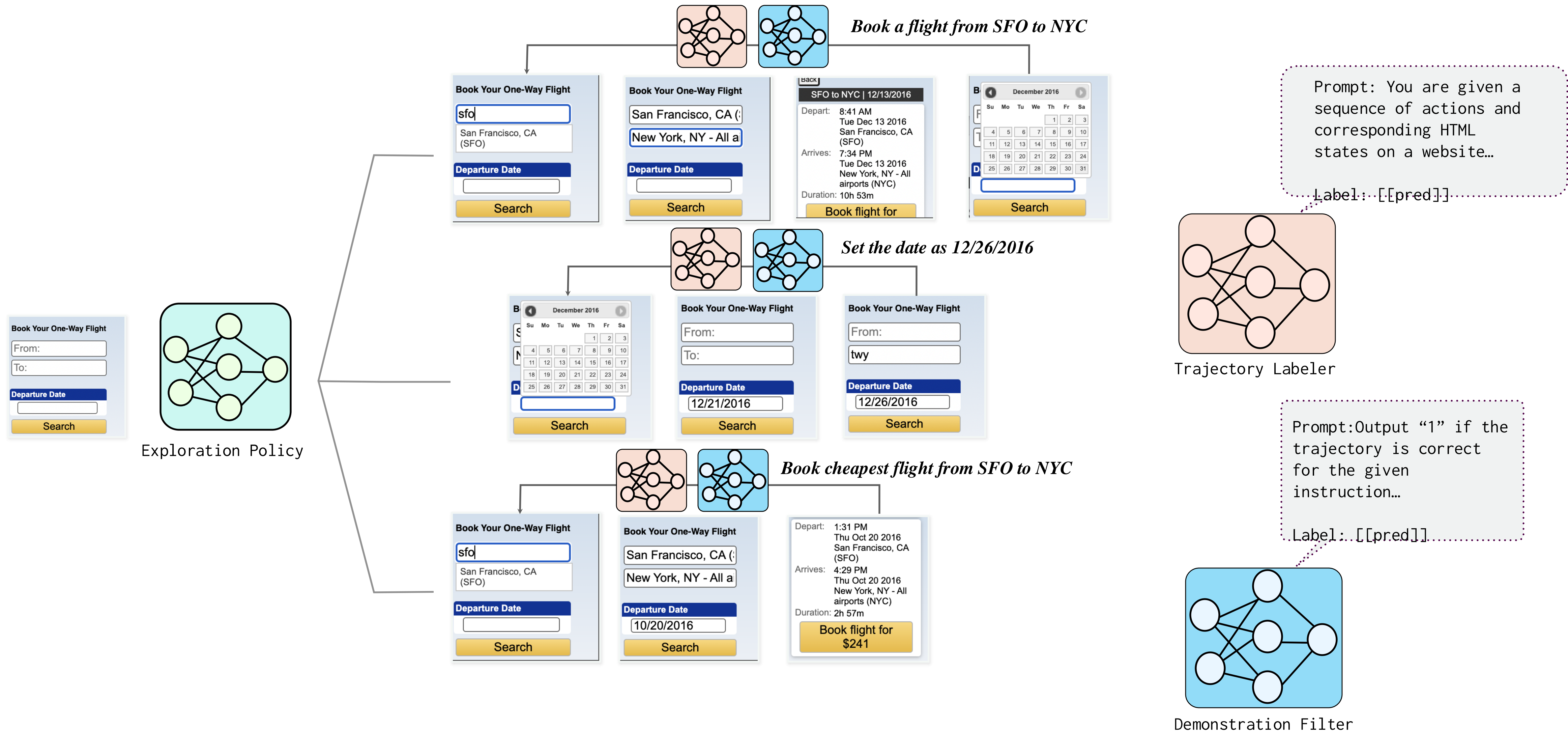
Grounded Instruction Following with *Synthetic Demonstrations*

BAGEL: Our first attempt for generating synthetic demonstrations via interaction



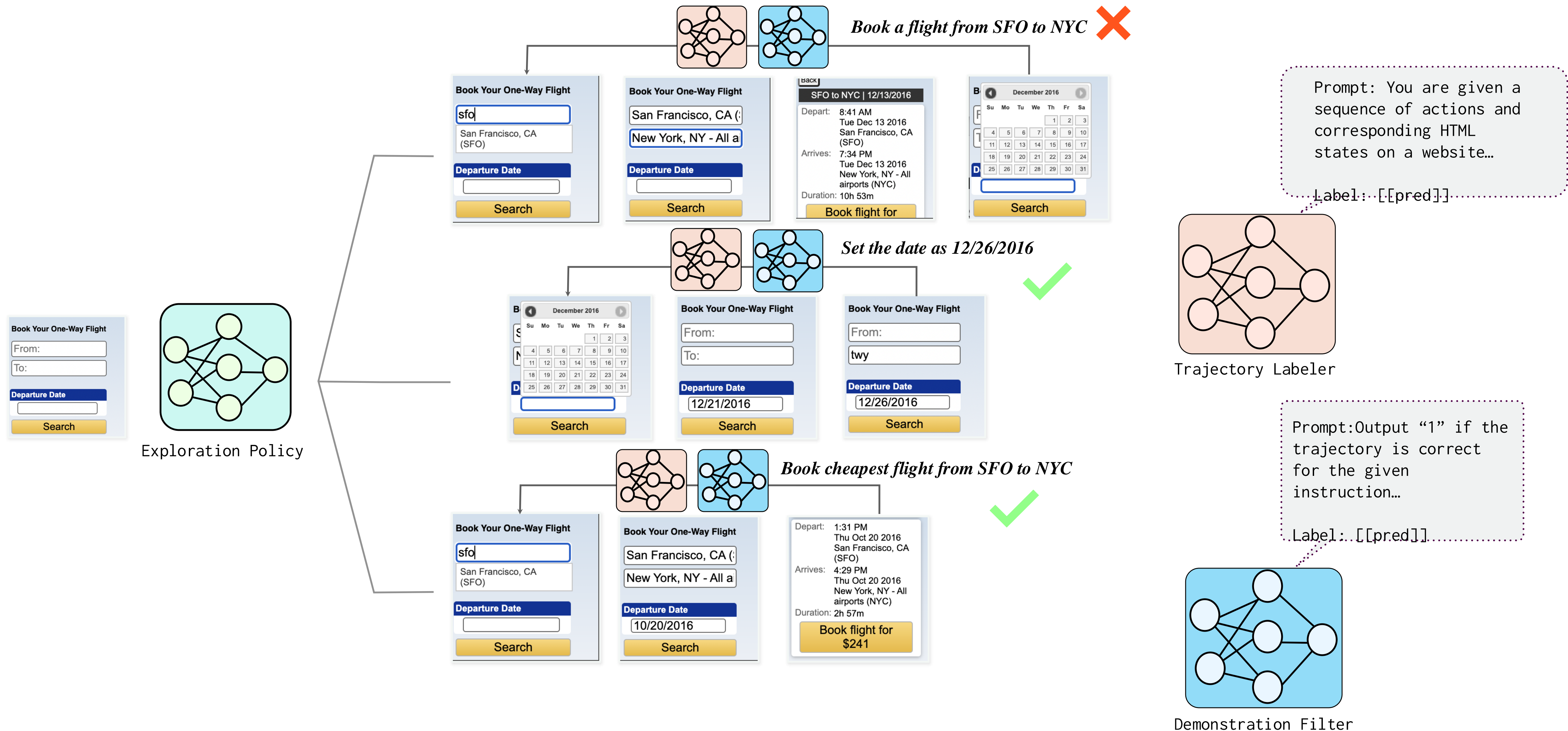
Grounded Instruction Following with *Synthetic Demonstrations*

BAGEL: Our first attempt for generating synthetic demonstrations via interaction



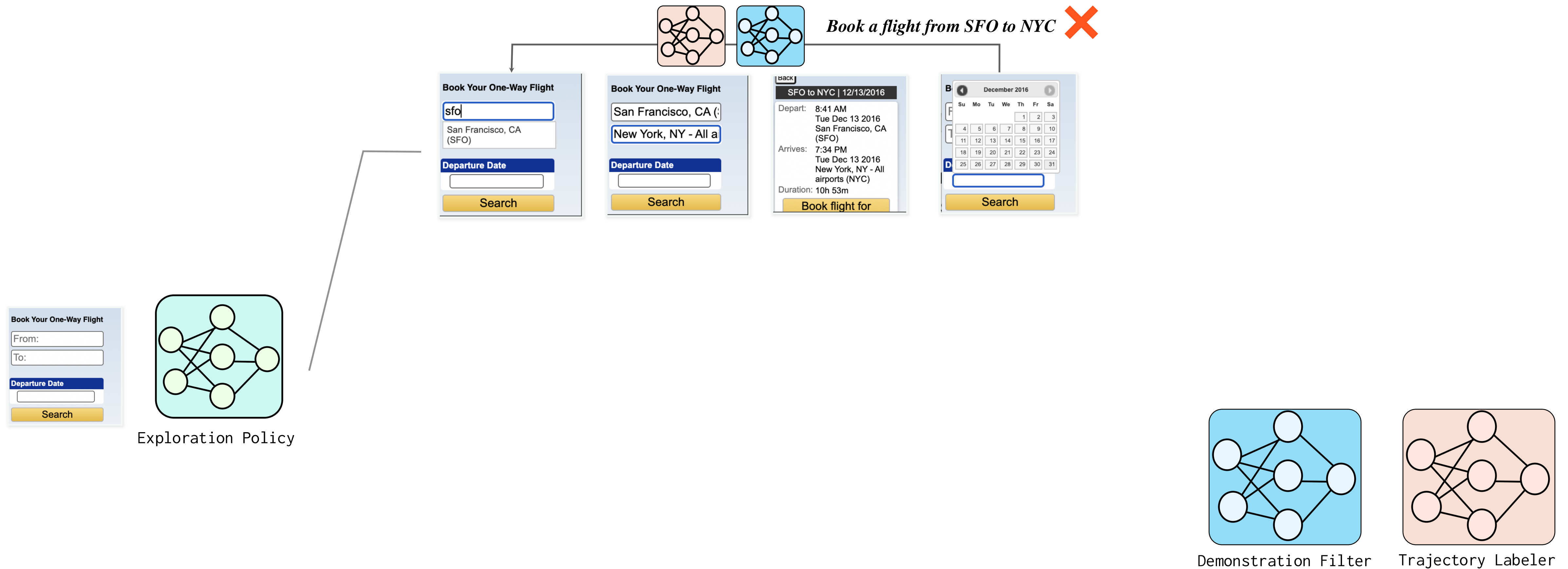
Grounded Instruction Following with *Synthetic* Demonstrations

BAGEL: Our first attempt for generating synthetic demonstrations via interaction



Grounded Instruction Following with *Synthetic* Demonstrations

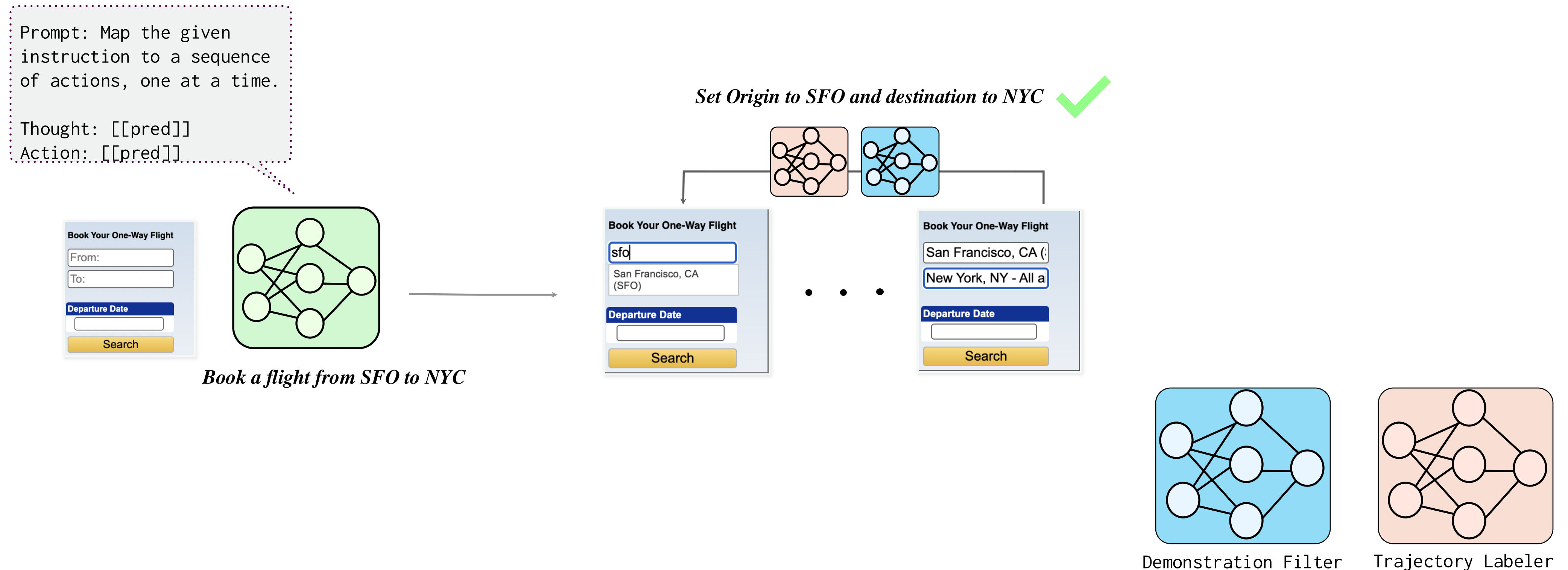
BAGEL: Our first attempt for generating synthetic demonstrations via interaction



Instead of throwing away bad (instruction, trajectory) pairs, BAGEL refines iteratively by going back and forth between language and actions

Grounded Instruction Following with *Synthetic* Demonstrations

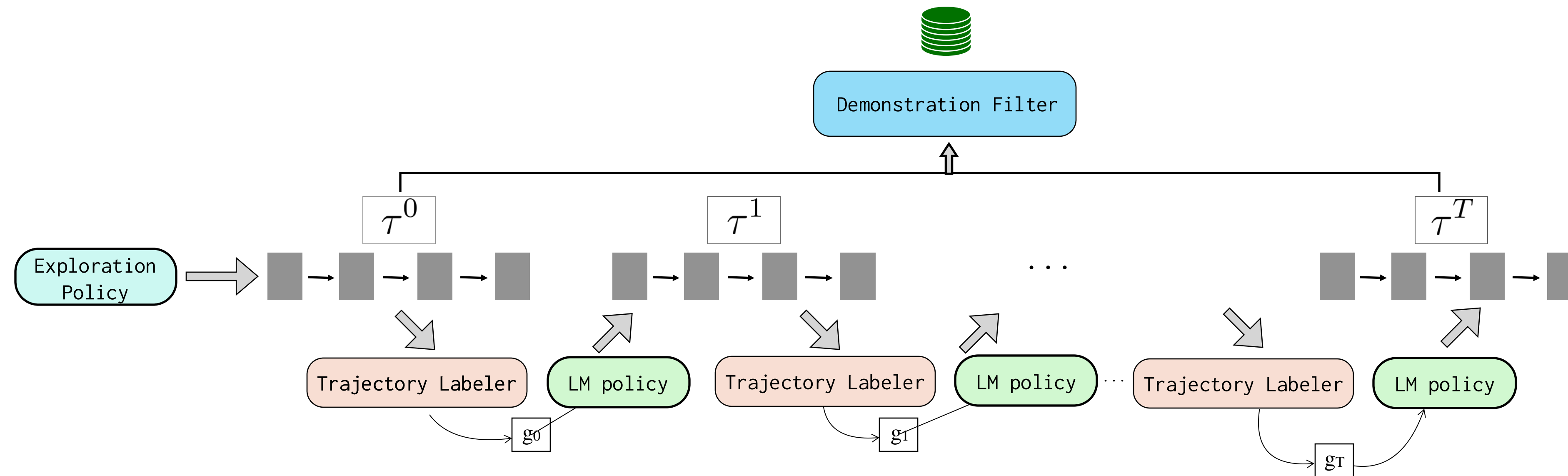
BAGEL: Our first attempt for generating synthetic demonstrations via interaction



Instead of throwing away bad (instruction, trajectory) pairs, BAGEL refines iteratively by going back and forth between language and actions

Grounded Instruction Following with *Synthetic* Demonstrations

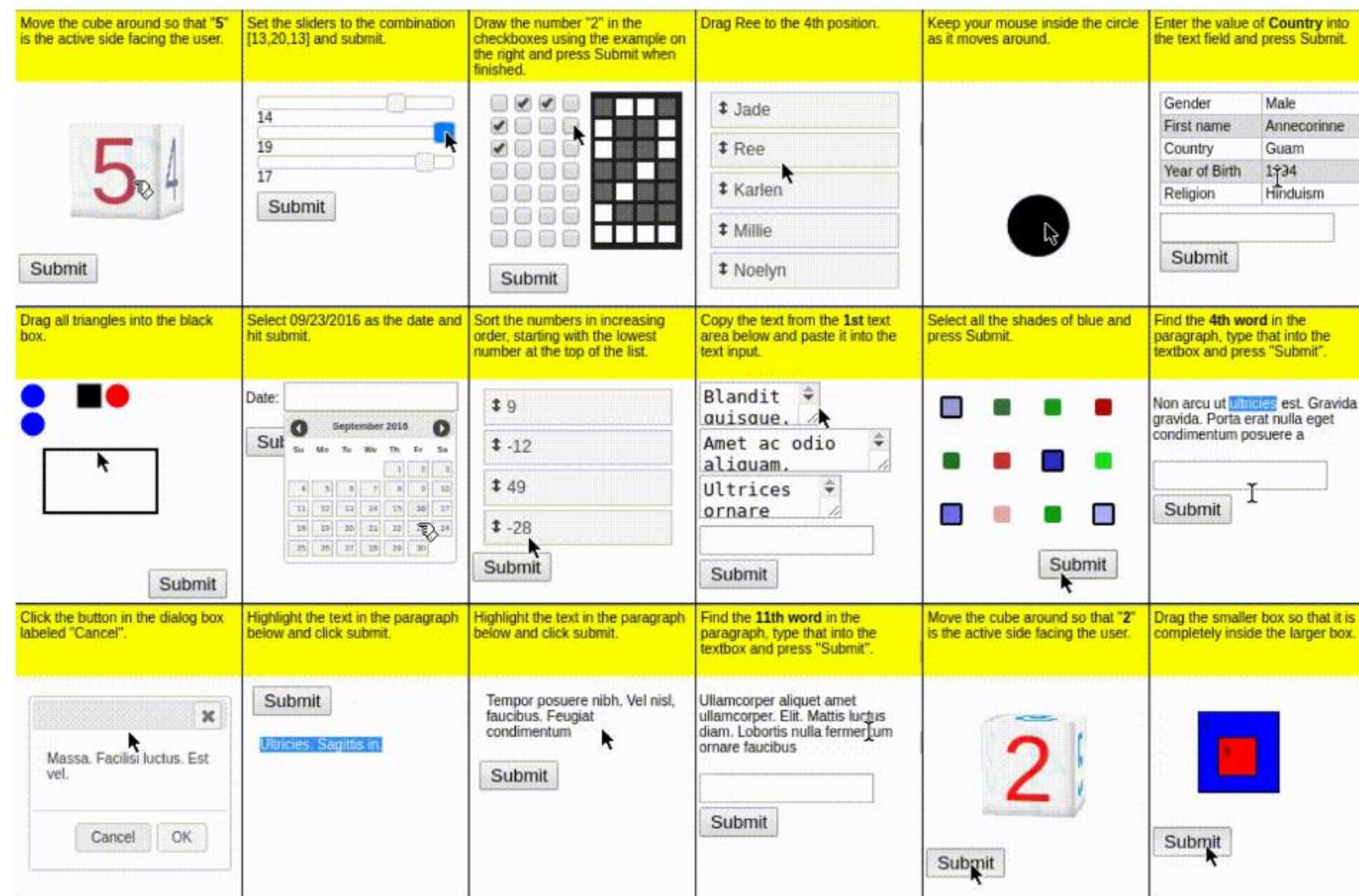
BAGEL: Our first attempt for generating synthetic demonstrations via interaction



Instead of throwing away bad (instruction, trajectory) pairs, BAGEL refines iteratively by going back and forth between language and actions

Some Results from In-Context Learning with BAGEL demonstrations

MiniWoB++: map instructions to sequence of mouse and keyboard actions



Sandboxed environment evaluating basic browser interactions across a range of applications from social media to email clients

Evaluates functional correctness

Not real world (limited functionality)

Relatively short-horizon

Zero-shot performance far from perfect!

Some Results from In-Context Learning with BAGEL demonstrations

(↑ is better)

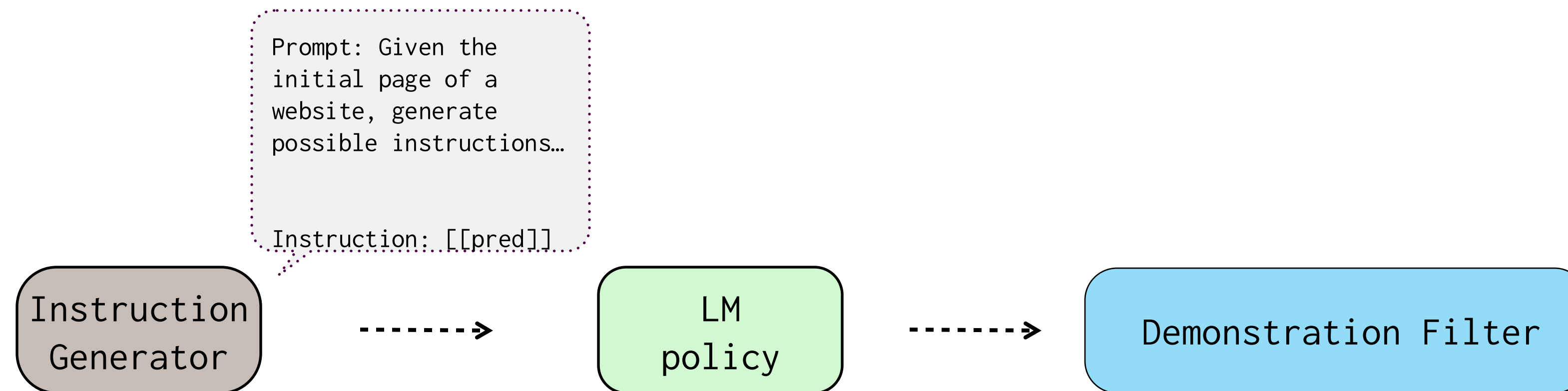
Domain	Zero-shot	+ BAGEL
book-flight-nodelay	0.05	0.15
email-inbox-all	0.88	1.00
choose-date-nodelay	0.2	0.4
social-media	0.6	0.7
...
Mean Reward	0.47	0.61

BAGEL improves zero-shot agents significantly

Some Results from In-Context Learning with BAGEL demonstrations

Baseline: *Instruction-first* approach

- ▶ Sample instructions from a prior, given first observation from environment
- ▶ Run zero-shot agent over these instructions
- ▶ Use the scoring function to filter out demonstrations



Some Results from In-Context Learning with BAGEL demonstrations

(↑ is better)

Domain	Instruction-First	BAGEL
book-flight-nodelay	0.05	0.15
email-inbox-all	0.85	1.00
choose-date-nodelay	0.35	0.4
social-media	0.7	0.7
...
Mean Reward	0.52	0.61

BAGEL improves performance over an instruction-first approach

Some Results from In-Context Learning with BAGEL demonstrations

(↑ is better)

Domain	BAGEL (no itrs)	BAGEL
book-flight-nodelay	0.15	0.15
email-inbox-all	0.60	1.00
choose-date-nodelay	0.15	0.4
social-media	0.6	0.7
...
Mean Reward	0.53	0.61

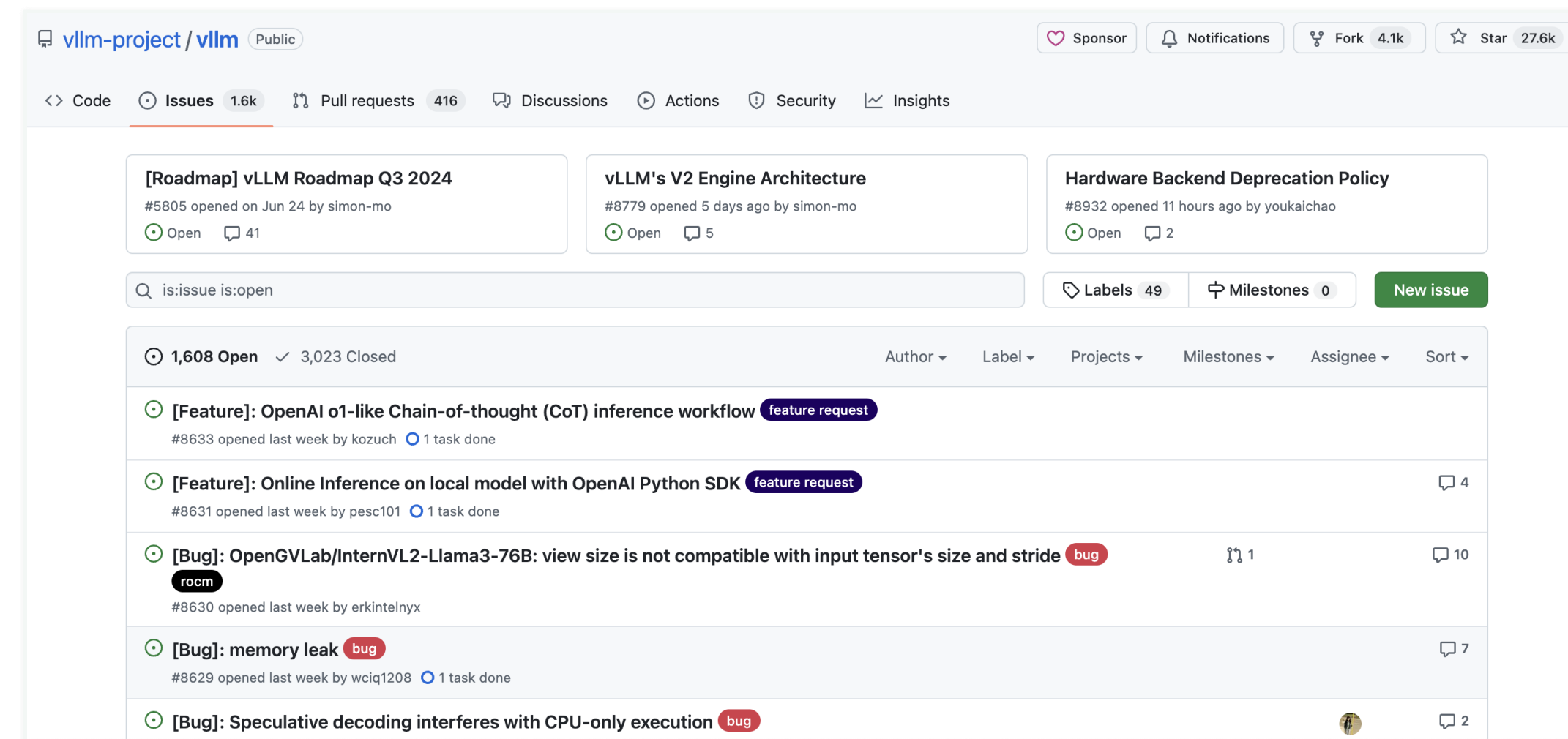
Multiple Iterations of relabeling improves performance

Lessons learned from BAGEL

- Linguistic priors can be a powerful tool for filtering useful interactions on web-interfaces.
- Instruction-first data generation has been extremely successful for ungrounded settings (e.g. self-instruct). But this does not work so well for grounded settings:
 - ▶ Given website landing page, no model can imagine the set of possible meaningful tasks.
 - ▶ This becomes even harder when website contains **hidden features** that can only be found via interaction.
- Round-trips between natural language instructions and sequence of actions eventually finds high quality correspondences. Lots of other places where similar ideas have been successful:
 - ▶ Cycle consistency for GAN
 - ▶ Machine Translation (Back-translation)

Grounded Instruction Following on Real Websites

- Exploration in BAGEL is unstructured and discovers simple demonstrations.
- Tasks on real-websites are hierarchical and complex:

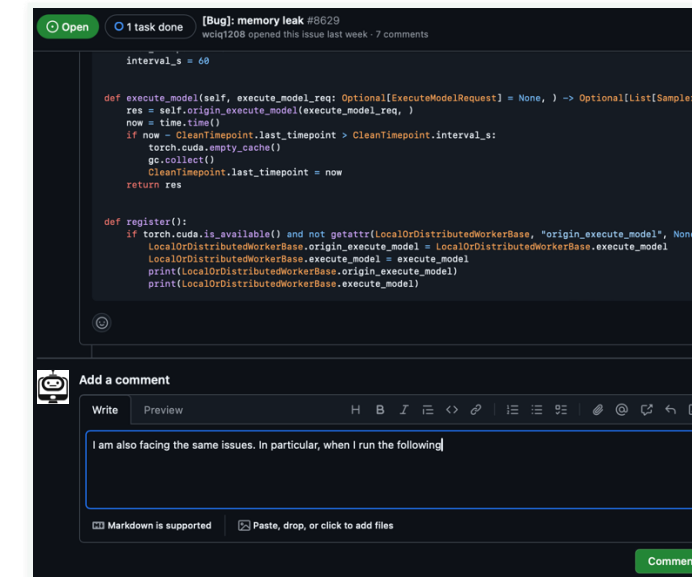
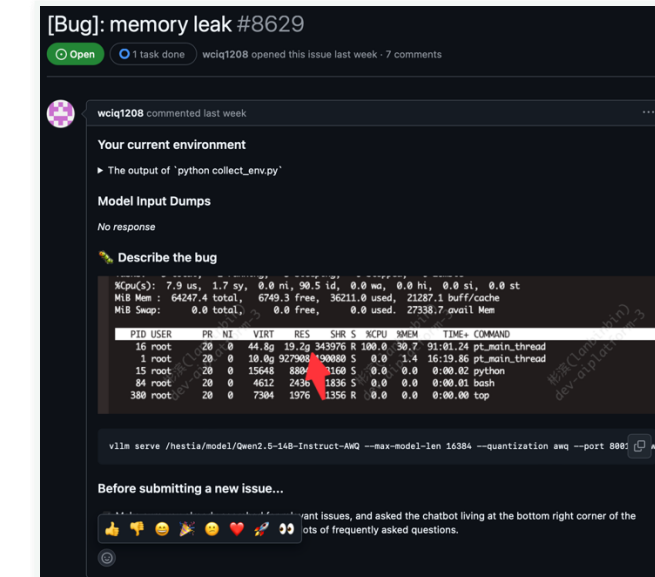
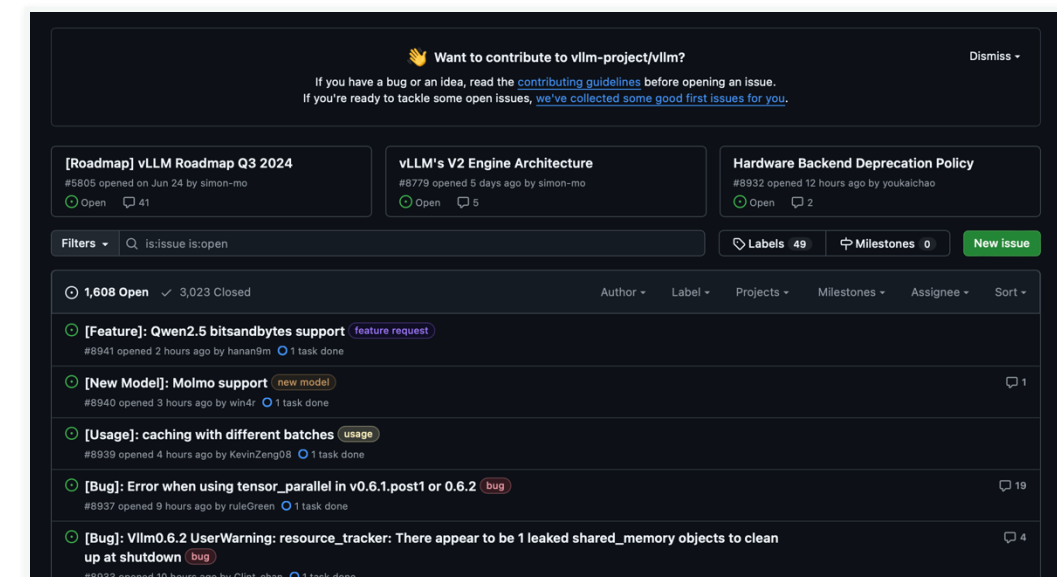
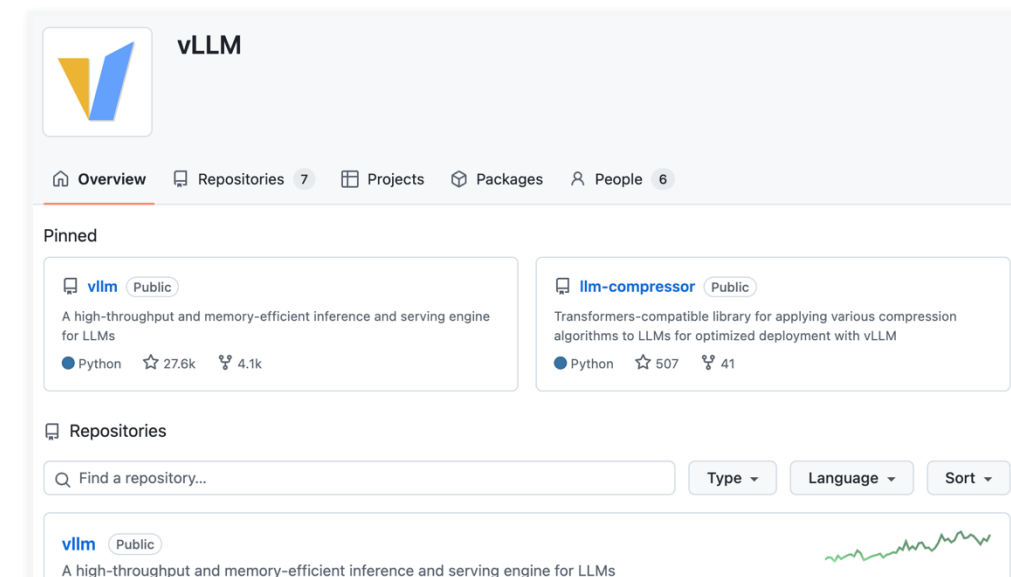
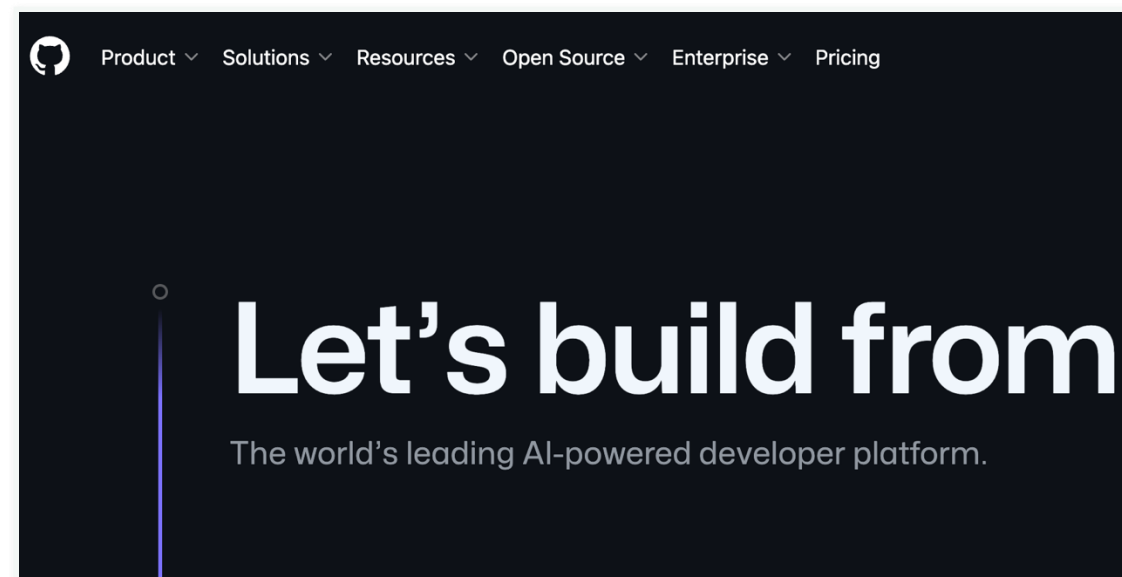


Navigate to the issue titled memory leak for the vllm project, like the comment by user wciq1208 and then respond to the post saying “I am also”

How can we search efficiently over the space of possibly exponential meaningful interactions?
Use Linguistic priors

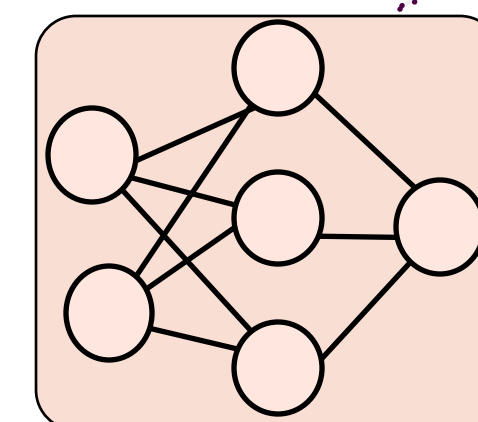
Grounded Instruction Following on Real Websites

Navigate to the issue titled memory leak for the vllm project, like the comment by user wciq1208 and then respond to the post saying “I am also”



Prompt: You are given a sequence of actions and corresponding HTML states on a website...

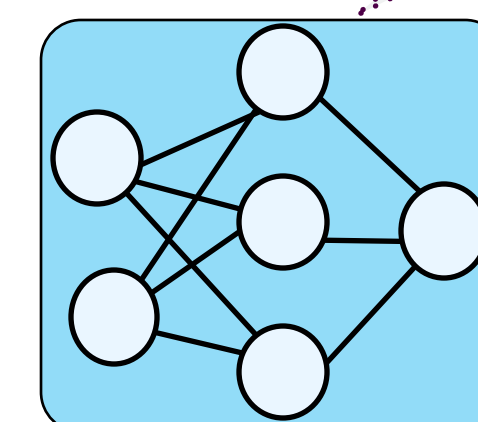
Label: [[pred]]



Trajectory Labeler

Prompt: Output “1” if the trajectory is correct for the given instruction...

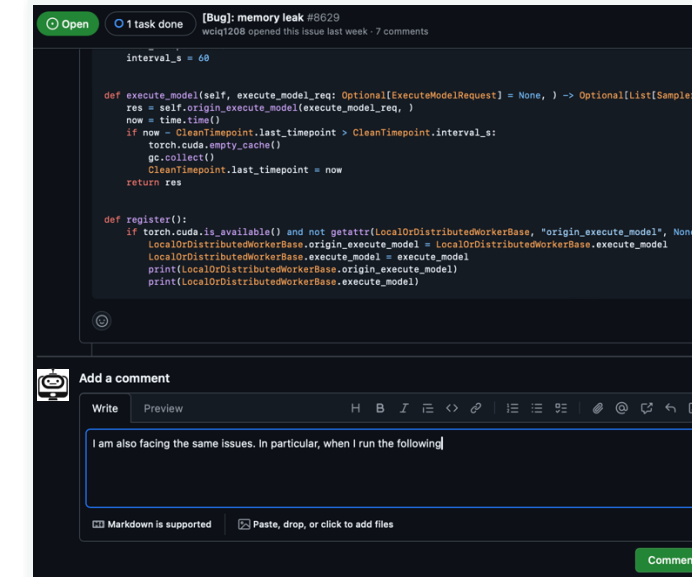
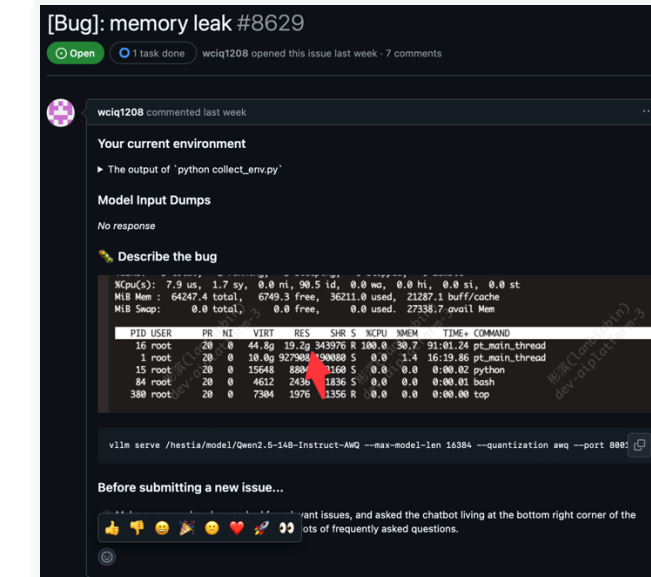
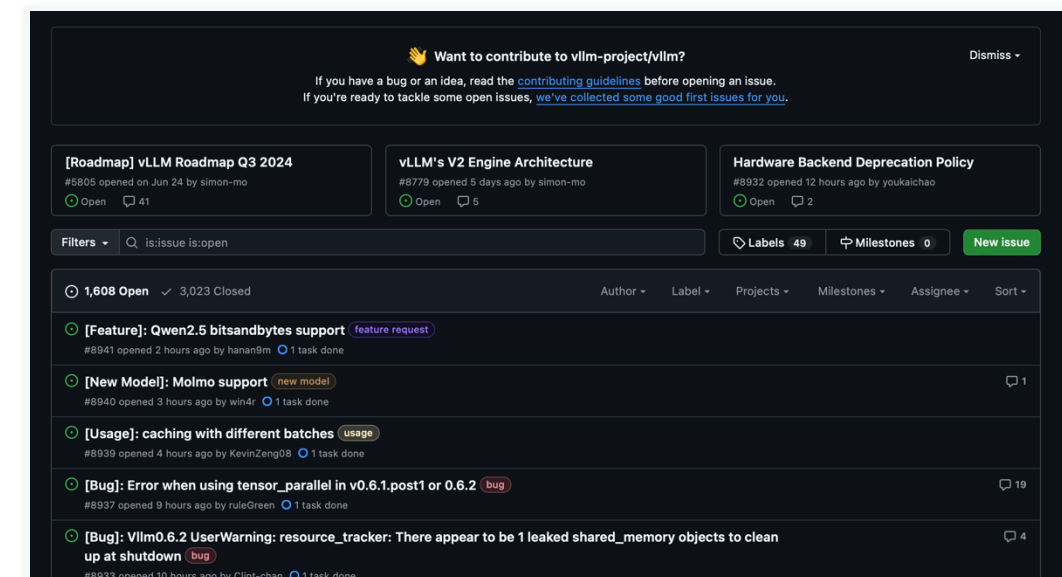
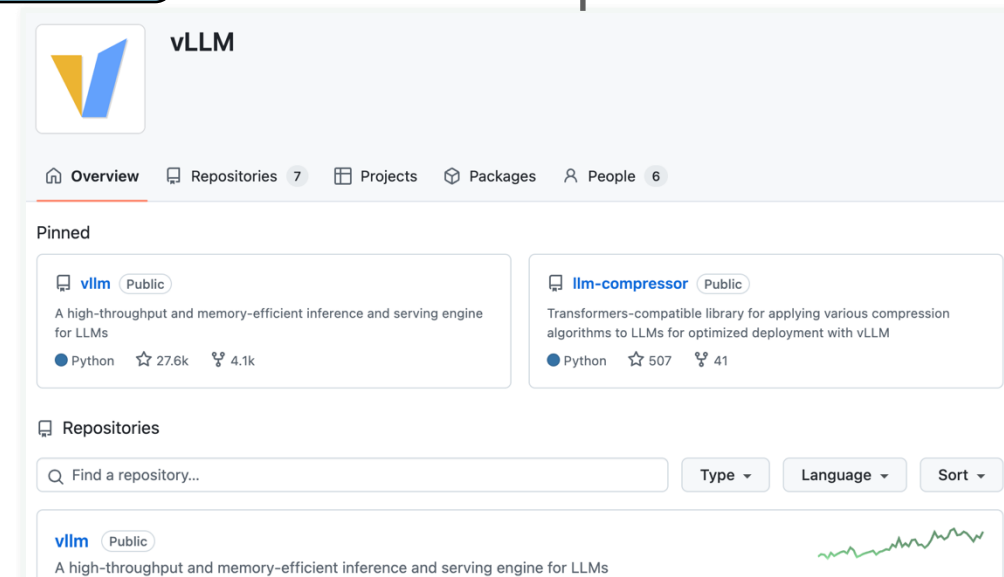
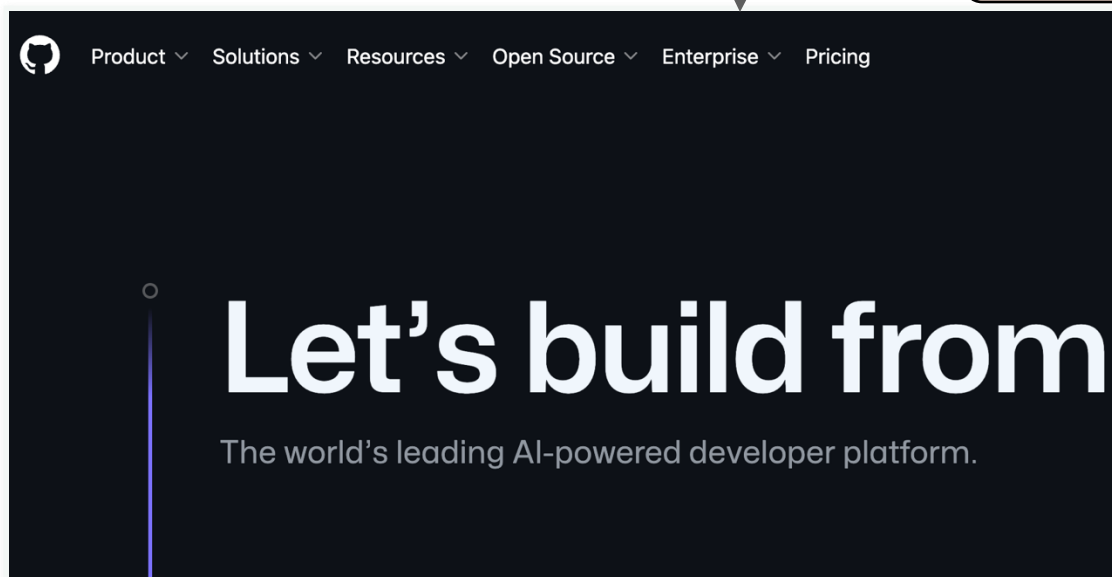
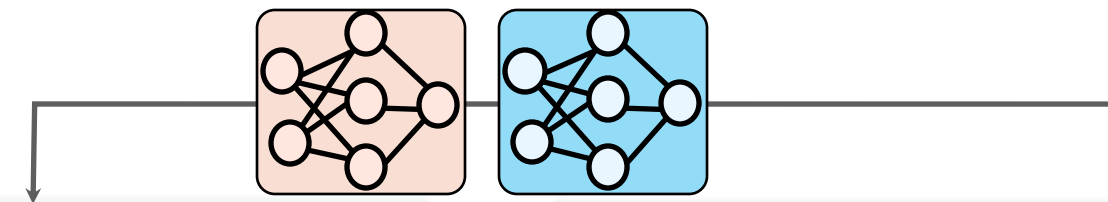
Label: [[pred]]



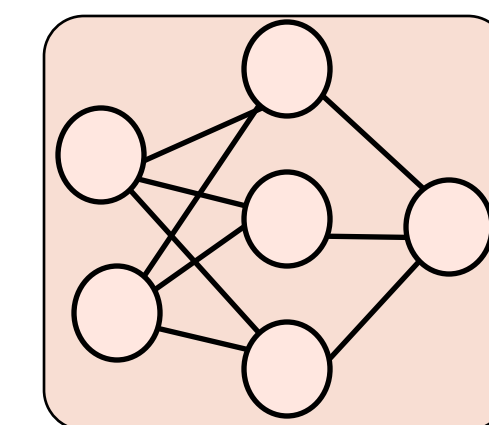
Demonstration Filter

Grounded Instruction Following on Real Websites

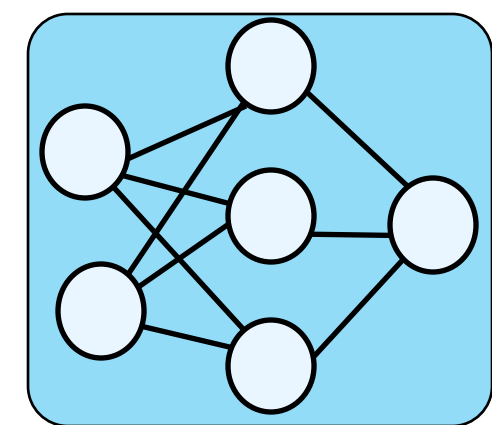
Navigate to the vllm repository on github.com



Navigate to the issue titled memory leak for the vllm project, like the comment by user wciq1208 and then respond to the post saying "I am also"



Trajectory Labeler

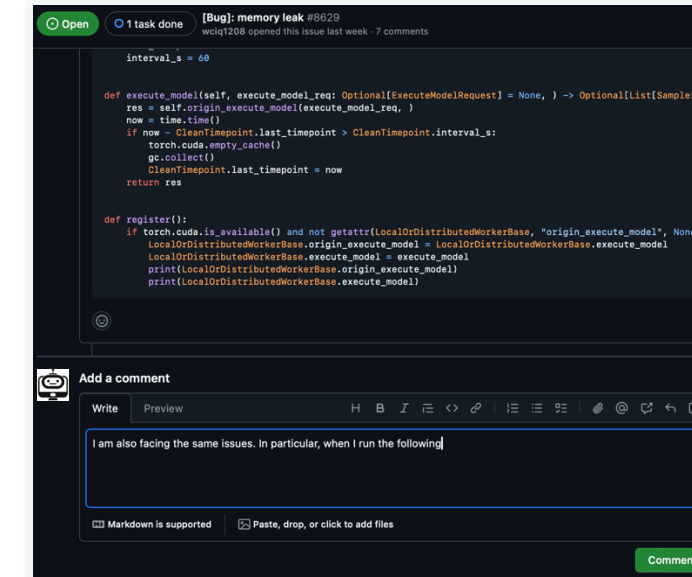
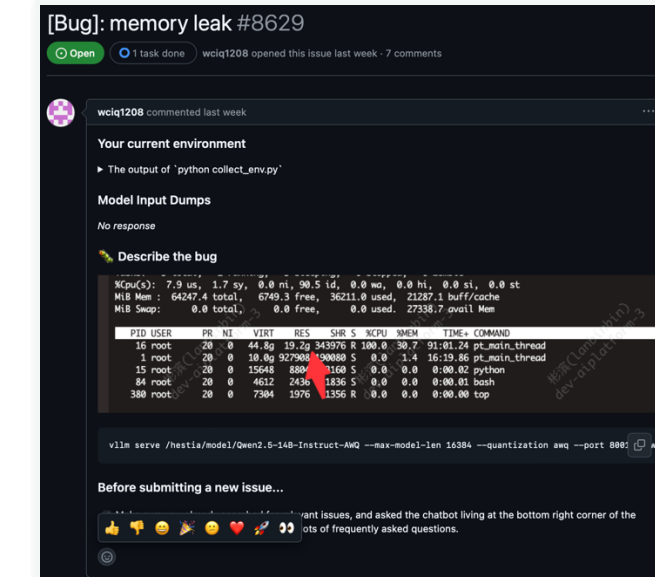
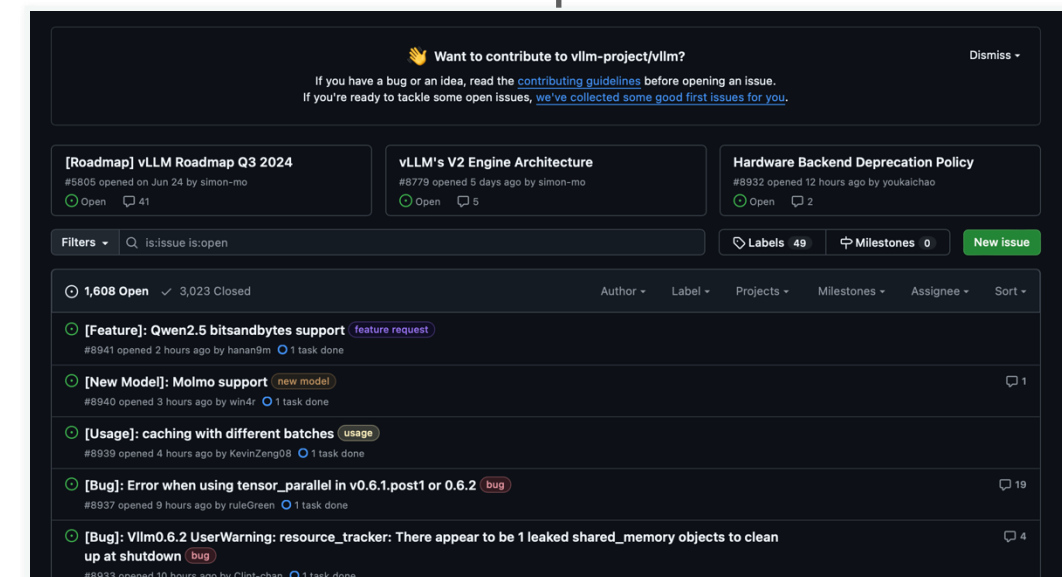
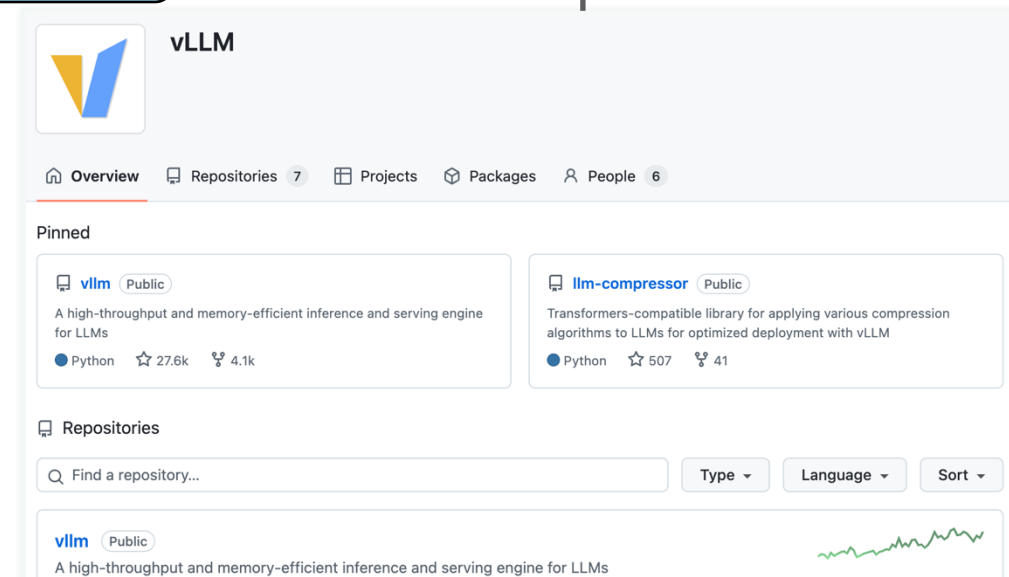
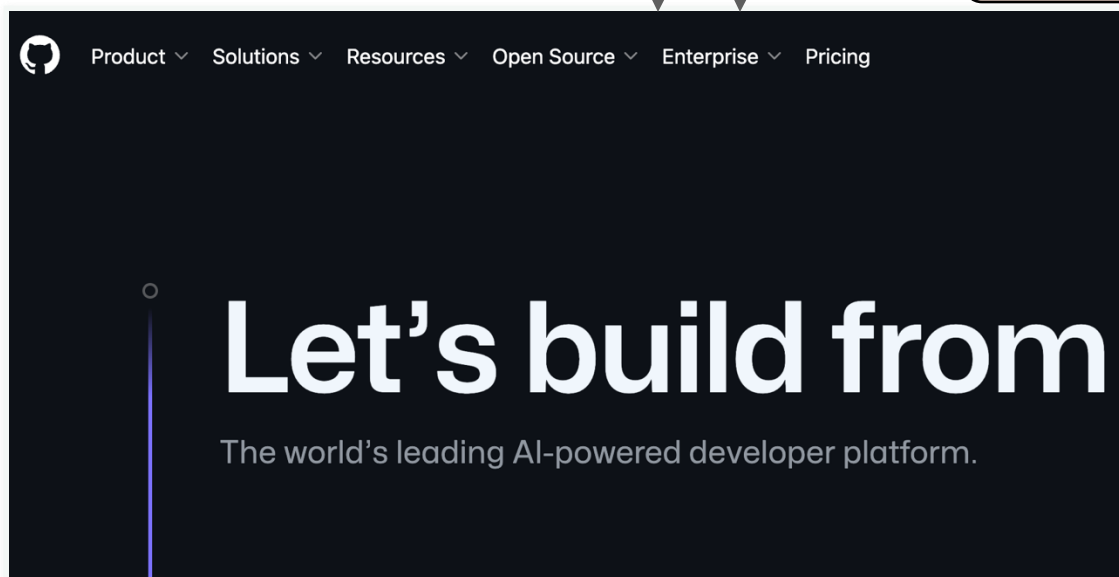
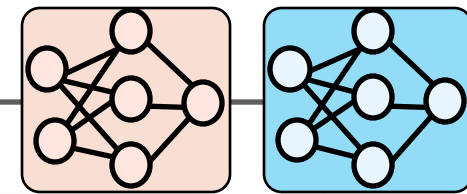
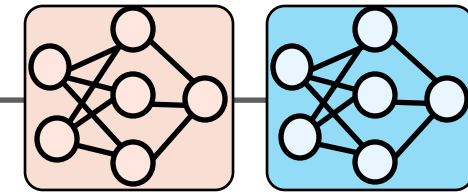


Demonstration Filter

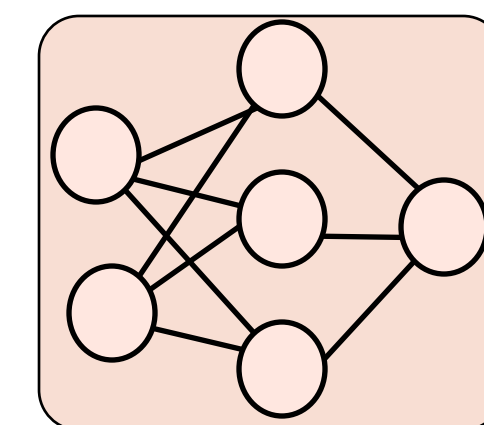
Grounded Instruction Following on Real Websites

Open the issues page for the vllm repository on github.com

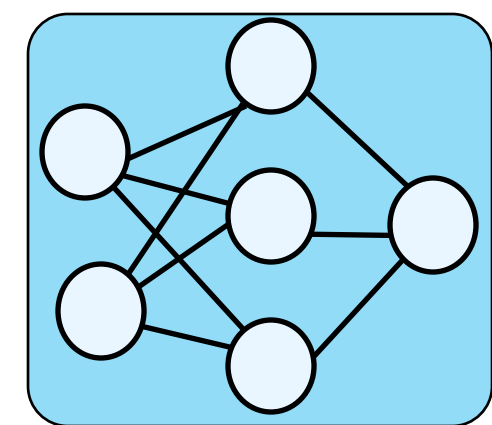
Navigate to the vllm repository on github.com



Navigate to the issue titled memory leak for the vllm project, like the comment by user wciq1208 and then respond to the post saying "I am also"



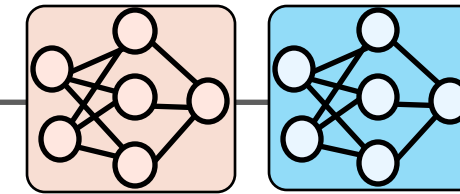
Trajectory Labeler



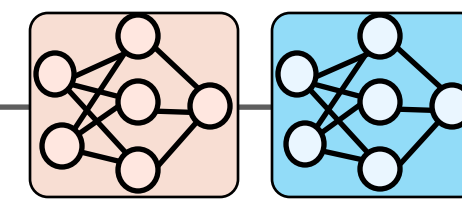
Demonstration Filter

Grounded Instruction Following on Real Websites

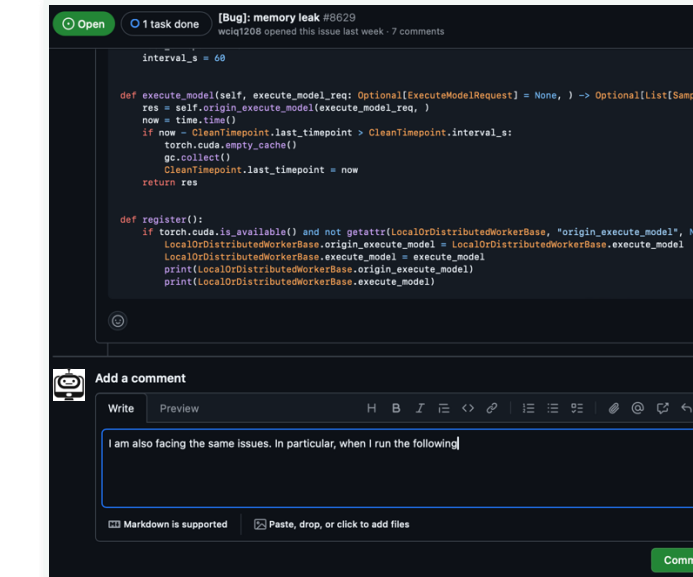
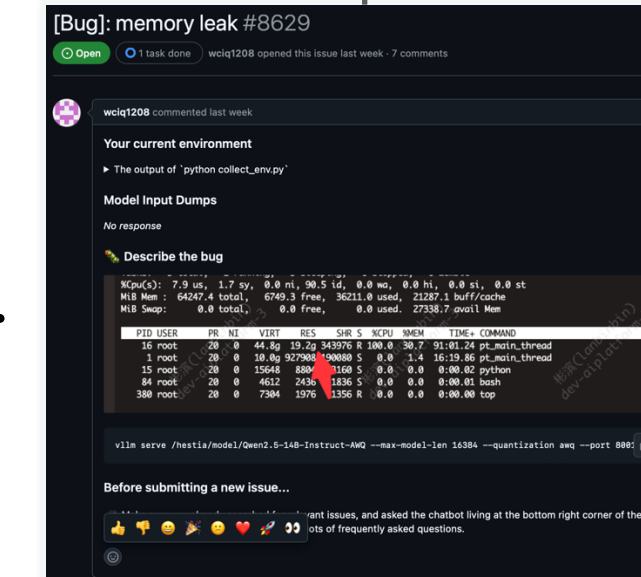
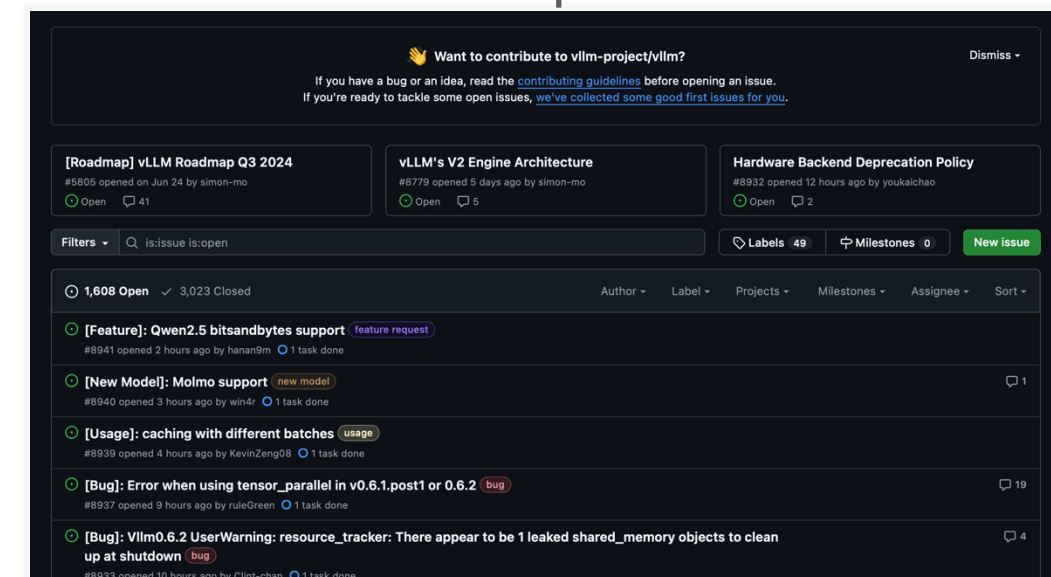
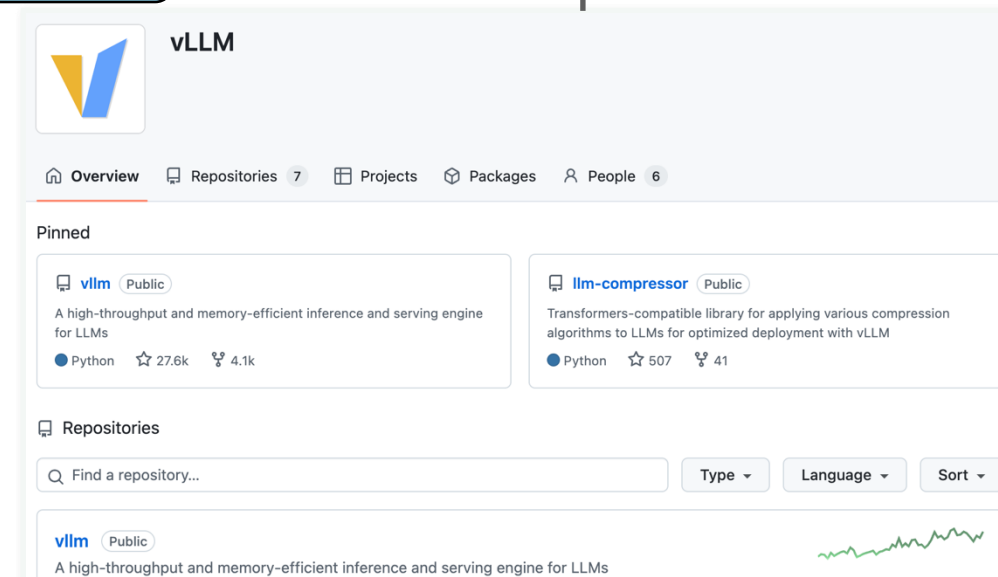
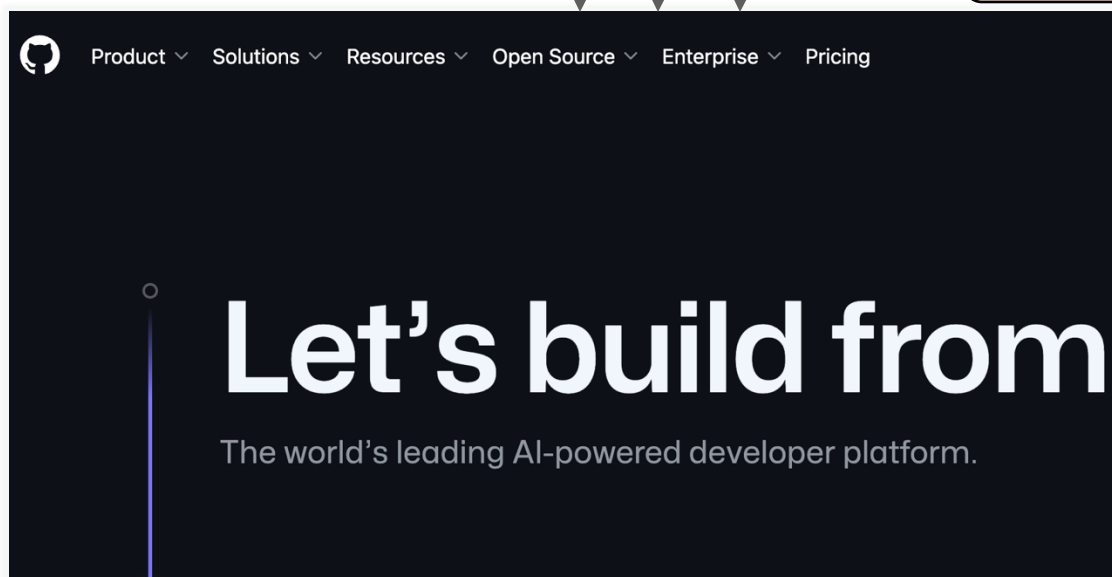
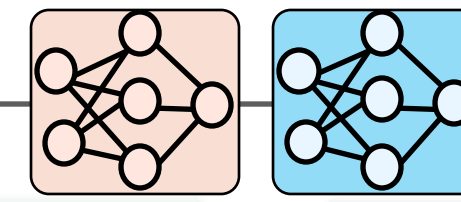
Navigate to issue titled memory leak for the vllm repository on github.com



Open the issues page for the vllm repository on github.com

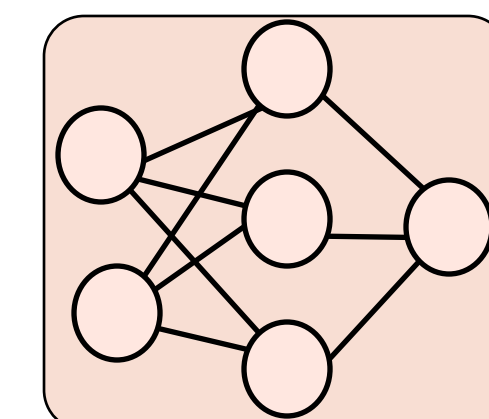


Navigate to the vllm repository on github.com

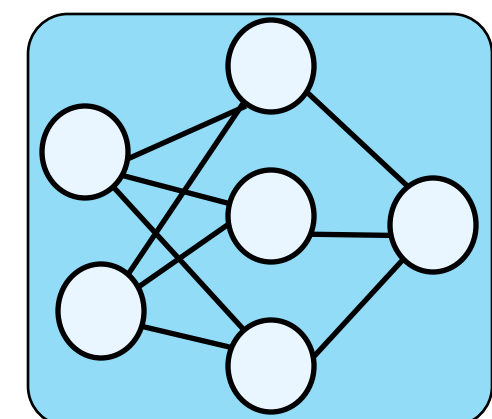


Complex trajectories can be segmented such that prefixes correspond to sub-tasks. We can use this as a pruning function for structuring exploration!

Navigate to the issue titled memory leak for the vllm project, like the comment by user wciq1208 and then respond to the post saying "I am also"



Trajectory Labeler



Demonstration Filter

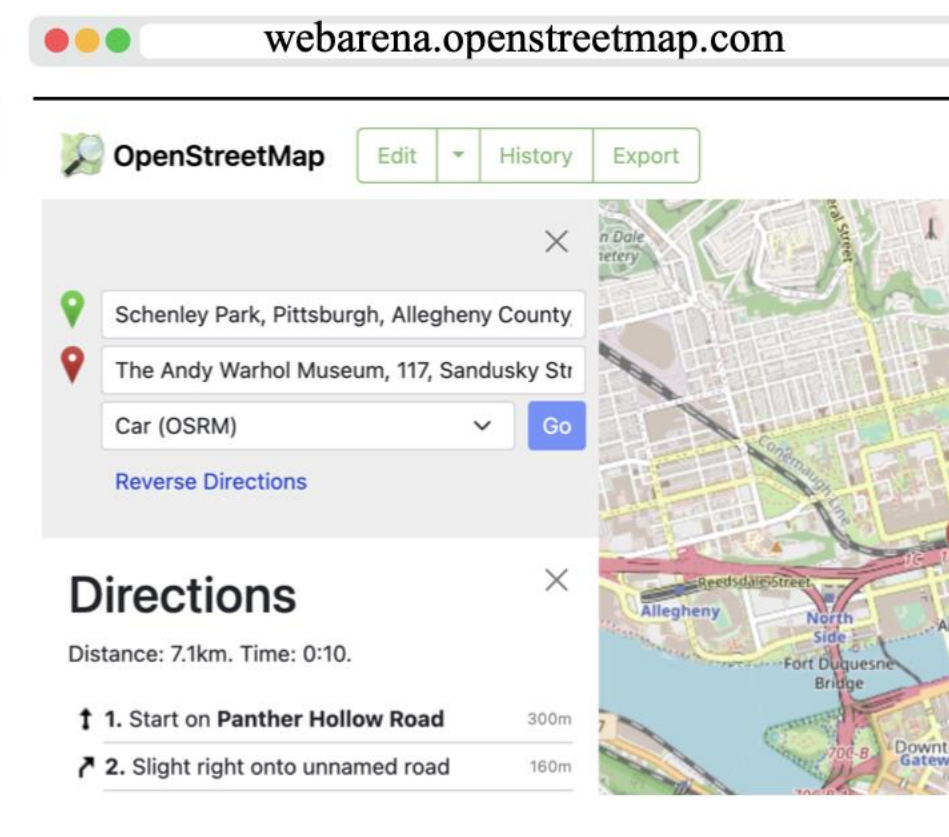
Grounded Instruction Following on Real Websites

WebArena: map instructions to sequence of mouse and keyboard actions

💡 “ Create an efficient itinerary to visit all of Pittsburgh's art museums with minimal driving distance starting from Schenley Park. Log the order in my “awesome-northeast-us-travel” repository ”

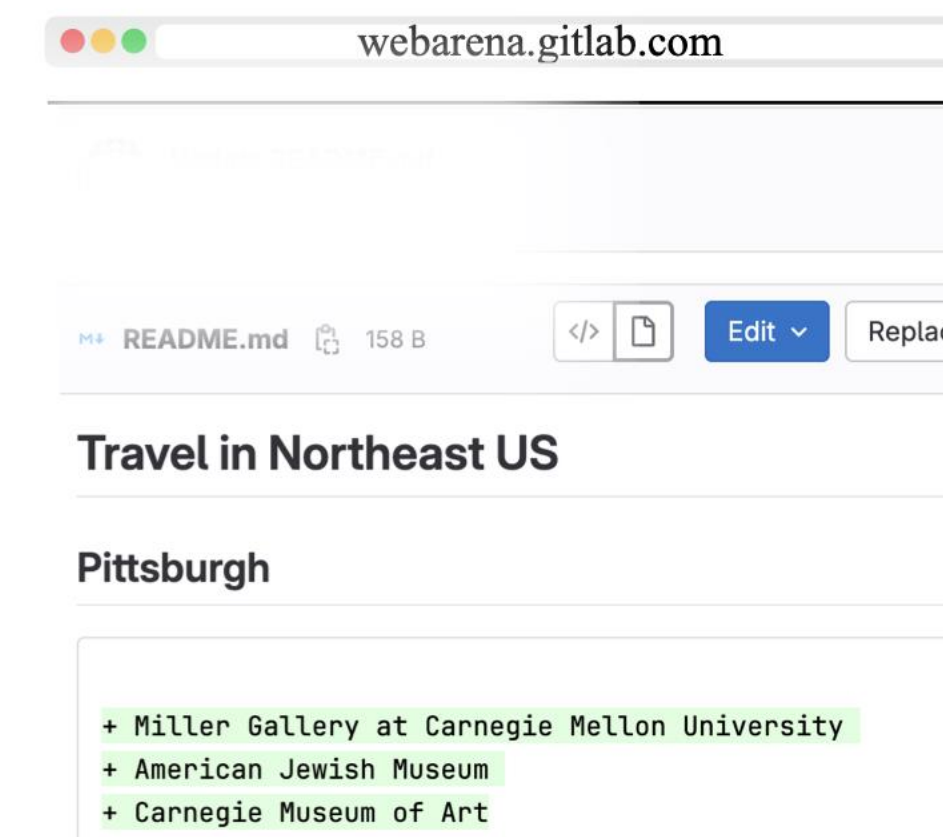


🖱️ Search for museums in Pittsburgh



🖱️ Search for each art museum on the Map

...



🖱️ Record the optimized results to the repo

Environment with sandboxed approximations of real websites spanning e-commerce, social media!

Additional utility tools: Maps, calculators, scratchpads, Wikipedia...

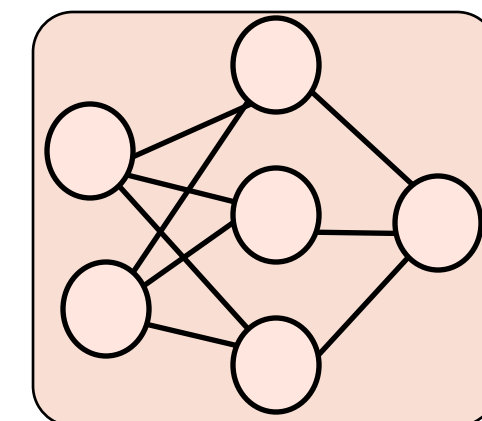
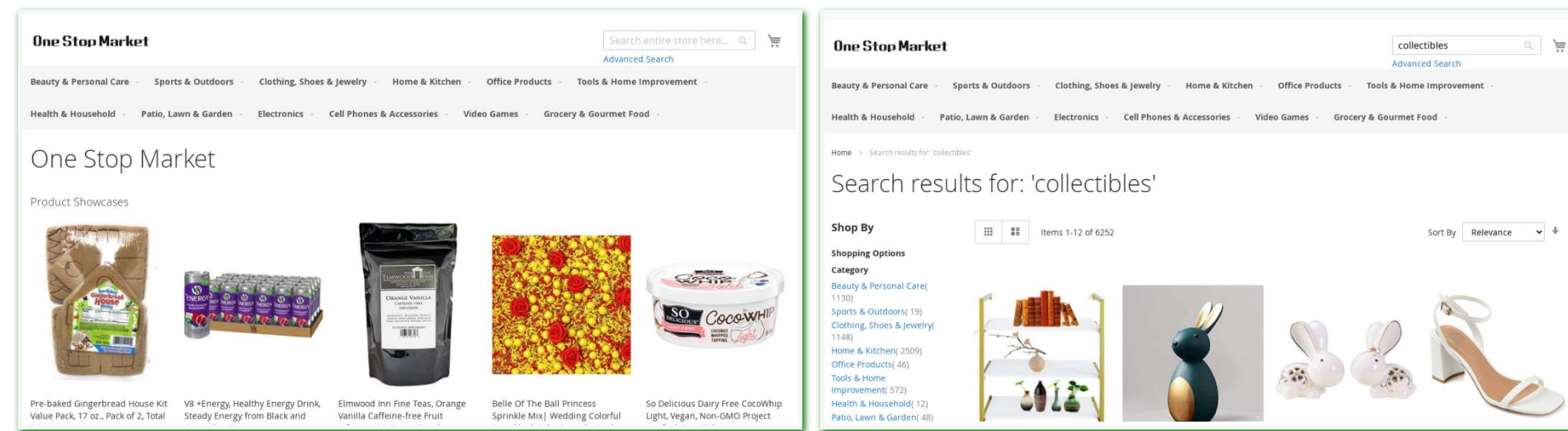
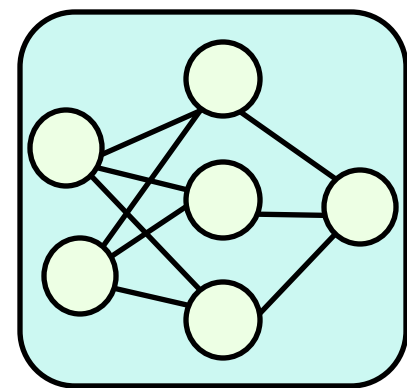
Multi-tab browsing

Long-horizon tasks

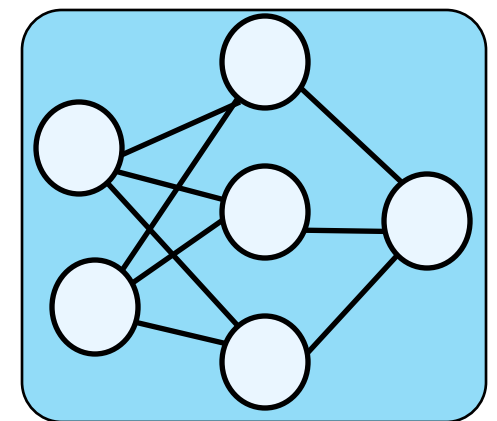
Evaluates functional correctness

Grounded Instruction Following on Real Websites

NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration



Trajectory Labeler

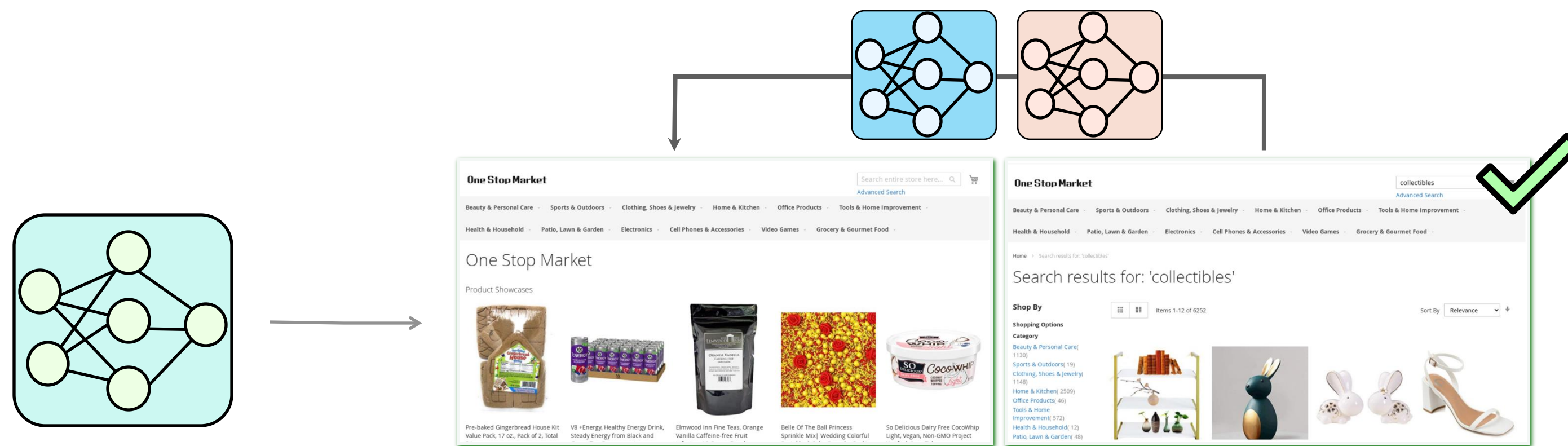


Demonstration Filter

Grounded Instruction Following on Real Websites

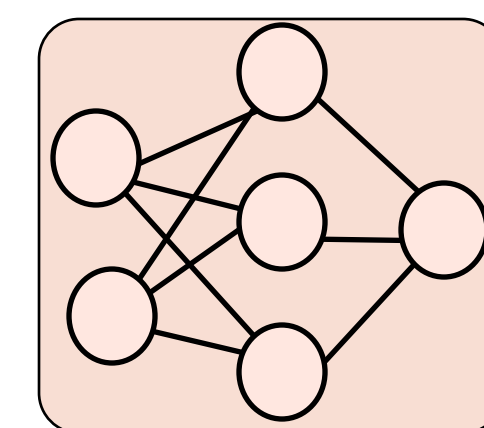
NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration

Search for collectible items and navigate to ceramic rabbit ornaments

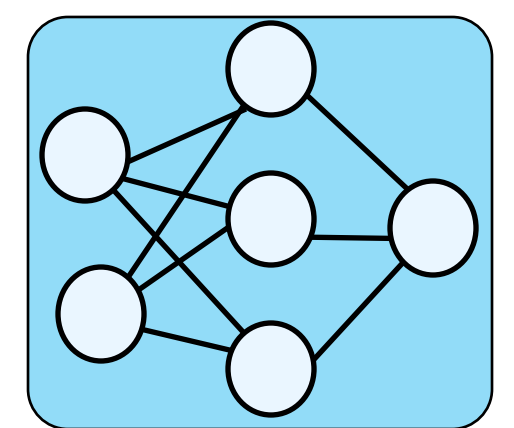


Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low



Trajectory Labeler

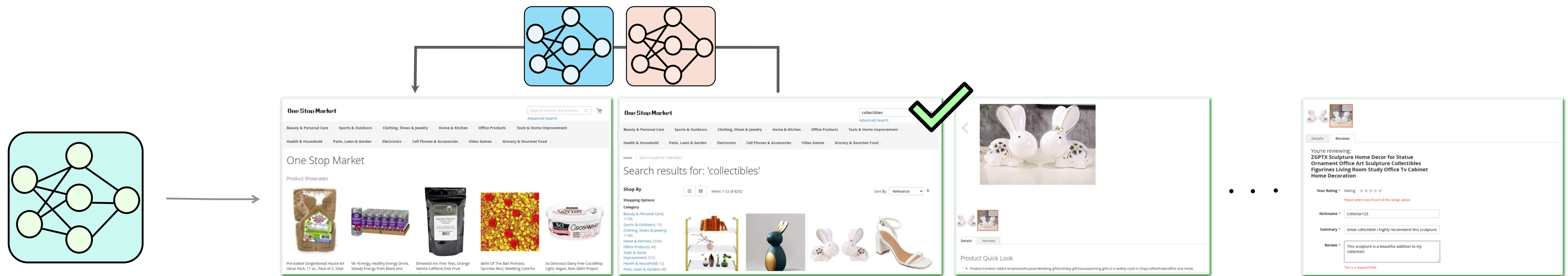


Demonstration Filter

Grounded Instruction Following on Real Websites

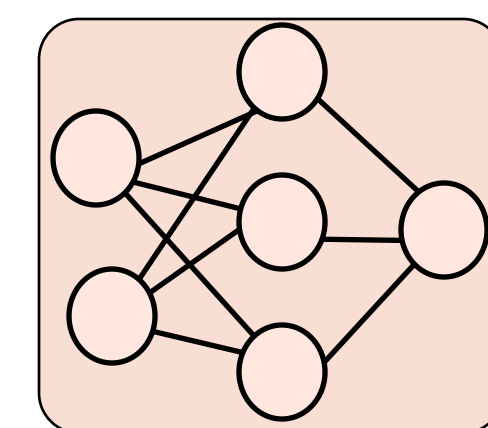
NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration

Search for collectible items and navigate to ceramic rabbit ornaments

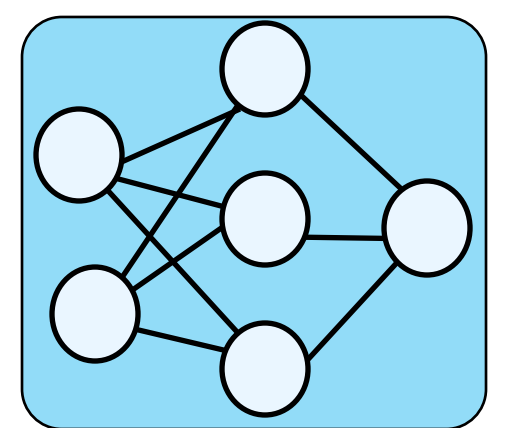


Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low



Trajectory Labeler

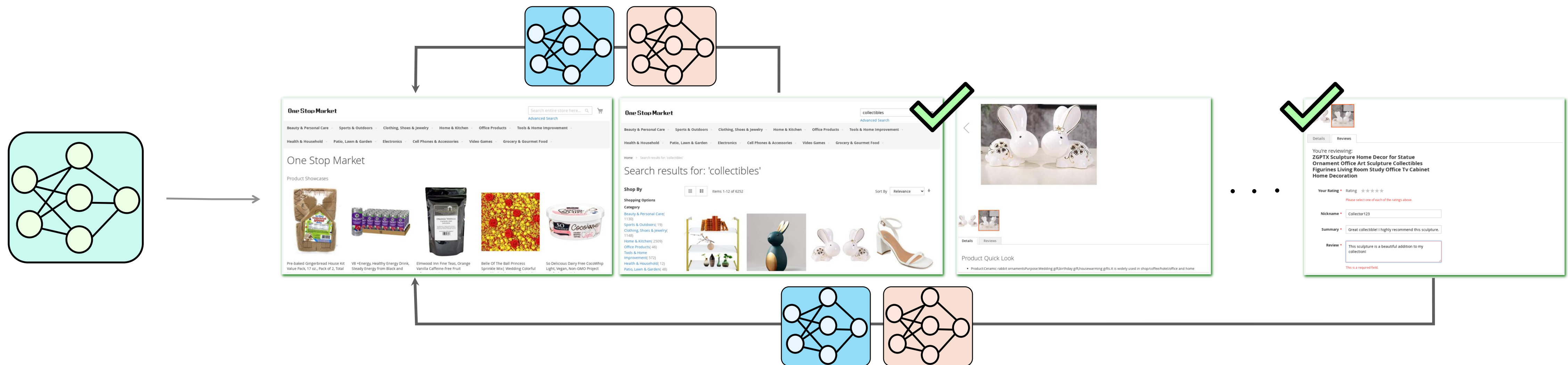


Demonstration Filter

Grounded Instruction Following on Real Websites

NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration

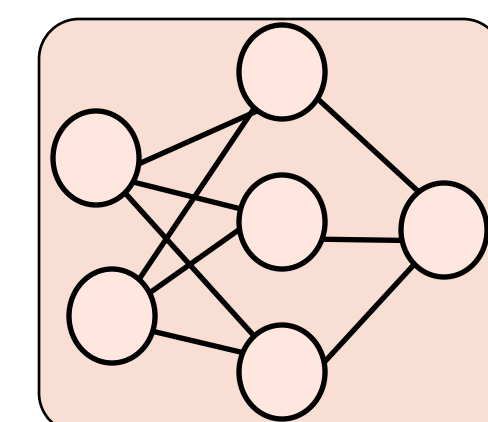
Search for collectible items and navigate to ceramic rabbit ornaments



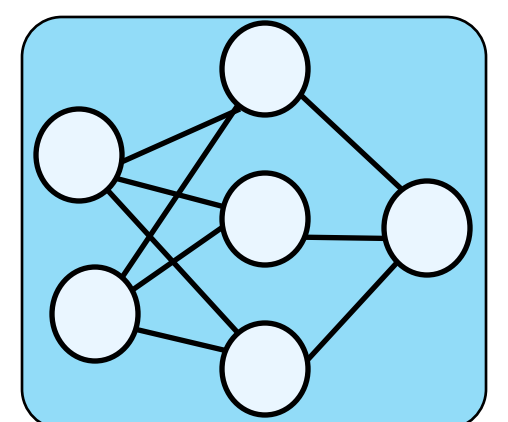
Search for collectible items, check their details and write a review.

Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low



Trajectory Labeler

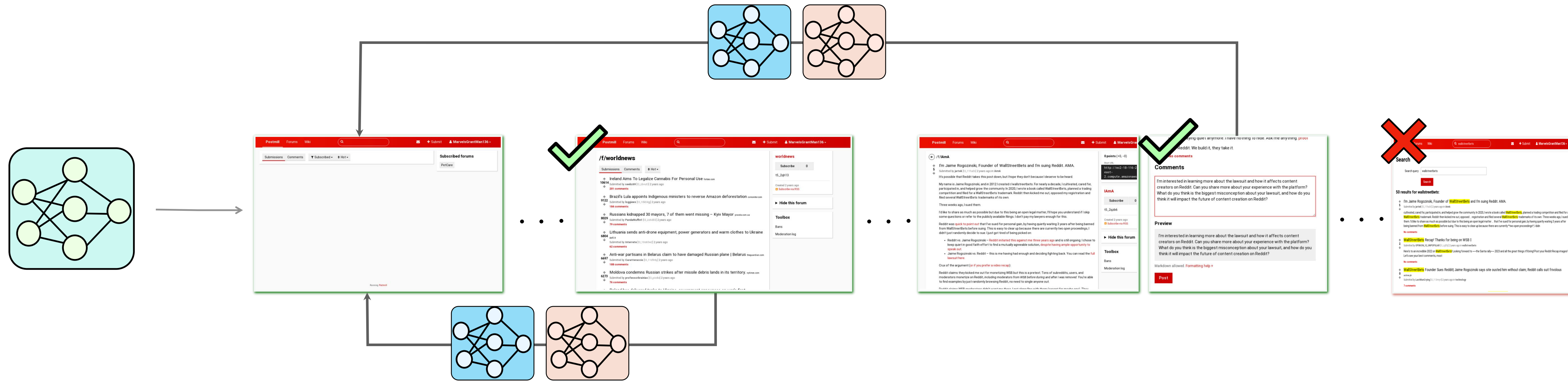


Demonstration Filter

Grounded Instruction Following on Real Websites

NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration

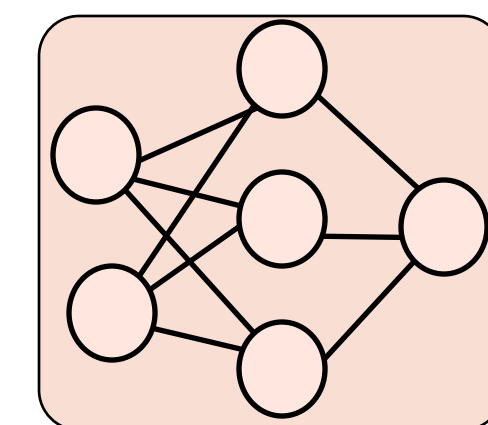
Find the post about Jaime Rogozinski, and his lawsuit against Reddit, and ask him about his experience.



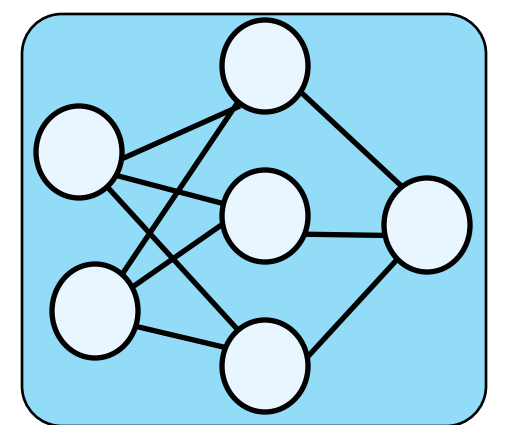
Subscribe to the r/wallstreetbets forum and navigate to world news

Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low



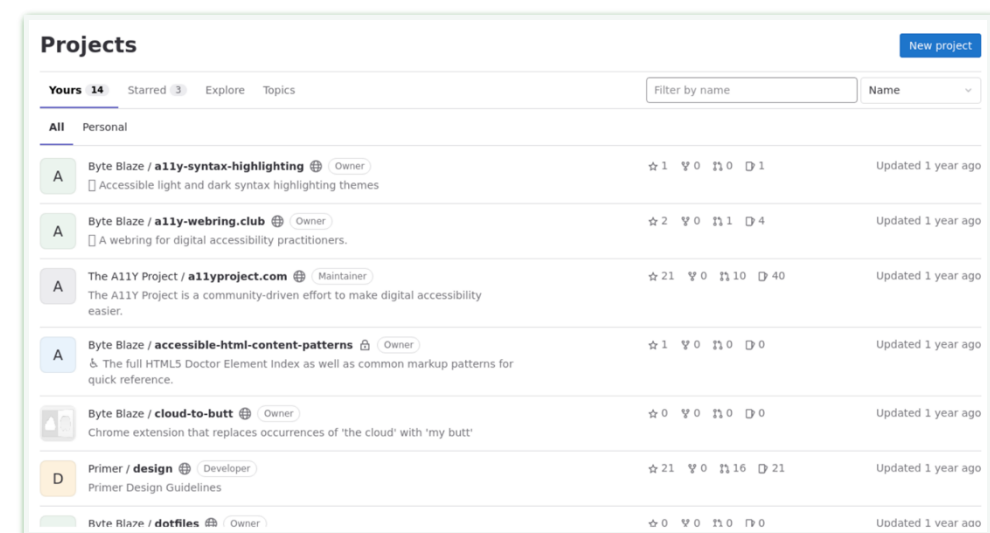
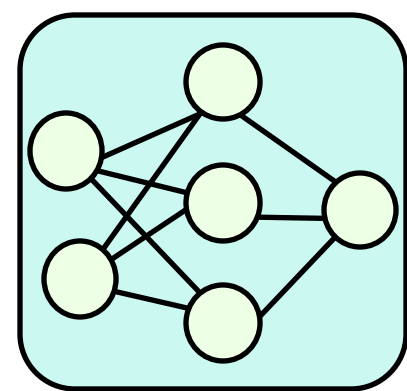
Trajectory Labeler



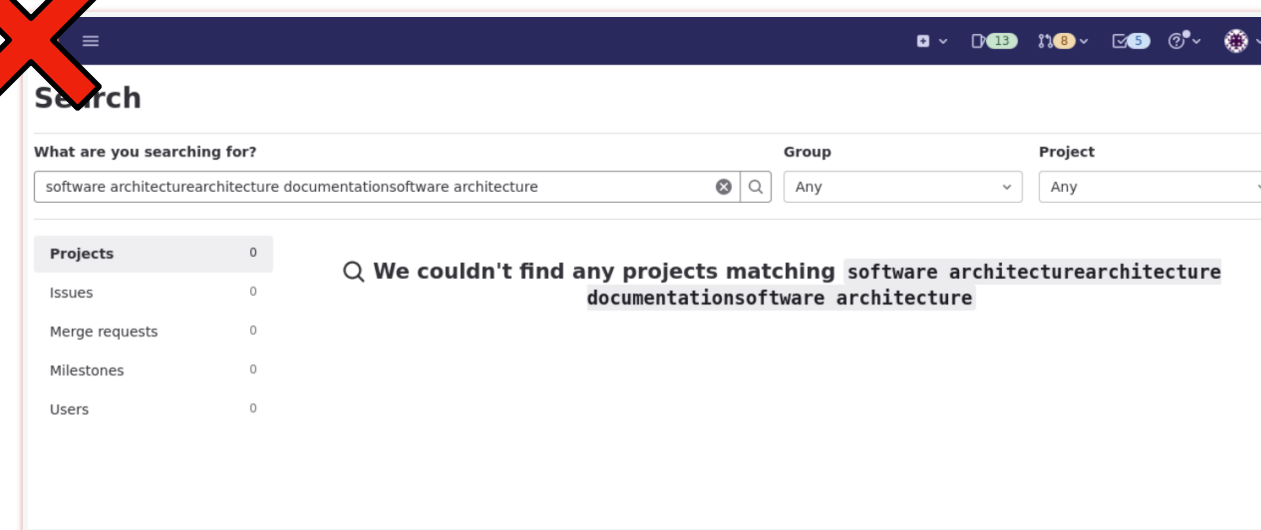
Demonstration Filter

Grounded Instruction Following on Real Websites

NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration

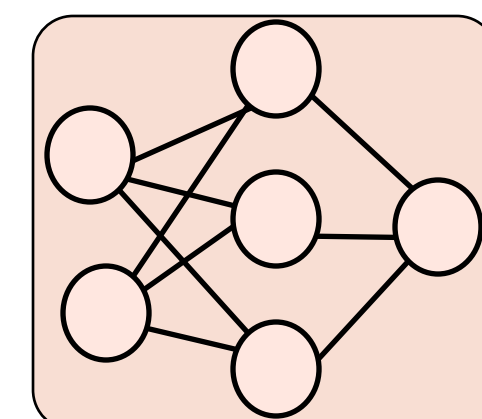


...

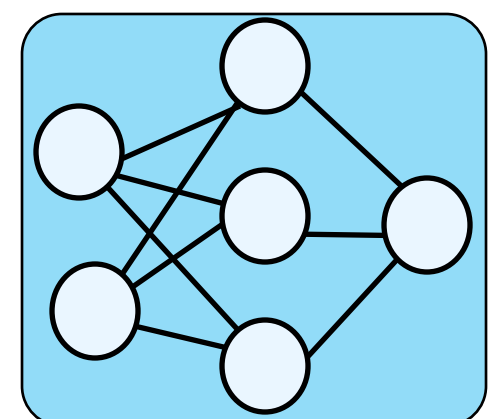


Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low



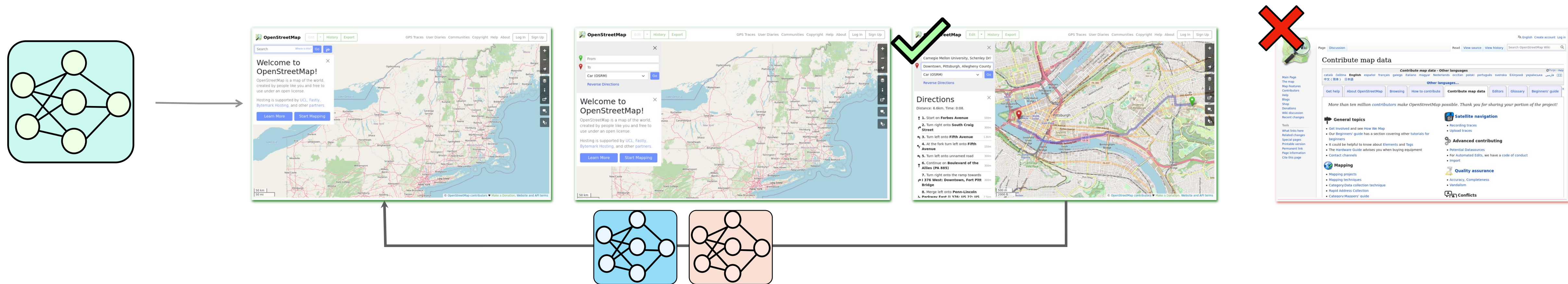
Trajectory Labeler



Demonstration Filter

Grounded Instruction Following on Real Websites

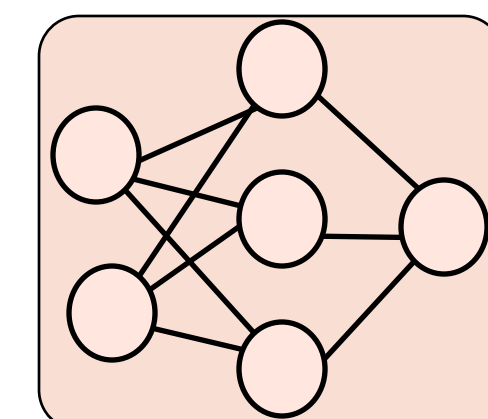
NNetscape Navigator (NNetnav): Our latest attempt for generating complex instructions on realistic websites with structured exploration



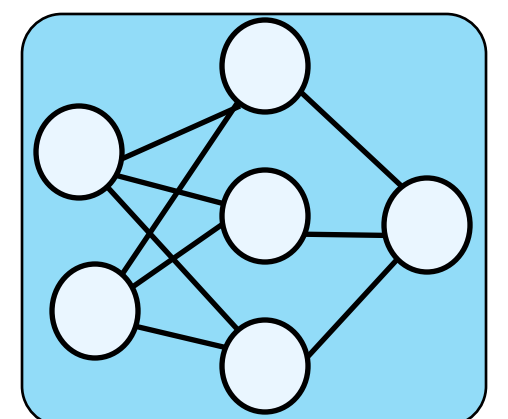
Find driving directions from CMU to downtown Pittsburgh

Pruning Function:

- ▶ Invoke Trajectory Labeler at fixed time-steps
- ▶ Assign reward to resulting (instruction, trajectory) pair
- ▶ Prune if reward is low

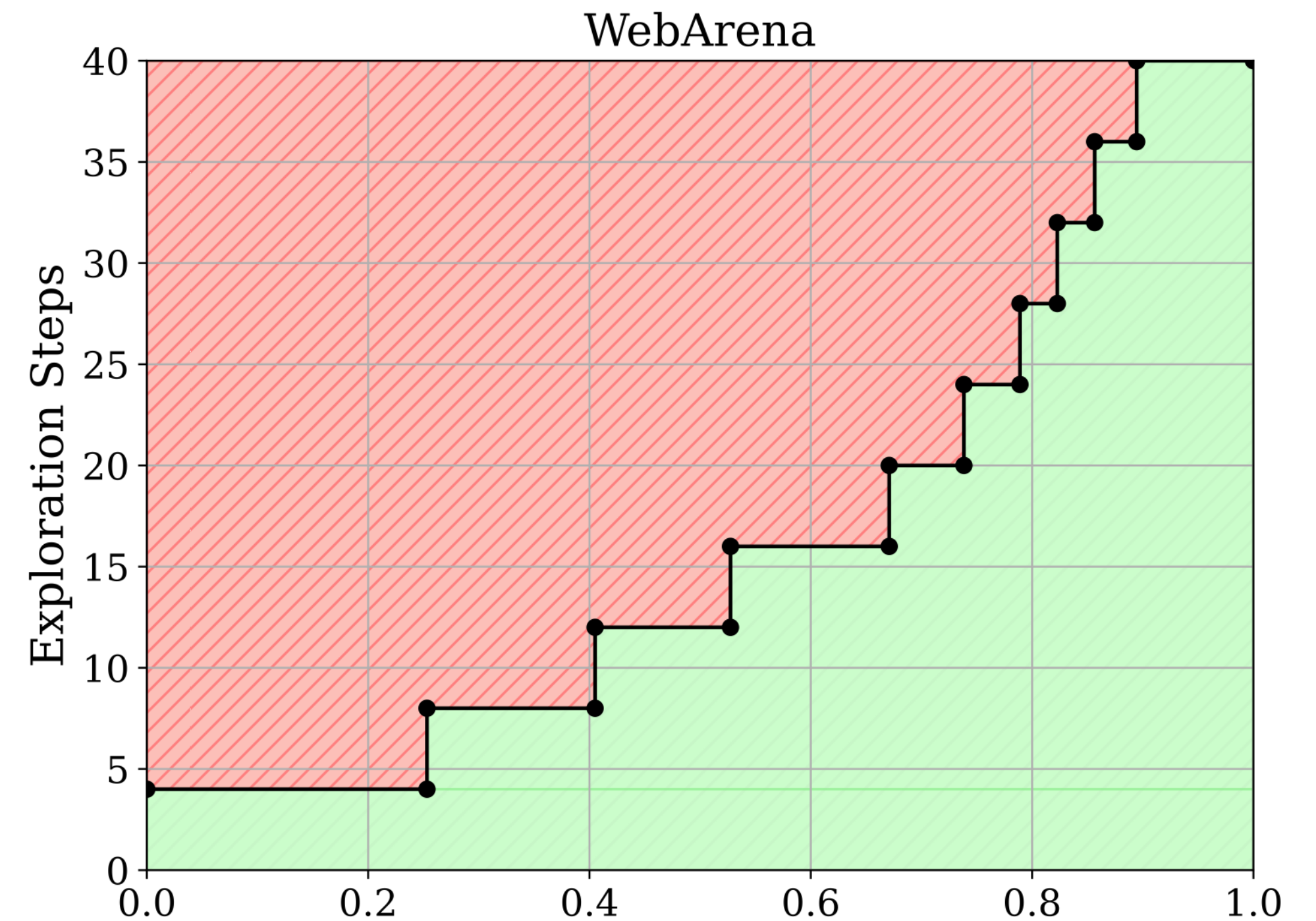
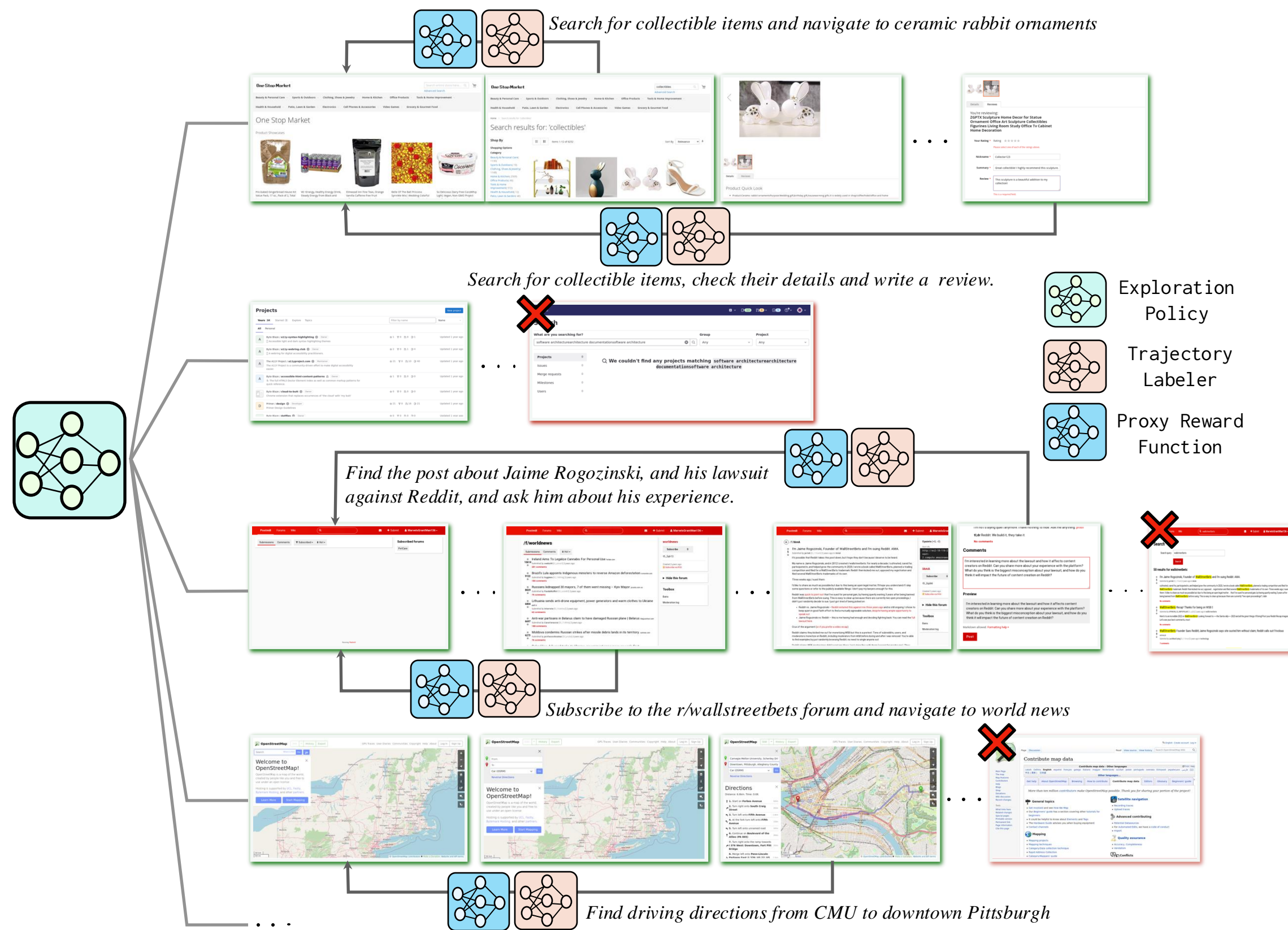


Trajectory Labeler



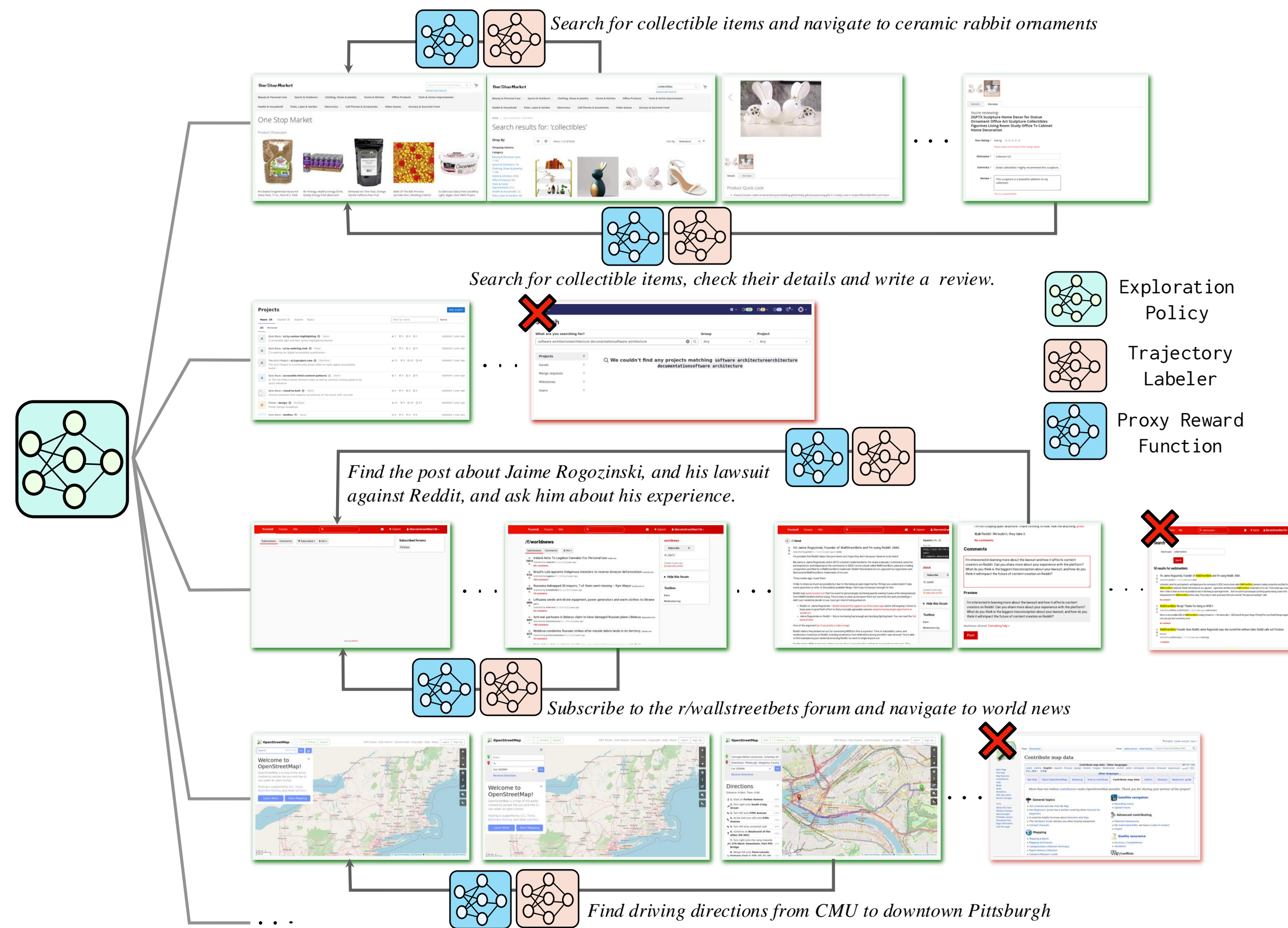
Demonstration Filter

Grounded Instruction Following on Real Websites



Such a pruning strategy leads to very efficient exploration. Here, area shaded in red corresponds to actions that were prevented due to early pruning

Grounded Instruction Following on Real Websites



Investigate the issue of offline downloads in the a11y-webring.club project and create a new task to implement a function to download PDF cards and JSON data for offline access.

Create a new forum for discussing AI and Machine Learning, and create a submission about a new AI-powered smartwatch, then search for reviews about the smartwatch on the website

Find the driving directions from TLC Medical Transportation Services in Syracuse to Times Square in Manhattan.

Add two products, “Abominable Hoodie” and “Samsung Smart TV”, with respective prices \$99.99 and \$50.00, and then start the process of adding a new customer.

Such a pruning strategy leads to instructions that are complex, hierarchical and plausible (by design)

Some Results from Fine-tuning LLama-8b with NNetnav demonstrations

Warmup: MiniWoB++

Domain	Llama-8b	LLama-8b-IF	Llama-8b-NNetnav
click-checkboxes-soft	0.4	0.25	0.65
email-inbox	0.25	0.3	0.3
use-autocomplete	0.25	0.55	0.7
phonebook	0.15	0.15	0.2
...
Mean Reward	0.28	0.28	0.48

Performs better than Instruction-first and Zero-shot LLama

Some Results from Fine-tuning LLama-8b with NNetnav demonstrations

Method	WebArena Success Rate (%)
GPT-3.5	6.2
GPT-4o	14.4
GPT-4o + tree-search	19.2
GPT-4o (BrowserGym)	23.5

- State-of-the-art results based on using GPT-4o, zero-shot + various inference-time procedures like Tree Search
- This work: Finetuning smaller agents (LLama-8b) with demonstrations

Some Results from Fine-tuning LLama-8b with NNetnav demonstrations

Method	WebArena Success Rate (%)	#Demonstrations
LLama-8b (zero-shot)	1	0
AutoWebGLM-7b (S1)*	2.5	240
Synatra-CodeLLama-7b*	6.3	30k

This work: Finetuning smaller agents (LLama-8b) with demonstrations

Some Results from Fine-tuning LLama-8b with NNetnav demonstrations

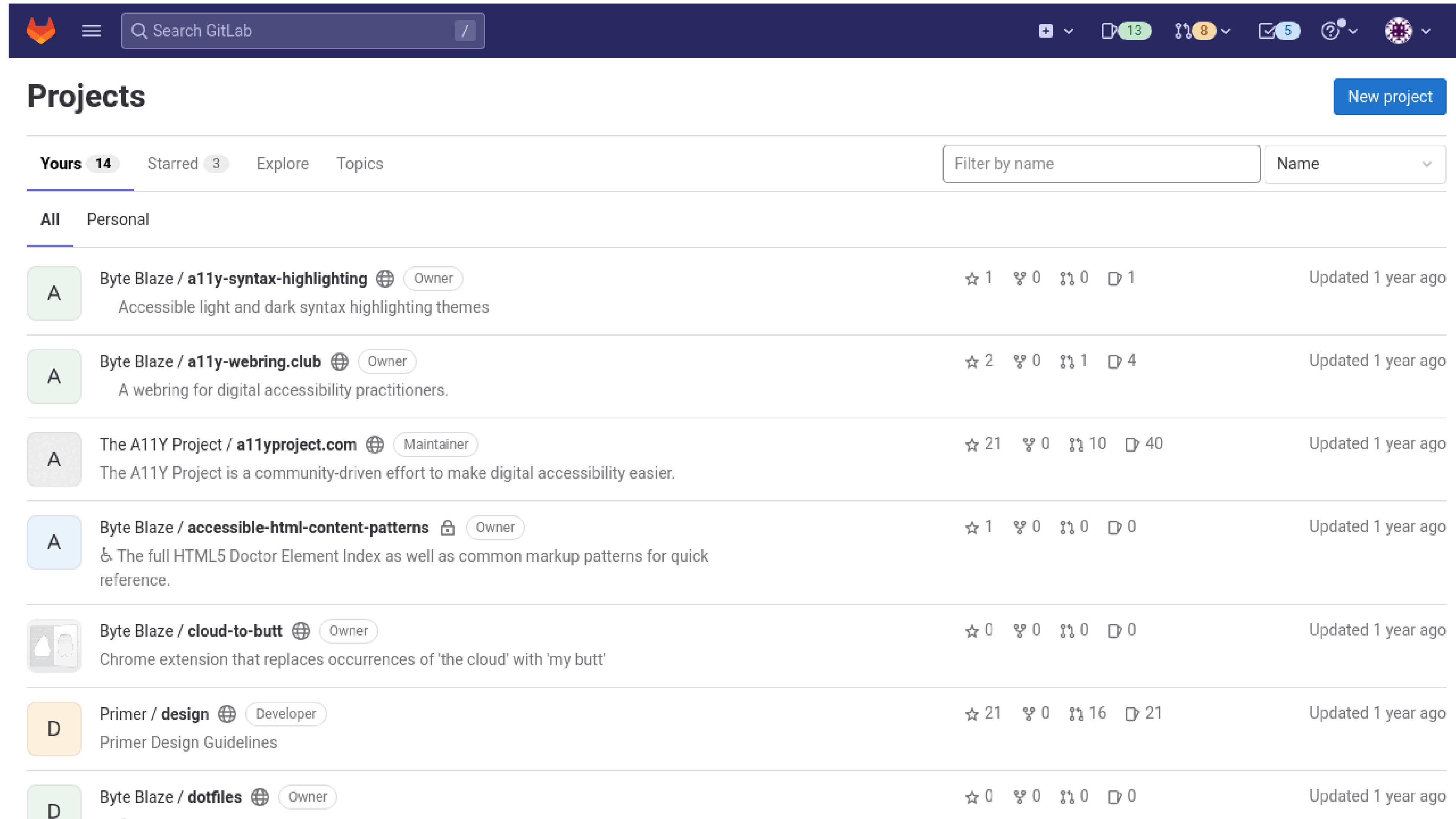
Method	WebArena Success Rate (%)	#Demonstrations
LLama-8b (zero-shot)	1	0
AutoWebGLM-7b (S1)*	2.5	240
Synatra-CodeLLama-7b*	6.3	30k
LLama-8b-IF	4.2	145
LLama-8b-nnetnav	7.2	650

This work: Finetuning smaller agents (LLama-8b) with demonstrations

- ▶ Outperforms prior approaches (sometimes with orders of magnitude fewer demonstrations)
- ▶ Outperforms our instruction-first baseline when controlling for exploration budget

Some rollouts from LLama-3-8b-nnetnav

closing an issue on a repository



The screenshot shows the GitLab interface with the 'Projects' section. The top navigation bar includes the GitLab logo, a search bar, and several utility icons. Below the navigation bar, the 'Projects' heading is followed by a 'New project' button. The main content area displays a list of projects under the 'Yours' filter, which is currently set to 14 items. The list includes projects like 'a11y-syntax-highlighting', 'a11y-webring.club', 'a11yproject.com', 'accessible-html-content-patterns', 'cloud-to-butt', 'design', and 'dotfiles'. Each project entry shows its name, description, owner/maintainer, and various metrics such as stars, forks, issues, and pull requests.

Project Name	Description	Owner/Maintainer	Stars	Forks	Issues	Pull Requests	Last Updated
Byte Blaze / a11y-syntax-highlighting	Accessible light and dark syntax highlighting themes	Owner	1	0	0	1	Updated 1 year ago
Byte Blaze / a11y-webring.club	A webring for digital accessibility practitioners.	Owner	2	0	1	4	Updated 1 year ago
The A11Y Project / a11yproject.com	The A11Y Project is a community-driven effort to make digital accessibility easier.	Maintainer	21	0	10	40	Updated 1 year ago
Byte Blaze / accessible-html-content-patterns	The full HTML5 Doctor Element Index as well as common markup patterns for quick reference.	Owner	1	0	0	0	Updated 1 year ago
Byte Blaze / cloud-to-butt	Chrome extension that replaces occurrences of 'the cloud' with 'my butt'	Owner	0	0	0	0	Updated 1 year ago
Primer / design	Primer Design Guidelines	Developer	21	0	16	21	Updated 1 year ago
Byte Blaze / dotfiles		Owner	0	0	0	0	Updated 1 year ago

Some rollouts from LLama-3-8b-nnetnav

making a comment on a post

The screenshot displays a forum interface with a red header bar. The header contains navigation links for 'Postmill', 'Forums', and 'Wiki', a search bar with a magnifying glass icon, and user controls including an envelope icon, a '+ Submit' button, and a user profile for 'MarvelsGrantMan136' with a dropdown arrow. Below the header, there are filter tabs for 'Submissions', 'Comments', 'Featured', and 'Hot'. A light blue information box states: 'You are not subscribed to any forum. Showing featured forums instead.' To the right, a 'Featured forums' section contains the text: 'There are no featured forums to display.' At the bottom center, the text 'Running Postmill' is visible.

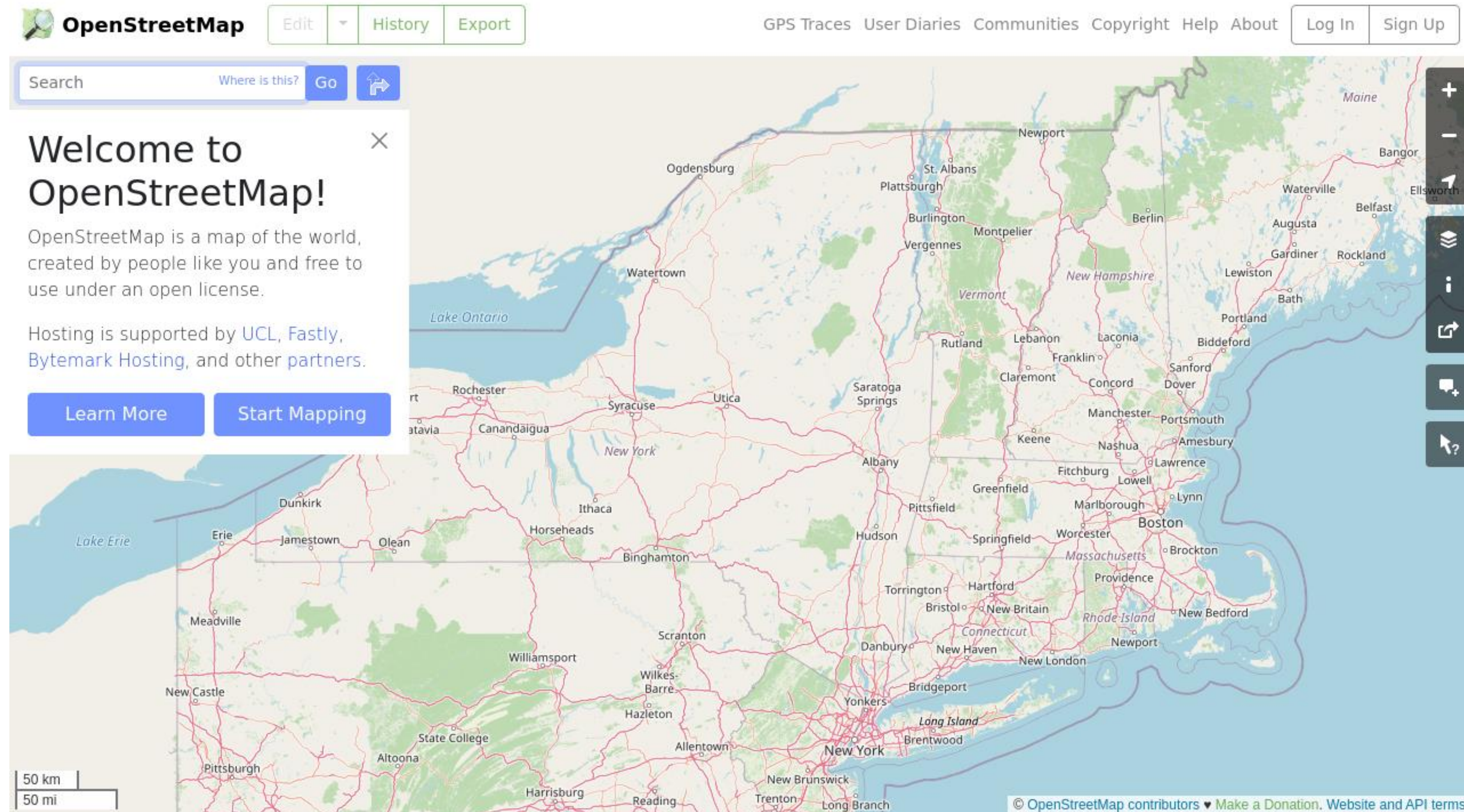
Some rollouts from LLama-3-8b-nnetnav

creating new discussion forum

The screenshot displays a forum interface with a red navigation bar at the top. The bar contains the following elements from left to right: the text 'Postmill', 'Forums', and 'Wiki'; a search input field with a magnifying glass icon; an envelope icon; a '+ Submit' button; and a user profile icon with the name 'MarvelsGrantMan136' and a dropdown arrow. Below the navigation bar, there are two main content areas. On the left, there is a filter bar with tabs for 'Submissions', 'Comments', 'Featured', and 'Hot'. The 'Submissions' tab is currently selected. Below the filter bar, a light blue information box contains an information icon and the text: 'You are not subscribed to any forum. Showing featured forums instead.' On the right, there is a box titled 'Featured forums' which contains the text: 'There are no featured forums to display.' At the bottom center of the page, there is a small footer that reads 'Running Postmill'.

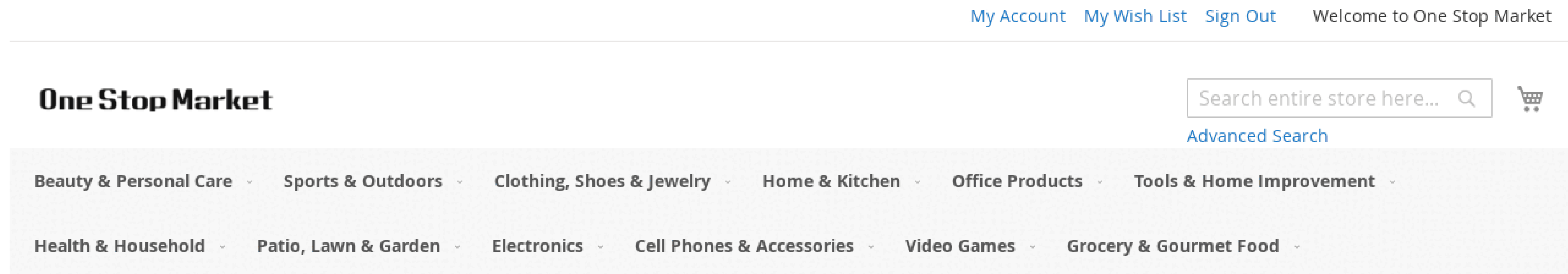
Some rollouts from LLama-3-8b-nnetnav

finding directions on maps



Some rollouts from LLama-3-8b-nnetnav

adding items from prior orders to cart



One Stop Market

Product Showcases



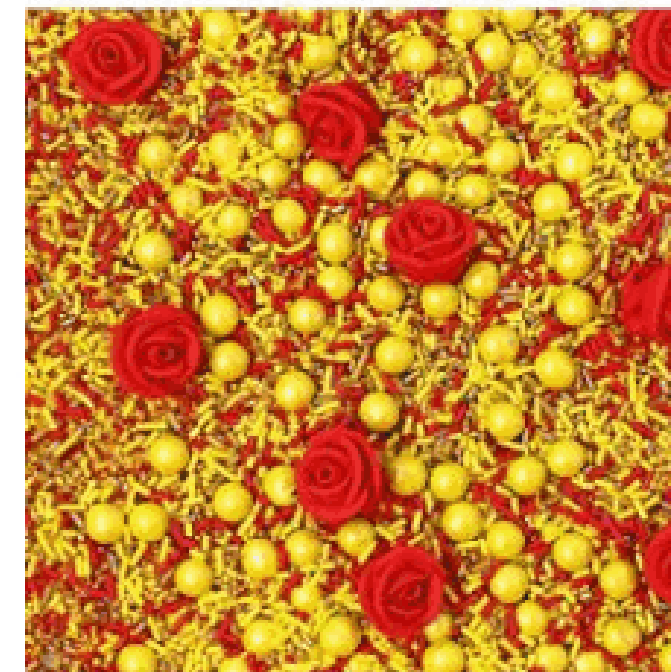
Pre-baked Gingerbread House Kit Value Pack, 17 oz., Pack of 2, Total



V8 +Energy, Healthy Energy Drink, Steady Energy from Black and



Elmwood Inn Fine Teas, Orange Vanilla Caffeine-free Fruit



Belle Of The Ball Princess Sprinkle Mix | Wedding Colorful



So Delicious Dairy Free CocoWhip Light, Vegan, Non-GMO Project

Some rollouts from LLama-3-8b-nnetnav

interacting with inventory

The screenshot shows a dashboard with a dark sidebar on the left containing navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, System, and Find Partners & Extensions. The main content area is titled 'Dashboard' and includes a search bar, a notification bell, and a user profile 'admin'. Below this is a 'Scope: All Store Views' dropdown with a 'Reload Data' button. The 'Advanced Reporting' section features a 'Go to Advanced Reporting' button and a description: 'Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data.' The 'Lifetime Sales' section shows '\$0.00' and a note that the chart is disabled. The 'Average Order' section shows '\$0.00'. The 'Last Orders' section contains a table with columns for Customer, Items, and Total, listing Sarah Miller and Grace Nguyen. The 'Bestsellers' section has tabs for 'Most Viewed Products', 'New Customers', and 'Customers', with a table showing 'Quest Lumaflex™ Band' with a price of \$19.00 and a quantity of 6.

Dashboard Search Notifications admin

Scope: All Store Views ? [Reload Data](#)

Advanced Reporting

Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data. [Go to Advanced Reporting](#)

Lifetime Sales

\$0.00

Chart is disabled. To enable the chart, click [here](#).

Revenue	Tax	Shipping	Quantity
\$0.00	\$0.00	\$0.00	0

Average Order

\$0.00

Last Orders

Customer	Items	Total
Sarah Miller	5	\$194.40
Grace Nguyen	4	\$190.00

Bestsellers

Most Viewed Products | New Customers | Customers

Product	Price	Quantity
Quest Lumaflex™ Band	\$19.00	6

Takeaways from NNetnav

- Yes, LLMs are not necessarily trained for grounded instruction following BUT:
 - ▶ Exploration via an LLM, is a powerful tool for creating training data for grounded instruction following.
 - ▶ Linguistic priors (coming from LLMs) are a powerful tool for structuring and pruning exploration in complex web environments!

BAGEL and NNetNav



Christopher Manning



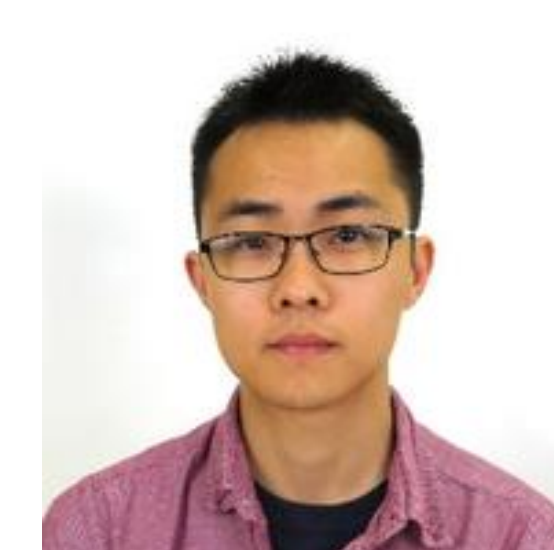
Shikhar Murty



Pete Shaw



Mandar Joshi



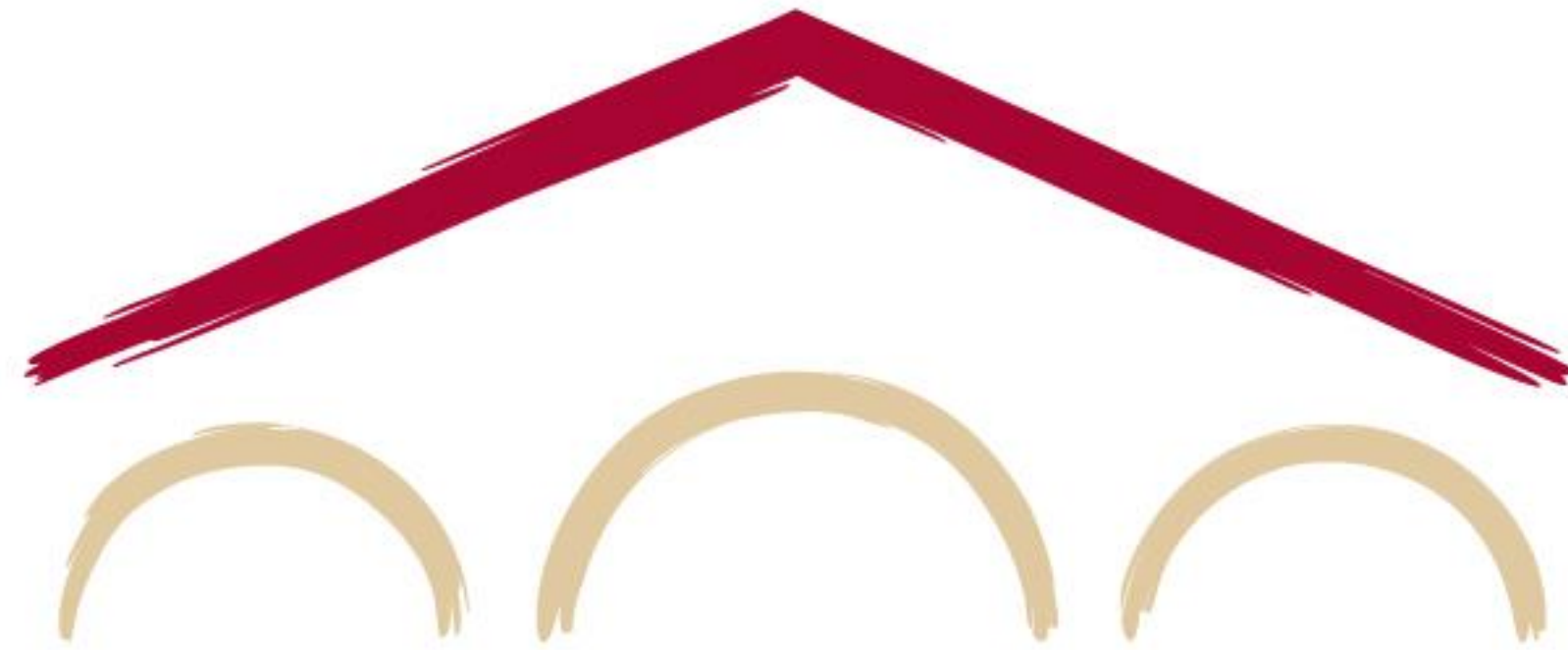
Kenton Lee



Dzmitry Bahdanau

- BAGEL: Bootstrapping Agents by Guiding Exploration with Language (ICML 2024)
[arXiv:2403.08140](https://arxiv.org/abs/2403.08140)
- NNetscape Navigator: Complex Demonstrations for Web Agents without a Demonstrator (In Submission)
<https://openreview.net/forum?id=hHF5AayC7O>

Meaning and Intelligence in Language Models: From Philosophy to Agents in a World



Christopher Manning

@chrmanning ✿ manning@stanford.edu

Stanford NLP Group ✿ Director, Stanford AI Lab

COLM, Philadelphia, 2024

