

MemAgent: A cache-inspired framework for augmenting conversational Web Agents with task-specific information

Nazmus Sakib^{1,*†}, Protoy Barai^{1,†}, Sifat Ishmam Parisa¹ and Anindya Iqbal¹

¹Bangladesh University of Engineering and Technology, Dhaka, Bangladesh

Abstract

Large Language Model (LLM) based web agents require users to repeatedly provide task-specific information across interactions, limiting their practical utility. To address this issue, we propose MemAgent, a framework that enhances web agents with a cache-inspired memory mechanism to store and retrieve task-specific information. MemAgent employs a two-phase architecture that separates information gathering (alignment) from task execution, and introduces a Memory Cache Bank (MCB) with time-based expiration policies. Our evaluation on 150 web tasks across three categories shows that MemAgent reduces the average conversation turns by 22.4% (5.00 to 3.88). Human evaluation with 15 participants demonstrates a 58% reduction in task completion time for recurring tasks. Our implementation code, data, and trained models are available at: https://github.com/DialogBased-Interaction/Goal_Alignment

Keywords

LLM Agents, Memory Cache Bank, MemAgent, Agentic Memory

1. Introduction

With the rise of the Large Language Model (LLM), we have seen an increase of automation in many aspects of our lives – given rise to the concept of *Web Agents* [1, 2, 3, 4, 5]. Broadly, web agents are all systems that use LLMs as their engines and can perform actions on the websites based on observations. These agents can automate users’ web experience such as: booking a flight [3], shopping in amazon [5] and so on.

Current state-of-the-art web agents typically require users to provide a well-crafted detailed task description to execute it. However, prior research shows that crafting effective prompts is a non-trivial task for users. Studies by [6, 7] highlight that users often provide abstract and incomplete prompts, struggling to anticipate and convey all the necessary information. This issue is further exacerbated for recurring tasks as users need to repeatedly provide the same level of detail *every time*, leading to an inefficient and frustrating user experience.

To overcome these issues, recent works have explored augmenting agents with short-term, long-term and working memory [8]. These agents typically store the information in their working/short-term memory and later bypass it into long-term memory. However, the transformation of these information is complex, and is not controllable. On the other hand, few works explored how to enable agents to ask follow-up questions when it is unsure [9] and there is missing information. Although these agents can engage with the users and ask follow-up questions *as it executes*, they still suffer from the memory limitation, i.e., users need to engage with agents every time they execute a task. This raises the question: *How can we bridge between these two paradigms with a simple yet effective agent framework?*

To this end, we present MemAgent, a simple yet effective agent that learns to store task information in a cache by *conversing* with the users. MemAgent works in two phases: *Alignment* and *Execution*. In the *Alignment* phase, the agent is trained to pose follow-up questions to users, capturing and storing

WOA 2025: The 26th Workshop From Objects to Agents, July 2-5, 2025, Trento, Italy

*Corresponding author.

†These authors contributed equally.

✉ 1905061@ugrad.cse.buet.ac.bd (N. Sakib); 1905068@ugrad.cse.buet.ac.bd (P. Barai); sifatiparisa@gmail.com (S. I. Parisa); anindya@cse.buet.ac.bd (A. Iqbal)

🌐 <https://thedeadcoder.github.io/> (N. Sakib)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

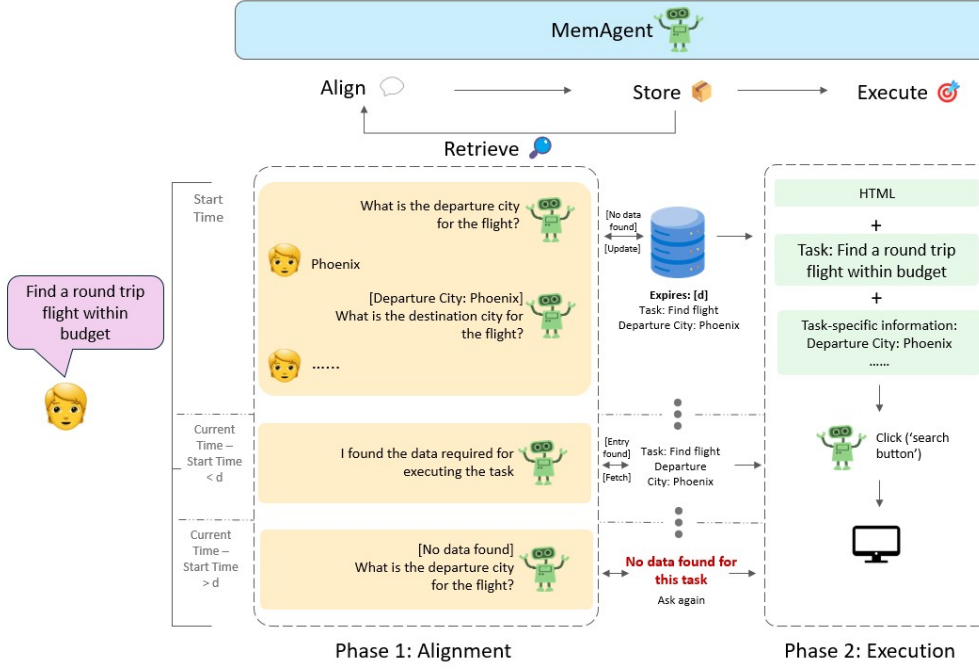


Figure 1: MemAgent Architecture. In *Alignment* phase, it engages in a multi-turn conversation with the users to extract and store task-specific information in a *memory cache bank (MCB)*. During *Execution* phase, MemAgent utilizes the MCB information to execute the task. Each MCB entry has a ‘expires’ field that determines how long it will stay valid.

their responses in our dedicated *memory cache bank (MCB)*. During the *Execution* phase, it leverages this stored information to perform tasks, thereby eliminating the need for users to repeatedly engage in lengthy dialogues, as required by existing models. Instead of using a short-term or long-term memory mechanism [10], we design a simpler, yet effective storage mechanism similar to cache. MCB saves the task details, including type and value information for each task entity and includes an auto-expiration field, which helps to refresh MemAgent’s storage periodically and model user’s dynamic preference.

Our contributions can be summarized as follows:

1. A novel web agent pipeline, MemAgent that can store task specific information in a memory cache bank (MCB). MemAgent learns to create and retrieve information from MCB by conversing with the users.
2. We evaluated MemAgent on a diverse set of tasks to showcase its abilities and improvement on top of existing web agents

2. Related Work

2.1. Autonomous Web Agent

There has been a large body of works on autonomous web agents, investigating how to efficiently utilize large language models for automating usual web activities [4, 11, 12, 2, 3, 5, 13, 14]. [11] performs an offline exploration and creates a transition graph, which is used to provide more contextual information to the LLM prompt. [12] introduces chain-of-action prompting that leverages previous action history and future action plans to decide the next action. Most of the early works on Web UI are based on synthetic frameworks, MiniWob [13] and WebShop [5]. To capture the complexity of real-world tasks, [3] and [2] introduce two realistic environments and datasets encompassing real-world tasks and extend them for evaluating Large Multimodal web agents, [15] and [16], respectively. [17] also introduces a real-world dataset for multimodal web agents and employs overlaying bounding boxes of the web elements, similar to Set-of-Mark prompting [18], to improve the web agent. Perhaps the closest to our work is WebLinX [9], which is a multi-turn dialog dataset for web activities. However, our approach

is significantly different from theirs. We separated the chat and operation actions into two separate phases - Alignment and Execution. We primarily focus on improving web agent’s performance for abstract task descriptions and repetitive tasks. Our MCB is also different from the approach used in WebLinX. Also, very similar to our approach, [19], builds a conversational dataset MT-Mind2Web by organizing and combining the tasks from the Mind2Web dataset based on the similarity of the website domain and instructions. Their approach also involves a memory bank, but unlike our MCB, it includes the conversation history, previous actions and the environmental state(HTML). They have employed multifaceted matching and reflection modules to filter out irrelevant memory components.

2.2. Memory augmentation for LLM Agent

There has been a growing interest on how to incorporate human cognitive principles into LLM agents [20]. CoALA proposes how a combination of procedural, semantic, and episodic memory can be useful for improving the reasoning capacity of agents [10]. Ret-LLM proposes simple ‘read and write’ memory operations for language models [21]. MemGPT proposes a memory augmentation for GPT models which can be accessed with a simple function calling [8]. MemoryBank [22] stores a summary of chat history and user portrait to help in future conversations and recommendations. Unlike their process, we do not store the summary, but rather the user-specific detailed information of each task individually, enabling more transparent and accurate replication in the future.

3. The MemAgent Framework

In this section, we outline the components of our MemAgent framework. MemAgent operates on the principles of *temporal decoupling*. We validate this design choice with a pilot study detailed in §6.

Preliminaries. Given an abstract task description T_a , MemAgent does the following:

1. **Extract** the necessary information $I_q = \{(type_i, value_i) | i = 1, ..., |q|\}$ through conversational interaction (§3.1)
2. **Store** this information in the MCB with appropriate expiration policies (§3.2)
3. **Execute** the task using the combination of T_a and retrieved information, I_q from MCB (§3.3)

3.1. Phase 1: Alignment

Given T_a , MemAgent engages in a multi-turn conversation with the users in *Alignment* phase to obtain all necessary details for I_q . In this phase, the agent has two key responsibilities - 1) *Enquire*: Only ask questions that are relevant to the current task; 2) *Extract*: Parse user response to find out the information type($type_i$) and value($value_i$).

3.2. Memory Cache Bank (MCB)

Central to MemAgent is the memory cache bank, MCB, which stores I_q for each T_a . Similar to cache, T_a has an ‘Expires’ field, which controls when I_q becomes stale. MCB provides several benefits to MemAgent: 1) *Reduced turn of conversation*: It stores the detailed information, I_q for T_a so that the user does not need to provide the detailed information every time they want to execute T_a . 2) *Integration with Retrieval Augmented Pipeline*: MCB can be easily integrated with Vector Databases to support retrieval augmented execution for web agents (please see §7.1 for detailed experiments with Vector database).

3.3. Phase 2: Execution

Given T_a and I_q , MemAgent completes the task in the *Execution* phase. In this phase, we adopt a two-step workflow similar to the Mind2Act framework proposed by Mind2Web [3]. Our approach differs in that we concatenate T_a and I_q instead of solely relying on the task description T_a . This concatenation

allows us to examine the efficacy of the additional context towards task completion, without altering execution strategy (§4.1). Similar to MindAct, our execution framework operates in two steps. – 1) candidate generation: a small LM ranks webpage elements based on T_a ; ¹ 2) action prediction: a larger LM predicts the action and target element from top-k candidates ranked in the first step ($k = 10$).

4. Experiments

4.1. Dataset

While there are multiple datasets on web agents, there is no specific dataset in our desired format that includes multi-turn conversation and task information in slot filling style [23]. Hence, we synthetically augment our dataset over Mind2Web [3] to create a conversational dialog between a user and an agent. Table 1 shows an example data from our augmented data. We use GPT-4-1106-preview to create this augmented data following Self-Refine framework [24]. Specifically, we tell the GPT model to generate the augmented data, followed by feedback in terms of conciseness (whether it includes repetitive conversation), usefulness (whether it includes useful questions), and verbosity (whether it asks the question with less verbosity) on a scale of 1 to 5. If score is below 5 on any metric, we ask the GPT to refine the augmented data further. Table 2 shows the data distribution used in MemAgent.

Table 1

An example of augmented data in MemAgent.

Abstract task, T_a	Followup Questions for Alignment Phase	Memory Bank, I_q
Calculate shipping cost for a package	What is the weight of the package?	Weight: 4 pounds
	Where is the package being shipped from ?	Shipped from: Texas
	What is the destination of the package?	Destination: New York
<i>Corresponding Task in Mind2Web</i>		
Calculate shipping cost for 4 pound package from Texas to New York		

4.2. Models.

Finetuning. For alignment, we have fine-tuned Vicuna 7B [25]. We initialize the training in two ways: 1) empty MCB: agent has to ask all the questions relevant to the task; 2) prefilled MCB: agent has to ask only the remaining questions relevant to the task. For execution, we finetune MindAct from Mind2Web in its three variants (Flan-T5 Base, Large, XL). Each training was completed either on a A100 or A6000 GPU. For hyperparameters, please see §4.4.

In-context Learning (ICL). We also report the effectiveness of MemAgent with few-shot prompting for LLMs. We report our results both on GPT-4o and Gemini-1.5-pro with 2-shot prompting. For Alignment, we explore basic, CoT [26] and ReAcT [27] prompting technique w/ or w/o MCB. For execution, we explore the 3-shot prompting similar to Mind2Web. Please see Appendix A.1 to find the corresponding prompt in each setting.

4.3. Evaluation Metrics

Alignment. To measure whether the task information is derived successfully, we adopt the BERTScore [28] and BLEUScore [29] metrics to calculate the similarity between the ground truth and the generated MCB. We also measure the turn of conversation between the user and agent (lower is better), to compute how well the model can ask relevant questions. For an objective evaluation of information extraction, we also measure the *Precision* and *Recall* of the extracted memory entities and the corresponding values.

Execution. To assess the successful execution of the task, we measure the metrics established in the literature [3]. The supported operations are: Click, Select, and Type. The element accuracy measures

¹We use their off-the-shelf candidate generator since the data augmentation does not impact the ranking.

Table 2

Train data(a) & Test data(b) distribution in MemAgent

Description	Count
# of data samples w/o MCB	779
# of data samples w/ MCB	15136
# of action steps	6659
Split ratio	0.9
Train sample count	13785
Eval sample count	1532

(a)

	Description	Count
Cross Task	# of data samples w/o MCB	50
	# of data samples w/ MCB	1752
	# of action steps	312
Cross Website	# of data samples w/o MCB	50
	# of data samples w/ MCB	442
	# of action steps	263
Cross Domain	# of data samples w/o MCB	50
	# of data samples w/ MCB	455
	# of action steps	244

(b)

the correct element prediction. The Operation F1 score calculates the F1 score for the predicted operation and is important for evaluating the input value of the Select and Type operations. The step success rate considers if the correct element and operation are identified. Finally, the overall success rate checks if all steps are executed accurately.

Evaluation Algorithm. We have shown the pseudocode of our evaluation algorithm in Listing 1. In each step, we ask the model to generate a relevant question. We calculate the cosine similarity of the generated question with the ground-truth questions and select the response of the most similar question from the ground-truth as the answer to the generated question. If the cosine similarity is below a threshold value, we select ‘not specified’ as the answer. We append the generated question and the chosen answer to the model input for the subsequent step. This generation and selection process continues until the model outputs ‘Finish’. We noticed LLMs can sometimes generate the same questions repetitively (Figure 13 Appendix), which makes the conversation very lengthy. Hence, we forcefully stop the conversation if the conversation turn exceeds 10.

Algorithm 1: MemAgent Evaluation

Data: task, $[GT_{conv}]$, GT_{bank} , $[GT_{dom}]$
Result: s_{bert} , s_{bleu} , $turn$, $F1$, $step_SR$, $elem. acc$, SR
 $turn = 0$; mem_bank , $message = []$;
if task in bank: $message.append(GT_{bank}.task)$
if task in bank: $mem_bank.append(GT_{bank}.task)$
while true **do**
 $q, mem = alignment(message)$;
 $gt_q, gt_a = find_closest(q, GT_{conv})$;
 $s_{bert}, s_{bleu} = calculate(q, mem, GT_{bank}.task)$;
 $turn += 1$;
 $message.append(gt_a)$;
 $mem_bank.append(mem)$;
 if ($turn > 10$ || ‘FINISH’ in q): **break**;
end
while true **do**
 $a = execution(mem_bank, task, GT_{dom})$;
 $F1, step_SR, elem. acc = calculate(a, GT_{dom}.a)$;
 if (‘FINISH’ in a): **break**;
end
 $SR = sum(step_SR) == len(GT_{dom})$;

Table 3
Hyperparameters Alignment(a) & Execution(b)

Vicuna 7b		
LoRA	r	32
	α	64
	dropout	.05
epoch: 4, learning rate: $2e^{-4}$		
2-shot prompting		
GPT-4o	temperature: 1	
Gemini-Pro	temperature: 1 top_p: 0.95	

(a)

Fine-tuned MindAct Models			
	epoch	batch size	LoRA
Flan-T5 _B	5	32	
Flan-T5 _L	5	32	r=8
			α =16 dropout=0.05
Flan-T5 _{XL}	3	64	r=16
			α =32 dropout=0.05
3-shot prompting			
GPT-4o	temperature: 0		
Gemini-Pro	temperature: 0.5, top_p: 0.5		

(b)

Table 4

MemAgent result for Alignment Phase. For ICL, CoT + MCB prompting performs best in most cases across the test splits. For fine-tuned model, the avg. turn of conversation is significantly less than the ICL version, denoting fine-tuning helps the model to learn to ask only contextualized questions.

	Model Name	Cross-Task			Cross-Website			Cross-Domain		
		BleuScore (↑)	BertScore (↑)	Avg. # (↓)	BleuScore (↑)	BertScore (↑)	Avg. # (↓)	BleuScore (↑)	BertScore (↑)	Avg. # (↓)
Finetuned model	Vicuna _{7B} (w/ <i>prefilled</i> MCB)	43.17	0.92	2.52	45.53	0.94	2.94	45.04	0.93	2.64
	Vicuna _{7B}	40.85	0.93	3.56	38.92	0.93	3.24	39.91	0.93	3.66
2-Shot Prompting	GPT-4o	-	-	8.66	-	-	8.90	-	-	9.04
	GPT-4o + MCB	22.13	0.80	7.04	18.32	0.82	6.94	13.62	0.78	7.82
	GPT-4o + CoT + MCB	23.25	0.86	6.96	20.72	0.85	6.96	15.66	0.80	7.32
	GPT-4o + ReAct + MCB	19.48	0.81	7.28	18.54	0.83	7.26	20.14	0.74	7.26
	Gemini-Pro	-	-	5.44	-	-	5.20	-	-	5.00
	Gemini-Pro + MCB	17.78	0.76	6.52	22.90	0.87	5.64	14.25	0.83	5.34
	Gemini-Pro + CoT + MCB	27.78	0.83	4.60	27.05	0.83	3.96	29.35	0.79	3.88
	Gemini-Pro + ReAct + MCB	22.62	0.85	5.08	27.03	0.89	5.22	20.27	0.86	5.06

Table 5

MemAgent result for Extraction Phase. Gemini-Pro+CoT performs the best among the the LLMs. But the finetuned Vicuna-7B model outperforms others with a significant margin.

	Model Name	Cross-Task				Cross-Website				Cross-Domain			
		Type (↑)		Value (↑)		Type (↑)		Value (↑)		Type (↑)		Value (↑)	
		Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall
Finetuned model	Vicuna _{7B}	0.34	0.28	0.45	0.39	0.34	0.20	0.53	0.30	0.38	0.27	0.50	0.34
2-Shot Prompting	GPT-4o + CoT + MCB	0.27	0.13	0.40	0.20	0.28	0.11	0.32	0.12	0.12	0.05	0.14	0.06
	GPT-4o + ReAct + MCB	0.27	0.12	0.44	0.17	0.20	0.08	0.36	0.14	0.12	0.05	<u>0.20</u>	<u>0.09</u>
	Gemini-Pro + CoT + MCB	0.41	0.17	0.52	0.22	0.30	0.15	0.39	0.17	0.13	0.06	0.16	0.08
	Gemini-Pro + ReAct + MCB	0.26	0.11	0.46	0.18	0.20	0.10	0.36	0.15	0.10	0.04	0.10	0.04

4.4. Experimental Setup

Framework. We use Fastchat and Axolotl framework for training the models in Alignment Phase. For Execution, we followed the official github repository by Mind2Web [3].

Hyperparameter setup

Alignment. Table 3a shows the hyperparameter settings of this phase.

Execution. We have fine-tuned all three MindAct Flan-T5 models with the learning rate $5e^{-5}$. Flan-T5_L and Flan-T5_{XL} were fine-tuned using LoRA. Table 3b shows the other hyperparameters: epoch, batch size, LoRA rank r, LoRA scaling factor α and the temperature parameters for ICL.

5. Results

Similar to Mind2Web, due to budget constraints, we evaluate MemAgent on 150 test samples (50 from each split: Cross-Task, Cross-Website, Cross-Domain). As we use the Mind2Web’s off-the-shelf candidate generator, the failure of ranking ground-truth (*positive*) candidates could impact overall

Table 6

MemAgent result for Execution Phase. Finetuned models perform better on the cross Task split, whereas in ICL, the performance is consistent across the splits.

Model Name	Cross-Task				Cross-Website				Cross-Domain			
	Ele. Acc. (↑)	Op. F1 (↑)	Step SR (↑)	SR (↑)	Ele. Acc. (↑)	Op. F1 (↑)	Step SR (↑)	SR (↑)	Ele. Acc. (↑)	Op. F1 (↑)	Step SR (↑)	SR (↑)
Fine-tuned	55.78	83.56	52.43	18.0	48.91	72.07	42.42	2.0	55.38	80.53	48.6	8.0
MindAct	62.04	82.51	57.13	14.0	53.9	71.63	47.14	2.0	62.61	82.57	56.82	10.0
Model	67.73	82.11	62.33	16.0	56.75	72.83	48.71	6.0	59.83	76.76	51.92	12.0
3-shot	60.34	79.44	54.62	6.0	56.03	73.05	47.44	6.0	63.1	84.75	58.88	16.0
GPT-4o												
Gemini-Pro	50.87	69.58	45.26	4.0	48.04	70.17	36.91	2.0	54.43	78.97	48.27	4.0

performance. To minimize this effect, we pick samples with the least missing candidates. Specifically, 50 samples in cross-domain have positive candidates for all task steps. For cross-task and cross-website, the values are 43 and 29 respectively. To pick the remaining samples in these splits, we randomly select samples with missing candidates in only one step. This approach ensures a more reliable evaluation of MemAgent’s performance.

5.1. Alignment

Table 4 shows the results for MemAgent Alignment phase.

Finetuned model. All the finetuned models perform consistently across the test splits, whereas Vicuna w/ prefilled MCB being slightly better than the rest in terms of avg. turn of conversation.

In-context learning. Gemini-pro performs best when CoT + MCB strategy is applied. For baseline prompting, we only calculate the avg. turn of conversation since there is no MCB generated in this setting. We also notice that finetuned models perform better than few-shot prompting in general. Notably, with ICL, the models can sometimes ask repetitive questions often unnecessary for a given task. To circumvent this, we conclude the conversation when Avg. # reaches 10. See Figure 13 in appendix for an example.

5.2. Extraction

The scores in the alignment phase do not depict the capabilities of our agent to extract task-specific memory entities. So, we take the first k(#no of turns in ground truth) number of model outputs from each conversation. Then, we extract the memory portions from the ground truth and model outputs. Given the types and values of ground truths and model outputs, we calculate the precision and recall of entity type and entity value separately by similarity matching. Table 5 shows that the finetuned Vicuna-7B outperforms all the tested models in extraction. Vicuna-7B-prefilled model is not evaluated because some of the memory entities are prefilled which may create a bias in overall model output. Gemini-Pro+CoT+MCB performs significantly well among all the LLMs. We only use CoT and ReAct prompts in evaluation because of their consistent performance in the alignment phase.

5.3. Execution

Table 6 shows the results for MemAgent Execution phase. Flan-T5_{XL} and the GPT-4o model perform better than the rest. Flan-T5 models perform well in the Cross-Task split due to the transferable knowledge between the training and test samples. GPT-4o generalizes better to the cross-domain split. The samples in our cross-domain split have fewer action steps (244) than the other two (312 and 263). The reduced number of steps has also contributed to GPT-4o’s better performance in the Cross-Domain split.

6. Human Evaluation

We conduct a pilot study with 15 participants to understand the impact of storing repetitive queries in MCB. We used a vector database to simulate MCB, as shown in Figure 2. Whenever a user queries the model, we first fetch similar tasks performed by the user from the vector database. There is a TTL

(Time-to-Live) involved which we fixed to simulate cache invalidation. In a certain TTL boundary, semantically similar task histories are fetched. They are re-ranked based on similarity and recency. In our vector Database, we kept 3 vectors. We have used **BM-25** as Sparse vector [30], **Text-Embedding-3-Large** as Dense vector [31] and **ColBERT** as Late Interaction model [32]. These histories serve as a cache. Then the model generates necessary questions with some of the answers auto-filled.

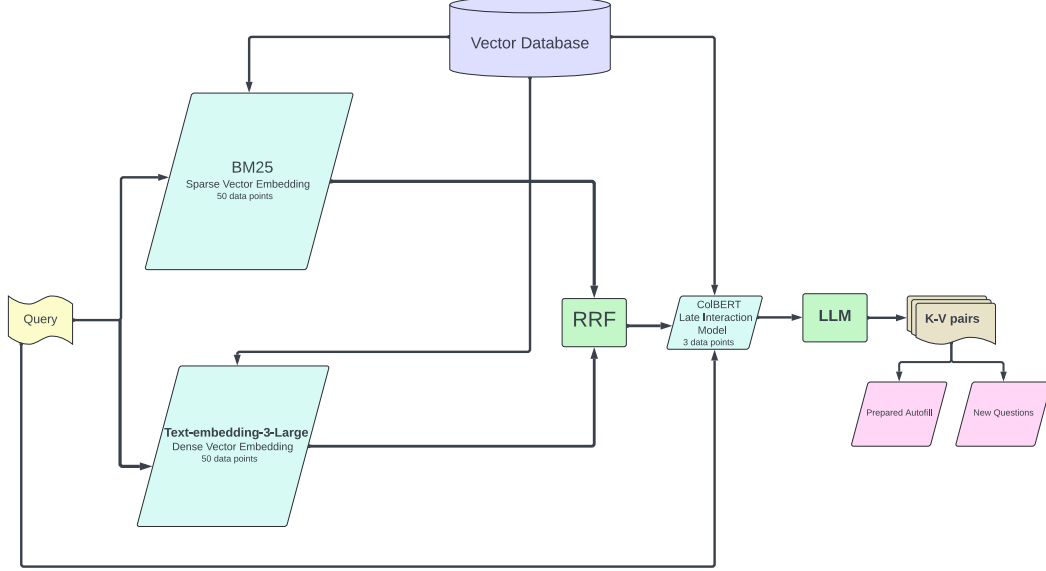


Figure 2: Query-serving pipeline

We developed an interactive application for testing the effectiveness of memory-based task assistance. This application leverages the cache mechanism described, where similar task histories are fetched based on semantic relevance and recency.

Figure 3b demonstrates the autofill feature, where user inputs such as shoe size and preferred brand are pre-populated based on previous queries. This feature reduces user effort in filling in redundant information, thus improving the overall user experience.

The purpose of integrating this cache simulation was to reduce the time and cognitive load required for users to perform similar tasks. In tasks where autofill is enabled, users can immediately confirm pre-filled fields, expediting the task completion process.

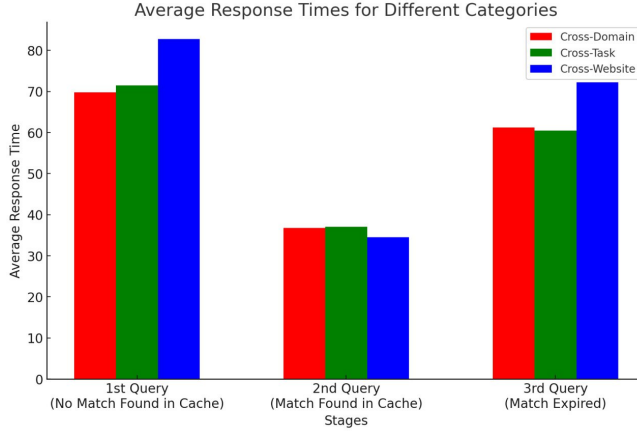
6.1. Study Setup

We assessed the time-saving benefits of our memory-based task assistant. The study evaluated the time required for users to complete tasks under three different scenarios: (1) cross-domain, (2) cross-task, and (3) cross-website interactions.

During the study, the user had to converse with an *assistant* to query three randomly chosen tasks from Mind2Web [3]. The procedure was as follows:

1. **First Query (No match found in cache):** Participants picked a task from the Mind2Web dataset and performed it without any cache assistance.
2. **Second Query (Match found in cache):** Participants performed a similar task with the aid of the caching system, which utilized previously stored information to enhance task performance.
3. **Third Query (Match expired):** The cache was expired, and participants attempted to perform the task again to measure performance without the benefits of caching.

After each round of query, users were asked to answer the following questions. We adopted a modified version of NASA-TLX [33] questionnaire to understand the workload in each query:



(a) Average response times (in seconds) for different task categories across three stages: Initial stage, With Cache, and Cache Invalidation.



(b) Autofill feature in action. Certain fields, such as shoe size and color, are auto-filled based on previous task history.

Figure 3: Average response time with & without successful MCB entry retrieval (a) & demo of the Autofill feature (b).

- How hard did you have to work to accomplish your level of performance before caching?
- How hard did you have to work to accomplish your level of performance after caching?
- How relevant were the auto-filled entries to your current goal?
- Do you prefer auto-filling the entries rather than entering the values yourself?
- How successful were you in accomplishing what you were asked to do with caching?
- Does setting the threshold and asking the questions again from scratch support your dynamic preference?

As shown in Figure 3a, the average response times demonstrate that enabling cache significantly reduces the time needed to complete tasks across all three categories. In the initial stage, without any cache, response times are considerably higher. After cache expires, the system performance returns to near-initial stage levels, but the reduction in time during cache-enabled stages shows the advantage of employing memory-based mechanisms in task repetition scenarios.

The graph highlights that the cross-website category exhibits the most substantial improvement, suggesting that tasks involving different websites but similar contexts benefit the most from cache-assisted processing.

In addition to the tasks associated with the caching mechanism, participants were asked to respond to various questions regarding their experience. While the focus here is on the responses to specific features, other questions were also part of the study to gain a comprehensive understanding of the system's impact.

6.2. Results

Figure 4 graph illustrates participants' responses to the various features assessed in the study. The responses are categorized based on their experience during the three stages of the experiment and are presented on a scale from 1-5 (very low to very high). We can see that workload significantly reduced when a matching entries were found in the cache, denoting the effectiveness of our mechanism.

7. Discussion

7.1. MemAgent for RAG

MemAgent's modular components allow integration with the RAG framework [34]. MCB can be stored and queried from a vector database. Moreover, the alignment models, finetuned with a prefilled memory

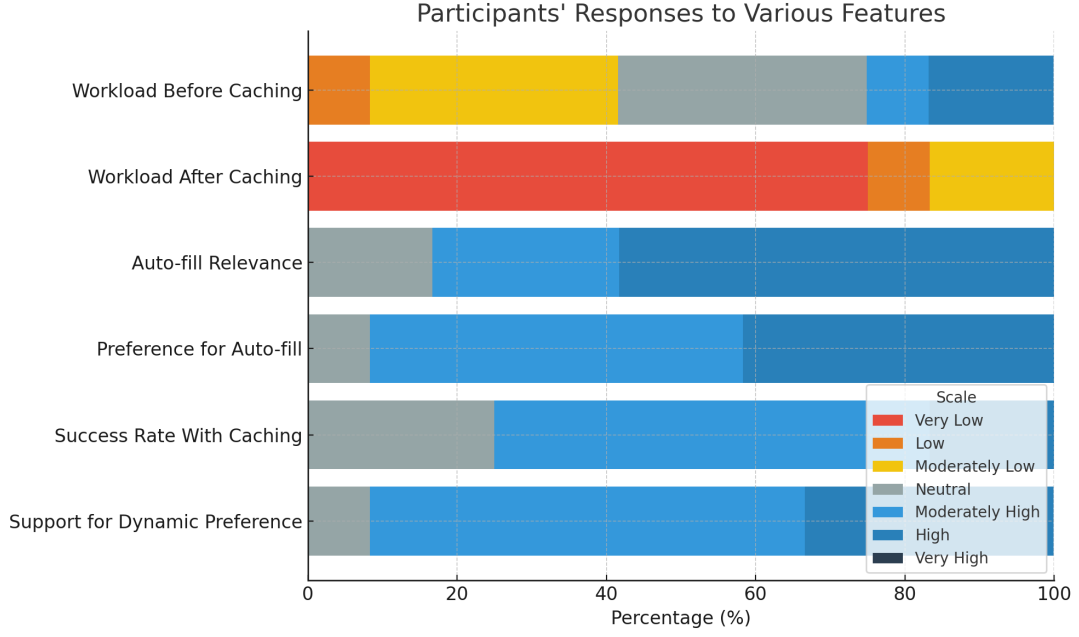


Figure 4: Participants’ responses to various features in the caching experiment.

bank, ask questions only when information is missing. We perform an additional analysis with prefilled MCB, reporting the ratio of conversations to MCB entries (Figure 5). As anticipated, the alignment model asked fewer questions when the MCB contained more information.

7.2. MemAgent for dynamic preference modeling

Current agents struggle with handling user preferences effectively [2]. Although memory-augmented agents show promises in storing information [8], the transformation of memory remains complex. In contrast, our MCB is straightforward yet powerful, to store user preferences for a defined period before automatic removal. This enables MemAgent to *dynamically* model user preferences.

7.3. MemAgent for generalistic web modeling

MemAgent’s information is generalizable across websites. For example, to book a flight, we always need to know the time, departure and arrival location no matter which booking website we are using. Since our MCB only stores I_q for each T_a and is independent of the website, it can reuse the task information across websites with similar usecases.

7.4. Effectiveness of Temporal Decoupling

We observe that the separation of alignment and execution phases provides several benefits:

7.4.1. Cognitive Load Distribution

Our pilot study reveals that by front-loading the information gathering process, users can focus entirely on providing accurate information without the distraction of watching the agent attempt (and potentially fail) at task execution. Prioritizing task information retrieval naturally maximizes time efficiency for users as well (58% reduction in user response time).

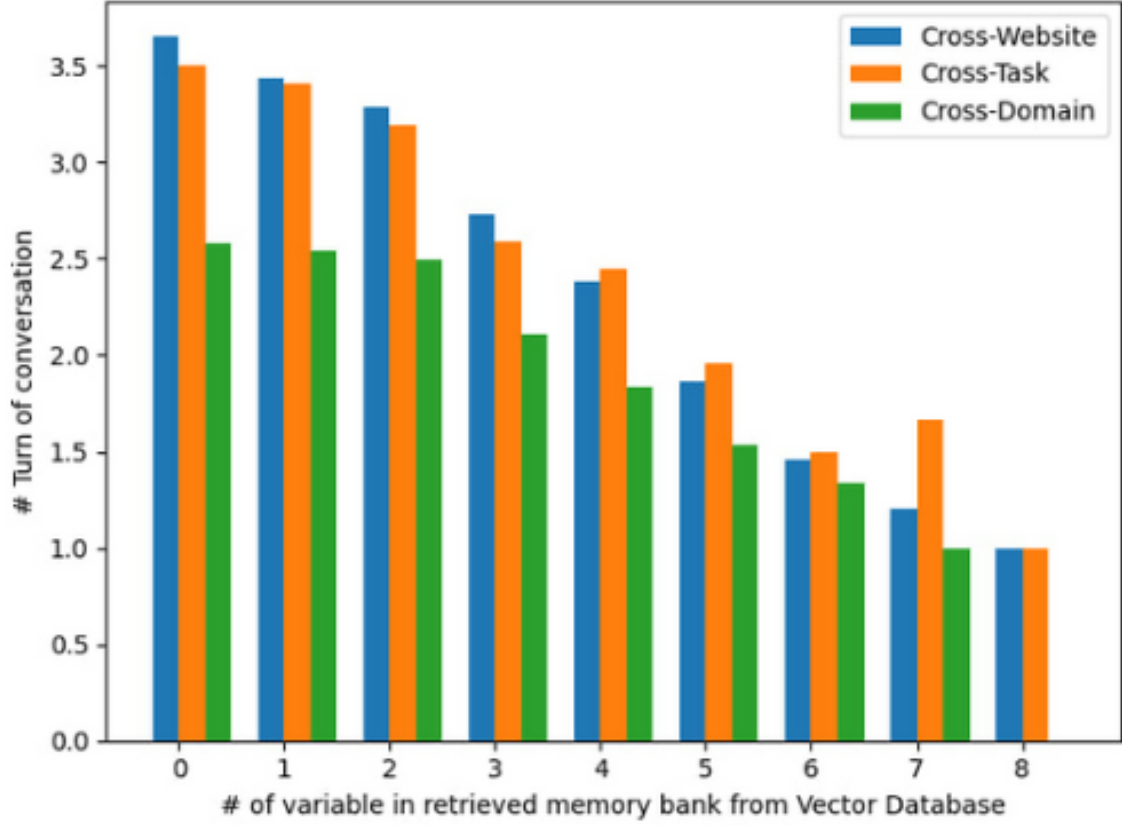


Figure 5: Statistics showing the average count of conversation turn concerning information present in the retrieved MCB. With more information present in the MCB, the conversation turn is significantly reduced without sacrificing the task completion accuracy.

7.4.2. Learning Efficiency

The alignment model learns a more focused objective—asking relevant questions—rather than the complex joint objective of conversation and action prediction. This specialization leads to more targeted and efficient conversations (up to 22.4% conversation turn reductions).

8. Conclusion

In this paper, we presented MemAgent, a novel pipeline designed to address the limitations of LLM web agents, particularly the misalignment between user expectations and the agent’s actions. By incorporating MCB, MemAgent effectively stores task-specific information, allowing it to proactively query for supplementary context. This approach reduces user interaction overhead and enhances task completion success. Our evaluations demonstrate significant improvements in both performance and usability of the agent, indicating that MemAgent is a promising step towards seamless integration of LLMs in web agent technologies.

Limitation

MemAgent has been tested on Mind2Web, which is a static dataset. There might be additional challenges when MemAgent is deployed in an interactive web environment, which is beyond the current scope. Currently, MemAgent supports the creation of one MCB per task. In cases where users might want to utilize multiple MCBs, it may not support well. For example, a user wants to concurrently book flights from New York - Florida and Chicago - Pennsylvania. MemAgent may not be able to store both of these

at the same time.

Acknowledgments

We would like to extend our gratitude to Faria Huq, PhD student at Carnegie Mellon University, for her contributions to this research project. Her consultation and guidance refined the depth of our methodology and the scope of our investigation. Additionally, her assistance in reviewing the manuscript has been pivotal in shaping the overall quality of this work.

Declaration on Generative AI

The authors utilized third-party writing assistants (ChatGPT, Gemini, Grammarly) to refine the manuscript. This usage was limited to improving the presentation and readability of the work and did not involve these tools in any intellectual or creative capacity [35]. The intellectual contributions and research content remain solely the product of the authors' efforts.

References

- [1] Z. Xi, W. Chen, X. Guo, W. He, Y. Ding, B. Hong, M. Zhang, J. Wang, S. Jin, E. Zhou, R. Zheng, X. Fan, X. Wang, L. Xiong, Y. Zhou, W. Wang, C. Jiang, Y. Zou, X. Liu, Z. Yin, S. Dou, R. Weng, W. Cheng, Q. Zhang, W. Qin, Y. Zheng, X. Qiu, X. Huang, T. Gui, The rise and potential of large language model based agents: A survey, 2023. [arXiv:2309.07864](#).
- [2] S. Zhou, F. F. Xu, H. Zhu, X. Zhou, R. Lo, A. Sridhar, X. Cheng, Y. Bisk, D. Fried, U. Alon, et al., Webarena: A realistic web environment for building autonomous agents, [arXiv preprint arXiv:2307.13854](#) (2023).
- [3] X. Deng, Y. Gu, B. Zheng, S. Chen, S. Stevens, B. Wang, H. Sun, Y. Su, Mind2web: Towards a generalist agent for the web, [arXiv preprint arXiv:2306.06070](#) (2023).
- [4] B. Wang, G. Li, Y. Li, Enabling conversational interaction with mobile ui using large language models, in: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI '23, Association for Computing Machinery, New York, NY, USA, 2023. URL: <https://doi.org/10.1145/3544548.3580895>. doi:10.1145/3544548.3580895.
- [5] S. Yao, H. Chen, J. Yang, K. Narasimhan, Webshop: Towards scalable real-world web interaction with grounded language agents, 2023. [arXiv:2207.01206](#).
- [6] J. Zamfirescu-Pereira, R. Y. Wong, B. Hartmann, Q. Yang, Why johnny can't prompt: how non-ai experts try (and fail) to design llm prompts, in: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 2023, pp. 1–21.
- [7] T. S. Kim, D. Choi, Y. Choi, J. Kim, Stylette: Styling the web with natural language, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22, Association for Computing Machinery, New York, NY, USA, 2022. URL: <https://doi.org/10.1145/3491102.3501931>. doi:10.1145/3491102.3501931.
- [8] C. Packer, S. Wooders, K. Lin, V. Fang, S. G. Patil, I. Stoica, J. E. Gonzalez, Memgpt: Towards llms as operating systems, 2024. [arXiv:2310.08560](#).
- [9] X. H. Lù, Z. Kasner, S. Reddy, Weblinx: Real-world website navigation with multi-turn dialogue, [arXiv preprint arXiv:2402.05930](#) (2024).
- [10] T. R. Sumers, S. Yao, K. Narasimhan, T. L. Griffiths, Cognitive architectures for language agents, 2023. [arXiv:2309.02427](#).
- [11] H. Wen, Y. Li, G. Liu, S. Zhao, T. Yu, T. J.-J. Li, S. Jiang, Y. Liu, Y. Zhang, Y. Liu, Empowering llm to use smartphone for intelligent task automation, 2023. [arXiv:2308.15272](#).
- [12] Z. Zhang, A. Zhang, You only look at screens: Multimodal chain-of-action agents, 2023. [arXiv:2309.11436](#).

- [13] T. Shi, A. Karpathy, L. Fan, J. Hernandez, P. Liang, World of bits: An open-domain platform for web-based agents, in: International Conference on Machine Learning, PMLR, 2017, pp. 3135–3144.
- [14] R. Kapoor, Y. P. Butala, M. Russak, J. Y. Koh, K. Kamble, W. Alshikh, R. Salakhutdinov, Omniact: A dataset and benchmark for enabling multimodal generalist autonomous agents for desktop and web, arXiv preprint arXiv:2402.17553 (2024).
- [15] B. Zheng, B. Gou, J. Kil, H. Sun, Y. Su, Gpt-4v(ision) is a generalist web agent, if grounded, in: Forty-first International Conference on Machine Learning, 2024. URL: <https://openreview.net/forum?id=piecKJ2DlB>.
- [16] J. Y. Koh, R. Lo, L. Jang, V. Duvvur, M. C. Lim, P.-Y. Huang, G. Neubig, S. Zhou, R. Salakhutdinov, D. Fried, Visualwebarena: Evaluating multimodal agents on realistic visual web tasks, ACL (2024).
- [17] H. He, W. Yao, K. Ma, W. Yu, Y. Dai, H. Zhang, Z. Lan, D. Yu, Webvoyager: Building an end-to-end web agent with large multimodal models, arXiv preprint arXiv:2401.13919 (2024).
- [18] J. Yang, H. Zhang, F. Li, X. Zou, C. Li, J. Gao, Set-of-mark prompting unleashes extraordinary visual grounding in gpt-4v, arXiv preprint arXiv:2310.11441 (2023).
- [19] Y. Deng, X. Zhang, W. Zhang, Y. Yuan, S.-K. Ng, T.-S. Chua, On the multi-turn instruction following for conversational web agents, in: L.-W. Ku, A. Martins, V. Srikumar (Eds.), Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), Association for Computational Linguistics, Bangkok, Thailand, 2024, pp. 8795–8812. URL: <https://aclanthology.org/2024.acl-long.477>.
- [20] Z. Zhang, X. Bo, C. Ma, R. Li, X. Chen, Q. Dai, J. Zhu, Z. Dong, J.-R. Wen, A survey on the memory mechanism of large language model based agents, 2024. arXiv:2404.13501.
- [21] A. Modarressi, A. Imani, M. Fayyaz, H. Schütze, Ret-llm: Towards a general read-write memory for large language models, 2023. arXiv:2305.14322.
- [22] W. Zhong, L. Guo, Q. Gao, H. Ye, Y. Wang, Memorybank: Enhancing large language models with long-term memory, 2023. arXiv:2305.10250.
- [23] H. Weld, X. Huang, S. Long, J. Poon, S. C. Han, A survey of joint intent detection and slot filling models in natural language understanding, ACM Computing Surveys 55 (2022) 1–38.
- [24] A. Madaan, N. Tandon, P. Gupta, S. Hallinan, L. Gao, S. Wiegrefe, U. Alon, N. Dziri, S. Prabhumoye, Y. Yang, et al., Self-refine: Iterative refinement with self-feedback, Advances in Neural Information Processing Systems 36 (2024).
- [25] L. Zheng, W.-L. Chiang, Y. Sheng, S. Zhuang, Z. Wu, Y. Zhuang, Z. Lin, Z. Li, D. Li, E. Xing, et al., Judging llm-as-a-judge with mt-bench and chatbot arena, arXiv preprint arXiv:2306.05685 (2023).
- [26] J. Wei, X. Wang, D. Schuurmans, M. Bosma, F. Xia, E. Chi, Q. V. Le, D. Zhou, et al., Chain-of-thought prompting elicits reasoning in large language models, Advances in neural information processing systems 35 (2022) 24824–24837.
- [27] S. Yao, J. Zhao, D. Yu, N. Du, I. Shafran, K. Narasimhan, Y. Cao, React: Synergizing reasoning and acting in language models, 2023. arXiv:2210.03629.
- [28] T. Zhang, V. Kishore, F. Wu, K. Q. Weinberger, Y. Artzi, Bertscore: Evaluating text generation with bert, arXiv preprint arXiv:1904.09675 (2019).
- [29] K. Papineni, S. Roukos, T. Ward, W.-J. Zhu, Bleu: a method for automatic evaluation of machine translation, in: P. Isabelle, E. Charniak, D. Lin (Eds.), Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics, Association for Computational Linguistics, Philadelphia, Pennsylvania, USA, 2002, pp. 311–318. URL: <https://aclanthology.org/P02-1040>. doi:10.3115/1073083.1073135.
- [30] S. Robertson, H. Zaragoza, The probabilistic relevance framework: Bm25 and beyond, in: Foundations and Trends in Information Retrieval, volume 3, Now Publishers Inc, 2009, pp. 333–389.
- [31] OpenAI, Openai text embedding models, 2023. <https://platform.openai.com/docs/guides/embeddings>.
- [32] O. Khattab, M. Zaharia, Colbert: Efficient and effective passage search via contextualized late interaction over bert, in: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20), ACM, 2020, pp. 39–48.
- [33] S. G. Hart, Nasa-task load index (nasa-tlx); 20 years later, in: Proceedings of the human factors

and ergonomics society annual meeting, volume 50, Sage publications Sage CA: Los Angeles, CA, 2006, pp. 904–908.

- [34] P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, H. Küttler, M. Lewis, W.-t. Yih, T. Rocktäschel, et al., Retrieval-augmented generation for knowledge-intensive nlp tasks, *Advances in Neural Information Processing Systems* 33 (2020) 9459–9474.
- [35] E. Nakazawa, M. Udagawa, A. Akabayashi, Does the use of ai to create academic research papers undermine researcher originality?, *AI* 3 (2022) 702–706.

A. Appendix

A.1. Prompts used for various LLM calls

This section includes some additional figures that provide visual insight into the discussed topics. Figure 6 shows the self-refining prompt for generating the dataset. Figure 7 shows the constructed task description. Figure 8-11 shows prompts used for 2-shot prompting in GPT-4o and Gemini-pro evaluations. Figure 12 shows the prompt used for the GPT-4o/Gemini-pro execution.

```
User wants to generate conversation data, (where <abs> includes the input task description and a consecutive list of
question (Q), answer (A), and memory (mem) tuple) for input task description.
However, the conversation data collected is not always clean. Your task is to filter out repetitive tuples that are
already present in <abs>.
Follow these guidelines:
1. If a question is already answered in the <abs>, discard it.
2. Rate the quality from 1-5 (1: bad, 5: good) for conciseness (whether it includes repetitive conversation),
usefulness (whether it includes useful questions), and verbosity (whether it asks the question with less verbosity.)
3. Do NOT delete any information that was present in the original description but not in <abs>.
4. If the data looks good to you, you can just reply noop.

Here is an example:
Original Description: Find a latest post with more than 10k upvotes in r/announcements community and upvote it.

Input:
<Abs> Upvote latest post with high engagement </Abs>
<Questions>
<Q> Which community's latest post should be searched for? </Q>
<A> r/announcements </A>
<mem> Target Community: r/announcements </mem>
<Q> What is the minimum number of upvotes required for the post to be considered? </Q>
<A> More than 10,000 upvotes </A>
<mem> Minimum Upvotes Required: More than 10,000 </mem>
<Q> What action should be taken once a suitable post is found? </Q>
<A> Upvote it </A>
<mem> Action to Take: Upvote the post </mem>
</Questions>

Thought: The abstract description already mentioned that the task is to upvote a post which is repeated in the
last question. So, I will discard the last question.

Rate:
conciseness: 3 (the last question is repetitive),
usefulness: 4 (count of upvotes is not a mandatory parameter, the rest are good),
verbosity: 2 (questions are too lengthy)

Output: <Abs> Upvote latest post with high engagement </Abs>
<Questions>
<Q> Which community's post? </Q>
<A> r/announcements </A>
<mem> Target Community: r/announcements </mem>
<Q> Minimum number of upvotes to be considered? </Q>
<A> More than 10,000 upvotes </A>
<mem> Minimum Upvotes Required: More than 10,000 </mem>
</Questions>

Now reply with your thought, rate, and output for the following.
Original Description: {tsk}
Input: {prompt}
Thought:
```

Figure 6: Self-Refine prompt used during data generation


```

<Abs> Book winery tour </Abs>
<Questions>
  <Q> What is the destination for the winery tour? </Q>
  <A> Napa Valley </A>
  <mem> Tour Destination: Napa Valley </mem>

  <Q> What type of cuisine should the winery serve? </Q>
  <A> Mediterranean cuisine </A>
  <mem> Cuisine Type: Mediterranean cuisine </mem>

  <Q> Does the tour include wine tasting? </Q>
  <A> Yes, it includes wine tasting. </A>
  <mem> Wine Tasting: Included </mem>

  <Q> How many guests will be attending the winery tour? </Q>
  <A> 4 guests </A>
  <mem> Number of Guests: 4 guests </mem>

  <Q> What is the date and time for the winery tour booking? </Q>
  <A> April 15, at 10 am. </A>
  <mem> Tour Date and Time: April 15, at 10 am. </mem>

  <Q> What type of setting is requested for the tour? </Q>
  <A> Outdoor setup. </A>
  <mem> Setup Preference: Outdoor setup. </mem>

</Questions>

```

Figure 7: Example of constructed task description

Given an initial task description, your task is to ask follow-up questions and parse the user's response. Only ask one question at a time. If you are done, reply with <Finish>. Please reply only with the question.

First Example:

User: Book me a flight

Agent: Where are you going?

Second Example:

User: Subscribe to newsletter

Agent: newsletter name to subscribe to?

User: Daily Fitness Tips

Agent: What email address should be used?

User: john.fitnessfan@example.com

Agent: <Finish>

Now complete the following task:

Figure 8: Prompt without MCB (Alignment)

Given an initial task description, your task is to ask follow-up questions and parse the use's response for answer type and value to be stored into <mem>type: value</mem>. Only ask one question at a time. If you are done, reply with <Finish>. Please reply only with the question and <mem> if any.

First Example:

User: Book me a flight

Agent: Where are you going?

Second Example:

User: Subscribe to newsletter

Agent: newsletter name to subscribe to?

User: Daily Fitness Tips

Agent: <mem> Newsletter Name: Daily Fitness Tips </mem> What email address should be used?

User: john.fitnessfan@example.com

Agent: <mem> Email Address: john.fitnessfan@example.com </mem><Finish>

Now complete the following task:

Figure 9: LLM + MCB prompt (alignment)

Given an initial task description, your task is to ask follow-up questions and parse the user's response for answer type and value to be stored into `<mem>type: value</mem>`. Only ask one question at a time. If you are done, reply with `<Finish>`. Please include your question in `<Q>` tag and parsed answer in `<mem>` tag.

First Example:

User: Book me a flight.

Agent: Let's think step by step. To book a flight, we need to know the departure, arrival location, and time. I will first ask about the departure location. `<Q>Where are you going? <Q>`

Second Example:

User: Subscribe to newsletter.

Agent: Let's think step by step. To subscribe, I need to know the newsletter name first. `<Q>What is the newsletter name to subscribe to?</Q>`

User: Daily Fitness Tips.

Agent: Let's think step by step. I will put the user response into the mem bank as a newsletter name. I also need to ask about their email address. `<mem> Newsletter Name: Daily Fitness Tips </mem> <Q>What email address should be used? </Q>`

User: john.fitnessfan@example.com.

Agent: Let's think step by step. Since all the information is already asked, I will finish now and store the email address from the last reply. `<mem>Email Address: john.fitnessfan@example.com </mem><Finish>`

Now complete the following task:

Figure 10: LLM + CoT+ MCB prompt (Alignment)

Given an initial task description, your task is to ask follow-up questions and parse the user's response for answer type and value to be stored into `<mem>type: value</mem>`. Only ask one question at a time and include your thought and action. If you are done, reply with `<Finish>`. Please include your question in `<Q>` tag and parsed answer in `<mem>` tag.

First Example:

User: Book me a flight

Agent: Thought: To book a flight, we need to know the departure, arrival location, and time. I will first ask about the departure location. Action: `<Q> Where are you going? <Q>`

Second Example:

User: Subscribe to newsletter

Agent: Thought: To subscribe, I need to know the newsletter name first. Action: `<Q> Newsletter name to subscribe to? </Q>`

User: Daily Fitness Tips

Agent: Thought: I will put the user response into the mem bank as a newsletter name. I also need to ask about their email address. Action: `<mem> Newsletter Name: Daily Fitness Tips </mem> <Q> What email address should be used? </Q>`

User: john.fitnessfan@example.com

Agent: Thought: Since all the information is already asked, I will finish now and store the email address from the last reply. Action: `<mem> Email Address: john.fitnessfan@example.com </mem><Finish>`

Now complete the following task:

Figure 11: LLM + ReACT + MCB prompt (alignment)

Role: System
Content: You are a helpful assistant that is great at website design, navigation, and executing tasks for the user.

Role: User
Content:
'''
<html> <div> <div> <a tock home page /> ... Explore now </div> </div> </div> </html>
'''

Based on the HTML webpage above, try to complete the following task:
Task: Check restaurant availability for pickup. City: Boston, NY, Date and Time: March 18, 5pm, Number of Guests: 1
Previous actions:
None
What should be the next action? Please select from the following choices (If the correct action is not in the page above, please select A. 'None of the above'):

A. None of the above
B. <button id=0 book a reservation. toggle open> Book a
C. <select id=1 type> <option reservations true> Dine in </option> <option
D. <div id=2> <p> Celebrating and supporting leading women shaking up

Role: Assistant
Content:
Answer: C.
Action: SELECT
Value: Pickup

Role: User
Content:
'''
<html> <div> <main main> <section tabpanel> ... </div> </footer> </div> ... </html>
'''

Based on the HTML webpage above, try to complete the following task:
Task: Compare fare types for booking a train ticket. Departure Location: Springfield, IL, Arrival Location: Austin, TX, Travel Date: April 29th, 2023, Number of Adults: 1
Previous actions:
[combobox] Enter your departing city, airport name, or airpor... -> TYPE: SPRINGFIELD
[button] Springfield, IL, US (SPI) -> CLICK
[combobox] Enter your destination city, airport name, or airp... -> TYPE: AUSTIN
[button] Austin, TX, US (AUS) -> CLICK
What should be the next action? Please select from the following choices (If the correct action is not in the page above, please select A. 'None of the above'):

A. None of the above
B. <li id=0 tab heading level 3 search and> Hotel
C. <div id=1> <div> Dates* <button button clear dates
D. <ul id=2> <a mobile tools> <a open united's tiktok

Role: Assistant
Content:
Answer: A.

Role: User
Content:
'''
<html> <div> <nav main menu> <div button> Car Sales </div> ... </html>
'''

Based on the HTML webpage above, try to complete the following task:
Task: Find a rental vehicle. Vehicle Type: Mini van, Rental Location: Brooklyn City, Rental Start Date: April 5th, Rental End Date: April 8th, Renter's Age: 22 years old
Previous actions:
[searchbox] Pick-up & Return Location (ZIP, City or Airport) (... -> TYPE: Brooklyn
[option] Brooklyn, NY, US Select -> CLICK
What should be the next action? Please select from the following choices (If the correct action is not in the page above, please select A. 'None of the above'):

A. None of the above
B. <div id=0> <div> <div> <div> Buy A Car </div> <div>
C. <div id=1> Enterprise Fleet Management </div>
D. <button id=2 selected pick-up date 03/19/2023> 19

Role: Assistant
Content:
Answer: D.
Action: CLICK

Figure 12: Prompt GPT-4o (Execution). The HTML part of the prompt is shortened here

Task: Open the most helpful 5 star reviews of Alpine Ridge
Q: Which product or service are the reviews for?
A: Alpine Ridge

Q: Would you like to see the most recent reviews or the top-rated ones?
A: Not specified

Q: Which platform would you like to open the reviews on? (e.g., Amazon, Yelp, Google Reviews)
A: Not specified

Q: Could you please provide more details or specify the context in which these 5-star reviews should be opened?
A: Not specified

Q: Are you looking to open the 5-star reviews for a particular purpose, such as market research, customer feedback, or for promotional use?
A: Not specified

Q: Can you specify whether you have a particular browser or tool that you would like to use to open the reviews?
A: Not specified

Q: Could you please clarify whether you need assistance finding these reviews, or do you already have a source and just need them opened?
A: Not specified

Q: Do you have any specific requirements or preferences regarding the format in which the reviews should be opened, such as a document, spreadsheet, or web page?
A: Not specified

Q: Are you looking for reviews in a specific language or region?
A: Not specified

Q: Is there a specific date range for the reviews you are interested in?
A: Not specified

Figure 13: Example of repetitive questions in Gemini-Pro baseline prompting.