### **000 001 002 003** CONTEXTUAL EXPERIENCE REPLAY FOR CONTINUAL LEARNING OF LANGUAGE AGENTS

Anonymous authors

Paper under double-blind review

# ABSTRACT

Large language model (LLM) agents have been applied to sequential decisionmaking tasks such as web navigation, but without any environment-specific experiences, they often fail in these complex tasks. Moreover, current LLM agents are not designed to continually learn from past experiences during inference time, which could be crucial for them to gain these environment-specific experiences. To address this, we propose Contextual Experience Replay (CER), a training-free framework to enable efficient continual learning for language agents in their context window. Specifically, CER accumulates and synthesizes past experiences into a dynamic memory buffer. These experiences encompass environment dynamics and common decision-making patterns, allowing the agents to retrieve and augment themselves with relevant knowledge in new tasks, enhancing their adaptability in complex environments. We evaluate CER on the challenging WEBARENA and VISUALWEBARENA benchmarks. On VISUALWEBARENA, CER surpasses the tree search method with much fewer token costs and achieves state-of-the-art performance of 31.9%. On WEBARENA, CER also gets a competitive average success rate of 33.16%, relatively improving the success rate of the GPT-4o agent baseline by 36.6%. We also show that CER can work even better if provided with a few annotated trajectories or combined with other methods, demonstrating its potential.

**032**

### 1 INTRODUCTION

**033 034 035 036 037 038 039 040 041 042 043 044** Building an autonomous agent that can help with people's daily tasks has been a long-standing goal of artificial intelligence research [\(Russell & Norvig, 1995;](#page-11-0) [Franklin & Graesser, 1996\)](#page-10-0). Recently, large language models [\(Achiam et al., 2023;](#page-10-1) [Anthropic, 2024;](#page-10-2) [Gemini Team, 2023\)](#page-10-3) have shown impressive performance in text [\(Hendrycks et al., 2021\)](#page-10-4) and code generation [\(Chen et al., 2021;](#page-10-5) [Xie](#page-11-1) [et al., 2024b\)](#page-11-1), reasoning [\(Wei et al., 2022;](#page-11-2) [Yao et al., 2023a\)](#page-12-0), and decision-making tasks [\(Yao et al.,](#page-12-1) [2023b;](#page-12-1) [Zhou et al., 2024a;](#page-12-2) [Xu et al., 2023;](#page-11-3) [Xie et al., 2024c\)](#page-11-4), which paves the way for building an agent to automate computer tasks. Web tasks, specifically, are a representative task type in computer tasks, which is more controllable than the OS environment [\(Xie et al., 2024a\)](#page-11-5) and more complex than the mobile environment [\(Rawles et al., 2023;](#page-11-6) [2024\)](#page-11-7). On two realistic web navigation benchmarks, WEBARENA [\(Zhou et al., 2024b\)](#page-12-3) and VISUALWEBARENA [\(Koh et al., 2024a\)](#page-10-6), humans can achieve success rates of 78.24% and 88.70%, correspondingly. However, the current methods, with the most frontier models, can only achieve a success rate of around or less 20% without human involvement.

**045 046 047 048 049** One important reason is the lack of prior knowledge of each environment, which is critical for such difficult multi-step task solving in the complex web environment. While training in each specific environment is costly, current language agents seldom have an efficient way to continually learn about the environment, so they need to explore the environment from scratch for every single task [\(Koh et al., 2024b\)](#page-10-7).

**050 051 052 053** In this work, we propose Contextual Experience Replay (CER), a novel and effective framework to enable the continual learning of language agents in complex environments. CER is loosely inspired by experience replay [\(Schaul et al., 2016;](#page-11-8) [Rolnick et al., 2019\)](#page-11-9), an important algorithm in reinforcement learning which highlights storing past trajectories into a buffer and training the agent with these data.

<span id="page-1-0"></span>

Figure 1: Overview of Contextual Experience Replay including offline and online settings. (1) In the online setting, it will start from stage C and loop between stage C and  $\bf{B}$  for each task, i.e. solve task i, learn experiences from it and solve task  $i + 1$  with previous experiences, and so on. (2) In the offline setting, stage A is needed to get offline trajectories, then it goes from stage B to C and finally stays in stage  $\mathbb C$ , i.e., learns experiences from offline trajectories and solves all tasks. (3) In the hybrid setting, it will begin from stage A and loop between B and  $\mathbb C$ , conducting both offline and online learning.

**080 081 082 083 084 085 086 087 088 089 090 091 092** Our approach allows agents to distill experience from trajectories, including environment dynamics and common decision-making patterns, from past trajectories, store them into a dynamic memory, retrieve them with the current task, and replay them in context when solving new tasks. Fig[.1](#page-1-0) shows how CER works under different settings. Online, offline, and hybrid settings are divided by the source of trajectories, i.e., the time to get the trajectories. As in Fig[.1,](#page-1-0) in the online setting, the agent will start from the inference stage (C) without any experience. After completing a task, CER gets the (online) trajectory from it, distills experiences from the trajectories, and merges it into the buffer. During the inference of the next task, the agent will be augmented with retrieved helpful experiences and so on. In the offline setting, a set of trajectories will be collected in advance (stage A), distilled into experiences, and stored. Then, the agent will solve tasks on the test set with retrieved experience from the fixed buffer. The hybrid setting is the combination of these two, i.e., going through the offline learning stage before online learning. Fig. [2](#page-2-0) also shows how the experience is utilized by the agent with an example.

- **093 094 095 096 097 098 099** We evaluated CER on two realistic web benchmarks WEBARENA [\(Zhou et al., 2024b\)](#page-12-3) and VISUAL-WEBARENA [\(Koh et al., 2024a\)](#page-10-6). CER improves the GPT-4o baseline by a large margin and achieves competitive results on these two benchmarks while orthogonal with most other methods. On WE-BARENA, CER shows a relative improvement of 33.7% over the GPT-4o baseline and achieves an overall success rate of 33.2%, competitive with other state-of-the-art (SOTA) methods. On VISU-ALWEBARENA, CER outperforms the tree search-based method by 20.8% in relative performance with dozens of times fewer token costs and achieves a SOTA success rate of 31.9%.
- **100 101 102 103 104** CER learns experience in an online style on WEBARENA [\(Zhou et al., 2024b\)](#page-12-3) and VISUALWE-BARENA [\(Koh et al., 2024a\)](#page-10-6) for lack of training set and fair comparison. We also did an extensive analysis to extend CER to offline and offline and online hybrid settings ([§5.1\)](#page-6-0). We found CER works well with the offline data provided. It can even improve further with a limited number of human-annotated trajectories to warm up before online learning.
- **105 106 107** We further investigate the improvements of CER with various metrics, such as cross-template success rate, stability (preservation of old knowledge), and plasticity (acquisition of new knowledge) [\(Grossberg, 1982;](#page-10-8) [Rolnick et al., 2019\)](#page-11-9) ([§5.2,](#page-7-0) [§5.3\)](#page-7-1), demonstrating its generalizability and effectiveness as a continual learning system. Also, we show that through the combination with a sampling-

<span id="page-2-0"></span>

**162 163 164 165 166 167 168 169 170 171 172 173** Web Agent Environments LLM agents are increasingly being employed to perform various digital tasks on behalf of humans, with interacting with websites being a common application area supported by numerous benchmarks. For instance, WebShop [\(Yao et al., 2022\)](#page-12-4) tasks agents with identifying products that meet specific user requirements by interacting with e-commerce platforms. Extensions such as WebArena [\(Zhou et al., 2024b\)](#page-12-3) and Mind2Web [\(Deng et al., 2023\)](#page-10-10) have broadened the scope of tasks to include a wider variety of websites and more realistic applications, encompassing activities like trip booking, information retrieval, website navigation, and social media management. VisualWebArena [\(Koh et al., 2024a\)](#page-10-6) designs challenging multimodal web navigation tasks that require agents to leverage visual grounding and understand image inputs. Among these benchmarks, WebArena and VisualWebArena provide the most realistic, controllable, and interactable environments, which makes the tasks more challenging and the results reproducible. The interactive characteristics are also beneficial for our continual learning paradigm.

**174 175 176 177 178** Learning from Memory or Past Experiences Some previous works have investigated the storage of memories of past agent trajectories. Generative agents [\(Park et al., 2023\)](#page-10-11) use similar strategies to investigate human behaviors with such a human-like strategy. Voyager [\(Wang et al., 2024a\)](#page-11-11) enables the agent to learn diverse skills in Minecraft.

**179 180 181 182 183 184 185 186 187 188 189 190 191 192** Similarly, frameworks such as ExpeL [\(Zhao et al., 2023\)](#page-12-5) and Synapse [\(Zheng et al., 2023\)](#page-12-6) leverage stored past task trajectories as memory, which are dynamically retrieved to support task execution. However, they either test on relatively simple web environments [\(Yao et al., 2022\)](#page-12-4) or use raw and long observation-action pairs as exemplars directly, which limits their applicability to more complex environments. In a concurrent work Agent Workflow Memory [\(Wang et al., 2024b\)](#page-11-12), they also propose the idea of summarizing workflows from past trajectories and augmenting the agent with the workflows. However, only successful trajectories are considered. Additionally, they do not have a retrieval module and only have a summarization module that summarizes all past trajectories each time and updates the whole workflow memory in a rewriting style, which hinders the accumulation of experiences and limits the applicability of their method to a more continual paradigm. In our work, we construct a well-designed, efficient, and scalable continual learning framework for autonomous language agents and test it in two challenging and realistic web environments. The experiences contain both environment dynamics and decision-making patterns. We also investigate it both qualitatively and quantitatively and demonstrate its advantage in terms of applicability in different learning paradigms and compatibility with other agent methods.

- **193**
- **194**
- **195**

# 3 CER: CONTEXTUAL EXPERIENCE REPLAY

**196 197 198 199 200 201 202** Consider a general setup for a language agent  $A$ , powered by a language model  $M$  with a context window  $C$ , to solve a sequential decision-making task in an environment. CER include four separate modules: distillation module D, retrieval module R, dynamic experience buffer  $\epsilon$  and the base decision-making agent itself  $A$  as shows in Fig[.1.](#page-1-0) CER can start working given a arbitrary set of trajectories  $\mathbb{T} = \{\tau_1, \tau_2, \ldots, \tau_n\}$ . All modules here are implemented by prompting a visual language model (VLM), i.e. GPT-4o in our implementation. Details of prompts for each module can be found in [A.1.](#page-13-0)

**203 204**

# 3.1 DISTILL EXPERIENCES FROM TRAJECTORIES

**205 206 207 208 209 210 211 212 213 214 215** Given a trajectory set  $\mathbb{T}$ , the distillation module will distill experiences  $\mathbb{E} = \{E_1, E_2, \ldots, E_n\}$  from them one by one where  $E_i = (D_i, S_i)$ .  $D_i$  stands for environment dynamics, or dynamics in short, and  $S_i$  represents useful decision-making patterns, or skills in short. The dynamics provide useful state information to help the agent make state-aware decisions or directly navigate to the state through its URL. These skills provide common decision-making patterns, inspiring agents to take better action. We use two separate modules for the distillation of dynamics and skills due to their different characteristics. The output format is similar to ReAct [\(Yao et al., 2023b\)](#page-12-1), asking the model to issue a think action before outputting each distillation. The dynamics distillation module will distill a list of summaries of different web pages, their corresponding URL, and inferred possible usages. The skill distillation module is instructed to summarize a list of useful skills. Each of them includes a brief overall summary (e.g. Navigate to forum  $\{$  forum name $\}$ ) and the corresponding detailed step-by-step guidelines. Specifically, the guideline contains both natural language summaries and **216 217 218 219 220 221 222** concrete action examples for each step, as the example in Fig[.2.](#page-2-0) While the natural language summaries provide flexible and general high-level instruction, the example helps the agent to understand the step and also format its output better. The model is required to output the final distillation in an abstract and general way, i.e. navigate to forum {forum name} instead of navigate to forum "books", to ensure that the experiences can be broadly applied. The model is also provided with existing experiences in the buffer to avoid repetitive distillation, allowing the continual accumulation of the experiences across time.

**223 224**

**225**

**234 235**

<span id="page-4-0"></span>**242**

**244**

# 3.2 RETRIEVE EXPERIENCES FROM BUFFER

**226 227 228 229 230 231 232 233** After the distillation period, the buffer  $\epsilon$  now includes a set of useful experiences  $\mathbb{E}$  =  $\{E_1, E_2, \ldots, E_n\}$ . Similar to the distillation module, we designed two separate modules to retrieve dynamics and skills correspondingly also using ReAct style output format [\(Yao et al., 2023b\)](#page-12-1), additionally prompting with general instructions, the current task goal, the website descriptions, and all dynamics or skills available in the buffer. Then, the module will retrieve the top- $k$  useful and informative experiences from the buffer by their ids and pass this to the language agent. This module makes it possible for the distillation module to continuously merge new experiences and help the agent filter out useful experiences for the current task.

## 3.3 DECISION-MAKING WITH CONTEXTUAL EXPERIENCE REPLAY

**236 237 238 239 240 241** To best utilize the in-context learning capability of language models, we transform the selected  $k$ experiences  $\mathbb{E} = \{E_1, E_2, \dots, E_k\}$  into natural language experience descriptions  $E_{NL} = f(\mathbb{E})$ through a programmatic mapping f and integrate them into the model's context  $C$ , resulting in a new augmented context  $C' = g(C, E_{NL})$ . Therefore, the decision-making policy underneath will be influenced by the additional experiences, and the agent A can issue better actions with reference to the experiences. The context comparison between the baseline agent and CER is shown in Fig[.2.](#page-2-0)

#### **243** 3.4 COMBINATION OF OFFLINE AND ONLINE LEARNING

**245 246 247 248 249 250 251 252 253** The source of the trajectories to learn from is important for CER. Depending on the source of trajectory data, CER can be divided into offline, online, and hybrid versions. Online data is collected from past task-solving trajectories in the environment during inference time. Specifically, in the online setting, there are no trajectories provided at the very beginning, but as the procedure goes on, there will be self-generated trajectories from past tasks. CER will run the distillation module after each task and run the retrieval and replay module in the next task. Different from an online setting, offline learning means there is a training set of trajectories at the beginning for CER to learn from but no further learning during inference. Additionally, these two settings can be combined to serve as a whole system, i.e., learn from a fixed training set first and then self-evolve in the environment with self-generated data. We investigate the effectiveness of these two settings in the section [5.1.](#page-6-0)

**254 255 256**

# 4 EXPERIMENTS

**257 258 259 260 261 262 263 264 265 266 267 268 269** We evaluate CER on the full set of WEBARENA [\(Zhou et al., 2024b\)](#page-12-3) (WA) and VISUALWEBARENA [\(Koh et al., 2024a\)](#page-10-6) (VWA) in online setting for fairness because training set is not provided in these benchmarks. Also, it would be interesting to see how CER performs without additional external data in a close-loop continual learning paradigm. We did further studies about offline and offline  $+$ online settings in section [5.1.](#page-6-0) The reason we chose these two is that they provide interactive, realistic, and reproducible web environments that are better for applying continual learning and still close to real-world scenarios. WEBARENA have 812 tasks across five different websites corresponding to different domains: shopping, shopping administration, online forum, map, and project collaboration (Gitlab). VISUALWEBARENA retains the shopping and forum website, adds another classifieds website, and designs 910 tasks on top of them. Although they share two websites, the focus of their tasks is different. Most of the tasks in WebArena only have text descriptions of task goals, while a large portion of tasks in VisualWebArena involve visual input as part of task goals and require an understanding of the visual information of the current website. This also leads to their large variations of task types.

**307**

**318**

<span id="page-5-0"></span>**271 272 273 274 275 276 277** Table 1: Success rates (SR) of published open-source methods and CER up to the completion of this work on WEBARENA, Bold represents the best result on the website while underline means the second best results. CER uses text observations (accessibility tree) only and  $CER<sub>v</sub>$  takes both text and visual observations. The results originate from the corresponding papers except BrowserGym which we reproduce the GPT-4o version by ourselves. \*: SteP [\(Sodhi et al., 2024\)](#page-11-13) uses humandesigned detailed policies for each website, so it is not comparable with other autonomous methods without human involvement and we set it apart just for references.



# 4.1 IMPLEMENTATION DETAILS

## 4.1.1 WEBARENA

**293 294 295 296 297 298 299 300 301 302 303 304 305 306** For WebArena, all tasks in it provide text-only task instruction, so we implement two versions of CER; CER takes text-only observation, and  $CER<sub>v</sub>$  takes both text and visual observation of the environment. The text observation is an accessibility tree representation of the current webpage, and the visual observation is a screenshot of the current page. For both versions, we use GPT-4o-2024- 0513 as the backbone language model with a temperature of 0.1. We use BrowserGym [\(Drouin](#page-10-13) [et al., 2024\)](#page-10-13) as the environment, which provides both text and visual observation for the agent and adds additional information for clickable and visible elements in the accessibility tree of the webpage. To fairly highlight the improvement of CER, we run GPT-4o w/ BrowserGym [\(Drouin](#page-10-13) [et al., 2024\)](#page-10-13) by ourselves as the baseline for comparison. CER is compatible with most off-theshelf language model agents since it only needs the past trajectories. Here, we test it with a simple method by prompting GPT-4o directly and using ReAct [\(Yao et al., 2023b\)](#page-12-1) as the output format as in BrowserGym [\(Drouin et al., 2024\)](#page-10-13) and WebArena [\(Zhou et al., 2024b\)](#page-12-3). We also combine it with another performant method and observe significant improvements $(\S 5.4)$ . We set the retrieval parameter to  $k_d = 5$  and  $k_s = 5$ , denoting the maximum number of dynamics/skills to retrieve and replay.

#### **308** 4.1.2 VISUALWEBARENA

**309 310 311 312 313 314 315 316 317** For VISUALWEBARENA, similar to WEBARENA, we still use BrowserGym [\(Drouin et al., 2024\)](#page-10-13) as our environment. Since BrowserGym does not support visual evaluation, we implemented the environment by ourselves and built CER on top of that. We also run BrowserGym results as the baseline for comparison. Using the same setting as [\(Koh et al., 2024a\)](#page-10-6), we apply Set-of-Marks (SoM) [\(Yang et al., 2023\)](#page-12-7) to the original screenshot of the webpage. This method marks each interactable element of the webpage with a highlighted bounding box and the corresponding unique element ID on the corner of the box to enable grounding. Besides the screenshot, the agent is also provided with text observation of the environment for better grounding, where the ID of each element is consistent with the one in the SoM-processed screenshot.

#### **319 320** 4.2 RESULTS

**321 322 323** Our results on these two benchmarks are summarized in Table [1](#page-5-0) and Table [2.](#page-6-1) On WEBARENA and VISUALWEBARENA, while orthogonal to the other methods, CER achieves state-of-the-art performance and improves the baseline agent, GPT-4o w/ BrowserGym [\(Drouin et al., 2024\)](#page-10-13), relatively by 36.6% and 21.8% respectively. It should be noted that SteP [\(Sodhi et al., 2024\)](#page-11-13) uses human-designed <span id="page-6-1"></span>Table 2: Success rates (SR) of published open-source methods and CER on VISUALWEBARENA, Bold represents the best result in the domain. Results are from the corresponding papers except BrowserGym. We implement the agent with BrowserGym by ourselves.



<span id="page-6-2"></span>Table 3: Success rates (SR) of different settings with different offline data source on the Forum tasks split of the WebArena.



**349 350 351**

**352 353 354**

**355 356 358** policies, i.e., step-by-step instructions for each website split, and can need much extra human effort when encountering new cases or on new websites. So we do not consider it when comparing CER with other methods. On VisualWebArena, CER achieves SOTA performance and outperforms the tree search method [\(Koh et al., 2024b\)](#page-10-7), which is also built on GPT-4o, with much lower token costs. The result of the tree search is obtained through a search algorithm that uses 20 times sampling at each step, and a maximum of 5 steps, with extra costs of GPT-4o used as a value function. In our implementation, we use a maximum of only 30 steps for each task, similar to the setting in [\(Zhou](#page-12-3) [et al., 2024b\)](#page-12-3) and [\(Koh et al., 2024a\)](#page-10-6), thus using at least 3 times fewer tokens.

**359 360**

**361**

**357**

# 5 ANALYSIS

**362 363 364 365 366** In this section, we conduct experiments on offline and offline + online hybrid settings of CER to show its potential with a few offline trajectories. Furthermore, we conduct extensive analysis to investigate and better understand CER's improvements through cross-template success rates and two interesting metrics for continual learning systems: stability and plasticity. Finally, we validate its compatibility and synergy with other performant methods, proving its wide applicability.

**367 368**

**369**

# <span id="page-6-0"></span>5.1 ONLINE AND OFFLINE LEARNING

**370 371 372** As mentioned in section [3.4,](#page-4-0) CER can also be run in offline or offline+online hybrid settings. We conduct offline and offline + online experiments on the Forum tasks split of WebArena with two sources of offline training trajectories: from human demonstrations or from self-guided explorations.

**373 374 375 376 377** For the human annotation data, We designed five tasks, which were validated as not appearing in the test set, and denoted corresponding oracle trajectories for Forum websites. For the random exploration data, we prompt a language model to propose diverse actions at each step and collect the final exploration trajectories. The details of prompts and tasks can be found in [A.3](#page-13-1) and [A.4.](#page-13-2) The overall results are shown in Table [3.](#page-6-2) Both training sources improve the performance over

the baseline in the offline setting. Notably, with five human annotations as the training set, the

**324 325**

**378 379 380 381 382 383 384 385 386 387** performance of offline + online learning surpasses the original online learning. To understand how offline and online learning synergize with each other, we take task 31 as an example: the agent is asked to get the count of comments that have received more downvotes than upvotes for the user who made the latest post on the photoshopbattles forum. In online settings, the agent does not know how to sort the posts on the Forum website either because this task is at the beginning, and it has not learned many experiences yet. However, from the training set, CER distilled the page summary of the forums page where all forums are displayed and also the skill of sorting the list of posts. Aware of the existence of the forums page, the agent knows to click the "forums" button to navigate to the list of forums. After that, it is inspired by the skill and sorts the posts correctly. It finishes the task successfully with dynamics and skills distilled from the training set.

**388 389 390 391 392 393** Although in the offline setting, both training sources help the agent outperform the baseline, offline + online settings with self-guided explorations perform even worse than the online-only setting. We analyzed the results and found that the trajectories collected through such explorations are highly unstructured and noisy. The exploration agent can jump from one action to another unrelated one. So, the distillation module can hardly distill useful patterns from it. So, the distilled experiences may even mislead the agent sometimes.

**394 395 396 397 398 399** In real-world scenarios, high-quality human-annotated training data is hard to collect, so online learning is still important and meaningful in most cases. It would be interesting to explore the potential of CER with more high-quality human-labelled trajectories. The negative impact of the training set derived from explorations also indicates that goal-oriented trajectory matters for CER because it has more structured, continuous, and relatively meaningful action sequences rather than unordered small pieces.

**400 401**

**402**

## <span id="page-7-0"></span>5.2 INVESTIGATING IMPROVEMENTS OF CER

**403 404** In this section, we try to understand where the improvements of CER come from and get some intuitions about how CER works.

**405 406 407 408 409 410 411 412 413** Intuitively, the state space and action space for the current step are extremely large. However, for human users, the states that we often navigate to and the actions that we usually take are only a small subset of the whole space. Experiences distilled from some goal-oriented trajectories tend to contain some informative and effective states and actions that are often navigated to or used. With the highlighted promising states, actions, and decision-making patterns, the agent can issue a correct action much more easily. Of course, some of the experiences can be noisy and misleading. We show in section [5.5](#page-8-1) that CER is still robust to the correctness of the trajectories. This intuition also aligns with the Recognition Primed Decision making Model proposed by [Klein](#page-10-14) [\(1998\)](#page-10-14), where humans tend to recognize promising actions when encountering complex environments.

**414 415 416 417 418 419 420 421 422 423 424 425 426** We also conduct quantitative comparisons between CER and baseline method to investigate the improvements. The tasks in WebArena are designed based on templates, and at most, five tasks share the same template. For example, What is the top-1 best-selling brand in Quarter 1 2022 is built based on the template: What is the top-n best-selling brand in period. Although many tasks do not share exactly the same problem-solving pattern, if the agent just memorizes the pattern of the whole task, it will be able to solve some other tasks in the same template more easily, thus improving the overall performance. So, we use the cross-template average success rate, calculated by the number of templates solved (at least one task is solved) divided by the total number of templates. We run experiments on Forum tasks of WebArena. The results are shown in Table [4.](#page-8-2) CER shows a significant improvement in cross-template success rates. This result validates that the improvement of CER does not come from memorizing the whole trajectory of a task. Instead, it distills more fine-grained experiences, which allows for the generalization of different types of tasks. Also, we analyze the improvements from the perspective of stability and plasticity, which measures the ability to retain original ability and learn new things. More details are in section [5.3.](#page-7-1)

<span id="page-7-1"></span>**427**

#### **428** 5.3 STABILITY AND PLASTICITY

**429**

**430 431** A well-designed continual learning system should demonstrate both stability (preservation of old knowledge) and plasticity (acquisition of new knowledge) [\(Grossberg, 1982;](#page-10-8) [Rolnick et al., 2019\)](#page-11-9). Since knowledge is hard to measure in our case, we measure the acquisition of new knowledge

#### **433 434** Table 4: Cross-template success rates (ct-SR), stability and plasticity of CER and baseline on the Forum split of WebArena



**441**

<span id="page-8-2"></span>**432**

**442 443 444 445 446 447 448 449 450 451 452** through problem-solving ability, i.e., success rates, in a specific environment. Therefore, we similarly measure the stability and plasticity of CER in cross-template success rate (ct-SR) since the success in new types of task demonstrates new problem-solving ability. Specifically, stability is measured through the percentage of tasks from the baseline that CER is able to solve, which reflects how well CER maintains the original capability of the baseline. Plasticity is measured by the improvement of CER on new cases, measuring how many additional tasks CER can solve compared to the baseline. Since CER can be understood as a continual learning system built on the baseline method agent. We set the stability and plasticity of the baseline to 100% and used the ct-SR to calculate the stability and plasticity of CER. The results are also shown in Table [4.](#page-8-2) With most of the original abilities retained, CER demonstrates 41% new problem types solved, proving the validity of CER as a continual learning framework. This also indicates the potential of the compatibility with other performant methods, which we discuss in detail in section [5.4.](#page-8-0)

**453 454 455**

### <span id="page-8-0"></span>5.4 SYNERGY WITH PERFORMANT METHODS

**456 457 458 459 460 461 462 463 464 465 466 467 468 469** We also analyze the compatibility of CER with other performant methods. Tree search [\(Koh et al., 2024b\)](#page-10-7) is a computing-intensive method with more explorations and backtracking to search for better action to take. However, due to the high costs and the long time it takes, we chose another comparable method of it: trajectory sampling and reranking. We sampled 3 times for each task with max steps of 20 and prompted a language model with the trajectories to give a score and select the trajectory with the highest score as the final one. The procedure of applying CER to such method is similar to what we do with baseline agent. We conduct experiments in an online setting on the Forums split of WebArena. The results are in Table [5.](#page-8-3) CER with sampling method improves CER w/ Re-Act performance by a relative success rate increase of 39.5%. This is because, firstly, such performant methods generally have better precision from start to end, so the experiences distilled from them

<span id="page-8-3"></span>Table 5: Comparison of success rates (SR) of CER and CER w/ trajectory sampling and reranking on the Forum split of WebArena



**470 471 472 473** are of higher quality. Additionally, high-quality experiences make performant methods more robust through the learned experiences and provide environment-specific knowledge to help better decision-making. Also, for exploration methods like tree search, CER should enable it to learn from past experiences and avoid searching from scratch each time, lowering its costs significantly.

**474 475**

**476**

### <span id="page-8-1"></span>5.5 ACCESS TO GROUND TRUTH REWARDS

**477 478 479 480 481 482** Currently, CER distills experiences from both successful and failed cases. To investigate whether the distillation from failed cases is a bottleneck of CER, we run CER for only successful trajectories evaluated by ground truth evaluators. We conduct the experiments on the full set of WebArena. The results are summarized in Table [6.](#page-9-0) The results show that CER performs better with the access to ground truth reward. The possible reason could be that the successful trajectories have higher quality and are more informative, while the failed trajectories provide some misleading action sequences that will negatively influence the agent's decision-making.

**483**

**484 485** Nevertheless, the acceptable gap and significant improvements over the baseline agent show the robustness of CER given noisy trajectories. This gives credit to the implicit reasoning ability and the flexible natural language representation of experiences. Although provided with a few noisy

<span id="page-9-0"></span>**487 488 489 490** Table 6: Success rates  $(SR)$  of CER and CER<sub>success</sub> on five website splits of the WebArena. CER is the main method we used before, which learns from both successful and failed trajectories.  $CER_{success}$  uses ground truth evaluators from the environment to filter out and learn from successful experiences only. Both method takes text observation for comparison



<span id="page-9-1"></span>Table 7: Success rates (SR) of CER on the Forum split of WebArena with different ablation settings to the experiences.



experiences, the agent can still filter out useful trajectories and issue reasonable action most of the time.

## <span id="page-9-2"></span>5.6 DIVISION OF DYNAMICS AND SKILLS

**513 514 515 516 517 518** We conduct an ablation experiment to investigate the necessity of the division of dynamics and skills. The experiment is run on the Forums split of WebArena. The results in Table [7](#page-9-1) show that both dynamics and skills are important for CER. Environment dynamics make the agent aware of the content of many pages and also provide the URL to navigate to. Skills inspire the agent and also provide promising actions to be taken in the current step. They provide heuristics in terms of states and actions correspondingly and synergize with each other.

**519 520**

### 5.7 LIMITATIONS AND FUTURE WORK

**521 522 523 524 525 526 527 528 529** Despite the substantial progress achieved with CER, there are several limitations that will influence its applicability and could be addressed in future work. First, section [5.1](#page-6-0) shows that although CER performs even better in offline + online settings, it requires the trajectories to be goal-oriented to distill high-quality experiences. The performance is limited if trajectories from random explorations are provided. The more fine-grained utilization of low-quality trajectories could be explored in the future. Secondly, the environment dynamics help much in web environments, as shown in section [5.6,](#page-9-2) partially because the agent can directly navigate to a specific page with its URL. It would be interesting to investigate how we can utilize the environment dynamics in other agent tasks, such as real-world navigation [\(Shridhar et al., 2021\)](#page-11-14) in future work.

**530 531**

**532**

# 6 CONCLUSIONS

**533 534 535 536 537 538 539** In this paper, we proposed a training-free framework for efficient and effective continual learning of language agents in complex web environments. Our framework enables language agents to learn from past experiences and replay during inference time for better decision-making. We also conduct extensive analysis to investigate the potential of CER under various different settings, including offline or offline + online paradigm. Furthermore, we validate the effectiveness of it as a continual learning system through stability and plasticity. We believe that learning from past experiences is crucial for building a helpful computer agent that can adapt to different environments and evolve autonomously.



<span id="page-10-3"></span>**567 568 569**

<span id="page-10-14"></span>**576**

- <span id="page-10-1"></span>J. Achiam, S. Adler, S. Agarwal, L. Ahmad, I. Akkaya, F. L. Aleman, D. Almeida, J. Altenschmidt, S. Altman, S. Anadkat, et al. Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*, 2023.
- <span id="page-10-2"></span>**544 545** A. Anthropic. The claude 3 model family: Opus, sonnet, haiku. *Claude-3 Model Card*, 1, 2024.
- <span id="page-10-5"></span>**546 547 548 549 550 551 552 553 554 555** Mark Chen, Jerry Tworek, Heewoo Jun, Qiming Yuan, Henrique Ponde de Oliveira Pinto, Jared Kaplan, Harri Edwards, Yuri Burda, Nicholas Joseph, Greg Brockman, Alex Ray, Raul Puri, Gretchen Krueger, Michael Petrov, Heidy Khlaaf, Girish Sastry, Pamela Mishkin, Brooke Chan, Scott Gray, Nick Ryder, Mikhail Pavlov, Alethea Power, Lukasz Kaiser, Mohammad Bavarian, Clemens Winter, Philippe Tillet, Felipe Petroski Such, Dave Cummings, Matthias Plappert, Fotios Chantzis, Elizabeth Barnes, Ariel Herbert-Voss, William Hebgen Guss, Alex Nichol, Alex Paino, Nikolas Tezak, Jie Tang, Igor Babuschkin, Suchir Balaji, Shantanu Jain, William Saunders, Christopher Hesse, Andrew N. Carr, Jan Leike, Josh Achiam, Vedant Misra, Evan Morikawa, Alec Radford, Matthew Knight, Miles Brundage, Mira Murati, Katie Mayer, Peter Welinder, Bob Mc-Grew, Dario Amodei, Sam McCandlish, Ilya Sutskever, and Wojciech Zaremba. Evaluating large language models trained on code, 2021. URL <https://arxiv.org/abs/2107.03374>.
- <span id="page-10-10"></span>**556 557 558 559** Xiang Deng, Yu Gu, Boyuan Zheng, Shijie Chen, Samuel Stevens, Boshi Wang, Huan Sun, and Yu Su. Mind2web: Towards a generalist agent for the web. *Advances in neural information processing systems, Datasets and Benchmarks Track*, 36, 2023.
- <span id="page-10-13"></span>**560 561 562 563** Alexandre Drouin, Maxime Gasse, Massimo Caccia, Issam H. Laradji, Manuel Del Verme, Tom Marty, Leo Boisvert, Megh Thakkar, Quentin Cappart, David Vazquez, Nicolas Chapados, and ´ Alexandre Lacoste. Workarena: How capable are web agents at solving common knowledge work tasks? *International Conference on Machine Learning*, 2024.
- <span id="page-10-0"></span>**564 565 566** Stan Franklin and Art Graesser. Is it an agent, or just a program? a taxonomy for autonomous agents. In *International Workshop on Agent Theories, Architectures, and Languages*, pp. 21–35. Springer, 1996.
	- Google Gemini Team. Gemini: A family of highly capable multimodal models. *arXiv preprint arXiv:2312.11805*, 2023.
- <span id="page-10-8"></span>**570 571** Stephen Grossberg. How does a brain build a cognitive code? In *Studies of Mind and Brain*, pp. 1–52. Springer, 1982.
- <span id="page-10-4"></span>**572 573 574 575** Dan Hendrycks, Collin Burns, Steven Basart, Andy Zou, Mantas Mazeika, Dawn Song, and Jacob Steinhardt. Measuring massive multitask language understanding. In *International Conference on Learning Representations*, 2021. URL [https://openreview.net/forum?id=](https://openreview.net/forum?id=d7KBjmI3GmQ) [d7KBjmI3GmQ](https://openreview.net/forum?id=d7KBjmI3GmQ).
- <span id="page-10-7"></span><span id="page-10-6"></span>**577** Gary Klein. *Sources of Power: How People Make Decisions*. MIT Press, 1998.
	- Jing Yu Koh, Robert Lo, Lawrence Jang, Vikram Duvvur, Ming Chong Lim, Po-Yu Huang, Graham Neubig, Shuyan Zhou, Ruslan Salakhutdinov, and Daniel Fried. Visualwebarena: Evaluating multimodal agents on realistic visual web tasks. *Annual Meeting of the Association for Computational Linguistics*, 62, 2024a.
	- Jing Yu Koh, Stephen McAleer, Daniel Fried, and Ruslan Salakhutdinov. Tree search for language model agents. 2024b. URL <https://arxiv.org/abs/2407.01476>.
	- Aman Madaan, Niket Tandon, Prakhar Gupta, Skyler Hallinan, Luyu Gao, Sarah Wiegreffe, Uri Alon, Nouha Dziri, Shrimai Prabhumoye, Yiming Yang, Sean Welleck, Bodhisattwa Prasad Majumder, Shashank Gupta, Amir Yazdanbakhsh, and Peter Clark. Self-refine: Iterative refinement with self-feedback. *ArXiv*, abs/2303.17651, 2023.
- <span id="page-10-12"></span><span id="page-10-9"></span>**589 590 591** Jiayi Pan, Yichi Zhang, Nicholas Tomlin, Yifei Zhou, Sergey Levine, and Alane Suhr. Autonomous evaluation and refinement of digital agents. *Conference on Language Modeling*, 2024.
- <span id="page-10-11"></span>**592 593** Joon Sung Park, Joseph C. O'Brien, Carrie J. Cai, Meredith Ringel Morris, Percy Liang, and Michael S. Bernstein. Generative agents: Interactive simulacra of human behavior. *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, 2023.

<span id="page-11-10"></span>**608**

- <span id="page-11-6"></span>**594 595 596** Christopher Rawles, Alice Li, Daniel Rodriguez, Oriana Riva, and Timothy Lillicrap. Android in the wild: A large-scale dataset for android device control. In *NeurIPS*, 2023.
- <span id="page-11-7"></span>**597 598 599 600 601** Christopher Rawles, Sarah Clinckemaillie, Yifan Chang, Jonathan Waltz, Gabrielle Lau, Marybeth Fair, Alice Li, William Bishop, Wei Li, Folawiyo Campbell-Ajala, Daniel Toyama, Robert Berry, Divya Tyamagundlu, Timothy Lillicrap, and Oriana Riva. Androidworld: A dynamic benchmarking environment for autonomous agents, 2024. URL [https://arxiv.org/abs/2405.](https://arxiv.org/abs/2405.14573) [14573](https://arxiv.org/abs/2405.14573).
- <span id="page-11-9"></span>**602 603** David Rolnick, Arun Ahuja, Jonathan Schwarz, Timothy P. Lillicrap, and Greg Wayne. Experience replay for continual learning. *Advances in neural information processing systems*, 32, 2019.
- <span id="page-11-0"></span>**605** Stuart J. Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall, 1995.
- <span id="page-11-8"></span>**606 607** Tom Schaul, John Quan, Ioannis Antonoglou, and David Silver. Prioritized experience replay. *International Conference on Learning Representations*, 2016.
- **609 610 611** Noah Shinn, Federico Cassano, Beck Labash, Ashwin Gopinath, Karthik Narasimhan, and Shunyu Yao. Reflexion: language agents with verbal reinforcement learning. In *Neural Information Processing Systems*, 2023.
- <span id="page-11-14"></span>**612 613 614 615** Mohit Shridhar, Xingdi Yuan, Marc-Alexandre Cote, Yonatan Bisk, Adam Trischler, and Matthew Hausknecht. {ALFW}orld: Aligning text and embodied environments for interactive learning. In *International Conference on Learning Representations*, 2021. URL [https://openreview.](https://openreview.net/forum?id=0IOX0YcCdTn) [net/forum?id=0IOX0YcCdTn](https://openreview.net/forum?id=0IOX0YcCdTn).
- <span id="page-11-13"></span>**616 617 618** Paloma Sodhi, S. R. K. Branavan, Yoav Artzi, and Ryan McDonald. Step: Stacked llm policies for web actions. *Conference on Language Modeling*, 2024.
- <span id="page-11-11"></span>**619 620 621 622** Guanzhi Wang, Yuqi Xie, Yunfan Jiang, Ajay Mandlekar, Chaowei Xiao, Yuke Zhu, Linxi Fan, and Anima Anandkumar. Voyager: An open-ended embodied agent with large language models. *Transactions on Machine Learning Research*, 2024a. ISSN 2835-8856. URL [https:](https://openreview.net/forum?id=ehfRiF0R3a) [//openreview.net/forum?id=ehfRiF0R3a](https://openreview.net/forum?id=ehfRiF0R3a).
- <span id="page-11-12"></span>**623 624 625** Zora Zhiruo Wang, Jiayuan Mao, Daniel Fried, and Graham Neubig. Agent workflow memory. *ArXiv*, 2024b.
- <span id="page-11-2"></span>**626 627 628 629 630** Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, brian ichter, Fei Xia, Ed H. Chi, Quoc V Le, and Denny Zhou. Chain of thought prompting elicits reasoning in large language models. In Alice H. Oh, Alekh Agarwal, Danielle Belgrave, and Kyunghyun Cho (eds.), *Advances in Neural Information Processing Systems*, 2022. URL [https://openreview.net/](https://openreview.net/forum?id=_VjQlMeSB_J) [forum?id=\\_VjQlMeSB\\_J](https://openreview.net/forum?id=_VjQlMeSB_J).
- <span id="page-11-5"></span>**631 632 633 634** Tianbao Xie, Danyang Zhang, Jixuan Chen, Xiaochuan Li, Siheng Zhao, Ruisheng Cao, Toh Jing Hua, Zhoujun Cheng, Dongchan Shin, Fangyu Lei, Yitao Liu, Yiheng Xu, Shuyan Zhou, Silvio Savarese, Caiming Xiong, Victor Zhong, and Tao Yu. Osworld: Benchmarking multimodal agents for open-ended tasks in real computer environments. In *NeurIPS*, 2024a.
- <span id="page-11-1"></span>**635 636 637 638** Tianbao Xie, Siheng Zhao, Chen Henry Wu, Yitao Liu, Qian Luo, Victor Zhong, Yanchao Yang, and Tao Yu. Text2reward: Reward shaping with language models for reinforcement learning. In *The Twelfth International Conference on Learning Representations*, 2024b. URL [https:](https://openreview.net/forum?id=tUM39YTRxH) [//openreview.net/forum?id=tUM39YTRxH](https://openreview.net/forum?id=tUM39YTRxH).
- <span id="page-11-4"></span>**640 641 642 643 644** Tianbao Xie, Fan Zhou, Zhoujun Cheng, Peng Shi, Luoxuan Weng, Yitao Liu, Toh Jing Hua, Junning Zhao, Qian Liu, Che Liu, Zeyu Liu, Yiheng Xu, Hongjin SU, Dongchan Shin, Caiming Xiong, and Tao Yu. Openagents: An open platform for language agents in the wild. In *First Conference on Language Modeling*, 2024c. URL [https://openreview.net/forum?id=](https://openreview.net/forum?id=sKATR2O1Y0) [sKATR2O1Y0](https://openreview.net/forum?id=sKATR2O1Y0).
- <span id="page-11-3"></span>**645 646 647** Yiheng Xu, Hongjin Su, Chen Xing, Boyu Mi, Qian Liu, Weijia Shi, Binyuan Hui, Fan Zhou, Yitao Liu, Tianbao Xie, Zhoujun Cheng, Siheng Zhao, Lingpeng Kong, Bailin Wang, Caiming Xiong, and Tao Yu. Lemur: Harmonizing natural language and code for language agents. *International Conference on Learning Representations*, 2023.

<span id="page-12-7"></span>

- <span id="page-12-4"></span> Shunyu Yao, Howard Chen, John Yang, and Karthik Narasimhan. Webshop: Towards scalable realworld web interaction with grounded language agents. *Advances in neural information processing systems, Datasets and Benchmarks Track*, 35, 2022.
- <span id="page-12-0"></span> Shunyu Yao, Dian Yu, Jeffrey Zhao, Izhak Shafran, Thomas L. Griffiths, Yuan Cao, and Karthik Narasimhan. Tree of thoughts: Deliberate problem solving with large language models. *ArXiv*, abs/2305.10601, 2023a.
- <span id="page-12-5"></span><span id="page-12-1"></span> Shunyu Yao, Jeffrey Zhao, Dian Yu, Nan Du, Izhak Shafran, Karthik Narasimhan, and Yuan Cao. React: Synergizing reasoning and acting in language models. *International Conference on Learning Representations*, 2023b.
	- Andrew Zhao, Daniel Huang, Quentin Xu, Matthieu Lin, Y. Liu, and Gao Huang. Expel: Llm agents are experiential learners. *ArXiv*, abs/2308.10144, 2023.
	- Longtao Zheng, R. Wang, and Bo An. Synapse: Trajectory-as-exemplar prompting with memory for computer control. In *International Conference on Learning Representations*, 2023.
- <span id="page-12-6"></span><span id="page-12-3"></span><span id="page-12-2"></span> Andy Zhou, Kai Yan, Michal Shlapentokh-Rothman, Haohan Wang, and Yu-Xiong Wang. Language agent tree search unifies reasoning, acting, and planning in language models. In *Forty-first International Conference on Machine Learning*, 2024a. URL [https://openreview.net/](https://openreview.net/forum?id=njwv9BsGHF) [forum?id=njwv9BsGHF](https://openreview.net/forum?id=njwv9BsGHF).
	- Shuyan Zhou, Frank F. Xu, Hao Zhu, Xuhui Zhou, Robert Lo, Abishek Sridhar, Xianyi Cheng, Tianyue Ou, Yonatan Bisk, Daniel Fried, Uri Alon, and Graham Neubig. Webarena: A realistic web environment for building autonomous agents. *International Conference on Learning Representations*, 2024b.

#### A APPENDIX

#### <span id="page-13-0"></span> A.1 CER PROMPTS

 Here we provide detailed prompts for each module in CER. Figure [3](#page-14-0) and [4](#page-15-0) show the system prompts for distillation modules, while Figure [5](#page-16-0) and [6](#page-17-0) are system prompts for retrieval modules.

#### A.2 EXPERIENCE EXAMPLES

 We provide experiences examples for WEBARENA and VISUALWEBARENA here. These natural language experiences are programmatically transformed from the structured experiences stored in the experience buffer and will be added to the system prompt of the model when solving tasks. The examples are shown in Figure [7](#page-18-0) and [8.](#page-18-1)

 

### <span id="page-13-1"></span>A.3 SELF-GUIDED EXPLORATION PROMPT

 As mentioned in section [5.1,](#page-6-0) we prompt a language model, i.e., GPT-4o, here to explore diverse actions in the environment and collect the corresponding trajectories. We limit the max steps to 30 and sample 10 trajectories. The instruction part of the prompt is shown in Figure [9.](#page-18-2)

 

### <span id="page-13-2"></span>A.4 HUMAN ANNOTATED TASKS

 As stated in section [5.1,](#page-6-0) we designed 5 tasks on the Forum website and asked a human annotator to annotate the oracle trajectory for each task. The full list of task instructions is as follows:

- *Find the title of the most commented post in forum 'history'.*
- *Find the title of the most controversial post of all time in forum 'Paterson'*
- *Go to the user's profile who made the comment "What are you doing in a deep learning sub?"*
- *Upvote the comment of the current user which replies to 'Maybe there's just something wrong with me.' by HedleyLamarrrr*
- *Reply to the first comment of the post titled 'It's the only logical explanation' with 'lol'*

<span id="page-14-0"></span>

Figure 3: System message for dynamics distillation module in CER

<span id="page-15-0"></span>

- **862**
- **863**

<span id="page-16-0"></span>

<span id="page-17-0"></span>

<span id="page-18-2"></span><span id="page-18-1"></span><span id="page-18-0"></span>