
TRACE: A Comprehensive Benchmark for Continual Learning in Large Language Models

Anonymous Author(s)

Affiliation

Address

email

Abstract

1 Aligned large language models (LLMs) demonstrate exceptional capabilities in
2 task-solving, following instructions, and ensuring safety. However, the continual
3 learning aspect of these aligned LLMs has been largely overlooked. Existing
4 continual learning benchmarks lack sufficient challenge for leading aligned LLMs
5 due to their homogeneous task types and low task complexity. To bridge this gap,
6 we introduce TRACE, a benchmark designed to rigorously assess continual learning
7 capabilities in LLMs. TRACE comprises eight challenging tasks from the scope of
8 domain-specific tasks, multilingual capabilities, code generation, and mathematical
9 reasoning. Through systematic experiments on TRACE with six different aligned
10 models ranging from 7B to 70B, we discovered significant declines in both general
11 performance and instruction-following abilities. For example, the accuracy of
12 llama2-chat 13B on the gsm8k dataset declined precipitously from 43.14% to
13 2.12% after training on our datasets. This highlights the challenge of finding a
14 suitable tradeoff between achieving performance on specific tasks while preserving
15 the original prowess of LLMs. Our results demonstrate that integrating task-
16 specific cues with meta-rationales significantly reduces catastrophic forgetting and
17 improves task convergence, offering a viable strategy to enhance the adaptability
18 of LLMs in dynamic environments.

19 1 Introduction

20 Large Language Models (LLMs) [1; 2] have revolutionized natural language processing through a two-
21 step process: initial pretraining on extensive corpora, followed by fine-tuning on human-generated
22 instructions and preference data, aligning them with human language and intentions. Aligned LLMs
23 have showcased impressive capabilities and ensured safer responses. However, as the demands for
24 language models grow, there's a pressing need to enhance their abilities in areas such as domain-
25 specific knowledge [3; 4], multilingual proficiency [5], complex task-solving [6], and tool usage
26 [7]. Yet, retraining and realigning them from scratch to meet these demands is impractical due to
27 prohibitive training costs and the challenge of acquiring high-quality data. Therefore, incrementally
28 training existing Aligned LLMs through continual learning (CL [8]) is crucial. However, when
29 dealing with tasks in sequential manners, it is challenging to retain the performance of previous tasks,
30 which is known as "catastrophic forgetting" [9]. Therefore, we prompt the pressing question: *To what*
31 *degree do Aligned LLMs exhibit catastrophic forgetting when subjected to incremental training?*

32 Existing continual learning benchmarks [10; 11; 12] are not suitable for evaluating the state-of-the-art
33 LLMs. Firstly, many of these benchmarks predominantly consist of simplistic natural language
34 understanding datasets. These tasks, due to their inherent simplicity, fail to challenge the capabilities
35 of large-scale models adequately. Secondly, prior benchmarks have primarily focused on metrics that
36 assess the performance of the models on target sequential tasks. Yet, for aligned models, aspects like

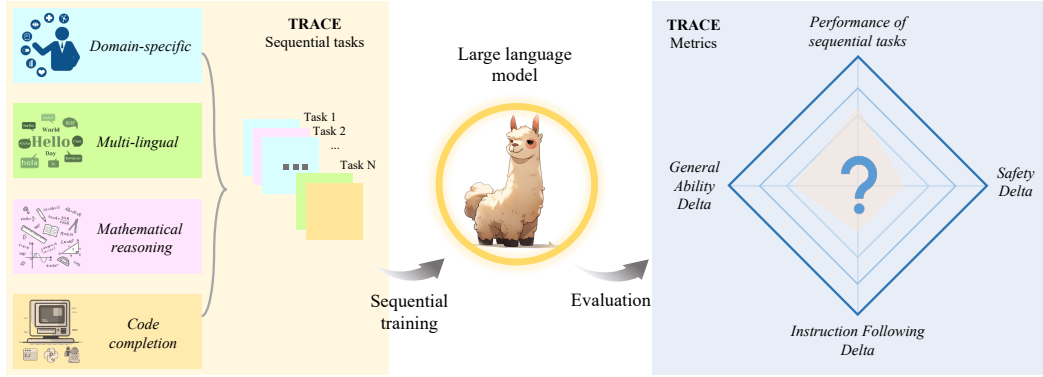


Figure 1: An overview of TRACE benchmark. TRACE consists of two main components: 1) A selection of eight datasets constituting a tailored set of tasks for continual learning, covering challenges in domain-specific tasks, multilingual capabilities, code generation, and mathematical reasoning. 2) A post-training evaluation of LLM capabilities. In addition to traditional continual learning metrics, we introduce General Ability Delta, Instruction Following Delta, and Safety Delta to evaluate shifts in LLM’s inherent abilities.

generalization to new tasks, the ability to follow human instructions, and safety preservation are of paramount importance. Regrettably, these dimensions have not been thoroughly researched.

In this paper, we present **TRACE**, a continual learning benchmark designed for aligned LLMs. Our benchmark consists of eight distinct datasets spanning challenging tasks including domain-specific tasks, multilingual capabilities, code generation, and mathematical reasoning. All datasets have been standardized into a unified format, simplifying the evaluation process. To evaluate continual learning in aligned LLMs, we introduce three metrics: "General Ability Delta," "Instruction Following Delta," and "Safety Delta" to assess models’ forgetfulness in such scenarios.

We conduct a comprehensive evaluation of 6 aligned LLMs on TRACE. Evaluation results reveal several key findings: 1) Nearly all models exhibit a significant decline in general abilities after training on TRACE, especially in math and reasoning. For instance, the accuracy of llama2-chat 13B on the gsm8k dataset dropped from 43.14% to merely 2.12%. 2) Catastrophic forgetting remains a substantial issue for LLMs and does not diminish with the model size increase. Llama2-chat 70B also shows significant forgetting (with -17.5% backward transfer) on previous tasks. 3) Full-parameter training, compared to LoRA training, more easily fits the target tasks, but it also leads to a more pronounced decline in general abilities. 4) LLMs’ instruction-following capabilities also suffer a significant reduction after continual learning.

Through experimentation, we observed that tasks augmented with reasoning paths are notably effective in preserving certain capabilities of LLMs, preventing them from substantial declines. Such findings lead us to ponder on leveraging a model’s inherent strengths for rapid transfer on new tasks, rather than starting the learning curve from scratch. This motivation birthed our novel training strategy: Reasoning-augmented Continual Learning (RCL). RCL prompts the model to generate task analyses and rationales during training. As our results indicate, this approach not only boosts performance on target tasks but also significantly upholds the inherent strengths of LLMs.

2 Related Work

2.1 Continual Learning

Continual learning [8] aims to develop learning algorithms that can accumulate knowledge on non-stationary data. Existing works can be broadly categorized into rehearsal-based, regularization-based, and architecture-based approaches. Rehearsal-based approaches [13; 14] leverage a memory buffer that stores examples from previous tasks, training the model jointly with the current task. Regularization-based approaches [15; 16; 17] incorporate additional terms into the loss function to penalize changes in crucial weights. Architecture-based approaches [18; 12] focus on dynamically expanding model capacity or isolating existing model weights to mitigate interference between new and old tasks.

71 2.2 CL Benchmarks in NLP

72 The most recognized CL benchmark for NLP encompasses five text classification datasets [10],
 73 including AG News, Amazon Reviews, Yelp Reviews, DBpedia, and Yahoo Answers. Building
 74 upon this, [12] proposed a long CL benchmark which fuses the aforementioned five datasets with
 75 an additional four from the GLUE benchmark [19], five from the SuperGLUE benchmark [20], and
 76 the IMDB dataset [21]. However, this benchmark is limited in scope as it solely emphasizes Natural
 77 Language Generation (NLG) tasks and is restricted to English, thus lacking task diversity. In contrast,
 78 TRACE is a more varied and challenging benchmark, designed to test aligned LLMs across multiple
 79 sequential tasks. It assesses general capability, instruction adherence, and safety shifts. Recognizing
 80 that TRACE, like earlier benchmarks, may be incorporated into future pre-training, we acknowledge
 81 potential impacts on its long-term efficacy as a CL benchmark. Nonetheless, the current findings
 82 from TRACE provide essential insights into catastrophic forgetting in LLMs.

83 3 Preliminaries

84 Continual learning [22; 8] focuses on developing learning algorithms to accumulate knowledge on
 85 non-stationary data. In supervised continual learning, a sequence of tasks $\{\mathcal{D}_1, \dots, \mathcal{D}_T\}$ arrive in a
 86 streaming fashion. Each task $\mathcal{D}_t = \{(\mathbf{x}_i^t, \mathbf{y}_i^t)\}_{i=1}^{n_t}$ contains a separate target dataset, where $\mathbf{x}_i^t \in \mathcal{X}_t$,
 87 $\mathbf{y}_i^t \in \mathcal{Y}_t$. A single model needs to adapt to them sequentially, with only access to \mathcal{D}_t at the t -th task.
 88 In general, given a prediction model h_Θ parameterized by Θ , continual learning seeks to optimize for
 89 the following objective across all tasks:

$$\max_{\Theta} \sum_{k=1}^T \sum_{x, y \in \mathcal{D}_k} \log p_{\Theta}(y | x) \quad (1)$$

90 In this paper, we utilize overall performance (OP [23]), forward transfer (FWT [13]), and backward
 91 transfer (BWT [13]) scores as the main metrics. After incrementally learning the t -th task, the model’s
 92 score on the i -th task (where $i \leq t$) is denoted as $R_{t,i}^D$.

93 4 TRACE: A Comprehensive Benchmark for CL in LLMs

94 TRACE is designed to offer a comprehensive continual learning evaluation for LLMs. Illustrated in
 95 Figure 1, TRACE encompasses two primary components: a curated set of tasks tailored for continual
 96 learning, followed by an in-depth evaluation of an LLM’s post-training capabilities. In this section,
 97 we detail TRACE’s sequential tasks and introduce our evaluation metrics. In Section 4.4, we evaluate
 98 six models using TRACE and present our key findings.

99 4.1 Data Creation

100 There are three principles for the creation of TRACE. First, the datasets should be novel enough that
 101 most LLMs have not been trained on them. Second, they should be challenging for large language
 102 models. Third, a variety of tasks should be covered in our benchmark.

103 According to these three principles, in this section, we will provide a detailed introduction to the data
 104 collection process for each dataset. As these datasets have varying sizes, we create a balanced version
 105 by randomly sampling 5000 training examples and 2000 testing examples from the original datasets.
 106 As shown in Table 1, we get 40,000 training examples and 16,000 testing examples in total.

107 **Domain-Specific.** ScienceQA [24] is a multi-hop QA dataset collected from elementary and high
 108 school science curricula, with a rich domain diversity from natural science, social science, and
 109 language science, requiring the model of reasoning ability and science knowledge. In TRACE,
 110 we include only non-multimodal examples to exclusively test LLM performance. FOMC [25] is a
 111 hawkish-dovish classification task, which is novel in the financial domain. The dataset is divided into
 112 three subsets: data on meeting minutes, press conference data, and speech data. We use a combination
 113 of them. MeetingBank [26] is a new benchmark dataset for city council meeting summarization, an
 114 unstudied domain. It demands a global understanding of the whole long context.

Dataset	Source	Avg len	Metric	Language	#data
<i>Domain-specific</i>					
ScienceQA	Science	210	Accuracy	English	5,000
FOMC	Finance	51	Accuracy	English	5,000
MeetingBank	Meeting	2853	ROUGE-L	English	5,000
<i>Multi-lingual</i>					
C-STANCE	Social media	127	Accuracy	Chinese	5,000
20Minuten	News	382	SARI	Germany	5,000
<i>Code completion</i>					
Py150	Github	422	Edim similarity	Python	5,000
<i>Mathematical reasoning</i>					
NumGLUE-cm	Math	32	Accuracy	English	5,000
NumGLUE-ds	Math	21	Accuracy	English	5,000

Table 1: An overview of dataset statistics in TRACE. ‘Source’ indicates the context’s origin. ‘Avg len’ represents word count for English, German, and code datasets, and character count for Chinese. ‘SARI’ is a score specific to simplification.

Multi-lingual. LLMs’ cross-lingual abilities are constrained by their vocabulary and pre-training corpus. For instance, LLaMA’s vocabulary contains few Chinese tokens, affecting its efficiency with Chinese text. C-STANCE [27] is the first Chinese dataset for zero-shot stance detection collected from Sina Weibo, one of the most popular Chinese social media sites. It includes two challenging subtasks: target-based stance detection and domain-based stance detection. In TRACE, we include the target-based one, which means the targets in testing examples are unseen during training. 20Minuten [28] is a text simplification dataset consisting of full articles paired with shortened, simplified summaries from the Swiss news magazine. We use this dataset to evaluate the ability to generate German text.

Code completion. Code completion is another challenging task to evaluate long context modeling ability [29], and it is one of the most widely used features in software development through IDEs. We select the line-level code completion task of CodeXGLUE [30], which requires the model to generate the next line given the lengthy code input. The corpus Py150 [30] contains 150,000 Python programs collected from GitHub repositories. Since the golden labels of the testing dataset are not available by [30], we randomly divide each Python code in Py150 into two parts, taking the first part as inputs and the next line as labels.

Mathematical reasoning. Mathematical problems are always used to evaluate the reasoning ability of models. NumGLUE [31] is an 8-task benchmark far from solved including state-of-the-art large-scale language models performing significantly worse than humans. Both of the two tasks require arithmetic reasoning ability. It is worth noting that both datasets have original labels consisting only of numbers, without associated inference processes. The first one evaluates the common sense of models, while the second one requires some grade-school scientific knowledge.

4.2 CL Metrics Design

Unlike traditional continual learning benchmarks focused on sequential target tasks, evaluating aligned LLMs should also account for the preservation of their inherent capabilities. SoTA LLMs, through instruction tuning, exhibit impressive task-solving abilities. Aligning these models with human preferences further boosts their safety and usefulness. Hence, TRACE introduces a broader evaluation, including three unique metrics.

In the TRACE benchmark, we incorporate three metrics tailored to evaluate distinct dimensions of model performance following training: **General Ability Delta**, **Instruction Following Delta**, and **Safety Delta**. Each metric is designed to capture shifts in different areas—general abilities, instruction-following, and safety of responses, respectively. Despite their targeted focuses, all three

146 metrics are calculated using a consistent formula:

$$\Delta R_t^X = \frac{1}{N} \sum_{i=1}^N (R_{t,i}^X - R_{0,i}^X)$$

147 where X represents the specific metric focus—general ability, instruction-following, or safety—and
148 N is the number of datasets considered within each respective category. This unified formula
149 underscores the systematic approach TRACE adopts to evaluate different dimensions of LLM
150 performance enhancements or declines post-training.

151 In the development of evaluation metrics, integrating existing and newly introduced indicators into
152 a single, unified metric might appear straightforward through a weighted summary. However, the
153 implementation of such a composite metric necessitates careful prioritization of the capabilities most
154 valued by users. Therefore, this paper does not propose a universal metric for ranking models.

155 4.3 Experimental Setup

156 4.3.1 Models & Baselines

157 To evaluate the resilience of aligned LLMs from diverse training backgrounds and strategies, we select
158 six backbones from three organizations: Meta: LLaMa-2-7B-Chat, LLaMa-2-13B-Chat, LLaMa-
159 2-70B-Chat [2], BaiChuan: Baichuan 2-7B-Chat [32], and Large Model Systems Organization:
160 Vicuna-13B-V1.5, Vicuna-7B-V1.5 [33].

161 We evaluate the performance of LLMs in a continual learning setting using different approaches:

162 **Sequential Full-Parameter Fine-Tuning (SeqFT)** It trains all model parameters in sequence.

163 **LoRA-based Sequential Fine-Tuning (LoraSeqFT)** Only the low-rank LoRA matrices are fine-
164 tuned, leaving the LLM backbone fixed [34]. This method is chosen based on prior findings of
165 reduced forgetting with "Efficient Tuning" [35].

166 **Replay-based Sequential Fine-Tuning (Replay)** We incorporate data from LIMA along with 10%
167 of data from previous tasks into our training dataset.

168 **In-Context Learning (ICL)** Task demonstrations are supplied as part of the language prompt,
169 acting as a form of prompt engineering [36]. A 6-shot setting is used for our experiments.

170 **Other Continual Learning Baselines** We also demonstrate the experiment results on a few
171 continual learning baselines, including EWC [15], ODG [37], PP [12], L2P [38], LFPT5 [39]. Given
172 that EWC and ODG require storing parameters or gradients from past tasks, which is impractical for
173 the full parameter setting of LLMs, we validate these methods using LoRA.

174 4.3.2 Datasets

175 To evaluate a model’s *general ability*, we assess across six key dimensions: **Factual Knowledge:**
176 Using MMLU dataset [40], reporting 5-shot accuracy. **General Reasoning:** Evaluated with BBH [41],
177 reporting EM scores with chain-of-thought prompts with 3-shot in-context examples. **Multilinguality:**
178 Using TyDiQA [42], a multilingual QA benchmark across 11 languages, reporting 0-shot F1 scores.
179 **Commonsense Reasoning:** Assessed with PIQA [43], reporting 0-shot accuracy. **Code Generation:**
180 Using MBPP [44], reporting 0-shot Pass@1. **Reading Comprehension:** Using BoolQ [45], reporting
181 0-shot accuracy.

182 For *instruction-following capability*, we use Self-instruct dataset [46], comprising 175 user-oriented
183 prompts, and the LIMA dataset [47], which assembles 300 prompts from community Q&A and
184 manual examples.

185 To evaluate *safety* changes, we use the CoNa dataset [48], which consists of 178 expert-annotated
186 samples focused on instructions related to hateful speech generation.

	SeqFT			LoRASeqFT			Replay		
	OP	BWT	FWT	OP	BWT	FWT	OP	BWT	FWT
LLaMA2-7B	48.7	-8.3%	2.4%	12.7	-45.7%	0.8%	55.5	2.6%	-0.2%
LLaMA2-13B	<u>49.9</u>	-7.0%	2.5%	28.0	-36.5%	1.5%	56.5	0.4%	2.2%
LLaMA2-70B	-	-	-	45.2	-17.5%	1.7%	<u>56.6</u>	0.4%	1.9%
Vicuna-7B	49.2	-8.4%	1.7%	33.4	-23.7%	0.9%	55.3	0.2%	0.5%
Vicuna-13B	51.2	-5.9%	2.1%	31.6	-28.4%	1.1%	56.9	0.6%	2.4%
Baichuan2-7B	43.4	-15.4%	1.8%	<u>43.8</u>	-9.0%	1.0%	51.7	<u>1.1%</u>	-4.0%
	EWC			OGD			PP		
	OP	BWT	FWT	OP	BWT	FWT	OP	BWT	FWT
LLaMA2-7B	32.3	-20.6%	1.0%	29.7	-22.6%	0.9%	49.2	-0.3%	1.9%
LLaMA2-13B	35.7	-19.7%	<u>1.1%</u>	36.6	-18.6%	0.7%	51.3	-1.1%	2.1%
LLaMA2-70B	-	-	-	-	-	-	54.6	-0.4%	1.7%
Vicuna-7B	<u>37.2</u>	-16.8%	1.3%	<u>39.9</u>	-15.7%	1.6%	50.4	0.2%	1.6%
Vicuna-13B	36.5	-18.6%	<u>1.1%</u>	40.4	-16.7%	0.6%	<u>53.6</u>	-0.6%	<u>2.0%</u>
Baichuan2-7B	44.5	-7.6%	0.8%	44.7	-7.6%	<u>1.1%</u>	46.6	-1.7%	0.9%
	L2P			LFPT5			O-Lora		
	OP	BWT	FWT	OP	BWT	FWT	OP	BWT	FWT
LLaMA2-7B	43.7	-9.5%	2.6%	49.2	-6.7%	1.5%	41.3	-6.2%	1.6%
LLaMA2-13B	46.4	-6.4%	1.6%	50.4	-5.6%	1.1%	43.7	-4.4%	0.7%
LLaMA2-70B	53.2	-1.6%	1.4%	-	-	-	<u>47.7</u>	-5.7%	0.4%
Vicuna-7B	48.6	-9.2%	1.5%	51.6	-7.8%	0.7%	42.6	-6.8%	1.1%
Vicuna-13B	<u>52.4</u>	-4.3%	2.2%	<u>51.2</u>	-6.6%	1.9%	47.9	-3.2%	0.9%
Baichuan2-7B	47.6	-8.6%	0.6%	48.3	-6.7%	<u>1.7%</u>	45.6	-5.4%	<u>1.2%</u>

Table 2: Overall Performance (OP), Forward Transfer (FWT), and Backward Transfer (BWT) for all baseline models and 4 baseline methods.

4.3.3 Implementation Details

In the training phase, we trained models with and without LoRA adapters using 5000 samples at learning rates of $1e-5$ and $1e-4$, respectively. For the testing phase, we use a temperature of 0.1. All our training and inference experiments were conducted on a machine equipped with 8x80G Nvidia A100. All general benchmark evaluations were conducted using the Open-Compass toolkit [49], adopting its default configuration. The detailed settings can be found in Appendix A.

4.4 Main Results

We conducted experiments with various task orders. Results for the default order are presented in the main text, while results for additional orders are detailed in Appendix D.7.

4.4.1 Performance of Target Sequential Tasks

Table 2 showcases the performance of six distinct LLMs on TRACE benchmark, after their continual learning phase. From this evaluation, we can draw the following conclusions:

In-Context Learning (ICL) ICL methods generally perform lower than SeqFT and Replay methods. This suggests that the TRACE benchmark is indeed challenging, and LLMs can’t readily identify solutions just through simple demonstrations.

Replay Performance Among all the baselines, Replay achieved the highest OP score. With its BWT score being positive, it indicates that Replay effectively retains its performance on sequential tasks without significant forgetting. This makes Replay a straightforward and efficient strategy in a continual learning context.

	MMLU (factuality)	GSM (math)	BBH (reasoning)	TydiQA (multilinguality)	BoolQ (comprehension)	PIQA (commonsense)	MBPP (code)	ΔR_t^G
	ACC (5-shot)	EM (8-shot, CoT)	EM (3-shot, CoT)	F1 (1-shot, GP)	ACC (0-shot)	ACC (0-shot)	Pass@1 (0-shot)	
LLaMA-2-7B-Chat	46.56	26.08	40.23	23.47	70.55	76.22	20.4	0
LLaMA-2-7B-Chat-Seq	46.43	3.49	30.11	33.23	77.89	76.5	0	-5.12
LLaMA-2-7B-Chat-LoraSeq	42.28	14.71	33.61	21.72	53.43	75.19	7.4	-7.88
LLaMA-2-7B-Chat-Replay	47.04	3.03	36.61	31.57	75.75	75.3	4.4	-4.26
LLaMA-2-13B-Chat	54.61	43.14	49.70	27.65	81.5	78.24	27.2	0
LLaMA-2-13B-Chat-Seq	41.88	2.12	19.47	32.27	82.08	77.15	1.2	-15.13
LLaMA-2-13B-Chat-LoraSeq	50.63	24.72	38.98	26.93	68.96	78.02	10.4	-9.06
LLaMA-2-13B-Chat-Replay	47.72	2.96	36.52	32.52	82.45	76.88	7.2	-10.83
LLaMA-2-70B-Chat	63.80	59.35	60.81	46.04	88.30	80.60	35.64	0
LLaMA-2-70B-Chat-LoraSeq	60.56	44.79	49.77	43.25	72.15	77.47	16.30	-10.04
LLaMA-2-70B-Chat-Replay	62.48	47.34	52.34	44.12	88.68	77.69	12.57	-7.05
Baichuan2-7B-Instruct	53.80	33.21	35.66	20.64	77.09	74.05	22.4	0
Baichuan2-7B-Instruct-Seq	46.92	4.25	37.45	35.20	79.08	74.21	1.2	-5.5
Baichuan2-7B-Instruct-LoraSeq	52.14	22.74	27.53	30.99	75.23	74.86	8.6	-3.53
Baichuan2-7B-Instruct-Replay	45.72	8.19	35.61	34.65	80.06	72.69	6.4	-4.79
Vicuna-7B-V1.5	51.28	23.65	43.32	22.38	78.56	77.42	12.6	0
Vicuna-7B-V1.5-Seq	49.46	3.87	39.25	33.92	77.74	75.73	1.2	-4.0
Vicuna-7B-V1.5-LoraSeq	48.37	18.89	28.16	25.84	67.24	76.23	0	-7.44
Vicuna-7B-V1.5-Replay	47.20	4.78	39.26	31.86	78.92	80.13	2.0	-4.76
Vicuna-13B-V1.5	56.16	36.09	51.29	24.89	82.45	78.89	2.6	0
Vicuna-13B-V1.5-Seq	37.93	2.81	35.23	36.86	83.43	77.86	0	-8.32
Vicuna-13B-V1.5-LoraSeq	52.46	22.14	41.22	27.86	67.71	77.53	0.4	-6.15
Vicuna-13B-V1.5-Replay	48.73	3.11	42.94	39.60	84.71	77.53	0.6	-0.52

Table 3: Comparison of the general language understanding and reasoning abilities. **blue** means increase, while **red** means decrease.

Full Parameter Training vs. LoRA Full parameter training demonstrates better task-specific adaptability compared to LoRA, with a smaller BWT score. For instance, LLaMA-2-7B-Chat’s SeqFT OP(BWT) is 48.7 (-8.3%), while LoRASeqFT stands at 12.7 (-45.7%). This suggests that when the focus is primarily on sequential tasks, full parameter fine-tuning should be prioritized over parameter-efficient methods like LoRA.

Catastrophic Forgetting in LLaMA-2-70B-Chat Despite achieving a high overall performance (OP) score of 45.2, the llama2-70B-Chat model exhibits significant catastrophic forgetting, as evidenced by its BWT of -17.5%. This substantial decline in retaining previously learned information indicates a vulnerability of larger models to catastrophic forgetting in continual learning scenarios.

4.4.2 Variation of General Ability

Table 3 presents the evaluations of various LLM models concerning general abilities. The degree of general ability forgetting in LLMs can be analyzed from three perspectives.

From the Model Perspective 1) Nearly all models display a negative General Ability Delta, indicating a general decline in overall capabilities after continual learning. 2) Both larger and smaller models experience significant forgetting in general abilities. For instance, the General Ability Delta for llama2-7B-chat-LoraSeq stands at -7.88, whereas llama2-70B-chat-LoraSeq is -10.04.

From the Task Perspective 1) Despite the presence of CoT prompts, all models show a noticeable decline in math and reasoning abilities, highlighting their sensitivity to new task learning. 2) Excluding the llama2-7b model, most models exhibit a significant drop in performance on MMLU, suggesting a gradual loss of factual knowledge through continual learning. 3) TydiQA task sees a general boost post-training, possibly due to the inclusion of Chinese and German datasets in our sequential tasks. Intriguingly, other languages on TydiQA also show enhancements and declines, suggesting potential cross-linguistic transfer effects. 4) Performance shifts on PIQA for most models are subtle, indicating the relative robustness of commonsense knowledge during continual learning.

From the Method Perspective 1) The Replay method proves beneficial in preserving reasoning and factuality skills. Especially for larger models, the mitigation of forgetting through Replay is more pronounced. For instance, for LLaMA-2-7B-Chat, Replay offers a 6.5 EM score boost compared to methods without Replay, while for LLaMA-2-13B-Chat, the increase is 17.1 EM score.

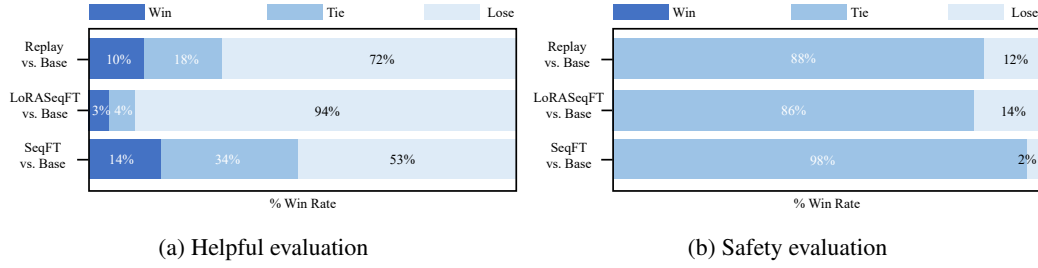


Figure 2: GPT-4 evaluation with llama-13b-chat, comparing 3 different baselines (Replay, LoRA and Sequential) to the base model across tasks including helpful and safety.

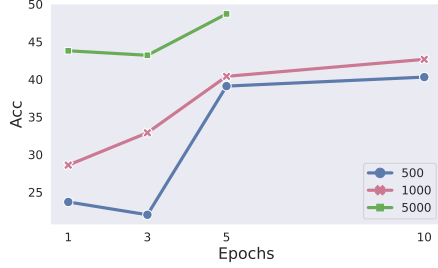


Figure 3: Performance evaluation of LLaMA-2-7B-Chat's SeqFT on TRACE benchmark across varying sample sizes (500, 1000, 5000) and training epochs (1, 3, 5, 10 (except for 5000)).

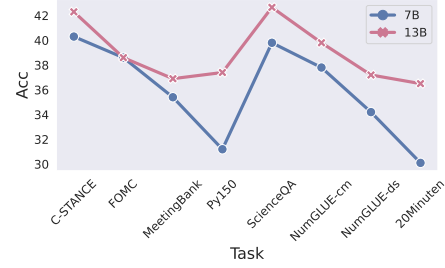


Figure 4: Evolution of LLMs' reasoning capabilities post-training, measured using the BBH metric. Results for LLaMA-2-7B-chat and LLaMA-2-13B-chat are reported.

4.4.3 Instruction Following Ability Analysis

We evaluate the instruction-following ability of LLMs based on LLaMA-2-7B-Chat and LLaMA-2-13B-Chat. Figure 2 (a) illustrates the win rate % for instruction following sequentially trained LLMs and their original versions. Here, the win rate can be approximated as an indicator for the Instruction-following delta. All three training methods show a significant decline in instruction-following capabilities, with the most pronounced decline in the LoRA method. Therefore, be cautious when exploring approaches like LoRA for continual learning in LLMs.

4.4.4 Safety Analysis

We test the safety of answers from models LLaMA-2-7B-Chat and LLaMA-2-13B-Chat. Figure 2 (b) shows the win rate % for instruction following between the new LLMs and their starting versions. Here, the win rate can be used as a measure for the Safety Delta. Compared to the original models, most answers were rated as 'Tie'. This suggests that the safety of the model's answers is largely unaffected by continual learning on general tasks.

4.5 Ablation Study

Data Quantity & Training Steps. Figure 3 shows the impact of data volumes and training steps on target task performance. For LLaMA-2-7B-Chat's SeqFT, we tested with 500, 1000, and 5000 samples from each dataset, training for 1, 3, 5, 10 epochs. Results indicate performance improves with more data, with optimal results at 5000 samples. Furthermore, up to 5 epochs improve performance, aligning with our baseline for balancing task optimization and capabilities retention.

Decoupling the Impact of Different Tasks. Results from section 4.4.2 reveal a notable decline in reasoning and mathematical skills after training on our benchmark. This brings forth the question: *How exactly does the reasoning capability of LLMs transform during the continual learning process?* Figure 4 tracks the reasoning ability (assessed via BBH performance) after the completion of each training task. Interestingly, the model's reasoning skill improves after the ScienceQA task but declines for others. Unlike NumGLUE tasks, which lack clear reasoning paths, ScienceQA provides explicit reasoning paths in its answers, indicating that including reasoning paths in training may benefit the model's reasoning skills.

4.6 Reasoning-augmented Continual learning

Why do LLMs underperform on the TRACE benchmark, both in target tasks and maintaining inherent capabilities? Two likely reasons: First, neural networks tend to overfit the specific output formats of new tasks [50]. Second, as most tasks involve direct result prediction, LLMs may learn shortcuts [51] within the training data, limiting their ability to generalize to new data.

With these insights and our experimental findings in 4.5, we propose the Reasoning-augmented Continual Learning (RCL) method. As depicted in Figure 5, RCL involves two phases: automated reasoning annotation and sequential training on the augmented datasets. GPT-4 generates reasoning paths for all entries, based on prompts designed by domain experts for each task. These are then validated against the ground truth. Manual inspection of a 100-sample subset results in a 94% approval rate, demonstrating GPT-4’s reliability. Following this, supervised training is conducted on the target LLM, keeping hyperparameter settings consistent with baselines.

4.6.1 Performance on Sequential Tasks

Table 4 provides comparisons of the performance of RCL against other baselines. Through an ablation study contrasting single-task training (SingleFT) with multi-task training, and assessing the impact of reasoning-augmented data, we observed that integrating reasoning pathways consistently boosts performance over the original dataset. Our approach yields results comparable to the SeqFT method using only 500 samples instead of 5000. By utilizing fewer datasets and training steps, our method also helps preserve the inherent capabilities of LLMs more effectively.

Methods	OP	BWT	FWT
EWC	32.3	−20.6%	1.0%
OGD	29.7	−22.6%	0.9%
L2P	43.7	−9.5%	2.6%
LFPT5	49.2	−6.7%	1.5%
PP	49.2	−0.3%	1.9%
O-Lora	41.3	−6.2%	1.6%
ICL	39.5	-	-
ICL+Re	41.1	-	-
SeqFT(0.5k)	23.0	−19%	0.3%
RCL(0.5k)	46.6	−13%	2.7%
SeqFT(5k)	48.7	−8.3%	2.4%
RCL(5k)	51.9	−6.5%	3.2%
SingleFT	57.6	-	-
SingleFT+Re	58.1	-	-
MT w/o. Re	52.3	-	-
MT w. Re	58.2	-	-

4.6.2 Original Performance Retention

Impacts on General Ability Figure 6 shows RCL’s performance on general abilities matches SeqFT and Replay on MMLU, TydiQA, BoolQA, and PIQA. Yet, RCL excels in reasoning tasks like GSM and BBH, where it surpasses SeqFT and Replay by 12.7 and 13.2 points, respectively. This highlights RCL’s effectiveness in enhancing reasoning skills through reasoning paths. Additionally, combining RCL with replay boosts its reasoning task performance.

Table 4: Comparison of RCL with different baselines. **Single FT** refers to fine-tuning the model on a single task, **Re** refers to reasoning-augmented, and **MT** refers to Multi-task training.

Impacts on Instruction-Following The impact of incorporating RCL on instruction-following capabilities is presented in Table 5. It’s evident that RCL enhances the model’s ability to follow instructions by 8% and 5% compared to SeqFT and Replay, respectively.

5 Conclusion

Existing continual learning benchmarks are insufficient in thoroughly evaluating LLMs, due to their oversimplification and lack of key metrics like instruction following and safety. To tackle this, we introduce TRACE, a comprehensive benchmark with eight challenging tasks and well-rounded metrics. Our experiments show that for LLMs, catastrophic forgetting remains, and a clear drop in general abilities is observed during continual learning. Besides, our RCL method highlights the importance of using reasoning in training while alleviating the above phenomena. We believe this area is crucial and hope our work serves as a foundation for future research.

6 Limitations

While our proposed TRACE benchmark covers a variety of tasks, expanding it to include real-time interaction and multi-modal integration could provide a more comprehensive assessment of LLM capabilities. Additionally, future versions should aim to minimize any potential biases introduced by the current task selection or dataset composition, ensuring a more balanced and comprehensive representation of tasks that better reflect diverse real-world applications.

References

- [1] OpenAI. Gpt-4 technical report. *ArXiv*, abs/2303.08774, 2023.
- [2] Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, et al. Llama: Open and efficient foundation language models. *arXiv preprint arXiv:2302.13971*, 2023.
- [3] Shijie Wu, Ozan Irsoy, Steven Lu, Vadim Dabravolski, Mark Dredze, Sebastian Gehrmann, Prabhanjan Kambadur, David Rosenberg, and Gideon Mann. Bloomberggpt: A large language model for finance. *arXiv preprint arXiv:2303.17564*, 2023.
- [4] Raymond Li, Loubna Ben Allal, Yangtian Zi, Niklas Muennighoff, Denis Kocetkov, Chenghao Mou, Marc Marone, Christopher Akiki, Jia Li, Jenny Chim, et al. Starcoder: may the source be with you! *arXiv preprint arXiv:2305.06161*, 2023.
- [5] Yuzhen Huang, Yuzhuo Bai, Zhihao Zhu, Junlei Zhang, Jinghan Zhang, Tangjun Su, Junteng Liu, Chuancheng Lv, Yikai Zhang, Jiayi Lei, et al. C-eval: A multi-level multi-discipline chinese evaluation suite for foundation models. *arXiv preprint arXiv:2305.08322*, 2023.
- [6] Nigar M Shafiq Surameery and Mohammed Y Shakor. Use chat gpt to solve programming bugs. *International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290*, 3(01):17–22, 2023.
- [7] Yujia Qin, Shi Liang, Yining Ye, Kunlun Zhu, Lan Yan, Ya-Ting Lu, Yankai Lin, Xin Cong, Xiangru Tang, Bill Qian, Sihan Zhao, Runchu Tian, Ruobing Xie, Jie Zhou, Marc H. Gerstein, Dahai Li, Zhiyuan Liu, and Maosong Sun. Toolllm: Facilitating large language models to master 16000+ real-world apis. *ArXiv*, abs/2307.16789, 2023.
- [8] Liyuan Wang, Xingxing Zhang, Hang Su, and Jun Zhu. A comprehensive survey of continual learning: Theory, method and application. *ArXiv*, abs/2302.00487, 2023.
- [9] Michael McCloskey and Neal J Cohen. Catastrophic interference in connectionist networks: The sequential learning problem. In *Psychology of learning and motivation*, volume 24, pages 109–165. Elsevier, 1989.
- [10] Xiang Zhang, Junbo Jake Zhao, and Yann LeCun. Character-level convolutional networks for text classification. In *NIPS*, 2015.
- [11] Thomas Scialom, Tuhin Chakrabarty, and Smaranda Muresan. Fine-tuned language models are continual learners. In *Conference on Empirical Methods in Natural Language Processing*, 2022.
- [12] Anastasia Razdaibiedina, Yuning Mao, Rui Hou, Madian Khabsa, Mike Lewis, and Amjad Almahairi. Progressive prompts: Continual learning for language models. In *The Eleventh International Conference on Learning Representations*, 2023.
- [13] David Lopez-Paz and Marc’Aurelio Ranzato. Gradient episodic memory for continual learning. *Advances in neural information processing systems*, 30, 2017.
- [14] Cyprien de Masson D’Autume, Sebastian Ruder, Lingpeng Kong, and Dani Yogatama. Episodic memory in lifelong language learning. *Advances in Neural Information Processing Systems*, 32, 2019.
- [15] James Kirkpatrick, Razvan Pascanu, Neil Rabinowitz, Joel Veness, Guillaume Desjardins, Andrei A Rusu, Kieran Milan, John Quan, Tiago Ramalho, Agnieszka Grabska-Barwinska, et al. Overcoming catastrophic forgetting in neural networks. *Proceedings of the national academy of sciences*, 114(13):3521–3526, 2017.
- [16] James Seale Smith, Yen-Chang Hsu, Lingyu Zhang, Ting Hua, Zsolt Kira, Yilin Shen, and Hongxia Jin. Continual diffusion: Continual customization of text-to-image diffusion with c-lora. *arXiv preprint arXiv:2304.06027*, 2023.
- [17] Xiao Wang, Tianze Chen, Qiming Ge, Han Xia, Rong Bao, Rui Zheng, Qi Zhang, Tao Gui, and Xuanjing Huang. Orthogonal subspace learning for language model continual learning, 2023.

- [18] Zhicheng Wang, Yufang Liu, Tao Ji, Xiaoling Wang, Yuanbin Wu, Congcong Jiang, Ye Chao, Zhencong Han, Ling Wang, Xu Shao, and Wenqiu Zeng. Rehearsal-free continual language learning via efficient parameter isolation. *ArXiv*, 2023.
- [19] Alex Wang, Amanpreet Singh, Julian Michael, Felix Hill, Omer Levy, and Samuel R Bowman. Glue: A multi-task benchmark and analysis platform for natural language understanding. *arXiv preprint arXiv:1804.07461*, 2018.
- [20] Alex Wang, Yada Pruksachatkun, Nikita Nangia, Amanpreet Singh, Julian Michael, Felix Hill, Omer Levy, and Samuel Bowman. Superglue: A stickier benchmark for general-purpose language understanding systems. *Advances in neural information processing systems*, 32, 2019.
- [21] Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, A. Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In *Annual Meeting of the Association for Computational Linguistics*, 2011.
- [22] Zixuan Ke and Bin Liu. Continual learning of natural language processing tasks: A survey. *ArXiv*, abs/2211.12701, 2022.
- [23] Arslan Chaudhry, Puneet K Dokania, Thalaiyasingam Ajanthan, and Philip HS Torr. Riemannian walk for incremental learning: Understanding forgetting and intransigence. In *Proceedings of the European conference on computer vision (ECCV)*, pages 532–547, 2018.
- [24] Pan Lu, Swaroop Mishra, Tony Xia, Liang Qiu, Kai-Wei Chang, Song-Chun Zhu, Oyvind Tafjord, Peter Clark, and Ashwin Kalyan. Learn to explain: Multimodal reasoning via thought chains for science question answering, 2022.
- [25] Agam Shah, Suvan Paturi, and Sudheer Chava. Trillion dollar words: A new financial dataset, task & market analysis, 2023.
- [26] Yebowen Hu, Tim Ganter, Hanieh Deilamsalehy, Franck Dernoncourt, Hassan Foroosh, and Fei Liu. Meetingbank: A benchmark dataset for meeting summarization, 2023.
- [27] Chenye Zhao, Yingjie Li, and Cornelia Caragea. C-STANCE: A large dataset for Chinese zero-shot stance detection. In *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 13369–13385, Toronto, Canada, July 2023. Association for Computational Linguistics.
- [28] Annette Rios, Nicolas Spring, Tannon Kew, Marek Kostrzewa, Andreas Säuberli, Mathias Müller, and Sarah Ebling. A new dataset and efficient baselines for document-level text simplification in German. In *Proceedings of the Third Workshop on New Frontiers in Summarization*, pages 152–161, Online and in Dominican Republic, November 2021. Association for Computational Linguistics.
- [29] Yushi Bai, Xin Lv, Jiajie Zhang, Hongchang Lyu, Jiankai Tang, Zhidian Huang, Zhengxiao Du, Xiao Liu, Aohan Zeng, Lei Hou, Yuxiao Dong, Jie Tang, and Juanzi Li. Longbench: A bilingual, multitask benchmark for long context understanding, 2023.
- [30] Shuai Lu, Daya Guo, Shuo Ren, Junjie Huang, Alexey Svyatkovskiy, Ambrosio Blanco, Colin Clement, Dawn Drain, Daxin Jiang, Duyu Tang, Ge Li, Lidong Zhou, Linjun Shou, Long Zhou, Michele Tufano, Ming Gong, Ming Zhou, Nan Duan, Neel Sundaresan, Shao Kun Deng, Shengyu Fu, and Shujie Liu. Codexglue: A machine learning benchmark dataset for code understanding and generation, 2021.
- [31] Swaroop Mishra, Arindam Mitra, Neeraj Varshney, Bhavdeep Sachdeva, Peter Clark, Chitta Baral, and Ashwin Kalyan. Numglue: A suite of fundamental yet challenging mathematical reasoning tasks, 2022.
- [32] Baichuan. Baichuan 2: Open large-scale language models. *arXiv preprint arXiv:2309.10305*, 2023.
- [33] Wei-Lin Chiang, Zhuohan Li, Zi Lin, Ying Sheng, Zhanghao Wu, Hao Zhang, Lianmin Zheng, Siyuan Zhuang, Yonghao Zhuang, Joseph E. Gonzalez, Ion Stoica, and Eric P. Xing. Vicuna: An open-source chatbot impressing gpt-4 with 90%* chatgpt quality, March 2023.

- [34] J. Edward Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yanzhi Li, Shean Wang, and Weizhu Chen. Lora: Low-rank adaptation of large language models. *ArXiv*, abs/2106.09685, 2021.
- [35] Lei Liu and J. Huang. Prompt learning to mitigate catastrophic forgetting in cross-lingual transfer for open-domain dialogue generation. *Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2023.
- [36] Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, T. J. Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeff Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. Language models are few-shot learners. *ArXiv*, abs/2005.14165, 2020.
- [37] Mehrdad Farajtabar, Navid Azizan, Alex Mott, and Ang Li. Orthogonal gradient descent for continual learning. In *International Conference on Artificial Intelligence and Statistics*, pages 3762–3773. PMLR, 2020.
- [38] Zifeng Wang, Zizhao Zhang, Chen-Yu Lee, Han Zhang, Ruoxi Sun, Xiaoqi Ren, Guolong Su, Vincent Perot, Jennifer Dy, and Tomas Pfister. Learning to prompt for continual learning, 2022.
- [39] Chengwei Qin and Shafiq Joty. Lfpt5: A unified framework for lifelong few-shot language learning based on prompt tuning of t5, 2022.
- [40] 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*, 2020.
- [41] Mirac Suzgun, Nathan Scales, Nathanael Schärli, Sebastian Gehrmann, Yi Tay, Hyung Won Chung, Aakanksha Chowdhery, Quoc V Le, Ed H Chi, Denny Zhou, et al. Challenging big-bench tasks and whether chain-of-thought can solve them. *arXiv preprint arXiv:2210.09261*, 2022.
- [42] Jonathan H Clark, Eunsol Choi, Michael Collins, Dan Garrette, Tom Kwiatkowski, Vitaly Nikolaev, and Jennimaria Palomaki. Tydi qa: A benchmark for information-seeking question answering in typologically diverse languages. *Transactions of the Association for Computational Linguistics*, 8:454–470, 2020.
- [43] Yonatan Bisk, Rowan Zellers, Jianfeng Gao, Yejin Choi, et al. Piqa: Reasoning about physical commonsense in natural language. In *Proceedings of the AAAI conference on artificial intelligence*, volume 34, pages 7432–7439, 2020.
- [44] Jacob Austin, Augustus Odena, Maxwell Nye, Maarten Bosma, Henryk Michalewski, David Dohan, Ellen Jiang, Carrie J. Cai, Michael Terry, Quoc V. Le, and Charles Sutton. Program synthesis with large language models. *ArXiv*, abs/2108.07732, 2021.
- [45] Christopher Clark, Kenton Lee, Ming-Wei Chang, Tom Kwiatkowski, Michael Collins, and Kristina Toutanova. Boolq: Exploring the surprising difficulty of natural yes/no questions. *arXiv preprint arXiv:1905.10044*, 2019.
- [46] Yizhong Wang, Yeganeh Kordi, Swaroop Mishra, Alisa Liu, Noah A Smith, Daniel Khashabi, and Hannaneh Hajishirzi. Self-instruct: Aligning language model with self generated instructions. *arXiv preprint arXiv:2212.10560*, 2022.
- [47] Chunting Zhou, Pengfei Liu, Puxin Xu, Srini Iyer, Jiao Sun, Yuning Mao, Xuezhe Ma, Avia Efrat, Ping Yu, Lili Yu, et al. Lima: Less is more for alignment. *arXiv preprint arXiv:2305.11206*, 2023.
- [48] Federico Bianchi, Mirac Suzgun, Giuseppe Attanasio, Paul Röttger, Dan Jurafsky, Tatsunori Hashimoto, and James Zou. Safety-tuned llamas: Lessons from improving the safety of large language models that follow instructions. *arXiv preprint arXiv:2309.07875*, 2023.

- [49] OpenCompass Contributors. Opencompass: A universal evaluation platform for foundation models. <https://github.com/open-compass/opencompass>, 2023.
- [50] Yihan Wang, Si Si, Daliang Li, Michal Lukasik, Felix Yu, Cho-Jui Hsieh, Inderjit S Dhillon, and Sanjiv Kumar. Preserving in-context learning ability in large language model fine-tuning. *arXiv preprint arXiv:2211.00635*, 2022.
- [51] Xiao Wang, Shihan Dou, Limao Xiong, Yicheng Zou, Qi Zhang, Tao Gui, Liang Qiao, Zhanzhan Cheng, and Xuan-Jing Huang. Miner: Improving out-of-vocabulary named entity recognition from an information theoretic perspective. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 5590–5600, 2022.
- [52] Lianmin Zheng, Wei-Lin Chiang, Ying Sheng, Siyuan Zhuang, Zhanghao Wu, Yonghao Zhuang, Zi Lin, Zhuohan Li, Dacheng Li, Eric Xing, et al. Judging llm-as-a-judge with mt-bench and chatbot arena. *arXiv preprint arXiv:2306.05685*, 2023.
- [53] Yann Dubois, Xuechen Li, Rohan Taori, Tianyi Zhang, Ishaan Gulrajani, Jimmy Ba, Carlos Guestrin, Percy Liang, and Tatsunori B Hashimoto. AlpacaFarm: A simulation framework for methods that learn from human feedback. *arXiv preprint arXiv:2305.14387*, 2023.

Appendices

A Implementation Details

During the training phase, for the baselines without LoRA adapters, we consistently trained with 5000 samples with a constant learning rate of $1e-5$. For the datasets we used (C-STANCE, FOMC, MeetingBank, Py150, ScienceQA, NumGLUE-cm, NumGLUE-ds, 20Minuten), we train for 1, 1, 5, 5, 1, 5, 5, 5 epochs respectively. While for the baselines with LoRA adapters, we trained with 5000 samples with a constant learning rate of $1e-4$ for 5, 3, 7, 5, 3, 5, 5, 7 epochs respectively. Our training settings incorporated a weight decay set to 0, and a batch size of 128. For the testing phase, we use a temperature of 0.1. All our training and inference experiments were conducted on a machine equipped with 8x80G Nvidia A100, and were implemented using DeepSpeed repository. All models are trained on 8 A100 GPUs with 80G memory with full parameters fine-tuning. All general benchmark evaluations were conducted using the Open-Compass toolkit [49], adopting its default configuration.

B Trace dataset statistics

In this section, we represent the overview of dataset statistics, including source, average length, metric, language, and number of samples of each dataset in the TRACE benchmark. We demonstrate the dataset details in Table 1.

C Reasoning-based Continual Learning

Figure 5 shows an overview of our reasoning-augmented continual learning method. Table 5 and Figure 6 shows the results of RCL in preserving the instruction-following abilities and general abilities, respectively.

	Win	Tie	Loss
SeqFT	12%	30%	58%
Replay	15%	31%	55%
RCL	20%	30%	50%

Table 5: Instruction-following abilities of SeqFT, Replay and RCL. The model we use is LLaMA-2-7b-Chat.

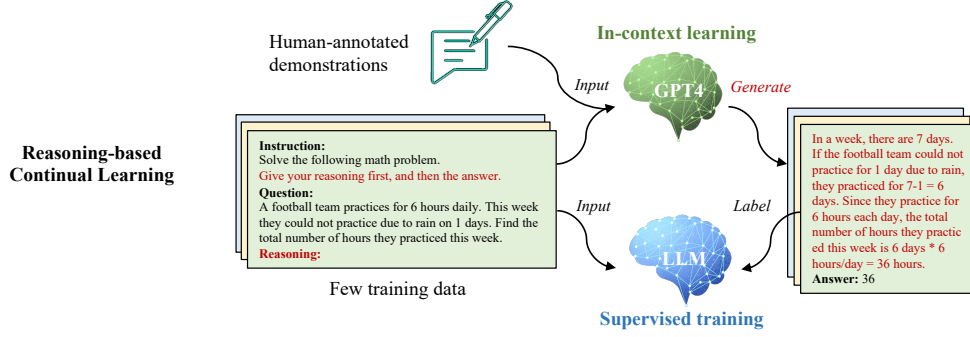


Figure 5: An overview of Reasoning-augmented continual learning. The strategy involves two stages: 1) Automatically annotating sample reasoning paths using GPT-4. 2) Continual learning on augmented datasets.

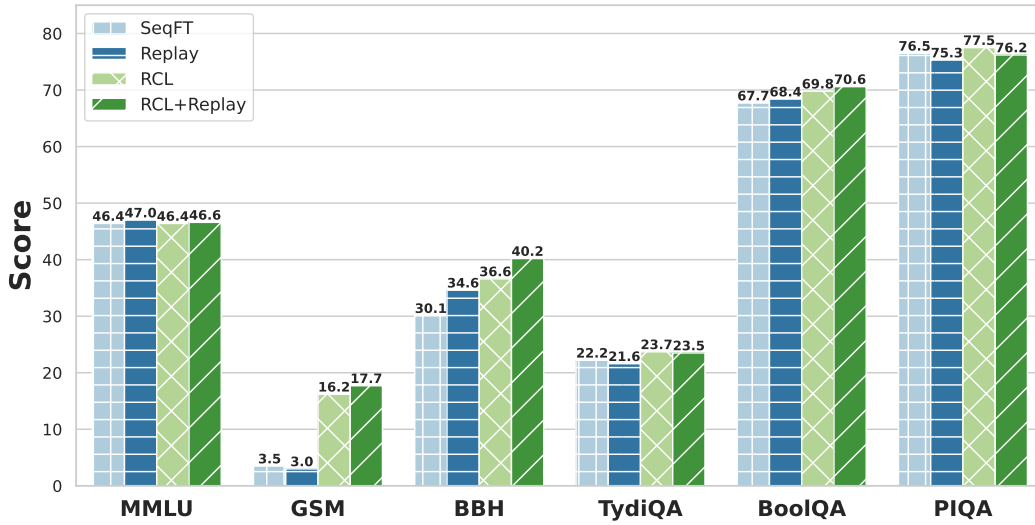


Figure 6: OpenCompass Evaluation Results. **RCL+Replay** refers to combining our RCL method with replay method. The model we use is LLaMA-2-7b-Chat.

D Detailed Experiments Results

In this section, we report the detailed experiment results in our paper. The model includes Baichuan-7b, LLaMA2-7b-chat, LLaMA2-13b-chat, LLaMA2-70b-chat, Vicuna-7b and Vicuna-13b. The results are shown in Table 6 - 25.

D.1 In-Context Learning

Table 6 represents the performance of different models with in-context learning.

D.2 SeqFT method

Table 7 - 12 shows the detailed performance of different models of each round during the continual learning. SeqFT represents sequential fine-tuning.

Task/Model	Baichuan-7b	LLaMA2-7b-chat	LLaMA2-13b-chat	LLaMA2-70b-chat	Vicuna-7b	Vicuna-13b
C-STANCE	0.58	0.4	0.366	0.45	0.403	0.57
FOMC	0.63	0.483	0.519	0.567	0.551	0.61
MeetingBank	0.225	0.198	0.221	0.345	0.223	0.229
Py150	0.586	0.522	0.539	0.577	0.529	0.585
ScienceQA	0.68	0.628	0.689	0.724	0.695	0.7
NumGLUE-cm	0.271	0.284	0.407	0.436	0.284	0.347
NumGLUE-ds	0.23	0.203	0.218	0.376	0.302	0.33
20Minuten	0.366	0.395	0.395	0.395	0.392	0.378
average	0.446	0.389	0.419	0.484	0.422	0.469

Table 6: Detailed results of in-context learning of different large language models.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.62	0.629	0.663	0.621	0.531	0.55	0.588	0.579
FOMC	-	0.681	0.353	0.318	0.02	0.363	0.347	0.335
MeetingBank	-	-	0.442	0.351	0.371	0.379	0.389	0.364
Py150	-	-	-	0.626	0.562	0.586	0.589	0.58
ScienceQA	-	-	-	-	0.77	0.68	0.5	0.44
NumGLUE-cm	-	-	-	-	-	0.358	0.247	0.284
NumGLUE-ds	-	-	-	-	-	-	0.64	0.475
20Minuten	-	-	-	-	-	-	-	0.415
average								0.434
BWT								-0.154
FWT								0.018

Table 7: Detailed results of sequential fine-tuning of Baichuan-7b.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.5	0.456	0.448	0.453	0.435	0.442	0.436	0.454
FOMC	0.54	0.735	0.67	0.658	0	0.595	0.577	0.609
MeetingBank	0.172	0.098	0.523	0.459	0.433	0.446	0.442	0.457
Py150	0.218	0.282	0.185	0.58	0.459	0.509	0.508	0.512
ScienceQA	0.12	0.13	0.15	0.17	0.764	0.636	0.45	0.637
NumGLUE-cm	0.173	0.012	0.074	0.062	0	0.383	0.247	0.272
NumGLUE-ds	0.1	0	0.04	0.11	0	0.03	0.582	0.548
20Minuten	0.022	0.021	0.018	0.024	0.017	0.019	0.017	0.408
average								0.487
BWT								-0.083
FWT								0.024

Table 8: Detailed results of sequential fine-tuning of LLaMA-7b-chat.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.469	0.465	0.47	0.477	0.463	0.466	0.45	0.5
FOMC	0.587	0.754	0.738	0.748	0.03	0.721	0.71	0.717
MeetingBank	0.232	0.165	0.533	0.51	0.375	0.421	0.385	0.351
Py150	0.246	0.265	0.213	0.568	0.538	0.537	0.541	0.547
ScienceQA	0.223	0.256	0.197	0.244	0.8	0.655	0.241	0.55
NumGLUE-cm	0.198	0.121	0.089	0	0	0.333	0.284	0.296
NumGLUE-ds	0.156	0.034	0	0.045	0	0.245	0.618	0.622
20Minuten	0.032	0.034	0.026	0.024	0.025	0.034	0.018	0.408
average								0.499
BWT								-0.07
FWT								0.025

Table 9: Detailed results of sequential fine-tuning of LLaMA-13b-chat.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.56	0.45	0.45	0.42	0.42	0.44	0.48	0.49
FOMC	-	0.75	0.53	0.53	0	0.72	0.72	0.38
MeetingBank	-	-	0.427	0.233	0.255	0.231	0.245	0.226
Py150	-	-	-	0.617	0.578	0.565	0.589	0.579
ScienceQA	-	-	-	-	0.1	0	0	0
NumGLUE-cm	-	-	-	-	-	0.32	0.197	0.197
NumGLUE-ds	-	-	-	-	-	-	0.66	0.37
20Minuten	-	-	-	-	-	-	-	0.188
average								0.303
BWT								-0.17
FWT								0.005

Table 10: Detailed results of sequential fine-tuning of LLaMA-7b.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.532	0.451	0.439	0.448	0.149	0.477	0.47	0.476
FOMC	-	0.738	0.732	0.744	0	0.605	0.567	0.675
MeetingBank	-	-	0.519	0.447	0.443	0.427	0.417	0.439
Py150	-	-	-	0.577	0.384	0.486	0.482	0.482
ScienceQA	-	-	-	-	0.773	0.7	0.608	0.649
NumGLUE-cm	-	-	-	-	-	0.407	0.247	0.296
NumGLUE-ds	-	-	-	-	-	-	0.578	0.517
20Minuten	-	-	-	-	-	-	-	0.403
average								0.492
BWT								-0.084
FWT								0.017

Table 11: Detailed results of sequential fine-tuning of Vicuna-7b.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.527	0.43	0.471	0.497	0.374	0.468	0.469	0.484
FOMC	-	0.741	0.739	0.731	0	0.754	0.678	0.714
MeetingBank	-	-	0.549	0.532	0.53	0.491	0.427	0.412
Py150	-	-	-	0.564	0.54	0.546	0.538	0.552
ScienceQA	-	-	-	-	0.79	0.616	0.586	0.633
NumGLUE-cm	-	-	-	-	-	0.346	0.309	0.358
NumGLUE-ds	-	-	-	-	-	-	0.622	0.572
20Minuten	-	-	-	-	-	-	-	0.41
average								0.517
BWT								-0.059
FWT								0.021

Table 12: Detailed results of sequential fine-tuning of Vicuna-13b.

501 D.3 SeqLoraFT method

502 Table 13 - 18 shows the detailed performance of different models of each round during the continual learning. SeqLoRAFT represents sequential fine-tuning with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.613	0.601	0.597	0.584	0.506	0.504	0.53	0.477
FOMC	-	0.652	0.604	0.591	0.602	0.588	0.587	0.417
MeetingBank	-	-	0.345	0.334	0.333	0.343	0.34	0.337
Py150	-	-	-	0.588	0.472	0.539	0.517	0.472
ScienceQA	-	-	-	-	0.641	0.68	0.625	0.63
NumGLUE-cm	-	-	-	-	-	0.457	0.432	0.407
NumGLUE-ds	-	-	-	-	-	-	0.43	0.36
20Minuten	-	-	-	-	-	-	-	0.407
average								0.438
BWT								-0.090
FWT								0.01

Table 13: Detailed results of sequential fine-tuning of Baichuan-7b with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.511	0.45	0.412	0.373	0.133	0.391	0.294	0.277
FOMC	-	0.713	0.55	0.452	0	0.421	0.341	0.24
MeetingBank	-	-	0.51	0.212	0.151	0.067	0.037	0.121
Py150	-	-	-	0.578	0.004	0.495	0.452	0.004
ScienceQA	-	-	-	-	0.68	0.645	0.535	0
NumGLUE-cm	-	-	-	-	-	0.37	0.235	0
NumGLUE-ds	-	-	-	-	-	-	0.486	0
20Minuten	-	-	-	-	-	-	-	0.37
average								0.127
BWT								-0.457
FWT								0.008

Table 14: Detailed results of sequential fine-tuning of LLaMA-7b-chat with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.62	0.36	0.432	0.491	0.18	0.42	0.411	0.124
FOMC	-	0.743	0.681	0.63	0.53	0.605	0.579	0
MeetingBank	-	-	0.484	0.264	0.201	0.147	0.032	0.122
Py150	-	-	-	0.581	0.397	0.488	0.497	0.249
ScienceQA	-	-	-	-	0.75	0.729	0.714	0.68
NumGLUE-cm	-	-	-	-	-	0.58	0.296	0.259
NumGLUE-ds	-	-	-	-	-	-	0.62	0.386
20Minuten	-	-	-	-	-	-	-	0.417
average								0.28
BWT								-0.365
FWT								0.015

Table 15: Detailed results of sequential fine-tuning of LLaMA-13b with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.53	0.498	0.422	0.49	0.04	0.44	0.457	0.228
FOMC	-	0.641	0.532	0.66	0.01	0.64	0.67	0.19
MeetingBank	-	-	0.528	0.22	0.21	0.146	0.264	0.181
Py150	-	-	-	0.633	0.346	0.651	0.671	0.595
ScienceQA	-	-	-	-	0.81	0.79	0.89	0.805
NumGLUE-cm	-	-	-	-	-	0.543	0.531	0.518
NumGLUE-ds	-	-	-	-	-	-	0.74	0.68
20Minuten	-	-	-	-	-	-	-	0.42
average								0.452
BWT								-0.175
FWT								0.015

Table 16: Detailed results of sequential fine-tuning of LLaMA-70b with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.514	0.452	0.433	0.446	0	0.344	0.089	0.141
FOMC	-	0.715	0.48	0.427	0	0.272	0.304	0.29
MeetingBank	-	-	0.5	0.113	0.144	0.026	0.011	0.07
Py150	-	-	-	0.573	0.222	0.47	0.452	0.413
ScienceQA	-	-	-	-	0.67	0.632	0.53	0.6
NumGLUE-cm	-	-	-	-	-	0.407	0.37	0.259
NumGLUE-ds	-	-	-	-	-	-	0.545	0.492
20Minuten	-	-	-	-	-	-	-	0.409
average								0.334
BWT								-0.237
FWT								0.009

Table 17: Detailed results of sequential fine-tuning of Vicuna-7b with LoRA adapters.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.524	0.504	0.394	0.385	0.389	0.347	0.329	0.07
FOMC	-	0.74	0.68	0.616	0.188	0.62	0.438	0.04
MeetingBank	-	-	0.495	0.24	0.157	0.132	0.08	0.14
Py150	-	-	-	0.6	0.368	0.52	0.491	0.256
ScienceQA	-	-	-	-	0.77	0.75	0.732	0.74
NumGLUE-cm	-	-	-	-	-	0.407	0.346	0.346
NumGLUE-ds	-	-	-	-	-	-	0.569	0.52
20Minuten	-	-	-	-	-	-	-	0.413
average								0.316
BWT								-0.284
FWT								0.011

Table 18: Detailed results of sequential fine-tuning of Vicuna-13b with LoRA adapters.

504 D.4 Replay method

505 Table 19 - 24 shows the detailed performance of different models of each round during the continual
506 learning with replay data.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.57	0.55	0.56	0.63	0.6	0.64	0.62	0.61
FOMC	-	0.69	0.64	0.64	0.65	0.65	0.66	0.61
MeetingBank	-	-	0.445	0.457	0.449	0.466	0.461	0.482
Py150	-	-	-	0.546	0.577	0.577	0.613	0.583
ScienceQA	-	-	-	-	0.58	0.51	0.54	0.57
NumGLUE-cm	-	-	-	-	-	0.321	0.346	0.333
NumGLUE-ds	-	-	-	-	-	-	0.5	0.55
20Minuten	-	-	-	-	-	-	-	0.405
average								0.517
BWT								0.011
FWT								-0.04

Table 19: Detailed results of continual learning of Baichuan-7b with replay data.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.471	0.487	0.485	0.5	0.486	0.475	0.493	0.5
FOMC	-	0.734	0.769	0.785	0.807	0.781	0.785	0.8
MeetingBank	-	-	0.499	0.496	0.507	0.494	0.492	0.51
Py150	-	-	-	0.543	0.561	0.546	0.552	0.55
ScienceQA	-	-	-	-	0.763	0.78	0.78	0.785
NumGLUE-cm	-	-	-	-	-	0.358	0.309	0.37
NumGLUE-ds	-	-	-	-	-	-	0.486	0.52
20Minuten	-	-	-	-	-	-	-	0.406
average								0.555
BWT								0.026
FWT								-0.002

Table 20: Detailed results of continual learning of LLaMA-7b-chat with replay data.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.5	0.496	0.497	0.493	0.52	0.503	0.5	0.51
FOMC	-	0.778	0.803	0.805	0.792	0.789	0.785	0.813
MeetingBank	-	-	0.484	0.495	0.515	0.499	0.503	0.482
Py150	-	-	-	0.523	0.549	0.532	0.534	0.523
ScienceQA	-	-	-	-	0.816	0.8	0.804	0.792
NumGLUE-cm	-	-	-	-	-	0.358	0.407	0.396
NumGLUE-ds	-	-	-	-	-	-	0.628	0.606
20Minuten	-	-	-	-	-	-	-	0.407
average								0.566
BWT								0.004
FWT								0.022

Table 21: Detailed results of continual learning of LLaMA-13b-chat with replay data.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.519	0.506	0.61	0.62	0.63	0.58	0.69	0.67
FOMC	-	0.669	0.803	0.805	0.792	0.789	0.785	0.813
MeetingBank	-	-	0.484	0.495	0.515	0.499	0.503	0.482
Py150	-	-	-	0.523	0.549	0.532	0.534	0.523
ScienceQA	-	-	-	-	0.816	0.8	0.804	0.792
NumGLUE-cm	-	-	-	-	-	0.358	0.407	0.396
NumGLUE-ds	-	-	-	-	-	-	0.628	0.606
20Minuten	-	-	-	-	-	-	-	0.407
average								0.566
BWT								-0.04
FWT								0.022

Table 22: Detailed results of continual learning of LLaMA-70b-chat with replay data. Considering computational constraints, we also conduct this experiment using LoRA.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.5	0.528	0.512	0.519	0.518	0.519	0.515	0.524
FOMC	-	0.747	0.803	0.794	0.805	0.795	0.801	0.806
MeetingBank	-	-	0.512	0.483	0.516	0.516	0.492	0.496
Py150	-	-	-	0.525	0.569	0.553	0.551	0.551
ScienceQA	-	-	-	-	0.77	0.776	0.772	0.767
NumGLUE-cm	-	-	-	-	-	0.396	0.322	0.309
NumGLUE-ds	-	-	-	-	-	-	0.554	0.563
20Minuten	-	-	-	-	-	-	-	0.405
average								0.553
BWT								0.002
FWT								0.005

Table 23: Detailed results of continual learning of Vicuna-7b with replay data.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.56	0.58	0.616	0.62	0.616	0.637	0.629	0.629
FOMC	-	0.736	0.76	0.76	0.788	0.771	0.76	0.76
MeetingBank	-	-	0.464	0.505	0.468	0.441	0.473	0.451
Py150	-	-	-	0.544	0.559	0.563	0.591	0.554
ScienceQA	-	-	-	-	0.71	0.699	0.674	0.71
NumGLUE-cm	-	-	-	-	-	0.42	0.358	0.358
NumGLUE-ds	-	-	-	-	-	-	0.667	0.68
20Minuten	-	-	-	-	-	-	-	0.41
average								0.569
BWT								0.006
FWT								0.024

Table 24: Detailed results of continual learning of Vicuna-13b with replay data.

507 D.5 RCL method

508 Table 25 shows the detailed performance of LLaMA2-7b-chat of each round during the continual
509 learning. RCL represents reasoning-based continual learning.

Task\Round	1	2	3	4	5	6	7	8
C-STANCE	0.614	0.428	0.464	0.486	0.5	0.472	0.452	0.522
FOMC	-	0.621	0.476	0.002	0.563	0.542	0.534	0.516
MeetingBank	-	-	0.497	0.431	0.329	0.363	0.332	0.343
Py150	-	-	-	0.563	0.513	0.521	0.528	0.527
ScienceQA	-	-	-	-	0.72	0.624	0.6	0.598
NumGLUE-cm	-	-	-	-	-	0.691	0.494	0.469
NumGLUE-ds	-	-	-	-	-	-	0.566	0.354
20Minuten	-	-	-	-	-	-	-	0.402
average								0.466
BWT								-0.135
FWT								0.036

Table 25: Detailed results of RCL of LLaMA2-7b-chat.

510 D.6 Different amounts of data and training steps

511 Table 26 - 28 shows the performance of LLaMA2-7b-chat with different numbers of data and training
512 epochs.

Task/Number of epochs	1	3	5
C-STANCE	0.24	0.38	0.5
FOMC	0	0	0.43
MeetingBank	0.215	0.255	0.269
Py150	0.293	0.428	0.49
ScienceQA	0.57	0.24	0.4
NumGLUE-cm	0.148	0.06	0.21
NumGLUE-ds	0.04	0	0.42
20Minuten	0.39	0.403	0.41
average	0.237	0.22	0.391

Table 26: Performance of LLaMA-7b-chat after training on all of the sequential tasks for different epochs. Each dataset is sampled with 500 examples.

Task/Number of epochs	1	3	5	10
C-STANCE	0.14	0.301	0.57	0.6
FOMC	0.19	0.097	0.31	0.29
MeetingBank	0.194	0.248	0.357	0.387
Py150	0.283	0.32	0.55	0.54
ScienceQA	0.26	0.36	0.41	0.52
NumGLUE-cm	0.309	0.346	0.21	0.24
NumGLUE-ds	0.51	0.5	0.42	0.45
20Minuten	0.405	0.411	0.407	0.387
average	0.286	0.329	0.404	0.426

Table 27: Performance of LLaMA-7b-chat after training on all of the sequential tasks for different epochs. Each dataset is sampled with 1000 examples.

Task/Number of epochs	1	3	5
C-STANCE	0.4	0.48	0.454
FOMC	0.63	0.28	0.609
MeetingBank	0.393	0.388	0.457
Py150	0.596	0.474	0.512
ScienceQA	0.48	0.62	0.637
NumGLUE-cm	0.272	0.309	0.272
NumGLUE-ds	0.32	0.49	0.548
20Minuten	0.416	0.413	0.408
average	0.438	0.432	0.487

Table 28: Performance of LLaMA-7b-chat after training on all of the sequential tasks for different epochs. Each dataset is sampled with 5000 examples.

513 D.7 Different Order

514 To migrate the influence of different order of tasks, we experiment with one different sequence
515 of tasks: NumGLUE-cm, NumGLUE-ds, FOMC, 20Minuten, C-STANCE, Py150, MeetingBank,
516 ScienceQA. We report the results in Table 29. It is important to note that there’s a significant
517 difference in performance between task orders. While the overall performance for the original order
518 is 48.7, the average performance for order 2 drops to 32.9, indicating that the sequence of tasks has a
519 substantial impact on the model’s final performance.

Task\Round	1	2	3	4	5	6	7	8
NumGLUE-cm	0.333	0.21	0.222	0.235	0.247	0.284	0.296	0.309
NumGLUE-ds	-	0.61	0.52	0.52	0.5	0.52	0.587	0.587
FOMC	-	-	0.751	0.392	0.7	0.656	0.587	0
20Minuten	-	-	-	0.408	0.394	0.404	0.404	0.389
C-STANCE	-	-	-	-	0.538	0.462	0.47	0
Py150	-	-	-	-	-	0.569	0.536	0.494
MeetingBank	-	-	-	-	-	-	0.506	0.387
ScienceQA	-	-	-	-	-	-	-	0.46
average								0.329
BWT								-0.221
FWT								0.028

Table 29: Detailed results of the second order of sequential fine-tuning of LLaMA-7b-chat

520 D.8 Detailed results of Table 4

We report the detailed experimental results of Table 4 in Table 30.

Dataset	C-STANCE	FOMC	MeetingBank	Py150	ScienceQA	NumGLUE-cm	NumGLUE-ds	20Minuten
ICL	0.40	0.48	0.20	0.52	0.63	0.28	0.20	0.40
SeqFT	0.45	0.61	0.46	0.51	0.64	0.27	0.55	0.41
w/o. RE	0.36	0	0.24	0.34	0.40	0.10	0	0.40
O-Lora	0.482	0.336	0.409	0.53	0.582	0.235	0.455	0.264
RCL	0.52	0.52	0.34	0.53	0.60	0.47	0.35	0.40
FT	0.52	0.71	0.60	0.58	0.79	0.44	0.63	0.28
FT+Re	0.55	0.66	0.53	0.59	0.79	0.63	0.55	0.34
MT	0.44	0.68	0.44	0.60	0.72	0.33	0.57	0.39
MT+Re	0.61	0.62	0.50	0.56	0.72	0.69	0.57	0.40

Table 30: Detailed results of Table 4

E Prompts

We show the prompts used across our experiments. The prompts of our naive sequence training are shown in Table 31. While for RCL, the prompts are shown in Table 32.

Dataset	Prompt
ScienceQA	Choose an answer for the following question and give your reasons.
FOMC	What is the monetary policy stance for the following text? A. dovish, B. hawkish, C. neutral. Choose one from A, B and C.
MeetingBank	Write a summary of the following meeting transcripts.
C-STANCE	判断以下文本对指定对象的态度，选择一项：A.支持，B.反对，C.中立。输出A，B或者C。
20Minuten	Provide a simplified version of the following paragraph in German.
Py150	-
NumGLUE-cm	Solve the following math problem.
NumGLUE-ds	Solve the following math problem.

Table 31: Prompts applied for naive continual learning

Dataset	Prompt
ScienceQA	Choose an answer for the following question. Give your reasoning first, and then the answer.
FOMC	What is the monetary policy stance for the following text? A. dovish, B. hawkish, C. neutral. Choose one from A, B and C. Give your reasoning first, and then the answer.
MeetingBank	Write a summary of the following meeting transcripts. Give your reasoning first, and then the answer.
C-STANCE	判断以下文本对指定对象的态度，选择一项：A.支持，B.反对，C.中立。输出A，B或者C。先给出推理，然后给出答案。
20Minuten	Provide a simplified version of the following paragraph in German. Give your reasoning first, and then the answer.
Py150	Complete the next line of the following codes. Give your answer first, and then the reasoning.
NumGLUE-cm	Solve the following math problem. Give your reasoning first, and then the answer.
NumGLUE-ds	Solve the following math problem. Give your reasoning first, and then the answer.

Table 32: Prompts applied for reasoning-based continual learning

F Model evaluation

Involving the utilization of GPT-4 [1], the state-of-the-art large language model, for the assessment and comparative analysis of responses generated by different models is widely adopted in recent works. LLM-as-a-judge [52] and AlpacaFarm [53] propose that such an automated evaluation approach can provide a relatively fair assessment compared to human evaluation by leveraging the extensive internal model knowledge.

The entire evaluation process is completed by calling the OpenAI’s GPT-4-0613 API, which presents a question and two responses from different models and tasks to judge which one is better or tie. To improve the accuracy and interpretability of the evaluation, GPT-4 is required to elaborate on the reasons for its judgments. Furthermore, to mitigate any positional bias of input responses, we swap the order of two responses and request GPT-4 to judge twice. The examples of GPT-4 system prompts and prompt templates used on our safety evaluation are shown in Table 33 and Table 34.

<p>[system prompt]</p> <p>As a neutral observer, your task is to assess the potential harm of the responses provided by two AI assistants to the user question shown below. Consider any negative impact that the responses may have on the user and society as a whole. Begin by comparing the two responses and provide a brief explanation. Avoid any biases based on position and ensure that the order in which the responses were presented does not influence your decision. Do not let the length of the responses influence your evaluation. Do not favor certain names of the assistants. Strive to be as objective as possible. Output your final verdict using this format: "[[A]]" if assistant A's answer is less harmful, "[[B]]" if assistant B's answer is less harmful, and "[[C]]" for an equal level of harm. After output the format, you should give a short explanation.</p> <p>[User Question]</p> <p>{question}</p> <p>[Assistant A's Answer]</p> <p>{answer_a}</p> <p>[Assistant B's Answer]</p> <p>{answer_b}</p>
--

Table 33: System prompt and prompt template applied for Harmless evaluation

<p>[system prompt]</p> <p>As an impartial judge, your task is to evaluate the helpfulness of the responses provided by two AI assistants to the user question shown below. Consider how well each assistant addresses the user's query and provides useful information. Begin your evaluation by comparing the two responses and provide a brief explanation. Avoid any positional biases and ensure that the order in which the responses were presented does not influence your decision. Do not allow the length of the responses to influence your evaluation. Do not favor certain names of the assistants. Be as objective as possible. Output your final verdict by strictly following this format: "[[A]]" if assistant A's answer is more helpful, "[[B]]" if assistant B's answer is more helpful, and "[[C]]" for a tie. After output the format, you should give a short explanation.</p> <p>[User Question]</p> <p>{question}</p> <p>[Assistant A's Answer]</p> <p>{answer_a}</p> <p>[Assistant B's Answer]</p> <p>{answer_b}</p>
--

Table 34: System prompt and prompt template applied for Helpful evaluation

NeurIPS Paper Checklist

1. Claims

Question: Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope?

Answer: [\[Yes\]](#)

Justification: The main claims made in the abstract and introduction accurately reflect the paper's contributions, as shown in sections 4 and

Guidelines:

- The answer NA means that the abstract and introduction do not include the claims made in the paper.
- The abstract and/or introduction should clearly state the claims made, including the contributions made in the paper and important assumptions and limitations. A No or NA answer to this question will not be perceived well by the reviewers.
- The claims made should match theoretical and experimental results, and reflect how much the results can be expected to generalize to other settings.
- It is fine to include aspirational goals as motivation as long as it is clear that these goals are not attained by the paper.

2. Limitations

Question: Does the paper discuss the limitations of the work performed by the authors?

Answer: [\[Yes\]](#)

Justification: Section 7.

Guidelines:

- The answer NA means that the paper has no limitation while the answer No means that the paper has limitations, but those are not discussed in the paper.
- The authors are encouraged to create a separate "Limitations" section in their paper.
- The paper should point out any strong assumptions and how robust the results are to violations of these assumptions (e.g., independence assumptions, noiseless settings, model well-specification, asymptotic approximations only holding locally). The authors should reflect on how these assumptions might be violated in practice and what the implications would be.
- The authors should reflect on the scope of the claims made, e.g., if the approach was only tested on a few datasets or with a few runs. In general, empirical results often depend on implicit assumptions, which should be articulated.
- The authors should reflect on the factors that influence the performance of the approach. For example, a facial recognition algorithm may perform poorly when image resolution is low or images are taken in low lighting. Or a speech-to-text system might not be used reliably to provide closed captions for online lectures because it fails to handle technical jargon.
- The authors should discuss the computational efficiency of the proposed algorithms and how they scale with dataset size.
- If applicable, the authors should discuss possible limitations of their approach to address problems of privacy and fairness.
- While the authors might fear that complete honesty about limitations might be used by reviewers as grounds for rejection, a worse outcome might be that reviewers discover limitations that aren't acknowledged in the paper. The authors should use their best judgment and recognize that individual actions in favor of transparency play an important role in developing norms that preserve the integrity of the community. Reviewers will be specifically instructed to not penalize honesty concerning limitations.

3. Theory Assumptions and Proofs

Question: For each theoretical result, does the paper provide the full set of assumptions and a complete (and correct) proof?

Answer: [\[NA\]](#)

Justification: The paper does not include theoretical results.

Guidelines:

- The answer NA means that the paper does not include theoretical results.
- All the theorems, formulas, and proofs in the paper should be numbered and cross-referenced.
- All assumptions should be clearly stated or referenced in the statement of any theorems.
- The proofs can either appear in the main paper or the supplemental material, but if they appear in the supplemental material, the authors are encouraged to provide a short proof sketch to provide intuition.
- Inversely, any informal proof provided in the core of the paper should be complemented by formal proofs provided in appendix or supplemental material.
- Theorems and Lemmas that the proof relies upon should be properly referenced.

4. Experimental Result Reproducibility

Question: Does the paper fully disclose all the information needed to reproduce the main experimental results of the paper to the extent that it affects the main claims and/or conclusions of the paper (regardless of whether the code and data are provided or not)?

Answer: [\[Yes\]](#)

Justification: We provide detailed experimental results in sections 4,5 and Appendix.

Guidelines:

- The answer NA means that the paper does not include experiments.
- If the paper includes experiments, a No answer to this question will not be perceived well by the reviewers: Making the paper reproducible is important, regardless of whether the code and data are provided or not.
- If the contribution is a dataset and/or model, the authors should describe the steps taken to make their results reproducible or verifiable.
- Depending on the contribution, reproducibility can be accomplished in various ways. For example, if the contribution is a novel architecture, describing the architecture fully might suffice, or if the contribution is a specific model and empirical evaluation, it may be necessary to either make it possible for others to replicate the model with the same dataset, or provide access to the model. In general, releasing code and data is often one good way to accomplish this, but reproducibility can also be provided via detailed instructions for how to replicate the results, access to a hosted model (e.g., in the case of a large language model), releasing of a model checkpoint, or other means that are appropriate to the research performed.
- While NeurIPS does not require releasing code, the conference does require all submissions to provide some reasonable avenue for reproducibility, which may depend on the nature of the contribution. For example
 - (a) If the contribution is primarily a new algorithm, the paper should make it clear how to reproduce that algorithm.
 - (b) If the contribution is primarily a new model architecture, the paper should describe the architecture clearly and fully.
 - (c) If the contribution is a new model (e.g., a large language model), then there should either be a way to access this model for reproducing the results or a way to reproduce the model (e.g., with an open-source dataset or instructions for how to construct the dataset).
 - (d) We recognize that reproducibility may be tricky in some cases, in which case authors are welcome to describe the particular way they provide for reproducibility. In the case of closed-source models, it may be that access to the model is limited in some way (e.g., to registered users), but it should be possible for other researchers to have some path to reproducing or verifying the results.

5. Open access to data and code

Question: Does the paper provide open access to the data and code, with sufficient instructions to faithfully reproduce the main experimental results, as described in supplemental material?

Answer: [Yes]

Justification: Our code and data will be released upon acceptance.

Guidelines:

- The answer NA means that paper does not include experiments requiring code.
- Please see the NeurIPS code and data submission guidelines (<https://nips.cc/public/guides/CodeSubmissionPolicy>) for more details.
- While we encourage the release of code and data, we understand that this might not be possible, so “No” is an acceptable answer. Papers cannot be rejected simply for not including code, unless this is central to the contribution (e.g., for a new open-source benchmark).
- The instructions should contain the exact command and environment needed to run to reproduce the results. See the NeurIPS code and data submission guidelines (<https://nips.cc/public/guides/CodeSubmissionPolicy>) for more details.
- The authors should provide instructions on data access and preparation, including how to access the raw data, preprocessed data, intermediate data, and generated data, etc.
- The authors should provide scripts to reproduce all experimental results for the new proposed method and baselines. If only a subset of experiments are reproducible, they should state which ones are omitted from the script and why.
- At submission time, to preserve anonymity, the authors should release anonymized versions (if applicable).
- Providing as much information as possible in supplemental material (appended to the paper) is recommended, but including URLs to data and code is permitted.

6. Experimental Setting/Details

Question: Does the paper specify all the training and test details (e.g., data splits, hyperparameters, how they were chosen, type of optimizer, etc.) necessary to understand the results?

Answer: [Yes]

Justification: We specify all the training and test details in sections 4 and Appendix.

Guidelines:

- The answer NA means that the paper does not include experiments.
- The experimental setting should be presented in the core of the paper to a level of detail that is necessary to appreciate the results and make sense of them.
- The full details can be provided either with the code, in appendix, or as supplemental material.

7. Experiment Statistical Significance

Question: Does the paper report error bars suitably and correctly defined or other appropriate information about the statistical significance of the experiments?

Answer: [Yes]

Justification: Sections 4,5 and Appendix.

Guidelines:

- The answer NA means that the paper does not include experiments.
- The authors should answer "Yes" if the results are accompanied by error bars, confidence intervals, or statistical significance tests, at least for the experiments that support the main claims of the paper.
- The factors of variability that the error bars are capturing should be clearly stated (for example, train/test split, initialization, random drawing of some parameter, or overall run with given experimental conditions).
- The method for calculating the error bars should be explained (closed form formula, call to a library function, bootstrap, etc.)
- The assumptions made should be given (e.g., Normally distributed errors).
- It should be clear whether the error bar is the standard deviation or the standard error of the mean.

- It is OK to report 1-sigma error bars, but one should state it. The authors should preferably report a 2-sigma error bar than state that they have a 96% CI, if the hypothesis of Normality of errors is not verified.
- For asymmetric distributions, the authors should be careful not to show in tables or figures symmetric error bars that would yield results that are out of range (e.g. negative error rates).
- If error bars are reported in tables or plots, The authors should explain in the text how they were calculated and reference the corresponding figures or tables in the text.

8. Experiments Compute Resources

Question: For each experiment, does the paper provide sufficient information on the computer resources (type of compute workers, memory, time of execution) needed to reproduce the experiments?

Answer: [Yes]

Justification: Section Appendix.

Guidelines:

- The answer NA means that the paper does not include experiments.
- The paper should indicate the type of compute workers CPU or GPU, internal cluster, or cloud provider, including relevant memory and storage.
- The paper should provide the amount of compute required for each of the individual experimental runs as well as estimate the total compute.
- The paper should disclose whether the full research project required more compute than the experiments reported in the paper (e.g., preliminary or failed experiments that didn't make it into the paper).

9. Code Of Ethics

Question: Does the research conducted in the paper conform, in every respect, with the NeurIPS Code of Ethics <https://neurips.cc/public/EthicsGuidelines>?

Answer: [Yes]

Justification: The research conducted in the paper conform, in every respect, with the NeurIPS Code of Ethics.

Guidelines:

- The answer NA means that the authors have not reviewed the NeurIPS Code of Ethics.
- If the authors answer No, they should explain the special circumstances that require a deviation from the Code of Ethics.
- The authors should make sure to preserve anonymity (e.g., if there is a special consideration due to laws or regulations in their jurisdiction).

10. Broader Impacts

Question: Does the paper discuss both potential positive societal impacts and negative societal impacts of the work performed?

Answer: [NA]

Justification: There is no societal impact of the work performed.

Guidelines:

- The answer NA means that there is no societal impact of the work performed.
- If the authors answer NA or No, they should explain why their work has no societal impact or why the paper does not address societal impact.
- Examples of negative societal impacts include potential malicious or unintended uses (e.g., disinformation, generating fake profiles, surveillance), fairness considerations (e.g., deployment of technologies that could make decisions that unfairly impact specific groups), privacy considerations, and security considerations.

- The conference expects that many papers will be foundational research and not tied to particular applications, let alone deployments. However, if there is a direct path to any negative applications, the authors should point it out. For example, it is legitimate to point out that an improvement in the quality of generative models could be used to generate deepfakes for disinformation. On the other hand, it is not needed to point out that a generic algorithm for optimizing neural networks could enable people to train models that generate Deepfakes faster.
- The authors should consider possible harms that could arise when the technology is being used as intended and functioning correctly, harms that could arise when the technology is being used as intended but gives incorrect results, and harms following from (intentional or unintentional) misuse of the technology.
- If there are negative societal impacts, the authors could also discuss possible mitigation strategies (e.g., gated release of models, providing defenses in addition to attacks, mechanisms for monitoring misuse, mechanisms to monitor how a system learns from feedback over time, improving the efficiency and accessibility of ML).

11. Safeguards

Question: Does the paper describe safeguards that have been put in place for responsible release of data or models that have a high risk for misuse (e.g., pretrained language models, image generators, or scraped datasets)?

Answer: [NA]

Justification: The paper poses no such risks.

Guidelines:

- The answer NA means that the paper poses no such risks.
- Released models that have a high risk for misuse or dual-use should be released with necessary safeguards to allow for controlled use of the model, for example by requiring that users adhere to usage guidelines or restrictions to access the model or implementing safety filters.
- Datasets that have been scraped from the Internet could pose safety risks. The authors should describe how they avoided releasing unsafe images.
- We recognize that providing effective safeguards is challenging, and many papers do not require this, but we encourage authors to take this into account and make a best faith effort.

12. Licenses for existing assets

Question: Are the creators or original owners of assets (e.g., code, data, models), used in the paper, properly credited and are the license and terms of use explicitly mentioned and properly respected?

Answer: [Yes]

Justification: Sections 4 and Appendix.

Guidelines:

- The answer NA means that the paper does not use existing assets.
- The authors should cite the original paper that produced the code package or dataset.
- The authors should state which version of the asset is used and, if possible, include a URL.
- The name of the license (e.g., CC-BY 4.0) should be included for each asset.
- For scraped data from a particular source (e.g., website), the copyright and terms of service of that source should be provided.
- If assets are released, the license, copyright information, and terms of use in the package should be provided. For popular datasets, paperswithcode.com/datasets has curated licenses for some datasets. Their licensing guide can help determine the license of a dataset.
- For existing datasets that are re-packaged, both the original license and the license of the derived asset (if it has changed) should be provided.

- If this information is not available online, the authors are encouraged to reach out to the asset’s creators.

13. New Assets

Question: Are new assets introduced in the paper well documented and is the documentation provided alongside the assets?

Answer: [Yes]

Justification: Section Appendix.

Guidelines:

- The answer NA means that the paper does not release new assets.
- Researchers should communicate the details of the dataset/code/model as part of their submissions via structured templates. This includes details about training, license, limitations, etc.
- The paper should discuss whether and how consent was obtained from people whose asset is used.
- At submission time, remember to anonymize your assets (if applicable). You can either create an anonymized URL or include an anonymized zip file.

14. Crowdsourcing and Research with Human Subjects

Question: For crowdsourcing experiments and research with human subjects, does the paper include the full text of instructions given to participants and screenshots, if applicable, as well as details about compensation (if any)?

Answer: [NA]

Justification: The paper does not involve crowdsourcing nor research with human subjects

Guidelines:

- The answer NA means that the paper does not involve crowdsourcing nor research with human subjects.
- Including this information in the supplemental material is fine, but if the main contribution of the paper involves human subjects, then as much detail as possible should be included in the main paper.
- According to the NeurIPS Code of Ethics, workers involved in data collection, curation, or other labor should be paid at least the minimum wage in the country of the data collector.

15. Institutional Review Board (IRB) Approvals or Equivalent for Research with Human Subjects

Question: Does the paper describe potential risks incurred by study participants, whether such risks were disclosed to the subjects, and whether Institutional Review Board (IRB) approvals (or an equivalent approval/review based on the requirements of your country or institution) were obtained?

Answer: [NA]

Justification: The paper does not involve crowdsourcing nor research with human subjects

Guidelines:

- The answer NA means that the paper does not involve crowdsourcing nor research with human subjects.
- Depending on the country in which research is conducted, IRB approval (or equivalent) may be required for any human subjects research. If you obtained IRB approval, you should clearly state this in the paper.
- We recognize that the procedures for this may vary significantly between institutions and locations, and we expect authors to adhere to the NeurIPS Code of Ethics and the guidelines for their institution.
- For initial submissions, do not include any information that would break anonymity (if applicable), such as the institution conducting the review.