

Check Your Facts and Try Again: Improving Large Language Models with External Knowledge and Automated Feedback*

Baolin Peng[†] Michel Galley[†] Pengcheng He[†] Hao Cheng[†] Yujia Xie[†]
 Yu Hu[†] Qiuyuan Huang[†] Lars Liden[†] Zhou Yu[‡] Weizhu Chen[†] Jianfeng Gao[†]
[†] Microsoft Research [‡] Columbia University

Abstract

Large language models (LLMs), such as ChatGPT, are able to generate human-like, fluent responses for many downstream tasks, e.g., task-oriented dialog and question answering. However, applying LLMs to real-world, mission-critical applications remains challenging mainly due to their tendency to generate hallucinations and their inability to use external knowledge. This paper proposes a LLM-AUGMENTER system, which augments a black-box LLM with a set of plug-and-play modules. Our system makes the LLM generate responses grounded in external knowledge, e.g., stored in task-specific databases. It also iteratively revises LLM prompts to improve model responses using feedback generated by utility functions, e.g., the factuality score of a LLM-generated response. The effectiveness of LLM-AUGMENTER is empirically validated on two types of scenarios, task-oriented dialog and open-domain question answering. LLM-AUGMENTER significantly reduces ChatGPT’s hallucinations without sacrificing the fluency and informativeness of its responses. We make the source code and models publicly available.¹

1 Introduction

Large Language models (LLMs), such as GPT-3 (Brown et al., 2020) and ChatGPT, have demonstrated an outstanding ability in generating fluent, coherent, and informative natural language texts. It is commonly understood that the impressive capabilities of these models stem from the abundance of world knowledge encoded therein and models’ ability to generalize from that knowledge. However, the knowledge encoding of LLMs is lossy and the knowledge generalization could lead to “memory distortion.” As a result, these models tend to *hallucinate*, which can cause damage when deployed for mission-critical tasks. In

*Correspondence: {bapeng,mgalley,jfgao}@microsoft.com

¹<https://aka.ms/llm-augmenter>

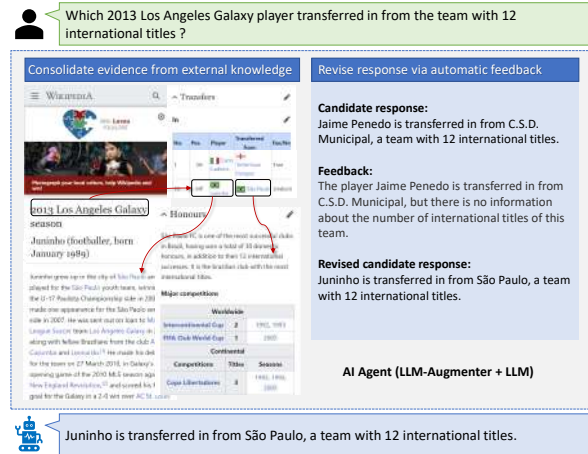


Figure 1: LLM-AUGMENTER improves a fixed LLM by (1) consolidating evidence from external knowledge for the LLM to generate responses grounded in evidence, and (2) revising LLM’s (candidate) responses using automated feedback.

addition, even with exponentially growing model sizes, LLMs can never encode all information needed for many applications. For example, constant changes in real-world settings cause LLMs to quickly become stale for time-sensitive tasks such as news question answering, and many proprietary datasets are not available for LLM training due to privacy. While there is a growing interest in improving LLMs using external knowledge (e.g., Ghazvininejad et al., 2017; Guu et al., 2020; Zhong et al., 2022; Gao et al., 2019, 2022), almost all the previously proposed methods require finetuning the parameters of a LLM, which can be prohibitively expensive as the size of LLMs grows exponentially. Thus, it is highly desirable to augment a *fixed* LLM with plug-and-play (PnP) modules for mission-critical tasks.

In this paper, we present LLM-AUGMENTER to improve LLMs with external knowledge and automated feedback using PnP modules. As illustrated by the example in Figure 1, given a user query (e.g., regarding a 2013 Los Angeles

Galaxy player transfer), LLM-AUGMENTER first retrieves evidence from external knowledge (*e.g.*, Web or task-specific datasets) and, if necessary, further consolidates evidence by linking retrieved raw evidence with related context (*e.g.*, information of the entity “2013 Los Angeles Galaxy”) and performing reasoning to form evidence chains (*e.g.*, table-passage in the figure). Then, LLM-AUGMENTER queries a fixed LLM (*i.e.*, ChatGPT in our study) using a prompt that contains the consolidated evidence for ChatGPT to generate a candidate response grounded in external knowledge (evidence). LLM-AUGMENTER then verifies the candidate response *e.g.*, by checking whether it hallucinates evidence. If so, LLM-AUGMENTER generates a feedback message (*e.g.*, about the team “C.S.D. Municipal”). The message is used to revise the prompt to query ChatGPT again. The process iterates until a candidate response passes the verification and is sent to the user.

In addition to proposing LLM-AUGMENTER, to be detailed in Section 2, we make the following contributions. We perform an empirical study to validate the effectiveness of LLM-AUGMENTER using two tasks, information seeking dialog (Section 3) and open-domain Wiki question answering (Wiki QA) (Section 4). The study shows that LLM-AUGMENTER significantly reduces ChatGPT’s hallucinations without sacrificing the fluency and informativeness of its generated responses. For example, on the dialog task of customer service, human evaluation shows LLM-AUGMENTER improve ChatGPT by 32.3% in Usefulness (measuring the groundedness or hallucination of model responses) and 12.9% in Humanness (measuring the fluency and informativeness of model responses). The Wiki QA task is extremely challenging to ChatGPT in that answering these questions often requires multi-hop reasoning to piece together information of various modalities scattered across different documents. Our results show that although the *closed-book* ChatGPT performs poorly and often hallucinates, LLM-AUGMENTER substantially improves the factuality score of the answers (absolute +10% in F1) by grounding ChatGPT’s responses in consolidated external knowledge and automated feedback.

2 LLM-AUGMENTER

The architecture of LLM-AUGMENTER is illustrated in Figure 2. It consists of a set of PnP

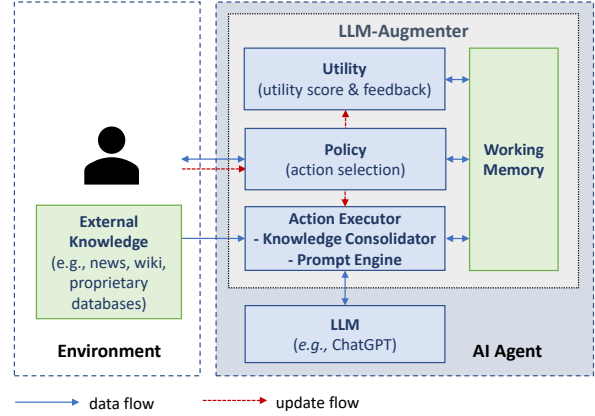


Figure 2: LLM-AUGMENTER architecture showing how its plug-and-play modules interact with the LLM and the user’s environment.

modules (*i.e.*, Working Memory, Policy, Action Executor, and Utility) to improve a fixed LLM (*e.g.*, ChatGPT) with external knowledge and automated feedback to mitigate generation problems such as hallucination.

We formulate human-system conversation as a Markov Decision Process (MDP) described by a five-tuple $(\mathcal{S}, \mathcal{A}, P, R, \gamma)$:

- \mathcal{S} is an infinite set of dialog states, which encode information stored in Working Memory, including dialog history, user query, evidence, candidate response;
- \mathcal{A} is a set of actions that Policy picks to execute, including (1) calling Knowledge Consolidator to consolidate evidence from external knowledge and (2) calling Prompt Engine to query the LLM to generate candidate responses;
- $P(s'|s, a)$ gives the transition probability of entering a new state s' after action a is taken in state s ;
- $R(s, a)$ is the external reward received after taking action a in state s , which is provided by the environment (*e.g.*, users or simulators); and
- $\gamma \in (0, 1]$ is a discount factor.

In what follows, we describe in detail the modules of LLM-AUGMENTER.

2.1 Working Memory

This module tracks the dialog state that captures all essential information in the conversation so

far. The state is represented using a six-tuple (q, e, o, u, f, h_q) :

- q is the current user query;
- e is evidence for q , consolidated from external knowledge by Knowledge Consolidator;
- o is a set of the LLM-generated candidate responses for q ;
- u is a score assessing the utility of each element of o , and f is a verbalized feedback to guide the LLM to improve its utility — both u and f are generated by the Utility module (see Section 2.4); and
- h_q is the dialog history before q .

Note that given user query q , LLM-AUGMENTER can take multiple iterations to revise its response, with each iteration generating a candidate response based on evidence, feedback and utility, before sending the final response to the user, as illustrated in Figure 1.

2.2 Policy

This module selects the next system action that leads to the best expected reward R . These actions include (1) acquiring evidence e for q from external knowledge, (2) calling the LLM to generate a candidate response, and (3) sending a response to users if it passes the verification by the Utility module.

The policy can be implemented using manually crafted rules, or trained on human-system interactions. In this study, we implement a trainable policy π as a neural network model parameterized by θ . π_θ is optimized using REINFORCE (Williams, 1992) to maximize the expected reward as:

$$\arg\max_{\theta} \mathbb{E}_{s \sim \mathcal{S}, a \sim \pi_\theta} [R(s, a)] \quad (1)$$

We find it effective to implement π using a pre-trained model (e.g., T5), which allows us to not only leverage the capacity of the pre-trained model, but also to incorporate additional information through finetuning.

Policy learning typically requires large amounts of human-machine interactions, which can be costly to collect. To address the challenge, policy learning can be done in three stages:

- Bootstrapping from a rule-based policy: Domain experts encode task-specific knowledge and business logic into IF-THEN rules. For example, if a product name is mentioned in a user query for customer service, it is wise to always call Knowledge Consolidator to collect information of the product from a product database.
- Learning with user simulators: We use a language model to simulate how human users interact with LLM-AUGMENTER. Any valid response from LLM-AUGMENTER that passes the evaluation of the Utility module can be used as a training example, allowing LLM-AUGMENTER to self-improve.
- Finally, LLM-AUGMENTER interacts with human users to further refine its policy.

In addition to Policy, the other trainable modules of LLM-AUGMENTER (*i.e.*, Knowledge Consolidator and Utility) can also be optimized using the same learning method.

2.3 Action Executor

This module performs an action selected by the policy. It is composed of two components, Knowledge Consolidator and Prompt Engine.

2.3.1 Knowledge Consolidator

The Knowledge Consolidator augments LLMs with the capability of grounding their responses on external knowledge to mitigate hallucination when completing tasks, such as answering questions regarding latest news, and booking a table in a restaurant. Following (Ma et al., 2022), the Knowledge Consolidator is designed in a modular fashion, consisting of a knowledge *retriever*, an entity *linker* and, an evidence *chainer*.

Specifically, the retriever first generates a set of search queries based on q and h_q , and then calls a set of APIs to retrieve raw evidence from various external knowledge sources, such as calling Bing Search APIs to query Web documents including Wiki articles and Reddit messages, and REST APIs to query task-specific databases for restaurant reviews and product specifications.

The retrieved raw evidence is sometimes incomplete and noisy. Thus, the entity linker enriches raw evidence with related context to form evidence graphs, *i.e.*, linking each entity mentioned in raw evidence to its corresponding description

based on Wikipedia. Then, the chainer prunes irrelevant evidence from the graphs and forms a shortlist of evidence chains that are most relevant to queries. The consolidated evidence e is then sent to Working Memory. Figure 1 shows an example of consolidated evidence for the anchored club “Los Angeles Galaxy”, *i.e.*, two evidence chains corresponding to the transfer players in 2013 season and the former clubs, respectively.

2.3.2 Prompt Engine

The Prompt Engine generates a prompt to query the LLM to generate a (candidate) response o for q . The prompt is a text string that consists of task instruction, user query q , dialog history h_q , evidence e if it is made available by Knowledge Consolidator, and feedback f if it is made available by the Utility module. Prompts are task-specific, and details thereof are provided in Appendix A.

2.4 Utility

Given a candidate response o , the Utility module generates utility score u and a corresponding feedback f using a set of task-specific utility functions.

These utility functions² access the alignment of the LLM’s responses with user expectations or specific business requirements. For example, in an information seeking dialog, it is important that all LLM’s responses are preciously grounded in external evidence to avoid generating misleading or inaccurate information. In a restaurant reservation dialog, the LLM responses should be conversational and focused on guiding the user through the reservation process, rather than engaging in off-topic chitchats.

Inspired by Glaese et al. (2022), there can be two distinct types of utility functions:

- Model-based utility functions assign preference scores to different dimensions of a response, such as fluency, informativeness and factuality. These functions are trained on pre-collected human preference data or annotated log data.
- Rule-based utility functions, implemented using heuristics or programmed functions, measure whether a response complies with a specific rule.

²Our experiments are with a single utility function. To allow multiple utility functions, we could learn a linear function mapping the outputs of these multiple functions to a single score using a linear function trained together with the other parameters of the policy.

In addition, we have developed a utility function to generate informative and actionable feedback to help revise prompts to allow the LLM to generate better responses. As shown in Figure 1, the utility function generates feedback “but there is no information about the number of international titles.” Such a utility function is a text generation model Q parameterized by ψ , and can be implemented as a seq2seq or auto-regression language model. It takes as input user query q , evidence e , candidate response o and dialog history h_q , and generates feedback in text f as

$$f = Q_{\psi}(q, e, o, h_q) \quad (2)$$

Alternatively, LLMs and rule-based natural language generator can be used for feedback generation.

In the next two sections, we present our experiments to validate the effectiveness of LLM-AUGMENTER in two types of distinct scenarios: (1) information seeking dialog, where the AI agent needs to generate informative and trustworthy responses based on a variety of external sources of knowledge, and (2) Wiki question answering, where the AI agent needs to answer questions by piecing together information of various modalities scattered among multiple Wiki documents.

3 Information Seeking Dialog

3.1 Datasets

News Chat: We repurpose the DSTC7 Track 2 task as an evaluation corpus for news conversation. The goal of this task is to generate informative responses that are grounded in external knowledge (*i.e.*, news) and go beyond chitchat. We followed the data crawling process used in DSTC7 Task 2 (Galley et al., 2019). We started by selecting Reddit discussion threads that contained URLs in the description, which were crawled from various news-related subreddits during the time period of 2021-2022. We then restricted the URL domain to a curated list of news websites, and extracted the relevant oracle passage by selecting the most appropriate passage for the context based on ROUGE-F1 scores (Lin, 2004). In order to reduce noisy or irrelevant information, we only kept examples with an F1 score higher than a certain threshold, resulting in a total of 1370 examples for evaluation.

Model	K.C.	Feedback	KF1 \uparrow	BLEU \uparrow	ROUGE \uparrow	chrF \uparrow	METEOR \uparrow	BERTScore \uparrow	BARTScore \uparrow	BLEURT \uparrow	Avg. length
CHATGPT	-	-	26.71	1.01	16.78	23.80	7.34	82.14	0.25	26.98	58.94
LLM-AUGMENTER	BM25	\times	34.96	6.71	22.25	27.02	9.35	83.46	0.34	26.89	46.74
LLM-AUGMENTER	BM25	\checkmark	36.41	7.63	22.80	28.66	10.17	83.33	0.35	27.71	54.24
LLM-AUGMENTER	gold	\times	57.44	19.24	38.89	40.02	17.21	86.65	0.82	40.55	44.35
LLM-AUGMENTER	gold	\checkmark	60.76	21.49	40.56	42.14	18.50	86.89	0.93	42.15	47.19

Table 1: Evaluation scores (in %) and average response lengths for the News Chat (DSTC7) dataset. BM25: Each model retrieves 5 knowledge snippets from the corresponding knowledge source. K.C. denotes Knowledge Consolidator.

Model	K.C.	Feedback	KF1 \uparrow	BLEU \uparrow	ROUGE \uparrow	chrF \uparrow	METEOR \uparrow	BERTScore \uparrow	BARTScore \uparrow	BLEURT \uparrow	Avg. length
CHATGPT	-	-	31.33	4.70	24.02	27.14	12.83	87.88	1.53	47.99	28.81
LLM-AUGMENTER	BM25	\times	34.07	4.78	24.52	28.95	13.61	87.96	1.78	47.21	32.65
LLM-AUGMENTER	BM25	\checkmark	37.41	3.86	24.20	30.90	14.74	87.58	2.09	44.71	45.07
LLM-AUGMENTER	gold	\times	45.63	6.54	29.77	33.32	16.93	89.35	2.59	54.38	33.04
LLM-AUGMENTER	gold	\checkmark	52.83	5.63	29.65	35.68	18.66	89.01	3.14	52.49	45.09

Table 2: Evaluation scores (in %) and average response lengths for the Customer Service (DSTC11) dataset. BM25: Each model retrieves 5 knowledge snippets from the corresponding knowledge source. K.C. denotes Knowledge Consolidator.

Customer Service: We use DSTC11 Track 5 (Kim et al., 2023) as a showcase in a conversational customer service scenario. It expands upon the DSTC9 Track 1 dataset by incorporating subjective knowledge from customer reviews in addition to factual knowledge from FAQs. This allows users to have an engaging and informative conversational experience with the AI system. The dataset evaluates the ability of the AI agent to understand relevant user review posts and FAQs, and generate responses based on both reviews and FAQ snippets. It is collected based on the MultiWOZ 2.1 (Eric et al., 2019) dataset and includes users’ knowledge-seeking queries that require the AI agent to use FAQs and user reviews to respond. There are 14768 dialog sessions for training and validation, and the test set is currently unavailable. Therefore, we used the validation set for our evaluations.

3.2 Experiment Setup

Language Model: Throughout this work, we focus on using ChatGPT as the backbone black-box LLM. It is straightforward to apply LLM-AUGMENTER to other LLMs, such as GPT-3 (Brown et al., 2020) or PaLM (Chowdhery et al., 2022).

Knowledge Consolidator: For News Chat, Knowledge Consolidator includes a BM25 retriever over web documents linked from Reddit posts. For the Customer Service task, Knowl-

edge Consolidator includes a BM25-based retriever over the knowledge bases of FAQs and Yelp reviews.

Additionally, we also experiment with ground-truth knowledge, referred to as *golden knowledge* henceforth, which is used by human annotators during data collection, in our oracle experiments.

Prompt Engine: The prompt templates utilized for News Chat and Customer Service are shown in the appendix in Table 7 and Table 8, respectively.

Utility: The goal of this task is to generate responses that are coherent to the context and grounded in external knowledge. To evaluate the degree to which the generated responses are grounded in consolidated evidence, we use the utility score, Knowledge F1 (Shuster et al., 2021), to measure the overlap between a prediction and evidence which is either consolidated by Knowledge Consolidator or provided as golden knowledge. Feedback generation is accomplished using a template-based natural language generator.³ In addition, we use ChatGPT as a utility function, *i.e.*, self-criticism to gather feedback by prompting ChatGPT to evaluate candidate responses and give feedback on how to improve them.

Policy: Due to ChatGPT’s current limited bandwidth, we use a rule-based policy for our ex-

³If the KF1 score falls below a certain threshold, the feedback is “The response is inconsistent with the knowledge. Please generate again.”

periments involving ChatGPT. The prior knowledge about this task inspired us to design a policy that always uses Knowledge Consolidator, evaluates the quality of a candidate response using ChatGPT, and provides feedback to revise the prompt. Additionally, to test the viability of LLM-AUGMENTER with a trainable policy, we employ offline RL to train the parameters of Policy as Equation 1, where the policy model is based on T5-Base.

Evaluation: We evaluate the performance of LLM-AUGMENTER on information-seeking dialog tasks using both automatic metrics and human evaluations. Following the literature, we consider commonly used metrics, Knowledge F1 (KF1) and BLEU-4, in grounded conversational response generation and task-oriented dialog. BLEU (Papineni et al., 2002) measures the overlap between the model’s output and the ground-truth human response, while KF1 (Lian et al., 2019) assesses the overlap with the knowledge that the human used as a reference during dataset collection. Additionally, we include ROUGE-1 (Lin, 2004) and METEOR (Banerjee and Lavie, 2005) as these metrics have been found to best correlate with human judgment on the DSTC9 and DSTC11 customer support tasks (Kim et al., 2020). We further include BLEURT (Sellam et al., 2020), BERTScore (Zhang et al., 2019), chrF (Popović, 2015), which have been shown to be among the best-performing text generation metrics on dialog (Yeh et al., 2021; Peng et al., 2022). Lastly, we also consider BARTScore as it has been reported to be one of the best model-based metrics (Yuan et al., 2021). Given that BARTScore can be interpreted as a log-probability, we report results with its natural exponent (positive scores). Additionally, we perform a turn-level human evaluation to investigate whether responses are (1) useful and (2) human-like. Following the evaluation protocol by (Peng et al., 2022), using Amazon Mechanical Turk, we hired master-level workers with lifetime HIT acceptance rate above 95%, and asked them to answer two questions on usefulness (*i.e.*, *which response sounds more useful*) and humanness (*i.e.*, *which speaker sounds more human*).

3.3 Automatic Evaluation Results

The impact of using external knowledge: Experiment results are shown in Tables 1 and 2. We observe that ChatGPT achieves reasonable perfor-

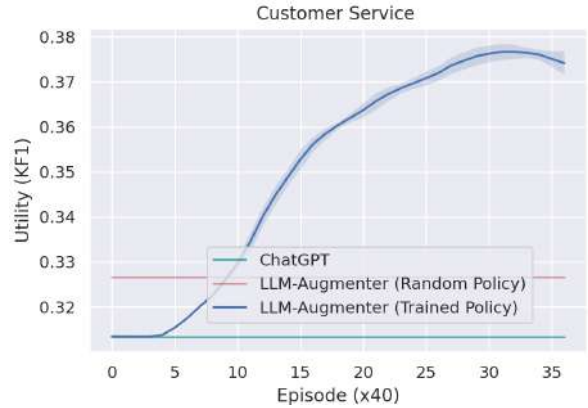


Figure 3: Learning curve of ChatGPT-Companion with T5-Base as the policy module. The solid curves are the mean and the shaded regions are the maximum and minimum utility scores over 5 runs.

mance even in the zero-shot setting. However, with access to golden knowledge, the performance is dramatically improved. This suggests that while LLMs are able to encode a large amount of general knowledge in their parameters, they can still benefit from more specific, targeted knowledge. This is likely because LLMs are designed to handle a wide range of tasks and therefore may not always have access to the most relevant or up-to-date information for a given task. Our experiments show that providing LLMs with task-specific knowledge can significantly mitigate hallucination without sacrificing the fluency and informativeness of model-generated responses. As demonstrated in Tables 1 and 2, LLM-AUGMENTER mitigates ChatGPT’s hallucination issue on both the news chat and customer service tasks. Specifically, we observe a significant improvement in KF1 scores of approximately 10 and 6 points, respectively, due to the use of evidence retrieved by Knowledge Consolidator.

The impact of using automated feedback: As listed in Tables 1 and 2, the results of using golden knowledge setting demonstrate that incorporating feedback from the Utility module leads to substantial improvement 3.3 points in KF1 on News Chat and 7.2 on Customer Service, respectively. Similarly, significant improvement can also be observed when using evidence provided by Knowledge Consolidator.

The impact of using trainable Policy: Figure 3 shows the learning curve of LLM-AUGMENTER on the customer service task. As we do not have an

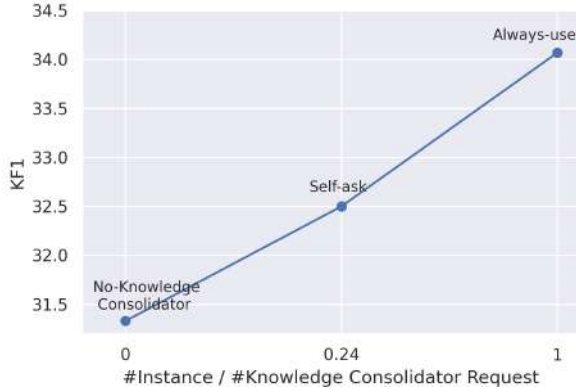


Figure 4: Ablation studies on different policies of LLM-AUGMENTER in Customer Service scenario.

Model	Usefulness \uparrow	Humanness \uparrow
ChatGPT	34.07	30.92
LLM-AUGMENTER	45.07	35.22

Table 3: Human evaluation of ChatGPT and LLM-AUGMENTER with BM25 in Customer Service scenario. All differences are significant ($p < 0.05$). Inter-annotator agreements according Krippendorff’s alpha (interval metric) are 0.15 and 0.07 respectively.

external reward that would require collecting data from real users, we instead define here our reward R as the KF1 utility function. This helps demonstrate the effectiveness of LLM-AUGMENTER in its reinforcement learning (RL) setup. As our experiments are akin to single turn interactions, we did not need to set discount factor γ , but future work may need to rely on it. We see that LLM-AUGMENTER’s reward on test data increases as the number of training episodes (dialog sessions) increases, surpassing a random policy after 600 interactions and ultimately reaching a KF1 score of approximately 37.5. Through these interactions, LLM-AUGMENTER is able to learn to effectively select the next system action to maximize the reward, which helps our system reduce hallucinations while generating fluent and informative responses.

3.4 Human Evaluation Results

We compare ChatGPT with and without LLM-AUGMENTER. A total of 948 randomly selected examples from the customer service dataset are used for human evaluation. The evaluation results are converted from a 5-point Likert-like scale to a win/tie/loss scale for reporting, as shown

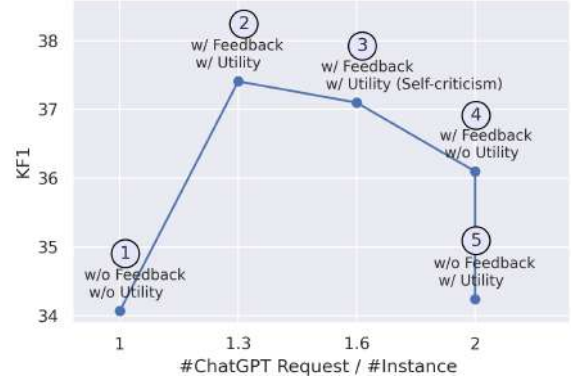


Figure 5: LLM-AUGMENTER benefits from the combination of using utility function and iterative improvement with feedback. The x-axis indicates the average number of ChatGPT prompting and the y-axis is the KF1. The studies are conducted in the Customer Service scenario with knowledge being provided by BM25.

in Table 3. We observe a strong preference for LLM-AUGMENTER over ChatGPT alone in terms of both Usefulness and Humanness. The result is consistent with the automatic evaluation result, discussed earlier.

3.5 Ablation Study

We conduct ablation experiments to evaluate the effect of various policies on the utilization of the knowledge consolidator. Figure 4 shows the performance of three different variants of the policy: 1) no-knowledge consolidator, in which the knowledge consolidator is not used, 2) Self-ask, in which the knowledge consolidator is only utilized when the LM suggests the use of external knowledge by prompting it whether to use, and (3) Always-use, in which the knowledge consolidator is always provided to the LM. Our results indicate that Self-ask policy achieves a significantly better KF1 score than the No-knowledge consolidator policy, with the ChatGPT model unable to answer user queries and suggesting knowledge consolidator access for 24% of examples. However, the Always-use policy, while achieving the best KF1 score, also incurred additional overhead in terms of knowledge consolidator access. These observations suggest that a trainable policy model should be employed to learn when to use external knowledge.

In addition, the evaluation results on the impact of different types of feedback for LLM-

Feedback	KF1 \uparrow
w/o Feedback	34.07
w/ Rule-based Feedback	37.41
w/ Self-criticism Feedback	37.10

Table 4: Ablation studies on different feedback of LLM-AUGMENTER in Customer Service scenario.

AUGMENTER are listed in Table 4. We observe that self-criticism feedback enhances response quality make it more knowledge-grounded. Although its performance is comparable to that of rule-based feedback, it provides more detailed suggestions. We speculate that self-criticism will be more helpful for complex tasks. Some examples can be found in 6.

To understand the impact of utility functions and feedback-augmented prompting on the performance of LLM-AUGMENTER, we conduct an analysis by turning each component on and off. Figure 5 illustrates the results of each variant. We observe that the combination of using utility functions and feedback-augmented prompting, *i.e.*, ②, achieves the best performance. In addition, always providing feedback (as shown in ④) also enhances the performance, although it requires additional model prompting. ⑤ represents prompting ChatGPT twice and re-ranking the response based on the utility functions, which results in a slightly higher KF1, but performs significantly worse than ②. These findings suggest that incorporating both utility functions and feedback is a more effective method for improving the alignment of LLMs.

4 Wiki QA

Instead of conversational evaluations, we focus on stress tests on ChatGPT here using open-domain question answering. As ChatGPT and other LLMs are mostly trained using abundant text from single web pages, we hypothesize that answering multi-hop questions involving scattered information across different pages/modalities can better serve the purpose. Due to this, closed-book LLMs are more likely to hallucinate. Moreover, the complex step-by-step reasoning can even be challenging for existing search systems to gather all necessary support evidence in one-shot. Thus, more advanced knowledge consolidation techniques are essential to elicit LLMs for proper grounding.

Lastly, different from conversational tasks where long-form responses are desirable, we mainly consider questions with concise short-form answers, *i.e.*, there exists a significant style shift in responses. To align ChatGPT to this new scenario with distinct characteristics, extra instructions are needed.

4.1 Dataset

OTT-QA: The OTT-QA dataset is an open-domain question answering benchmark that considers multi-step joint reasoning over both tabular and textual information. It consists of around 40K instances built upon Wikipedia, including 400K tables and 6M passages as the knowledge source. Solving the questions in OTT-QA requires diverse reasoning skills and can be divided into three categories: single-hop questions (13%), two-hop questions (57%), and multi-hop questions (30%). In this paper, we denote the dataset as Wiki QA.

4.2 Experiment Setups

In the following, we describe the experimental setup for Wiki QA. Unless specified otherwise, the setups are identical to those used in Section 3.

Knowledge Consolidator: Here, the Knowledge Consolidator uses Wikipedia passages and tables as the knowledge source. Instead of using BM25 as done for dialog tasks, we resort to a dense model, DPR (Karpukhin et al., 2020), as the backbone retriever. For DPR, both question and passage/table inputs are represented by the corresponding special token [CLS] embeddings from their respective encoders, and retrieval is simply done via maximum inner product search in the vector space. Given a question, we use DPR to obtain the initial set of evidence, which includes tables and passages. As most WikiQA questions require reasoning hops across different pieces of information (*e.g.*, hopping from the album table to its entry artist page in Figure 1), we contend that directly feeding this raw evidence set to Working Memory is insufficient for prompting LLMs. Thus, we further use additional intermediary modules, *i.e.*, linker and chainer, from CORE (Ma et al., 2022) to consolidate the raw evidence, including connecting relevant documents, reranking evidence, and splicing them into evidence chains. We refer to Ma et al. (2022) for more details.

Prompt Engine: The prompt templates utilized for Wiki QA is shown in the appendix in Table 9.

Model	Knowledge Consolidator	Feedback	Wiki QA		
			P \uparrow	R \uparrow	F1 \uparrow
CHATGPT	-	-	0.48	1.52	0.59
LLM-AUGMENTER	DPR	\times	2.08	4.31	2.38
LLM-AUGMENTER	CORE	\times	7.06	14.77	8.08
LLM-AUGMENTER	CORE	\checkmark	8.93	33.87	11.80

Table 5: Evaluation results on Wiki QA. Each model retrieves top-5 knowledge snippets from the corresponding knowledge source. The top-5 answer recall of consolidated evidence (CORE) is 50.83.

Utility: Here, as a response to a given question is deemed to leverage information from the consolidated knowledge, we use recall as the utility score, *i.e.*, preferring responses with higher token overlap with the corresponding evidence set. Similar to Section 3, we again consider a template-based natural language generator for giving feedback to ChatGPT.

Evaluation Metrics: As WikiQA mainly concerns short-form answers, we evaluate the generated responses using the token-level precision, recall and F1 scores against the annotated answers.

4.3 Results

Table 5 presents the evaluation results on Wiki QA. As expected, the closed-book model alone performs very poorly. Based on our manual inspections, we find that most error cases are hallucinated answers and ChatGPT abstains from answering for 17% cases. We observe that incorporating knowledge obtained from either DPR or CORE significantly improves the F1 score. The substantial improvements observed over the closed-book ChatGPT model indicate the importance of enhancing LLMs with external knowledge. Compared with raw evidence from DPR (row 2), we observe that consolidated evidence from our proposed Knowledge Consolidator with CORE (row 3) is more useful to the frozen ChatGPT model, achieving more pronounced improvements across the board. This suggests that it is crucial to consolidate knowledge for eliciting black-box LLMs to perform grounded reasoning. Lastly, consistent with the observations for news chat and customer service scenarios in Section 3, augmenting ChatGPT with automated feedback further improves alignments (adapting ChatGPT to perform multi-step grounded reasoning), leading to a substantial increase in recall and F1 scores.

Compared with the state-of-the-art fine-tuned model (Ma et al., 2022) using top-50 consolidated evidence, there still remains a noticeable gap in performance. Besides a lower answer recall of the consolidated evidence, we attribute it to extra alignments required for ChatGPT to respond in a more concise way and conduct faithful step-by-step reasoning. Therefore, there is ample room for future explorations on elicitive prompting to achieve further improvements.

5 Related Work

Numerous LLMs for text generation (Radford et al., 2018) have been proposed over the years, including very competitive ones such as GPT-3 (Brown et al., 2020; Ouyang et al., 2022), OPT (Zhang et al., 2022), GPT-j (Wang and Komatsuzaki, 2021), and ChatGPT. However, most of them do not naturally incorporate external knowledge. To address this limitation, various works augment LLMs with knowledge consisting of *e.g.*, personalized recommendations (Ghazvininejad et al., 2017), Wikipedia article and web search (Dinan et al., 2018; Shuster et al., 2022), structured and unstructured knowledge of task-oriented dialog (Peng et al., 2022). Recent advances have focused on jointly finetuning the retriever and generation components of retrieval-augmented text generation systems (Lewis et al., 2020; Zhang et al., 2021), but these methods are not applicable to black-box LLMs.

More recent work attempts to combine black-box LLMs with external knowledge, such as incorporating external knowledge into prompts (Madaan et al., 2022; Lazaridou et al., 2022), making GPT-3 more faithful (He et al., 2022), and combining web knowledge with GPT-3 (Nakano et al., 2021). In very recent works related to ours, Shi et al. (2023) tune the ranker of a black-box LLM. Schick et al. (2023) tune black-box LLMs’

access to different APIs and show improvement on a variety of understanding and reasoning tasks. We consider these works to be complementary to ours, as we assume our set of APIs to be given and fixed, and we instead focus more on when and what APIs to request, interactive feedback with the LLM, and developing a self-learning ability through utility functions.

6 Limitations and Future Directions

A main limitation of this work is that interactive feedback with a computationally expensive model such as ChatGPT can significantly slow down the user experience, as ChatGPT is often queried twice for a single response. However, we think this can translate into more choice for the user. For example, the initial ChatGPT response can be shown to the user as it is being decoded, and the user could then be informed that a more accurate response is available (depending on the utility function). Then, an impatient user can decide to ignore this option, while a user more mindful of response accuracy may decide to see the improved ChatGPT response. In task-oriented and high-stakes scenarios, we believe many users would prefer the slower but more accurate option.

The main results of the paper are with a policy designed manually, as due to the current high-demand for ChatGPT and its limited bandwidth. As reinforcement learning can be quite sample inefficient, we trained our policy using an LLM (T5-Base) we could easily query, and these RL experiments demonstrate the effectiveness of LLM-AUGMENTER. As ChatGPT becomes more available, we plan to update the paper with RL experiments involving ChatGPT. The current version of the paper does not include human evaluation, as the goal with our current utility function (KF1) shown we can make ChatGPT more grounded and our experiments suggest the responses of our best system are better at capturing the words of the (gold) knowledge. As we move towards much utility functions such as safety, it will be important to add more fine-grained analyses of the responses, and we will add human evaluation. In future work, we also plan to leverage interactions with real users and user feedbacks to train LLM-AUGMENTER.

7 Conclusions

We introduced LLM-AUGMENTER, a framework for augmenting black-box LLMs (e.g., ChatGPT) with external knowledge and automated feedback. The external knowledge provided as part of the LLM prompts helps generate more responses that are more grounded into external knowledge relevant to the current conversation. The automated feedback elicits the “follow-up correction” abilities of models such as ChatGPT and InstructGPT in order to produce revised responses that rank higher according to some given utility functions (e.g., groundedness as measured by KF1). These various components are integrated together as part of an RL framework, which we optimize end-to-end using policy gradient. End-to-end experiments with T5 show the effectiveness of LLM-AUGMENTER, while experiments on ChatGPT show significant increases both in terms of KF1 and a host of text generation metrics.

Ethics Statement

It is widely understood that large language models have the potential to generate harmful, offensive, and inappropriate content (Bender et al., 2021; Bommasani et al., 2021; Weidinger et al., 2021). This paper is an attempt to address a major harm of LLMs, namely factual integrity. This paper does not address the problem of offensive content generation, but future work on LLM-AUGMENTER could help mitigate such harm via, e.g., offensiveness-related utility functions.

As with other knowledge-augmented text generation applications, we cannot rule out that external sources could compromise the factuality of generated text. It is, therefore, important to encourage users to check the relevance of external sources that supplement the generated text.

Acknowledgements

We thank Saleema Amershi, Ahmed Awadallah, Nguyen Bach, Paul Bennett, Chris Brockett, Weixin Cai, Dhivya Eswaran, Adam Fourney, Hsiao-Wuen Hon, Chunyuan Li, Ricky Loynd, Hoifung Poon, Corby Rosset, Bin Yu, Sheng Zhang, and members of the Microsoft Research Deep Learning group for valuable discussions and comments.

References

- Satanjeev Banerjee and Alon Lavie. 2005. ME-TOR: An automatic metric for mt evaluation with improved correlation with human judgments. In *ACL Workshop on Intrinsic and Extrinsic Evaluation Measures for Machine Translation and/or Summarization*, pages 65–72.
- Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. 2021. On the dangers of stochastic parrots: Can language models be too big? *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*.
- Rishi Bommasani, Drew A. Hudson, Ehsan Adeli, Russ Altman, Simran Arora, Sydney von Arx, Michael S. Bernstein, Jeannette Bohg, Antoine Bosselut, Emma Brunskill, Erik Brynjolfsson, S. Buch, Dallas Card, Rodrigo Castellon, Niladri S. Chatterji, Annie S. Chen, Kathleen A. Creel, Jared Davis, Dora Demszky, Chris Donahue, Moussa Doumbouya, Esin Durmus, Stefano Ermon, John Etchemendy, Kawin Ethayarajh, Li Fei-Fei, Chelsea Finn, Trevor Gale, Lauren E. Gillespie, Karan Goel, Noah D. Goodman, Shelby Grossman, Neel Guha, Tatsunori Hashimoto, Peter Henderson, John Hewitt, Daniel E. Ho, Jenny Hong, Kyle Hsu, Jing Huang, Thomas F. Icard, Saahil Jain, Dan Jurafsky, Pratyusha Kalluri, Siddharth Karamcheti, Geoff Keeling, Fereshte Khani, O. Khattab, Pang Wei Koh, Mark S. Krass, Ranjay Krishna, Rohith Kuditipudi, Ananya Kumar, Faisal Ladhak, Mina Lee, Tony Lee, Jure Leskovec, Isabelle Levent, Xiang Lisa Li, Xuechen Li, Tengyu Ma, Ali Malik, Christopher D. Manning, Suvir Mirchandani, Eric Mitchell, Zanele Munyikwa, Suraj Nair, Avani Narayan, Deepak Narayanan, Benjamin Newman, Allen Nie, Juan Carlos Niebles, Hamed Nilforoshan, J. F. Nyarko, Giray Ogut, Laurel J. Orr, Isabel Papadimitriou, Joon Sung Park, Chris Piech, Eva Portelance, Christopher Potts, Aditi Raghunathan, Robert Reich, Hongyu Ren, Frieda Rong, Yusuf H. Roohani, Camilo Ruiz, Jack Ryan, Christopher R’e, Dorsa Sadigh, Shiori Sagawa, Keshav Santhanam, Andy Shih, Krishna Parasuram Srinivasan, Alex Tamkin, Rohan Taori, Armin W. Thomas, Florian Tramèr, Rose E. Wang, William Wang, Bohan Wu, Jiajun Wu, Yuhuai Wu, Sang Michael Xie, Michihiro Yasunaga, Jiaxuan You, Matei A. Zaharia, Michael Zhang, Tianyi Zhang, Xikun Zhang, Yuhui Zhang, Lucia Zheng, Kaitlyn Zhou, and Percy Liang. 2021. On the opportunities and risks of foundation models. *ArXiv*, abs/2108.07258.
- Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel Ziegler, Jeffrey Wu, Clemens Winter, Chris Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. 2020. Language models are few-shot learners. In *Advances in Neural Information Processing Systems*, volume 33, pages 1877–1901.
- Aakanksha Chowdhery, Sharan Narang, Jacob Devlin, Maarten Bosma, Gaurav Mishra, Adam Roberts, Paul Barham, Hyung Won Chung, Charles Sutton, Sebastian Gehrmann, et al. 2022. Palm: Scaling language modeling with pathways. *arXiv preprint arXiv:2204.02311*.
- Emily Dinan, Stephen Roller, Kurt Shuster, Angela Fan, Michael Auli, and Jason Weston. 2018. Wizard of Wikipedia: Knowledge-powered conversational agents. In *International Conference on Learning Representations*.
- Mihail Eric, Rahul Goel, Shachi Paul, Adarsh Kumar, Abhishek Sethi, Peter Ku, Anuj Kumar Goyal, Sanchit Agarwal, Shuyang Gao, and Dilek Hakkani-Tur. 2019. Multiwoz 2.1: A consolidated multi-domain dialogue dataset with state corrections and state tracking baselines. *arXiv preprint arXiv:1907.01669*.
- Michel Galley, Chris Brockett, Xiang Gao, Jianfeng Gao, and Bill Dolan. 2019. Grounded response generation task at DSTC7. In *AAAI Dialog System Technology Challenges Workshop*.
- Jianfeng Gao, Michel Galley, and Lihong Li. 2019. Neural approaches to conversational AI. *Foundations and Trends in Information Retrieval*, 13(2-3):127–298.
- Jianfeng Gao, Chenyan Xiong, Paul Bennett, and Nick Craswell. 2022. Neural approaches to conversational information retrieval. *arXiv preprint arXiv:2201.05176*.
- Marjan Ghazvininejad, Chris Brockett, Ming-Wei Chang, Bill Dolan, Jianfeng Gao, Wen-tau Yih, and Michel Galley. 2017. A knowledge-grounded neural conversation model. *CoRR*, abs/1702.01932.
- Amelia Glaese, Nathan McAleese, Maja Trkebacz, John Aslanides, Vlad Firoiu, Timo Ewalds, Maribeth Rauh, Laura Weidinger, Martin Chadwick, Phoebe Thacker, Lucy Campbell-Gillingham, Jonathan Uesato, Po-Sen Huang, Ramona Comanescu, Fan Yang, A. See, Sumanth Dathathri, Rory Greig, Charlie Chen, Doug Fritz, Jaume Sanchez Elias, Richard Green, Sovna Mokr’a, Nicholas Fernando, Boxi Wu, Rachel Foley, Susannah Young, Iason Gabriel, William S. Isaac, John F. J. Mellor, Demis Hassabis, Koray Kavukcuoglu, Lisa Anne Hendricks, and Geoffrey Irving. 2022. Improving alignment of dialogue agents via targeted human judgements. *ArXiv*, abs/2209.14375.
- Kelvin Guu, Kenton Lee, Zora Tung, Panupong Paspupat, and Ming-Wei Chang. 2020. REALM: Retrieval-augmented language model pre-training. *ArXiv*, abs/2002.08909.

- Hangfeng He, Hongming Zhang, and Dan Roth. 2022. Rethinking with retrieval: Faithful large language model inference. *arXiv preprint arXiv:2301.00303*.
- Vladimir Karpukhin, Barlas Oguz, Sewon Min, Patrick Lewis, Ledell Wu, Sergey Edunov, Danqi Chen, and Wen-tau Yih. 2020. Dense passage retrieval for open-domain question answering. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 6769–6781, Online. Association for Computational Linguistics.
- Seokhwan Kim, Mihail Eric, Karthik Gopalakrishnan, Behnam Hedayatnia, Yang Liu, and Dilek Hakkani-Tur. 2020. Beyond domain APIs: Task-oriented conversational modeling with unstructured knowledge access. In *Proceedings of the 21th Annual Meeting of the Special Interest Group on Discourse and Dialogue*, pages 278–289.
- Seokhwan Kim, Spandana Gella, Di Jin, Alexandros Papangelis, Behnam Hedayatnia, Yang Liu, and Dilek Hakkani-Tür. 2023. DSTC11 track proposal: Task-oriented conversational modeling with subjective knowledge. <https://github.com/alexa/dstc11-track5>.
- Angeliki Lazaridou, Elena Gribovskaya, Wojciech Stokowiec, and Nikolai Grigorev. 2022. Internet-augmented language models through few-shot prompting for open-domain question answering. *arXiv preprint arXiv:2203.05115*.
- Patrick Lewis, Ethan Perez, Aleksandara Piktus, Fabio Petroni, Vladimir Karpukhin, Naman Goyal, Heinrich Kuttler, Mike Lewis, Wen tau Yih, Tim Rocktäschel, Sebastian Riedel, and Douwe Kiela. 2020. Retrieval-augmented generation for knowledge-intensive nlp tasks. *ArXiv*, abs/2005.11401.
- Rongzhong Lian, Min Xie, Fan Wang, Jinhua Peng, and Hua Wu. 2019. Learning to select knowledge for response generation in dialog systems. In *International Joint Conference on Artificial Intelligence*.
- Chin-Yew Lin. 2004. ROUGE: A package for automatic evaluation of summaries. In *ACL workshop*, pages 74–81.
- Kaixin Ma, Hao Cheng, Xiaodong Liu, Eric Nyberg, and Jianfeng Gao. 2022. Open-domain question answering via chain of reasoning over heterogeneous knowledge. *arXiv preprint arXiv:2210.12338*.
- Aman Madaan, Niket Tandon, Peter Clark, and Yiming Yang. 2022. Memory-assisted prompt editing to improve GPT-3 after deployment. *arXiv preprint arXiv:2201.06009*.
- Reiichiro Nakano, Jacob Hilton, Suchir Balaji, Jeff Wu, Long Ouyang, Christina Kim, Christopher Hesse, Shantanu Jain, Vineet Kosaraju, William Saunders, et al. 2021. WebGPT: Browser-assisted question-answering with human feedback. *arXiv preprint arXiv:2112.09332*.
- Long Ouyang, Jeff Wu, Xu Jiang, Diogo Almeida, Carroll L. Wainwright, Pamela Mishkin, Chong Zhang, Sandhini Agarwal, Katarina Slama, Alex Ray, John Schulman, Jacob Hilton, Fraser Kelton, Luke E. Miller, Maddie Simens, Amanda Askell, Peter Welinder, Paul Francis Christiano, Jan Leike, and Ryan J. Lowe. 2022. Training language models to follow instructions with human feedback. *ArXiv*, abs/2203.02155.
- Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. 2002. BLEU: a method for automatic evaluation of machine translation. In *ACL*, pages 311–318.
- Baolin Peng, Michel Galley, Pengcheng He, Chris Brockett, Lars Lidén, Elnaz Nouri, Zhou Yu, Bill Dolan, and Jianfeng Gao. 2022. GODEL: Large-scale pre-training for goal-directed dialog. *ArXiv*, abs/2206.11309.
- Maja Popović. 2015. chrF: character n-gram F-score for automatic MT evaluation. In *Proceedings of the Tenth Workshop on Statistical Machine Translation*, pages 392–395, Lisbon, Portugal. Association for Computational Linguistics.
- Alec Radford, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. 2018. Improving language understanding by generative pre-training.
- Timo Schick, Jane Dwivedi-Yu, Roberto Dessì, Roberta Raileanu, Maria Lomeli, Luke Zettlemoyer, Nicola Cancedda, and Thomas Scialom. 2023. Toolformer: Language models can teach themselves to use tools.
- Thibault Sellam, Dipanjan Das, and Ankur Parikh. 2020. BLEURT: Learning robust metrics for text generation. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pages 7881–7892, Online.
- Weijia Shi, Sewon Min, Michihiro Yasunaga, Minjoon Seo, Rich James, Mike Lewis, Luke Zettlemoyer, and Wen tau Yih. 2023. REPLUG: Retrieval-augmented black-box language models. *ArXiv*, abs/2301.12652.
- Kurt Shuster, Spencer Poff, Moya Chen, Douwe Kiela, and Jason Weston. 2021. Retrieval augmentation reduces hallucination in conversation. *arXiv preprint arXiv:2104.07567*.
- Kurt Shuster, Jing Xu, Mojtaba Komeili, Da Ju, Eric Michael Smith, Stephen Roller, Megan Ung, Moya Chen, Kushal Arora, Joshua Lane, Morteza Behrooz, W.K.F. Ngan, Spencer Poff, Naman Goyal, Arthur D. Szlam, Y-Lan Boureau, Melanie Kam-bador, and Jason Weston. 2022. BlenderBot 3: a deployed conversational agent that continually learns to responsibly engage. *ArXiv*, abs/2208.03188.
- Ben Wang and Aran Komatsuzaki. 2021. GPT-J-6B: A 6 billion parameter autoregressive language model. <https://github.com/kingoflolz/mesh-transformer-jax>.

- Laura Weidinger, John F. J. Mellor, Maribeth Rauh, Conor Griffin, Jonathan Uesato, Po-Sen Huang, Myra Cheng, Mia Glaese, Borja Balle, Atoosa Kasirzadeh, Zachary Kenton, Sande Minnich Brown, William T. Hawkins, Tom Stepleton, Courtney Biles, Abeba Birhane, Julia Haas, Laura Rimell, Lisa Anne Hendricks, William S. Isaac, Sean Legassick, Geoffrey Irving, and Iason Gabriel. 2021. Ethical and social risks of harm from language models. *ArXiv*, abs/2112.04359.
- Ronald J. Williams. 1992. Simple statistical gradient-following algorithms for connectionist reinforcement learning. *Machine Learning*, 8:229–256.
- Yi-Ting Yeh, Maxine Eskenazi, and Shikib Mehri. 2021. A comprehensive assessment of dialog evaluation metrics. In *arXiv*.
- Weizhe Yuan, Graham Neubig, and Pengfei Liu. 2021. BARTScore: Evaluating generated text as text generation.
- Susan Zhang, Stephen Roller, Naman Goyal, Mikel Artetxe, Moya Chen, Shuohui Chen, Christopher Dewan, Mona Diab, Xian Li, Xi Victoria Lin, Todor Mihaylov, Myle Ott, Sam Shleifer, Kurt Shuster, Daniel Simig, Punit Singh Koura, Anjali Sridhar, Tianlu Wang, and Luke Zettlemoyer. 2022. OPT: Open pre-trained transformer language models. *ArXiv*, abs/2205.01068.
- Tianyi Zhang, Varsha Kishore, Felix Wu, Kilian Q. Weinberger, and Yoav Artzi. 2019. BERTScore: Evaluating text generation with BERT. *CoRR*, abs/1904.09675.
- Yizhe Zhang, Siqi Sun, Xiang Gao, Yuwei Fang, Chris Brockett, Michel Galley, Jianfeng Gao, and Bill Dolan. 2021. RetGen: A joint framework for retrieval and grounded text generation modeling. In *AAAI Conference on Artificial Intelligence*.
- Zexuan Zhong, Tao Lei, and Danqi Chen. 2022. Training language models with memory augmentation. *ArXiv*, abs/2205.12674.

A Appendix

Table 6 provides sample responses contrasting ChatGPT and LLM-AUGMENTER. First, we can see that ChatGPT fails to provide a response related to specific knowledge related to the user, *e.g.*, a local Indian restaurant. In the second part of the table, we show LLM-AUGMENTER’s Working Memory, which highlights the richer information retrieved from external knowledge to help the underlying LLM (*i.e.*, ChatGPT as well) generate more contentful responses. The first LLM response received by LLM-AUGMENTER is unfortunately not satisfactory, as the quality and specificity of LLM generation can be unpredictable. In this case, the Utility module has determined that the first response did not meet its criteria (*i.e.*, KF1 above a given threshold), and issues a feedback to the LLM module (*i.e.*, “response is inconsistent with the knowledge”). The second response received by LLM-AUGMENTER is much more satisfactory according to the utility function, and therefore sent to the user.

Instruction	I want you to act as a chatbot AI for travel planning. You need to answer customer's questions nicely.
Context	<p>User: Hello, I am looking for a moderately priced restaurant on the north side of town.</p> <p>Assistant: I recommend golden wok. It is in the north part of town with a moderate price range.</p> <p>User: Yes, I am looking for a moderately priced restaurant in the north part of town.</p> <p>Assistant: I recommend golden wok. It is in the north part of town with a moderate price range.</p> <p>User: I don't want Golden Wok, is there anything else?,</p> <p>Assistant: Yes, your other option is The Nirala. It serves Indian food and is also located in the north part of town.</p> <p>User: Is their beer a good value for the money?</p>
ChatGPT Response	I am sorry, I do not have information on the beer prices at The Nirala. It is best to contact the restaurant directly for more information.
Working Memory	<p>Review: They also have a modest drinks menu with some affordable prices, but I was more interested in the beautiful view from my window seat, which allowed me to watch the sun setting as I dined.</p> <p>Q: Is alcohol served at this restaurant? A: Yes, alcohol is served at this restaurant.</p> <p>Review: I found them to be overpriced and mediocre.</p> <p>Review: The drinks ae priced well.</p> <p>Review: Something that I disliked, however was the prices for their drinks.</p>
LLM-AUGMENTER Response	I am sorry, I do not have information on the value of their beer. I only have information on the location and price range of the restaurant.
Rule-based Feedback	The response is inconsistent with the knowledge. Please generate again?
LLM-AUGMENTER Response	Some reviews mention that the drinks at the restaurant are priced well, while others mention that they found the prices to be overpriced and mediocre.
Human Response	Unfortunately the reviews are split, half say they are overpriced and have say they are affordable.

Table 6: Prompt and example responses of different models for the customer service scenarios.

I want you to act as a chatbot. You need to answer user' questions nicely.

Context:

User: $[U_1]$

Assistant: $[R_1]$

...

User: $[U_t]$

Assistant: $[R_t]$

I want you to act as a chatbot. You will be presented with knowledge snippets. You need to answer user' questions nicely and accurately based on the knowledge snippets.

Working Memory: $[M_t]$

Context:

User: $[U_1]$

Assistant: $[R_1]$

...

User: $[U_t]$

Assistant: $[R_t]$

Table 7: Prompt Templates for News Chat. LLMs generated responses is highlighted with $[R_t]$.

I want you to act as a chatbot AI for travel planning. You need to answer customer's questions nicely.

Context:

User: $[U_1]$

Assistant: $[R_1]$

...

User: $[U_t]$

Assistant: $[R_t]$

I want you to act as a chatbot AI for travel planning. You will be presented with knowledge snippets. You need to answer customer's questions nicely and accurately based on the knowledge snippets.

Working Memory: $[M_t]$

Context:

User: $[U_1]$

Assistant: $[R_1]$

...

User: $[U_t]$

Assistant: $[R_t]$

Table 8: Prompt Templates for Customer Service. LLMs generated response are highlighted with $[R_t]$.

I am a highly intelligent question answering bot that can answer questions. If you ask me a question that is rooted in truth, I will give you the answer. If you ask me a question that is nonsense, trickery, or has no clear answer, I will respond with "Unknown".

Question: $[Q]$

Answer: $[A]$

I am a highly intelligent question answering bot, and can answer questions given some documents and tables. If you ask me a question that is rooted in truth, I will give you the answer. If you ask me a question that is nonsense, trickery, or has no clear answer, I will respond with "Unknown".

Working Memory: $[M]$

Question: $[Q]$

Answer: $[A]$

Table 9: Prompt Templates for Wiki QA. LLMs generated response are highlighted with $[A]$.