**Abstract**

Personalizing conversational agents can enhance the quality of conversations and increase user engagement. However, they often lack external knowledge to appropriately tend to a user’s persona. This is crucial for practical applications like mental health support, nutrition planning, culturally sensitive conversations, or reducing toxic behavior in conversational agents. To enhance the relevance and comprehensiveness of personalized responses, we propose using a two-step approach that involves (1) selectively integrating user personas and (2) contextualizing the response by supplementing information from a background knowledge source.

We develop $\mathcal{K}$-PERM (Knowledge-guided Personalization with Reward Modulation), a dynamic conversational agent that combines these elements. $\mathcal{K}$-PERM achieves state-of-the-art performance on the popular FoCuS dataset, containing real-world personalized conversations concerning global landmarks. We show that using responses from $\mathcal{K}$-PERM can improve performance in state-of-the-art LLMs (GPT 3.5) by 10.5%, highlighting the impact of $\mathcal{K}$-PERM for personalizing chatbots. Our code is released to the public for further explorations: https://github.com/kanak8278/DialogKPERM.

**Introduction**

Recent trends in Large Language Models (LLMs) have demonstrated remarkable abilities in conversational AI (Jo et al. 2023)(Shin, Hsieh, and Kim 2023). However, personalization is a potential area for LLMs that requires improvement (Zhang et al. 2023). Personalization in conversational AI can go beyond chit-chat conversations and aid in user engagement by understanding their personas better and providing accurate responses (Bender et al. 2021)(Joshi, Mi, and Faltings 2017).

Prior research on personalization has primarily focused on casual conversations, emphasizing details such as a user’s preferences. The lack of external knowledge hinders a model’s ability to adapt to different personas (Deshpande et al. 2023). Therefore, recent shifts in chatbot personalization utilize both persona information and knowledge (Qian et al. 2021) (Liu et al. 2023). However, identifying a suitable context aligned with user preferences during a conversation remains a significant challenge for current LLMs.

While using various prompting methods may allow a user to steer LLMs toward desired behavior, they only work at an utterance level. This may not be feasible for longer conversations, as the context often shifts (Shuster et al. 2021). Therefore, we require the chatbot to learn how to retrieve appropriate content based on a user’s query and assess whether a response requires contextualization (retrieval of meta-information) and personalization (selecting appropriate persona, if necessary).

To address this issue, we propose using Knowledge-guided Personalization of response generation with Reward Modulation ($\mathcal{K}$-PERM). $\mathcal{K}$-PERM uses dynamic knowledge retrieval along with personalization to improve a machine’s adaptive capabilities to different personas and contexts. Our Personalized Response Generation task involves two major components:

1. **Understanding Conversation Context:** We use Dense Passage Retrieval (DPR) (Karpukhin et al. 2020) to select the most pertinent information from a larger text corpus containing real-world information.

2. **Incorporating Appropriate Personas:** We introduce a selector module capable of choosing a persona that aligns with the user query. We model persona selection as a multiple-choice question-answering task, which includes an option to opt for “no-persona” in generic cases.

To the best of our knowledge, our study is the first to dynamically and flexibly incorporate knowledge, persona, and conversation history into a learning strategy that can be used to train or guide LLMs to be personalized. Our model-agnostic framework can be utilized to train conversational agents for personalized response generation in open-domain settings. $\mathcal{K}$-PERM outperforms prior attempts in personalization despite being a 24 times smaller model. We also augment GPT 3.5 with $\mathcal{K}$-PERM’s responses and show a considerable improvement of 10.5% when compared to GPT3.5 in
personalized responses. Our method personalizes based on formation to select compatible user personas and generate their relevance. This allows us to leverage the retrieved in-store, retrieve pertinent passages, and rank them based on Figure 1 explains the entire model architecture of \( \mathcal{K} \)-PERM. The model architecture comprises a Persona Selector and Knowledge Extractor, which leverages the history and question prompt to identify pertinent persona and knowledge.

a zero-shot setting. Our results demonstrate that knowledge-guided learning can help guide conversational agents toward better personalization.

**Methodology**

Let \( U^t = \{ u^t_1, u^t_2, \ldots, u^t_H \} \) be the history of \( H \) user utterances on a topic \( t \). Each utterance \( u^t_i \in U^t \) is a question and response pair denoted as \((q^t_i, r^t_i)\). The \( q^t_i \) are questions by the user, specific to the topic \( t \), and the \( r^t_i \) are responses that are either tailored according to a set of \( n \) user personas \( P = \{ p_1, p_2, \ldots, p_n \} \) or generic (no-persona). Our goal is to model the probability of the latest user response \( r^t_H \) given a set of \( K \) passages, denoted by \( Z^t_K \), relevant to the utterance history \( U^t \) (the passages are drawn from an external knowledge source, e.g., a document store). Thus, our goal is to learn the probability distribution

\[
 \mathbb{P}_\theta(r^t_H | Z^t_K) \tag{1}
\]

where \( \theta \) are the parameters of the probability distribution.

\( \mathbb{P}_\theta \) can be any auto-regressive language model capable of generating sentences token-wise. Since the user is likely to have responded according to their set of personas, we train a persona selector module \( P_{\text{select}} \), that as input the user’s utterance history \( U^t \), and the set of passages \( Z^t_K \), and outputs one or more personas from \( P \) (denoted as \( P' \)) for customizing responses using \( \mathbb{P}_\theta \). Therefore, Equation (1) is modified as

\[
 P' = P_{\text{select}}(Z^t_K, P), \quad P' \subseteq P, \quad \mathbb{P}_\theta(r^t_H | Z^t_K, P') \tag{2}
\]

\( \mathcal{K} \)-PERM

Figure 1 explains the entire model architecture of \( \mathcal{K} \)-PERM. Utilizing the conversation history \( U^t \), we access a document store, retrieve pertinent passages, and rank them based on their relevance. This allows us to leverage the retrieved information to select compatible user personas and generate personalized responses. Our method personalizes based on the personas in \( P' \). If \( P' = \emptyset \), generic responses are generated.

**Knowledge Retriever**

For dynamically retrieving passages based on \( U^t \), we built upon a process called DPR – \( P_{\text{select}} \) in Equation (2). DPR uses semantic similarity search to retrieve passages from a vectorized database. This allows us to go beyond an exact-match by retrieving passages that can answer reasoning-type questions (what is? what if? what could be?) by automatically adapting to the input queries in \( U^t \).

We improve DPR in two ways. First, we utilize a Sentence-BERT model for performing a *retrieve-rank process using a paired cross-encoder and bi-encoder*. A cross-encoder retrieves a set of passages given the last query \( q^t_H \in U^t \), and subsequently, the bi-encoder ranks and selects the top-\( K \) passages to result in \( Z^t_K \). We create dense encodings of the passages in \( Z^t_K \) using the MPNet model from the Sentence-BERT transformer family (Reimers and Gurevych 2019). Likewise, the encoding for \( q^t_H \) is represented as \( z^t_H \). We fine-tune MPNet on our dataset before using it to obtain dense encodings (refer Appendix D) (Song et al. 2020).

**Persona Selector (\( P_{\text{select}} \))**

We model persona selection as a commonsense inference task, conditioned upon the query knowledge \( Z^t_K \) retrieved using the information in \( q^t_H \) and the set of user-personas \( P \), formally written as \( P' = P_{\text{select}}(Z^t_K, P) \) as shown in Equation (2). The dataset contains the ground truth for the user’s personas corresponding to the responses in the utterance history \( U^t \). Using this, we train the \( P_{\text{select}} \) model as a multi-label classifier and sample the top-2 classes from the resulting logits (\(|P'| = 2\)). For the base \( P_{\text{select}} \) model, we empirically observed XLNET as the best performer (Yang et al. 2019).
Response Generation through Reward Modulation

The response is generated by pairing a BART(Base) generator with an ELECTRA(Base) evaluator that measures the similarity between the generated response and the ground truth (Clark et al. 2019). We introduce a balancing reward function \( R_t \) modulating generative capabilities (e.g., coherency) of the BART model and high fidelity to the ground truth responses (in terms of matched words).

**Reward Function**

Consider the ground truth response for a query \( q^i_t \) to be \( r^i_t \), which consists of \( n \) tokens, where each token is indexed using \( t_i \). Let \( r^k_t \) be the \( k \)th response in the generated response list comprising \( m \) tokens, where each token is indexed using \( t_j \). We generate BERT encodings for each word in the response vectors, both for the \( n \) words in \( r^i_t \) and the \( m \) words in \( r^k_t \). The reward \( R_t \) is

\[
R_t = \alpha \cdot \text{BLEU}(r^i_t, r^k_t) + (1 - \alpha) \sum_{(t_i, r^i_t, t_j, r^k_t)} \max_{t_i} \text{WMD}(t_i, t_j) \tag{3}
\]

where WMD denotes the Word Mover Distance (Kusner et al. 2015) and \( \alpha[s] \in [0, 1] \) balances between a well-generated response by BART (given by the WMD distance) and closeness to the ground truth responses (provided by the BLEU score).

**Persona-tailored Reward Function**

In addition to producing syntactically sound responses and responses that are close to the ground truth, the responses need to be tailored to user-personas, i.e., the output of the \( P_{\text{select}} \) model. Thus, we modify Equation (3) as follows:

\[
R_t = \alpha \text{BLEU}(r^i_t, r^k_t) + \beta \sum_{(t_i, r^i_t, t_j, r^k_t)} \max_{t_i} \text{WMD}(t_i, t_j) + \gamma \cdot \text{Loss}(P_{\text{select}}, P_{\text{gt}}), \quad \alpha + \beta + \gamma = 1 \tag{4}
\]

where \( gt \) is the ground truth, and \( \text{Loss}(P_{\text{select}}, P_{\text{gt}}) \) refers to the loss function, i.e., the training error in the persona selected and the ground truth persona (if present).

**Experiments**

We utilize the FoCus dataset developed by Jang et al. (2022) for our experiments, as it contains customized answers built with persona and Wikipedia knowledge instead of just personas ((Zhang et al. 2018)). See Appendix A for dataset details. Our experiments use BART as the language model \( \mathcal{F}_{\theta} \). Fine-tuning details are described in Appendix C.

**Evaluation Criteria**

We used Rouge-1/2/L/L-Sum and BLEU scores to evaluate \( K \)-PERM. In addition, we use two transformer-based metrics for evaluating natural language generation: BERTScore (BF1: BERTScore F1-score) and NUBIA, which measure semantic relations, contractions, irrelevancy, and logical agreement (Zhang et al. 2020; Kane et al. 2020). Semantic relations evaluate whether the generated text is relevant and coherent and maintains the intended meaning and context of the input query. Measuring these characteristics for our proposed model is important to ensure LLMs’ correct merging of knowledge and persona.

**Baselines**

We compare our model with two baselines – (1) GODEL: A large pre-trained Transformer-based encoder-decoder model for goal-directed dialogues similar to FoCus (Peng et al. 2022). We used the pre-trained GODEL model and enhanced it with personalization by incorporating a persona selected by our persona selector model; (2) BART_FoCus: We utilized the BART model provided with the FoCus dataset (Jang et al. 2022). We fine-tuned this model (BART_FoCus) using our training and validation sets for a fair comparison. Results are reported on our test set, although it was not made available by the authors of the FoCus dataset.

**Results and Discussion**

Table 1 compares three models: BART_FoCus (406 Million Parameters), GODEL (6 Billion parameters), and \( K \)-PERM (250 Million parameters). The results show that the pre-trained version of GODEL, without personalization, performed worse than BART_FoCus. However, when GODEL incorporated our persona selector model, it achieved a syntactic similarity closer to BART_FoCus, suggesting that the persona-based approach improved GODEL’s syntactic quality—in terms of semantic similarity measured by BERTScore, GODEL with persona outperformed BART_FoCus, indicating that GODEL, when utilizing personas, generated responses that were more semantically similar to the desired outputs. \( K \)-PERM significantly outperformed GODEL in terms of syntactic generation quality and semantic similarity. Ablation studies (see Appendix Table 2) on \( K \)-PERM showed that using the ground persona and our persona selector resulted in the highest quality generation both syntactically and semantically. However, there were cases where \( K \)-PERM ignored the persona for specific queries requiring personalization, resulting in errors compared to using the ground persona. Despite this limitation, the knowledge retriever used in \( K \)-PERM demonstrated competitive performance, relying on information from Wikipedia articles rather than handcrafted knowledge in the FoCus dataset.

Another set of experiments with \( K \)-PERM using NUBIA as the metric (see Table 2) showed that using personas yielded better semantic relations, logical agreement, lower contradiction, and lower irrelevancy compared to providing all personas simultaneously. When using retrieved knowledge, \( K \)-PERM achieved a higher NUBIA score compared to using handcrafted knowledge in BART_FoCus. In a blind assessment of responses obtained from 5 different systems, generated across 90 user queries with varying numbers of personas, \( K \)-PERM consistently outperformed the competition. It achieved the top position in 54 query cases, showcasing
Table 1: Performance of $\mathcal{K}$-PERM on FoCUs dataset.

<table>
<thead>
<tr>
<th>Models</th>
<th>BLEU</th>
<th>R1</th>
<th>R2</th>
<th>RL</th>
<th>BF1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptGODEL</td>
<td>5.21</td>
<td>25.82</td>
<td>9.87</td>
<td>21.2</td>
<td>43.86</td>
</tr>
<tr>
<td>ptGODEL ($P_{select}$)</td>
<td>6.18</td>
<td>30.02</td>
<td>13.77</td>
<td>26.11</td>
<td>44.34</td>
</tr>
<tr>
<td>BART_FoCus</td>
<td>6.24</td>
<td>30.98</td>
<td>14.22</td>
<td>26.81</td>
<td>43.85</td>
</tr>
<tr>
<td>$\mathcal{K}$-PERM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(without P, GK)</td>
<td>2.14</td>
<td>24.68</td>
<td>9.46</td>
<td>21.89</td>
<td>44.15</td>
</tr>
<tr>
<td>(GP only)</td>
<td>11.2</td>
<td>31.14</td>
<td>15.49</td>
<td>26.73</td>
<td>43.26</td>
</tr>
<tr>
<td>(GP only)</td>
<td>2.4</td>
<td>27.47</td>
<td>12.03</td>
<td>22.37</td>
<td>44.35</td>
</tr>
<tr>
<td>(All P+Z_k)</td>
<td>11.22</td>
<td>35.19</td>
<td>19.27</td>
<td>31.18</td>
<td>43.45</td>
</tr>
<tr>
<td>(GP+Z_k)</td>
<td>14.72</td>
<td>43.09</td>
<td>25.43</td>
<td>37.95</td>
<td>47.36</td>
</tr>
<tr>
<td>($P_{select}$+Z_k)</td>
<td>12.01</td>
<td>37.53</td>
<td>23.96</td>
<td>33.47</td>
<td>46.06</td>
</tr>
</tbody>
</table>

Table 1: Performance of $\mathcal{K}$-PERM on FoCus dataset.


Figure 2: $\mathcal{K}$-PERM improves personalization in GPT 3.5 via zero-shot prompting. This experiment aimed to assess the performance improvement of GPT 3.5 when combined with $\mathcal{K}$-PERM. M1 is GPT 3.5 and M2, M3, and M4 represents zero-shot prompting of GPT 3.5 using responses from $\mathcal{K}$-PERM with (All P+Z_k), (GP+Z_k), and ($P_{select}$+Z_k) respectively. Score were rounded off for visibility.

- Our methodology did not thoroughly experiment with all the state-of-the-art LLMs such as Llama and Mistral (Jiang et al. 2023). However, as our methods are model-agnostic, applying our work to these models should yield comparable results.

Appendix

A Dataset

We utilize the publicly available FoCus dataset, which consists of passages describing landmarks (Jang et al. 2022). The dataset includes 13,484 dialogs for training and validation, with an average of 5.6 rounds per dialog and approximately 7,715 Wikipedia landmarks. The dialogs contain a total of 75,971 utterances, with an average length of 24.0 per utterance. We split the dataset into three sets: train (10,284 samples), validation (1,600 samples), and test (1,600 samples), comprising 57,928, 9,008, and 9,035 utterances, respectively. The training set includes 36,472 knowledge-based utterances and 21,456 utterances with both persona and knowledge, coming from 4,918 landmarks. Validation and test datasets consist of 5,664 and 5,707 knowledge-based utterances, respectively. Additionally, the validation set includes 3,344 utterances featuring both persona and knowledge, while the test set comprises 3,328 such utterances. The validation set encompasses 1,414 Wikipedia landmarks, whereas the test set involves 1,383 landmarks. The dataset references “ground persona” and “ground knowledge,” representing the ground truth persona and passage selected by crowd workers. Additionally, all the questions in the dataset were rewritten using T5-CANARD, a query-rewriting model (Qian and Oard 2021) (Table 4 shows why question rewriting was needed).

B Related Work

PersonaChat and PersonaChat 2.0 are chit-chat conversation datasets used to train conversational agents (Liu, Peng, and Ni 2022; Wu et al. 2020). They incorporate encoder-decoder
models, reinforcement learning, few-shot learning, and hierarchical attention mechanisms to improve personalization by considering persona and conversational history (Li et al. 2016; Qiu and Zhang 2021; Young et al. 2022). In previous personalization work, external knowledge was not a significant factor until Mazumder et al. introduced retrieval as a sub-task in PersonaChat to enhance personalization (Mazumder et al. 2021). However, their method was not specifically evaluated on retrieval performance, using ROC Stories as a proxy knowledge source. This approach did not adequately capture personalization, especially for goal-oriented or information-seeking dialogues. K-PERM addresses this gap by introducing retrieval augmented generation as a practical baseline to improve personalization (Gaur et al. 2022; Lewis et al. 2020). Unlike previous approaches that fine-tuned models on PersonaChat, K-PERM uses base generative models for evaluation and achieves desired behaviors through reinforcement learning as the evaluator (Lipton et al. 2018; Huang et al. 2023). Additionally, K-PERM introduces unique persona selection, making it the first realistic response generation model for real-time goal-oriented or information-seeking dialogues.

C Human Evaluation

We conducted a blind evaluation of 90 responses generated from 5 systems. As the task was trivial, the authors instructed the annotators verbally. The task was made available on a participant pool management system which credits students completing the task. We experimented with five systems: K-PERM, BART_FoCus, ChatGPT, GODEL, and Ground Truth. Our model, K-PERM, consistently stood out as a top performer by securing first place in 11 instances and maintaining a strong second position in 68 instances. This underscores its exceptional performance. The Top 3 results and percentage of times any specific model is selected are depicted in Figure 3. Table 3 shows a sample from our human evaluation. More examples are present https://shorturl.at/ujP023.

D Fine-Tuning MPNet for DPR

We used contrastive fine-tuning as described in (Song et al. 2020). Next, we employed a combination of locality-sensitive hashing (LSH) and Facebook AI Semantic Search (FAISS), which uses Maximum Inner Product Search (MIPS) (Johnson, Douze, and Jégou 2019) to efficiently obtain \( Z_K \). We evaluated the knowledge retriever’s efficiency using BERTScore, which is commonly used to compare retriever-augmented generations (Lim et al. 2023).

We varied \( K \) between 5 and 20 and observed high similarity (BERTScore) with ground truth passages (from the FoCus dataset) at \( K = 10 \). Therefore, we agreed that the appropriate number of retrieved passages would be 10. We also experimented with different Sentence Transformer models for dense encodings other than MPNet and standard retrievers such as TF-IDF and BM25 (refer to Appendix Table 4).

E Training Process

We employed BART, an auto-regressive encoder-decoder model, for generating personalized responses by incorporating special tags like \( <\text{question}> \), \( <\text{knowledge}> \), \( <\text{history}> \), and \( <\text{persona}> \) during fine-tuning. Training took approximately 16 hours on a single NVIDIA T4 GPU, and response generation utilized beam search with a beam size of 5 for stability over nucleus sampling (Chen and Yang 2021; Shaham and Levy 2022).

Acknowledgements

We acknowledge partial support from the UMBC Faculty Fellowship to Dr. Manas Gaur. We also acknowledge High-Performance Computing Support from HealthcareNLP Softtech LLC and NSF MRI Award #1920079. Any opinions, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF, UMBC, or HealthcareNLP Softtech LLC.

References


Table 2: Performance of $K$-PERM using NUBIA Score. Results are compared with baseline BART\textsubscript{FoCus}. Bold-faced are best (GP), and Underlined are second-best ($P_{select}$). LA: Logical Agreement, SR: Semantic Relatedness.

<table>
<thead>
<tr>
<th>Models</th>
<th>NUBIA</th>
<th>SR</th>
<th>Contraction (%)</th>
<th>Irrelevancy (%)</th>
<th>LA (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$BART_{FoCus}$</td>
<td>0.10</td>
<td>1.601</td>
<td>28.72</td>
<td>72.71</td>
<td>16.75</td>
</tr>
<tr>
<td>$K$-PERM (GK only)</td>
<td>0.24</td>
<td>2.20</td>
<td>11.78</td>
<td>74.4</td>
<td>13.5</td>
</tr>
<tr>
<td>$K$-PERM (All P + $Z_k$)</td>
<td>0.22</td>
<td>1.90</td>
<td>13.18</td>
<td>70.1</td>
<td>17.5</td>
</tr>
<tr>
<td>$K$-PERM (GP + $Z_k$)</td>
<td><strong>0.34</strong></td>
<td><strong>2.80</strong></td>
<td><strong>11.87</strong></td>
<td><strong>66.38</strong></td>
<td><strong>21.75</strong></td>
</tr>
<tr>
<td>$K$-PERM (SP + $Z_k$)</td>
<td>0.31</td>
<td>2.42</td>
<td>11.85</td>
<td>69.61</td>
<td>19.44</td>
</tr>
</tbody>
</table>

Wikipedia Topic | /wiki/MountMonadnock
Query | Where is the mountain?

Personalized Response Generation: Example 1

<table>
<thead>
<tr>
<th>Ground Truth</th>
<th>Mount Monadnock is a mountain in the towns of Jaffrey and Dublin, New Hampshire.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BART\textsubscript{FoCus}</td>
<td>Mount Monadnock is at New Hampshire.</td>
</tr>
<tr>
<td>GODEL</td>
<td>It’s near the Rivers and the Masses.</td>
</tr>
<tr>
<td>ChatGPT</td>
<td>Based on the context and your persona, you have already visited Mount Monadnock! It is located in the towns of Jaffrey and Dublin, New Hampshire.</td>
</tr>
<tr>
<td>$K$-PERM*</td>
<td>Mount Monadnock is a 3,165-ft (965 m) mountain in the towns of Jaffrey and Dublin, New Hampshire, a place you have visited.</td>
</tr>
</tbody>
</table>

Wikipedia Topic | /wiki/Assiniboine_Park_Zoo
Query | Where is this place?

Personalized Response Generation: Example 1

| ChatGPT, “The query “Where is this place?” is referring to the Assiniboine Park Zoo in Winnipeg, Manitoba, Canada. If you like Canada, you should check out this zoo when possible! It’s been a staple of the city since 1904! |
| $K$-PERM†        | Assiniboine Park Zoo is an 80-acre (32 ha) zoo in Manitoba, Canada that was established in 1904. |

Table 3: Human Assessment: $K$-PERM did better than ChatGPT in terms of personalized response generation. The personas “I have been to New Hampshire” (top) and “I like visiting Canada” (bottom) were used in the examples above. We boldface numeric values to show focus on the correctness of information delivery using a retrieval-augmented generation mechanism.

Table 4: Evaluating knowledge retrievers over the indexed landmark Wikipedia articles in the FoCus dataset. Each score represents the maximum BERTScore computed between the retrieved passages and ground truth knowledge in FoCUS. pTECE: pre-trained ELECTRA Cross Encoder (Clark et al. 2020). Bold: Best, Underlined: 2nd best.


Kusner, M.; Sun, Y.; Kolkin, N.; and Weinberger, K. 2015. From word embeddings to document distances. In International conference on machine learning, 957–966. PMLR.


