

# 000 001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020 021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040 041 042 043 044 045 046 047 048 049 050 051 052 053 LEARNING TO ROUTE LLMS FROM BANDIT FEEDBACK: ONE POLICY, MANY TRADE-OFFS

Anonymous authors

Paper under double-blind review

## ABSTRACT

Efficient use of large language models (LLMs) is critical for deployment at scale: without adaptive routing, systems either overpay for strong models or risk poor performance from weaker ones. Selecting the right LLM for each query is fundamentally an online decision problem: models differ in strengths, prices fluctuate, and users value accuracy and cost differently. Yet most routers are trained offline with labels for all candidate models, an assumption that breaks in deployment, where only the outcome of the chosen model is observed. We bridge this gap with BaRP, a Bandit-feedback Routing with Preferences approach that trains under the same partial-feedback restriction as deployment, while supporting preference-tunable inference: operators can dial the performance–cost trade-off at test time without retraining. Framed as a contextual bandit over prompt features and a user preference vector, our method simulates an online feedback setting during training and adapts its routing decisions to each new prompt, rather than depending on full-information offline supervision. Comprehensive experiments show that our method consistently outperforms strong offline routers by at least 12.46% and the largest LLM by at least 2.45%, and generalizes robustly for unseen tasks.

## 1 INTRODUCTION

Large language models (LLMs) vary substantially in their strengths, weaknesses, and operating costs. No single model dominates across all prompts and tasks, and both pricing and quality change over time. Users and applications also vary in how they prioritize accuracy and cost. At deployment scale, a system must therefore decide *per query* which model to call under a performance–cost trade-off. A common solution is to employ a *router*, a learned policy that selects an LLM for each incoming prompt. The challenge is that, once deployed, the router only receives feedback from the model it actually calls: it observes the accuracy and cost of the selected model but learns nothing about the alternatives. This setting, where supervision is restricted to the chosen action, is known as *bandit feedback*. In contrast, most existing routers are trained offline with labels for all candidate models on every prompt, creating a mismatch between training and deployment.

Prior work illustrates two recurring limitations. The first is the reliance on *full-information offline supervision*, where training requires labels from all candidate LLMs on each prompt. For example, RouterDC (Chen et al., 2024) compares every prompt across multiple LLM outputs, so it cannot be trained once deployed, when only the chosen model’s feedback is available. GraphRouter (Feng et al., 2025) faces the same limitation, as it learns graph-structured representations that rely on full-information labels. The second limitation is the lack of *preference-tunable inference*, the ability to adjust routing at test time to reflect user-specified performance–cost trade-offs without retraining. For instance, RouterDC (Chen et al., 2024) yields a routing policy tied to the trade-off during

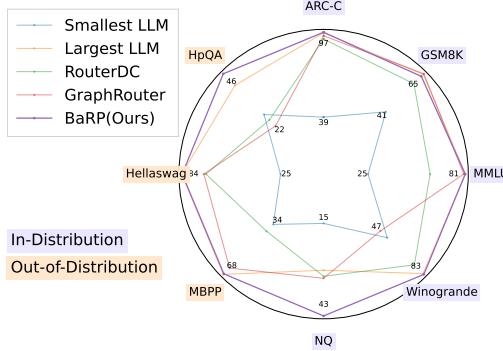


Figure 1: Testing score of baselines and BaRP on in-distribution and out-of-distribution tasks.

054  
 055 Table 1: Comparison of routing methods. “Full-information Offline Supervision” indicates that  
 056 training requires labels from all candidate LLMs for each prompt. “Preference-tunable In-  
 057 ference” refers to whether the method can adjust routing at test time to accommodate user-specified  
 058 performance–cost trade-offs without retraining.

Method	Full-information Offline Supervision	Preference-tunable Inference
GraphRouter (Feng et al., 2025)	Required	No
RouterDC (Chen et al., 2024)	Required	No
C2MAB-V (Dai et al., 2024)	Not required	No
MAR (Zhang et al., 2025)	Not required	No
LLM Bandit (Li, 2025)	Required	Yes
<b>BARP (Ours)</b>	<b>Not required</b>	<b>Yes</b>

060  
 061 training, GraphRouter (Feng et al., 2025) supports only three predefined scenarios and is therefore  
 062 not fully preference-tunable, while our method can shift its choices depending on whether a user  
 063 prioritizes performance or cost. Bandit-style approaches such as C2MAB-V (Dai et al., 2024) and  
 064 Multi-Armed Router (MAR) (Zhang et al., 2025) avoid full-information supervision but still lack  
 065 this controllability, and LLM Bandit (Li, 2025) introduces preferences but relies on offline pre-  
 066 training that assumes full labels. Table 1 summarizes these methods across the two dimensions of  
 067 supervision and controllability. Additional related work is discussed in Section 5.

068 We propose BARP, a Bandit-feedback Routing with Preferences framework that addresses both lim-  
 069 itations in a unified manner. Our formulation treats routing as a *multi-objective contextual bandit*  
 070 problem: the router must balance two competing objectives, performance and cost, given only band-  
 071 it feedback. To capture user preferences, we condition the policy on a trade-off vector that specifies  
 072 the relative importance of performance and cost. The router encodes each prompt together with this  
 073 vector and outputs a distribution over candidate LLMs. The policy is trained with policy-gradient  
 074 updates regularized by entropy for exploration and stabilized by calibrated cost scaling. This de-  
 075 sign removes the need for labels from all models during training while allowing operators to adjust  
 076 performance–cost preference at inference without retraining. By aligning training with the partial-  
 077 feedback setting of deployment and providing controllability at test time, BARP offers a practical  
 078 solution for real-world routing.

079 In summary, our main contributions are as follows:

- 080 • We formulate multi-objective LLM routing as a contextual bandit problem in which the  
 081 router learns from bandit feedback while conditioning on a user preference vector that  
 082 specifies the trade-off between accuracy and cost. This formulation eliminates the need for  
 083 full supervision across all candidate models and enables per-request controllability.
- 084 • We design a routing policy that integrates prompt representations with the preference vector,  
 085 and train it using entropy-regularized policy gradients with calibrated cost scaling,  
 086 which encourages exploration and ensures stable optimization under partial feedback.
- 087 • We validate our framework on RouterBench and two question-answering datasets, demon-  
 088 strating significant performance gains over strong baselines. On **in-distribution** tasks, our  
 089 method surpasses the top-performing individual LLM by 3.81% and full-information of-  
 090 fline routers by 12.46%. On **out-of-distribution** tasks, the gains are 2.45% and 25.99%  
 091 respectively, as shown in Fig. 1.

## 100 2 APPROACH

101 We present BARP, a **Bandit–feedback Router with Preferences**. The core idea is to treat routing as  
 102 a *multi-objective contextual bandit*: the router balances performance and cost while observing feed-  
 103 back only for the selected model. This section introduces the problem setting (Sec. 2.1), then defines  
 104 the policy architecture (Sec. 2.2), followed by the objective and learning procedure (Sec. 2.3). The  
 105 training and inference procedures are provided in Algorithm 1 and Sec. 2.4. For intuition, Fig. 2  
 106 illustrates a single request in the training process: a prompt and a user preference enter the router,  
 107 which selects an LLM, receives bandit feedback, and updates the policy.

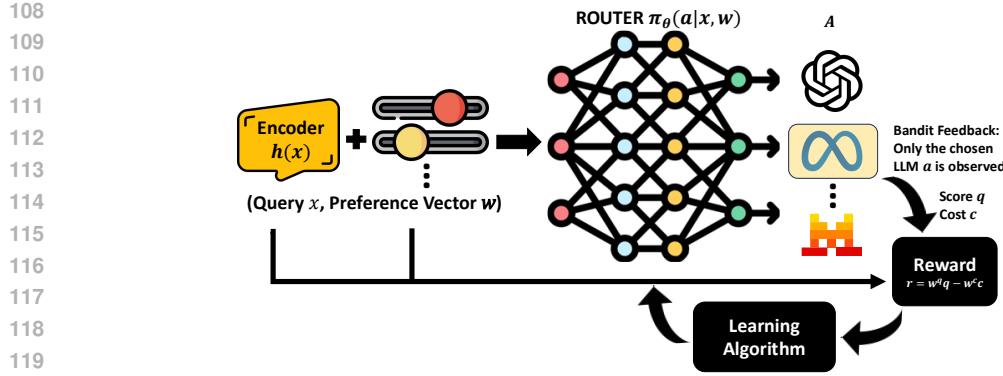


Figure 2: The training pipeline of BARP. The router takes the context (query  $x_t$  and preference  $w_t$ ) and selects an LLM. It then receives bandit feedback (the score and cost of the chosen LLM only) to calculate a reward  $r_t$ . This reward drives a **learning algorithm** to update the router’s parameters, including policy gradient methods like REINFORCE (Sec. 2.3) and classic bandit algorithms such as LinUCB, Thompson Sampling, and  $\epsilon$ -greedy (Sec. 4.6).

## 2.1 PROBLEM SETTING

We formally define the preference-conditioned LLM routing task as a contextual bandit problem. In each round  $t$ , an agent observes a context and selects an arm, receiving a reward based on its choice. The **Context** ( $s_t$ ) is a tuple  $s_t = (x_t, w_t)$ , where  $x_t$  is the input prompt and  $w_t = (w_t^q, w_t^c)$  is a user preference vector on the 1-simplex. Here,  $w_t^q$  represents the weight the user places on the performance score, while  $w_t^c$  represents the weight on minimizing cost. The set of  $K$  available LLMs constitutes the **Arms** ( $A$ ), or the action space  $\{1, \dots, K\}$ . The router selects an **Action** ( $a_t$ ) from this set, corresponding to choosing a single LLM to process the prompt. Upon selection, the router receives a scalar **Reward** ( $r_t$ ) based on bandit feedback for the chosen arm. This reward combines the two objectives according to the user’s preference:

$$r_t = w_t^q q_t - w_t^c \tilde{c}_t, \quad \text{where } \tilde{c}_t = \min\left(\frac{c_t}{\tau}, 1\right). \quad (1)$$

where the score  $q_t$  is a task-appropriate metric scaled to  $[0, 1]$ ,  $\tau > 0$  caps cost  $c_t$  so that score and (normalized) cost are on comparable scales. The overall goal is to learn a policy that maximizes the expected cumulative reward.

## 2.2 POLICY ARCHITECTURE

The routing policy  $\pi_\theta(a | s)$  is a neural network that maps a context  $s = (x, w)$  to a probability distribution over the  $K$  LLMs. The architecture is composed of three sequential components. First, a **Prompt Encoder**, a frozen pre-trained sentence transformer  $h$ , encodes the prompt  $x$  into a semantic vector  $h(x) \in \mathbb{R}^{d_e}$ . Second, a **Preference Encoder**, a small multilayer perceptron (MLP)  $\phi$ , maps the 2-dimensional preference vector  $w$  into a higher-dimensional embedding  $\phi(w) \in \mathbb{R}^{d_p}$ . Finally, the prompt and preference embeddings are concatenated to form a joint representation,  $z = [h(x); \phi(w)]$ , which is passed to a **Decision Head**,  $g_\theta$ , to produce logits  $o \in \mathbb{R}^K$ . The final policy is obtained by applying a softmax function to these logits:

$$\pi_\theta(a | x, w) = \text{softmax}(g_\theta(z))_a = \frac{\exp(o_a)}{\sum_{a'=1}^K \exp(o_{a'})}. \quad (2)$$

During training we sample  $a_t \sim \pi_\theta(\cdot | x_t, w_t)$  to ensure exploration. At inference, we output the deterministic choice:

$$a^*(x, w) = \arg \max_{a \in A} \pi_\theta(a | x, w), \quad (3)$$

---

162 **Algorithm 1** The Training and Inference Procedure for BARP.

---

```

163 1: Inputs: encoder  $h$ , preference MLP  $\phi$ , head  $g_\theta$ ; cost cap  $\tau$ ; entropy coeff  $\beta$ .
164 2: Initialize parameters  $\theta$ .
165 3: for  $t = 1$  to  $T$  do
166 4:   Receive prompt  $x_t$  and sample preference  $w_t$  (random on the 1-simplex).
167 5:   Compute  $h_t \leftarrow h(x_t)$  and  $u_t \leftarrow \phi(w_t)$ ; form  $z_t \leftarrow [h_t; u_t]$ .
168 6:    $o_t \leftarrow g_\theta(z_t)$ ,  $\pi_t \leftarrow \text{softmax}(o_t)$ .
169 7:   Sample  $a_t \sim \text{Categorical}(\pi_t)$ .
170 8:   Query LLM  $a_t$ ; observe  $q_t$  and  $c_t$  (only for  $a_t$ ).
171 9:    $\tilde{c}_t \leftarrow \min(c_t / \tau, 1)$ ;  $r_t \leftarrow w_t^q q_t - w_t^c \tilde{c}_t$ .
172 10:  Compute batch baseline  $b_t \leftarrow \frac{1}{B} \sum_{i=1}^B r^{(i)}$ .
173 11:   $\mathcal{L}_t \leftarrow -(r_t - b_t) \log \pi_t[a_t] - \beta H(\pi_t)$ .
174 12:  Update  $\theta \leftarrow \theta - \eta \nabla_\theta \mathcal{L}_t$ .
175 13: end for
176 14: Inference (no retraining): given  $x$  and  $w$ , output  $a^*(x, w) = \arg \max_a \pi_\theta(a | x, w)$ .


---


177
178 2.3 OBJECTIVE AND LEARNING ALGORITHM
179
180 Given the policy in equation 2 and reward in equation 1, the training objective is to find the parameters  $\theta$  that maximize the expected cumulative reward:
181
182
183 
$$\max_{\theta} J(\theta) = \mathbb{E}_{s_t \sim \mathcal{D}, a_t \sim \pi_\theta(\cdot | s_t)} \left[ \sum_{t=1}^T r_t \right]. \quad (4)$$

184
185 where the expectation is taken over the data distribution of contexts,  $\mathcal{D}$ , and the actions sampled from
186 the policy. We optimize this objective using the REINFORCE policy gradient algorithm, enhanced
187 with a baseline for variance reduction and entropy regularization for improved exploration. The
188 per-sample loss function to be minimized is:
189
190 
$$\mathcal{L}_t(\theta) = -(r_t - b_t) \log \pi_\theta(a_t | s_t) - \beta H(\pi_\theta(\cdot | s_t)), \quad (5)$$

191 where  $H(\cdot)$  is the Shannon entropy of the policy distribution,  $\beta \geq 0$  is a coefficient controlling the
192 strength of the entropy regularization, and  $b_t$  is a baseline used for variance reduction. We employ
193 the mean reward over the current mini-batch as the baseline, defined as:
194
195 
$$b_t = \frac{1}{B} \sum_{i=1}^B r_t^{(i)}, \quad (6)$$

196 where  $B$  is the batch size and  $r_t^{(i)}$  is the reward for the  $i$ -th example in the batch. While policy
197 gradient methods are well-suited for training our policy, the formulation of our framework is general
198 and can accommodate other classic learning algorithms, which we explore in our analysis in Sec. 4.6.
199
200 2.4 TRAINING AND INFERENCE
201
202 Training. The policy network's parameters  $\theta$  are optimized to maximize the expected reward using
203 the REINFORCE algorithm detailed in Sec. 2.3. The training procedure has two key methodological
204 features. First, to train a single policy that can serve diverse user preferences, we randomly sample
205 the preference vector  $w_t$  for each training instance (uniformly on the 1-simplex). Second, while
206 our training utilizes pre-existing benchmark logs with complete information, we simulate a bandit
207 environment to match deployment conditions. For each instance, after an action  $a_t$  is sampled from
208 the policy, the supervision signal is restricted to only the outcome of that specific action. The policy
209 gradient updates are performed using the Adam optimizer (Kingma & Ba, 2017).
210
211 Inference. At deployment time, the router operates deterministically to exploit the learned policy.
212 Given a prompt  $x$  and a user-specified preference vector  $w$ , the router selects the action with the
213 highest probability:
214 
$$a^*(x, w) = \arg \max_{a \in A} \pi_\theta(a | x, w). \quad (7)$$

215 This allows operators to adjust the performance-cost behavior on a per-request basis by simply
216 modifying the input vector  $w$ , without any need for retraining the model.

```

216 3 EXPERIMENTS SETUP  
217218 3.1 DATASETS AND BENCHMARKS  
219220 We evaluate on **RouterBench** (Hu et al., 2024) and two question-answering datasets (Kwiatkowski  
221 et al., 2019; Yang et al., 2018), which provide prompt-level logs with multiple candidate LLMs per  
222 query, including a task identifier, a performance score per LLM, and a monetary cost per LLM.  
223 While the benchmark logs contain scores/costs for *all* LLMs, our training strictly uses *bandit-consistent*  
224 supervision (only the chosen arm is observed).225 Our experiments evaluate routing across a diverse set of widely used large language models, spanning  
226 both open-source and proprietary offerings. A detailed list and description of these models is  
227 provided in Appendix A.3.  
228229 **Tasks and Evaluation.** To evaluate our framework, we curate a set of eight distinct tasks(the  
230 dataset details are in A.4). Our model is trained on a mixture of data from five of these tasks:  
231 **GSM8K** (Cobbe et al., 2021), **MMLU** (Hendrycks et al., 2021), **ARC-C** (Clark et al., 2018),  
232 **Winogrande** (Sakaguchi et al., 2021), and **Natural Questions (NQ)** (Kwiatkowski et al., 2019).  
233 We create an 80%/20% training/testing split for each of these tasks and combine the training splits  
234 to form the full training set.  
235

236 Our evaluation is then conducted in two settings:

237 • **In-Distribution Evaluation:** We test the model on the held-out 20% test sets of the five tasks it  
238 was trained on. This measures the model’s ability to unseen examples from familiar tasks.  
239 • **Out-of-Distribution Generalization:** To assess generalization to entirely new tasks, we evaluate  
240 the trained model on three benchmarks it has never seen during training: **MBPP** (Austin et al.,  
241 2021), **Hellaswag** (Zellers et al., 2019), and **HotpotQA** (Yang et al., 2018).  
242243 3.2 BASELINE METHODS  
244245 We compare our method against representative routers and common-sense baselines:  
246247 • **Smallest LLM** always routes to the smallest model.  
248 • **Largest LLM** always routes to the largest model.  
249 • **RouterDC** (Chen et al., 2024) learns dual-contrastive embeddings for queries and models, re-  
250quires full-information labels.  
251 • **GraphRouter** (Feng et al., 2025) learns graph-structured representations over queries, tasks, and  
252models, also requires full labels.  
253254 3.3 METRICS  
255256 Following RouterBench (Hu et al., 2024), we evaluate methods on two axes:  
257258 • **Performance score** is a normalized value in  $[0, 1]$  that indicates task success, derived either from  
259exact match accuracy or from GPT-4 ratings for more open-ended tasks.  
260 • **Monetary cost** is the estimated API call cost per query in USD.  
261262 3.4 IMPLEMENTATION DETAILS  
263264 Our policy is implemented in PyTorch. We use frozen all-MiniLM-L6-v2 (Wang et al., 2020) as the  
265 prompt encoder. The trainable components consist of two small MLPs with ReLU activations: one  
266 to encode the preference vector and a decision head that produces the final logits over the candidate  
267 LLMs. All prompts are tokenized to a maximum length of 512. We train our policy for 100 epochs  
268 using the Adam optimizer (Kingma & Ba, 2017) with a learning rate of  $1 \times 10^{-4}$  and a batch size  
269 of 32. For the REINFORCE algorithm, we set the entropy regularization coefficient  $\beta$  to 0.05. All  
experiments were conducted on NVIDIA A100 80GB GPUs.

270 Table 2: Testing score (%) on in-distribution tasks. The **best** results are highlighted in bold, and the  
 271 second-best results are underlined.

Methods	ARC-C	GSM8K	MMLU	Winogrande	NQ	Avg ↑
Smallest LLM	38.78	41.15	25.43	52.41	14.95	34.54
Largest LLM	<u>96.19</u>	<u>65.88</u>	<b>81.19</b>	<u>81.93</u>	29.15	<u>70.87</u>
RouterDC	91.99	59.68	60.98	74.74	31.00	63.68
GraphRouter	94.18	<b>66.28</b>	80.20	46.83	<u>31.60</u>	65.42
Ours	<b>96.60</b>	64.58	<u>81.06</u>	<b>82.61</b>	<b>43.01</b>	<b>73.57</b>

## 281 4 EXPERIMENTS RESULTS

### 283 4.1 PERFORMANCE ON IN-DISTRIBUTION TASKS

285 We first evaluate our method (BARP) against four baselines on in-distribution tasks, with results  
 286 illustrated in Fig. 1 and reported in Table 2. BARP achieves the strongest trade-off between per-  
 287 formance and cost. It delivers the highest average score (73.57%), outperforming the strong, full-  
 288 information routers, RouterDC and GraphRouter, by a relative **15.53%** and **12.44%** respectively. It  
 289 also establishes new best scores on ARC-C, Winogrande, and NQ. While the Largest LLM base-  
 290 line is competitive on some tasks, its high monetary cost makes it impractical. In contrast, BARP  
 291 achieves a performance level comparable to the strongest baselines while maintaining a cost signif-  
 292 icantly lower than other learned routers, establishing its superior efficiency on familiar tasks.

### 293 4.2 GENERALIZATION ABILITY TO NEW TASKS

295 To assess robustness, we further evaluate the trained models on out-of-distribution tasks they have  
 296 never seen during training. As shown in Table 3, the full-information routers (RouterDC and  
 297 GraphRouter) struggle to generalize, with their performance dropping sharply on MBPP and HpQA.  
 298 In contrast, BARP demonstrates robust generalization, achieving the highest average score (66.08%)  
 299 among all methods. It obtains the best score on HpQA, where other learned methods fail, and main-  
 300 tains performance competitive with the much more expensive Largest LLM baseline on MBPP and  
 301 Hellaswag. This confirms that BARP preserves its superiority not only on in-distribution tasks but  
 302 also when adapting to unseen tasks, confirming its robustness and practical deployment value.

303 Table 3: Testing score (%) on out-of-distribution tasks. The **best** results are highlighted in bold, and  
 304 the second-best results are underlined.

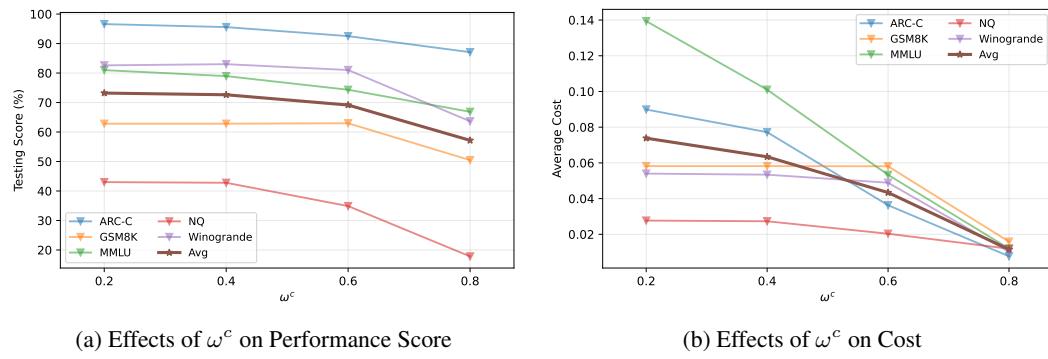
Methods	MBPP	Hellaswag	HpQA	Avg ↑
Smallest LLM	34.43	25.48	27.49	29.14
Largest LLM	<b>68.62</b>	<b>83.96</b>	<u>40.93</u>	<u>64.50</u>
RouterDC	39.06	69.60	25.00	44.55
GraphRouter	64.29	70.87	22.20	52.45
Ours	<u>68.24</u>	<u>83.72</u>	<b>46.29</b>	<b>66.08</b>

### 314 4.3 OVERALL PERFORMANCE AND COST-EFFECTIVENESS

316 Finally, to provide a holistic measure of performance and cost across all evaluation settings, we  
 317 summarize the results by averaging across all eight tasks in Table 4. This view confirms that BARP  
 318 provides the best balance of performance and cost. Compared to GraphRouter, the strongest offline  
 319 baseline, our method improves the overall average score by **16.84%** while simultaneously reducing  
 320 monetary cost by **50.00%**. In contrast, RouterDC provides a significant cost reduction but at the  
 321 expense of a lower score, while the Largest LLM improves accuracy by 13.08% but at the expense  
 322 of a more than threefold increase in cost. These results validate that our preference-conditioned,  
 323 bandit-feedback approach is not only more effective but also substantially more cost-efficient than  
 methods relying on full-information supervision.

324  
 325 Table 4: Comparison of methods in terms of Score, Cost, and the corresponding percentage Score  
 326 improvements and Cost reduction rate, relative to the state-of-the-art method(GraphRouter (Feng  
 327 et al., 2025)). The score and cost are averaged over in-distribution and out-of-distribution tasks. The  
 328 cost is multiplied by  $10^3$  for readability.

Method	Score	Score Improvement (%)	Monetary Cost	Cost Reduction (%)
Smallest LLM	32.52	-46.30	0.05	94.68
Largest LLM	68.48	13.08	3.29	-250.00
RouterDC	56.51	-6.69	0.79	15.96
GraphRouter	60.56	0	0.94	0
BARP (Ours)	70.76	16.84	0.47	50.00

346 (a) Effects of  $\omega^c$  on Performance Score347 (b) Effects of  $\omega^c$  on Cost348 Figure 3: Effects of  $\omega^c$ 349  
 350 4.4 SENSITIVITY ANALYSIS

## 351 4.4.1 ANALYSIS OF THE PREFERENCE TRADE-OFF

352 We analyze the sensitivity of our router to the user-specified preference, which provides a direct  
 353 trade-off between performance and cost. Recall from Sec. 2.1 that the preference vector is  $w =$   
 354  $(w^q, w^c)$ , where  $w^c$  is the weight on cost reduction. In this analysis, we vary the cost weight  $w^c \in$   
 355  $[0, 1]$  (with  $w^q = 1 - w^c$ ) at inference time and observe its effect on the router’s behavior. Figure 3  
 356 reports the effects of varying  $w^c$  on both performance score and monetary cost across tasks.

357 As shown in Figure 3a, smaller values of the cost weight  $w^c$  (e.g., 0.2) lead the router to prioritize  
 358 performance, achieving strong scores across most tasks. For example, ARC-C remains above a 95%  
 359 score and Winogrande above 80%. However, as  $w^c$  increases, the average score gradually declines,  
 360 most noticeably on NQ and MMLU, reflecting the router’s increasing preference for cheaper models  
 361 even when they are less performant.

362 Conversely, Figure 3b shows that larger  $w^c$  values yield significant reductions in average cost. The  
 363 cost decreases steadily from \$0.074 at  $w^c = 0.2$  to only \$0.015 at  $w^c = 0.8$ , with consistent  
 364 reductions across all tasks. This demonstrates that the router effectively adapts its selections in line  
 365 with the user-specified trade-off, choosing lower-cost models when cost is emphasized.

366 Overall, these results confirm that the preference vector provides a clear and interpretable control  
 367 knob for operators. Lower cost weights favor high performance at a higher cost, while higher cost  
 368 weights sacrifice some performance to achieve substantial cost savings. This allows the behavior of  
 369 BARP to be tuned to specific deployment requirements without any need for retraining.

## 370 4.4.2 IMPACT OF PROMPT ENCODER CHOICE

371 We analyze how the choice of the frozen prompt encoder affects routing performance. A more  
 372 powerful encoder might provide better representations, but could also be less efficient. We compare  
 373 three widely-used pre-trained models of increasing size: **all-MiniLM-L6-v2** (Wang et al., 2020)  
 374 (384-dim), **BERT-base-uncased** (Devlin et al., 2018) (768-dim), and **E5-large-v2** (Wang et al.,

2022) (1024-dim). For each, we train only the preference encoder and the router’s decision head using the same bandit-feedback procedure.

The results, averaged over all in-distribution tasks with a balanced preference ( $w^q = w^c = 0.5$ ), are presented in Table 5. The all-MiniLM-L6-v2 encoder achieves the highest average score (0.7432), establishing the best trade-off between performance and model size. While the much larger E5-large-v2 performs comparably on score, its increased representational capacity does not translate into a significant routing advantage. Conversely, BERT-base-uncased yields a noticeably lower score, suggesting its representations are less effective for this task.

These findings provide a valuable insight: our routing framework does not require a large, resource-intensive model for prompt encoding. A compact, efficient sentence-level encoder like MiniLM is sufficient to capture the necessary semantics for routing. We hypothesize this is because modern sentence transformers, trained with contrastive objectives, produce more suitable sentence-level embeddings for this task than older models like BERT, which were trained on token-level objectives. Given its superior performance and smaller footprint, we use all-MiniLM-L6-v2 as the default encoder for all other experiments in this paper.

Prompt Encoder	Avg Score	Avg Monetary Cost
MiniLM-L6-v2	<b>0.7432</b>	0.0007
BERT-base-uncased	0.7226	<b>0.0005</b>
E5-large-v2	0.7418	0.0007

Table 5: Comparison of different frozen prompt encoders. Results are averaged across in-distribution tasks using a balanced preference ( $w^q = w^c = 0.5$ ) during inference. The Avg Cost refers to the monetary cost of the LLMs selected by the router, not the encoder’s cost. Given its superior performance and smaller footprint, we use all-MiniLM-L6-v2 as the default encoder for all other experiments in this paper.

#### 4.5 IMPACT OF DECISION HEAD ARCHITECTURE

We also analyze the impact of the decision head’s architecture, which sits atop the frozen encoder and maps the context representation to action logits. We evaluate three types of decision heads mentioned in Sec. 2.2: a simple **linear** layer, a parameter-efficient **bilinear** model, and a two-layer **MLP** with a ReLU non-linearity.

As shown in Table 6, the MLP head achieves the best overall performance, reaching the highest average score (0.7432). The linear head is competitive, suggesting that a direct mapping is a strong baseline, while the bilinear head underperforms. These results provide a key insight: while a simple linear mapping is effective, the added representational capacity of the MLP’s non-linearity is beneficial for learning the complex function that maps a prompt and a user preference to the optimal LLM choice.

We hypothesize that the bilinear head, despite being designed to model interactions, may be more difficult to optimize with the sparse signal provided by bandit feedback, potentially leading to its lower score. Given that the MLP head provides the best performance without a significant increase in complexity, we adopt it as the default architecture for all other experiments.

Head Type	Avg Score	Avg Monetary Cost
Linear	0.7396	0.0007
Bilinear	0.7317	<b>0.0006</b>
MLP	<b>0.7432</b>	0.0007

Table 6: Comparison of different decision head architectures. Results are averaged across in-distribution tasks, using a balanced preference ( $w^q = w^c = 0.5$ ) during inference.

#### 4.6 ANALYSIS OF LEARNING ALGORITHMS

A key feature of our framework is its flexibility to accommodate different learning algorithms. To analyze the impact of the algorithm choice, we compare our policy-gradient approach (REINFORCE) with several classic contextual bandit strategies: **Linear Thompson Sampling (LinTS)** (Agrawal & Goyal, 2013), **LinUCB** (Li et al., 2010), and  $\epsilon$ -**greedy**. To ensure a fair comparison, all algorithms operate on the identical context representation (the concatenated prompt and preference embeddings). As is standard, the classic bandit strategies are paired with a linear model to map these features to rewards, while our main approach uses a non-linear MLP.

Table 7 presents the results evaluated with a balanced preference ( $w^q = w^c = 0.5$ ). The policy-gradient method (REINFORCE) achieves a substantially higher average score, demonstrating supe-

432 prior performance on this task. Notably, bandit approaches tend to yield slightly lower costs, suggesting  
 433 that their conservative exploration might favor cheaper models at the expense of performance.  
 434

435 The primary finding from this analysis is that  
 436 the routing decision function is inherently  
 437 complex. While classic bandit algorithms pro-  
 438 vide a strong baseline, their performance is  
 439 limited by the linear assumptions they make  
 440 about the relationship between context and re-  
 441 ward. The significant performance gap sug-  
 442 gests that an algorithm capable of learning a  
 443 non-linear policy, such as REINFORCE paired  
 444 with an MLP, is necessary to effectively model  
 the nuances of LLM routing.

## 445 446 447 5 ADDITIONAL RELATED WORK

448  
 449 **LLM routing.** With the rapid growth of LLMs, there is increasing interest in routing strategies  
 450 that decide which model to query for each input. Early approaches often rely on ensembles, such  
 451 as majority voting over all outputs, or static heuristics like always choosing the largest or small-  
 452 est model. Recently, learning-based routers have been proposed. GraphRouter (Feng et al., 2025)  
 453 learns graph-structured representations across prompts, tasks, and models to exploit relational in-  
 454 formation. RouterDC (Chen et al., 2024) introduces dual-contrastive objectives for aligning query  
 455 and model embeddings. Other efforts design mixture-of-experts systems that dynamically allocate  
 456 queries across LLMs (Varangot-Reille et al., 2025).

457  
 458 **Contextual bandits.** The contextual bandit framework (Langford & Zhang, 2007) formalizes  
 459 decision-making under partial feedback: at each round, the learner observes a context, selects an  
 460 action, and only receives feedback for that action. Classical bandit algorithms include LinUCB (Li  
 461 et al., 2010), which uses optimism in linear reward models; Thompson Sampling (Agrawal & Goyal,  
 462 2013), which maintains a posterior over reward parameters; and  $\epsilon$ -greedy strategies, which trade off  
 463 exploration and exploitation through randomization. Beyond linear settings, neural contextual bandit  
 464 s extend these ideas with non-linear function approximators (Riquelme et al., 2018; Zhou et al.,  
 465 2020). Bandit methods have been applied to recommendation (Li et al., 2010), online advertising  
 466 (Chapelle & Li, 2011), and adaptive experiment design.

## 467 468 469 6 CONCLUSION AND DISCUSSION

470  
 471 In this work, we address the challenge of efficiently selecting the optimal LLM from a pool of  
 472 candidates to balance performance and cost. We formalize this task as a preference-conditioned  
 473 contextual bandit problem and introduce BARP. Trained with policy gradients on bandit feedback,  
 474 our method learns to map a user’s prompt and specific performance-cost preference to the most  
 475 suitable LLM. Extensive experiments demonstrate that BARP significantly outperforms both top-  
 476 performing individual LLMs and strong offline routers on both in-distribution and out-of-distribution  
 477 tasks. Crucially, we show that the preference vector provides an effective and interpretable control  
 478 mechanism, allowing operators to tune the router’s behavior at inference time without retraining.

479 We acknowledge several limitations for future improvement. Our method trains on static, offline  
 480 logs, which is practical but differs from a truly online setting where a router could learn continuously  
 481 from live feedback. We only consider performance and monetary cost, while real deployments  
 482 may require richer, possibly task-specific preferences and constraints (e.g., latency). The current  
 483 contextual bandit formulation also models routing as a single-step decision, making it well-suited  
 484 for many tasks but not explicitly designed for multi-turn, conversational scenarios. Furthermore, our  
 485 experiments focused on a pool of general-purpose LLMs, and future work could explore routing to  
 highly specialized, domain-expert models.

Method	Avg Score	Avg Monetary Cost
LinTS	0.6430	0.00046
LinUCB	0.6166	<b>0.00044</b>
$\epsilon$ -greedy	0.6556	0.00056
REINFORCE	<b>0.7432</b>	0.00070

Table 7: Comparison between REINFORCE and classical bandit algorithms. Results are averaged across in-distribution tasks, using a balanced preference ( $w^q = w^c = 0.5$ ) during inference.

486 ETHICS STATEMENT  
487488 The primary goal of this research is to improve the efficiency of using large language models, a  
489 direction with a positive societal impact. By enabling users to select smaller, less expensive mod-  
490 els when appropriate without a significant loss in performance, our work contributes to reducing  
491 the overall energy consumption and carbon footprint associated with deploying these powerful but  
492 resource-intensive technologies. Our work relies on existing, publicly available benchmark datasets  
493 and pre-trained language models. We do not use any private or personally identifiable information,  
494 and our research does not involve human subjects. As with any system that improves the efficiency  
495 of LLM routing, there is a possibility of misuse, for example, in routing to optimize spam or mis-  
496 information generation. However, we believe the risk is limited and outweighed by the benefits of  
497 more efficient LLM routing.  
498499 REPRODUCIBILITY STATEMENT  
500501 We are committed to ensuring the reproducibility of our work. To this end, all code required to  
502 replicate our experiments, including scripts for training, evaluation, and all analyses presented in the  
503 paper, will be made publicly available upon publication in an open-source repository.  
504505 **Datasets.** Our primary experiments are conducted on the publicly available benchmarks. We will  
506 provide scripts to download and process all data into the format required by our codebase. Our data  
507 splits are deterministic, based on the random seed provided in our code.  
508509 **Models and Hyperparameters.** The specific pre-trained models used for the prompt encoder and  
510 the full list of candidate LLMs are detailed in the appendix. All critical hyperparameters, includ-  
511 ing learning rates, batch sizes, and regularization coefficients, are reported in 3.4. Our code is  
512 implemented in PyTorch.  
513514 **Computational Resources.** All experiments were conducted on a single NVIDIA A100 GPU with  
515 80GB of memory. The training for our main model completes in approximately 2-3 hours. The code  
516 for the classic bandit baselines is also provided and runs efficiently on a standard CPU.  
517518 REFERENCES  
519

520 Shipra Agrawal and Navin Goyal. Thompson sampling for contextual bandits with linear payoffs.  
521 In Sanjoy Dasgupta and David McAllester (eds.), *Proceedings of the 30th International Con-  
522 ference on Machine Learning*, volume 28 of *Proceedings of Machine Learning Research*, pp.  
523 127–135, Atlanta, Georgia, USA, 17–19 Jun 2013. PMLR. URL <https://proceedings.mlr.press/v28/agrawal13.html>.  
524

525 Anthropic. Model card and evaluations for claude models, 2023. URL  
526 <https://www-cdn.anthropic.com/files/4zrzovbb/website/bd2a28d2535bfb0494cc8e2a3bf135d2e7523226.pdf>.  
527

528 Jacob Austin, Augustus Odena, Maxwell Nye, Maarten Bosma, Henryk Michalewski, David Dohan,  
529 Ellen Jiang, Carrie Cai, Michael Terry, Quoc Le, et al. Program synthesis with large language  
530 models. *arXiv preprint arXiv:2108.07732*, 2021.  
531

532 Olivier Chapelle and Lihong Li. An empirical evaluation of thompson sampling. In  
533 J. Shawe-Taylor, R. Zemel, P. Bartlett, F. Pereira, and K.Q. Weinberger (eds.), *Ad-  
534 vances in Neural Information Processing Systems*, volume 24. Curran Associates, Inc.,  
535 2011. URL [https://proceedings.neurips.cc/paper\\_files/paper/2011/file/e53a0a2978c28872a4505bdb51db06dc-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2011/file/e53a0a2978c28872a4505bdb51db06dc-Paper.pdf).  
536

538 Shuhao Chen, Weisen Jiang, Baijiong Lin, James T. Kwok, and Yu Zhang. Routerdc: Query-  
539 based router by dual contrastive learning for assembling large language models, 2024. URL  
540 <https://arxiv.org/abs/2409.19886>.

540 Peter Clark, Isaac Cowhey, Oren Etzioni, Tushar Khot, Ashish Sabharwal, Carissa Schoenick, and  
 541 Oyvind Tafjord. Think you have solved question answering? try arc, the ai2 reasoning challenge.  
 542 *arXiv preprint arXiv:1803.05457*, 2018.

543 Karl Cobbe, Vineet Kosaraju, Mohammad Bavarian, Mark Chen, Heewoo Jun, Lukasz Kaiser,  
 544 Matthias Plappert, Jerry Tworek, Jacob Hilton, Reiichiro Nakano, et al. Training verifiers to  
 545 solve math word problems. *arXiv preprint arXiv:2110.14168*, 2021.

546 Xiangxiang Dai, Jin Li, Xutong Liu, Anqi Yu, and John C. S. Lui. Cost-effective online multi-  
 547 llm selection with versatile reward models, 2024. URL <https://arxiv.org/abs/2405.16587>.

548 Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: pre-training of deep  
 549 bidirectional transformers for language understanding. *CoRR*, abs/1810.04805, 2018. URL  
 550 <https://arxiv.org/abs/1810.04805>.

551 Tao Feng, Yanzhen Shen, and Jiaxuan You. Graphrouter: A graph-based router for llm selections,  
 552 2025. URL <https://arxiv.org/abs/2410.03834>.

553 Aaron Grattafiori, Abhimanyu Dubey, Abhinav Jauhri, Abhinav Pandey, Abhishek Kadian, Ahmad  
 554 Al-Dahle, Aiesha Letman, Akhil Mathur, Alan Schelten, Alex Vaughan, et al. The llama 3 herd  
 555 of models. *arXiv preprint arXiv:2407.21783*, 2024.

556 Dan Hendrycks, Collin Burns, Steven Basart, Andy Zou, Mantas Mazeika, Dawn Song, and  
 557 Jacob Steinhardt. Measuring massive multitask language understanding. *arXiv preprint  
 558 arXiv:2009.03300*, 2021.

559 Qitian Jason Hu, Jacob Bieker, Xiuyu Li, Nan Jiang, Benjamin Keigwin, Gaurav Ranganath, Kurt  
 560 Keutzer, and Shriyash Kaustubh Upadhyay. Routerbench: A benchmark for multi-llm routing  
 561 system, 2024. URL <https://arxiv.org/abs/2403.12031>.

562 Albert Q. Jiang, Alexandre Sablayrolles, Arthur Mensch, Chris Bamford, Devendra Singh Chaplot,  
 563 Diego de las Casas, Florian Bressand, Gianna Lengyel, Guillaume Lample, Lucile Saulnier,  
 564 Lélio Renard Lavaud, Marie-Anne Lachaux, Pierre Stock, Teven Le Scao, Thibaut Lavril,  
 565 Thomas Wang, Timothée Lacroix, and William El Sayed. Mistral 7b, 2023. URL <https://arxiv.org/abs/2310.06825>.

566 Albert Q Jiang, Alexandre Sablayrolles, Arthur Mensch, Chris Bamford, Devendra S Chaplot, Diego  
 567 de las Casas, Florian Bressand, Gianna Lengyel, Guillaume Lample, Lucile Saulnier, et al. Mixtral  
 568 of experts. *arXiv preprint arXiv:2401.04088*, 2024.

569 Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization, 2017. URL  
 570 <https://arxiv.org/abs/1412.6980>.

571 Tom Kwiatkowski, Jennimaria Palomaki, Olivia Redfield, Michael Collins, Ankur Parikh, Chris  
 572 Alberti, Danielle Epstein, Illia Polosukhin, Jacob Devlin, Kenton Lee, Kristina Toutanova, Llion  
 573 Jones, Matthew Kelcey, Ming-Wei Chang, Andrew M. Dai, Jakob Uszkoreit, Quoc Le, and Slav  
 574 Petrov. Natural questions: A benchmark for question answering research. *Transactions of the  
 575 Association for Computational Linguistics*, 7:452–466, 2019. doi: 10.1162/tacl\_a\_00276. URL  
 576 <https://aclanthology.org/Q19-1026/>.

577 John Langford and Tong Zhang. The epoch-greedy algorithm for multi-armed bandits  
 578 with side information. In J. Platt, D. Koller, Y. Singer, and S. Roweis (eds.), *Ad-  
 579 vances in Neural Information Processing Systems*, volume 20. Curran Associates, Inc.,  
 580 2007. URL [https://proceedings.neurips.cc/paper\\_files/paper/2007/file/4b04a686b0ad13dce35fa99fa4161c65-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2007/file/4b04a686b0ad13dce35fa99fa4161c65-Paper.pdf).

581 Lihong Li, Wei Chu, John Langford, and Robert E. Schapire. A contextual-bandit approach to  
 582 personalized news article recommendation. In *Proceedings of the 19th international conference  
 583 on World wide web*, WWW ’10, pp. 661–670. ACM, April 2010. doi: 10.1145/1772690.1772758.  
 584 URL <http://dx.doi.org/10.1145/1772690.1772758>.

585 Yang Li. Llm bandit: Cost-efficient llm generation via preference-conditioned dynamic routing,  
 586 2025. URL <https://arxiv.org/abs/2502.02743>.

594 OpenAI, Josh Achiam, Steven Adler, Sandhini Agarwal, Lama Ahmad, Ilge Akkaya, Floren-  
 595 cia Leoni Aleman, Diogo Almeida, Janko Altenschmidt, Sam Altman, Shyamal Anadkat, et al.  
 596 Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*, 2023.

597

598 Carlos Riquelme, George Tucker, and Jasper Snoek. Deep bayesian bandits showdown: An em-  
 599 pirical comparison of bayesian deep networks for thompson sampling, 2018. URL <https://arxiv.org/abs/1802.09127>.

600

601 Baptiste Rozière, Jonas Gehring, Fabian Gloeckle, Sten Sootla, Itai Gat, Xiaoqing Ellen Tan, Yossi  
 602 Adi, Jingyu Liu, Romain Sauvestre, Tal Remez, Jérémie Rapin, Artyom Kozhevnikov, Ivan Ev-  
 603 timov, Joanna Bitton, Manish Bhatt, Cristian Canton Ferrer, Aaron Grattafiori, Wenhan Xiong,  
 604 Alexandre Défossez, Jade Copet, Faisal Azhar, Hugo Touvron, Louis Martin, Nicolas Usunier,  
 605 Thomas Scialom, and Gabriel Synnaeve. Code llama: Open foundation models for code, 2024.  
 606 URL <https://arxiv.org/abs/2308.12950>.

607

608 Keisuke Sakaguchi, Ronan Le Bras, Chandra Bhagavatula, and Yejin Choi. Winogrande: An adver-  
 609 sarial winograd schema challenge at scale. *Communications of the ACM*, 2021.

610

611 Gemma Team, Morgane Riviere, Shreya Pathak, Pier Giuseppe Sessa, Cassidy Hardin, Surya Bhu-  
 612 patiraju, Léonard Hussonot, Thomas Mesnard, Bobak Shahriari, Alexandre Ramé, et al. Gemma  
 613 2: Improving open language models at a practical size. *arXiv preprint arXiv:2408.00118*, 2024.

614

615 Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Niko-  
 616 lay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, et al. Llama 2: Open founda-  
 617 tion and fine-tuned chat models. *arXiv preprint arXiv:2307.09288*, 2023.

618

619 Clovis Varangot-Reille, Christophe Bouvard, Antoine Gourru, Mathieu Ciancone, Marion Schaeffer,  
 620 and François Jacquet. Doing more with less: A survey on routing strategies for resource op-  
 621 timisation in large language model-based systems, 2025. URL <https://arxiv.org/abs/2502.00409>.

622

623 Liang Wang, Nan Yang, Xiaolong Huang, Binxing Jiao, Linjun Yang, Dixin Jiang, Rangan Ma-  
 624 jumder, and Furu Wei. Text embeddings by weakly-supervised contrastive pre-training. *arXiv  
 625 preprint arXiv:2212.03533*, 2022.

626

627 Wenhui Wang, Furu Wei, Li Dong, Hangbo Bao, Nan Yang, and Ming Zhou. Minilm: Deep  
 628 self-attention distillation for task-agnostic compression of pre-trained transformers, 2020. URL  
 629 <https://arxiv.org/abs/2002.10957>.

630

631 Can Xu, Qingfeng Sun, Kai Zheng, Xiubo Geng, Pu Zhao, Jiazhan Fung, Yining Yin, and Lida  
 632 Mou. Wizardlm: Empowering large language models to follow complex instructions. *arXiv  
 633 preprint arXiv:2304.12244*, 2023.

634

635 Qwen An Yang, Baosong Yang, Beichen Zhang, Binyuan Hui, Bo Zheng, Bowen Yu, Chengyuan  
 636 Li, Dayiheng Liu, Fei Huang, Guanting Dong, Haoran Wei, Huan Lin, Jian Yang, Jianhong Tu,  
 637 Jianwei Zhang, Jianxin Yang, Jiaxin Yang, Jingren Zhou, Junyang Lin, Kai Dang, Keming Lu,  
 638 Keqin Bao, Kexin Yang, Le Yu, Mei Li, Mingfeng Xue, Pei Zhang, Qin Zhu, Rui Men, Runji  
 639 Lin, Tianhao Li, Tingyu Xia, Xingzhang Ren, Xuancheng Ren, Yang Fan, Yang Su, Yi-Chao  
 640 Zhang, Yunyang Wan, Yuqi Liu, Zeyu Cui, Zhenru Zhang, Zihan Qiu, Shanghaoran Quan, and  
 641 Zekun Wang. Qwen2.5 technical report. *ArXiv*, abs/2412.15115, 2024. URL <https://api.semanticscholar.org/CorpusID:274859421>.

642

643 Zhilin Yang, Peng Qi, Saizheng Zhang, Yoshua Bengio, William W. Cohen, Ruslan Salakhutdinov,  
 644 and Christopher D. Manning. HotpotQA: A dataset for diverse, explainable multi-hop question  
 645 answering. In *Conference on Empirical Methods in Natural Language Processing (EMNLP)*,  
 646 2018.

647

Alex Young, Bei Chen, Chao Li, Chengen Huang, Ge Zhang, Guanwei Zhang, Guoyin Wang, Heng  
 648 Li, Jiangcheng Zhu, Jianqun Chen, et al. Yi: Open foundation models by 01. ai. *arXiv preprint  
 649 arXiv:2403.04652*, 2024.

650

Rowan Zellers, Ari Holtzman, Yonatan Bisk, Ali Farhadi, and Yejin Choi. Hellaswag: Can a ma-  
 651 chine really finish your sentence? *arXiv preprint arXiv:1905.07830*, 2019.

648 Bowen Zhang, Gang Wang, Qi Chen, and Anton van den Hengel. How do we select right LLM for  
649 each query?, 2025. URL <https://openreview.net/forum?id=AfA3qNY0Fq>.  
650

651 Dongruo Zhou, Lihong Li, and Quanquan Gu. Neural contextual bandits with ucb-based exploration,  
652 2020. URL <https://arxiv.org/abs/1911.04462>.  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701

702 **A APPENDIX**  
703704 **A.1 NOTATION**  
705706 **Table 8: Summary of notations.**  
707

709 <b>Symbol</b>	710 <b>Description</b>
<i>Problem Formulation</i>	
711 $K$	712 Total number of candidate LLMs (actions).
712 $A$	713 The set of actions $\{1, \dots, K\}$ .
713 $t$	714 The time step or round index.
714 $x_t$	715 The input prompt at round $t$ .
715 $w_t$	716 The user preference vector $(w_t^q, w_t^c)$ at round $t$ .
716 $w_t^q, w_t^c$	717 The weights for performance score and cost, respectively.
717 $s_t$	718 The context (state) at round $t$ , defined as the tuple $(x_t, w_t)$ .
718 $a_t$	719 The action (chosen LLM) at round $t$ .
719 $q_t$	720 The performance score of the chosen LLM's output, $q_t \in [0, 1]$ .
720 $c_t$	721 The monetary cost of using the chosen LLM.
721 $\tilde{c}_t$	722 The normalized monetary cost, $\min(c_t/\tau, 1)$ .
722 $r_t$	723 The scalar reward at round $t$ .
$\mathcal{D}$ The underlying data distribution of contexts.	
<i>Policy and Learning</i>	
724 $\theta$	725 The trainable parameters of the policy network.
725 $\pi_\theta(a s)$	726 The policy; probability of selecting action $a$ given context $s$ .
726 $h(\cdot)$	727 The frozen prompt encoder function.
727 $\phi(\cdot)$	728 The preference encoder (MLP) function.
728 $z$	729 The concatenated context representation $[h(x); \phi(w)]$ .
729 $g_\theta(\cdot)$	730 The decision head of the policy network.
730 $o$	731 The vector of logits produced by the decision head.
731 $a^*$	732 The optimal action selected at inference time (via argmax).
732 $J(\theta)$	733 The expected cumulative reward objective function.
733 $\mathcal{L}_t(\theta)$	734 The policy gradient loss function at round $t$ .
734 $b_t$	735 The reward baseline (batch-mean reward).
735 $B$	736 The batch size used during training.
736 $H(\cdot)$	737 The Shannon entropy function.
737 $\beta$	738 The entropy regularization coefficient.
$\tau$ The cost scaling and capping hyperparameter.	

739 **A.2 ADDITIONAL RESULTS**  
740741 **Table 9: Testing score (%) of each candidate LLM on in-distribution tasks.**  
742

745 <b>Candidate LLM</b>	746 <b>ARC-C</b>	747 <b>GSM8K</b>	748 <b>MMLU</b>	749 <b>Winogrande</b>	750 <b>Avg <math>\uparrow</math></b>
746 WizardLM/WizardLM-13B-V1.2	747 61.02	748 50.63	749 44.65	750 50.75	751 51.76
747 claudie-instant-v1	748 80.27	749 62.72	750 59.64	751 61.96	752 66.15
748 claudie-v1	749 86.87	750 65.08	751 65.72	752 65.98	753 70.91
749 claudie-v2	750 86.87	751 66.26	752 62.81	753 66.06	754 70.50
750 gpt-3.5-turbo-1106	751 83.06	752 60.48	753 64.71	754 57.93	755 66.55
751 gpt-4-1106-preview	752 96.19	753 65.88	754 81.19	755 81.93	756 81.30
752 meta/code-llama-instruct-34b-chat	753 37.35	754 45.66	755 0.48	756 38.44	757 30.48
753 meta/llama-2-70b-chat	754 73.40	755 52.30	756 2.68	757 48.22	758 44.15
754 mistralai/mistral-7b-chat	755 38.78	756 41.15	757 25.43	758 52.41	759 39.44
755 mistralai/mistral-8x7b-chat	756 83.20	757 51.90	758 63.51	759 55.25	760 63.47
756 zero-one-ai/Yi-34B-Chat	757 86.12	758 54.81	759 65.85	760 62.90	761 67.42

756 Table 10: Testing score (%) of each candidate LLM on out-of-distribution tasks.  
757

Candidate LLM	MBPP	Hellaswag	Avg ↑
WizardLM/WizardLM-13B-V1.2	37.00	33.38	35.19
claude-instant-v1	60.42	58.51	59.47
claude-v1	59.72	56.85	58.29
claude-v2	64.17	62.42	63.30
gpt-3.5-turbo-1106	65.34	58.66	62.00
gpt-4-1106-preview	68.62	83.96	76.29
meta/code-llama-instruct-34b-chat	51.76	20.82	36.29
meta/llama-2-70b-chat	33.02	52.59	42.81
mistralai/mistral-7b-chat	34.43	25.48	29.96
mistralai/mixtral-8x7b-chat	54.10	41.69	47.90
zero-one-ai/Yi-34B-Chat	38.64	74.26	56.45

758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772 A.3 CANDIDATE LLMs  
773

774 For tasks from RouterBench (Hu et al., 2024), we have candidate LLMs as follows: (i) **WizardLM-13B-V1.2** (Xu et al., 2023) is a fine-tuned instruction-following model from the WizardLM series;  
775 (ii) **Claude-instant-v1** is a lightweight model from Anthropic optimized for speed; (iii) **Claude-v1** is Anthropic’s first-generation flagship model; (iv) **Claude-v2** (Anthropic, 2023) is an improved  
776 successor with stronger reasoning ability; (v) **GPT-3.5-turbo-1106** is OpenAI’s production-grade  
777 model designed for efficiency and broad coverage; (vi) **GPT-4-1106-preview** (OpenAI et al., 2023)  
778 is OpenAI’s most capable general-purpose model at the time of release; (vii) **Code Llama Instruct-34B-Chat** (Rozière et al., 2024) is a code-specialized instruction-tuned model; (viii) **Llama-2-70B-Chat**  
779 (Touvron et al., 2023) is a general conversational model trained with reinforcement learning  
780 from human feedback; (ix) **Mistral-7B-Chat** (Jiang et al., 2023) is an efficient chat-optimized model  
781 from Mistral AI; (x) **Mixtral-8x7B-Chat** (Jiang et al., 2024) is Mistral’s mixture-of-experts model  
782 offering higher throughput; and (xi) **Yi-34B-Chat** (Young et al., 2024) is a large-scale bilingual chat  
783 model with strong performance in both English and Chinese.

784 For NQ and HpQA datasets, the candidate LLMs consist of Llama-3.1-8b-instruct (Grattafiori  
785 et al., 2024), Llama-3.1-70b-instruct (Grattafiori et al., 2024)2, mistral-7b-instruct-v0.3 (Jiang et al.,  
786 2023), qwen2.5-7b-instruct (Yang et al., 2024), gemma-2-27b-it (Team et al., 2024), mixtral-8x22b-  
787 instruct-v0.1 (Jiang et al., 2024).  
788  
789

790  
791 A.4 DATASET DETAILS  
792

793

- **GSM8K** (Cobbe et al., 2021): A dataset of diverse grade school math word problems, testing a  
794 model’s ability to perform multi-step mathematical reasoning.
- **MMLU** (Hendrycks et al., 2021): A benchmark that measures the knowledge acquired by models  
795 during pretraining and evaluates models in zero-shot and few-shot settings across 57 tasks, testing  
796 both knowledge and reasoning on different fields of human knowledge.
- **ARC-C** (Clark et al., 2018): A rigorous question answering dataset, ARC-Challenge includes  
797 complex, different grade-school level questions that require reasoning beyond simple retrieval,  
798 testing the true comprehension capabilities of models. Arc Challenge dataset contains those that  
799 both a retrieval and a co-occurrence method fail to answer correctly)
- **Winogrande** (Sakaguchi et al., 2021): A large-scale and increased harness dataset inspired by  
800 the original Winograd Schema Challenge(WSC) tests models on their ability to resolve pronoun  
801 ambiguity and their ability to understand the context with commonsense knowledge.
- **NQ** (Kwiatkowski et al., 2019): A comprehensive collection of real user queries submitted to  
802 Google Search, with answers sourced from Wikipedia by expert annotators.
- **MBPP** (Austin et al., 2021): The benchmark is designed to be solvable by entry-level program-  
803 mers, covering programming fundamentals, standard library functionality, etc. Each problem  
804 comprises a task description, code solution, and 3 automated test cases.

810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863

- **Hellaswag** (Zellers et al., 2019): This dataset challenges models to pick the best ending choice for a given sentence. It uses Adversarial Filtering(AF) to create a Goldilocks zone of complexity, wherein generations are largely nonsensical to humans but always make models struggle.
- **HpQA** (Yang et al., 2018): This dataset is designed for question answering and features natural, multi-hop questions. It provides strong supervision for supporting facts, enabling the development of more explainable question answering systems.

## A.5 USE OF LLMs

The LLM’s role was strictly a writing and editing assistant, used to augment and refine the work.

The primary uses of the LLM included:

- **Refining Prose and Tone:** Improving the clarity, flow, and academic tone of sentences and paragraphs across all sections.
- **Ensuring Consistency:** Cross-referencing the manuscript to identify and correct inconsistencies in terminology, notation, and quantitative claims between the text and tables.

All scientific contributions, including the core ideas, experimental design, analysis, and final claims, were conceived and executed by the authors. The LLM served as a tool to help articulate these contributions more effectively.