
AcTracer: Active Testing of Large Language Model via Multi-Stage Sampling

Anonymous Submission #15763

Abstract

Performance evaluation plays a crucial role in the development life cycle of large language models (LLMs). It estimates the model’s capability, elucidates behavior characteristics, and facilitates the identification of potential issues and limitations, thereby guiding further improvement. Given that LLMs’ diverse task-handling abilities stem from large volumes of training data, a comprehensive evaluation also necessitates abundant, well-annotated, and representative test data to assess LLM performance across various downstream tasks. However, the demand for high-quality test data often entails substantial time, computational resources, and manual efforts, sometimes causing the evaluation to be inefficient or impractical. To address these challenges, researchers propose active testing, which estimates the overall performance by selecting a subset of test data. Nevertheless, the existing active testing methods tend to be inefficient, even inapplicable, given the unique new challenges of LLMs (*e.g.*, diverse task types, increased model complexity, and unavailability of training data). To mitigate such limitations and expedite the development cycle of LLMs, in this work, we introduce AcTracer, an active testing framework tailored for LLMs that strategically selects a small subset of test data to achieve a nearly optimal performance estimation for LLMs. AcTracer utilizes both internal and external information from LLMs to guide the test sampling process, reducing variance through a multi-stage pool-based active selection. Our experiment results demonstrate that AcTracer achieves state-of-the-art performance compared to existing methods across various tasks, with up to 38.83% improvement over previous SOTA.

1 Introduction

Evaluating Large Language Models (LLMs) is crucial for assessing their performance and identifying potential limitations, which provides an understanding of LLMs’ capability and facilitates guiding directions for future improvements. However, considering the intricate auto-regressive nature [1], the diverse tasking-oriented handling capabilities, and the corresponding large-volume training data, a thorough-paced evaluation is often impractical for the current LLM development life cycle considering the high costs of LLM execution on test data and time, especially when the available data for testing purposes are huge in size. Unlike Deep Neural Networks (DNNs) designed for specific tasks, LLMs serve as general foundation models capable of addressing a wide range of tasks, making the test spaces to be explored far larger than traditional DNN models. Furthermore, LLMs often operate under the free-form autoregressive generation mechanism, which makes testing of LLM even more challenging, requiring higher expenses to evaluate the generated responses in contrast to the classification or regression problems. Additionally, LLMs’ outputs can change significantly across different versions (*e.g.*, from GPT3 to GPT4), making frequent re-labelling necessary. Therefore, the volume of test data required and the labelling cost per test point (data instant) present significant challenges to the progression of LLM evaluation technologies.

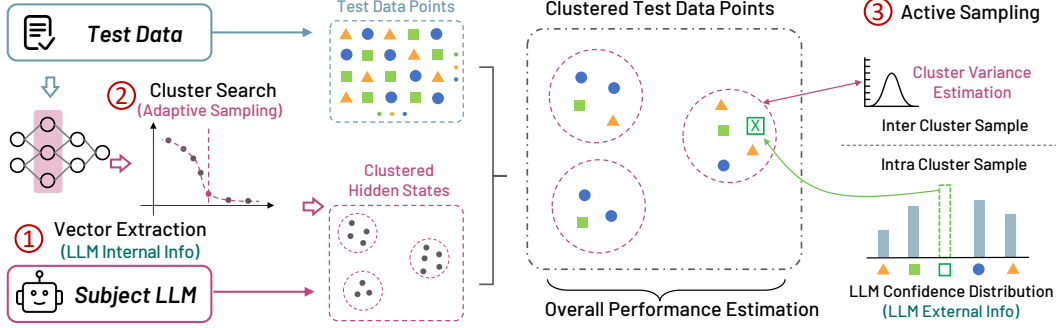


Figure 1: Overall Workflow of AcTracer. ①: Internal and external information extraction from LLMs during inference. ②: An automated search mechanism to identify a suitable number of clusters corresponding to a given LLM and test data. The geometry structure obtained through the clustering algorithm partitions the input test spaces for more efficient sampling. ③: An intra-cluster and inter-cluster sampling strategy to actively select the next data point for labelling.

While the complete evaluation of all possible test data becomes impractical, researchers often resort to an alternative feasible solution: sampling. In particular, by choosing only a subset of test data and performing subsequent labelling, it is possible to estimate models’ performance at a lower cost. Although random sampling is a commonly used baseline across various domains [2, 3, 4], the estimation accuracy can be further improved in an active sampling manner [5, 6, 7, 8], namely *active testing*. Specifically, given test data D , we iteratively choose a data point d to sample and obtain its label l . At each step t , we collect and analyze an existing drawn set $\mathcal{T}_{t-1} = \{(d_1, l_1), \dots, (d_{t-1}, l_{t-1})\}$ to actively decide the next point to label, (d_t, l_t) . Finally, the performance on \mathcal{T}_n is used for the estimation given labelling budget n . However, with the aforementioned LLM-specific characteristics, active testing of LLMs introduces new challenges:

(1) **Complexity of Output Analysis.** LLMs’ outputs consist of mixed information that can potentially mislead the output-guided active testing. While model outputs, such as uncertainty, serve as key indicators in guiding testing in related fields [8, 9, 10, 11, 12, 13], accurately gauging the confidence of LLMs is still an unsolved problem since their responses usually consist of hundreds or even thousands of tokens that encompass intertwined information. According to recent studies, naive aggregation strategies are not always reliable in the context of LLMs [14, 15, 16]. Furthermore, Arora *et al.* [17] pointed out that LLM training involves minimizing both inherent *language entropy*—which arises from multiple possible vocabulary choices conveying similar meanings—as well as *excess cross-entropy*, which reflects model capability. Thus, the uncertainty in LLM inference is entwined with these dual entropies, which may introduce biases in output-guided sampling.

(2) **Accessibility to Prior Knowledge.** Given existing prior knowledge (*e.g.*, labelled training data), it is possible to leverage supervised learning to learn the relationship between models’ output and their performance, thereby directly obtaining an overall estimation for unlabeled ones. However, the situation becomes intricate in the context of LLMs. The training data of LLMs are usually inaccessible, and even with the training data, linking training loss to task performance is non-trivial. While training-based estimation is still useful for training guidance purposes, it is commonly recognized that it is important and necessary to develop completely training-free methods.

(3) **Aggregated Benchmarks.** In response to the emergent abilities of LLM in diverse downstream tasks, the current model evaluations tend to shift focus from single-task assessment to aggregated multi-task benchmark. For example, LLM evaluations now probe deeper into mathematical reasoning within complex scenarios [18, 19, 20], testing model problem-solving abilities across varied domains [21, 22], or assessing trustworthiness and safety from multiple perspectives [23, 24]. Among these aggregated benchmarks, the behavior of LLMs can vary significantly across different tasks. Collecting labeled data for each task to train a robust and universal estimator or to leverage domain-specific guidance for sampling – which are quite common in single-task-oriented active testing – may be impractical for LLMs.

Given these challenges, in this paper, we aim to investigate the following research question:

76 *Can we design an active testing framework for LLMs that is purely unsupervised (as a plug-and-play*
77 *tool) to enable label-efficient evaluations?*

78 We propose AcTracer, a novel approach that leverages both internal (*e.g.*, neuron activity) and external
79 (*e.g.*, output confidence score) information from LLMs to estimate the overall performance of the
80 subject LLM in a pool-based multi-stage active selection manner. The overall workflow is illustrated
81 in Fig 1. The internal states of the models provide a unified representation across various tasks,
82 serving as the foundation for our analysis. Building on this structure, we attempt to perform unbiased
83 sampling guided by LLMs’ confidence score. Extensive studies on seven datasets across different
84 domains demonstrate the effectiveness of our method, which achieves state-of-the-art estimation
85 accuracy for LLM evaluation. Further ablation studies are conducted to investigate the impact of each
86 component on our Framework.

87 In summary, our main contribution is the design and development of a novel active testing framework
88 for LLMs that utilizes a combination of sampling strategies derived from model analysis. We also
89 introduce an extensive active testing testbed designed to support and enrich future research in this
90 area. Our accompanying source code is anonymously available at <https://anonymous.4open.science/r/Neurips24-AcTracer-22C5/README.md>.
91

92 2 Related Work

93 **Model Performance Estimation.** Estimating AI models’ performance in a label-efficient manner is
94 crucial for applications such as model selection [25], improvement [26], and performance monitor-
95 ing [27]. Most prior research concentrated on classification models, often addressing the estimation
96 problem through learning-based or model-based analysis methods. For learning-based approaches, a
97 key step is selecting and processing the appropriate features for subsequent learning. It is possible to
98 learn the relationship between models’ output [10, 11, 12, 13] or models’ internal states [28, 29] w.r.t
99 their performance. Fu *et al.* [7] recently explored using traditional classifiers such as Multi-Layer
100 Perceptron (MLP) and labelled data to comprehend the relationship between LLMs’ confidence and
101 performance. Although these learning-based methods present promising capabilities, they heavily
102 depend on prior knowledge and differ significantly in their settings and tasks in contrast to our
103 sample-based evaluations. Model-based analysis approaches offer alternatives by examining models’
104 behaviors, for instance, estimating performance by observing inconsistencies across an ensemble
105 of models [30] or analyzing model reactions to input perturbations [31, 32]. Nevertheless, these
106 methods usually focus more on anomaly detection, such as predicting out-of-distribution (OOD)
107 cases, rather than estimating the general performance of models.

108 Another widespread evaluation approach involves leveraging LLMs themselves to assess the quality of
109 their outputs [33, 34, 35, 36, 37]. This solution takes advantage of LLMs’ ability on human language
110 understanding and can be scaled up without human intervention. For instance, TruthfulQA [33]
111 utilizes a fine-tuned GPT-3 to evaluate truthfulness, while LLM-EVAL [34] introduces a unified
112 schema to label open-domain conversations. PandaLM [35] adapts a judge language model trained to
113 rank the outputs from other models. However, recent studies indicate that LLM-centric evaluations
114 can be biased and may not always provide reliable results, underscoring the necessity for human
115 labelling [38]. Moreover, LLM evaluator and active testing are not mutually exclusive, as the latter
116 can be integrated into the evaluation process based on the former to further reduce costs.

117 **Active Testing.** Active testing involves sequentially selecting test data for labelling from a pool of
118 unlabeled samples, aiming to estimate a model’s behavior under certain metrics. The primary goal
119 is to achieve unbiased sampling and reduce the overall variance of the estimations. Different from
120 performance estimation, which relies heavily on prior knowledge of the model and the task, active
121 testing is designed to be more universally applicable as a plug-and-play tool. As an early effort in
122 this direction, CES [9] utilizes the neuron activation patterns from the last hidden layer of each test
123 data point to actively select a representative subset based on these hidden representations. Then, a
124 data point is selected to minimize the cross-entropy between the sampled set and the entire dataset.
125 PACE [39] extends this method further by identifying representative sets using the MMD-critic
126 algorithm actively based on the geometric structure of the last hidden layer.

127 In addition, Kossen *et al.* [5] explore the connection between active testing and active learning,
128 proposing a framework that selects data points according to acquisition functions. These functions
129 are derived from uncertainty estimates made by actively trained surrogate models. The framework is

130 further refined by ASEs [6], which introduces a more robust acquisition function with theoretical
131 guarantees. However, implementing such functions in testing autoregressive generation models can
132 be non-trivial. Again, such type of estimation approach might be hard to be applied to LLMs.

133 More recently, DiffUse [40] was introduced to facilitate label-efficient model selection by actively
134 selecting data points for labelling through an analysis of embeddings from LLM outputs. Although
135 this method was initially designed for model selection, it has the potential to be adapted for active
136 testing. Despite all these advancements, to the best of our knowledge, there is no systematic research
137 on performing effective active testing on LLMs. We hope our work can serve as one of the baselines
138 along the direction and pave the way for more cost-efficient LLM evaluation and development.

139 3 Methodology

140 3.1 General Framework

141 AcTracer encompasses the following three steps at a high level: (1) Extract vector representations for
142 each data point in the test set from LLMs; (2) Conduct a distance-based partitioning for the test set
143 based on the extracted vectors; (3) Perform adaptive active sampling empowered by the partitioned
144 vector space. Detailed explanations of the methodology are provided in the following subsections.

145 The first two steps of our framework rely on hidden representation analysis of LLMs. Recent
146 studies find that the internal states of LLMs contain important information capable of revealing
147 important properties such as the LLMs’ truthfulness [41, 42], knowledge [43, 44], beliefs [45], and
148 emotions [46]. Based on these findings, our intuition and study results show that the internal neurons
149 of LLMs often exhibit similar behavioral characteristics to human neurons, where different neurons
150 exhibit diverse behavioral patterns in response to varying tasks [47]. The hidden representation of
151 neurons for each test point spans a high-dimensional space that represents the geometric structure of
152 LLMs’ internal reactions to presented queries. Within this space, test points associated with similar
153 tasks tend to aggregate into compact groups, which naturally form distinct clusters. These clusters
154 partition the entire test set into subsets, and within each subset, we assume that LLMs have alike
155 behavior patterns, resulting in lower performance variance. Namely, the evaluation results of test
156 points falling in the same subset should be similar.

157 Based on the geometric structure of LLMs’ internal patterns, step 3 in AcTracer aims to achieve a
158 more accurate and unbiased estimation. This is achieved through adaptive stratified sampling [48] on
159 the clusters. This strategy actively selects a data point to label in each round, thereby accelerating
160 the convergence speed of the estimation error reduction. Beyond this inter-cluster sampling strategy,
161 we also leverage the output confidence of LLMs as a guide for intra-cluster test selection, aiming
162 to achieve distribution-aware, unbiased sampling within each cluster. Eventually, by combining the
163 estimated performance across different clusters, it is expected to obtain a precise assessment of the
164 overall performance of LLMs in terms of the complete test set.

165 3.1.1 Vector Representation Extraction

166 The initial step of our framework is to extract the internal hidden states of LLMs to guide further
167 testing. After feeding the prompt to LLMs, we can collect a series of hidden states, which we consider
168 retaining the behavior patterns of the LLM. Specifically, we draw the neural activities preceding the
169 generation of the first token (*e.g.*, LLMs’ reactions to the prompt), which have been demonstrated to
170 effectively represent the LLM’s knowledge of the question [46, 49, 43]. Ideally, all neuron activations
171 within the LLM should be analyzed to form the representation of each data point. Nevertheless, given
172 the computational constraints in real-world scenarios, particularly during the continuous development
173 and integration phases of LLMs, such comprehensive analysis is impractical. Therefore, we opt to
174 take features from only one layer. Based on the findings from recent works, we select an intermediate
175 layer (*e.g.*, Layer 16 of a 32-layer LLM) as it has been recognized as the most informative for various
176 downstream tasks [41, 46, 50, 42]. Additional results of utilizing the final layer for hidden state
177 extraction are discussed in Appendix A.1.1. To further reduce time complexity and avoid the curse of
178 dimensionality [51], we apply Principal Component Analysis (PCA) for dimension reduction.

3.1.2 Automated Search for Cluster Number

With the extracted internal representations of each data point, unsupervised clustering algorithms can be applied to perform a distance-based partition on the vectorized test set. In this study, we select Balanced K-means [52] as the partition algorithm, which is an adapted version of the original K-means that assigns an equal number of data points to each cluster. We choose this algorithm since (1) naive K-means can sometimes lead to extremely uneven partition sizes, which consequently lower the test estimation performance; (2) related work pointed out that Balanced K-means can achieve better performance for unsupervised domain discovery on LLMs [53]. We employ the implementation detailed in [53] for this work.

Given the candidate partition algorithm, the subsequent crucial step is to determine the cluster number that optimizes the partition performance. This can be particularly challenging in active testing, where the available test samples and underlying intrinsic structure of data vary widely across different tasks, which demands a significantly different number of clusters for adequate partition. Moreover, testing LLMs across a broad spectrum of dimensions introduces additional complexities, as performing extensive cross-validation for the optimal cluster number is impractical. Given the critical role of the number of clusters in establishing a valid representation of the test data to guide testing, we propose a solution called CluSearch that performs an automated, model- and task-specific search for the cluster number without any ground truth.

The designed search is empowered by the *inertia* metric, namely, the objective function of naive K-means that measures the sum of distances between each data point and its corresponding cluster center (the details can be found in Appendix A.1.2). Given a fixed number of clusters, lower *inertia* indicates better results. However, as this metric is a convex decreasing function in terms of cluster number, simply minimizing it by maximizing the number of clusters is trivial and ineffective. Instead, the relationship between cluster number and inertia is more of a trade-off, where the *elbow* point of the cluster num-inertia curve is a widely used heuristic for appropriate cluster number search [54]. In our study, we employ the Kneedle algorithm [55] to automatically identify the elbow point as the proper number of clusters. To enhance the efficiency of the search process, we leverage adaptive sampling [56] to intensively sample cluster number-inertia pairs in regions of rapid function change. Our preliminary experiments show that adaptive sampling can reduce the search space exponentially, achieving efficient search with a limited budget.

3.1.3 Adaptive Active Sampling Based on Partition

In this section, we briefly introduce our sampling strategy given the partitions created by the clustering algorithm.

Inter-cluster wise. The main objective of the strategy is to identify representative points within each cluster and minimize the variance in the performance estimation. If the variances are given in advance, the optimal allocation would be the ideal strategy, which distributes samples based on known variances within each cluster. However, it is infeasible in our setting as we are actively selecting points to label. To address this challenge, Carpentier *et al.* [48] suggested an approach to progressively estimate variances. This method involves calculating the Monte Carlo Upper Confidence Bound (MC-UCB) for each cluster (treated as an ‘arm’ in a multi-armed bandit problem) and selecting the arm with the highest upper bound for subsequent sampling. At current search round t , the MC-UCB score of cluster k is computed as follows:

$$B_{k,t} = \frac{w_k}{T_{k,t-1}} (\delta_{k,t-1} + \frac{2\beta}{\sqrt{T_{k,t-1}}}), \quad (1)$$

where w_k is the cluster size, $T_{k,t-1}$ is the number of points sampled in the previous round, $\delta_{k,t-1}$ is the empirical standard deviation within each cluster, and β is a hyper-parameter. Under most LLM evaluation scenarios where the performance metric is bounded, the parameter β can be set according to number of sample n as follows, where Carpentier *et al.* provided formal discussions on this point:

$$\beta = \sqrt{\log(2/n^{-9/2})} \quad (2)$$

225 **Intra-cluster wise.** Although the algorithm so far specifies the target cluster to apply sampling, it
 226 does not determine the sub-sampling strategy within each cluster. In other words, the algorithm needs
 227 to determine which specific data point in the cluster should get sampled and labelled. While random
 228 sampling remains a feasible option, more unbiased but resource-intensive sampling techniques can
 229 also be applied since the partition divides the space into smaller subsets, enabling high-complexity
 230 algorithms. Our intra-cluster sample is guided by the output *confidence* of the LLMs. Although
 231 LLMs’ confidence patterns may vary across different sub-tasks in an aggregated benchmark, our
 232 clustering analysis has already alleviated such a problem by partitioning the test space into subsets
 233 characterized by LLMs’ internal states. Our goal in this stage is to maintain the confidence distribution
 234 of the sample drawn to be as close as possible to the distribution of the entire cluster, aiming for
 235 an intra-cluster level unbiased sampling. This is achieved by selecting candidate sample points that
 236 greedily minimize the distance between the confidence distributions of the sampled points and the
 237 entire cluster. For measuring the distance between these distributions, the two-sample Kolmogorov-
 238 Smirnov test [57] and the Wasserstein distance [58, 59] are applied. We further discuss related details
 239 in the Appendix A.1.3. The overall algorithm is shown in Algorithm 1.

Algorithm 1 Overall Structure of AcTracer

Require: LLM M , Test input prompt set P , Parameter β , Sample budget n , extracted features emb
Ensure: Estimated performance $\hat{\mu}$

```

1:  $k^* \leftarrow \text{Algo\_3}(M, P, emb)$  ▷ Search for target cluster number  $k^*$ . Details in Appendix
2:  $C \leftarrow \text{Cluster}(M, P, k^*, emb)$  ▷ Perform Balanced-K-means clustering.
3: # Initialize selection of each cluster with two samples following [48] to avoid dividend by zero case.
4: for  $i = 1$  to  $k^*$  do
5:    $S_i \leftarrow \emptyset$ 
6:   for  $m = 1$  to 2 do
7:     # Select the data point that minimizes the distribution distance (DIST) function.
8:      $\hat{q} \leftarrow \arg \min_{q \in C_i \wedge q \notin S_i} \text{DIST}(C_i, S_i \cup \{q\})$ 
9:      $S_i \leftarrow S_i \cup \{\hat{q}\}$ 
10:   end for
11: end for
12: # Begin Stratified Monte Carlo Sampling
13: for  $t = 2 \times k^* + 1$  to  $n$  do
14:   for  $k = 1$  to  $k^*$  do
15:      $B_{k,t} \leftarrow \text{Compute\_B}(C_k, t, \beta)$  ▷ Compute B according to Eq. 1
16:   end for
17:    $\hat{a} \leftarrow \arg \max_{1 \leq a \leq k^*} B_{a,t}$  ▷ Select cluster to sample according to MC-UCB
18:    $\hat{q} \leftarrow \arg \min_{q \in C_{\hat{a}} \wedge q \notin S_{\hat{a}}} \text{DIST}(C_{\hat{a}}, S_{\hat{a}} \cup \{q\})$  ▷ Intra-cluster sample
19:    $S_{\hat{a}} \leftarrow S_{\hat{a}} \cup \{\hat{q}\}$ 
20: end for
21:  $\hat{\mu} = \sum_{k=1}^{k^*} w_k \hat{\mu}_k$  ▷ Compute the estimation given the mean of each cluster.
22: return  $\hat{\mu}$ 

```

240 4 Experiments

241 4.1 Dataset

242 A key advancement of LLMs over their predecessors is their ability to handle a diverse spectrum
 243 of tasks via free-form generation. Taking this unique characteristic into account, we select seven
 244 evaluation datasets in eight settings to cover a range of model capabilities, including common
 245 knowledge, mathematical reasoning, problem-solving, and code generation. The included datasets
 246 are listed below:

- 247 • **Common Knowledge.** We select TriviaQA ([60]) and NQ-open ([61]) as two question-answering
 248 datasets designed to evaluate the World Knowledge of LLM.
- 249 • **Mathematical Reasoning.** We evaluate our method on GSM8K ([19]), a dataset that focuses on
 250 basic math problems that require multi-step reasoning.
- 251 • **Problem Solving.** We use AGIEval ([21]), an aggregated benchmark aimed at assessing LLMs
 252 within the context of human-centric standardized exams to gauge their general abilities in human
 253 cognition and problem-solving.

- **Truthfulness.** We choose TruthfulQA ([33]), a benchmark tailored for imitative falsehoods measurement to assess the truthfulness and informativeness of the LLMs. In our experiment, we refer to informativeness evaluation as TruthfulQA-I and truthfulness evaluation as TruthfulQA-T.
- **Code Generation.** MBPP ([62]) and HumanEval ([63]) datasets are selected to test LLMs’ ability to understand human intentions and perform corresponding code generation.

We aim to select a range of diverse and representative datasets to perform a rigorous evaluation for the testing methods under complex conditions that closely mirror real-world scenarios. The datasets vary in size, from over one hundred (HumanEval) to nearly 18,000 (TriviaQA), spanning three orders of magnitude. With the evaluation of various downstream tasks, we aim to reveal the strengths and weaknesses of different methods and offer practical guidelines for the following applications.

4.2 Evaluation Metric

One common widely adopted approach to evaluate the effectiveness of active testing methods is to measure the errors between the estimation and the ground truth, typically using metrics like RMSE [8]. However, in our pool-based setting, where data points are actively and progressively selected, a single-point estimation error may not provide a complete picture for the effectiveness assessment. To tackle this issue, in this study, we conduct evaluations for sampling proportion (labelling budgets) p ranging from 5% to 50% of the original dataset, with increments of 1%, and use the results to construct a 2-D diagram. This diagram plots the number of sampling points (x-axis) against the relative error of the estimation (y-axis). We then calculate the Area Under the Curve (AUC) as an indicator of each method’s effectiveness. A lower AUC value indicates a better performance. We only report AUC value in the main text due to space limit. Full results are shown in Appendix A.3.

4.3 Main Result

Baselines For the selection of baseline methods, we adhere to the following criteria: (1) the methods should function as plug-and-play tools for test estimation without the need for training data; (2) the methods selected should either be widely accepted in the industry, published in top-tier conferences or journals and proved to be useful for classical DNNs, or available as pre-print versions that demonstrate promising results on more recent LLMs. Aligned with these criteria, we selected five baseline methods as follows:

- *RandomSelection*, which serves as the default strategy in many practical scenarios;
- Confidence-based Stratified Sampling (*CSSampling*) [9], which enhances test estimation efficiency by dividing the models’ confidence scores across the entire dataset into k sections and then applying stratified sampling according to the confidence distribution within each bin;
- Cross Entropy-based Sampling (*CESampling*) [9]¹, which guides the sampling process through distribution analysis of the last layers’ neurons between selected points and the entire test set;
- Practical ACcuracy Estimation (*PACESampling*) [39], which utilizes the MMD-critic algorithm to select the most representative test inputs for test estimation; and
- *DiffuseSampling* [40], a recent approach for label-efficient model selection of LLMs based on clustering analysis of their output text embeddings².

Experiment Configurations. In terms of experiments, we select Llama 2-7B [64] for natural language processing tasks and Code Llama-7B-Python [65] for code generation tasks. To mitigate the inherent randomness in the experiment, we repeat our experiments ten times and use the median relative error for the AUC computation. Accordingly, this process results in a total of 6 (methods) \times 46 (labelling budget settings) \times 10 (repetitions) \times 8 (dataset settings) = 22,080 experiments. Other details are shown in Appendix A.2.

Results. The experiment results are presented in Table 1, which demonstrates that AcTracer achieves lower estimation errors when assessing the performance of LLMs across a variety of settings with different dataset sizes. Notably, the most significant performance gain is observed with the AGIEval

¹We optimized the code by implementing vectorization, achieving an approximate 100x speedup, thereby making the algorithm practical for LLMs.

²Model selection and performance estimation share similar settings. By assigning the ground truth label to LLMs’ performance, this approach can be effectively adapted for test estimation.

Table 1: AUC for relative estimation error across sampling proportions from 5% to 50% on seven datasets under eight settings. The best performance is indicated by the *top-1* color, and the second best by the *top-2* color. Additionally, we report our method’s performance gain compared with the best method in baselines.

	AGIEval	TriviaQA	NQ-open	GSM8K	TruthfulQA-I	TruthfulQA-T	MBPP	HumanEval
<i>RandomSelection</i>	0.0162	0.0035	0.0193	0.0377	0.0040	0.0200	0.0321	0.0633
<i>CSSampling</i>	0.0162	0.0033	0.0211	0.0418	0.0038	0.0195	0.0308	0.0575
<i>CESSampling</i>	0.0164	0.0030	0.0281	0.0610	0.0067	0.0239	0.0497	0.0627
<i>PACESampling</i>	0.0310	0.0405	0.0634	0.0362	0.0069	0.0104	0.0326	0.2210
<i>DiffuseSampling</i>	0.0539	0.0331	0.0547	0.0294	0.0070	0.0331	0.0331	0.0419
AcTracer	0.0099	0.0028	0.0166	0.0262	0.0031	0.0172	0.0232	0.0361
Performance Gain	+38.83%	+8.00%	+13.94%	+10.82%	+18.53%	-39.75%	+24.64%	+13.84%

dataset, a benchmark with ten distinct tasks in English specifically designed to assess the problem-solving ability of LLMs. This substantial improvement (38.83%) over the baseline methods proves the usefulness of our methods in evaluating LLMs on aggregated benchmarks. Furthermore, AcTracer consistently delivers stable performance gains across other datasets of various sizes.

The only exception occurred in the Truthfulness evaluation, where AcTracer is only the 2nd place. We further investigate this problem and find that truthfulness and performance are fundamentally *different properties*. The latter evaluates the LLMs’ capability to solve a problem, whereas the former assesses whether LLMs are lying. Although previous studies have shown that the internal states can, to some extent, reveal the truthfulness of the model [41], it might require specific approaches to capture such information explicitly. For example, training classifiers [41] or feeding prompts that activate the truthfulness-related neurons within LLMs [46]. Since we directly use PCA and do not perform any other techniques for truthfulness mining, the clustering process loses such information, and the resulting partitions are biased. Nevertheless, we argue that this result retroactively supports our hypothesis about the importance of LLMs’ internal state. If the extracted states do not retain any LLM behavior-related information, AcTracer would likely deliver close or beyond performance to the random selection approach, as shown in TruthfulQA-T. However, current experiment results reveal that the sampling is biased in other directions because the internal states contain *other information* that is irrelevant to the truthfulness property. On the other hand, AcTracer still achieves 18.53% performance gain on evaluating informativeness (which is more revolved around LLMs’ capability) on the same dataset (TruthfulQA). For future improvements, we believe it is feasible to leverage techniques such as representation engineering [46] to deliberately activate neurons based on specific properties of interest to be measured.

Another interesting finding is that *RandomSelection* actually achieves relatively adequate performance in three out of eight settings. While it seems surprising, we consider this because when the sampling space is well-defined, random testing can behave as a strong baseline. For example, it is able to find bugs in complex distributed systems even with formal guarantee [3, 4]. It is also a moderate technique in compressed sensing [2], where the random sampling matrix is widely used in practice for signal recovery [66]. Conversely, the baseline methods that work well for classification models can sometimes result in more biased estimations in the context of LLMs. This may stem from the inherent differences between LLMs and classification DNNs, particularly the free-form autoregressive generation mechanism. It also points out that the prior experience, findings, and solutions for traditional DNNs may no longer be applicable to LLMs. Therefore, when the internal information or the designated knowledge is not clear, falling back to a random selection strategy may be a conservative alternative.

5 Ablation Study

In this section, we conduct ablation studies to assess and understand the effectiveness of each component in AcTracer’s framework design. In particular, we focus on three components: (1) The automatic cluster number search algorithm in charge of extracting the underlying LLMs’ behavior patterns in the test space (CluSearch); (2) The adaptive strategy that utilizes stratified sampling based on the computation of Monte Carlo Upper Confidence Bound (MC-UCB); (3) The sub-sampling strategy inside each cluster to preserve an unbiased data selection with respect to LLMs’s confidence distribution (SubSample). Corresponding to the three key components of AcTracer, we establish three distinct configurations for our ablation studies:

- AcTracer without CluSearch (AcTracer-CluSearch). We employ a fixed number of clusters³ for the unsupervised learning algorithm across all datasets and sampling proportions.
- AcTracer without adaptive stratified sampling (AcTracer-Inter-cluster Search) In this setting, we replace the adaptive approach with uniform allocation (*i.e.*, assigning sampling numbers proportional to the size of each cluster) which is at least as precise as random sampling [67].
- AcTracer without the sub-sampling strategy within each cluster (AcTracer-Intra-cluster Search). When a cluster is selected by the MC-UCB, we randomly choose a point within the cluster for sampling.

Table 2: Ablation study results across three settings: performance comparison and relative drops.

	AGIEval	TriviaQA	NQ-open	GSM8K	TruthfulQA-I	TruthfulQA-T	MBPP	HumanEval
AcTracer-CluSearch	0.0168 -41.08%	0.0025 +8.66%	0.019 -13.35%	0.0385 -31.90%	0.0036 -12.79%	0.0183 -5.93%	0.0308 -24.62%	0.0938 -61.50%
AcTracer-Inter	0.0105 -5.26%	0.0027 +1.10%	0.0173 -3.93%	0.0272 -3.74%	0.0032 -1.71%	0.0184 -6.14%	0.0226 +2.67%	0.0352 +2.44%
AcTracer-Intra	0.0164 -39.39%	0.0030 -6.44%	0.0193 -13.85%	0.0418 -35.26%	0.0037 -15.64%	0.0173 -0.46%	0.0314 -26.00%	0.0587 -38.46%

We conduct in total $3 \times 46 \times 10 \times 8 = 11,040$ experiments based on the aforementioned configurations, and the corresponding results are shown in Table 2. We notice that both CluSearch and SubSample are essential for the performance of AcTracer in most settings. Omitting CluSearch leads to a significant accuracy degradation, with a drop as steep as 61.50% observed in the HumanEval dataset. On the other hand, the SubSample component substantially accelerates estimation divergence in certain scenarios. By removing it, the performance can drop by as much as 39.39% in AGIEval. We speculate that SubSample is particularly vital when the output contains more information on models’ uncertainty w.r.t the problem rather than the language entropy of vocabulary selection, which is likely the case with the classification-based AGIEval benchmark. We do not observe significant gains in evaluating truthfulness on TruthfulQA as expected since it is hard to extract related patterns by simply analyzing the model output. Lastly, the MC-UCB component contributes modestly, as it may slightly impair performance when the available number of samples for variance estimation is limited (*e.g.*, MBPP and HumanEval). Despite these limitations, we believe that retaining MC-UCB can make AcTracer more robust, particularly in extreme cases. We believe it is possible to further increase the performance of our framework by integrating more advanced stratified sampling strategies suitable in our scenarios [68, 69].

6 Conclusion

In this paper, we introduce a novel active testing framework called AcTracer, designed to select a subset of test data via a multi-stage sampling scheme, thereby accomplishing a comprehensive performance estimation for LLMs. Different from the existing active testing methods, AcTracer considers the distinct characteristics of LLMs and leverages both internal hidden states and external output confidence scores to collaboratively select a subset of the most representative test data for LLM performance estimation. Extensive experiments across a variety of tasks and LLMs have demonstrated the effectiveness of AcTracer, outperforming state-of-the-art baselines on most datasets. We hope that our exploratory work can inspire further research in this direction, aiming to establish comprehensive, efficient, and accurate performance evaluation techniques for LLMs.

Limitations and Future Directions. Although AcTracer has demonstrated promising effectiveness on most experiment datasets, it still shows drawbacks in estimating certain LLMs’ properties, such as truthfulness. Our framework could potentially be enhanced by incorporating an improved internal state extraction technique tailored to the target metric, a more adaptive partition algorithm for inter-cluster search, and a more advanced uncertainty estimation method for intra-cluster search.

³We set the cluster number as 8 according to the sklearn K-means default parameter.

References

- [1] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, et al. Language models are few-shot learners. *Advances in neural information processing systems*, 33:1877–1901, 2020.
- [2] David L Donoho. Compressed sensing. *IEEE Transactions on information theory*, 52(4):1289–1306, 2006.
- [3] Rupak Majumdar and Filip Niksic. Why is random testing effective for partition tolerance bugs? *Proceedings of the ACM on Programming Languages*, 2(POPL):1–24, 2017.
- [4] Burcu Kulahcioglu Ozkan, Rupak Majumdar, Filip Niksic, Mitra Tabaei Befrouei, and Georg Weissenbacher. Randomized testing of distributed systems with probabilistic guarantees. *Proceedings of the ACM on Programming Languages*, 2(OOPSLA):1–28, 2018.
- [5] Jannik Kossen, Sebastian Farquhar, Yarin Gal, and Tom Rainforth. Active testing: Sample-efficient model evaluation. In *International Conference on Machine Learning*, pages 5753–5763. PMLR, 2021.
- [6] Jannik Kossen, Sebastian Farquhar, Yarin Gal, and Thomas Rainforth. Active surrogate estimators: An active learning approach to label-efficient model evaluation. *Advances in Neural Information Processing Systems*, 35:24557–24570, 2022.
- [7] Harvey Yiyun Fu, Qinyuan Ye, Albert Xu, Xiang Ren, and Robin Jia. Estimating large language model capabilities without labeled test data. *arXiv preprint arXiv:2305.14802*, 2023.
- [8] Antonio Guerriero, Roberto Pietrantuono, and Stefano Russo. Deepsample: Dnn sampling-based testing for operational accuracy assessment. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, pages 1–12, 2024.
- [9] Zenan Li, Xiaoxing Ma, Chang Xu, Chun Cao, Jingwei Xu, and Jian Lü. Boosting operational dnn testing efficiency through conditioning. In *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 499–509, 2019.
- [10] Weijian Deng and Liang Zheng. Are labels always necessary for classifier accuracy evaluation? In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 15069–15078, 2021.
- [11] Devin Guillory, Vaishaal Shankar, Sayna Ebrahimi, Trevor Darrell, and Ludwig Schmidt. Predicting with confidence on unseen distributions. In *Proceedings of the IEEE/CVF international conference on computer vision*, pages 1134–1144, 2021.
- [12] Weijian Deng, Yumin Suh, Stephen Gould, and Liang Zheng. Confidence and dispersity speak: characterizing prediction matrix for unsupervised accuracy estimation. In *International Conference on Machine Learning*, pages 7658–7674. PMLR, 2023.
- [13] Qiang Hu, Yuejun Guo, Xiaofei Xie, Maxime Cordy, Mike Papadakis, Lei Ma, and Yves Le Traon. Aries: Efficient testing of deep neural networks via labeling-free accuracy estimation. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 1776–1787. IEEE, 2023.
- [14] Lorenz Kuhn, Yarin Gal, and Sebastian Farquhar. Semantic uncertainty: Linguistic invariances for uncertainty estimation in natural language generation. In *The Eleventh International Conference on Learning Representations*, 2023. URL <https://openreview.net/forum?id=VD-AYtP0dve>.
- [15] Yuheng Huang, Jiayang Song, Zhijie Wang, Huaming Chen, and Lei Ma. Look before you leap: An exploratory study of uncertainty measurement for large language models. *arXiv preprint arXiv:2307.10236*, 2023.

- [16] Miao Xiong, Zhiyuan Hu, Xinyang Lu, YIFEI LI, Jie Fu, Junxian He, and Bryan Hooi. Can LLMs express their uncertainty? an empirical evaluation of confidence elicitation in LLMs. In *The Twelfth International Conference on Learning Representations*, 2024. URL <https://openreview.net/forum?id=gjeQKFxFpZ>.
- [17] Sanjeev Arora and Anirudh Goyal. A theory for emergence of complex skills in language models. *arXiv preprint arXiv:2307.15936*, 2023.
- [18] Dan Hendrycks, Collin Burns, Saurav Kadavath, Akul Arora, Steven Basart, Eric Tang, Dawn Song, and Jacob Steinhardt. Measuring mathematical problem solving with the MATH dataset. In *Thirty-fifth Conference on Neural Information Processing Systems Datasets and Benchmarks Track (Round 2)*, 2021. URL <https://openreview.net/forum?id=7Bywt2mQsCe>.
- [19] Karl Cobbe, Vineet Kosaraju, Mohammad Bavarian, Mark Chen, Heewoo Jun, Lukasz Kaiser, Matthias Plappert, Jerry Tworek, Jacob Hilton, Reiichiro Nakano, Christopher Hesse, and John Schulman. Training verifiers to solve math word problems. *arXiv preprint arXiv:2110.14168*, 2021.
- [20] Hugh Zhang, Jeff Da, Dean Lee, Vaughn Robinson, Catherine Wu, Will Song, Tiffany Zhao, Pranav Raja, Dylan Slack, Qin Lyu, et al. A careful examination of large language model performance on grade school arithmetic. *arXiv preprint arXiv:2405.00332*, 2024.
- [21] Wanjun Zhong, Ruixiang Cui, Yiduo Guo, Yaobo Liang, Shuai Lu, Yanlin Wang, Amin Saied, Weizhu Chen, and Nan Duan. Agieval: A human-centric benchmark for evaluating foundation models. *arXiv preprint arXiv:2304.06364*, 2023.
- [22] Xiao Liu, Hao Yu, Hanchen Zhang, Yifan Xu, Xuanyu Lei, Hanyu Lai, Yu Gu, Hangliang Ding, Kaiwen Men, Kejuan Yang, et al. Agentbench: Evaluating llms as agents. *arXiv preprint arXiv:2308.03688*, 2023.
- [23] Boxin Wang, Weixin Chen, Hengzhi Pei, Chulin Xie, Mintong Kang, Chenhui Zhang, Chejian Xu, Zidi Xiong, Ritik Dutta, Rylan Schaeffer, et al. Decodingtrust: A comprehensive assessment of trustworthiness in gpt models. 2023.
- [24] Lichao Sun, Yue Huang, Haoran Wang, Siyuan Wu, Qihui Zhang, Chujie Gao, Yixin Huang, Wenhan Lyu, Yixuan Zhang, Xiner Li, et al. Trustllm: Trustworthiness in large language models. *arXiv preprint arXiv:2401.05561*, 2024.
- [25] Lin Zhao, Tianchen Zhao, Zinan Lin, Xuefei Ning, Guohao Dai, Huazhong Yang, and Yu Wang. Flasheval: Towards fast and accurate evaluation of text-to-image diffusion generative models. *arXiv preprint arXiv:2403.16379*, 2024.
- [26] Ozan Sener and Silvio Savarese. Active learning for convolutional neural networks: A core-set approach. In *International Conference on Learning Representations*, 2018. URL <https://openreview.net/forum?id=H1aIuk-RW>.
- [27] Yuzhe Lu, Yilong Qin, Runtian Zhai, Andrew Shen, Ketong Chen, Zhenlin Wang, Soheil Kolouri, Simon Stepputtis, Joseph Campbell, and Katia Sycara. Characterizing out-of-distribution error via optimal transport. *Advances in Neural Information Processing Systems*, 36, 2024.
- [28] Shuyu Miao, Lin Zheng, Jingjing Liu, and Hong Jin. K-means clustering based feature consistency alignment for label-free model evaluation. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 3298–3306, 2023.
- [29] Shuyu Miao, Jian Liu, Lin Zheng, and Hong Jin. Divide-and-aggregate learning for evaluating performance on unlabeled data. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, pages 21395–21402, 2024.
- [30] Aman Mehra, Rahul Saxena, Taeyoun Kim, Christina Baek, Zico Kolter, and Aditi Raghunathan. Predicting the performance of foundation models via agreement-on-the-line. *arXiv preprint arXiv:2404.01542*, 2024.

- [31] Neel Jain, Khalid Saifullah, Yuxin Wen, John Kirchenbauer, Manli Shu, Aniruddha Saha, Micah Goldblum, Jonas Geiping, and Tom Goldstein. Bring your own data! self-supervised evaluation for large language models. *arXiv preprint arXiv:2306.13651*, 2023.
- [32] JoonHo Lee, Jae Oh Woo, Hankyu Moon, and Kwonho Lee. Unsupervised accuracy estimation of deep visual models using domain-adaptive adversarial perturbation without source samples. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 16443–16452, 2023.
- [33] Stephanie Lin, Jacob Hilton, and Owain Evans. TruthfulQA: Measuring how models mimic human falsehoods. In Smaranda Muresan, Preslav Nakov, and Aline Villavicencio, editors, *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 3214–3252, Dublin, Ireland, May 2022. Association for Computational Linguistics. doi: 10.18653/v1/2022.acl-long.229. URL <https://aclanthology.org/2022.acl-long.229>.
- [34] Yen-Ting Lin and Yun-Nung Chen. Llm-eval: Unified multi-dimensional automatic evaluation for open-domain conversations with large language models. *arXiv preprint arXiv:2305.13711*, 2023.
- [35] Yidong Wang, Zhuohao Yu, Wenjin Yao, Zhengran Zeng, Linyi Yang, Cunxiang Wang, Hao Chen, Chaoya Jiang, Rui Xie, Jindong Wang, Xing Xie, Wei Ye, Shikun Zhang, and Yue Zhang. PandaLM: An automatic evaluation benchmark for LLM instruction tuning optimization. In *The Twelfth International Conference on Learning Representations*, 2024. URL <https://openreview.net/forum?id=5Nn2BLV7SB>.
- [36] Chengwei Qin, Aston Zhang, Zhuosheng Zhang, Jiaao Chen, Michihiro Yasunaga, and Diyi Yang. Is chatGPT a general-purpose natural language processing task solver? In *The 2023 Conference on Empirical Methods in Natural Language Processing*, 2023. URL <https://openreview.net/forum?id=u03xn1C0s0>.
- [37] Yejin Bang, Samuel Cahyawijaya, Nayeon Lee, Wenliang Dai, Dan Su, Bryan Wilie, Holy Lovenia, Ziwei Ji, Tiezheng Yu, Willy Chung, Quyet V. Do, Yan Xu, and Pascale Fung. A multitask, multilingual, multimodal evaluation of ChatGPT on reasoning, hallucination, and interactivity. In *Proceedings of the 13th International Joint Conference on Natural Language Processing and the 3rd Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 675–718, Nusa Dua, Bali, November 2023. Association for Computational Linguistics. doi: 10.18653/v1/2023.ijcnlp-main.45. URL <https://aclanthology.org/2023.ijcnlp-main.45>.
- [38] Arjun Panickssery, Samuel R Bowman, and Shi Feng. Llm evaluators recognize and favor their own generations. *arXiv preprint arXiv:2404.13076*, 2024.
- [39] Junjie Chen, Zhuo Wu, Zan Wang, Hanmo You, Lingming Zhang, and Ming Yan. Practical accuracy estimation for efficient deep neural network testing. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 29(4):1–35, 2020.
- [40] Shir Ashury-Tahan, Benjamin Sznajder, Leshem Choshen, Liat Ein-Dor, Eyal Shnarch, and Ariel Gera. Label-efficient model selection for text generation. *arXiv preprint arXiv:2402.07891*, 2024.
- [41] Amos Azaria and Tom Mitchell. The internal state of an LLM knows when it’s lying. In *The 2023 Conference on Empirical Methods in Natural Language Processing*, 2023. URL <https://openreview.net/forum?id=y2V6YgLaW7>.
- [42] Chao Chen, Kai Liu, Ze Chen, Yi Gu, Yue Wu, Mingyuan Tao, Zhihang Fu, and Jieping Ye. INSIDE: LLMs’ internal states retain the power of hallucination detection. In *The Twelfth International Conference on Learning Representations*, 2024. URL <https://openreview.net/forum?id=Zj12nz1Qbz>.
- [43] Roei Hendel, Mor Geva, and Amir Globerson. In-context learning creates task vectors. In Houda Bouamor, Juan Pino, and Kalika Bali, editors, *Findings of the Association for Computational Linguistics: EMNLP 2023*, pages 9318–9333, Singapore, December 2023. Association for

- 527 Computational Linguistics. doi: 10.18653/v1/2023.findings-emnlp.624. URL [https://](https://aclanthology.org/2023.findings-emnlp.624)
528 aclanthology.org/2023.findings-emnlp.624.
- 529 [44] Yuheng Chen, Pengfei Cao, Yubo Chen, Kang Liu, and Jun Zhao. Journey to the center of the
530 knowledge neurons: Discoveries of language-independent knowledge neurons and degenerate
531 knowledge neurons. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38,
532 pages 17817–17825, 2024.
- 533 [45] Peter Hase, Mona Diab, Asli Celikyilmaz, Xian Li, Zornitsa Kozareva, Veselin Stoyanov, Mohit
534 Bansal, and Srinivasan Iyer. Methods for measuring, updating, and visualizing factual beliefs in
535 language models. In Andreas Vlachos and Isabelle Augenstein, editors, *Proceedings of the 17th*
536 *Conference of the European Chapter of the Association for Computational Linguistics*, pages
537 2714–2731, Dubrovnik, Croatia, May 2023. Association for Computational Linguistics. doi: 10.
538 18653/v1/2023.eacl-main.199. URL <https://aclanthology.org/2023.eacl-main.199>.
- 539 [46] Andy Zou, Long Phan, Sarah Chen, James Campbell, Phillip Guo, Richard Ren, Alexander Pan,
540 Xuwang Yin, Mantas Mazeika, Ann-Kathrin Dombrowski, et al. Representation engineering: A
541 top-down approach to ai transparency. *arXiv preprint arXiv:2310.01405*, 2023.
- 542 [47] Noah Zarr and Joshua W Brown. Foundations of human spatial problem solving. *Scientific*
543 *Reports*, 13(1):1485, 2023.
- 544 [48] Alexandra Carpentier, Remi Munos, and András Antos. Adaptive strategy for stratified monte
545 carlo sampling. *J. Mach. Learn. Res.*, 16:2231–2271, 2015.
- 546 [49] Asma Ghandeharioun, Avi Caciularu, Adam Pearce, Lucas Dixon, and Mor Geva. Patchscope:
547 A unifying framework for inspecting hidden representations of language models. *arXiv preprint*
548 *arXiv:2401.06102*, 2024.
- 549 [50] Wes Gurnee and Max Tegmark. Language models represent space and time. In *The Twelfth*
550 *International Conference on Learning Representations*, 2024. URL [https://openreview.](https://openreview.net/forum?id=jE8xbmvFin)
551 [net/forum?id=jE8xbmvFin](https://openreview.net/forum?id=jE8xbmvFin).
- 552 [51] Piotr Indyk and Rajeev Motwani. Approximate nearest neighbors: towards removing the
553 curse of dimensionality. In *Proceedings of the thirtieth annual ACM symposium on Theory of*
554 *computing*, pages 604–613, 1998.
- 555 [52] Mikko I Malinen and Pasi Fränti. Balanced k-means for clustering. In *Structural, Syntactic, and*
556 *Statistical Pattern Recognition: Joint IAPR International Workshop, S+ SSPR 2014, Joensuu,*
557 *Finland, August 20-22, 2014. Proceedings*, pages 32–41. Springer, 2014.
- 558 [53] Suchin Gururangan, Margaret Li, Mike Lewis, Weijia Shi, Tim Althoff, Noah A Smith, and
559 Luke Zettlemoyer. Scaling expert language models with unsupervised domain discovery. *arXiv*
560 *preprint arXiv:2303.14177*, 2023.
- 561 [54] Robert L Thorndike. Who belongs in the family? *Psychometrika*, 18(4):267–276, 1953.
- 562 [55] Ville Satopaa, Jeannie Albrecht, David Irwin, and Barath Raghavan. Finding a" kneedle" in a
563 haystack: Detecting knee points in system behavior. In *2011 31st international conference on*
564 *distributed computing systems workshops*, pages 166–171. IEEE, 2011.
- 565 [56] Bas Nijholt, Joseph Weston, Jorn Hoofwijk, and Anton Akhmerov. Adaptive: Parallel active
566 learning of mathematical functions. *Zenodo*. <https://doi.org/10.5281/zenodo.1182437>, 2019.
- 567 [57] John W Pratt, Jean D Gibbons, John W Pratt, and Jean D Gibbons. Kolmogorov-smirnov
568 two-sample tests. *Concepts of nonparametric theory*, pages 318–344, 1981.
- 569 [58] Nicolas Fournier and Arnaud Guillin. On the rate of convergence in wasserstein distance of the
570 empirical measure. *Probability theory and related fields*, 162(3):707–738, 2015.
- 571 [59] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein gan, 2017.

- [60] Mandar Joshi, Eunsol Choi, Daniel Weld, and Luke Zettlemoyer. TriviaQA: A large scale distantly supervised challenge dataset for reading comprehension. In Regina Barzilay and Min-Yen Kan, editors, *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 1601–1611, Vancouver, Canada, July 2017. Association for Computational Linguistics. doi: 10.18653/v1/P17-1147. URL <https://aclanthology.org/P17-1147>.
- [61] Kenton Lee, Ming-Wei Chang, and Kristina Toutanova. Latent retrieval for weakly supervised open domain question answering. In Anna Korhonen, David Traum, and Lluís Màrquez, editors, *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 6086–6096, Florence, Italy, July 2019. Association for Computational Linguistics. doi: 10.18653/v1/P19-1612. URL <https://aclanthology.org/P19-1612>.
- [62] Jacob Austin, Augustus Odena, Maxwell Nye, Maarten Bosma, Henryk Michalewski, David Dohan, Ellen Jiang, Carrie Cai, Michael Terry, Quoc Le, et al. Program synthesis with large language models. *arXiv preprint arXiv:2108.07732*, 2021.
- [63] Mark Chen, Jerry Tworek, Heewoo Jun, Qiming Yuan, Henrique Ponde de Oliveira Pinto, Jared Kaplan, Harri Edwards, Yuri Burda, Nicholas Joseph, Greg Brockman, et al. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*, 2021.
- [64] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, et al. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288*, 2023.
- [65] Baptiste Rozière, Jonas Gehring, Fabian Gloeckle, Sten Sootla, Itai Gat, Xiaoqing Ellen Tan, Yossi Adi, Jingyu Liu, Tal Remez, Jérémy Rapin, et al. Code llama: Open foundation models for code. *arXiv preprint arXiv:2308.12950*, 2023.
- [66] Holger Rauhut. Compressive sensing and structured random matrices. *Theoretical foundations and numerical methods for sparse recovery*, 9(1):92, 2010.
- [67] Garrett Glasgow. Stratified sampling types. In Kimberly Kempf-Leonard, editor, *Encyclopedia of Social Measurement*, pages 683–688. Elsevier, New York, 2005. ISBN 978-0-12-369398-3. doi: <https://doi.org/10.1016/B0-12-369398-5/00066-9>.
- [68] Akram Erraqabi, Alessandro Lazaric, Michal Valko, Emma Brunskill, and Yun-En Liu. Trading off rewards and errors in multi-armed bandits. In *Artificial Intelligence and Statistics*, pages 709–717. PMLR, 2017.
- [69] Tavor Z Baharav, Gary Cheng, Mert Pilanci, and David Tse. Approximate function evaluation via multi-armed bandits. In *International Conference on Artificial Intelligence and Statistics*, pages 108–135. PMLR, 2022.
- [70] Yoshua Bengio, Grégoire Mesnil, Yann Dauphin, and Salah Rifai. Better mixing via deep representations. In *International conference on machine learning*, pages 552–560. PMLR, 2013.
- [71] Reuben Feinman, Ryan R Curtin, Saurabh Shintre, and Andrew B Gardner. Detecting adversarial samples from artifacts. *arXiv preprint arXiv:1703.00410*, 2017.
- [72] Jinhan Kim, Robert Feldt, and Shin Yoo. Guiding deep learning system testing using surprise adequacy. In *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)*, pages 1039–1049. IEEE, 2019.
- [73] Zhijie Wang, Yuheng Huang, Lei Ma, Haruki Yokoyama, Susumu Tokumoto, and Kazuki Munakata. An exploratory study of ai system risk assessment from the lens of data distribution and uncertainty. *arXiv preprint arXiv:2212.06828*, 2022.
- [74] Leo Gao, Jonathan Tow, Baber Abbasi, Stella Biderman, Sid Black, Anthony DiPofi, Charles Foster, Laurence Golding, Jeffrey Hsu, Alain Le Noac’h, Haonan Li, Kyle McDonell, Niklas Muennighoff, Chris Ociepa, Jason Phang, Laria Reynolds, Hailey Schoelkopf, Aviya Skowron, Lintang Sutawika, Eric Tang, Anish Thite, Ben Wang, Kevin Wang, and Andy Zou. A framework for few-shot language model evaluation, 12 2023. URL <https://zenodo.org/records/10256836>.

A Appendix

A.1 Algorithm Details

A.1.1 Vector Representation Extraction

When selecting a target layer as a feature layer for various downstream tasks, studies on classification models typically favor selecting the last hidden layer, assuming it has the most pertinent information regarding their decisions [9, 70, 71, 72, 73]. However, recent research on LLMs indicates that the optimal layer for feature extraction varies depending on the task, with intermediate layers often demonstrating superior performance in various downstream application [41, 46, 50, 42].

Among related studies, Patchscopes [49] demonstrates an interesting way to inspect the usefulness of each layer through patching. Given a prompt, it patches one layer of hidden states to another round of inference conditioned on a different prompt and observes the resulting answers. Under their experiments, the intermediate layer still achieves relatively the best performance. This might be because the intermediate layers are responsible for decision-making while the later layer focuses more on token prediction. Motivated by this study, we once wondered whether it is possible to detect a feature layer that is suitable in our cases automatically. As a result, we designed an algorithm shown in Algo 2. Generally speaking, we patch a layer given the query prompt and take it into a new inference round conditioned on the empty prompt. We then measure the KL divergence on the output distributions of both cases. Intuitively, the last layer will yield the smallest KL divergence since it preserves all the information for the next-token prediction. However, the layer-KL divergence diagram also presents us with a trade-off similar to the cluster num-inertia diagram, and the elbow point might be an important turning point containing information on the models’ high-level decision-making. So, we also conducted experiments based on this strategy.

The results for the middle, last, and automated-detected layers (Auto Layer) are shown in the table 3.

Algorithm 2 Search for Approximated Optimal Feature Layer

Require: LLM M , Test input prompt set P , Search layer set SL

Ensure: Target layer at the elbow point

```

1: for  $sl \in SL$  do
2:    $plist_{sl} \leftarrow \emptyset$  ▷ Data structure to store KL-divergence of each prompt at each layer
3: end for
4: for  $p \in P$  do
5:    $inter_p, logit_p = \text{RUN}(M, p)$  ▷ Perform clean run on  $M$  with  $p$  and obtain the intermediate states and final logit distribution
6:    $p^* \leftarrow \text{CONCAT}(p[0], p[-1])$ 
7:   for  $sl \in SL$  do
8:      $inter_{p^*}^{sl}, logit_{p^*}^{sl} = \text{RUN}(M, p^*)$  ▷ Perform patching for each target layer in the set
9:      $diff^{sl} \leftarrow \text{KL\_divergence}(logit_{p^*}^{sl}, logit_p)$ 
10:     $plist_{sl} \leftarrow plist_{sl} \cup diff^{sl}$ 
11:   end for
12: end for
13: for  $sl \in SL$  do
14:    $pmed_{sl} \leftarrow \text{MEDIAN}(plist_{sl})$  ▷ Compute median of the KL-divergence of each layer
15: end for
16:  $elb_l = \text{FIND\_ELBOW}(pmed)$  ▷ Find the elbow point
17: return  $elb_l$ 

```

Table 3: Ablation study on target layer selection with performance on different datasets and relative performance difference.

	AGIEval	TriviaQA	NQ-open	GSM8K	TruthfulQA-I	TruthfulQA-T	MBPP	HumanEval
Middle Layer	0.0099	0.0028	0.01661	0.0262	0.0031	0.0172	0.0232	0.0361
Last Layer	0.0112 -11.6 %	0.0028 -1.81 %	0.01961 -15.28 %	0.02333 +12.39 %	0.0032 -3.52 %	0.0183 -5.88 %	0.0241 -3.73 %	0.0697 -48.24 %
Auto Layer	0.0115 -13.73%	0.0034 -17.71%	0.0168 -1.34%	0.0247 + 6.18%	0.0033 -7.39%	0.0170 + 1.36%	0.0245 -5.18%	0.0521 -30.66%

As a result, the middle layer is still the most straightforward layer to choose as the target feature layer. Nonetheless, we believe it is worth trying more complicated algorithms in future work.

Finally, for the PCA algorithm applied in the feature pre-processing stage, we reduced the vector dimension from 4096 to 64. Our preliminary study shows that 64 is large enough, and a larger value (e.g., 128) can actually slightly hurt the performance.

A.1.2 Automated Search for Cluster Number

Cluster Algorithm

For the cluster search in the second phase of our framework, we leverage Balanced K-means, which is an extended version of naive K-means that formulate the clustering problem as:

$$\max_{a_1, \dots, a_D} \sum_{d=1}^D -\text{dist}(\vec{h}_{a_d}, \vec{x}_d) \text{ s.t. } \forall k, \sum_{d=1}^D \mathbb{1}_{a_d=k} = \frac{D}{K} \quad (3)$$

where $a_d \in \{0, \dots, K\}$ is the cluster assignment index for each data point, D is the number of test points, dist is the distance function, \vec{h}_{a_d} is the cluster centers, \vec{x}_d is the hidden vector of d -th data point, $\mathbb{1}$ is the indicator function.

Following [53], we use Balanced K-means for cluster center estimation and greedy inference when predicting clusters.

Search Algorithm

As we discussed in the main text, finding the appropriate cluster number for analysis is important. We perform a n search to identify the cluster number, and each search includes one Balanced-K-means model fitting. This search is guided by *inertia*, as defined in Eq. 4:

$$\text{inertia} = \sum_{d \in \{0, \dots, D\}} \min_{a_d \in \{0, \dots, K\}} \|\vec{x}_d - \vec{h}_{a_d}\|^2 \quad (4)$$

In Eq. 4, D is the number of clusters, \vec{x}_d is the vector representation of each data point, \vec{h}_{a_d} is the cluster center.

Our search goal is to identify the elbow point as a cutoff point on the cluster number-inertia curve. Mathematically, given a function f , the curvature of f at point x is:

$$K_f(x) = \frac{f''(x)}{(1 + f'(x)^2)^{1.5}} \quad (5)$$

where $f''(x)$ is the second derivative and $f'(x)$ is the first derivative. The elbow point is the point of maximum negative curvature of the curve. In this work, we utilized Kneedle algorithm [55] to find this point.

To improve the search efficiency of the elbow point, our study further leverages *adaptive* sampling, as proposed by Tinkerer *et al.* [56]. This method intensifies sampling frequencies in regions where the inertia function changes rapidly. This is achieved by iteratively dividing a given interval in the direction that can maximize the loss function:

$$L_{lb,ub} = \sqrt{(ub - lb)^2 + (f(ub) - f(lb))^2} \quad (6)$$

where lb and ub are the lower bound and upper bound of the interval, $f(x)$ is the inertia value at the point x .

In summary, our cluster number search algorithm is summarized in Algo. 3.

A.1.3 Adaptive Active Sampling Based on Partition

Inter-cluster

Algorithm 3 Search for Target Cluster Number

Require: LLM M , Test input prompt set P , Target feature layer l^* , Search budget w , Search lower bound lb , Search upper bound ub
Ensure: Target cluster number at the elbow point

```
1:  $SP \leftarrow \text{SPLIT}(lb, ub, w^i)$   $\triangleright$  Split search interval into  $w^i$  equally spaced points
2:  $ilist \leftarrow \emptyset$   $\triangleright$  Data structure for recording search history
3: for  $i = 0$  to  $w$  do
4:    $cn \leftarrow \text{ADP\_SAMPLE}(ilist)$   $\triangleright$  Perform adaptive sampling given the past record
5:    $S_i \leftarrow \text{CLUSTER}(M, P, l^*, cn)$   $\triangleright$  Perform Balanced-Kmeans given the cluster number  $cn$ 
6:    $ine_i \leftarrow \text{GET\_INERTIA}(S_i)$   $\triangleright$  Compute inertial according to Eq. 4
7:    $ilist \leftarrow ilist \cup (cn, ine_i)$ 
8: end for
9:  $elb \leftarrow \text{FIND\_ELBOW}(ilist)$   $\triangleright$  Perform Elbow-point detection based on search history
10: return  $elb$ 
```

679 One additional detail is that in the formal proof part of the MC-UCB algorithm, the authors assume
680 the sample size N satisfies the condition of $N \leq 4K$, where K is the cluster number. As a result, we
681 set the search upper bound based on this condition in Algo 3.

682 Intra-cluster

683 Our intra-cluster sampling is guided by the confidence level of LLMs. One important detail is
684 how to aggregate the confidence scores of generated tokens. For natural language-based question-
685 answering tasks (*e.g.*, TrivialQA, NQ-open, TruthfulQA), we leverage geometric mean since it
686 better characterizes the probability-driven generation chain of LLMs. For classification tasks (*e.g.*,
687 AGIEval), we directly utilize the first symbol confidence score. For tasks involving math symbols
688 and code blocks (*e.g.*, GSM8K, MBPP, HumanEval), previous studies show that simply aggregating
689 through all tokens might lead to sub-optimal performance for uncertainty estimation [15]. As such,
690 we also directly take the confidence of the first non-empty token (*e.g.*, ignoring space). Although it is
691 worth designing a more sophisticated aggregation method, we think it is beyond the scope of this
692 paper, and we want to avoid over-feature engineering.

693 For distribution distance measurement, we use the Wasserstein metric to measure confidence estimated
694 through geometric mean. For the single-token estimation method, we use two-sample Kolmogorov-
695 Smirnov statistics because it is less sensitive to outliers and, thus, more robust for the single-token
696 scenario.

697 We unified the above setting when conducting experiments on all confidence-based methods.

698 A.2 Experiment Settings

699 Dataset Description

700 The size of each dataset is shown in Table 4. We perform our experiments using evaluation framework
701 *Language Model Evaluation Harness* [74] for all NLP tasks and implement code generation evaluation
702 with a similar result format to achieve unified I/O for further sampling and analysis.

Table 4: Number of data points for each dataset in our evaluation.

AGIEval	TriviaQA	NQ-open	GSM8K	TruthfulQA	MBPP	HumanEval
3852	17944	3610	1319	817	500	164

703 We also report LLMs’ performance on evaluated datasets in table 5, which include experiments of
704 Llama 2-7B on AGIEval, TriviaQA, NQ-open, GSM8K, TruthfulQA-I, TruthfulQA-T, and Code
705 Llama-7B-Python on HumanEval and MBPP. For the evaluation metrics, we use *exact match* for
706 TriviaQA, NQ-open, GSM8K, *accuracy* for AGIEval, probabilities of different fine-tuning models on
707 TruthfulQA, and *pass@1* on MBPP and HumanEval.

Table 5: LLM performance on all evaluated datasets

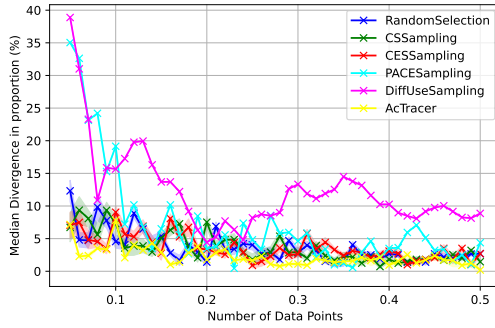
Dataset	AGIEval	TrivialQA	NQ-OPEN	GSM8K	TruthfulQA-I	TruthfulQA-T	MBPP	HumanEval
Mean	0.2313	0.6414	0.1889	0.144	0.8066	0.339	0.406	0.3598
std	0.4217	0.4796	0.3914	0.3511	0.1523	0.3076	0.4911	0.4799

Hardware Specification

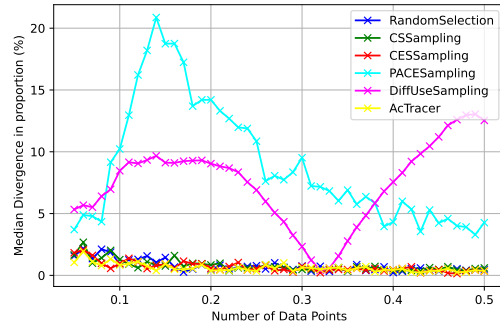
To conduct our large-scale experiments, we utilize a server with AMD 3955WX CPU (3.9GHz), 256GB RAM, and four NVIDIA A4000 GPUs (16GB VRAM of each). The experiments shown in the main text take at least 8,050 CPU Hours and 400 GPU Hours.

A.3 Supplementary Experiment Results

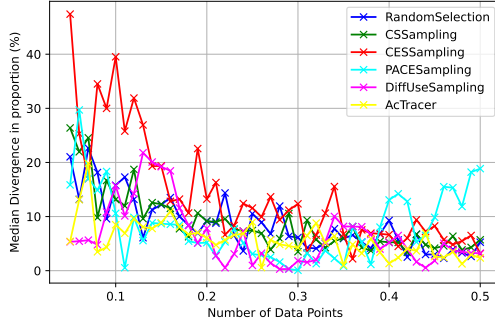
We show all the estimation error curves in Table 1 in the following:



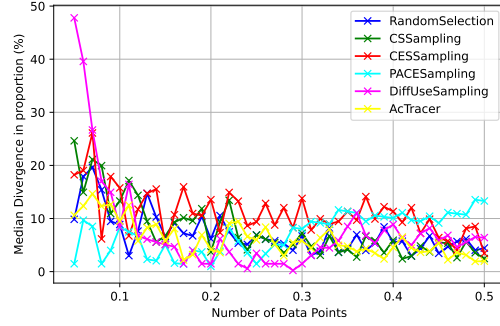
Active testing evaluation result on AGIEval



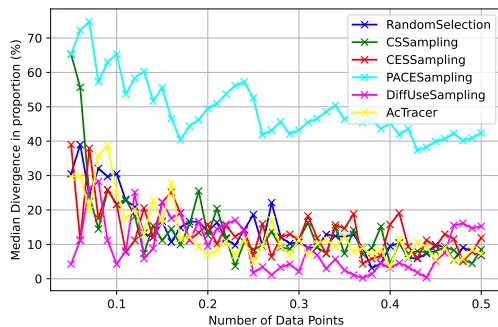
Active testing evaluation result on TriviaQA



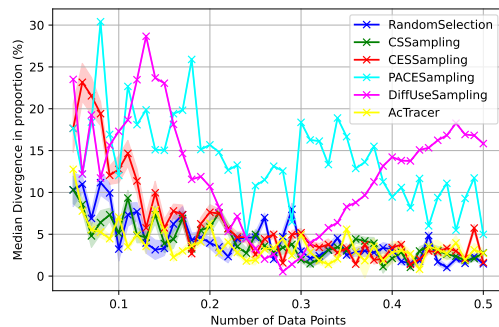
Active testing evaluation result on GSM8K



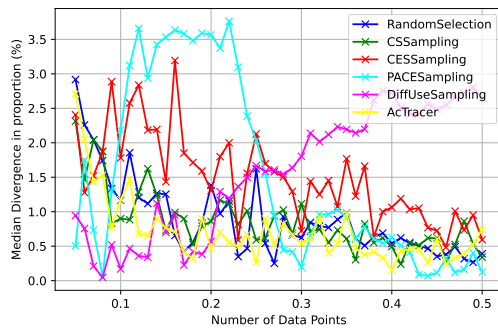
Active testing evaluation result on MBPP



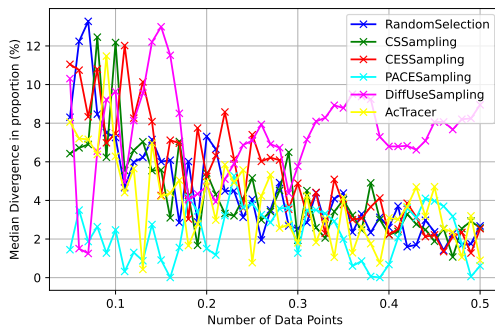
Active testing evaluation result on HumanEval



Active testing evaluation result on NQ-open



Active testing evaluation result on TruthfulQA-I



Active testing evaluation result on TruthfulQA-T

NeurIPS Paper Checklist

1. Claims

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

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

Justification: [The claim made in the abstract is directly backed up by experiment results.](#)

Guidelines:

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

2. Limitations

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

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

Justification: [The paper describes Limitations and Future Directions as a sub-section.](#)

Guidelines:

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

3. Theory Assumptions and Proofs

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

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

Justification: [We do not present theoretical results in this paper.](#)

Guidelines:

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

4. Experimental Result Reproducibility

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

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

Justification: [The paper gives open-source code with additional details for reproduction in the Appendix.](#)

Guidelines:

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

5. Open access to data and code

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

Answer: [Yes]

Justification: [The paper provides link to its open-source code](#)

Guidelines:

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

6. Experimental Setting/Details

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

Answer: [Yes]

Justification: [Details are shown in Appendix](#)

Guidelines:

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

7. Experiment Statistical Significance

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

Answer: [Yes]

Justification: [The paper performed repeated experiments and reported the median to alleviate randomness issues.](#)

Guidelines:

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

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

8. Experiments Compute Resources

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

Answer: [Yes]

Justification: [The information is provided in the Appendix.](#)

Guidelines:

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

9. Code Of Ethics

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

Answer: [Yes]

Justification: [Yes](#)

Guidelines:

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

10. Broader Impacts

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

Answer: [NA]

Justification: [No societal impact is performed within the scope of this work.](#)

Guidelines:

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

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

11. Safeguards

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

Answer: [NA]

Justification: [No corresponding risks in this work.](#)

Guidelines:

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

12. Licenses for existing assets

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

Answer: [Yes]

Justification: [The model and data used in the paper are cited.](#)

Guidelines:

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

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

13. New Assets

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

Answer: [NA]

Justification: [No new assets are introduced in this paper.](#)

Guidelines:

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

14. Crowdsourcing and Research with Human Subjects

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

Answer: [NA]

Justification: [No crowdsourcing or human subjects are involved in this work.](#)

Guidelines:

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

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

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

Answer: [NA]

Justification: [No crowdsourcing or human subjects are involved in this work.](#)

Guidelines:

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