

---

# ML-Agent: Reinforcing LLM Agents for Autonomous Machine Learning Engineering

---

Zexi Liu<sup>1,2\*</sup> Jingyi Chai<sup>1,2\*</sup> Xinyu Zhu<sup>1</sup> Shuo Tang<sup>1</sup> Rui Ye<sup>1</sup>  
 Bo Zhang<sup>2</sup> Lei Bai<sup>2†</sup> Siheng Chen<sup>1†</sup>

<sup>1</sup> Shanghai Jiao Tong University <sup>2</sup> Shanghai AI Laboratory

\* Equal Contribution † Corresponding Author

ML-Agent: <https://github.com/zeroxleo/ML-Agent>

## Abstract

The emergence of large language model (LLM)-based agents has significantly advanced the development of autonomous machine learning (ML) engineering. However, most existing approaches rely heavily on manual prompt engineering, failing to adapt and optimize based on diverse experimental experiences. Focusing on this, for the first time, we explore the paradigm of learning-based agentic ML, where an LLM agent learns through interactive experimentation on ML tasks using online reinforcement learning (RL). To realize this, we propose a novel agentic ML training framework with three key components: (1) exploration-enriched fine-tuning, which enables LLM agents to generate diverse actions for enhanced RL exploration; (2) step-wise RL, which enables training on a single action step, accelerating experience collection and improving training efficiency; (3) an agentic ML-specific reward module, which unifies varied ML feedback signals into consistent rewards for RL optimization. Leveraging this framework, we train ML-Agent, driven by a 7B-sized Qwen-2.5 LLM for autonomous ML. Remarkably, despite being trained on merely 9 ML tasks, our 7B-sized ML-Agent outperforms the 671B-sized DeepSeek-R1 agent. Furthermore, it achieves continuous performance improvements and demonstrates exceptional cross-task generalization capabilities.

## 1 Introduction

Machine Learning (ML) engineering is a critical yet labor-intensive process, requiring expert researchers to invest significant time—potentially days or even months—designing architectures, tuning parameters, and iteratively refining models through trial and error [1]. This challenge has sparked an ambitious vision of autonomous ML: building autonomous AI systems that independently orchestrate the entire ML lifecycle, from conceptual design and code implementation to refinement.

Fortunately, the advent of LLM-based agents, equipped with capabilities of interaction [2, 3], coding [4, 5, 6, 7] and tool-calling [8], has propelled us significantly closer to realizing this vision (Agentic ML) [9, 10]. Unlike traditional automated ML with pre-defined limited search and action spaces [11, 12, 13, 14, 15], these LLM agents, when provided with instructions in natural language, can autonomously propose effective actions, generate executable codes, and iteratively improve solutions based on environmental feedback [9, 16]. For example, AIDE [16] and SELA [17] both leverage LLM agents together with experimental environments to automate ML process.

Despite their significant potential, a common and fundamental limitation of current methods is that they are all heuristically designed through prompt engineering (prompt-based agentic ML), which prevents the automatic and flexible optimization of LLM agents. This human-involved design paradigm restricts the agent’s ability to learn across different task-solving trajectories, as prompts are

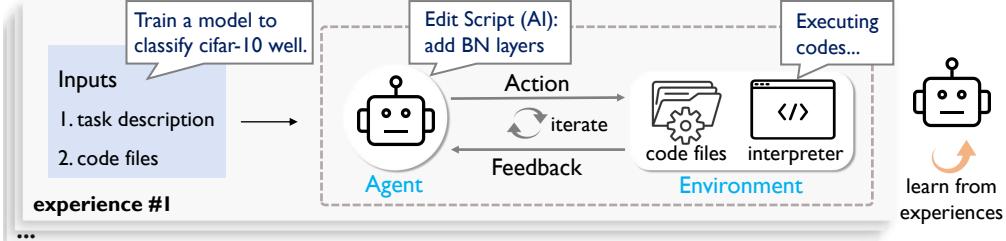


Figure 1: Overview of LLM agent interaction with environment for autonomous machine learning. The environment contains editable code files and an interpreter to execute code. In each experience, the agent takes actions (e.g., add BN layers), and the environment returns feedback (e.g., execution results). Our proposed ML-Agent learn from previous experiences and improves itself by training.

tailored to individual outcomes rather than enabling the agent to generalize from diverse experiences. Additionally, researchers are required to wait several hours to observe execution results before refining the prompts, leading to time inefficiencies and a lack of scalability.

Addressing this key limitation, this paper for the first time explores the paradigm of learning-based agentic ML, where the LLM agents can learn from task-solving trajectories in ML tasks using online reinforcement learning (RL). This allows agents to actively explore different strategies, accumulate knowledge across runs, steadily refine their decisions, continuously learn from their own experiences and improve their autonomous ML performance through training [18].

While being straightforward, employing online RL to train autonomous ML agents poses three key challenges. (1) *Limited exploration*: agents often propose similar actions for the same ML task across runs, leading to narrow exploration trajectories in RL [19]. (2) *Slow experience collection*: ML experiments can take minutes to hours, making online RL data gathering inefficient and thus limiting feedback-driven training samples [10]. (3) *Complex reward design*: agentic ML involves various outcomes, such as task-specific metrics, out-of-memory failures, and compilation errors. This requires a unified reward function to reconcile varied feedback signals [20].

In response to these challenges, we propose a novel agentic ML training framework, the first designed to train LLM agents for autonomous ML engineering using online RL. This framework enables agents to explore diverse ML trajectories, collect rewards efficiently, and iteratively enhance their capabilities through learned experience. (1) To improve exploration diversity, we introduce *exploration-enriched fine-tuning*, generating a diverse action pool from fast-executable ML tasks to finetune agents for broader RL exploration. (2) To accelerate experience collection, we design a *step-wise RL paradigm*, evaluating atomic actions using expert trajectories as single-step queries, significantly boosting training efficiency. (3) To tackle reward design, we develop an *agentic ML-specific reward module* that dynamically handles errors (e.g., runtime failures) and quantifies performance via normalized, task-specific metrics (e.g., accuracy gains).

By leveraging our proposed agentic ML training framework, we train ML-Agent, an agent driven by 7B-sized Qwen2.5 LLM for autonomous ML. During training, our ML-Agent can efficiently explore the environment, learn from experience, and achieve continuous performance improvement through iterative exploration across various ML tasks. Surprisingly, despite trained on only 9 ML tasks, our 7B-sized ML-Agent not only surpasses the 671B-sized DeepSeek-R1 agent, but also exhibits unprecedented cross-task generalization capabilities. Specifically, it surpasses state-of-the-art agents on 3 held-in and 10 held-out ML tasks, covering diverse data modalities and training objectives.

In summary, our work makes the following significant contributions to the field:

- We introduce a new paradigm for autonomous ML: learning-based agentic ML, where an LLM agent learns through interactive experimentation on ML tasks via online reinforcement learning.
- We propose a novel training framework for agentic ML, which incorporates three technical designs: exploration-enriched fine-tuning, step-wise RL, and agentic ML-specific rewards.
- Extensive experiments show that despite training on only 9 ML tasks, our 7B-sized ML-Agent surpasses state-of-the-art agents (e.g., those powered by 671B-sized DeepSeek-R1).

## 2 Related Work

**Autonomous Machine Learning.** Autonomous machine learning aims to automate the manual and expertise-intensive aspects of machine learning, including data preprocessing, model selection and hyperparameter tuning. Autonomous machine learning has evolved from classical hyperparameter and pipeline search to agentic frameworks powered by large language models. Classical autonomous machine learning frameworks focus on automating model selection, hyperparameter optimization, and pipeline construction within a fixed search space [11, 21, 22, 23, 24, 25]. For example, AutoGluon-Tabular [24] ensembles multiple models and stackings to deliver state-of-the-art performance on tabular data with minimal user effort. These classical autonomous machine learning works remain constrained by predefined search spaces and static configurations, lacking the adaptability and continuous learning capabilities.

**LLM Agents in Autonomous Machine Learning.** Recent advancements in large language models (LLMs) have empowered them to autonomously generate and refine machine learning solutions, opening new possibilities in machine learning. Methods such as AutoML-GPT [26] and MLCopilot [27] prompt LLMs to automate the entire machine learning pipeline, where MLCopilot introduces past experience retrieval to help decision-making. AIDE [16] and SELA [17] focus on optimizing the ML engineering process through iterative search and refinement strategies. AIDE formats ML task as a code optimization problem, employing trial-and-error strategies to explore potential solutions. Other works like AutoKaggle [28] employ a multi-agent framework to address Kaggle competitions. Although LLMs in these works autonomously generate actions and refine their own with potential past experience, they do not train on their past experience. As a result, their strategies remain static across different tasks, heavily rely on prompts, without the capacity for improvement over time.

**Reinforcement Learning for LLMs.** Reinforcement learning (RL) significantly enhances the ability of large language models, particularly in preference alignment and complex reasoning [29, 30, 31]. By facilitating exploration and exploitation, RL trains LLMs to adapt and improve their policy based on feedback, thus refining their performance in dynamic environments. One line of work is preference optimization [32], with methods such as Reinforcement Learning from Human Feedback (RLHF)[33]. RL is also utilized to train LLMs for complex reasoning tasks [34, 35]. Another line of research involves training LLM agents for specific tasks using RL. For example, IPR [18] and AgentQ [36] use DPO [37] to iteratively refine their policy. While StarPO [38] discusses the multi-turn reinforcement learning considering episode-wise reward. However, applying RL to train LLM agents for autonomous machine learning remains unexplored.

## 3 Problem Setup and Preliminaries

**Problem Formulation.** Agentic ML leverages an LLM agent to autonomously orchestrate the machine learning lifecycle by interacting iteratively with the experimental environment. This environment consists of a workspace of editable task-related code files together with an interpreter executing code. A key feature of the ML-related environment provides explicit experimental feedback, such as code execution results or error messages. At each time step, the agent takes actions (e.g., add BN layers in the model architecture) and receives feedback (e.g., code execution output or error messages) from the environment. The interaction loops until it reaches a maximum number of steps or time limit. We follow the action space defined in prior literature [9] (see Table 4).

**Agentic ML as a MDP.** We format agentic ML as a Markov Decision Process (MDP)  $\mathcal{M} = (\mathcal{S}, \mathcal{A}, \mathcal{P})$ , where  $\mathcal{S}$  is the state space,  $\mathcal{A}$  the action space and  $\mathcal{P}$  the state transition dynamics. Let the environment feedback at time  $t$  be  $f_t \in \mathcal{F}$ , where  $\mathcal{F}$  denotes the feedback space. We define  $s_t = (f_1, f_2, \dots, f_{t-1})$  as a history-based state representation to capture richer contextual information from past feedback. The agent policy  $\pi_\theta$  generates an action  $a_t \in \mathcal{A}$  conditioned on current state  $s_t$ , forming a trajectory of interactions  $\tau = (s_0, a_0, s_1, \dots, a_{n-1}, s_n)$ . Note that  $\theta$  is the LLM’s parameters within the agent and  $n$  is trajectory length. The goal is to maximize the expected trajectory reward:

$$\mathcal{J}(\theta) = \mathbb{E}_{\tau \sim \pi_\theta} [R(\tau)], \quad (1)$$

where the reward function  $R(\tau)$  denotes the cumulative reward over the entire trajectory.

**Challenges.** Although the formulation of agentic ML is relatively straightforward, employing online RL to train LLM agents for autonomous machine learning poses several key challenges, including: **(1) Limited exploration.** Agents often repeat similar actions across episodes, narrowing their exploration

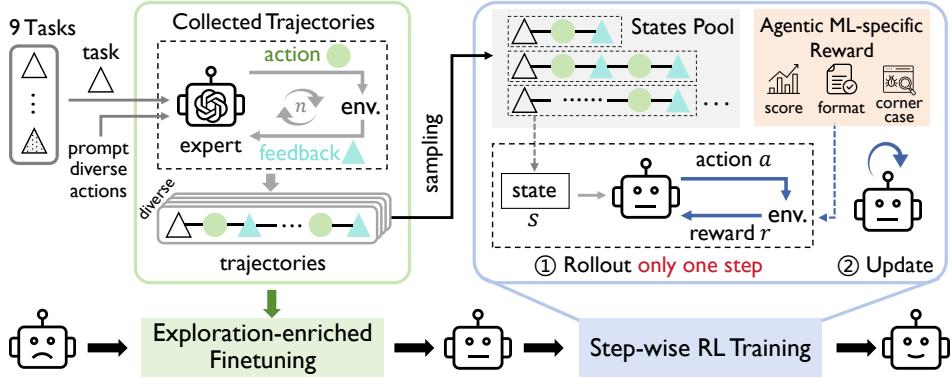


Figure 2: Overview of the agentic ML training framework, introducing (1) exploration-enriched fine-tuning for diverse action pool creation, (2) a step-wise RL paradigm for efficient experience collection using expert trajectories, and (3) an agentic ML-specific reward module for various ML feedback handling and task-specific performance evaluation.

and limiting their ability to discover innovative ML solutions. **(2) Slow experience collection.** ML experiments can take minutes to hours, slowing down the online data collection process for RL training. **(3) Complex reward design.** Agentic ML produces varied outcomes (e.g., execution results or resource errors), making it challenging to design a unified reward function that effectively guides the agent. The subsequent section presents our agentic ML training framework designed to overcome these challenges, with the overall architecture illustrated in Figure 2.

## 4 Agentic ML Training Framework

Our agentic ML training framework is designed to train LLM agents for autonomous machine learning. As shown in Figure 2, it comprises three key steps for efficient learning. First, *exploration-enriched fine-tuning* builds a diverse action pool to enhance RL exploration. Second, a *step-wise RL paradigm* uses expert trajectories as single-step queries to accelerate experience collection in RL. Third, an *agentic ML-specific reward module* handles errors and quantifies agentic ML task-specific performance. These steps sequentially enable diverse exploration, efficient training, and unified feedback, enabling agents to iteratively improve agentic ML performance across varied ML tasks.

### 4.1 Exploration-enriched fine-tuning

In agentic ML, limited exploration hinders autonomous machine learning workflows. Agents often repeat similar actions (e.g., small code edits) across episodes, leading to narrow exploration and preventing the discovery of innovative architectures or optimization strategies.

To address this, we introduce exploration-enriched fine-tuning, which enhances the diversity of agent actions through carefully curated prompts. To implement this, we utilize a set of  $N$  fast-executable ML tasks. For each task, we first generate at least 100 candidate ideas (e.g., “add L1 or L2 weight regularization”, see Table 8 for more examples) and compute their pairwise embedding distances. We select the 10 most diverse ideas with the largest embedding distance to others and randomly sample 1–3 to include in the task prompt. A GPT-4o-mini powered expert agent interacts with the environment using sampled enriched prompts across 9 fast-executable ML tasks. This process generates a dataset of expert trajectories, denoted as  $\mathcal{D} = \{\tau^{(i)}\}_{i=1}^{|\mathcal{D}|}$ , where  $|\mathcal{D}|$  is the number of expert trajectories. This process leverages fast-executable ML tasks to ensure rapid trajectory generation, mitigating the computational burden of ML experiments.

We use these expert trajectories to fine-tune the LLM agent’s policy  $\pi_\theta$ , via supervised fine-tuning (SFT) with the loss function:

$$\mathcal{L}_{\text{SFT}}(\theta) = -\mathbb{E}_{\tau \sim \mathcal{D}} [\log P_{\pi_\theta}(\tau | s_0)] = -\mathbb{E}_{\tau \sim \mathcal{D}} \left[ \log \prod_{t=0}^{n-1} \pi_\theta(a_t | s_t) \right] = -\mathbb{E}_{\tau \sim \mathcal{D}} \left[ \sum_{t=0}^{n-1} \log \pi_\theta(a_t | s_t) \right]. \quad (2)$$

This exploration-enriched fine-tuning approach ensures agents output format-compliant actions critical for agentic ML workflows while learning diverse strategies, significantly broadening the exploration scope in subsequent RL phases.

## 4.2 Step-wise RL paradigm

**Objective.** Due to the time-consuming nature of AI experiments, directly applying reinforcement learning methods (e.g., PPO) is impractical, as sampling a single trajectory during rollout takes hours. To address this issue, we propose a step-wise reinforcement learning approach that reformulates the objective function (1), where we sample only a single step of action during the rollout phase instead of the entire trajectory. This approach extensively reduces the computational cost of the rollout phase and makes the overall training process more efficient. Specifically, we expand (1) into steps according to the state distribution  $d^{\pi_\theta}(s)$ :

$$\mathcal{J}(\theta) = \sum_{t=0}^{n-1} \sum_{s_t \in \mathcal{S}} d^{\pi_\theta}(s_t) \left[ \sum_{a_t \in \mathcal{A}} \pi_\theta(a_t | s_t) R(s_t, a_t) \right], \quad (3)$$

where  $R(s_t, a_t)$  stands for the reward function at each time step  $t$ . The state distribution  $d^{\pi_\theta}(\cdot)$  can be calculated recursively based on the policy  $\pi_\theta$  and the state transition dynamics  $\mathcal{P}$ ; see Appendix A for details. The time-consuming components in Equation (3) include: 1)  $d^{\pi_\theta}(s_t)$ , which involves multiple state transition dynamics from  $s_t$  to  $s_{t+1}$ , and 2)  $R(s_t, a_t)$ , where the reward is determined based on feedback from the environment (e.g., code execution platform). Since  $d^{\pi_\theta}(\cdot)$  relies on  $\pi_\theta$ , the trajectory sampling process operates repeatedly in standard RL training, making the computational cost even higher. However, using  $d^{\pi_\theta}$  to sample state distribution is not necessary for two reasons: 1)  $\pi_\theta$  poorly aligns with the environment format during the early stage of RL training, hindering effective state exploration; 2) Once  $\pi_\theta$  can interact properly with the environment, the set of states it could explore tends to vary only slightly as  $\pi_\theta$  updates. Hence, we sample the states from a states pool according to a fixed expert distribution  $d^{\pi_e}(s_t)$ , which forms the step-wise objective function

$$\mathcal{J}_{\text{step}}(\theta) = \sum_{s_t \in \mathcal{S}} d^{\pi_e}(s_t) \left[ \sum_{a_t \in \mathcal{A}} \pi_\theta(a_t | s_t) R(s_t, a_t) \right] = \mathbb{E}_{s_t \sim d^{\pi_e}, a_t \sim \pi_\theta(\cdot | s_t)} [R(s_t, a_t)]. \quad (4)$$

This objective function  $\mathcal{J}_{\text{step}}(\theta)$  reformulates multi-step trajectory reinforcement learning into step-wise training. This reformulation offers two advantages: 1) The state sampling process is decoupled from the reinforcement learning of the model. This allows us to directly sample states from a pre-collected set and avoids expensive online sampling during training, significantly reducing the overall training time. 2) The state sampling process is performed before RL training, rather than during the rollout phase. This enables us to perform extensive sampling from the expert distribution, making training more scalable.

**Training approach.** Based on the step-wise RL formulation, our goal is to maximize the expected reward  $R(s_t, a_t)$  shown in equation (4) according to the state distribution  $d^{\pi_e}$  and  $\pi_\theta$ . This aligns with the approach used in RLVR methods [39], where the policy represents a token generation process and  $R(s_t, a_t)$  is the outcome reward of  $\pi_\theta(a_t | s_t)$ . Hence, any RL training approach can be applied to this objective  $\mathcal{J}_{\text{step}}(\theta)$ . For our implementation, we choose Proximal Policy Optimization (PPO) [40] as the training algorithm because of its widespread use and proven effectiveness. Specifically, suppose we expand the token generating process of  $\pi_\theta(a_t | s_t)$ , our PPO loss function can be defined as follows:

$$\mathcal{J}_{\text{step}}^{\text{PPO}}(\theta) = \mathbb{E}_{s \sim d^e, o \leq i \sim \pi_{\theta_{\text{old}}}(\cdot | s)} \left[ \min \left( \frac{\pi_\theta(o_i | s, o_{<i})}{\pi_{\theta_{\text{old}}}(o_i | s, o_{<i})} \hat{A}_i, \text{clip} \left( \frac{\pi_\theta(o_i | s, o_{<i})}{\pi_{\theta_{\text{old}}}(o_i | s, o_{<i})}, 1 - \varepsilon, 1 + \varepsilon \right) \hat{A}_i \right) \right], \quad (5)$$

where  $o_i$  is the  $i$ th token of  $a_t$  and  $\hat{A}_i$  is an estimator of the advantage at the token generation step  $i$ .

## 4.3 Agentic ML-specific reward

Having enabled efficient reinforcement learning (RL) for agentic ML via the step-wise RL paradigm, the next crucial step is to convert the varied feedback into a unified, meaningful reward. While numerical metrics like validation accuracy or loss naturally serve as RL rewards, non-numerical feedback, such as compilation errors or out-of-memory failures, must be carefully incorporated to ensure the reward function remains coherent.

To address this, we propose an agentic ML-specific reward module that dynamically processes these diverse signals while quantifying performance improvements through scaled task-specific metrics. The key idea is to translate every execution outcome (success, corner case, or error) into a unified scalar value. Here, we define  $\mathcal{A}_{\text{valid}}$  is the set of valid actions, and  $\mathcal{A}_{\text{edit}} \subset \mathcal{A}_{\text{valid}}$  is the subset of actions that edit ML codes.  $\mathcal{F}_{\text{error}}$  denotes feedback indicating errors (e.g., compilation failures),  $\mathcal{F}_{\text{corner}}$  denotes corner cases (e.g., resource exhaustion), and  $\mathcal{F}_{\text{success}}$  denotes successful executions. Let  $m_t$  be the task-specific metric at state  $s_t$  (e.g., loss or accuracy), and define the ML task-specific scaling factor  $\alpha_i = \frac{100}{m_{\text{best}} - m_{\text{init}}}$ ,  $1 \leq i \leq N$ , where  $m_{\text{init}}$  and  $m_{\text{best}}$  denote the baseline and best human-achievable scores. Then the reward  $R(s_t, a_t)$  is:

$$R(s_t, a_t) = \begin{cases} \sigma(-\infty) = 0 & , \text{if } a_t \notin \mathcal{A}_{\text{valid}} \text{ or } f_{t+1} \in \mathcal{F}_{\text{error}} \\ \sigma(0) = 0.5 & , \text{if } a_t \in \mathcal{A}_{\text{valid}} / \mathcal{A}_{\text{edit}} \text{ or } f_{t+1} \in \mathcal{F}_{\text{corner}} \\ \sigma(\alpha_i(m_{t+1} - m_t)) & , \text{if } a_t \in \mathcal{A}_{\text{edit}} \text{ and } f_{t+1} \in \mathcal{F}_{\text{success}}, \end{cases} \quad (6)$$

where  $\sigma(\cdot)$  is the sigmoid function. The reward module handles all possible agentic ML scenarios: (1) Invalid Actions or Error. If the agent takes an invalid action ( $a_t \notin \mathcal{A}_{\text{valid}}$ ) or gets an error feedback ( $f_{t+1} \in \mathcal{F}_{\text{error}}$ , e.g., compilation failure), it receives a reward of 0. This penalizes faulty outputs and enforces correct format. (2) Valid Non-Editing Actions or Corner Cases. For valid but non-editing actions ( $a_t \in \mathcal{A}_{\text{valid}} \setminus \mathcal{A}_{\text{edit}}$ ) (e.g. list files) or for corner cases ( $f_{t+1} \in \mathcal{F}_{\text{corner}}$ , e.g., out-of-memory), the reward is 0.5. This neutral score acknowledges their legitimacy while recognizing external constraints. (3) Success. When the agent applies a valid edit ( $a_t \in \mathcal{A}_{\text{edit}}$ ) and the execution succeeds ( $f_{t+1} \in \mathcal{F}_{\text{success}}$ ), the reward is  $\sigma(\alpha_i(m_{t+1} - m_t))$ , where  $m_t$  and  $m_{t+1}$  are pre- and post-edit performance metrics. The scaling factor  $\alpha_i$  normalizes across diverse ML metrics, and the sigmoid  $\sigma(\cdot)$  maps improvements into  $(0, 1)$ , incentivizing meaningful enhancements.

By unifying penalties for errors, neutrality for non-editing actions, and task-driven rewards for edits, our module provides consistent, informative feedback that drives iterative refinement and continuous improvement across diverse ML tasks.

## 5 Experiments

### 5.1 Experimental setups

**Training.** For training data collection, we adopt a GPT-4o-mini-driven [41] agent scaffolded by MLAB [9]. This agent interacts with the MLAGentBench [9] agentic ML environment to generate expert trajectories. We collect 10k expert trajectories across 9 ML tasks, comprising 4 tasks from MLAGentBench and 5 from MLE-bench [10], with each trajectory limited to 15 steps and 30 minutes of runtime. Additional data collection details are provided in Appendix B. For exploration-enhanced fine-tuning, we train Qwen2.5-7B [42] using these 10k expert trajectories via supervised fine-tuning (SFT). For step-wise RL, we select 10k states sampled from expert trajectories to further train the SFT model using Proximal Policy Optimization (PPO). All training is conducted on 8 A100 GPUs. The fine-tuning stage runs for 2 epochs with a learning rate of  $2e-5$ , while the RL stage runs for 1 epoch with an actor learning rate of  $1e-6$  and a critic learning rate of  $1e-5$ . Additional training hyperparameter details are available in Appendix C.1.

**Testing.** To verify the generalization ability across ML tasks of ML-Agent, we select 10 held-out tasks from MLE-Bench, which are not seen during training and generally more challenging than the training tasks. Details of these tasks are provided in Appendix B.1. During testing, the MLAGentBench environment settings remain consistent with those used in training. To comprehensively assess the LLM agent’s ability in autonomous ML, we propose three metrics: (1) **avg@K**, the mean score across  $K$  evaluation trajectories, reflecting agent stability. (2) **best@K**, the highest score among  $K$  evaluation trajectories, showing the maximum quality with the same compute/step budget. (3) **Relative gain**  $\Delta_r$ , the relative improvement over the initial script, defined as  $\Delta_r = \beta \frac{p_{\text{avg}@8} - p_{\text{init}}}{p_{\text{init}}}$  where  $p_{\text{avg}@8}$  is the mean score over 8 trajectories,  $p_{\text{init}}$  is the initial script’s score, and  $\beta \in \{-1, 1\}$  adjusts for metrics (e.g. MAE, RMSE) to ensure positive  $\Delta_r$  indicates improvement.

**Baselines.** To provide a comprehensive comparison, we compare ML-Agent with five MLAB-scaffolded agents: agents driven by Qwen2.5-7B-Instruct [42] with equivalent parameter scale to ours, Qwen2.5-32B-Instruct[42] with larger-scale, expert-level GPT-4o-mini [41] and GPT-4o [43], and a 671B reasoning model DeepSeek-R1 [39]. As agents scaffolded with AIDE represent the

Table 1: ML-Agent outperforms baselines on 3 held-in tasks (included in training) and 10 held-out tasks (unseen during training). For each task, we report the average and best score over 8 trajectories. The top-performing model is highlighted in **bold**, and the second-best result is underlined.

Task	Data Type	Metric	Level	Qwen-7B-Instruct	Qwen-32B-Instruct	GPT-4o-mini	GPT-4o	DeepSeek-R1	ML-Agent
<b>Held-in Tasks</b>									
cifar-10	Image	Acc. (%) $\uparrow$	Avg	52.19	59.12	53.96	61.70	66.39	<b>68.88</b>
			Best	61.55	76.05	63.82	<u>80.83</u>	80.34	<b>81.45</b>
house-price	Tabular	MAE $\downarrow$	Avg	21626	21134	<u>20671</u>	20850	20929	<b>20209</b>
			Best	21412	20440	<u>19905</u>	20441	20234	<b>18440</b>
feedback	Text	MCRMSE $\downarrow$	Avg	0.6735	0.6273	<u>0.6211</u>	0.6435	0.6452	<b>0.5910</b>
			Best	0.6116	<u>0.5783</u>	0.5940	0.6098	0.5973	<b>0.5777</b>
<b>Held-out Tasks</b>									
denoising-dirty-documents	Image	RMSE $\downarrow$	Avg	0.1523	<u>0.1344</u>	0.1459	0.1471	0.1419	<b>0.0741</b>
			Best	0.0926	0.0829	0.0662	<u>0.0661</u>	0.1326	<b>0.0556</b>
leaf-classification	Image	Logloss $\downarrow$	Avg	0.0780	0.0786	<u>0.0747</u>	0.0785	0.0761	<b>0.0689</b>
			Best	0.0653	<u>0.0473</u>	0.0601	0.0499	0.0540	<b>0.0373</b>
statoil-iceberg-classifier-challenge	Image	Logloss $\downarrow$	Avg	0.3093	0.3052	0.2908	0.3209	<u>0.2908</u>	<b>0.2868</b>
			Best	0.2683	<u>0.2664</u>	0.2719	0.2914	0.2701	<b>0.2617</b>
whale-categorization-playground	Image	MAP@5 $\uparrow$	Avg	0.1304	0.1268	0.1198	0.1417	<u>0.1551</u>	<b>0.2009</b>
			Best	0.2276	0.2019	0.1421	0.2185	<u>0.2456</u>	<b>0.2524</b>
learning-agency-lab-automated-essay-scoring-2	Text	QWK $\uparrow$	Avg	0.7422	<u>0.7464</u>	0.7386	0.7437	0.7336	<b>0.7472</b>
			Best	0.7545	<u>0.7615</u>	0.7441	0.7484	0.7488	<b>0.7693</b>
detecting-insults-in-social-commentary	Text	Acc. (%) $\uparrow$	Avg	80.13	<u>80.89</u>	80.06	80.33	79.92	<b>81.11</b>
			Best	80.75	<u>82.01</u>	80.44	81.70	80.41	<b>82.73</b>
spooky-author-identification	Text	Logloss $\downarrow$	Avg	0.4515	0.4660	<u>0.4443</u>	0.4474	0.4454	<b>0.4415</b>
			Best	0.4285	0.4285	0.4285	0.4422	<u>0.4248</u>	<b>0.4078</b>
jigsaw-toxic-comment-classification-challenge	Text	AUC $\uparrow$	Avg	0.9746	0.9751	0.9744	0.9751	<u>0.9752</u>	<b>0.9753</b>
			Best	0.9752	<u>0.9753</u>	0.9752	0.9752	0.9752	<b>0.9763</b>
us-patent-phrase-to-phrase-matching	Tabular	PCC $\uparrow$	Avg	0.4700	0.4725	0.4695	<u>0.4882</u>	0.4651	<b>0.5117</b>
			Best	0.4859	0.4908	0.4905	<u>0.5599</u>	0.4813	<b>0.5791</b>
tabular-playground-series-dec-2021	Tabular	Acc. (%) $\uparrow$	Avg	95.94	<u>95.97</u>	95.90	95.91	95.78	<b>96.09</b>
			Best	96.06	<u>96.12</u>	96.07	96.10	96.12	<b>96.13</b>

state-of-the-art (SOTA) on MLEbench[10], we further compared ML-Agent with AIDE [16] agents driven by GPT-4o, o1-preview [44] and DeepSeek-R1. We keep the same time limit and number of ML code modifications to ensure a fair comparison between agents with different scaffolds.

## 5.2 Main results

We conduct extensive experiments to evaluate the performance of ML-Agent, a learning-based LLM agent trained through our proposed framework for autonomous ML. Our results demonstrate that ML-Agent achieves strong and consistent performance across both held-in and held-out tasks, and exhibits continuous performance improvements during RL training.

**ML-Agent achieves superior performance across both held-in and held-out tasks.** We compare ML-Agent with 5 powerful LLM-based agents across 3 held-in and 10 held-out tasks. As shown in Table 1, ML-Agent consistently achieves the highest average and best performance across both task types. For example, on the house-price task, ML-Agent reaches a best value of 18440, outperforming GPT-4o-mini’s 19905; on whale., it attains an average score of 0.2009, surpassing all other baselines. Notably, despite being trained on only 9 tasks, ML-Agent delivers top-tier results across all 10 held-out tasks, demonstrating strong generalization and effective learning from limited experience.

**ML-Agent outperforms stat-of-the-art agents.** To further demonstrate the effectiveness of our training framework, we compare ML-Agent with AIDE [16], a tree-search-based LLM agent specifically designed for autonomous ML. We present the normalized relative gain results for each task in Figure 3. Specifically, after calculating the relative gain for each task, we normalize it by dividing the value of our ML-Agent. Results show that ML-Agent outperforms AIDE-scaffolded agents across nearly all tasks while only slightly trailing AIDE-o1 on jigsaw and AIDE-r1 on cifar-10. This underscores the efficacy of our agentic ML training framework across diverse ML tasks.

**ML-Agent achieves continuous performance improvements.** Figure 4 shows that ML-Agent demonstrates consistent performance improvement across both held-in and held-out tasks as training progresses. This highlights the effectiveness of our step-wise RL paradigm and exploration-enriched fine-tuning in enabling continuous learning from ML environmental feedback, ultimately allowing ML-Agent to outperform all baseline methods.

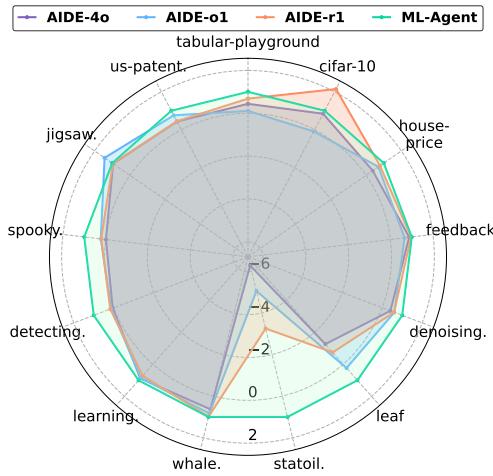


Figure 3: Comparison results with AIDE framework on 13 tasks. We plot the normalized relative gain for each task. Specifically, we normalize the relative gain of each task via dividing by our ML-Agent value.

### 5.3 Analysis

**Exploration-enriched fine-tuning is crucial for step-wise RL training.** To validate the efficacy of exploration-enriched fine-tuning in enhancing subsequent RL training, we replace our exploration-enriched fine-tuned model(ML-Agent-SFT) with Qwen2.5-7B(Qwen-7B-Base), Qwen2.5-7B-Instruct(Qwen-7B-Instruct), and DeepSeek-R1-Distill-Qwen-7B [39](Qwen-7B-Distill) as base models for the RL training. We evaluate the average relative gain of the resulting RL-trained agents on held-in and held-out tasks. As shown in Figure 5, we observe the following: (1) The agent trained from Qwen-7B-Distill fails to follow instructions and generate valid actions in both held-in and held-out tasks. This is likely due to the use of a default output format during distillation, which tends to include a <think> process rather than valid executable actions for autonomous ML. Consequently, during the data collection phase of RL training, the agent also fails to produce format-compliant actions, leading to largely ineffective learning. (2) The agent trained from Qwen-7B-Base exhibits overall performance degradation, which may be attributed to its limited instruction-following capabilities. (3) The agent trained from Qwen-7B-Instruct achieves positive improvements on held-in tasks (+13%), but shows negative performance gains on held-out tasks (-12%). This suggests that while the model’s ability to follow instructions contributes to solving ML tasks, it does not suffice for generalizing to more challenging, unseen ML tasks. (4) In contrast, the agent trained from our ML-Agent-SFT achieves a 18% improvement on held-in tasks and a 16% improvement on held-out tasks. Furthermore, we analyze the action diversity of ML-Agent-SFT during autonomous ML experimentation. The results in Figure 8 show that ML-Agent-SFT generates a broader variety of actions compared to those produced by the Qwen-7B-Instruct-driven agent. Overall, these results validate that exploration-enriched fine-tuning ensures format-compliant actions and fostering diverse actions, significantly enhancing both the exploration scope and generalization capability in step-wise RL training.

**Effectiveness of Step-wise RL Training.** To improve training efficiency and scalability, we propose a step-wise RL approach that samples single states from expert trajectories and evaluates atomic actions.

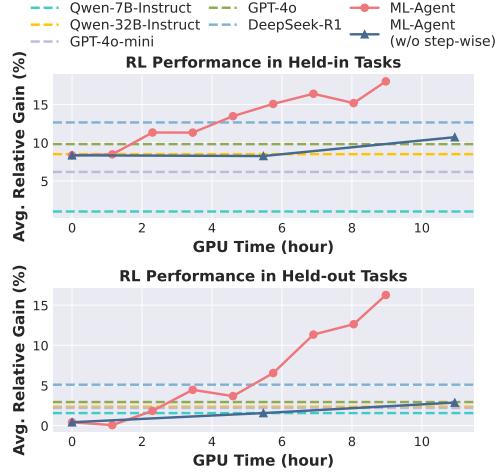


Figure 4: Step-wise RL is more efficient than episode-wise RL on both held-in and held-out tasks. Both RL training methods begin with ML-Agent-SFT. The gap of red points is 5 steps while the gap of blue triangles is 1 step.

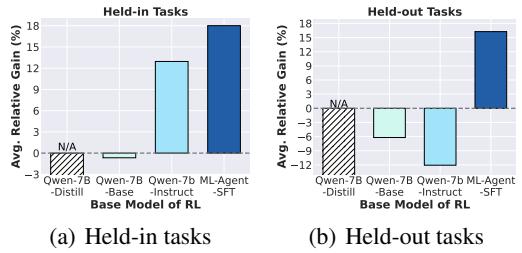


Figure 5: Exploration-enriched fine-tuning is crucial for RL training. "N/A" means the training based on the model fails to generate valid results.

While the model’s ability to follow instructions contributes to solving ML tasks, it does not suffice for generalizing to more challenging, unseen ML tasks. The results in Figure 8 show that ML-Agent-SFT generates a broader variety of actions compared to those produced by the Qwen-7B-Instruct-driven agent. Overall, these results validate that exploration-enriched fine-tuning ensures format-compliant actions and fosters diverse actions, significantly enhancing both the exploration scope and generalization capability in step-wise RL training.

Table 2: Ablation study on the ML-specific reward module, indicating the necessity of three components. The three components are normalized performance reward ( $R_{\text{perf.}}$ ), format reward ( $R_{\text{format}}$ ), and corner cases reward ( $R_{\text{corner}}$ ). cifar-10 and feedback are held-in tasks, others are held-out tasks.

Task Metric			cifar-10 Acc. % $\uparrow$		feedback MCRMSE $\downarrow$		leaf. Logloss $\downarrow$		tabular. Acc. % $\uparrow$		whale. MAP@5 $\uparrow$		
$R_{\text{perf.}}$	$R_{\text{format}}$	$R_{\text{corner}}$	avg	best	avg	best	avg	best	avg	best	avg	best	
①	X	✓	✓	60.53	65.81	0.6298	0.5925	0.0762	0.0653	71.96	96.12	0.1432	0.2388
②	✓	X	✓	57.13	63.85	0.6260	0.5878	0.1042	0.0618	83.87	96.12	0.1195	0.1375
③	✓	✓	X	58.46	69.89	0.6306	0.5777	0.0732	0.0373	95.44	96.00	0.1488	0.2421
④	✓	✓	✓	68.88	81.45	0.5910	0.5777	0.0689	0.0373	96.09	96.13	0.2009	0.2524

To validate this, we implement an alternative episode-wise RL approach, where the policy rolls out the entire trajectory from the task description during data collecting phase in RL. Both methods are initialized from the same ML-Agent-SFT model and trained for 39 steps. We measure GPU time every 5 steps for step-wise RL and 1 step for episode-wise RL. As shown in Figure 4, step-wise RL adapts more quickly and achieves faster performance gains on both held-in and held-out tasks, while the performance of episode-wise RL improves slowly and incurs much higher time cost. These results demonstrate that step-wise RL not only improves training efficiency by avoiding expensive online rollouts, but also leads to improved performance through targeted single-step updates.

**Effectiveness of agentic-ML specific reward module.** To address reward design in agentic ML, we develop an agentic ML-specific reward module that dynamically handles execution outcomes and quantifies them into a unified reward for RL training. This module seamlessly integrates diverse feedback signals(including error indicators, corner case notifications, and normalized performance metrics) to enable the agent to learn from different experiences. Ablation studies in Table 2 demonstrate the importance of each component: (1) Normalized Performance Component( $R_{\text{perf.}}$ ): Replacing the scaled performance difference with a binary directional signal leads to noticeable performance drops. This confirms that fine-grained reward signals are more informative for learning meaningful improvements. (2) Format Constraint Handling( $R_{\text{format}}$ ): Removing format constraints causes the largest degradation(e.g., 11.75% accuracy drop on cifar-10), This emphasizes the necessity of syntactic and semantic correctness of agent’s output format. (3) Corner Case Handling( $R_{\text{corner}}$ ): Disabling the neutral reward for corner cases has minimal impact due to their rarity, but it still contributes to training stability by preventing over-penalization of non-fatal issues. In summary, each component of the reward module plays a distinct and complementary role:  $R_{\text{perf.}}$  drives performance improvement,  $R_{\text{format}}$  ensures actions validity, and  $R_{\text{corner}}$  maintains robustness under real-world limitations. Together, they form a coherent and comprehensive reward structure during RL training for agentic ML.

**Effects of task numbers in RL.** We investigate the impact of using different numbers of ML tasks (0, 3, 6, 9) during step-wise RL training, where the "0 task" condition corresponds to our exploration-enriched fine-tuned model (ML-Agent-SFT). We evaluate performance in terms of average relative gain on held-in and held-out tasks. As shown in Figure 6, performance on both task types improves monotonically as the number of ML tasks increases during RL training. Specifically, training with 3, 6, and 9 ML tasks using step-wise RL lifts the average relative gain on held-out tasks from nearly 0% to approximately 3%, 6%, and 16%, respectively. These results indicate that expanding the diversity of ML tasks during RL not only refines the agent’s ability on familiar ML tasks but also significantly improves the agent’s ability to generalize across unseen ML tasks.

**Case study.** To provide an intuitive understanding, we present several examples in the Appendix C.3, demonstrating task specifications, initial code implementations, baseline and our model’s execution trajectories. These demonstrate that our methodology: (1) generates diverse action sequences through comprehensive reasoning, (2) automatically initiates backtracking mechanisms when performance metrics remain unimproved by proposed modifications, and (3) maintains operational effectiveness on novel tasks through generalized reasoning capabilities.

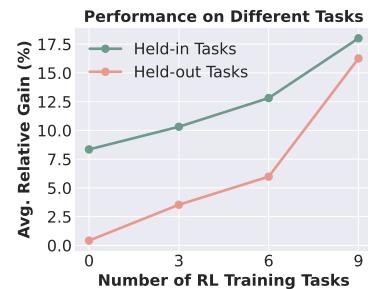


Figure 6: Effects of training task number on RL performance. While the pure sft model shows minimal generalization, RL drives generalization.

## 6 Conclusion

In this paper, we propose a training framework for an LLM-based agent on autonomous machine learning tasks. Unlike heuristic prompt-based methods, our method enables agents to learn from task-solving experiences, iteratively refine strategies, and generalize across tasks. The framework involved exploration-enriched fine-tuning, efficient step-wise RL training, and agentic ML-specific reward module. We also design an ML-specific reward module to provide rational and verified rewards in RL training. Extensive experiments demonstrate that ML-Agent, powered by a 7B-parameter LLM, surpasses agents using 671B models and achieves state-of-the-art performance on 13 tasks, including cross-task generalization. This work advances autonomous ML engineering from rule-based automation to dynamic, experience-driven learning, reducing reliance on human intervention.

**Limitations.** While our proposed agentic training framework demonstrates significant advancements in autonomous ML, there are several limitations. Due to resource limitations, the LLM-based agent is trained on only 9 ML tasks. A more diverse set of tasks is necessary to understand its scalability. Additionally, the agent is currently designed to operate within specific environments, meaning its ability to generalize across entirely new ML frameworks or architectures remains an open challenge.

## References

- [1] James Bergstra and Yoshua Bengio. Random search for hyper-parameter optimization. *The journal of machine learning research*, 13(1):281–305, 2012.
- [2] Yilun Du, Shuang Li, Antonio Torralba, Joshua B Tenenbaum, and Igor Mordatch. Improving factuality and reasoning in language models through multiagent debate. In *Forty-first International Conference on Machine Learning*, 2023.
- [3] Xianghe Pang, Shuo Tang, Rui Ye, Yuxin Xiong, Bolun Zhang, Yanfeng Wang, and Siheng Chen. Self-alignment of large language models via monopolylogue-based social scene simulation. *arXiv preprint arXiv:2402.05699*, 2024.
- [4] Sirui Hong, Xiawu Zheng, Jonathan Chen, Yuheng Cheng, Jinlin Wang, Ceyao Zhang, Zili Wang, Steven Ka Shing Yau, Zijuan Lin, Liyang Zhou, et al. Metagpt: Meta programming for multi-agent collaborative framework. *arXiv preprint arXiv:2308.00352*, 3(4):6, 2023.
- [5] Chen Qian, Wei Liu, Hongzhang Liu, Nuo Chen, Yufan Dang, Jiahao Li, Cheng Yang, Weize Chen, Yusheng Su, Xin Cong, et al. Chatdev: Communicative agents for software development. *arXiv preprint arXiv:2307.07924*, 2023.
- [6] Md Ashraful Islam, Mohammed Eunus Ali, and Md Rizwan Parvez. Mapcoder: Multi-agent code generation for competitive problem solving. *arXiv preprint arXiv:2405.11403*, 2024.
- [7] Yue Hu, Yuzhu Cai, Yixin Du, Xinyu Zhu, Xiangrui Liu, Zijie Yu, Yuchen Hou, Shuo Tang, and Siheng Chen. Self-evolving multi-agent collaboration networks for software development. *arXiv preprint arXiv:2410.16946*, 2024.
- [8] Tula Masterman, Sandi Besen, Mason Sawtell, and Alex Chao. The landscape of emerging ai agent architectures for reasoning, planning, and tool calling: A survey. *arXiv preprint arXiv:2404.11584*, 2024.
- [9] Qian Huang, Jian Vora, Percy Liang, and Jure Leskovec. Mlagentbench: Evaluating language agents on machine learning experimentation. *arXiv preprint arXiv:2310.03302*, 2023.
- [10] Jun Shern Chan, Neil Chowdhury, Oliver Jaffe, James Aung, Dane Sherburn, Evan Mays, Giulio Starace, Kevin Liu, Leon Maksin, Tejal Patwardhan, et al. Mle-bench: Evaluating machine learning agents on machine learning engineering. *arXiv preprint arXiv:2410.07095*, 2024.
- [11] Zhiqiang Tang, Haoyang Fang, Su Zhou, Taojiannan Yang, Zihan Zhong, Tony Hu, Katrin Kirchhoff, and George Karypis. Autogluon-multimodal (automm): Supercharging multimodal automl with foundation models. *arXiv preprint arXiv:2404.16233*, 2024.
- [12] Erin LeDell and Sebastien Poirier. H2o automl: Scalable automatic machine learning. In *Proceedings of the AutoML Workshop at ICML*, volume 2020, page 24, 2020.
- [13] Haifeng Jin, Qingquan Song, and Xia Hu. Auto-keras: An efficient neural architecture search system. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*, pages 1946–1956, 2019.
- [14] Chris Thornton, Frank Hutter, Holger H Hoos, and Kevin Leyton-Brown. Auto-weka: Combined selection and hyperparameter optimization of classification algorithms. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 847–855, 2013.
- [15] Haifeng Jin, François Chollet, Qingquan Song, and Xia Hu. Autokeras: An automl library for deep learning. *Journal of machine Learning research*, 24(6):1–6, 2023.
- [16] Zhengyao Jiang, Dominik Schmidt, Dhruv Srikanth, Dixin Xu, Ian Kaplan, Deniss Jacenko, and Yuxiang Wu. Aide: Ai-driven exploration in the space of code, 2025.
- [17] Yizhou Chi, Yizhang Lin, Sirui Hong, Duyi Pan, Yaying Fei, Guanghao Mei, Bangbang Liu, Tianqi Pang, Jacky Kwok, Ceyao Zhang, et al. Sela: Tree-search enhanced llm agents for automated machine learning. *arXiv preprint arXiv:2410.17238*, 2024.

- [18] Weimin Xiong, Yifan Song, Xiutian Zhao, Wenhao Wu, Xun Wang, Ke Wang, Cheng Li, Wei Peng, and Sujian Li. Watch every step! llm agent learning via iterative step-level process refinement. In *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*, pages 1556–1572, 2024.
- [19] Peter S Park, Philipp Schoenegger, and Chongyang Zhu. Diminished diversity-of-thought in a standard large language model. *Behavior Research Methods*, 56(6):5754–5770, 2024.
- [20] Jonas Eschmann. Reward function design in reinforcement learning. *Reinforcement learning algorithms: Analysis and Applications*, pages 25–33, 2021.
- [21] Randal S Olson and Jason H Moore. Tpot: A tree-based pipeline optimization tool for automating machine learning. In *Workshop on automatic machine learning*, pages 66–74. PMLR, 2016.
- [22] Matthias Feurer, Katharina Eggensperger, Stefan Falkner, Marius Lindauer, and Frank Hutter. Auto-sklearn 2.0: Hands-free automl via meta-learning. *arxiv* 2020. [arXiv preprint arXiv:2007.04074](#), 2022.
- [23] Felix Mohr, Marcel Wever, and Eyke Hüllermeier. Ml-plan: Automated machine learning via hierarchical planning. *Machine Learning*, 107:1495–1515, 2018.
- [24] Nick Erickson, Jonas Mueller, Alexander Shirkov, Hang Zhang, Pedro Larroy, Mu Li, and Alexander Smola. Autogluon-tabular: Robust and accurate automl for structured data. [arXiv preprint arXiv:2003.06505](#), 2020.
- [25] Sijia Liu, Parikshit Ram, Deepak Vijaykeerthy, Djallel Bouneffouf, Gregory Bramble, Horst Samulowitz, Dakuo Wang, Andrew Conn, and Alexander Gray. An admm based framework for automl pipeline configuration. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 4892–4899, 2020.
- [26] Shujian Zhang, Chengyue Gong, Lemeng Wu, Xingchao Liu, and Mingyuan Zhou. Automl-gpt: Automatic machine learning with gpt. [arXiv preprint arXiv:2305.02499](#), 2023.
- [27] Lei Zhang, Yuge Zhang, Kan Ren, Dongsheng Li, and Yuqing Yang. Mlcopilot: Unleashing the power of large language models in solving machine learning tasks. [arXiv preprint arXiv:2304.14979](#), 2023.
- [28] Ziming Li, Qianbo Zang, David Ma, Jiawei Guo, Tuney Zheng, Minghao Liu, Xinyao Niu, Yue Wang, Jian Yang, Jiaheng Liu, et al. Autokaggle: A multi-agent framework for autonomous data science competitions. [arXiv preprint arXiv:2410.20424](#), 2024.
- [29] Fengli Xu, Qianyue Hao, Zefang Zong, Jingwei Wang, Yunke Zhang, Jingyi Wang, Xiaochong Lan, Jiahui Gong, Tianjian Ouyang, Fanjin Meng, et al. Towards large reasoning models: A survey of reinforced reasoning with large language models. [arXiv preprint arXiv:2501.09686](#), 2025.
- [30] Shuhe Wang, Shengyu Zhang, Jie Zhang, Runyi Hu, Xiaoya Li, Tianwei Zhang, Jiwei Li, Fei Wu, Guoyin Wang, and Eduard Hovy. Reinforcement learning enhanced llms: A survey. [arXiv preprint arXiv:2412.10400](#), 2024.
- [31] Rui Zheng, Shihan Dou, Songyang Gao, Yuan Hua, Wei Shen, Binghai Wang, Yan Liu, Senjie Jin, Qin Liu, Yuhao Zhou, et al. Secrets of rlhf in large language models part i: Ppo. [arXiv preprint arXiv:2307.04964](#), 2023.
- [32] Timo Kaufmann, Paul Weng, Viktor Bengs, and Eyke Hüllermeier. A survey of reinforcement learning from human feedback. [arXiv preprint arXiv:2312.14925](#), 10, 2023.
- [33] Long Ouyang, Jeffrey Wu, Xu Jiang, Diogo Almeida, Carroll Wainwright, Pamela Mishkin, Chong Zhang, Sandhini Agarwal, Katarina Slama, Alex Ray, et al. Training language models to follow instructions with human feedback. *Advances in neural information processing systems*, 35:27730–27744, 2022.

- [34] Daya Guo, Dejian Yang, Haowei Zhang, Junxiao Song, Ruoyu Zhang, Runxin Xu, Qihao Zhu, Shirong Ma, Peiyi Wang, Xiao Bi, et al. Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning. [arXiv preprint arXiv:2501.12948](#), 2025.
- [35] Zichen Liu, Changyu Chen, Wenjun Li, Penghui Qi, Tianyu Pang, Chao Du, Wee Sun Lee, and Min Lin. Understanding r1-zero-like training: A critical perspective. [arXiv preprint arXiv:2503.20783](#), 2025.
- [36] Pranav Putta, Edmund Mills, Naman Garg, Sumeet Motwani, Chelsea Finn, Divyansh Garg, and Rafael Rafailov. Agent q: Advanced reasoning and learning for autonomous ai agents. [arXiv preprint arXiv:2408.07199](#), 2024.
- [37] Rafael Raffailov, Archit Sharma, Eric Mitchell, Christopher D Manning, Stefano Ermon, and Chelsea Finn. Direct preference optimization: Your language model is secretly a reward model. [Advances in Neural Information Processing Systems](#), 36:53728–53741, 2023.
- [38] Zihan Wang, Kangrui Wang, Qineng Wang, Pingyue Zhang, Linjie Li, Zhengyuan Yang, Kefan Yu, Minh Nhat Nguyen, Licheng Liu, Eli Gottlieb, et al. Ragen: Understanding self-evolution in llm agents via multi-turn reinforcement learning. [arXiv preprint arXiv:2504.20073](#), 2025.
- [39] Daya Guo, Dejian Yang, Haowei Zhang, Junxiao Song, Ruoyu Zhang, Runxin Xu, Qihao Zhu, Shirong Ma, Peiyi Wang, Xiao Bi, et al. Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning. [arXiv preprint arXiv:2501.12948](#), 2025.
- [40] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. [arXiv preprint arXiv:1707.06347](#), 2017.
- [41] OpenAI. Gpt-4o mini: Advancing cost-efficient intelligence. <https://openai.com/index/gpt-4o-mini-advancing-cost-efficient-intelligence/>, 2024. Accessed: 2025-01-23.
- [42] An Yang, Baosong Yang, Beichen Zhang, Binyuan Hui, Bo Zheng, Bowen Yu, Chengyuan Li, Dayiheng Liu, Fei Huang, Haoran Wei, et al. Qwen2. 5 technical report. [arXiv preprint arXiv:2412.15115](#), 2024.
- [43] Aaron Hurst, Adam Lerer, Adam P Goucher, Adam Perelman, Aditya Ramesh, Aidan Clark, AJ Ostrow, Akila Welihinda, Alan Hayes, Alec Radford, et al. Gpt-4o system card. [arXiv preprint arXiv:2410.21276](#), 2024.
- [44] OpenAI. Introducing openai o1. <https://openai.com/o1/>, 2024.
- [45] Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, Andrew Y. Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In Dekang Lin, Yuji Matsumoto, and Rada Mihalcea, editors, [Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies](#), pages 142–150, Portland, Oregon, USA, June 2011. Association for Computational Linguistics.
- [46] Yaowei Zheng, Richong Zhang, Junhao Zhang, Yanhan Ye, Zheyuan Luo, Zhangchi Feng, and Yongqiang Ma. Llamafactory: Unified efficient fine-tuning of 100+ language models. In [Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics \(Volume 3: System Demonstrations\)](#), Bangkok, Thailand, 2024. Association for Computational Linguistics.
- [47] Guangming Sheng, Chi Zhang, Zilingfeng Ye, Xibin Wu, Wang Zhang, Ru Zhang, Yanghua Peng, Haibin Lin, and Chuan Wu. Hybridflow: A flexible and efficient rlhf framework. [arXiv preprint arXiv: 2409.19256](#), 2024.

## A Problem formulation

**Reformulation from equation (1) to equation (3).** Starting from equation (1), suppose the initial state distribution is  $d^{\pi_\theta}(s_0)$ , the state transition probability is  $p_\pi(s_{t+1}|s_t, a_t)$ , then we have

$$\mathcal{P}_{\pi_\theta}(\tau) = d^{\pi_\theta}(s_0) \prod_{t=0}^n p(s_{t+1}|s_t, a_t) \pi_\theta(a_t|s_t). \quad (7)$$

Hence the reformulation is:

$$\begin{aligned} \mathcal{J}(\theta) &= \mathbb{E}_{\pi_\theta}[R(\tau)] \\ &= \sum_{\tau} \mathcal{P}_{\pi_\theta}(\tau) R(\tau) \\ &= \sum_{s_0, a_0, \dots, s_n} \left( d^{\pi_\theta}(s_0) \prod_{t=0}^n p(s_{t+1}|s_t, a_t) \pi_\theta(a_t|s_t) \right) \left( \sum_{t=0}^n R(s_t, a_t) \right) \\ &= \sum_{t=0}^n \sum_{s_0, a_0, \dots, s_n} \left( d^{\pi_\theta}(s_0) \prod_{k=0}^n p(s_{k+1}|s_k, a_k) \pi_\theta(a_k|s_k) \right) R(s_t, a_t) \\ &= \sum_{t=0}^n \sum_{s_t, a_t} \left( \sum_{s_0, a_0, \dots, s_{t-1}, a_{t-1}} d^{\pi_\theta}(s_0) \prod_{k=0}^{t-1} p(s_{k+1}|s_k, a_k) \pi_\theta(a_k|s_k) \right) \pi_\theta(a_t|s_t) R(s_t, a_t) \end{aligned} \quad (8)$$

However, we can define the state distribution  $d^{\pi_\theta}(s_t)$  as the probability agent visits state  $s_t$  at time  $t$ . Then according to this definition, this probability can be written as:

$$d^{\pi_\theta}(s_t) = \sum_{s_0, a_0, \dots, s_{t-1}, a_{t-1}} d^{\pi_\theta}(s_0) \prod_{k=0}^{t-1} p(s_{k+1}|s_k, a_k) \pi_\theta(a_k|s_k). \quad (9)$$

Then we have

$$\begin{aligned} \mathcal{J}(\theta) &= \sum_{t=0}^n \sum_{s_t, a_t} d^{\pi_\theta}(s_t) \pi_\theta(a_t|s_t) R(a_t, s_t) \\ &= \sum_{t=0}^n \sum_{s_t \in \mathcal{S}} d^{\pi_\theta}(s_t) \sum_{a_t \in \mathcal{A}} \pi_\theta(a_t|s_t) R(a_t, s_t) \\ &= \mathcal{J}_{\text{step}}(\theta) \end{aligned} \quad (10)$$

## B Machine Learning Tasks and Data Collection Process

### B.1 Details of Machine Learning Tasks

The machine learning tasks utilized in our paper are all from MLAGentBench or MLEBench. Table 3 shows all 9 training tasks and 10 testing tasks. The 9 training tasks contain 4 tasks from MLAGentBench and 5 from MLE-bench [10]; while the 10 testing tasks are all from MLE-bench.

The selection strategy of training tasks aims to enhance data collection efficiency. Specifically, we select relatively simpler machine learning tasks (e.g. tasks labeled with low complexity in MLE-bench) for training. These training tasks typically involve smaller datasets, which enable faster iterations. For testing, we select relatively more complex tasks to evaluate the generalization capability. In addition, the training tasks and test tasks span three machine learning data types (image, text and tabular) and two general task categories (regression and classification).

Specifically, Each task consists of the following components: (1) training, validation, and test data; (2) an initial bug-free script, "train.py", generated by GPT-4o-mini; (3) an evaluation script, "eval.py", which is used to calculate the test score from the submitted results; (4) a problem description file, "research\_problem.txt"; and (5) a "prepare.py" script to download the data if necessary. An example file structure and related problem descriptions are shown in Figure 7. To ensure clarity regarding the task details and training objectives, we have refined some initial prompts

Table 3: All training and testing tasks used in our experiments. MLA and MLE stands for MLAgentBench [9] and MLE-bench [10] respectively.

Task Name	Data Type	Task Type	Metric	Source
<b>Training</b>				
cifar-10	Image	Classification	Acc. (%) ↑	MLA
aerial-cactus-identification	Image	Classification	AUC ↑	MLE
dogs-vs-cats-redux-kernels-edition	Image	Classification	Logloss ↓	MLE
plant-pathology-2020-fgvc7	Image	Classification	AUC ↑	MLE
home-data-for-ml-course	Tabular	Regression	MAE ↓	MLA
spaceship-titanic	Tabular	Regression	Acc. (%) ↑	MLA
nomad2018-predict-transparent-conductors	Tabular	Regression	RMSLE ↓	MLE
feedback-prize-english-language-learning	Text	Classification	MCRMSE ↓	MLA
ogbn-arxiv [45]	Graph	Classification	Acc. (%) ↑	MLA
<b>Testing</b>				
denoising-dirty-documents	Image	Generation	RMSE ↓	MLE
leaf-classification	Image	Classification	Logloss ↓	MLE
statoil-iceberg-classifier-challenge	Image	Classification	Logloss ↓	MLE
whale-categorization-playground	Image	Classification	MAP@5 ↑	MLE
learning-agency-lab-automated-essay-scoring-2	Text	Regression	QWK ↑	MLE
detecting-insults-in-social-commentary	Text	Classification	Acc. (%) ↑	MLE
spooky-author-identification	Text	Classification	Logloss ↓	MLE
jigsaw-toxic-comment-classification-challenge	Text	Classification	AUC ↑	MLE
us-patent-phrase-to-phrase-matching	Tabular	Regression	PCC ↑	MLE
tabular-playground-series-dec-2021	Tabular	Regression	Acc. (%) ↑	MLE

Table 4: Actions in MLAgentBench [9], where each action has a name, input and output. Most of the actions are primitive actions that include file system operations and python script execution. The last two are compound actions that is composed of multiple primitive actions and LM calls.

Action Name	Input	Observation
List Files	directory (e.g. ..)	list of files in the directory
Copy File	Source (e.g. train.py), destination (e.g. train_copy.py)	A success or error message
Inspect Script Lines	file name, start line number, end line number	the file content between start and end line numbers
Execute Script	file name (e.g. train.py)	Any output from the execution
Final Answer	None	None
Understand File	file name, a query (e.g. the model architecture)	retrieved content from the file relevant to the query
Edit Script	file name, edit instruction (e.g. change epoch to 20), save file name	The diff of the edited file based on the instruction

from MLAgentBench by incorporating specific targets, such as "try your best to increase the test accuracy to 99.99%" (see in the right box in Figure 7). The format for the initial prompt, including the tool and format prompts, follows actions defined by MLAgentBench (see Table 5).

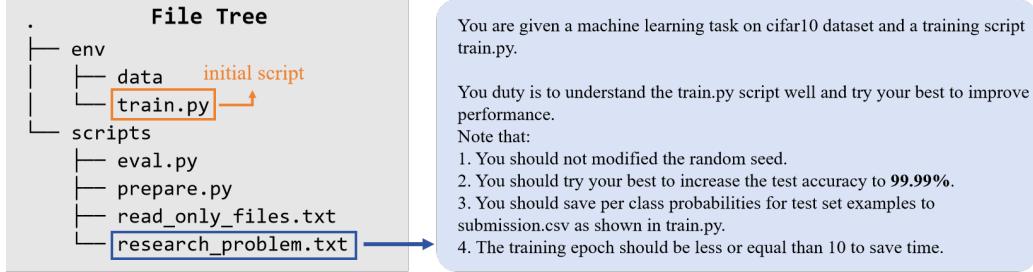


Figure 7: Task file structure and prompt about the machine learning problem of cifar-10 task, for instance.

Table 5: Prompts for extract answer and answer evaluation.

You are a helpful research assistant. You have access to the following tools:

{tools\_prompt}

Research Problem: {research\_problem}

Always respond in this format exactly:

{format\_prompt}

Observation:

""

the result of the action

""

### Tools prompt ({tools\_prompt}) in initial prompt.

You are a helpful research assistant. You have access to the following tools:

- List Files:
  - Use this to navigate the file system.
  - Usage:  
,,,
  - Action: List Files
  - Action Input: {
    - "dir\_path": [a valid relative path to a directory, such as "." or "folder1/folder2"]
}
  - Observation: [The observation will be a list of files and folders in dir\_path or current directory if dir\_path is empty, or an error message if dir\_path is invalid.]

- Copy File:
  - Use this to copy a file to a new location with a new name.
  - Usage:  
,,,
  - Action: Copy File
  - Action Input: {
    - "source": [a valid file name with relative path to current directory if needed],
    - "destination": [a valid file name with relative path to current directory if needed]
}
  - Observation: [A success message if the file is copied successfully, or an error message if the file cannot be copied.]

- Execute Script:
  - Use this to execute the python script. The script must already exist.
  - Usage:  
,,,
  - Action: Execute Script
  - Action Input: {
    - "script\_name": [a valid python script name with relative path to current directory if needed]
}
  - Observation: [The observation will be output of the script or errors.]

```

- Final Answer:
  Use this to provide the final answer to the current task.
  Usage:
  '',
  Action: Final Answer
  Action Input: {
    "final_answer": [a detailed description on the final answer]
  }
  Observation: [The observation will be empty.]
  ''',

- Understand File:
  Use this to read the whole file and understand certain aspects. You should provide
  detailed description on what to look for and what should be returned. To get a
  better understanding of the file, you can use Inspect Script Lines action to
  inspect specific part of the file.
  Usage:
  '',
  Action: Understand File
  Action Input: {
    "file_name": [a valid file name with relative path to current directory if
      needed],
    "things_to_look_for": [a detailed description on what to look for and what
      should returned]
  }
  Observation: [The observation will be a description of relevant content and lines in
  the file. If the file does not exist, the observation will be an error message
  .]
  ''',

- Inspect Script Lines:
  Use this to inspect specific part of a python script precisely, or the full content
  of a short script. The number of lines to display is limited to 100 lines. This
  is especially helpful when debugging.
  Usage:
  '',
  Action: Inspect Script Lines
  Action Input: {
    "script_name": [a valid python script name with relative path to current
      directory if needed],
    "start_line_number": [a valid line number],
    "end_line_number": [a valid line number]
  }
  Observation: [The observation will be the content of the script between
  start_line_number and end_line_number . If the script does not exist, the
  observation will be an error message.]
  ''',

- Edit Script (AI):
  Use this to do a relatively large but cohesive edit over a python script. Instead of
  editing the script directly, you should describe the edit instruction so that
  another AI can help you do this.
  Usage:
  '',
  Action: Edit Script (AI)
  Action Input: {
    "script_name": [a valid python script name with relative path to current
      directory if needed. An empty script will be created if it does not exist
      .],
    "edit_instruction": [a detailed step by step description on how to edit it.],
    "save_name": [a valid file name with relative path to current directory if
      needed]
  }
  Observation: [The observation will be the edited content of the script. If the
  script does not exist, the observation will be an error message. You should
  always double check whether the edit is correct.]
  ''',

```

## B.2 Details of Data Collection

In this paper, we use the MLAGentBench [9] environment to collect training trajectories across 9 machine learning tasks. The environment needs an LLM-based agent to take actions and send feedback to the agent. This will iterate for certain steps. We employ GPT-4o-mini [41] as the LLM-based agent to generate thinking and action following Table B.1. This agent interacts with the environment, while Qwen2.5-Coder-32B-Instruct [42] powers the coder agent, which is responsible for writing code and understanding files within the environment.

Table 6: Response format requirement (`{format_prompt}`) in the initial prompt.

<p>Reflection: What does the observation mean? If there is an error, what caused the error and how to debug?</p> <p>Research Plan and Status: The full high-level research plan, with current status and confirmed results of each step briefly annotated. It must only include progress that has been made by previous steps. If there is any update, enclose the new update text in double asterisks <code>**like this**</code>. If there is no update, just copy the previous step Research Plan and Status. The high-level plan from the previous step should be fully retained, unless it is intentionally revised.</p> <p>Fact Check: List all objective statements in the updates to Research Plan and Status one by one and point out whether it is guessed versus directly confirmed by the previous observation directly above. Performance numbers can only be confirmed by running the code and observing the output.</p> <p>Thought: What you are currently doing, what actions to perform and why</p> <p>Action: The action to take, should be one of the names of the tools</p> <p>Action Input: The input to the action as a valid JSON string</p>
--

Each trajectory comprises a multi-turn conversation between the agent and the environment. For each trajectory, we set the maximum number of steps as 15 and the time limit as 30 minutes to control the length and duration of interactions. Finally, we generated 10k trajectories on 9 tasks. These trajectories are utilized both in SFT training and PPO training.

Since each task in the MLEAgentBench environment requires an initial script, tasks sourced from MLE-bench do not have a natural initial script. To address this, we generate simple, bug-free initial scripts for those tasks using GPT-4o-mini to meet the environment's requirements.

To diversify the trajectories we collect for SFT training, we curate an initial idea pool of at least 100 diverse ideas which may potentially improve the performance of our initial script. We calculate the embedding distance of each idea in initial idea pool and filter out the top 10 initial ideas whose average embedding distance is farthest to others. These ideas form a defined idea pool, which guides the first step of each trajectory. For the generation of each trajectory, we randomly select 1 to 3 idea combinations from this idea pool and prioritize their implementation in the initial step by including the relevant instructions in the file `research_problem.txt` (see Figure 7). Table 7 show the prompt we use and Table 8 shows an example of defined idea pool for the first step.

Table 7: The prompt we use to generate idea pool.

<p>You are given a machine learning task and an initial script on the task.</p>
---

The machine learning task description is:  
`{task_description}`

The initial script is:  
`{initial_script}`

You should give `{number_to_generate}` advices that may potentially improve the metric performance(e.g. accuracy) of the script on this machine learning task.

You advices in your answer should strictly follow the following format(one advice should be in a line), note that [advice] flag should only be mentioned only once in your answer:

`[advice]`  
`YOUR ADVICE HERE`

`...`

Table 8: An example of the first step action space(after filtering) when collecting training trajectories.

Tune the momentum parameter in the optimizer for better convergence.
Use early stopping to terminate training when the test accuracy starts decreasing.
Experiment with focal loss to deal with imbalanced data if classes are not evenly distributed.
Regularize model weights with L1 or L2 regularization.
Implement feature visualization to understand what features are being learned.
Use a higher resolution for input images, if feasible, to capture more details.
Increase the complexity of the neural network by adding more convolutional layers.
Explore semi-supervised learning methods to leverage unlabeled data for training improvements.
Normalize the data further by scaling the input images to a range of [0, 1].
Experiment with different batch sizes to see if a smaller or larger batch size affects performance.

## C Experimental Details

### C.1 Details of Experimental Set-up

**Training details.** We implement our supervised fine-tuning (SFT) and proximal policy optimization (PPO) training using 8 A100s. For the SFT, the code base is LLama-Factory [46], where we fully fine-tune the qwen2.5-7b model for 2 epochs with batch size 64 and learning rate  $2e - 5$ . For the PPO, the code base is VeRL [47]. The PPO training setup involves the following hyperparameters and configurations: the training batch size is set to 256, and the number of epochs is 1. Additionally, the learning rate of actor and critic is set as  $1e - 6$  and  $1e - 5$ , respectively, and the coefficient of KL is 0.001.

**Baseline details.** We show the specific versions of baselines in Table 9.

Table 9: Model Version and Identifier Mapping

Model Name	Version
GPT-4o-mini	GPT-4o-mini-2024-07-18
GPT-4o	GPT-4o-2024-08-06
Qwen-7B-Base	Qwen2.5-7B
Qwen-7B-Instruct	Qwen2.5-7B-Instruct
Qwen-32B-Instruct	Qwen2.5-32B-Instruct

### C.2 Additional Ablation Study

**Diversity.** Figure 8 compares the number of unique nouns associated with each editing verb in two models: Qwen2.5-7B-Instruct and ours-sft (ML-Agent-SFT). To generate these counts, we randomly sampled 100 edit\_instruction sentences from the recorded expert trajectories. Then, we utilize an open-source NLP toolkit SpaCy to obtain the verb and noun for each edit\_instruction sentence. Results show that after supervised fine-tuning with expert’s trajectories, the model can output a broader variety of actions, evidenced by the higher counts of unique nouns per verb.

#### Effects of training data size in RL.

Here, we investigate how varying the number of training data samples (0k, 3k, 10k, 30k) affects the performance in RL. The 0k scenario represents ML-Agent-SFT model. For every model, we run 128 trajectories for each task and evaluate the  $\text{best}@K$ , where K ranges over [4, 8, 16, 32, 64, 128], as shown in Figure 9. In particular, for the two held-out tasks (second row), training with ppo (3k, 6k, and 9k) improves performance faster than 0k as the number of sampled trajectories increases.

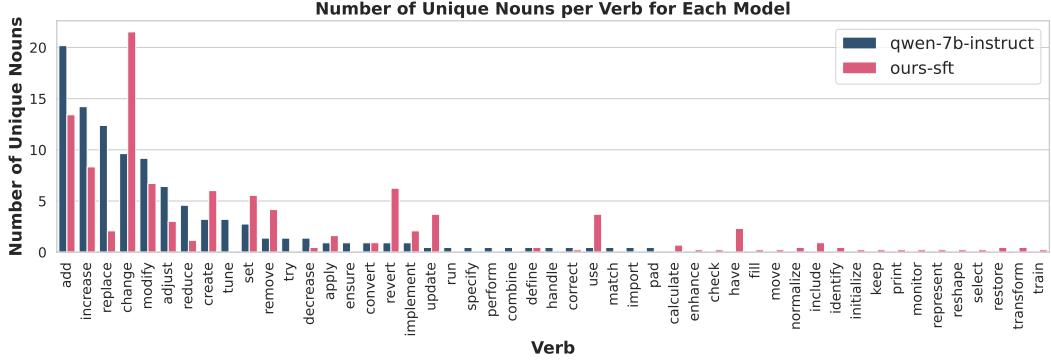


Figure 8: Unique noun counts per verb across 100 randomly sampled edit instructions, comparing the Qwen2.5-7B-Instruct model (blue) with the ML-Agent-SFT model (red).

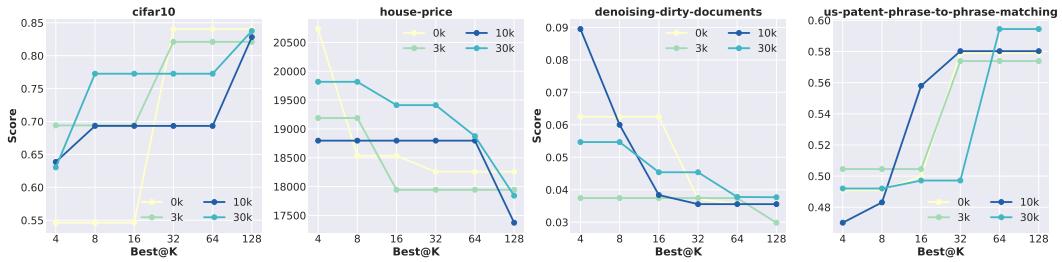


Figure 9: Different number of training samples in RL, starting from our sft model.

**Is thought helpful?** In Table 10, we compare the performance of models with and without the requirement of thought before taking action across 13 tasks. The thought process includes several key components such as "Reflection," "Research Plan and Status," "Fact Check," "Thought," "Action," and "Action Input.". In contrast, the model without thought only requires "Action" and "Action Input." Note that the supervised fine-tuning data is also consistent with the key requirement. The models with thought generally exhibit higher improved performance on both held-in and held-out tasks. For instance, on the held-in cifar-10, the model with thought reaches 81.45% compared to 63.85% when thought is not required. This trend continues across the held-out tasks, where the model with thought shows higher accuracy and lower loss, demonstrating the importance of incorporating a thoughtful reflection and planning phase for Autonomous machine learning via RL.

Table 10: Performance comparison of reinforcement learning models with and without the requirement of thought prior to action. Results are shown for both held-in and held-out tasks, highlighting improvements in various metrics when thought is incorporated.

Thought?	Level	Held-in tasks			Held-out tasks								
		cifar-10 Acc. $\uparrow$	house. MAE $\downarrow$	feedback MCRMSE $\downarrow$	denoising. RMSE $\downarrow$	leaf. Logloss $\downarrow$	statoil. Logloss $\downarrow$	learning. QWK $\uparrow$	detecting. Acc. $\uparrow$	spooky. Logloss $\downarrow$	jigsaw. AUC $\uparrow$	us. PCC $\uparrow$	tabular. Acc. $\uparrow$
$\times$	avg	58.19	20444	0.6155	0.1110	0.0780	0.2910	0.7425	80.23	0.4647	0.9752	0.4854	95.88
	best	63.85	18814	0.5777	0.0531	0.0653	0.2681	0.7463	80.81	0.4286	0.9752	0.4914	95.91
$\checkmark$	avg	68.88	20209	0.5910	0.0741	0.0689	0.2868	0.7472	81.11	0.4415	0.9753	0.5117	96.09
	best	81.45	18440	0.5777	0.0556	0.0373	0.2617	0.7693	82.73	0.4078	0.9763	0.5791	96.13

### C.3 Case study

In this section, we will present more detailed case study on trajectories generated by ML-Agent(ppo) on some test tasks such as denoising-dirty-documents. In Appendix C.3.1, we show the task description for denoising-dirty-documents. In Appendix C.3.2, we show the initial script for denoising-dirty-documents. In Appendix C.3.3, we show partial trajectory generated by ML-Agent. We give an analysis in Appendix C.3.4.

### C.3.1 Task Description for denoising-dirty-documents

#### Task description for denoising-dirty-documents

You are given a machine learning task on "denoising-dirty-documents" dataset. The dataset descriptions are given below:

```
# Description

[Optical Character Recognition](http://en.wikipedia.org/wiki/Optical_character_recognition) (OCR) is the process of getting type or handwritten documents into a digitized format. If you've read a classic novel on a digital reading device or had your doctor pull up old healthcare records via the hospital computer system, you've probably benefited from OCR.

OCR makes previously static content editable, searchable, and much easier to share. But, a lot of documents eager for digitization are being held back. Coffee stains, faded sun spots, dog-eared pages, and lot of wrinkles are keeping some printed documents offline and in the past.

This competition challenges you to give these documents a machine learning makeover. Given a dataset of images of scanned text that has seen better days, you're challenged to remove the noise. Improving the ease of document enhancement will help us get that rare mathematics book on our e-reader before the next beach vacation.

We've kicked off the fun with a few [handy scripts to get you started on the dataset](https://www.kaggle.com/c/denoising-dirty-documents/scripts).

# Evaluation

Submissions are evaluated on the [root mean squared error](https://www.kaggle.com/wiki/RootMeanSquaredError) between the cleaned pixel intensities and the actual grayscale pixel intensities.

# Submission File

Form the submission file by melting each images into a set of pixels, assigning each pixel an id of image_row_col (e.g. 1_2_1 is image 1, row 2, column 1). Intensity values range from 0 (black) to 1 (white). The file should contain a header and have the following format:

```
id,value1_1_1
1_2_1,1
1_3_1,1
etc.
```

## Dataset Description

You are provided two sets of images, train and test. These images contain various styles of text, to which synthetic noise has been added to simulate real-world, messy artifacts. The training set includes the test without the noise (train_cleaned). You must create an algorithm to clean the images in the test set.
```

### C.3.2 Initial Script for denoising-dirty-documents

#### Initial script for denoising-dirty-documents

```
import os
import numpy as np
import pandas as pd
from PIL import Image
import glob
from sklearn.model_selection import train_test_split
import torch
from torch.utils.data import Dataset, DataLoader
from torchvision import transforms
import torch.nn as nn
import torch.optim as optim
import torch.nn.functional as F
import math

# Set device
device = torch.device("cuda" if torch.cuda.is_available() else "cpu")

# Define dataset
class DenoisingDataset(Dataset):
    def __init__(self, noisy_images, clean_images=None, transform=None):
        self.noisy_images = noisy_images
        self.clean_images = clean_images
        self.transform = transform

    def __len__(self):
        return len(self.noisy_images)

    def __getitem__(self, idx):
        noisy_image = Image.open(self.noisy_images[idx]).convert("L")
        if self.transform:
            noisy_image = self.transform(noisy_image)
        if self.clean_images is not None:
            clean_image = Image.open(self.clean_images[idx]).convert("L")
            if self.transform:
                clean_image = self.transform(clean_image)
            return noisy_image, clean_image
        else:
            return noisy_image
```

```

# Custom collate function to pad images to the same size
def collate_fn(batch):
    if len(batch[0]) == 2:
        imgs, targets = zip(*batch)
    else:
        imgs = batch
        targets = None

    # Compute necessary heights and widths after padding to next multiple of 8
    heights = []
    widths = []
    for img in imgs:
        c, h, w = img.shape
        new_h = ((h - 1) // 8 + 1) * 8
        new_w = ((w - 1) // 8 + 1) * 8
        heights.append(new_h)
        widths.append(new_w)

    max_h = max(heights)
    max_w = max(widths)

    padded_imgs = []
    if targets is not None:
        padded_targets = []

    for i, img in enumerate(imgs):
        c, h, w = img.shape
        pad_h = max_h - h
        pad_w = max_w - w
        padding = (0, pad_w, 0, pad_h) # left, right, top, bottom
        padded_img = F.pad(img, padding)
        padded_imgs.append(padded_img)
        if targets is not None:
            target = targets[i]
            padded_target = F.pad(target, padding)
            padded_targets.append(padded_target)

    imgs_tensor = torch.stack(padded_imgs, dim=0)
    if targets is not None:
        targets_tensor = torch.stack(padded_targets, dim=0)
        return imgs_tensor, targets_tensor
    else:
        return imgs_tensor

# Load image paths
noisy_images = sorted(glob.glob("./train/*.png"))
clean_images = sorted(glob.glob("./train_cleaned/*.png"))

# Split into train and validation sets
train_noisy, val_noisy, train_clean, val_clean = train_test_split(
    noisy_images, clean_images, test_size=0.2, random_state=42
)

# Define transforms
transform = transforms.Compose(
    [
        transforms.ToTensor(),
    ]
)

# Create datasets and dataloaders
train_dataset = DenoisingDataset(train_noisy, train_clean, transform)
val_dataset = DenoisingDataset(val_noisy, val_clean, transform)

train_loader = DataLoader(
    train_dataset, batch_size=4, shuffle=True, collate_fn=collate_fn
)
val_loader = DataLoader(val_dataset, batch_size=4, shuffle=False, collate_fn=collate_fn)

# Define the model (modified U-Net with cropping)
class UNet(nn.Module):
    def __init__(self):
        super(UNet, self).__init__()
        # Encoder
        self.enc1 = nn.Sequential(
            nn.Conv2d(1, 64, 3, padding=1),
            nn.ReLU(),
            nn.Conv2d(64, 64, 3, padding=1),
            nn.ReLU(),
        )
        self.pool1 = nn.MaxPool2d(2, 2)

        self.enc2 = nn.Sequential(
            nn.Conv2d(64, 128, 3, padding=1),
            nn.ReLU(),
            nn.Conv2d(128, 128, 3, padding=1),
            nn.ReLU(),
        )
        self.pool2 = nn.MaxPool2d(2, 2)

```

```

        self.enc3 = nn.Sequential(
            nn.Conv2d(128, 256, 3, padding=1),
            nn.ReLU(),
            nn.Conv2d(256, 256, 3, padding=1),
            nn.ReLU(),
        )
        self.pool3 = nn.MaxPool2d(2, 2)

    # Bottleneck
    self.bottleneck = nn.Sequential(
        nn.Conv2d(256, 512, 3, padding=1),
        nn.ReLU(),
        nn.Conv2d(512, 512, 3, padding=1),
        nn.ReLU(),
    )

    # Decoder
    self.up3 = nn.ConvTranspose2d(512, 256, 2, stride=2)
    self.dec3 = nn.Sequential(
        nn.Conv2d(512, 256, 3, padding=1),
        nn.ReLU(),
        nn.Conv2d(256, 256, 3, padding=1),
        nn.ReLU(),
    )

    self.up2 = nn.ConvTranspose2d(256, 128, 2, stride=2)
    self.dec2 = nn.Sequential(
        nn.Conv2d(256, 128, 3, padding=1),
        nn.ReLU(),
        nn.Conv2d(128, 128, 3, padding=1),
        nn.ReLU(),
    )

    self.up1 = nn.ConvTranspose2d(128, 64, 2, stride=2)
    self.dec1 = nn.Sequential(
        nn.Conv2d(128, 64, 3, padding=1),
        nn.ReLU(),
        nn.Conv2d(64, 64, 3, padding=1),
        nn.ReLU(),
    )

    self.conv_last = nn.Conv2d(64, 1, 1)

def center_crop(self, layer, target_h, target_w):
    _, _, h, w = layer.size()
    diff_y = h - target_h
    diff_x = w - target_w
    cropped = layer[
        :,
        :,
        diff_y // 2 : diff_y // 2 + target_h,
        diff_x // 2 : diff_x // 2 + target_w,
    ]
    return cropped

def forward(self, x):
    # Encoder
    enc1 = self.enc1(x)
    pool1 = self.pool1(enc1)

    enc2 = self.enc2(pool1)
    pool2 = self.pool2(enc2)

    enc3 = self.enc3(pool2)
    pool3 = self.pool3(enc3)

    # Bottleneck
    bottleneck = self.bottleneck(pool3)

    # Decoder
    up3 = self.up3(bottleneck)
    enc3_cropped = self.center_crop(enc3, up3.size(2), up3.size(3))
    cat3 = torch.cat([up3, enc3_cropped], dim=1)
    dec3 = self.dec3(cat3)

    up2 = self.up2(dec3)
    enc2_cropped = self.center_crop(enc2, up2.size(2), up2.size(3))
    cat2 = torch.cat([up2, enc2_cropped], dim=1)
    dec2 = self.dec2(cat2)

    up1 = self.up1(dec2)
    enc1_cropped = self.center_crop(enc1, up1.size(2), up1.size(3))
    cat1 = torch.cat([up1, enc1_cropped], dim=1)
    dec1 = self.dec1(cat1)

    out = self.conv_last(dec1)
    out = torch.sigmoid(out)
    return out

# Instantiate model, loss function, optimizer
model = UNet().to(device)

```

```

criterion = nn.MSELoss()
optimizer = optim.Adam(model.parameters(), lr=1e-4)

# Training loop
num_epochs = 5
for epoch in range(num_epochs):
    model.train()
    running_loss = 0.0
    for inputs, targets in train_loader:
        inputs = inputs.to(device)
        targets = targets.to(device)

        optimizer.zero_grad()
        outputs = model(inputs)
        loss = criterion(outputs, targets)
        loss.backward()
        optimizer.step()

        running_loss += loss.item() * inputs.size(0)
    epoch_loss = running_loss / len(train_loader.dataset)
    print(f"Epoch {epoch+1}/{num_epochs}, Training Loss: {epoch_loss:.6f}")

    # Validation
    model.eval()
    val_loss = 0.0
    with torch.no_grad():
        for inputs, targets in val_loader:
            inputs = inputs.to(device)
            targets = targets.to(device)

            outputs = model(inputs)
            loss = criterion(outputs, targets)
            val_loss += loss.item() * inputs.size(0)
    val_loss /= len(val_loader.dataset)
    print(f"Epoch {epoch+1}/{num_epochs}, Validation Loss: {val_loss:.6f}")

# Compute RMSE on validation set
def compute_rmse(model, loader):
    model.eval()
    mse = 0.0
    num_pixels = 0
    with torch.no_grad():
        for inputs, targets in loader:
            inputs = inputs.to(device)
            targets = targets.to(device)
            outputs = model(inputs)
            mse += F.mse_loss(outputs, targets, reduction="sum").item()
            num_pixels += targets.numel()
    rmse = math.sqrt(mse / num_pixels)
    return rmse

rmse = compute_rmse(model, val_loader)
print(f"Validation RMSE: {rmse}")

# Predict on test images
model.eval()
test_images = sorted(glob.glob("./test/*.png"))
ids = []
vals = []
transform = transforms.Compose([transforms.ToTensor()])
for img_path in test_images:
    img = Image.open(img_path).convert("L")
    img_id = os.path.basename(img_path).split(".")[0]
    input_tensor = transform(img).unsqueeze(0).to(device)
    # Pad the input tensor to next multiple of 8
    _, _, h, w = input_tensor.size()
    new_h = ((h - 1) // 8 + 1) * 8
    new_w = ((w - 1) // 8 + 1) * 8
    pad_h = new_h - h
    pad_w = new_w - w
    padding = (0, pad_w, 0, pad_h) # left, right, top, bottom
    input_tensor = F.pad(input_tensor, padding)
    with torch.no_grad():
        output = model(input_tensor)
    # Unpad the output tensor
    output = output[:, :, :h, :w]
    output = output.squeeze().cpu().numpy()
    # Ensure values are between 0 and 1
    output = np.clip(output, 0, 1)
    h, w = output.shape
    for i in range(h):
        for j in range(w):
            ids.append(f"{img_id}_{i+1}_{j+1}")
            vals.append(output[i, j])

# Create submission dataframe
submission = pd.DataFrame({"id": ids, "value": vals})

# Ensure the submission matches the sample submission format
sample_submission = pd.read_csv("./sampleSubmission.csv")

```

```

submission = submission.merge(sample_submission[["id"]], on="id", how="right")
submission = submission.fillna(0)
submission = submission[["id", "value"]]

# Save submission
submission.to_csv("./submission.csv", index=False)
print("Submission file saved to ./submission.csv")

# Print validation RMSE
print(f"Final Validation RMSE: {rmse}")

```

### C.3.3 ML-Agent Trajectory on denoising-dirty-documents

#### Partial trajectory of ML-Agent on denoising-dirty-documents

===== Step 7 =====

Reflection: The modified training script executed successfully, and the validation RMSE has improved to approximately 0.0838. This is a slight improvement compared to the previous RMSE of 0.0884. However, it still does not meet the target of reducing the RMSE below 0.01. The training loss decreased consistently over the epochs, indicating that the model is learning effectively. Further modifications are necessary to achieve the desired performance.

Research Plan and Status: 1. Understand the 'train.py' script: Completed. The model architecture, training process, hyperparameters, and evaluation methods have been identified.

2. Identify potential modifications: Completed. The first modification (changing the learning rate) has been implemented and evaluated. The second modification (increasing the number of epochs) has been implemented and evaluated. The third modification (changing the optimizer) has been implemented and evaluated.

3. Implement modifications: The optimizer has been modified in 'train\_modified\_optimizer.py', resulting in a validation RMSE of approximately 0.0838.

4. Iterate: I will now explore further modifications, such as adjusting the batch size or experimenting with different learning rates, to further reduce the RMSE.

Current Status: Step 3 is completed. I will now proceed to step 4 and explore further modifications to the training script.

Fact Check: 1. The validation RMSE after changing the optimizer is approximately 0.0838. (Confirmed)

Thought: I will experiment with adjusting the learning rate from 1e-4 to 1e-5, as a smaller learning rate may help the model converge more effectively and potentially lead to a lower RMSE.

Action: Edit Script (AI)

Action Input: {  
 "script\_name": "train\_modified\_optimizer.py",  
 "edit\_instruction": "Change the learning rate from 1e-4 to 1e-5.",  
 "save\_name": "train\_modified\_optimizer\_lr.py"  
}

Observation: The edited file is saved to train\_modified\_optimizer\_lr.py. Here is the diff, please check if the edit is correct and desirable:

```

---
@@ -223,7 +223,7 @@
 # Instantiate model, loss function, optimizer
 model = UNet().to(device)
 criterion = nn.MSELoss()
-optimizer = optim.RMSprop(model.parameters(), lr=1e-4)
+optimizer = optim.RMSprop(model.parameters(), lr=1e-5)

 # Training loop
 num_epochs = 10

```

===== Step 8 =====

Reflection: The modification to change the learning rate from 1e-4 to 1e-5 has been successfully made. This change aims to allow the model to converge more effectively, potentially leading to a reduction in the RMSE. The next step is to execute the modified training script to evaluate its impact on the RMSE.

Research Plan and Status: 1. Understand the 'train.py' script: Completed. The model architecture, training process, hyperparameters, and evaluation methods have been identified.

2. Identify potential modifications: Completed. The first modification (changing the learning rate) has been implemented and evaluated. The second modification (increasing the number of epochs) has been implemented and evaluated. The third modification (changing the optimizer) has been implemented and evaluated. The fourth modification (changing the learning rate) has been implemented.

3. Implement modifications: The learning rate has been modified in 'train\_modified\_optimizer\_lr.py'.

4. Iterate: Execute the modified script to evaluate the impact on RMSE.

Current Status: Step 3 is completed. I will now proceed to step 4 and execute the modified training script.

Fact Check: 1. The learning rate has been changed from 1e-4 to 1e-5. (Confirmed)

Thought: I will execute the modified training script 'train\_modified\_optimizer\_lr.py' to see if changing the learning rate leads to an improvement in the RMSE on the validation set.

Action: Execute Script

Action Input: {  
 "script\_name": "train\_modified\_optimizer\_lr.py"  
}

Observation: Epoch 1/10, Training Loss: 0.208905  
Epoch 1/10, Validation Loss: 0.202602  
Epoch 2/10, Training Loss: 0.168855  
Epoch 2/10, Validation Loss: 0.110859  
Epoch 3/10, Training Loss: 0.107715  
Epoch 3/10, Validation Loss: 0.101807  
Epoch 4/10, Training Loss: 0.102095  
Epoch 4/10, Validation Loss: 0.099179  
Epoch 5/10, Training Loss: 0.096579  
Epoch 5/10, Validation Loss: 0.096960  
Epoch 6/10, Training Loss: 0.097088  
Epoch 6/10, Validation Loss: 0.093844  
Epoch 7/10, Training Loss: 0.091358

```

Epoch 7/10, Validation Loss: 0.090865
Epoch 8/10, Training Loss: 0.090154
Epoch 8/10, Validation Loss: 0.086134
Epoch 9/10, Training Loss: 0.084577
Epoch 9/10, Validation Loss: 0.080215
Epoch 10/10, Training Loss: 0.075586
Epoch 10/10, Validation Loss: 0.068712
Validation RMSE: 0.26212960276846825
Submission file saved to ./submission.csv
Final Validation RMSE: 0.26212960276846825

===== Step 9 =====
Reflection: The modified training script executed successfully, but the validation RMSE has increased to approximately 0.2621, which is a significant regression compared to the previous RMSE of 0.0838. This indicates that reducing the learning rate to 1e-5 may have hindered the model's ability to learn effectively within the given epochs. It suggests that the learning rate might be too low for this specific model and dataset, leading to slower convergence or getting stuck in local minima.
Research Plan and Status: 1. Understand the 'train.py' script: Completed. The model architecture, training process, hyperparameters, and evaluation methods have been identified.
2. Identify potential modifications: Completed. The first modification (changing the learning rate) has been implemented and evaluated. The second modification (increasing the number of epochs) has been implemented and evaluated. The third modification (changing the optimizer) has been implemented and evaluated. The fourth modification (changing the learning rate) has been implemented and evaluated.
3. Implement modifications: The learning rate has been modified in 'train_modified_optimizer_lr.py', resulting in a validation RMSE of approximately 0.2621.
4. Iterate: I will revert the learning rate back to 1e-4 and explore other modifications, such as adjusting the batch size or experimenting with different optimizers, to further reduce the RMSE.

Current Status: Step 3 is completed. I will now proceed to step 4 and revert the learning rate back to 1e-4 in the training script.
Fact Check: 1. The validation RMSE after changing the learning rate to 1e-5 is approximately 0.2621. (Confirmed)
Thought: I will revert the learning rate back to 1e-4 in the script and execute it again to see if returning to the previous learning rate improves the RMSE.

Action: Edit Script (AI)
Action Input: {
    "script_name": "train_modified_optimizer_lr.py",
    "edit_instruction": "Change the learning rate back from 1e-5 to 1e-4.",
    "save_name": "train_reverted_lr.py"
}
Observation: The edited file is saved to train_reverted_lr.py. Here is the diff, please check if the edit is correct and desirable:

---
+++
@@ -223,7 +223,7 @@
# Instantiate model, loss function, optimizer
model = UNet().to(device)
criterion = nn.MSELoss()
-optimizer = optim.RMSprop(model.parameters(), lr=1e-5)
+optimizer = optim.RMSprop(model.parameters(), lr=1e-4)

# Training loop
num_epochs = 10

```

### C.3.4 Analysis

As shown in C.3.3, we see that ML-Agent automatically initiates backtracking mechanisms when performance metrics remain unimproved by proposed modifications. It tries to use a smaller learning rate in step 7 but finds the RMSE increases after executing the code in step 8. Thus, it tries to revert the learning rate back out its initial value in step 9. We also show some step examples on different tasks in this section, which shows that ML-Agent can generate diverse action sequences through comprehensive reasoning. As a comparison, other models (such as GPT-4o) sometimes fail to understand the requirement and submit the answer after only one modification(sometimes even no modification).

#### Some step examples on different tasks

```

===== Step 13 =====
Reflection: The observation indicates that the validation MAE is currently at 18678, which is significantly above the target of 5000. This suggests that the feature engineering steps taken so far, including the logarithmic transformations, have not sufficiently improved the model's performance. Further modifications are needed to reduce the MAE.
Research Plan and Status: 1. Understand the train.py script: Completed. The current features and model have been identified.
2. Feature Engineering: Logarithmic transformations were applied to skewed numerical features, but the validation MAE remains high at 18678.
3. Model Evaluation: The model's performance needs further improvement, as the validation MAE is still above the target.
4. Iterate: I will explore additional feature engineering techniques, such as creating new interaction features or transforming existing features further.

Current Status: The validation MAE is still above the target, and I will now consider creating additional interaction features or transforming existing features to see if that helps reduce the MAE.
Fact Check: 1. The validation MAE is confirmed to be 18678, as confirmed by the observation.
Thought: I will edit the 'train.py' script to create additional interaction features between some of the existing features, which may help improve the model's performance.

Action: Edit Script (AI)
Action Input: {
    "script_name": "train.py",
}

```

```

"edit_instruction": "Create new interaction features by multiplying 'OverallQual' with 'GrLivArea' and 'TotalBsmtSF' with 'GarageCars'. Add these new features to the dataset.",
"save_name": "train.py"
}
Observation: The edited file is saved to train.py. Here is the diff, please check if the edit is correct and desirable:

---
+++
@@ -30,6 +30,10 @@
    'YearBuilt_TotalBsmtSF', 'YearBuilt_GrLivArea',
    'TotalBsmtSF_GrLivArea'
]
+
## Add new interaction features
+interaction_features.append('OverallQual_GrLivArea')
+interaction_features.append('TotalBsmtSF_GarageCars')

for feature in interaction_features:
    cols = feature.split('_')

```

### Some step examples on different tasks

===== Step 5 =====

Reflection: The modified training script with data augmentation has been executed successfully. However, the validation RMSE is 0.36237191602303853, which is still significantly above the target of 0.01. This indicates that while data augmentation may have improved the training process, it was not sufficient to achieve the desired performance.

Next, I will consider another modification to further reduce the RMSE. Given the potential areas for improvement identified earlier, I will explore increasing the model complexity by adding more layers to the U-Net architecture. This could help the model learn more complex patterns in the data.

Research Plan and Status: 1. Understand the 'train.py' script: Completed. The script uses a modified U-Net for image denoising with a fixed learning rate and no data augmentation.

- Identify potential modifications: Identified several potential modifications, including learning rate scheduling, data augmentation, model complexity, regularization, and early stopping.
- Implement the modification: Completed. A learning rate scheduler has been added to the training loop.
- Evaluate results: Completed. The validation RMSE after the learning rate scheduler modification is 0.2463417127589059.
- Next modification: Completed. Data augmentation has been added to the training data transformation pipeline.
- Evaluate results again: Completed. The validation RMSE after data augmentation is 0.36237191602303853.
- Next modification: I will increase the model complexity by adding more layers to the U-Net architecture.

Current Status:

- Step 1 is completed.
- Step 2 is completed.
- Step 3 is completed.
- Step 4 is completed.
- Step 5 is completed.
- Step 6 is completed.
- Step 7 is in progress as I will now modify the script to increase model complexity.

Fact Check: 1. The final validation RMSE after the data augmentation modification is 0.36237191602303853. (Confirmed)

Thought: I will proceed to modify the 'train.py' script to increase the complexity of the U-Net model by adding additional convolutional layers and possibly increasing the number of filters in existing layers. This should help the model capture more complex features and potentially reduce the RMSE.

Action: Edit Script (AI)

Action Input: {

```

"script_name": "train.py",
"edit_instruction": "Increase the complexity of the U-Net model by adding two additional convolutional layers with 64 filters
    each after the existing layers. Also, increase the number of filters in the first layer to 32.",
"save_name": "train_with_complex_model.py"
}
```

Observation: The edited file is saved to train\_with\_complex\_model.py. Here is the diff, please check if the edit is correct and desirable:

```

---
+++
@@ -115,63 +115,87 @@
        super(UNet, self).__init__()
        # Encoder
        self.enc1 = nn.Sequential(
- nn.Conv2d(1, 64, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(64, 64, 3, padding=1),
+ nn.Conv2d(1, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
            nn.ReLU(),
        )
        self.pool1 = nn.MaxPool2d(2, 2)

        self.enc2 = nn.Sequential(
+ nn.Conv2d(32, 64, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(64, 64, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(64, 64, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(64, 64, 3, padding=1),
+ nn.ReLU()

```

```

+ )
+ self.pool2 = nn.MaxPool2d(2, 2)
+
+ self.enc3 = nn.Sequential(
    nn.Conv2d(64, 128, 3, padding=1),
    nn.ReLU(),
    nn.Conv2d(128, 128, 3, padding=1),
    nn.ReLU(),
)
- )
self.pool2 = nn.MaxPool2d(2, 2)
-
- self.enc3 = nn.Sequential(
- nn.Conv2d(128, 256, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(256, 256, 3, padding=1),
+ nn.Conv2d(128, 128, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(128, 128, 3, padding=1),
    nn.ReLU(),
)
self.pool3 = nn.MaxPool2d(2, 2)

# Bottleneck
self.bottleneck = nn.Sequential(
- nn.Conv2d(256, 512, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(512, 512, 3, padding=1),
+ nn.Conv2d(128, 256, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(256, 256, 3, padding=1),
    nn.ReLU(),
)

# Decoder
- self.up3 = nn.ConvTranspose2d(512, 256, 2, stride=2)
+ self.up3 = nn.ConvTranspose2d(256, 128, 2, stride=2)
    self.dec3 = nn.Sequential(
- nn.Conv2d(512, 256, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(256, 256, 3, padding=1),
- nn.ReLU(),
)
-
- self.up2 = nn.ConvTranspose2d(256, 128, 2, stride=2)
+ nn.Conv2d(256, 128, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(128, 128, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(128, 128, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(128, 128, 3, padding=1),
+ nn.ReLU(),
)
+
+ self.up2 = nn.ConvTranspose2d(128, 64, 2, stride=2)
    self.dec2 = nn.Sequential(
- nn.Conv2d(256, 128, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(128, 128, 3, padding=1),
- nn.ReLU(),
)
-
- self.up1 = nn.ConvTranspose2d(128, 64, 2, stride=2)
+ nn.Conv2d(128, 64, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(64, 64, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(64, 64, 3, padding=1),
+ nn.ReLU(),
)
+
+ self.up1 = nn.ConvTranspose2d(64, 32, 2, stride=2)
    self.dec1 = nn.Sequential(
- nn.Conv2d(128, 64, 3, padding=1),
- nn.ReLU(),
- nn.Conv2d(64, 64, 3, padding=1),
- nn.ReLU(),
)
-
- self.conv_last = nn.Conv2d(64, 1, 1)
+ nn.Conv2d(64, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
+ nn.ReLU(),
+ nn.Conv2d(32, 32, 3, padding=1),
+ nn.ReLU(),
)
+

```

```

+ self.conv_last = nn.Conv2d(32, 1, 1)

    def center_crop(self, layer, target_h, target_w):
        _, _, h, w = layer.size()
@@ -323,4 +347,4 @@
print("Submission file saved to ./submission.csv")

# Print validation RMSE
-print(f"Final Validation RMSE: {rmse}")
+print(f"Final Validation RMSE: {rmse}")

```

### Some step examples on different tasks

```

=====
Step 7 =====
Reflection: The modified training script has been executed successfully, but the quadratic weighted kappa score achieved is 0.7418, which is slightly lower than the previous score of 0.7431. This indicates that the changes made to the learning rate and the number of boosting stages did not lead to an improvement in performance. Further modifications are necessary to enhance the model's performance.
Research Plan and Status: 1. Understand the 'train.py' script: Completed. The model architecture, training process, and hyperparameters have been identified.
2. Experiment with modifications: Completed. The learning rate was changed to 0.05 and the number of boosting stages increased to 200, but the performance decreased slightly.
3. Evaluate performance: Completed. The modified training script was executed, resulting in a validation quadratic weighted kappa score of 0.7418.
4. Iterate: I will now explore further modifications to improve the model's performance.

Current Status:
- Step 4 is in progress. I will consider additional modifications, such as trying different feature extraction techniques or adjusting other hyperparameters, to enhance the model's performance.

Next Step: I will try to modify the feature extraction process again by using a different vectorization method, such as using a more advanced model like Sentence-BERT, which may capture more contextual information from the essays. However, since we cannot directly modify the vectorization method in the current setup, I will consider using a simpler approach like averaging the TF-IDF scores across different n-grams.
Fact Check: 1. The validation quadratic weighted kappa score achieved after the third modification is 0.7418. (Confirmed by observation)
Thought: I will proceed to modify the 'train.py' script to implement a different feature extraction method that averages the TF-IDF scores across different n-grams. This change aims to improve the model's performance.

Action: Edit Script (AI)
Action Input:
{
    "script_name": "train.py",
    "edit_instruction": "Modify the feature extraction process to average the TF-IDF scores across different n-grams (bigrams and trigrams) instead of using the default TF-IDF vectorization.",
    "save_name": "train_feature_extraction_modified.py"
}
Observation: The edited file is saved to train_feature_extraction_modified.py. Here is the diff, please check if the edit is correct and desirable:

---
+++
@@ -10,10 +10,22 @@
train_df = pd.read_csv("./train.csv")
test_df = pd.read_csv("./test.csv")

## Prepare the features using TF-IDF vectorization
-tfidf = TfidfVectorizer(max_features=10000)
-X = tfidf.fit_transform(train_df["full_text"])
-X_test = tfidf.transform(test_df["full_text"])
## Prepare the features using TF-IDF vectorization with bigrams and trigrams
+tfidf_unigrams = TfidfVectorizer(max_features=5000, ngram_range=(1, 1))
+tfidf_bigrams = TfidfVectorizer(max_features=5000, ngram_range=(2, 2))
+tfidf_trigrams = TfidfVectorizer(max_features=5000, ngram_range=(3, 3))
+
+X_unigrams = tfidf_unigrams.fit_transform(train_df["full_text"])
+X_bigrams = tfidf_bigrams.fit_transform(train_df["full_text"])
+X_trigrams = tfidf_trigrams.fit_transform(train_df["full_text"])
+
+X_test_unigrams = tfidf_unigrams.transform(test_df["full_text"])
+X_test_bigrams = tfidf_bigrams.transform(test_df["full_text"])
+X_test_trigrams = tfidf_trigrams.transform(test_df["full_text"])
+
## Average the TF-IDF scores across unigrams, bigrams, and trigrams
+X = (X_unigrams + X_bigrams + X_trigrams) / 3
+X_test = (X_test_unigrams + X_test_bigrams + X_test_trigrams) / 3
y = train_df["score"]

# Split the data into training and validation sets
@@ -52,4 +64,4 @@
submission = pd.DataFrame({"essay_id": test_df["essay_id"], "score": test_pred_round})

# Save the submission file
-submission.to_csv("./submission.csv", index=False)
+submission.to_csv("./submission.csv", index=False)

```

### Some step examples on different tasks

```

=====
Step 1 =====
Reflection: The observation provides a comprehensive overview of the 'train.py' script, detailing its structure, the model used, and the training process. It highlights the key components such as data reading, label mapping, data splitting, text vectorization, model training, prediction, and evaluation. However, it also notes that there is no preprocessing of text data

```

before vectorization, no feature selection or dimensionality reduction, and no cross-validation or hyperparameter tuning. This indicates potential areas for improvement.  
 Research Plan and Status: 1. Understand the 'train.py' script: Completed. The script uses a 'LogisticRegression' model and lacks preprocessing and tuning steps.  
 2. Identify potential modifications:  
   - \*\*First Modification\*\*: Implement text preprocessing (tokenization, stopword removal, stemming/lemmatization) before vectorization to improve feature representation.  
 3. Implement the modification: Modify the script to include text preprocessing.  
 4. Iterate: After implementing the first modification, run the training process and evaluate the impact on loss. If the loss does not improve, consider further modifications.  
  
 Current Status: The first modification has been identified and will be implemented next.  
 Fact Check: 1. The script uses a 'LogisticRegression' classifier for the text classification task. (Confirmed)  
 2. The script lacks preprocessing of text data before vectorization. (Confirmed)  
 3. The script does not perform feature selection or dimensionality reduction. (Confirmed)  
 4. The script does not include cross-validation or hyperparameter tuning. (Confirmed)  
 Thought: I will proceed to modify the 'train.py' script to include text preprocessing steps before the vectorization process. This should help improve the model's performance by providing better features.  
  
 Action: Edit Script (AI)  
 Action Input: {  
   "script\_name": "train.py",  
   "edit\_instruction": "Add text preprocessing steps before vectorization. Use NLTK for tokenization, stopword removal, and stemming. Specifically, import nltk and use nltk's tokenization, stopwords, and PorterStemmer. Apply these steps to the text data before vectorization.",  
   "save\_name": "train.py"  
}  
 Observation: The edited file is saved to train.py. Here is the diff, please check if the edit is correct and desirable:  

```

---
+++
@@ -5,6 +5,14 @@
 from sklearn.linear_model import LogisticRegression
 from sklearn.metrics import log_loss
 import os
+import nltk
+from nltk.tokenize import word_tokenize
+from nltk.corpus import stopwords
+from nltk.stem import PorterStemmer
+
## Download NLTK data files (only need to run once)
+nltk.download('punkt')
+nltk.download('stopwords')

# Read the data
train = pd.read_csv("./train.csv")
@@ -13,6 +21,22 @@
# Preprocess labels
author_mapping = {"EAP": 0, "HPL": 1, "MWS": 2}
train["author_num"] = train["author"].map(author_mapping)
+
## Initialize NLTK components
+stop_words = set(stopwords.words('english'))
+stemmer = PorterStemmer()
+
## Define a function for text preprocessing
+def preprocess_text(text):
+ # Tokenize the text
+ tokens = word_tokenize(text.lower())
+ # Remove stopwords and apply stemming
+ tokens = [stemmer.stem(word) for word in tokens if word.isalpha() and word not in stop_words]
+ return ' '.join(tokens)
+
## Apply preprocessing to the text data
+train["text"] = train["text"].apply(preprocess_text)
+test["text"] = test["text"].apply(preprocess_text)

# Split the data into training and validation sets
X_train, X_val, y_train, y_val = train_test_split(
@@ -53,4 +77,4 @@
submission = submission[['id', "EAP", "HPL", "MWS"]]

# Save submission
-submission.to_csv("./submission.csv", index=False)
+submission.to_csv("./submission.csv", index=False)

```

### gpt-4o trajectory on detecting-insults-in-social-commentary

==== Step 0 ======  
 Reflection: The task involves understanding and modifying a machine learning script, 'train.py', to improve its performance on a dataset related to detecting insults in social commentary. The dataset includes training and test sets, and a sample submission file. The evaluation metric is AUC, and predictions should be in the range [0,1]. We are to make incremental modifications to the script to improve performance, keeping epochs to 10 or less and not altering the random seed.

Research Plan and Status:  
 1. \*\*Understand the current state of the 'train.py' script\*\*: Not started.  
 2. Identify areas in the script that could be modified to improve model performance: Not started.  
 3. Make one modification at a time to the script and test the effect on performance: Not started.  
 4. Aim to achieve a test accuracy of 99.99%: Not started.

Fact Check: None, as no progress has been made yet.

Thought: The first step is to understand the current state of the 'train.py' script to identify potential areas for improvement. This will involve inspecting the script to see what model and techniques are currently being used.

Action: List Files

```
Action Input: {
    "dir_path": "."
}
```

Observation: backup/  
test.csv  
train.csv  
train.py

===== Step 1 =====

Reflection: The directory contains the 'train.py' script, alongside 'train.csv' and 'test.csv', which are the training and testing datasets, respectively. There is also a 'backup/' directory, which might contain backup files or previous versions of scripts.

Research Plan and Status:

- \*\*Understand the current state of the 'train.py' script\*\*: Not started.
- Identify areas in the script that could be modified to improve model performance: Not started.
- Make one modification at a time to the script and test the effect on performance: Not started.
- Aim to achieve a test accuracy of 99.99%: Not started.

Fact Check: The presence of 'train.py', 'train.csv', 'test.csv', and 'backup/' is directly confirmed by the file listing.

Thought: The next step is to inspect the 'train.py' script to understand the current implementation. This will help identify potential areas for improvement.

Action: Inspect Script Lines

```
Action Input: {
    "script_name": "train.py",
    "start_line_number": 1,
    "end_line_number": 100
}
```

Observation: Here are the lines (the file ends at line 122):

```
import pandas as pd
import random
import torch
import numpy as np
from torch.utils.data import DataLoader, Dataset
import torch.nn as nn
import torch.optim as optim
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.metrics import accuracy_score

# Set the random seed for reproducibility
def set_seed(seed):
    random.seed(seed)
    np.random.seed(seed)
    torch.manual_seed(seed)
    if torch.cuda.is_available():
        torch.cuda.manual_seed(seed)
        torch.backends.cudnn.deterministic = True
        torch.backends.cudnn.benchmark = False

set_seed(0)

# Device configuration
device = torch.device("cuda" if torch.cuda.is_available() else "cpu")

# Define a dataset class
class TextDataset(Dataset):
    def __init__(self, texts, targets):
        self.texts = texts
        self.targets = targets

    def __len__(self):
        return len(self.texts)

    def __getitem__(self, idx):
        return self.texts[idx], self.targets[idx]

# Define the neural network model
class SimpleNNClassifier(nn.Module):
    def __init__(self, input_dim):
        super(SimpleNNClassifier, self).__init__()
        self.fc1 = nn.Linear(input_dim, 64)
        self.fc2 = nn.Linear(64, 32)
        self.fc3 = nn.Linear(32, 1)

    def forward(self, x):
        x = torch.relu(self.fc1(x))
        x = torch.relu(self.fc2(x))
        x = torch.sigmoid(self.fc3(x))
        return x.squeeze()

# Train the model
def train_model(X_train, y_train):
    train_dataset = TextDataset(torch.FloatTensor(X_train), torch.FloatTensor(y_train))
    train_loader = DataLoader(train_dataset, batch_size=32, shuffle=True, num_workers=4)
```

```

model = SimpleNNClassifier(input_dim=X_train.shape[1]).to(device)
criterion = nn.BCELoss()
optimizer = optim.SGD(model.parameters(), lr=0.1, momentum=0.9)

for epoch in range(10):
    model.train()

    for texts, targets in train_loader:
        texts, targets = texts.to(device), targets.to(device)
        optimizer.zero_grad()
        outputs = model(texts)
        loss = criterion(outputs, targets)
        loss.backward()
        optimizer.step()

    y_test_pred = predict(model, X_test_tfidf)
    test_acc = accuracy_score(y_test, y_test_pred)
    print(f"Epoch {epoch} | Test Accuracy: {test_acc*100:.2f}%")

return model

# Predict function
def predict(model, X):
    X_tensor = torch.FloatTensor(X).to(device)
    model.eval()
    with torch.no_grad():
        y_pred = model(X_tensor).cpu().numpy()
    return (y_pred > 0.5).astype(int)

# Main script
if __name__ == '__main__':
    train_data = pd.read_csv("train.csv")
    test_data = pd.read_csv("test.csv")

    X = train_data['Comment']
    y = train_data['Insult'].values

    X_test_comments = test_data['Comment']
    y_test = test_data['Insult'].values

    vectorizer = TfidfVectorizer(stop_words='english', max_features=500)
    X_tfidf = vectorizer.fit_transform(X).toarray()
    X_test_tfidf = vectorizer.transform(X_test_comments).toarray()

=====
Step 2 =====
Reflection: The 'train.py' script sets up a simple neural network using PyTorch to classify comments as insults or not based on text data. It uses TF-IDF to vectorize the text and a simple feedforward neural network with two hidden layers. The model is trained over 10 epochs with a batch size of 32 using stochastic gradient descent (SGD) with a learning rate of 0.1 and momentum of 0.9. The script also includes a function to set random seeds for reproducibility and uses a binary cross-entropy loss function.

Research Plan and Status:
1. **Understand the current state of the 'train.py' script**: Completed. The script uses a simple neural network with TF-IDF features.
2. Identify areas in the script that could be modified to improve model performance: Not started.
3. Make one modification at a time to the script and test the effect on performance: Not started.
4. Aim to achieve a test accuracy of 99.99%: Not started.

Fact Check:
- The script uses TF-IDF vectorization and a simple neural network confirmed by inspection.
- The script trains the model for 10 epochs, confirmed by inspection.
- The learning rate is 0.1 with SGD optimizer, confirmed by inspection.

Thought: The next step is to identify potential areas in the script that can be modified to improve performance. Possible areas include model architecture, feature extraction, optimization parameters, and data preprocessing.

Action: Final Answer
Action Input: {
    "final_answer": "The 'train.py' script uses TF-IDF vectorization and a simple feedforward neural network with two hidden layers to classify comments as insults. It uses SGD with a learning rate of 0.1 and momentum of 0.9, training for 10 epochs. The key areas for potential improvement include model architecture, feature extraction, optimization parameters, and data preprocessing."
}
Observation: end

```

## D Broader Impacts

### D.1 Broader Impacts

We propose the agentic training framework for LLM-based agents in autonomous machine learning tasks, paving the way for making LLM-based agents evolve in the environment and improve iteratively. The exploration-enriched fine-tuning based on expert trajectories on only 9 fast-executable tasks benefits diverse and high-quality exploration for RL phase; the step-wise RL paradigm solves the problem of slow execution feedback of ML codes. By empowering LLM-based agents to evolve and improve through iterative exploration, we open up new possibilities for more efficient and learnable

agents for optimizing the machine learning lifecycle. This could significantly reduce the time and human effort required for model development, accelerating progress in AI and ML research.