002

003 004

EXPOSING THE ACHILLES' HEEL: EVALUATING LLMS ABILITY TO HANDLE MISTAKES IN MATHEMATICAL REASONING

Anonymous authors

Paper under double-blind review

ABSTRACT

Large Language Models (LLMs) have significantly impacted the field of Math Word Problems (MWPs), transforming how these problems are approached and solved, particularly in educational contexts. However, existing evaluations often focus on final accuracy, neglecting the critical aspect of reasoning capabilities. This work addresses that gap by evaluating LLMs' abilities to detect and correct reasoning mistakes. We present a novel dataset, MWP-MISTAKE, containing MWPs with both correct and incorrect reasoning steps generated through rule-based methods and smaller language models. Our comprehensive benchmarking of state-of-the-art models such as GPT-4o and GPT4 uncovers important insights into their strengths and limitations. While GPT-4o excels in mistake detection and rectification, gaps remain, particularly in handling complex datasets and novel problems. Additionally, we identify concerns with data contamination and memorization, which affect LLM reliability in real-world applications. While OpenAI's O1 model demonstrates 90% accuracy in reasoning and final answers on complex tasks, it remains weak in mistake detection. Our findings highlight the need for improved reasoning evaluations and suggest ways to enhance LLM generalization and robustness in math problem-solving.

028 029 030

031

1 INTRODUCTION

032 033 034 035 036 037 038 039 040 041 042 Large Language Models (LLMs) have transformed artificial intelligence applications across diverse domains, including healthcare, agriculture, and education [\(OpenAI, b](#page-11-0)[;a\)](#page-11-1). Their remarkable capabilities in natural language understanding, question answering, and mathematical problem-have shown potential to revolutionize various human endeavors [\(Liu et al., 2024b\)](#page-11-2). Recent advancements have fueled extensive research into applying LLMs to interpret and solve a wide array of mathematical tasks, from basic arithmetic to complex algebraic equations and calculus problems [\(Hendrycks et al.,](#page-11-3) [2021;](#page-11-3) [Zhang et al., 2024a\)](#page-12-0). Math Word Problems (MWPs) involve interpreting narrative scenarios to extract mathematical concepts and apply reasoning for solutions [\(Srivatsa & Kochmar, 2024\)](#page-12-1). Studies [\(Xu et al., 2024;](#page-12-2) [He-Yueya et al., 2023;](#page-11-4) [Deb et al., 2023\)](#page-10-0) show LLMs can convert text into mathematical expressions and generate accurate results, but a critical element *mathematical reasoning* is often underexplored.

043 044 045 046 047 048 049 050 051 052 053 Despite achieving remarkable accuracy rates exceeding 90% on datasets like GSM-8K (Grade School Math dataset with linguistically diverse word problems) [\(Cobbe et al., 2021a\)](#page-10-1), foundational LLMs such as Claude-3-Opus [\(noa, a\)](#page-10-2), Gemini Ultra [\(Team et al., 2024\)](#page-12-3), and OpenAI GPT-4 [\(OpenAI](#page-11-5) [et al., 2024\)](#page-11-5) reveal a significant gap in our understanding of their capabilities in mathematical reasoning [\(Deb et al., 2023\)](#page-10-0). Current research predominantly focuses on evaluating the final accuracy of MWPs [\(Luo et al., 2023;](#page-11-6) [Yu et al., 2024\)](#page-12-4), neglecting the intricate reasoning processes necessary to derive solutions. We argue that the reasoning steps play a pivotal role, and it is imperative to assess them to comprehensively analyze the foundational capabilities of these models. This necessity is further underscored by the increasing utilization of LLMs in domains such as education [\(Gan et al.,](#page-10-3) [2023\)](#page-10-3), where they serve as personalized tutors for students, aiding in teaching concepts and solving mathematical problems. Simply deriving the final answer is insufficient; the ability to guide students through correct steps, identify errors in their reasoning, and provide corrective guidance is paramount for such applications.

061 062 063 Figure 1: Model is prompted with a question along with incorrect reasoning steps to detect any mistake and correct the reasoning step to get to the correct final answer. GPT-4o generates the correct output, while GPT-3.5Turbo fails to identify any mistake in the reasoning step. (Task - T1)

064 065 066 067 068 069 070 071 This paper aims to bridge this gap by providing a comprehensive benchmark and evaluation of LLMs' performance on math word problems, including their capabilities in mistake detection and correction within the reasoning steps (Figure [1\)](#page-1-0). Analyzing LLMs' ability to detect and rectify errors along the reasoning steps yields valuable insights into their overall problem-solving capabilities. Our objectives are threefold: firstly, to comprehensively evaluate LLMs' capabilities in mathematical reasoning, with a particular emphasis on mistake detection and correction; secondly, to identify the specific strengths and weaknesses of these models in handling various types of mathematical challenges; and thirdly, to propose potential directions for enhancing LLM capabilities in this domain.

072 073 074 075 076 077 To achieve this comprehensive evaluation, we have developed our own mistake dataset, designed to include errors in the reasoning steps. This dataset allows the assessment of models' proficiency not only in providing correct solutions but also in detecting and correcting mistakes within the reasoning steps. We evaluate 12 different foundational models including large, small and fine-tuned on math, language models on our curated dataset MWP-MISTAKE. We are releasing this dataset for further evaluation and benchmarking^{[1](#page-1-1)}.

078 079 080 081 082 083 Our analysis reveals several key insights into the performance of LLMs on MWPs. Firstly, detecting mistakes, even trivial ones remains a significant challenge for these models. Secondly, LLMs often derive correct answers despite this difficulty in mistake detection. This can be attributed to data memorization and potential contamination in training datasets, where models may have encountered similar/same problems before. However, the ability to recover from or correct errors in the reasoning process is generally poor across most models. Our contributions to this paper are as follows:

- **084 085 086 087 088** 1. We collect and release to the research community MWP-MISTAKE, a dataset containing MWPs with both correct and incorrect reasoning obtained from state-of-the-art MWP datasets such as SVAMP [\(Patel et al., 2021\)](#page-11-7), GSM-8K [\(Cobbe et al., 2021b\)](#page-10-4), MATH [\(Hendrycks et al., 2021\)](#page-11-3), MATHBENCH [\(Liu et al., 2024a\)](#page-11-8), and JEEBENCH [\(Arora et al., 2023\)](#page-10-5). Incorrect reasoning is derived through meticulously crafted rules to alter the reasoning steps and using smaller models, leveraging their inherent limitations in solving MWPs.
- **089 090 091 092 093** 2. We provide benchmark results for our dataset to evaluate the reasoning capabilities of LLMs such as GPT-4o [\(OpenAI, a\)](#page-11-1), GPT-4 [\(OpenAI et al., 2024\)](#page-11-5), GPT-3.5Turbo [\(noa, b\)](#page-10-6), Claude [\(noa,](#page-10-2) [a\)](#page-10-2), as well as smaller language models like Llama [\(Touvron et al., 2023\)](#page-12-5), Phi [\(Abdin et al.,](#page-10-7) [2024a\)](#page-10-7), and Mixtral [\(Jiang et al., 2024\)](#page-11-9) and also models fine-tuned on Math datasets. Our analysis demonstrates that all SOTA LLMs struggle with mistake detection and correction.

3. Through meticulous evaluation and comparison of different LLMs, we offer a detailed analysis of their strengths and weaknesses in handling mathematical reasoning tasks. We also provide early preliminary evaluations with OpenAI o1 models, which still does not excel in mistake detection.

2 MWP-MISTAKE DATASET

099 100 101 102 103 104 105 Most Math Word Problem (MWP) datasets provide math problems with final answers, occasionally including correct reasoning steps. To evaluate LLMs' ability to detect and correct errors, we created the MWP-MISTAKE dataset using five sources: SVAMP [\(Patel et al., 2021\)](#page-11-7), GSM-8K [\(Cobbe et al.,](#page-10-4) [2021b\)](#page-10-4), MATH [\(Hendrycks et al., 2021\)](#page-11-3), MATHBENCH [\(Liu et al., 2024a\)](#page-11-8), and JEEBENCH [\(Arora](#page-10-5) [et al., 2023\)](#page-10-5), with MATHBENCH and JEEBENCH being more recent. These five datasets form the basis of the MWP-MISTAKE dataset, covering a wide range of complexities from middle, high school to college levels. While GSM-8K and MATH offer ground truth corect reasoning steps, the others do not. For those, we used GPT-4 to generate chain-of-thought reasoning steps, which were

¹⁰⁶ 107

¹Anonymous repository for source code and dataset: [https://anonymous.4open.science/r/](https://anonymous.4open.science/r/Exposing-the-Achille-Heel-1D11/) [Exposing-the-Achille-Heel-1D11/](https://anonymous.4open.science/r/Exposing-the-Achille-Heel-1D11/)

114 115 Figure 2: Examples of MWPs with correct reasoning, rule-based incorrect and smaller model based incorrect reasoning from MATH.

116 117 118 119 then extensively manually verified for correctness. The final dataset includes MWP questions, correct reasoning steps, and final answers from all five sources (see Appendix [A](#page-12-6) for additional details). To create incorrect reasoning steps, we propose two approaches: (i) meticulously crafted rules, and (ii) using smaller models as bad reasoners, which we describe next.

120 121 122

113

2.1 METICULOUSLY CRAFTED RULES TO PROGRAMMATICALLY INJECT ERRORS

These rules are motivated and derived from common mistakes observed in educational settings, ensuring the errors introduced are realistic and representative of actual student errors.

- 1. Shuffle numerical values: Numerical values are shuffled among themselves to verify if models can correctly understand the question and select appropriate numerical values from the question.
- 2. **Replace numerical values:** Numerical values are replaced with random numbers ranging from 0 to 100. It identifies if the model can correctly pick the numerical values present in the question.
- 3. **Shuffle operations:** We randomly swap operators with other operators to test the model's ability to perform numerical operations.
- 4. Insert random reasoning steps: A random reasoning step is added at a random position to test the model's ability to identify incorrect reasoning.
- 5. Shuffle reasoning steps: The reasoning steps are shuffled to introduce ambiguity in the thought process. This tests whether the model can identify changes in reasoning order.
- **134 135** 6. Delete reasoning steps: One reasoning step is deleted in solutions that have two or more steps. This helps to identify if the model can spot omissions in the reasoning process.

136 137 138 139 140 141 142 These rules mimic real-world student behavior by reflecting tendencies to get the order of steps wrong, skip steps, misinterpret numerical values, use incorrect numbers, apply the wrong mathematical operations, and add irrelevant steps in problem-solving. While rules #5 and #6 do not introduce explicit errors in reasoning, they are considered mistakes in our dataset to prompt the model to identify scenarios lacking clarity. Table [1](#page-2-0) shows the number of questions selected from each of the five datasets to which these six rules are applied to curate incorrect reasoning. Thus, for every question selected, we created seven variations of reasoning steps (one correct + six incorrect).

143 2.2 SMALLER MODELS AS BAD REASONERS

144 145 146 147 148 149 150 151 Recently, SLMs are gaining popularity with increased performance, however, they still lack several capabilities, including advanced mathematical reasoning, resulting in poorer performance on MWPs. To curate incorrect reasoning steps, we use SLMs to generate Chain-of-Thought (COT) reasoning and final

Table 1: MWP-MISTAKE Dataset details with the total number of questions and reasoning steps.

152 153 154 155 156 157 158 159 answers for all dataset questions. Questions with incorrect final answers, identified by comparing them to the ground truth, are retained, and their reasoning steps are classified as incorrect. We then perform an extensive human validation of the answer and reasoning steps to make sure their is a mistake (as there could few instances where the answer can be incorrect, but reasoning steps could be correct). We employ state-of-the-art SLMs, such as Llama-2-7b-chat, Phi-3-mini, and Mixtral-8x7B, to generate COT reasoning steps and Appendix [C](#page-14-0) provides examples of such incorrect reasoning steps with final wrong answer. Table [1](#page-2-0) provides statistics for each model across datasets. The entire dataset, including reasoning steps, was exhaustively manually verified to eliminate errors.

160 161 Our dataset includes questions with original correct reasoning, rule-based incorrect reasoning, and SLM-generated incorrect reasoning. For evaluation, we split the data into two parts: (1) Default, with correct reasoning and rule-based incorrect steps, and (2) **SLM reason**, featuring SLM-generated **162 163 164** incorrect reasoning. Table [1](#page-2-0) provides the complete details of the curated MWP-MISTAKE dataset with the above two splits.

165 3 EXPERIMENTAL SETUP

166 167

194

200 201

206

208

Task Details. Our aim is to assess the performance of LLMs on MWPs, focusing on their ability to detect and correct mistakes within the reasoning steps. We have two task variants to accomplish this:

- **168 169 170** 1. Task-1 (T1): Given a question and its reasoning steps, the model must identify correctness, rectify mistakes if needed and compute the final answer.(Figure [1\)](#page-1-0).
- **171 172** 2. Task-2 (T2): The model only needs to identify whether the reasoning steps provided are correct or incorrect and provide the final answer. No correction of reasoning steps is explicitly required.

173 174 175 In essence, T1 evaluates the model's ability to detect mistakes, rectify them, and derive the correct answer, while T2 focuses solely on detecting mistakes and solving MWP correctly. Both tasks operate under few-shot settings, with specific prompt details provided in Appendix [D.](#page-16-0)

176 177 Models. To evaluate LLMs' mathematical reasoning capabilities, we utilize foundational LLMs, SLMs and math-finetuned SLMs.

- **178 179 180** 1. LLMs: We utilize 6 LLMs that have shown tremendous performance in MWPs such as GPT-4o, GPT-4, GPT-3.5Turbo, Claude-3-Opus, Llama-2-70b [\(Touvron et al., 2023\)](#page-12-5), Llama-3-70B [\(Dubey et al., 2024\)](#page-10-8).
- **181 182 183 184 185** 2. SLMs. Additionally, we evaluate six popular SLMs—Phi-3-mini [\(Abdin et al., 2024b\)](#page-10-9), Mixtral-8x7B [\(Jiang et al., 2024\)](#page-11-9), Llama-2-7b-chat [\(Touvron et al., 2023\)](#page-12-5), Qwen2-7B [\(Yang](#page-12-7) [et al., 2024\)](#page-12-7), Llama-3-8B [\(Dubey et al., 2024\)](#page-10-8), and Llama-3-8b-finetuned [\(Chen & Li, 2024\)](#page-10-10) trained on high-quality data to assess their reasoning capabilities. Appendix [E](#page-17-0) provides the details of the models, including their last training date.

186 187 188 189 190 191 Metrics. We compute the F1 score for all experiments as follows: for mistake detection, the model outputs either "yes" (indicating correct reasoning) or "no" (indicating incorrect reasoning). The ground truth labels are similarly "yes" for correct reasoning and "no" for incorrect reasoning, and the model's predictions are compared against these labels to calculate the F1 score. For performance evaluation, the generated final answer is compared to the ground truth final answer to compute the F1 score for accuracy.

- **192 193** 4 RESULTS AND ANALYSIS
	- 4.1 MISTAKE DETECTION ANALYSIS WITH SIMPLE MWPS

195 196 197 198 199 We evaluated the models' ability to detect reasoning mistakes using the SVAMP dataset, which contains simple arithmetic word problems (up to a 4th-grade level) and variations testing question sensitivity, reasoning ability, and structural invariance (Appendix [B](#page-13-0) for more details on the variations included). Mistakes were introduced using both rule-based methods and outputs from SLMs, with human validation ensuring accuracy.

Table 2: Mistake Detection Performance (F1 score) on SVAMP dataset with all variations

209 210 211 212 213 214 Table [7](#page-14-1) shows presents the models' mistake detection performance across these variations. The results show that none of the models consistently detected mistakes, with F1 scores across all variations falling below 80%. The highest F1 score, 81%, was achieved by Llama-3-8b-finetuned, a fine-tuned model specifically trained on 13 math-related datasets, which outperformed even more advanced models like GPT-4o and GPT-4. This suggests that fine-tuning on domain-specific data offers significant benefits for mathematical tasks.

215 Despite these improvements, even the fine-tuned model showed significant sensitivity to problem variations. When question sensitivity variations were introduced, performance dropped by 0.08, **216 217** Table 3: Mistake Detection Performance (F1 score) on MWP-MISTAKE dataset for Task T1. (D-Default reasoning steps, SM-Smaller model reasoning steps) (Bold: Best)

229 230

235

237

> while reasoning ability and structural invariance variations resulted in reductions of 0.06 and 0.02, respectively. GPT-4o exhibited a similar performance decline, suggesting that even the most advanced models are vulnerable to small variations in problem structure (See Table [7,](#page-14-1) Appendix [B\)](#page-13-0).

231 232 233 234 These findings highlight a key gap: even on relatively simple problems, models fail to generalize when minor variations are introduced. This suggests that fine-tuning, while beneficial, is insufficient to fully address the deeper issues in mistake detection across mathematical reasoning tasks. More robust methods are needed to improve generalization.

236 4.2 CAN LLMS EFFECTIVELY IDENTIFY MISTAKES IN REASONING STEPS?

238 239 We evaluate the ability of various models to detect mistakes in the reasoning steps of MWPs, with F1 scores across five datasets, as shown in Table [3](#page-4-0) for both default (D) and smaller models (SM).

240 241 242 243 244 245 246 GPT-4o Performance. GPT-4o is the top performer, outperforming models like GPT-4, GPT-3.5Turbo, and several smaller models. However, despite an overall F1 score of 87% across all datasets, it struggles with consistent mistake detection, particularly on simpler datasets such as SVAMP, and on more complex datasets like JEEBENCH, where its performance notably declines. For instance, on JEEBENCH, GPT-4o 's F1 score drops by 6% compared to its performance on GSM-8K. This shows that while GPT-4o excels in many areas, its precision for comprehensive mistake detection is still lacking, especially when faced with varying levels of complexity.

247 248 249 250 251 252 Rule-based vs. SLM-generated Mistakes. One notable observation is that GPT-4o and other models detect SLM-generated mistakes with higher accuracy compared to rule-based mistakes. For instance, GPT-4o achieves an F1 score of 94% for SLM errors versus 80% for rule-based errors across all datasets. This discrepancy suggests potential exposure to SLM-generated data during GPT-4o 's training, giving it an advantage in detecting these mistakes. This is an important insight into how training data might influence the model's effectiveness in mistake detection.

253 254 255 256 257 Performance of GPT-4 vs. GPT-3.5Turbo. While GPT-3.5Turbo performs similarly to GPT-4 and even surpasses it on certain datasets like GSM-8K, it struggles with errors generated by smaller models. On these, GPT-4 handles mistakes more effectively, likely due to potential data contamination or overfitting during its training. For instance, GPT-4 's F1 score for smaller model-generated mistakes is 86%, compared to GPT-3.5Turbo 's 56%.

258 259 260 261 262 Smaller Models and Fine-tuning. Smaller fine-tuned models, such as Llama-3-8b-finetuned, demonstrate a competitive performance close to that of GPT-4. Llama-3-8b-finetuned achieves an F1 score of 76%, outperforming other SLMs and even rivaling GPT-4 (77%) in certain cases. This highlights the effectiveness of domain-specific fine-tuning, especially for mathematical tasks, where tailored training significantly improves mistake detection accuracy.

263 264 265 266 267 268 269 Challenges with Newer Datasets. All models, including GPT-4o, face significant challenges with newer and more complex datasets such as MATHBENCH and JEEBENCH. For instance, GPT-4o 's F1 score drops by 6% on JEEBENCH compared to its performance on GSM-8K. This stark decline across models shows that their reasoning capabilities do not generalize well to unseen and more complex problem types. While GPT-4o still leads the pack, its limitations on these datasets underscore the need for better generalization in handling deeper reasoning challenges. Appendix [F](#page-17-1) shows additional detailed results showcasing the F1 score analysis on different types of rule-based reasoning mistakes across different models.

²²⁶ 227 228

270 Table 4: Performance in deriving correct answers (F1 score) on MWP-MISTAKE dataset for Task T1. (D-Default reasoning steps, SM-Smaller model reasoning steps) (Bold: Best)

271 272 273

279 280 281

4.3 CAN LLMS ACCURATELY DERIVE CORRECT ANSWERS DESPITE MISTAKES?

282 283 284 We assess the models' ability to generate correct answers even when reasoning steps contain mistakes. Table [4](#page-5-0) presents the F1 scores for Task 1, where models are explicitly tasked with detecting and rectifying mistakes to compute the final answer.

285 286 287 288 289 290 291 292 293 294 295 296 GPT-4o Performance. GPT-4o achieves an overall F1 score of 79% across all datasets, demonstrating an impressive ability to derive correct answers despite flawed reasoning. Specifically, it performs exceptionally well on simpler datasets like GSM-8K (99%), MATH (90%), and MATHBENCH (90%) in rectifying rule-based reasoning errors. However, its performance plummets to 48% on the more complex JEEBENCH dataset. Similar trend is seen in mistakes with SLMs, however this performance drop highlights a critical limitation: even though GPT-4o detects SLM based reasoning mistakes with over 90% accuracy, its ability to rectify them and generate correct answers is inconsistent, with F1 scores falling to 70-80%. This suggests that when faced with simple, rule-based mistakes, GPT-4o can often produce the correct answer, either through error correction or data memorization. However, when confronted with more intricate, SLM-generated mistakes, GPT-4o struggles to correct the errors and derive the correct answer, exposing significant shortcomings in the model's reasoning capabilities.

297 298 299 300 301 Performance of Other Models. Similar trends are observed for other models. Claude-3-Opus and GPT-4 rank second and third, respectively, in terms of performance. SLMs such as Phi, Llama, and Mixtral perform notably worse, with F1 scores ranging between 40-60%, significantly lower than GPT-4o and GPT-4. These results suggest that larger models like GPT-4o have a clear advantage in mistake rectification compared to smaller and fine-tuned models.

302 303 304 305 Challenges with Complex Datasets. All models, including GPT-4o, perform poorly on complex datasets like JEEBENCH, where the ability to derive correct answers drops significantly. This sharp decline underscores a critical limitation of current LLMs: their lack of robustness when confronted with deeper reasoning tasks and more intricate problem sets.

314 315 Figure 3: Performance in deriving final answer between T1 and T2. A significant drop in performance when the model does not rectify the incorrect reasoning steps.

316 317 318 319 320 Comparing Performance on Task 2: Identifying Mistakes Without Correction. In Task 2, models are required to identify the presence of a mistake but are not explicitly tasked with correcting it before providing the final answer. Figure [3](#page-5-1) illustrates the F1 scores of GPT-4o, GPT-4, and GPT-3.5Turbo across all datasets for both Task 1 (detect and rectify mistakes) and Task 2 (identify mistakes and compute the answer without rectification).

321 322 323 GPT-4o Performance. There is a noticeable drop in GPT-4o's performance between Task 1 and Task 2 across all datasets. In Task 1, where the model is prompted to both detect and correct mistakes, GPT-4o achieves higher accuracy, particularly on simpler datasets. However, in Task 2, where it only identifies whether a mistake is present, its F1 score significantly decreases. This decline suggests that **324 325 326** GPT-4o lacks the inherent ability to rectify mistakes unless it is explicitly instructed to do so. This inability to naturally correct mistakes without guidance reveals a key weakness in its reasoning.

327 328 329 330 331 332 GPT-4 Performance. While GPT-4 follows a similar trend to GPT-4o in showing a performance drop from Task 1 to Task 2, the gap between its Task 1 and Task 2 performance is smaller. This indicates that although GPT-4's overall performance is lower than GPT-4o, it experiences less of a drop when transitioning between the two tasks. This could suggest that GPT-4 is more consistent in detecting mistakes but, like GPT-4o, struggles to correct them when not explicitly prompted. The lower overall performance compared to GPT-4o indicates that GPT-4 is less capable of achieving high accuracy on both tasks.

333 334 335

4.4 EXPLORING DATA CONTAMINATION AND MEMORIZATION EFFECTS IN MATH REASONING TASKS

336 337 338 339 340 341 In our analysis of LLMs' mathematical reasoning performance, we've identified potential instances of data contamination and memorization, both of which can significantly impact the effectiveness of these models. Data contamination, characterized by the presence of test data from downstream tasks in LLMs' training data, poses a major challenge in accurately assessing their real-world performance. Meanwhile, memorization occurs when models replicate solutions from training data without grasping the underlying principles, thereby hindering their ability to generalize to new problems.

342 343 344 345 346 347 The presence of data contamination is evident in instances of unexpectedly high performance on certain datasets. For example, GPT-3.5Turbo's superior performance over GPT-4 on the GSM-8K dataset raises concerns about biases in GPT-4's training data. Similarly, the comparable performance between smaller and larger models suggests the potential presence of memorization. These findings underscore the critical need for rigorous evaluation to mitigate the impacts of memorization, ensuring the reliability and effectiveness of LLMs in real-world applications.

348 349 350 351 352 353 Investigating data contamination and memorization poses challenges due to restricted pre-training data access and computational limitations. To tackle this, we employ an approach outlined in [\(Golchin](#page-10-11) [& Surdeanu, 2024\)](#page-10-11), utilizing an LLM to replicate individual instances of the dataset. This involves guiding the LLM with instructions containing unique identifiers from the source dataset, like dataset name, partition (e.g., train, test, or validation), and a fragment of the reference instance. By instructing the LLM to complete these partial instances, we can evaluate contamination and memorization.

354 355 356 357 358 359 360 To detect contamination, a heuristic is applied comparing the average overlap score between generated completions and reference instances using ROUGE-L [\(Lin, 2004\)](#page-11-10). This comparison is made between guided instructions (including dataset and partition identifiers) and general instructions (lacking such identifiers). If the overlap score is significantly larger with guided instructions, it suggests contamination. This method relies on the premise that the only distinction between the two instructions is the inclusion of dataset and partition names in guided instructions, implying any improvement can be attributed to contamination (Appendix [I](#page-19-0) for more details).

361 362 363 364 Figure [4](#page-7-0) illustrates the difference in ROUGE-L scores between guided and general instructions across all datasets for various models. The results highlight notable discrepancies, providing early evidence of data contamination, particularly among the larger models.

365 366 367 368 GPT-4o Performance. GPT-4o exhibits the highest ROUGE-L scores across all datasets, suggesting a significant level of data contamination. This is consistent with its earlier performance, where it excelled in simpler tasks but struggled with more complex datasets, likely due to reliance on memorized data rather than true reasoning capabilities.

369 370 371 372 373 Comparative Contamination Across Models. Following GPT-4o, both GPT-4 and GPT-3.5Turbo show progressively lower ROUGE-L scores, though they still indicate some level of contamination. This pattern reinforces the earlier performance trends, where these models performed well but not as dominantly as GPT-4o, suggesting that their performance may also benefit from memorized data (especially on GSM-8K), albeit to a lesser degree.

374 375 376 377 SLMs' Minimal Contamination. In contrast, smaller language models (SLMs) such as Llama and Phi display negative ROUGE-L scores, suggesting minimal to no contamination. These models seem to rely more on reasoning rather than memorization, as their performance is not inflated by exposure to the test data during training. However, their lower overall performance on complex tasks highlights that they lack the advanced reasoning capabilities needed to match the larger models.

390 391 392 Figure 4: Difference between guided and general instructions rouge-L score across all datasets. A high positive difference indicates high contamination and a low positive or negative difference indicates, little to no contamination.

Table 5: Ability to Rectify mistakes and derive correct final answer on MWP-MISTAKE dataset for Task T1. (D-Default reasoning steps, SM-Smaller model reasoning steps) (Bold: Best)

403 404 405

4.5 CAN LLMS CORRECTLY RECTIFY MISTAKES IN REASONING STEPS?

406 407 408 409 410 411 412 In Task 1, the model not only detects mistakes but also attempts to rectify them to arrive at the correct answer. We evaluate the model's ability to rectify mistakes once detected by examining the number of questions where mistakes were identified and calculating how many times the model produced the correct answer after rectification. The assumption is that if the model reaches the correct final answer after detecting a mistake, it has successfully rectified the incorrect reasoning step. For instance, if the model identifies mistakes in 90 out of 100 questions and rectifies them in 45 cases (resulting in final correct answer), the rectification score would be 50% (45/90).

413 414 Table [5](#page-7-1) illustrates the performance of different models in rectifying reasoning steps and producing the correct final answer across various datasets.

415 416 417 418 419 420 421 GPT-4o shows high proficiency in rectifying mistakes, achieving an overall rectification score of 78% across all datasets. It outperforms GPT-4 by 11% and exceeds other models, including SLMs, by over 35%. Specifically, GPT-4o excels in correcting mistakes caused by rule-based reasoning compared to those induced by SLMs. However, its ability to fix mistakes decreases with more complex datasets like MATHBENCH and JEEBENCH. On simpler datasets, such as GSM-8K, MATH, and SVAMP, GPT-4o demonstrates high accuracy in rectification, potentially due to either data contamination (as discussed earlier) or the simpler nature of rule-based mistakes.

422 423 424 As observed earlier, Claude-3-Opus performs comparably to GPT-4o in rectifying mistakes. Other models, however, exhibit poorer rectification abilities, with scores ranging between 30-50%. Notably, Llama-3-70B achieves performance similar to GPT-4, indicating strong rectification capabilities.

425 426 427 428 429 430 431 To delve deeper into the rectification process, we also compute the percentage of questions where the model rectified the reasoning steps but still arrived at incorrect answers. Across the MWP-MISTAKE dataset, GPT-4o failed to derive the correct answer in 17% of cases after correcting the reasoning, while other models like GPT-4, GPT-4, Llama-2-7b-chat, Mixtral-8x7B, and Phi-3-mini resulted in 30%, 43.5%, 80.9%, 40.2%, and 55.6% incorrect answers, respectively. Additionally, we evaluated the rectified reasoning steps by comparing them with ground-truth reasoning steps to assess the effectiveness and alignment of the rectification process across models (detailed in Appendix [G](#page-18-0) and [H\)](#page-19-1). This comparison is quantified using traditional NLP metrics such as BERTScore.

432 4.6 HOW DOES OPENAI O1 MODEL PERFORM ON MWP-MISTAKE DATASET?

433 434

435 436 437 438 439 OpenAI recently introduced the O1 model, designed to enhance reasoning capabilities by spending more time processing tasks before responding. In a preliminary analysis comparing the performance of O1 and GPT-4O on 120 questions from the complex JEEBENCH dataset (38 correct reasoning steps, 56 rule-based mistakes, and 26 SLM-generated mistakes), several key insights emerged. O1 consistently outperforms GPT-4O, particularly in deriving correct final answers, showcasing its superior reasoning abilities across complex tasks (Table [15](#page-20-0) Appendix [J\)](#page-20-1).

440 441 442 443 444 445 446 447 448 Rule-based mistake identification. both O1 and GPT-4O perform similarly, with F1 scores of 0.4759 and 0.45, respectively. This suggests that both models struggle to consistently identify simple rule-based errors, detecting them with less than 50% accuracy. However, the significant divergence becomes apparent when comparing their ability to derive the correct final answer despite the mistakes. While GPT-4O manages an F1 score of only 0.43, O1 excels with a final answer F1 score of 0.8277, showing a notable improvement in reasoning capabilities. O1's ability to achieve such high final accuracy, despite similar mistake detection rates, underscores its advanced reasoning abilities, which may benefit from improved rectification strategies or more sophisticated handling of mistakes during the reasoning process.

449 450 451 452 453 454 455 SLM-generated mistakes. When analyzing SLM-generated mistakes, both models achieve 100% mistake detection accuracy, reflecting strong capabilities in identifying these more complex errors. However, the models diverge significantly in their ability to correct these mistakes and derive the correct final answer. O1 reaches a final answer F1 score of 0.9, while GPT-4O lags significantly behind with a score of only 0.62. This stark contrast highlights O1's substantial advancement not only in detecting mistakes but also in rectifying them to produce the correct final answer, showcasing its enhanced reasoning and generalization capabilities on more challenging datasets.

456 457 458 459 460 In summary, while both models are comparable in terms of mistake identification, O1 demonstrates a clear advantage in final answer generation and rectification, particularly on SLM-based mistakes. These results illustrate the superior reasoning capabilities of O1 over GPT-4O, making it a more effective model for handling intricate reasoning tasks. However, issues like potential data contamination and inefficiencies in processing time and token usage with O1 remain areas for further optimization.

461 462

475 476 477

5 KEY INSIGHTS, TAKEAWAYS, AND POTENTIAL DIRECTIONS FOR IMPROVING MATHEMATICAL REASONING

- 1. GPT-4o's Performance Strengths and Limitations: GPT-4o is the top performer across all datasets, achieving an overall F1 score of 87%. Its foundational capabilities enable strong performance in both mistake detection and rectification, particularly on simpler datasets like GSM-8K. However, its performance drops significantly on more complex datasets such as JEEBENCH and MATHBENCH, indicating limitations in handling highly complex or novel problems and highlighting the need for improved reasoning capabilities.
- **471 472 473 474** 2. Data Contamination and Overfitting Concerns: GPT-4o's unexpectedly high performance on datasets like GSM-8K and SVAMP suggests possible data contamination and overfitting, with models benefiting from memorized examples. To ensure fair evaluation, cleaner datasets and rigorous training methods are needed to assess true reasoning abilities rather than memorization.
	- 3. Challenges with Smaller Language Models (SLMs): There is a notable performance gap between smaller models (SLMs) and larger models like GPT-4o. While some SLMs, like Llama-3-8b-finetuned and Llama-3-70B, show competitive results, this may stem from similar contamination issues. Enhancing SLMs' reasoning abilities, is a key area for improvement.
- **478 479 480 481** 4. Generalization Difficulties Across Datasets: The performance decline on newer datasets such as MATHBENCH and JEEBENCH points to a generalization issue in LLMs. While models perform well on familiar datasets, they struggle with novel problems. Addressing this requires improved training strategies and more diverse datasets to broaden models' reasoning skills.
- **482 483 484 485** 5. Inconsistent Rectification Abilities: Despite strong mistake detection, GPT-4o shows inconsistent rectification performance, especially in complex datasets. Its ability to correct errors drops significantly between simple tasks (like rule-based errors) and more challenging ones (SLMgenerated mistakes). This highlights the need for more robust error correction capabilities in diverse reasoning scenarios.

486 487 488 489 Future research should prioritize cleaner datasets and techniques to reduce data contamination and overfitting, enabling better generalization to new tasks. Improving error rectification and enhancing smaller models through fine-tuning are key, as is advancing models' ability to handle complex rule-based reasoning for better performance on structured problems.

490 491 6 RELATED WORK

492 493 494 495 496 497 498 499 500 Current research on large language models (LLMs) for solving math word problems (MWPs) primarily emphasizes generating correct answers, often focusing on overall accuracy rather than evaluating the underlying reasoning processes. Studies like MathPrompter [\(Imani et al., 2023\)](#page-11-11) and WizardMath [\(Luo et al., 2023\)](#page-11-6) showcase impressive results in solving MWPs by generating complex reasoning steps. However, their focus remains heavily centered on achieving the correct answer without rigorously evaluating the correctness, relevance, or verification of the individual reasoning steps. For instance, works such as [\(Liu et al., 2024b;](#page-11-2) [Yuan et al., 2023;](#page-12-8) [Schulman et al., 2017\)](#page-11-12) focus primarily on enhancing LLMs' ability to reach accurate answers but do not delve into assessing whether the reasoning process itself is correct or aligned with logical problem-solving paths.

501 502 503 504 505 506 507 508 509 Several recent works have begun shifting their attention toward reasoning quality, but these efforts remain limited in scope. Studies like [\(Sawada et al., 2023\)](#page-11-13) evaluate reasoning by comparing the similarity of generated and reference reasoning, while others, such as [\(Xia et al., 2024\)](#page-12-9), introduce the idea of assessing reasoning steps through metrics like validity and redundancy. ROSCOE[\(Golovneva](#page-10-12) [et al., 2023\)](#page-10-12) takes this further by offering a suite of unsupervised metrics that evaluate various aspects of reasoning quality, such as semantic consistency and logicality, rather than just the final answer. While these methods attempt to scrutinize reasoning steps, they often fall short of addressing the detection and rectification of specific reasoning mistakes within MWPs, leaving a gap in understanding how well LLMs can manage flawed reasoning.

510 511 512 513 514 515 516 517 518 A third significant gap in the literature pertains to the limited exploration of LLMs' foundational reasoning abilities, particularly in mistake detection and rectification. While some works propose LLMs as verifiers for their own reasoning [\(Zhang et al., 2024b;](#page-12-10) [Zheng et al., 2023\)](#page-12-11), they typically assess reasoning correctness without tackling the deeper issue of identifying and correcting logical mistakes. Moreover, studies like [\(Olausson et al., 2024\)](#page-11-14) demonstrate that LLMs struggle to find and correct their own reasoning errors, especially in tasks involving code generation. Recent works such as Alice in Wonderland [\(Nezhurina et al., 2024\)](#page-11-15) breakdown the function and reasoning capabilities of LLMs and show that even small variations in such common sense tasks has drastic performance reduction. However, there remains a lack of rigorous benchmarking for mistake detection and correction in MWPs, especially for foundational models.

519 520 521 522 523 524 525 Our work addresses this gap by introducing the MWP-Mistake dataset, which includes diverse, systematic reasoning mistakes in MWPs. Unlike prior research, our analysis focuses not only on models' ability to detect mistakes but also on their ability to rectify these errors and generate correct answers. We provide a comprehensive benchmark, comparing state-of-the-art models on both simple and complex datasets. Through this work, we aim to provide a clearer understanding of current models' limitations in handling reasoning mistakes and propose a framework for evaluating LLMs' true reasoning abilities, rather than relying on answer accuracy alone.

526 527 7 CONCLUSIONS

528 529 530 531 532 533 534 535 536 537 538 539 This study evaluates large language models (LLMs) such as GPT-4o, GPT-4, GPT-3.5Turbo, alongside smaller models like Llama-2-7b-chat, Mixtral-8x7B, and Phi-3-mini, on their ability to detect and correct errors in mathematical reasoning. Using our MWP-MISTAKE dataset, which includes incorrect reasoning steps generated through both rule-based methods and smaller models, we comprehensively assess LLMs' performance in error detection and rectification. While GPT-4o outperforms other models, there remains a gap in its ability to consistently detect mistakes, as it struggles with several simple problems and its performance degrades on more complex tasks. We also uncover issues of data contamination and overfitting, especially in GPT-4's performance on GSM8K, and observe a performance drop on newer datasets like MATHBENCH and JEEBENCH, highlighting generalization challenges. Addressing these limitations—such as enhancing generalization and minimizing data contamination—is essential for making LLMs more reliable and applicable to real-world mathematical problem-solving. Future research should focus on refining training processes and strengthening models' reasoning abilities to meet these challenges.

540 541 REFERENCES

580 581 582

587 588

542 543 Introducing the next generation of Claude \ Anthropic, a. URL [https://www.anthropic.](https://www.anthropic.com/news/claude-3-family) [com/news/claude-3-family](https://www.anthropic.com/news/claude-3-family).

544 545 OpenAI Platform, b. URL <https://platform.openai.com>.

546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 Marah Abdin, Sam Ade Jacobs, Ammar Ahmad Awan, Jyoti Aneja, Ahmed Awadallah, Hany Awadalla, Nguyen Bach, Amit Bahree, Arash Bakhtiari, Jianmin Bao, Harkirat Behl, Alon Benhaim, Misha Bilenko, Johan Bjorck, Sébastien Bubeck, Qin Cai, Martin Cai, Caio César Teodoro Mendes, Weizhu Chen, Vishrav Chaudhary, Dong Chen, Dongdong Chen, Yen-Chun Chen, Yi-Ling Chen, Parul Chopra, Xiyang Dai, Allie Del Giorno, Gustavo de Rosa, Matthew Dixon, Ronen Eldan, Victor Fragoso, Dan Iter, Mei Gao, Min Gao, Jianfeng Gao, Amit Garg, Abhishek Goswami, Suriya Gunasekar, Emman Haider, Junheng Hao, Russell J. Hewett, Jamie Huynh, Mojan Javaheripi, Xin Jin, Piero Kauffmann, Nikos Karampatziakis, Dongwoo Kim, Mahoud Khademi, Lev Kurilenko, James R. Lee, Yin Tat Lee, Yuanzhi Li, Yunsheng Li, Chen Liang, Lars Liden, Ce Liu, Mengchen Liu, Weishung Liu, Eric Lin, Zeqi Lin, Chong Luo, Piyush Madan, Matt Mazzola, Arindam Mitra, Hardik Modi, Anh Nguyen, Brandon Norick, Barun Patra, Daniel Perez-Becker, Thomas Portet, Reid Pryzant, Heyang Qin, Marko Radmilac, Corby Rosset, Sambudha Roy, Olatunji Ruwase, Olli Saarikivi, Amin Saied, Adil Salim, Michael Santacroce, Shital Shah, Ning Shang, Hiteshi Sharma, Swadheen Shukla, Xia Song, Masahiro Tanaka, Andrea Tupini, Xin Wang, Lijuan Wang, Chunyu Wang, Yu Wang, Rachel Ward, Guanhua Wang, Philipp Witte, Haiping Wu, Michael Wyatt, Bin Xiao, Can Xu, Jiahang Xu, Weijian Xu, Sonali Yadav, Fan Yang, Jianwei Yang, Ziyi Yang, Yifan Yang, Donghan Yu, Lu Yuan, Chengruidong Zhang, Cyril Zhang, Jianwen Zhang, Li Lyna Zhang, Yi Zhang, Yue Zhang, Yunan Zhang, and Xiren Zhou. Phi-3 technical report: A highly capable language model locally on your phone, 2024a.

- **564 565 566** Marah Abdin, Sam Ade Jacobs, Ammar Ahmad Awan, Jyoti Aneja, Ahmed Awadallah, Hany Awadalla, Nguyen Bach, Amit Bahree, Arash Bakhtiari, Harkirat Behl, et al. Phi-3 technical report: A highly capable language model locally on your phone. *arXiv preprint arXiv:2404.14219*, 2024b.
- **567 568 569** Daman Arora, Himanshu Gaurav Singh, and Mausam. Have llms advanced enough? a challenging problem solving benchmark for large language models, 2023.
- **570 571** Wei Chen and Zhiyuan Li. Octopus v4: Graph of language models. *arXiv preprint arXiv:2404.19296*, 2024.
- **572 573 574 575** Karl Cobbe, Vineet Kosaraju, Mohammad Bavarian, Mark Chen, Heewoo Jun, Lukasz Kaiser, Matthias Plappert, Jerry Tworek, Jacob Hilton, Reiichiro Nakano, Christopher Hesse, and John Schulman. Training verifiers to solve math word problems, 2021a.
- **576 577 578 579** Karl Cobbe, Vineet Kosaraju, Mohammad Bavarian, Mark Chen, Heewoo Jun, Lukasz Kaiser, Matthias Plappert, Jerry Tworek, Jacob Hilton, Reiichiro Nakano, Christopher Hesse, and John Schulman. Training Verifiers to Solve Math Word Problems, November 2021b. URL [http:](http://arxiv.org/abs/2110.14168) [//arxiv.org/abs/2110.14168](http://arxiv.org/abs/2110.14168). arXiv:2110.14168 [cs].
	- Aniruddha Deb, Neeva Oza, Sarthak Singla, Dinesh Khandelwal, Dinesh Garg, and Parag Singla. Fill in the blank: Exploring and enhancing llm capabilities for backward reasoning in math word problems, 2023.
- **583 584 585 586** Abhimanyu Dubey, Abhinav Jauhri, Abhinav Pandey, Abhishek Kadian, Ahmad Al-Dahle, Aiesha Letman, Akhil Mathur, Alan Schelten, Amy Yang, Angela Fan, et al. The llama 3 herd of models. *arXiv preprint arXiv:2407.21783*, 2024.
	- Wensheng Gan, Zhenlian Qi, Jiayang Wu, and Jerry Chun-Wei Lin. Large language models in education: Vision and opportunities, 2023.
- **589 590 591** Shahriar Golchin and Mihai Surdeanu. Time travel in llms: Tracing data contamination in large language models, 2024.
- **592 593** Olga Golovneva, Moya Chen, Spencer Poff, Martin Corredor, Luke Zettlemoyer, Maryam Fazel-Zarandi, and Asli Celikyilmaz. Roscoe: A suite of metrics for scoring step-by-step reasoning, 2023. URL <https://arxiv.org/abs/2212.07919>.

648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 KV Aditya Srivatsa and Ekaterina Kochmar. What makes math word problems challenging for llms?, 2024. Gemini Team, Rohan Anil, Sebastian Borgeaud, Jean-Baptiste Alayrac, and Jiahui Yu. Gemini: A family of highly capable multimodal models, 2024. Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, et al. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288*, 2023. Shijie Xia, Xuefeng Li, Yixin Liu, Tongshuang Wu, and Pengfei Liu. Evaluating mathematical reasoning beyond accuracy, 2024. Xin Xu, Tong Xiao, Zitong Chao, Zhenya Huang, Can Yang, and Yang Wang. Can llms solve longer math word problems better?, 2024. An Yang, Baosong Yang, Binyuan Hui, Bo Zheng, Bowen Yu, Chang Zhou, Chengpeng Li, Chengyuan Li, Dayiheng Liu, Fei Huang, et al. Qwen2 technical report. *arXiv preprint arXiv:2407.10671*, 2024. Longhui Yu, Weisen Jiang, Han Shi, Jincheng Yu, Zhengying Liu, Yu Zhang, James T. Kwok, Zhenguo Li, Adrian Weller, and Weiyang Liu. MetaMath: Bootstrap Your Own Mathematical Questions for Large Language Models, May 2024. URL <http://arxiv.org/abs/2309.12284>. arXiv:2309.12284 [cs]. Zheng Yuan, Hongyi Yuan, Chengpeng Li, Guanting Dong, Keming Lu, Chuanqi Tan, Chang Zhou, and Jingren Zhou. Scaling relationship on learning mathematical reasoning with large language models, 2023. Hugh Zhang, Jeff Da, Dean Lee, Vaughn Robinson, Catherine Wu, Will Song, Tiffany Zhao, Pranav Raja, Dylan Slack, Qin Lyu, Sean Hendryx, Russell Kaplan, Michele Lunati, and Summer Yue. A careful examination of large language model performance on grade school arithmetic, 2024a. Yunxiang Zhang, Muhammad Khalifa, Lajanugen Logeswaran, Jaekyeom Kim, Moontae Lee, Honglak Lee, and Lu Wang. Small language models need strong verifiers to self-correct reasoning, 2024b. Lianmin Zheng, Wei-Lin Chiang, Ying Sheng, Siyuan Zhuang, Zhanghao Wu, Yonghao Zhuang, Zi Lin, Zhuohan Li, Dacheng Li, Eric P. Xing, Hao Zhang, Joseph E. Gonzalez, and Ion Stoica. Judging LLM-as-a-Judge with MT-Bench and Chatbot Arena, December 2023. URL [http:](http://arxiv.org/abs/2306.05685) [//arxiv.org/abs/2306.05685](http://arxiv.org/abs/2306.05685). arXiv:2306.05685 [cs]. APPENDIX The dataset and code to run all experiments are provided in this [repository.](https://anonymous.4open.science/r/Exposing-the-Achille-Heel-1D11/) A MWP-MISTAKE DATASET MWP-MISTAKE dataset is curated using 4 different types of well-known datasets. Below are the details of each of the datasets. • SVAMP [Patel et al.](#page-11-7) [\(2021\)](#page-11-7): SVAMP is a MWP dataset created by applying a carefully chosen variations over examples sampled from existing datasets, AsDiv-A [Miao et al.](#page-11-16) [\(2020\)](#page-11-16) and MAWPS [Koncel-Kedziorski et al.](#page-11-17) [\(2016\)](#page-11-17). • GSM-8K [Cobbe et al.](#page-10-4) [\(2021b\)](#page-10-4):GSM-8K is a dataset of diverse grade school math word problems created by human writers, involving basic arithmetic operations. Released in November 2021.

754 755 Across all these simple variations, we observed a performance drop of 10% in GPT-4 and around 6% in GPT-4o, highlighting the sensitivity of these models. Interestingly, fine-tuned models like Llama-3-8B-Finetuned demonstrated greater robustness, with just a 2% performance drop.

Table 7: Mistake Detection Performance (F1 score) on SVAMP dataset with all variations)

Table 8: Max Performance change with introduction of variations on SVAMP dataset.)

808 809

Figure 5: Variations in SVAMP dataset on simple Math Problems [Patel et al.](#page-11-7) [\(2021\)](#page-11-7)

C SLMS REASONING STEPS

SLMs were used to generate chain of thought (COT) reasoning step and final answers for all dataset questions. Each model Llama-2-7b-chat, Mixtral-8x7B, Phi-3-mini where prompted using [Listing 1](#page-13-1) to curate the reasoning step without an answer. If the final answer was incorrect we filtered out the reasoning steps as incorrect. Table [9](#page-15-1) shows examples of SLM incorrect reasoning steps from GSM-8K dataset.

Table 9: Example of incorrect reasoning steps generated using SLM's (GSM-8K dataset)

864 865 D TASK T1 AND T2

915 916 917

```
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
      Task T1 evaluates the model's ability to detect mistakes rectify them and derive the correct answer.
      Listing 2 was used in a few shot settings for task T1.
      1 You are a mathematics educator with a deep understanding of
          elementary and middle school mathematics. You are experienced
          in teaching multi-step problem-solving techniques and have a
          knack for breaking down complex problems into manageable steps
           . Your expertise lies in basic arithmetic operations such as
          addition, subtraction, multiplication, and division. You can
          provide clear, step-by-step solutions to mathematical problems
           that require multi-step reasoning.
     2
      3 You are provided with a mathematical question and a step-by-step
          solution along with it. The solution might have some mistakes.
           Identify if the solution is correct or incorrect. If the
          solution is correct, output the final answer with the help of
          the solution provided. If the solution is incorrect, correct
          the existing solution and determine the final answer with the
          help of the corrected solution.
      Reasoning chain Correct (Yes/No):
      Corrected reasoning chain or NA:
      Final answer (just the number):
                                 Listing 2: Prompt for Task T1
      Task T2 evaulates the model's ability to detect mistake and solve MWP based on the provided
      reasoning step. Listing 3 was used in a few shot setting for task T2. Here we insure that final answer
      is generated with the help of the reasoning steps provided, which may or may not be correct.
      You are a mathematics educator with a deep understanding of
          elementary and middle school mathematics. You are experienced
          in teaching multi-step problem-solving techniques and have a
          knack for breaking down complex problems into manageable steps
           . Your expertise lies in basic arithmetic operations such as
          addition, subtraction, multiplication, and division. You can
          provide clear, step-by-step solutions to mathematical problems
           that require multi-step reasoning.
     2
      You are provided with a mathematical question and a step-by-step
          solution along with it. The solution might have some mistakes.
           Identify if the solution is correct or incorrect and output
          the final answer based on the provided solution.
      Reasoning chain Correct (Yes/No):
      Final answer (just the number):
                                 Listing 3: Prompt for Task T2
      E MODEL USED
      Below are brief details of the models we have used for benchmarking our MWP-MISTAKE dataset.
           1. GPT-4o: GPT-4o is a multimodal model by OpenAI, and it has the same high intelligence
             as GPT-4 Turbo but is much more efficient—it generates text 2x faster and is 50% cheaper.
             Additionally, GPT-4o has the best vision and performance across non-English languages of
```
2. GPT-4: GPT-4 is a large multimodal model by OpenAI that can solve difficult problems with greater accuracy than any of OpenAI previous models, thanks to its broader general knowledge and advanced reasoning capabilities. Last training data: September 2021.

any OpenAI model. Last training data: October 2023.

- 3. GPT-3.5Turbo: GPT-3.5Turbo is a large language model by OpenAI GPT-3.5 that can understand and generate natural language or code and has been optimized for chat using the Chat Completions API but work well for non-chat tasks as well. Last training date: September 2021.
- 4. Claude-3-Opus: Claude-3-Opus is Anthropic's most capable and intelligent model yet, ideal for navigating complex tasks like in-depth analysis, research, and task automation. Last training data: August 2023.
- 5. Llama-2-7b-chat: Llama 2 is a collection of pretrained and fine-tuned generative text models ranging in scale from 7 billion to 70 billion parameters from meta. This is the 7B fine-tuned model, optimized for dialogue use cases. Training date: September 2022.
- 6. Mixtral-8x7B: Mixtral is a Mixture of Experts (MoE) model with 8 experts per MLP, with a total of 45 billion parameters. Despite the model having 45 billion parameters, the compute required for a single forward pass is the same as that of a 14 billion parameter model. This is because even though each of the experts have to be loaded in RAM (70B like ram requirement) each token from the hidden states are dispatched twice (top 2 routing) and thus the compute (the operation required at each forward computation) is just 2 X sequence length.
	- 7. Phi-3-mini: The Phi-3-Mini-128K-Instruct is a 3.8 billion-parameter by microsoft, lightweight, state-of-the-art open model trained using the Phi-3 datasets. This dataset includes both synthetic data and filtered publicly available website data, with an emphasis on high-quality and reasoning-dense properties. Last training data: October 2023.

F CATEGORIES WISE RESULTS

922

Table [10](#page-17-2) shows the F1 score analysis on different types of Rule-based reasoning mistakes on GSM-8K dataset. Furthermore Figure [6,](#page-17-3) [7,](#page-18-1) [8](#page-18-2) and [9](#page-18-3) shows the GPT-4o Mistake detection and Performance F1 score on different type of rule based and SLM based mistakes on GSM-8K, MATH, MATHBENCH andJEEBENCH respectively.

Figure 6: Category Wise mistake detection and performance results on GSM-8K dataset.

Figure 8: Category Wise mistake detection and performance results on MATHBENCH dataset.

1014 1015 1016

999

985

Figure 9: Category Wise mistake detection and performance results on JEEBENCH dataset.

G METEOR AND BERTSCORE RESULTS

1017 1018 1019 1020 1021 BertScore computes a similarity score for each token in the candidate sentence with each token in the reference sentence using the BERT embeddings. Metric for Evaluation of Translation with Explicit Ordering (METEOR) score is a metric that measures the quality of generated text based on the alignment between the generated text and the reference text. The metric is based on the harmonic mean of unigram precision and recall, with recall weighted higher than precision.

1022 1023 1024 1025 Table [11](#page-19-2) and Table [12](#page-19-3) present the BertScore and Meteor Score respectively for all the datasets across all models. We observed that these two metric evaluations where not fully able to capture the nuance capabilities of LLMs in rectifying the mistakes within reasoning steps. This can be seen in the results. GPT-4o has a consistently high performance across all the dataset, but when you compare the BERTScore between the corrected reasoning step and ground truth reasoning step you see the rest of **1026 1027 1028** the models clearly performing better than GPT-4o. GPT-4 has performed better than GPT-3.5Turbo in most datasets.

1029 1030 Table 11: BERTscores for correct and incorrect final answers derived after mistake rectification across all models and datasets.

1038 1039

1040

1043 1044 1045 Table 12: Meteor Score for correct and incorrect final answers derived after mistake rectification across all models and datasets.

1048 1049

H AVERAGE REASONING STEP LENGTH

We noticed that the average word length of rectified reasoning for correct and incorrect for GPT-4o was higher than other models. Table [13](#page-19-4) presents the average word length of the rectified reasoning step for all datasets across the models.

Table 13: Average length of rectified reasoning steps on MWP-MISTAKE dataset

1062 1063 1064

1065 1066 I DATA CONTAMINATION AND MEMORIZATION

1067 1068 1069 1070 1071 Two different types of prompts were used to test out memorization of individual instances of the dataset. The reasoning step was split into two halves, and models were prompted in two different ways (general and guided) to complete the second half of the reasoning step. To detect contamination we evaluated the overlap score between generated and reference instances using ROUGE-L Score. [Listing 4](#page-19-5) and [Listing 5](#page-20-2) shows the prompt used for guided and generation instructions respectively.

¹ You are provided with a full question and the first answer piece from the test split of the GSM8K dataset. Finish the second answer piece of the instance as exactly appeared in the dataset. Only rely on the original form of the instance in the dataset to finish the second answer piece. Output only the second answer piece.

1078 1079

Listing 4: Guided instruction for dataset GSM8K

 piece.

Here GSM-8K and test are the extra information provided for the model to uniquely identify instances from the source dataset and complete the reasoning step.

Listing 5: General instruction for dataset GSM8K

Based on the provided question, finish the second answer piece based on the first answer piece, such that these two pieces become a single instance answer. Output only the second answer

 Table [14](#page-20-3) presents the complete result for the average ROUGE-L score of guided and general for all datasets across all models.

Table 14: Rouge L score between guided and general instructions on MWP-MISTAKE dataset

J OPENAI O1 MODEL ANALYSIS

 Table 15: Performance of o1 vs GPT4o on 120 sample questions from JEEBENCH with MWP-MISTAKE

K RUNNING EXPERIMENT MULTIPLE TIMES

 While running experiments on all models (LLMs and SLMs) we used the default hyperparameters to generate tokens. We ran a subset of the dataset on different prompt variations and saw comparable performance for various prompts. Due to the limitation of the API key, we were only able to run GPT-4o model on the GSM-8K dataset. On rerun we got very similar results, with an error rate of \le 0.01.

L OUTPUT FROM EACH MODEL

 The raw output of each model has been provided in this [repository.](https://anonymous.4open.science/r/Exposing-the-Achille-Heel-1D11/) Additional details are present in the README.md file of the repository.

-
-
-
-
-
-
-