The Great Replacement : LLM-bot replacing TAs

Anthony Kalaydjian | 370837 | anthony.kalaydjian@epfl.ch
Anton Balykov | 368883 | anton.balykov@epfl.ch
Eric Saikali | 326450 | eric.saikali@epfl.ch
ShAIkerspear

Abstract

TODO

1 Introduction

Large Language Models (LLMs) have shown the beginning of a revolution in many sectors, with the advent of closed source models such as ChatGPT which was just integrated in the Apple's Apple Intelligence system, Claude as well as open source alternatives such as Mistral AI's models or Meta's LLAMA. As time passes, the performance of these models and their range of skills increases. As such, multi-modal models and API-augmented models are starting to surge in our phones with better voice assistants and computers with coding assistants, as well as in other tools.

Nonetheless, one sector that lacks behind when it comes to LLM integration is education. Even though LLMs are getting better and better, they have yet to match proper professor/expert level in some education fields, especially in science, technology, engineering, and math (STEM) related domains. But, as for the other sectors, having educative LLMs could heavily reduce the resources required for teaching and improve it by enabling students to access a 24/7 tutor in the palm of their hands.

In this optic, this paper focuses on creating a language model specialized in answering EPFL MCQA exam questions. Question answering is one of the most used ways of interacting with a LLM system and has been democratized with the appearance of systems such as ChatGPT, Gemini etc. Although these models are able to provide coherent answers most of the time, this task remains challenging. And it is even more so when the questions deal with science as they usually require some sort of reasoning on the question and specific knowledge. This is the case that is tackled here as the main goal is to create a system that answers STEM related MCQAs.

The approach of this project revolves around 3 main parts. The first part tackles data collection, with the generation of a custom DPO training set from synthetically generated answers to EPFL exam question which have been evaluated by EPFL students, as well as carefully selected available SFT and DPO datasets. These additional datasets facilitated model's fine-tuning as they have different distributions and provide wider range of information to train on. The second part tackles the fine-tuning of the Phi-2 model according to a well defined strategy. After the training, the last part deals with evaluating the performance of the trained model when compared to a baseline.

As the Phi-2 model is quite big one and takes a lot of space both for storing and during inference, an approach to reduce its size (named quantization) was chosen as a way to mitigate this issue. This way model would become smaller and faster, allowing its usage on more devices.

2 Related Work

Different question answering LLMs and systems have been developed throughout the last couple of years. Some of them try to specialize in a particular domain such as Codellama (Rozière et al., 2024) which focuses on code generation or Meditron (Chen et al., 2023) which specializes in medical question answering while others remain general such as GPT3 (Brown et al., 2020). In this work, the goal is to train a model to answer MCQAs which cover a relatively broad gamut of fields.

Choosing to have a specialized or a more general purpose LLM yields to make a choice between having a model that performs better on a very specific task, but poorly on others or having a model that performs well on any task but has lower performance when compared to the former on its specialization field. In this matter works have shown how to strike a balance between the two (Zhang et al., 2023) and inspire the design choices that will be

made here to yield a model capable of answering a wide range of STEM questions. In this matter, the model will be trained on both general STEM MCQAs as well as more domain specific (Maths in this case) ones.

Given a specific task with a dataset, (Yigit and Amasyali, 2023) shows that first training sequentially on different datasets that encounter the same task before training on the target dataset yields better results than simply training on the target dataset.

Pairing therefore the data balancing from (Zhang et al., 2023) with the sequential training from (Yigit and Amasyali, 2023) seems to be an interesting approach whose results will be assessed against other paradigms.

For instance, Meditron (Chen et al., 2023), which is a model developed for answering medical questions, was trained in a similar manner, on a broad variety of medical MCQA datasets with different scales and granularities. This model has good results on many medical benchmarks and this means that the approach that was chosen for the current project was already expoited and resulted in a well-performing LLM.

Furthermore; by introducing, for each question, the correct answer as well as a explanation of the answer in the training prompt, the model is expected, at inference time, to use a Chain of Thought reasoning approach (Zhang et al., 2022) to yield its answer which has been proven to improve the model's accuracy.

3 Approach

3.1 Model architecture

Phi-2 (Hughes, 2023) is a transformer based model with next-word prediction objective. It has 2.78B parameters, a context length of 2048 tokens and has been pretrained on 1.4T tokens. The Phi-2 Model architecture consists of several layers, with first an embedding of the tokens going from an a one hot encoding of 51,200 tokens to a vector space of dimension 2,560. This is followed by a succession of 32 decoding layers consisting of self attention modules of same input/output dimension with the addition of rotational embedding which make computations more efficient. This is followed by an MLP with GeLU activations and the following layer sizes : 2560 - 10240 - 2560. The model is completed by a linear head.

The base model has been pretrained on the data on which its predecessors Phi-1.5 and Phi-1 were trained, consisting of subsets of Python codes from The Stack v1.2 (Kocetkov et al., 2022), Q&A content from StackOverflow, competition code from *code_contests* (Li et al., 2022), and synthetic Python textbooks and exercises generated by gpt-3.5-turbo-0301. The training dataset was 250B tokens long consisting of combined NLP synthetic data created by GPT-3.5, and filtered web data from Falcon RefinedWeb (Penedo et al., 2023) and SlimPajama (Shen et al., 2024), both assessed by GPT-4.

3.2 Training architecture

For fast and efficient training purposes, the Transformer Reinforcement Learning library from HuggingFace (von Werra et al., 2020) was used. It allows to define a complex and robust training procedure, utilizing modern training techniques. The base phi-2 model was fine-tuned using LoRA (Hu et al., 2021) with a peft (pef, 2023) adapter, which allow to only train specific layers of the model with low rank approximations matrices to update the weights, which significantly reduces memory consumption and training time.

The LoRA adapter is used with rank 16, $\alpha = 16$ and a dropout of 5% (according to (Hu et al., 2021), these values are reasonable for having much less trainable parameters while still being able to train the model to have reasonably good performance). As a result, the only part of the model that needs to be saved is the adapter itself, which reduces the size of the checkpoint and accelerates transfer times.

3.3 Training Strategy

As stated in section 2, the main training strategy revolves on sequentially training the model on various datasets, going from the most general to the most specific one.

The training consists of two different modes:

Supervise Fine Tuning (SFT) Trains the model to generate proper answers with given reference answers. The mean squared error (MSE) is the loss used here.
$\mathrm{L}(\hat{y}, y) = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$

Direct Preference Optimization (DPO) Aligns the model to human preference, by training it to prefer the better answer between annotated pairs for a given question. As seen in the following DPO objective, the training modifies the parameters θ in order to increase

the policy the model would give to the better answer while reducing the one of the worse.

$$\mathrm{L}(\pi_\theta; \pi_{ref}) = -E_{(x,y_w,y_l)\sim\mathcal{D}}\left[\log\sigma\left(\beta\log\frac{\pi_\theta(y_w|x)}{\pi_{ref(y_w|x}} - \beta\log\frac{\pi_\theta(y_l|x)}{\pi_{ref}(y_l|x)}\right)\right]$$

Each dataset is associated to one of the two modes. When training on a given dataset, the associated training is performed.

3.4 Quantization

Once trained, the best model will be quantized using the BitsAndBytesConfig from the transformers library in order to reduce its size while keeping most of its performance. The quantization's degree will be assessed by comparing the performance/size ratio with different quantization amounts. The best one will be kept.

4 Experiments

4.1 Data

Fine-tuning the base model was experimented on multiple and diverse datasets, for both Supervised Fine Tuning (SFT) and Direct Preference Optimisation (DPO). These datasets were first processed to reach a consistent format all across.

- The DPO json lines file has the following format ["prompt", "rejected" "choosen"].
- The SFT json lines file has the following format ["id", "subject", "question", "answer" and "answer_text", "choices"].

The *answer_text* and *subject* fields help to store the explanations and subjects of their questions, allowing to improve the answer generation step by adding step by making the model use a step by step reasoning scheme. The *choices* field is also preserved to keep track of the gold answer.

The datasets experimented on for training are the following :

- EPFL dataset : A collection of around 20K/30K preference data pairs, split into two subsets.
  - **EPFL_SFT** : 40% of the *chosen* field of the EPFL data used for SFT training in order to accommodate the model to the distribution of inputs it will infer on.
  - **EPFL_DPO** : used for DPO training, which was processed by keeping 60% of all DPO pairs.
- **MathQA** (SFT) (Aida Amini and Hajishirzi, 2019) : Used to fine tune the model to reason and to answer STEM (science, technology, engineering, and math) questions. Formatting this dataset is straight forward except for retrieving the *answer_text* as a formatted answer ("Answer : <letter>") is not consistently used. The answer was still retrieved by splitting the text properly and using RegEx.
- **helpSteer** (DPO) (Zhilin Wang, 2023) : Aimed at aligning the model to become more helpful, factually correct and coherent.
- **OpenBookQA** (or OpenQA) (SFT) (Todor Mihaylov, 2018): Used to train the model to answer open-domain questions.
- **ScienceQA** (SFT) (Lu et al., 2022): Used to train the model on more general STEM questions.
- **tal_scq5k** (SFT) (TAL, 2023) : Also used to fine tune the model to reason and to answer STEM questions on a mathematical point of view.
- **all_mcqa** (SFT) : A dataset containing all of the data entries from the previous SFT datasets but this time shuffled.
- **balanced_merged** (SFT) : the all_mcqa but balanced to have the same proportion of answer classes (A,B, C or D).

For testing, the MMLU (Hendrycks et al., 2021) dataset was used as well for further evaluation. It has been processed to have the normalized SFT format.

In addition, the longest data-points (>512 tokens) were removed from all datasets to accelerate training and reduce memory consumption, as most samples (>90%) contain less than 512 tokens. The datasets were also randomly sub-sampled to reduce further their size and accelerate training. Datasets with less than 20k datapoints are kept as is while the ones with more datapoints are clipped to have a 20k datapoints size.

All of these datasets were split into train/test_overfit/test_comparison/test_quantization datasets with a proportion of 50%, 25%, 10%, 15% per dataset respectively.

Further considerations of the data, is about its usage, while all datasets being used are free of use, the usage of the EPFL dataset present some ethical repercussion as this data might consist of re-used

exam questions which might therefore contains answer. direct access to this dataset and its usage could compromise the veracity of a quiz grade.

4.2 Preliminary training results

A few models were trained based on different training data compositions:

① The base model trained successively on all of the datasets without modification. With a number of trained epochs of: [2, 2, 3, 1, 2]

② The base model trained on the same dataset list without Helpsteer. Number of trained epochs: [2, 2, 4, 3]

③ Same as model 2 but clipping the EPFL datasets to only keeping 2 answers for each DPO question to control the number of appearances of each question. Number of trained epochs: [2, 2, 4, 5]

The base model is the original pretrained Phi-2 model.

For this phase, no additional context information was used. The answer only comprised of the letter answer itself.

Data	EPFL_DPO	EPFL_SFT	HelpSteer	MathQA	OpenQA
①	0,4767	0,5082	0,4596	0,2657	0,7133
②	0,4793	0,5089	0,4686	0,2587	0,72
③	0,4841	0,5023	0,4641	0,2652	0,72
base	0,2225	0,1852	0,3318	0,2624	0,72

Table 1: Test results

The results from table 1 are not great in most test datasets except for OpenQA. Although the trained model barely reaches around 50% accuracy on the EPFL_DPO and EPFL_SFT evaluations, it still shows massive improvements when compare to the base model which got very poor results.

On the other hand, it seems like the model wasn't able to properly learn from the MCQA task. This may be due to two factors. First, the fact that context and answer explanation wasn't yet fed into the model and second, that DPO training might confuse the model and make it forget about its previous SFT training on MCQA datasets.

4.3 Further training

Given the insights of the first training phase, it is clear that the crux of the matter lies both on the data's nature as well as on the step at which DPO is performed.

Taking these in consideration, the data has been modified and a few other models were trained with the inclusion of proper explanations in the input prompt. The format used for training is the following:

Question ... ### Explanation ... ### Answer ...

The chosen training data configurations are the following:

④ The base model trained successively on all of the datasets without modification. With a number of trained epochs of: [2, 2, 3, 1, 2]

⑤ The base model trained on the same dataset list without Helpsteer. Number of trained epochs: [2, 2, 4, 3]

⑥ Same as model 2 but clipping the EPFL datasets to only keeping 2 answers for each DPO question to control the number of appearances of each question. Number of trained epochs: [2, 2, 4, 5]

4.4 Evaluation method

Evaluation is assessed on the MCQA datasets by computing the accuracy of each model on the validation set. For the preference data, accuracy of choosing the preferred alternative is used.

4.5 Baselines

The finetuned and compared models have been compared in parallel with the untrained initial model, Phi-2.

4.6 Experimental details

Report how you ran your experiments (e.g. model configurations, learning rate, training time, etc.)

4.7 Results

Report the quantitative results that you have found so far. Use a table or plot to compare results and compare against baselines. Comment on your quantitative results. Are they what you expected? Why do you think that is? What does that tell you about your approach?

5 Analysis

Your report can include qualitative evaluation. You should try to understand your system (e.g. how it works, when it succeeds and when it fails) by inspecting key characteristics or outputs of your model.

Types of qualitative evaluation include: commenting on selected examples, error analysis, measuring the performance metric for certain subsets

of the data, ablation studies, comparing the behaviors of two systems beyond just the performance metric, and visualizing attention distributions or other activation heatmaps.

6 Ethical considerations

From an ethical point of view, a generator model like the one described above has multiple vulnerabilities imposed upon its stakeholders. These are EPFL students accessing the model, professors and online services. Some threats and attacks are: allowing for repudiation that an exam answer is generated by the model would disable teacher to identify cheating, this renders authenticity obsolete. It could also harm people by compromising the outputs' integrity as they are not sanitized and could have discriminatory biases or incorrect answers. As the model is fine-tuned on course data, malicious people could query help for performing cyber-attacks like denial of service resulting in a breach of availability. It could also breach confidentiality by revealing re-used confidential questions in exams. These attacks are severe as they compromise the legitimacy of a diploma. To mitigate most issues, a second model could be used to check for both harmful inputs and model outputs, and not show the latter when it concerns sensible content. Further vulnerabilities of this model giving potential or malicious prompts which upon question-answering could tamper with a person's, or entity's preservation like "How to create a bomb?". Other, could be cultural bias induced by the fine-tuning of the model toward one defined truth or even generation of incorrect information and hallucinations.

7 Conclusion

- Somehow achievable for answering questions on a 2.8 billion model - Easier to achieve on general questions - Learns how to answer a bit more STEM oriented questions - Balanced data is key for training - Manage to get an impressive score on MMMLU compared to initial phi-2 model and improved on the others from up to 2% !

- How to quantize - How to finetune - LoRA usage - High volume data training and testing - Handle limited ressources (In the sence of torch.cuda.OutOfMemoryError) - Optimize timewise operations to ensure direct runs (through simplistic tests and small runs (data of only 10 lines).

- Timewise limitations for good training. - scitas cluster's ressource limitations to run bigger model

Summarize the main findings of your project, and what you have learned. Highlight your achievements, and note the primary limitations of your work. If you like, you can describe avenues for future work.

References

2023. State-of-the-art parameter-efficient fine-tuning (peft) methods.

Shanchuan Lin Rik Koncel-Kedziorski Yejin Choi Aida Amini, Saadia Gabriel and Hannaneh Hajishirzi. 2019. Mathqa.

Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeffrey Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. 2020. Language models are few-shot learners.

Zeming Chen, Alejandro Hernández Cano, Angelika Romanou, Antoine Bonnet, Kyle Matoba, Francesco Salvi, Matteo Pagliardini, Simin Fan, Andreas Köpf, Amirkeivan Mohtashami, Alexandre Sallinen, Alireza Sakhaeirad, Vinitra Swamy, Igor Krawczuk, Deniz Bayazit, Axel Marmet, Syrielle Montariol, Mary-Anne Hartley, Martin Jaggi, and Antoine Bosselut. 2023. Meditron-70b: Scaling medical pretraining for large language models.

Dan Hendrycks, Collin Burns, Steven Basart, Andy Zou, Mantas Mazeika, Dawn Song, and Jacob Steinhardt. 2021. Measuring massive multitask language understanding.

Edward J. Hu, Yelong Shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, and Weizhu Chen. 2021. Lora: Low-rank adaptation of large language models.

Alyssa Hughes. 2023. Phi-2: The surprising power of small language models.

Denis Kocetkov, Raymond Li, Loubna Ben Allal, Jia Li, Chenghao Mou, Carlos Muñoz Ferrandis, Yacine Jernite, Margaret Mitchell, Sean Hughes, Thomas Wolf, Dzmitry Bahdanau, Leandro von Werra, and Harm de Vries. 2022. The stack: 3 tb of permissively licensed source code.

Yujia Li, David Choi, Junyoung Chung, Nate Kushman, Julian Schrittwieser, Rémi Leblond, Tom Eccles, James Keeling, Felix Gimeno, Agustin Dal Lago, Thomas Hubert, Peter Choy, Cyprien de Masson d'Autume, Igor Babuschkin, Xinyun Chen, Po-Sen Huang, Johannes Welbl, Sven Gowal, Alexey

Cherepanov, James Molloy, Daniel J. Mankowitz, Esme Sutherland Robson, Pushmeet Kohli, Nando de Freitas, Koray Kavukcuoglu, and Oriol Vinyals. 2022. Competition-level code generation with alphacode. *Science*, 378(6624):1092–1097.

Pan Lu, Swaroop Mishra, Tony Xia, Liang Qiu, Kai-Wei Chang, Song-Chun Zhu, Oyvind Tafjord, Peter Clark, and Ashwin Kalyan. 2022. Learn to explain: Multimodal reasoning via thought chains for science question answering.

Guilherme Penedo, Quentin Malartic, Daniel Hesslow, Ruxandra Cojocaru, Alessandro Cappelli, Hamza Alobeidli, Baptiste Pannier, Ebtesam Almazrouei, and Julien Launay. 2023. The refinedweb dataset for falcon llm: Outperforming curated corpora with web data, and web data only.

Baptiste Rozière, Jonas Gehring, Fabian Gloeckle, Sten Sootla, Itai Gat, Xiaoqing Ellen Tan, Yossi Adi, Jingyu Liu, Romain Sauvestre, Tal Remez, Jérémy Rapin, Artyom Kozhevnikov, Ivan Evtimov, Joanna Bitton, Manish Bhatt, Cristian Canton Ferrer, Aaron Grattafiori, Wenhan Xiong, Alexandre Défossez, Jade Copet, Faisal Azhar, Hugo Touvron, Louis Martin, Nicolas Usunier, Thomas Scialom, and Gabriel Synnaeve. 2024. Code llama: Open foundation models for code.

Zhiqiang Shen, Tianhua Tao, Liqun Ma, Willie Neiswanger, Zhengzhong Liu, Hongyi Wang, Bowen Tan, Joel Hestness, Natalia Vassilieva, Daria Soboleva, and Eric Xing. 2024. Slimpajama-dc: Understanding data combinations for llm training.

TAL. 2023. Tal-scq5k. Github repository of the dataset.

Tushar Khot Ashish Sabharwal Todor Mihaylov, Peter Clark. 2018. Can a suit of armor conduct electricity? a new dataset for open book question answering.

Leandro von Werra, Younes Belkada, Lewis Tunstall, Edward Beeching, Tristan Thrush, Nathan Lambert, and Shengyi Huang. 2020. Trl: Transformer reinforcement learning. `https://github.com/huggingface/trl`.

Gulsum Yigit and Mehmet Fatih Amasyali. 2023. Enhancing multiple-choice question answering through sequential fine-tuning and curriculum learning strategies. *Knowledge and Information Systems*, 65(11):5025–5042.

Zheng Zhang, Chen Zheng, Da Tang, Ke Sun, Yukun Ma, Yingtong Bu, Xun Zhou, and Liang Zhao. 2023. Balancing specialized and general skills in llms: The impact of modern tuning and data strategy.

Zhuosheng Zhang, Aston Zhang, Mu Li, and Alex Smola. 2022. Automatic chain of thought prompting in large language models.

Jiaqi Zeng Virginia Adams-Makesh Narsimhan Sreedhar Daniel Egert Olivier Delalleau Jane Polak Scowcroft Neel Kant Aidan Swope Oleksii Kuchaiev Zhilin Wang, Yi Dong. 2023. Helpsteer: Multi-attribute helpfulness dataset for steerlm.

A Appendix (optional)

If you wish, you can include an appendix, which should be part of the main PDF, and does not count towards the page limit. Appendices can be useful to supply extra details, examples, figures, results, visualizations, etc., that you couldn't fit into the main paper. However, your grader does not have to read your appendix, and you should assume that you will be graded based on the content of the main part of your paper only.