Unraveling LLMs: Understanding Their Strengths, Challenges, and Future

In this blog, we are going to deep dive into LLMs, which are the heart of models like ChatGPT and Gemini, etc. The main thing we are going to discuss is the psychology of LLMs—the areas where they excel and lack confidence. Here, we are talking about the pretraining of these models, the tokenization used and the problems faced in that, post-training, and other aspects of the lifecycle of these LLM models.

Topics:

1. Introduction:

LLM, or Large Language Models, are a type of artificial intelligence program that can recognize and generate text like humans do. These models are trained on huge datasets, hence the name "Large." These models are mainly built for understanding and recognizing human data. They are trained on a huge amount of data gathered from the internet, amounting to thousands of gigabytes.

LLMs have a huge scope in the field of machine learning, deep learning, and data science, which are subfields of AI. Large Language Models (LLMs) are AI systems that use deep learning, a subset of machine learning, to process and generate human-like text. They rely on neural networks, particularly transformer models, which help them understand language context through self-attention mechanisms. This allows LLMs to respond to natural language queries flexibly, unlike traditional rule-based programs. However, their accuracy depends on the quality of the data they are trained on, and they sometimes generate incorrect or biased information, a phenomenon known as hallucination. Additionally, LLMs pose security risks, such as exposure of confidential data, and can be manipulated through malicious inputs.

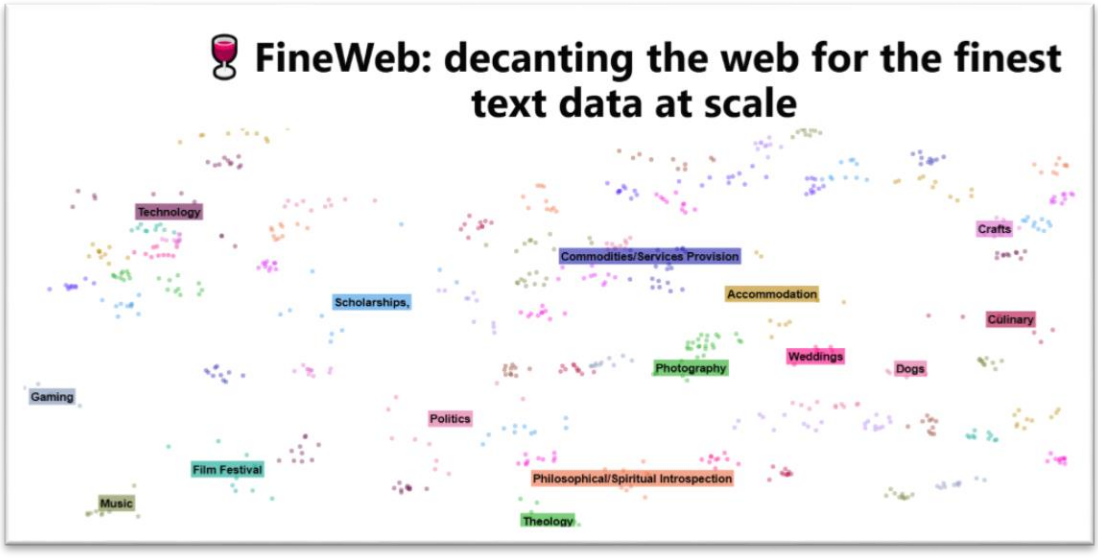
2. Pre training:

What is pretraining?

As we all know, before we use a model, it has to be trained on some data. But in this case, it is not just "some" data—it is *large*. Yes, these models are trained on a huge amount of data. Pretraining is the initial stage of training, where the model learns the patterns and structure of language.

Many factors come into play during this training process. As we know, in machine learning, we have supervised, unsupervised, and reinforcement learning. Similarly, these training approaches are used in LLMs as well. The concepts remain the same, but here, the data is primarily text-based and sequential.

.Here I want to mention about the FineWeb Dataset. This is the PreTraining Dataset from Hugging Face.



The main X-factor behind the working of state-of-the-art models is their pretrained data. Models perform better when the data is both vast and high-quality. This fine web data is enormous, consisting of 15 trillion tokens and occupying 44TB of disk space. In addition to FineWeb, it includes FineWeb-Edu, a specialized subset designed with educational value in mind. FineWeb-Edu has been tested against popular educational benchmarks like MMLU, ARC, and OpenBookQA, consistently outperforming other open web datasets. To enhance accessibility, it is available in two versions: 1.3 trillion tokens for those seeking highly focused educational content and 5.4 trillion tokens for a broader, high-quality educational dataset.

2. Tokenization:

You know that machines can't recognize words or letters, right? To solve this problem, we use tokenization, a powerful method that converts words or letters into numbers, including special characters, symbols, and emojis.
Now that we understand what tokenization is, did you know that tokenization is not just of one type or that it doesn't always work the same way? Instead of diving into different types of tokenizers, we will focus on how it works in different LLM models. To test this, I am using TickTokenizer.

Text: "The cost was $19.99—nearly ⅓ of my budget! □"
This is the text lets check how this is converted to numbers with different models

1. GPT 3.5 Turbo

Here we can see that there are almost 10 words with emoji's in the text and the text is converted in to text as 20 tokens where the leading space are taken along with the words, and these are the word tokenizers.

2. GPT 4.O

Here It becomes Intresting previously we had used GPT 3.5 Turbo and now GPT 4.O and clearly we can see the difference below.

Now here we can see that for the same text we have used in both the cases but the token size it took are different. Even though the token size has not much difference. It is more impact when the size of the data is very large. The choice of an LLM helps us in saving our memory and also the fast computation power.

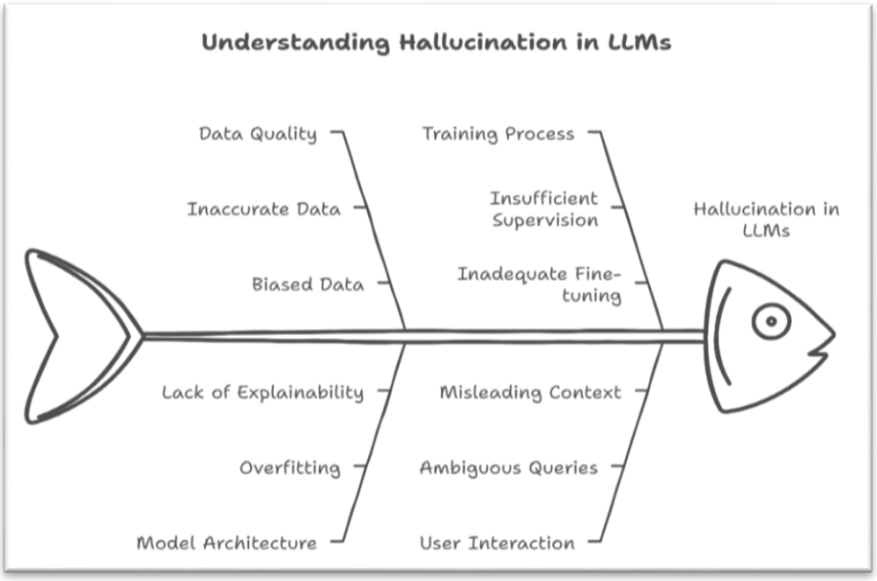
3. Post Trainig:

Post-training is a crucial step in training LLM models that follows pretraining. During pretraining, a massive amount of raw data is used, making the process highly memory-intensive and time-consuming. Once pretraining is complete, post-training is performed to refine the model and improve its accuracy. This stage mainly involves human-labeled data, which helps enhance the model's performance, correctness, and alignment with human expectations.
Eg:Human: What is 2+2?
Assistant: 2+2=4
Human: What if it was '*' instead of '+'?
Assistant: 2*2=4, same as 2+2!

this is the dataset which created by the human experts and the training of the model is based on this data. But one intresting thing is, these kind of data's are now created by the LLM's it self. The Human experts are using the models such as UltraChat. This is the easy method where the huge datasets can be prepared in less amount of time.

4. Hallucination:

One of the biggest challenges with Large Language Models (LLMs) is a phenomenon called hallucination, where the AI generates false or misleading information that sounds completely believable. Since LLMs don't actually "know" facts but rather predict words based on patterns, they sometimes produce content that isn't real.



LLMs can sometimes hallucinate, generating false but convincing information due to their reliance on pattern recognition rather than verified facts. This happens when the AI encounters gaps in knowledge, leading it to fill in missing details with guesses. It can also result from overgeneralization, where the model applies learned patterns incorrectly, or unclear prompts that cause it to fabricate details. Unlike search engines, LLMs lack real-time fact-checking, making them prone to errors in areas like research, history, or even legal and medical advice. To minimize hallucinations, it's crucial to fact-check AI responses, use models that retrieve live data, and train them on high-quality sources. As AI continues to evolve, reducing hallucinations remains a key challenge, ensuring that these models become more accurate and trustworthy.

5. Knowledge of the self:

This is what knowledge know about it self. Ie which model it is and who build it.when we ask these kind of questions models are tend to hallucinate like it was built by OpenAI. This can be reduced by overwriting or explicitly programming these kinds of questions.

Let us go into some topics like Models need tokens to think. This means that while asking questions we can ask model to give us answer in a single token or it can use unlimited tokens to answer. When we ask for single it will give us only a single answer and ask for unlimited it is not restricted by the use of tokens so we it will use as much as tokens it requires but here the answers are generated by guessing or using its knowledge. To get a required answer we can also ask the models to use the code and answer the question accordingly.

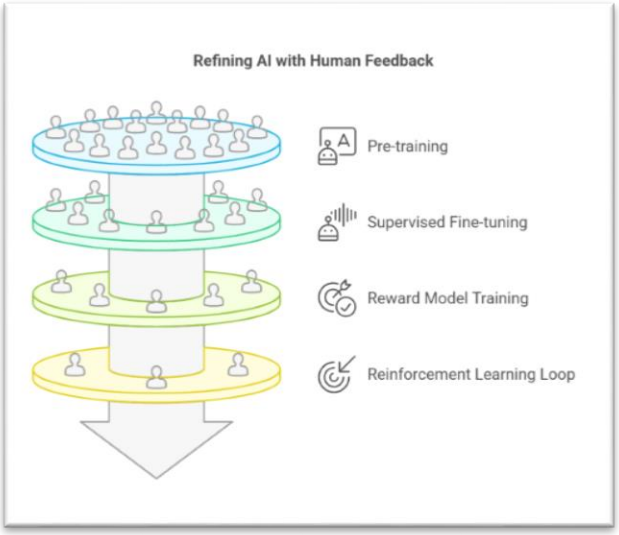
6. Reinforcement Learning:

Reinforcement Learning (RL) is a machine learning technique where an AI model learns by interacting with an environment and receiving rewards or penalties based on its actions. In Large Language Models (LLMs), RL enhances performance by optimizing response generation. The process begins with initial training, where the LLM is pre-trained on vast datasets using deep learning. Next, the agent-environment interaction allows the model to generate responses, which are evaluated by a reinforcement learning system.

A reward system then assigns positive reinforcement for useful responses and penalties for incorrect or undesirable ones. Over time, the model undergoes optimization, adjusting its outputs based on past rewards to improve performance. RL is crucial in LLMs as it optimizes response quality, helping the model learn better responses over time, increases adaptability by enabling dynamic responses to different prompts, and enhances decision-making by allowing AI to make context-aware choices rather than relying purely on static training data.

7. Reinforcement Learning with Human Feedback:

Reinforcement Learning with Human Feedback (RLHF) in LLMs is a specialized form of RL where human reviewers evaluate AI-generated responses and provide feedback to guide the model toward more useful and ethical outputs. This approach enhances how LLMs align with human preferences and societal values. The process begins with pre-training on vast datasets, followed by supervised fine-tuning, where human reviewers label correct responses to help the AI recognize high-quality answers.



Next, a reward model is trained to predict the quality of AI responses based on human feedback. Finally, the model undergoes a reinforcement learning loop, optimizing responses using human-labeled rewards. Reinforcement Learning from Human Feedback (RLHF) is crucial for LLMs as it reduces bias and toxicity, preventing harmful outputs; improves alignment with human intent, ensuring ethical and socially acceptable responses; and enhances user experience by making interactions more natural, context-aware, and valuable.

8. Conclusion

Large Language Models (LLMs) like GPT and Gemini represent a groundbreaking shift in AI-driven text generation, but their capabilities come with complexities. From pretraining on vast datasets to tokenization and post-training refinement, each stage plays a crucial role in shaping their performance. However, challenges such as hallucination and self-knowledge limitations highlight the need for continuous improvements. Reinforcement Learning and RLHF have emerged as effective techniques to enhance model accuracy, ethical alignment, and user experience. While LLMs are powerful tools, their responsible use requires careful oversight, high-quality training data, and fact-checking mechanisms. As AI continues to evolve, refining these models will be key to making them more reliable, efficient, and beneficial for real-world applications.