Generative AI with LLM

(General purpose technology)

→ useful for different application. (LLM)

→ Generative AI is subset of Machine learning, learned their ability by finding statistical pattern in massive datasets (human)

LLM

→ GPT → LLAMA
→ Bert → PALM
→ Flan-T5 → BLOOM

(more parameter & more sophisticated task.)

Transformer Model → Neural Network that learns context & tracking relationship in sequential data.
(foundation Model)

LLM use cases & tasks

(Next word prediction is basic task)

→ Essay writer → code AI
→ summarize → Entity Extraction. (word classification)
→ Translate → External API

Smaller Model can be fine tuned to perform well on specific focussed tasks.

LLM capability → Architecture powers them

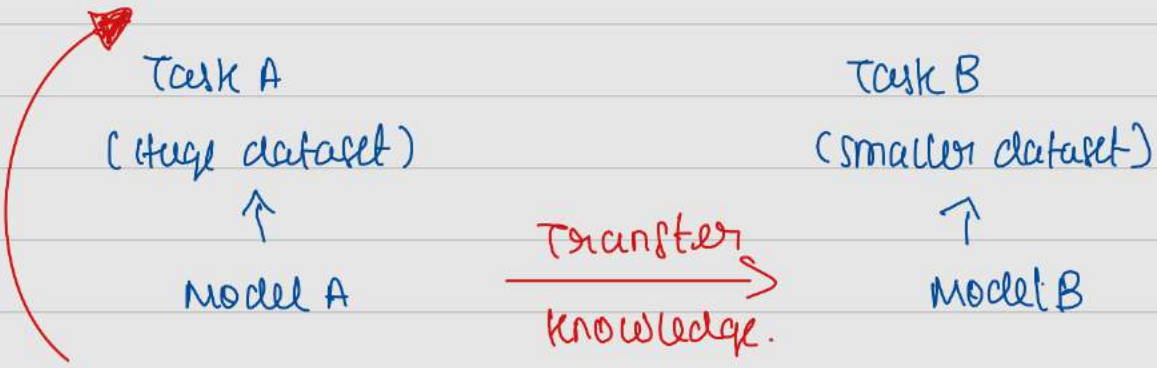
understanding language can be challenging., language is complex single word has multiple meaning. (homonyms)

Previous generation of language model made use of 'RNN'

Self-Supervised learning:

type of training in which the objective is automatically computed from inputs of the model. Means that humans are not needed to label the data.

Transfer learning



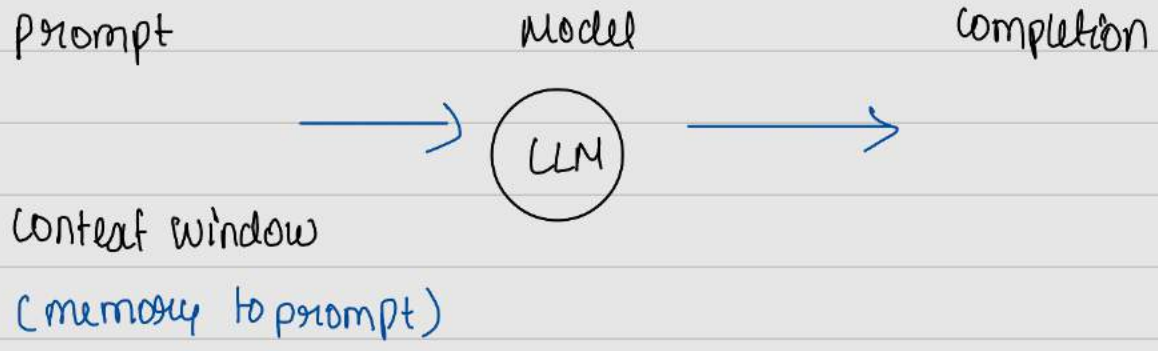
Act of initializing a model with another model's weight

Training from scratch requires more data and more compute to achieve comparable results.

Transformer model are built with special layer called Attention layer

Fine-tuning

* Full fine tuning
* parameter efficient fine tuning (PEFT)



Inference : using Model to generate text.

Generating text : RNN

RNN is limited by the amount of compute & memory.

then, transformer Architecture had arrived -> 'Attention is all you need'
(Attention to input meaning)

"Attention is All you Need" -> by Google in 2017.

-> Neural Network Architecture replaces the RNN / CNN with attention based mechanism.

-> encoder & Decoder, Multi-head self attention mechanism layers. & feedforward NN

-> it uses self attention to capture input sequence. capture long term dependencies

Transformer

-> learn the relevance & context in all the word in the sentences. and apply attention weights. (attention map -> each word with every word)

Model process the Number not the text.

Word Embedding.

↳ technique where individual words are represented as real valued vectors in a lower-dimensional space and captures inter word semantics.

Langchain

Document Loaders → Text Splitters → Embedding Models → [Number] → Vector Stores

langchain Agents

- → RetrievalQA Chain
- → SQL Database Chain
- → SearchAPI

→ Knows which tool to use

Output parsers → response from LLM follow certain format.

Generative Models ?

Learns patterns and distribution in unstructured Data. So, Reinforcement learning through human feedback is also applied.

LLM → transformer, a type of Neural Network architecture.

language Model

↳ A language Model is a Model which understands language more precisely how words occur together in Natural language, A language Model is used to predict what word comes Next.

temperature = 0 } argmax sampling.

lower temperature means less randomness, vice versa.

top-p (Nucleus sampling)

↳ It controls how many random results should be considered for completion as per the temperature

Generative AI project life-cycle

(Own)

1. foundation Model | pre-training Model (decision)
2. fine-tuning - custom data.

Self Supervised learning to optimize these Models.

Issue with RNN for Generative part is, understanding language can be challenging (homonyms)

then transformer architecture has arrived → increases the performance of Natural language task.

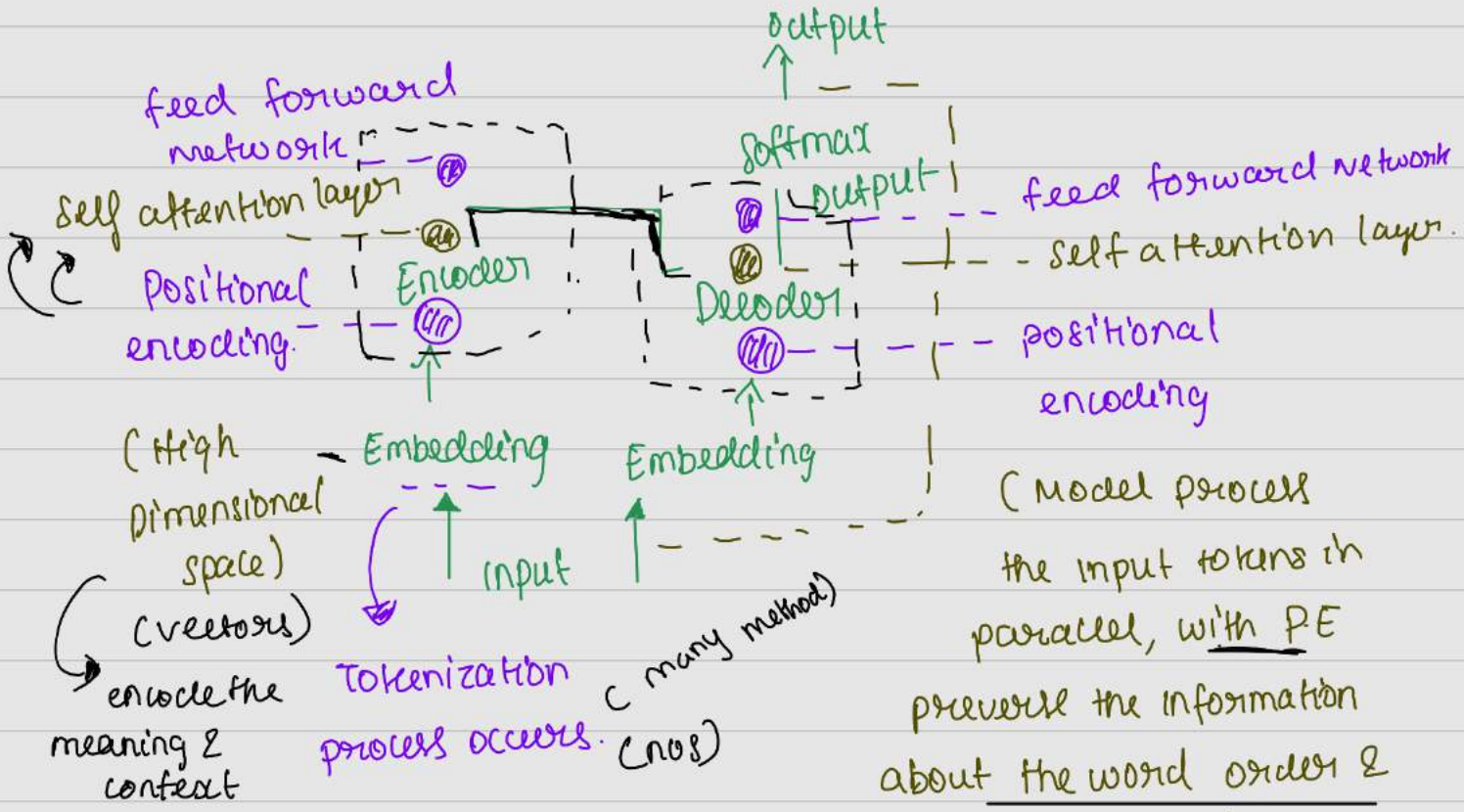
→ Scale efficiently
→ parallel process
→ Attenuation to input meaning.

(Self-attention)

power of transformer architecture, its ability to learn the relevance and context of all of the words in a sentence, every other word in a sentence. (Attention Map)

Apply attenuation weights to relationship for relvance of each word to other word.

Transformer



Self attention, model analayze the relationship between the tokens in the input sequence.

layer's weights are stored.

↓

(Reflects the importance of each word in the input sequence)

↳ to capture the contextual dependencies between the words

transformer has Multi-headed self attention (12-100)

means that multiple sets of self-attention weights / heads are learned in parallel independently of each other.

1. Realtionship 2. Activity 3. other properties

Each self-attention head will learn different aspects of language, weights of each head is randomly initialized.

output is processed through feed forward network, proportional to probility score for every token then passed to Softmax layer → P(E) for each word. (Higher)

Language Model

What should be the next words == word with highest probability.

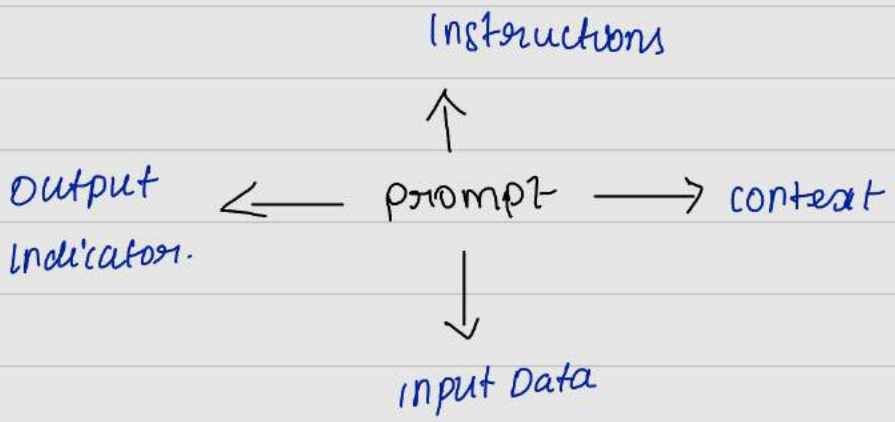
Given a sequence of words

$x_1, x_2, \ldots x_t$

compute the probability of the next word

$$p(x_{t+1} \mid x_1, x_2, \ldots, x_t)$$

LLM → trained on huge amount of data.



Zero-shot prompt (popular) → accuracy (limitation)

prompt does not contain any explicit instructions or example for the model to follow. Instead it relies on the model's ability to understand & interpret Natural language.

(without specific training)

Embeddings

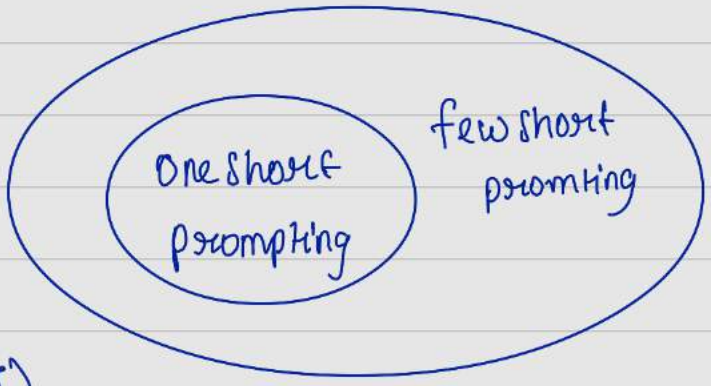
classic technique in NLP. The idea is to create a vectorspace from the text such that the distance between the vectors in the space have a certain meaning.

Vector → simply a sequence of Numbers. (represent complex Model)

vector databases is a database that is saving those embeddings.
(pinecone)

few Short prompts

model is given a few examples of the result you want.
useful where there is limited data available for a given tasks.



(COT)
Chain of thought prompting (Google)

↳ improve reasoning abilities of LLM, It decomposes the multi-step problems into intermediate steps, allowing to solve a complex problem.

→ prompt Engineering technique.

→ it's how human solves the problem. (problem solving)

(major step in prompt Engineering)

① zero Shot chain of thought
↳ let think step by step (prompt)

② few short chain of thought (similar to few shot learning)

Embedding in transformer (High dimensional space)
↳ each token represented as a vector & occupies a location. (word2vec)

fine tuning

fine tuning is taking these general purpose models like GPT-3 & specializing them into something chatGPT

Gets the model to learn the data, rather than just get access to it.

Reduces hallucinations & process is similar to the model's earlier training.

Generating text with tranformer

The attention mechanism is used in both the encoder & decoder layers of the transformer mechnanism.

The data leaves the encoder is, a deep representation of the structure and meaning of the input sequences. This representation is inserted into the middle of the decoder to influence decoder's self-attention mechanism.

Encoder → Encodes inputs ('prompts') with contextual understanding & produces one vector per input token.

Decoder → Accepts input tokens and generates new token.

does this in a loop

Encoder only models → Sentiment analysis, BERT

Encoder-decoder model → sequence to sequence tasks, translation.
len(input) ≠ len(output)
→ Google Bard

→ Decoder only model → GPT, BLOOM, Llama (models)

prompting & prompt Engineering

The develop & improve the prompt is known as prompt Engineering.

providing examples inside the context window is called in-context learning. (ICL) → there is a limit to context window.

→ zero shot inferences.
→ one-shot inferences
→ few shot inferences.

→ engineering your prompts to encourage the model to learn by examples.

Large models are good at zero shot inferences.

Generative configuration (inference parameters)

* max-new tokens → number of tokens that model will generates.

The output from the transformers' softmax layer is a probability distribution across the entire dictionary of words.

Most LLM by default will operate with so-called greedy decoding,

↳ greedy:

The word/token with the highest probability is selected.

So, bring random sampling.

Random (weighted) sampling, select a token using a random-weighted strategy across the probabilities of all tokens.

---

top-K & top-P } sampling techniques.

↳ limit the random sampling & increase the output to be sensible

---

top-K → select an output from the top-K results after applying random-weighted strategy using the probabilities.

top-P → select an output using the random weighted strategy with the top-ranked consecutive results by p(E) and with a cumulative $p(E) \leq p$

↳ specify no. of tokens to randomly choose from.

↳ specify the total p(E) want model to choose from.

temperature

↳ higher temperature, higher randomness.

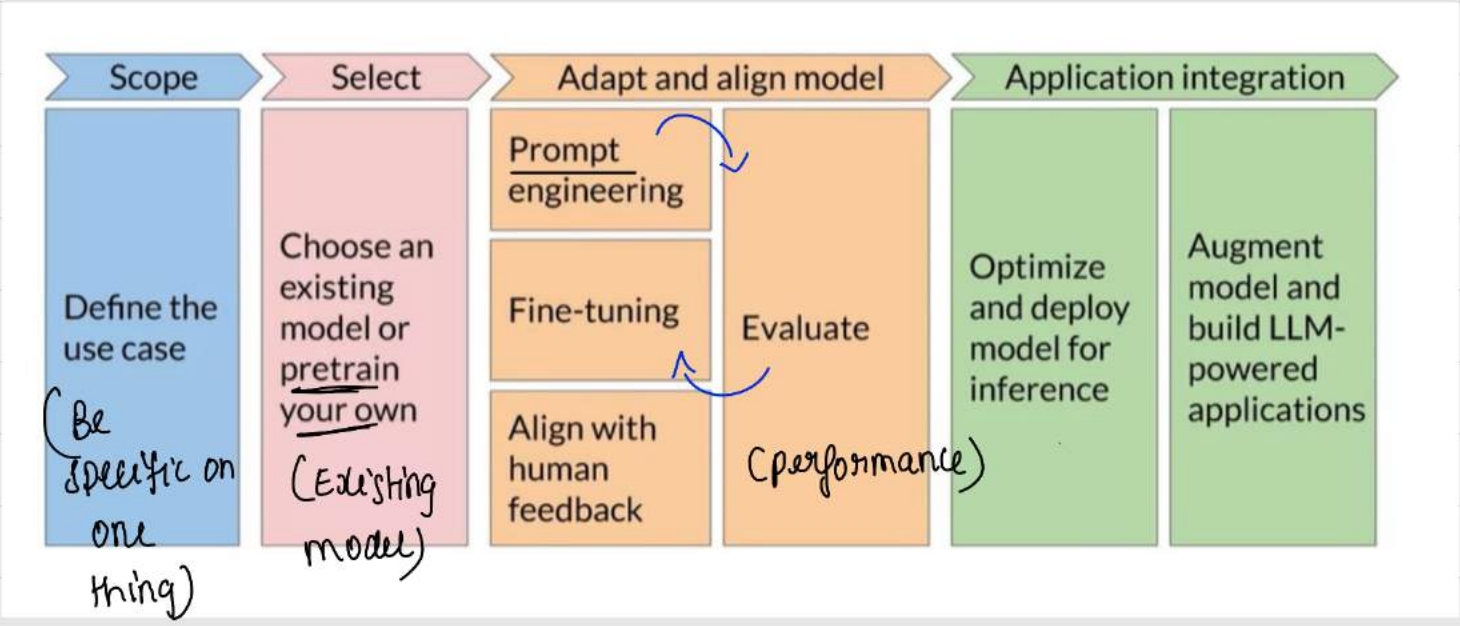
applied in the final softmax layer.

temperature <1 → Strongly peaked probability distribution

temperature >1 → Broader, flatter probability distribution.

Generative AI project lifecycle

fine tuning ~ supervised learning.



pre-training large language model

consideration for choosing a Models.

→ foundation model (pretrained LLM)

→ Train your own Model (custom LLM)

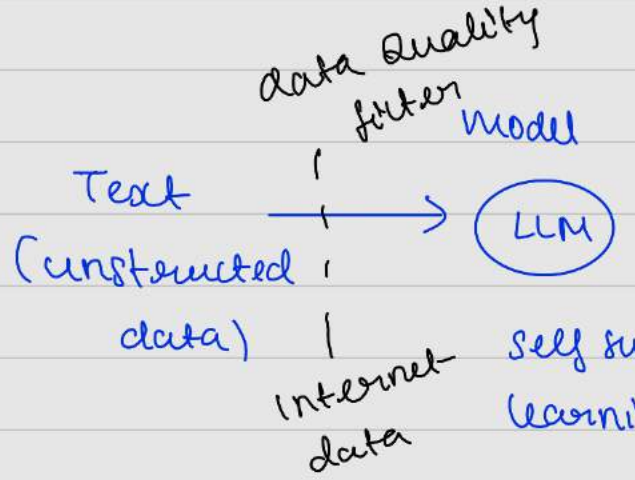
Huggingface → Have Model cards
(Hub) (imp details & best usecases for each model)

BloombergGPT → Decoder only language model, pretrained using an extensive financial datasets.

The Goal of pre-training is to teach the model the general pattern and structure of language, allowing it capture the relationship b/w words.

The Goal of fine-tuning is to adjust the model's parameters to make it better at performing the desired task.

LLM encode a deep statistical representation of language. developed during model pretraining phase.



{encoders generates embeddings}

training → architecture of model. { weights updated }

pre-training also requires a large amount of compute & use of GPUs

Encoder only models are also called Autoencoding models, they are pre-trained using masked language modelling.

masked language modelling (MLM)

The teacher teaches the student
(mask) (randomly Masked)

training objective is to predict the mask token in order to reconstruct the original sentences.

objective : Reconstruct text ('denoising')

The teacher <u>teaches</u> the student.

→ ← Bidirectional context

model has understanding of full context of a token.

Good use cases:

- → sentiment analysis
- → named entity recognition
- → word classification

[Good for tasks that require understanding of the input, such as sentence classification & named entity recognition]

Example models:

- → BERT
- → ROBERTA

Decoder only model | Autoregressive models, which are pretrained using Causal Language Modelling (CLM)

Here training objective is to predict the next tokens based on the previous sequences of tokens.

↳ Fully language modelling.

objective: Predict next token.

The ? [CLM] {No knowledge of the end of sentences}

↳ The teacher

↳ iterate one by one tokens for next word, context is unidirectional.

Good use cases	Example models
→ Text generation	→ GPT
→ Other emergent behaviour	→ BLOOM.
↳ depends on model size	

[Good for generative tasks such as text generation]

Encoder-decoder model | Sequence to sequence models, Good for generative tasks that require an input, such as translation or summarization.

Span corruption

Original text ⟶ Encoder - Decoder LLM

Span corruption

The teacher <mask> <mask> student

The teacher <x> student

↳ sentinel token

Objective: Reconstruct span

<x> teaches the

[Sequence to sequence models are best suited for tasks revolving around generating new sentences depending on a given input such as summarization]

Models:

→ T5

→ BART

Growth of models powered by;

→ Introduction of transformer

→ Access to massive datasets

→ more powerfull compute resources.

computional challenges of training LLM

→ CUDA out of memory

(Compute unified Device Architecture)

↳ tools developed for Nvidia GPUs

Pytorch | tensorflow uses this.

Approximate GPU RAM needed to Store 1B parameters.

1 Parameter → 4 bytes.

1B para → 4×10^9 bytes → 4GB

memory needed to Store model		memory needed to train model.
4GB @ 32-bit full precision	→ Single processor.	24GB @ 32-bit full precision.

(1.) Reduce the memory,

reduce the memory required for training is called quantization

↳ reduce the memory required to Store weight by reducing their precision from 32-bit floating to 16-bit floating point numbers. 18-bit

By reducing the precision of the model weights. ←

As model sizes get larger, you will need to split your model across multiple GPUs for training.

Approximate GPU RAM needed to train 1B parameters.

Additional GPU RAM needed to train 1B parameters

	Bytes per parameter
Model Parameters (Weights)	4 bytes per parameter
Adam optimizer (2 states)	+8 bytes per parameter
Gradients	+4 bytes per parameter
Activations and temp memory (variable size)	+8 bytes per parameter (high-end estimate)
TOTAL	**=4 bytes per parameter +20 extra bytes per parameter**

~20 extra bytes per parameter

Quantization: Summary.

	Bits	Exponent	Fraction	Memory needed to store one value
FP32	32	8	23	4 bytes
FP16	16	5	10	2 bytes
BFLOAT16	16	8	7	2 bytes
INT8	8	-/-	7	1 byte

FLAN T5

- Reduce required memory to store and train models
- Projects original 32-bit floating point numbers into lower precision spaces
- Quantization-aware training (QAT) learns the quantization scaling factors during training
- BFLOAT16 is a popular choice

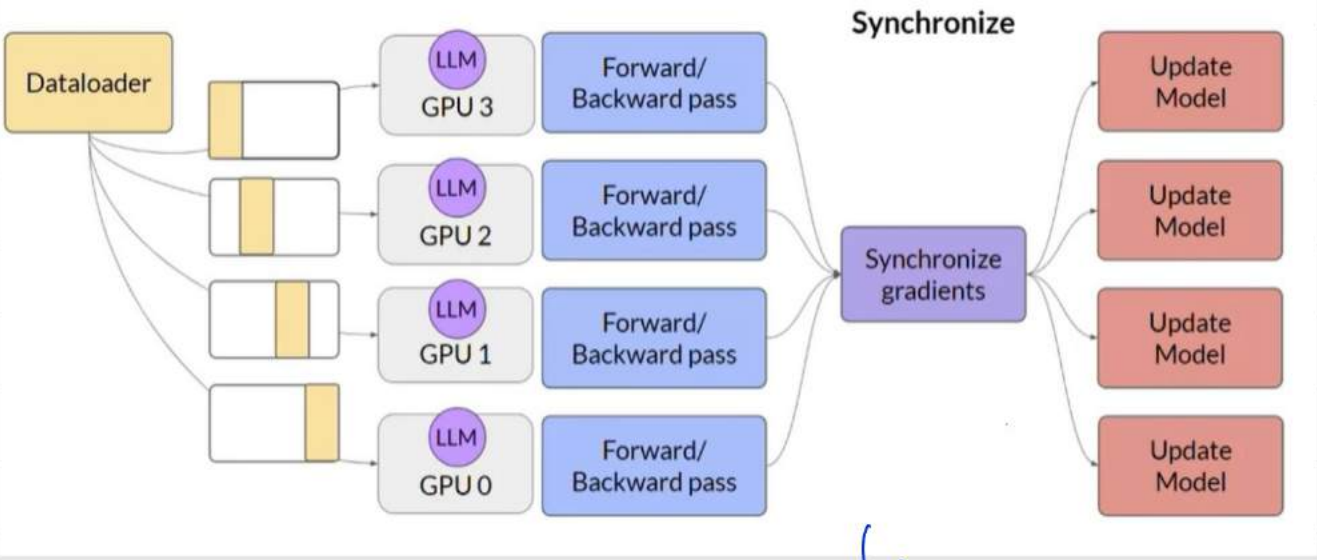
By Quantization, we can reduce memory consumption required to store the model parameters.

Efficient multi-GPU compute strategies

This implementation allows parallel computations across all GPU's that results in faster training.

Distributed Data Parallel (DDP)

(dataset is distributed)



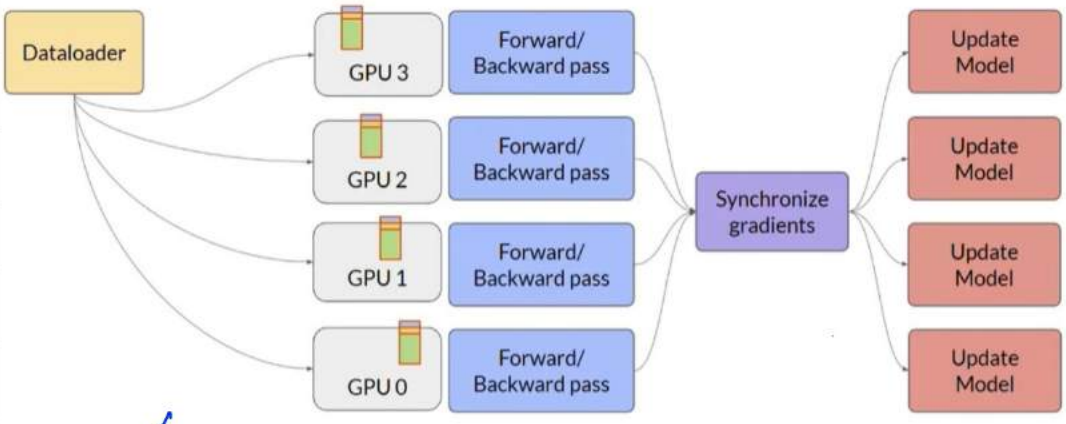
↳ requires model weights and additional parameter.

If model is too big for this, look for model sharding technique.

fully sharded Data parallel (FSDP), motivated by the 'ZeRO' paper - zero data overlap between GPUs

Zero ⇒ Zero Redundancy optimizer. (reducing the memory by distributing (sharding)

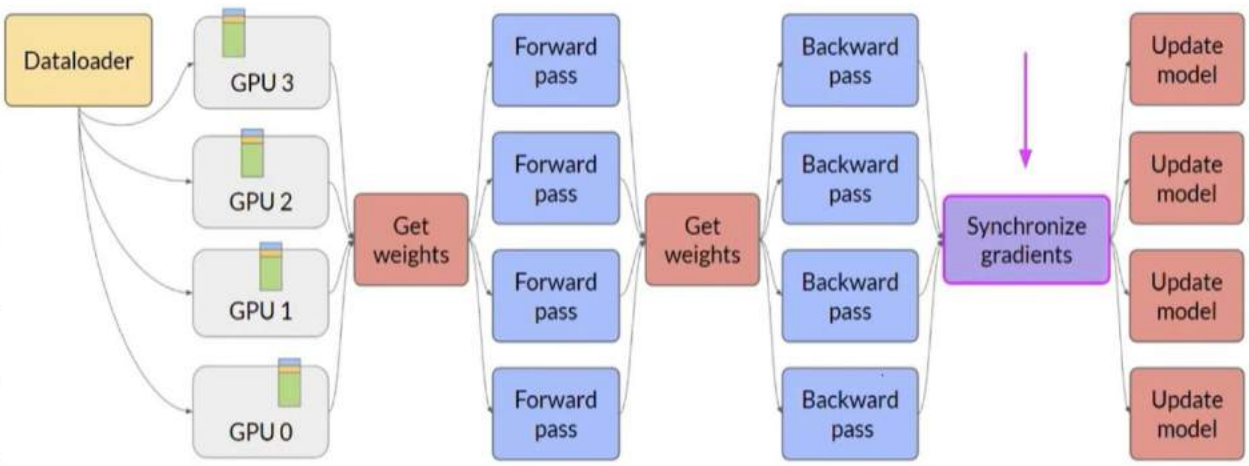
Fully Sharded Data Parallel (FSDP)



↳ also distribute the model parameter, gradients & optimizes the states across the GPU nodes.

using GPU

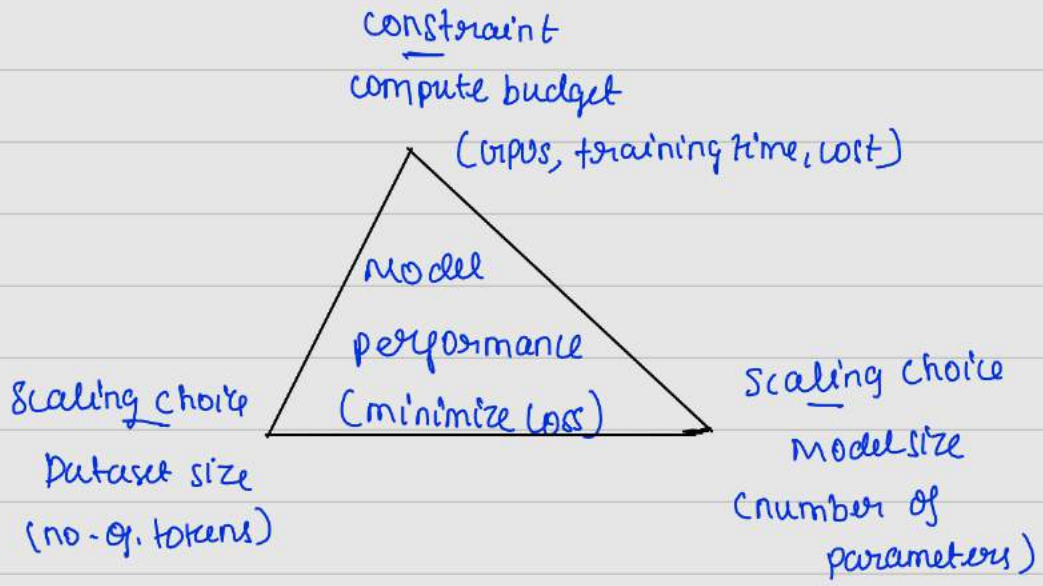
Fully Sharded Data Parallel (FSDP)



→ Helps to reduce overall GPU memory utilization
→ supports offloading to CPU if needed.
→ configure level of sharding via sharding factor.

Scaling laws and compute-optimal models

pre-training a model } → maximize model performance.



''petaflop/s-day' = floating point operations performed at rate of 1 petaflop per seconds for one day.

→ increase the compute budget to achieve better model performance. (Hardware, project timeline, financial budget)

→ dataset ↑ performance ↑ ∫ model size ↑ performance ↑

compute optimal models

→ very large models may be over-parameterized and under trained

→ smaller models trained on more data could perform as well as large models.

Chinchilla scaling laws for model and dataset size

Model	# of parameters	Compute-optimal* # of tokens (~20x)	Actual # tokens
Chinchilla	70B	~1.4T	1.4T
LLaMA-65B	65B	~1.3T	1.4T
GPT-3	175B	~3.5T	300B
OPT-175B	175B	~3.5T	180B
BLOOM	176B	~3.5T	350B

Compute optimal training datasize is ~**20x** number of parameters

* assuming models are trained to be compute-optimal per Chinchilla paper

Sources: Hoffmann et al. 2022, "Training Compute-Optimal Large Language Models"
Touvron et al. 2023, "LLaMA: Open and Efficient Foundation Language Models"

pre-training for domain adaptation

words are rarely used, which means that they are unlikely to have appeared widely in the training text of existing LLMs.

↳ Models have difficulty in understanding them, using correctly.

Pre-training your model from scratch will result in better models for highly specialized domains like law, medicine, finance.

BloombergGPT → domain adaptation for finance.

(pretraining) → financial (private + public) 51%

+ other (public) (49%)

∴ Chinchilla scaling laws for guidance.

Week-2

Instruction fine-tuning

fine-tuning an LLM with instruction prompts.

→ In context learning may not work for smaller models (LLM)

→ Examples take up space in the context window. So, Instead try fine-tuning the model.

LLM pretraining

unstructured textual data → pre-trained LLM (model) } pretraining, self-supervised learning

LLM fine-tuning, } supervised learning.

pre-trained model (model) → task specific examples (labelled example of specific domain) → fine-tuned LLM (model)

prompt - completion pair. examples

(improved performance)

output of LLM is a probability distribution across tokens.

Model pre-trained LLM → Model Fine-tuned LLM (Instruct LLM)

The fine tuning process results in a new version of the base model is Instruct model. (common way)

Fine-tuning with instruction prompts is common way, fine-tuning always means Instruction fine-tuning

Instruction fine-tuning trains the model using examples that demonstrate how it should respond to a specific instruction.

Full-fine-tuning updates all parameters.

Model pre-trained LLM → Task specific examples → Model Fine-tuned LLM

training data → formatted as instruction.

LLM- fine-tuning

prepared instruction dataset → training splits
- Training
- validation
- test

(prompt) → Model (pretrained LLM) → Model completion.

loss: cross entropy.

fine-tuning on a single task

parameter efficient fine-tuning } → set of techniques that preserves the weights of the original LLM (Most of pre-trained weights are left unchanged)

model (pre-trained LLM) → Single task training dataset, eg. Summarization → Model. instruct LLM

example: 500 - 1000 single task.

catastrophic forgetting,

↳ full fine tuning can significantly increase the performance of a model on a specific task. (modifies original LLM weights)

↳ but can lead to reduction in ability on other tasks.

Avoidance?

1. First note that you might not have to!
2. Fine-tune on multiple tasks at the same time.
3. consider PEFT
   ↳ trains only task-specific adaptor layers and parameter.

Multi-task Instruction fine-tuning

Model pre-trained LLM → Instruction fine-tune on many tasks → Model instruct LLM.

(many examples of each needed for training)
(50,000 - 100k)

FLAN → Fine tuned Language Net.

FLAN models refers to a specific set of Instruction used to perform instruction fine-tuning

Flan-T5 } fine-tuned version of pre-trained T5 Model
(general purpose (Instruct Model)

SAMSum: A dialogue dataset } FLAN-T5 give some abilities to summarize the conversation.
(dialogsum)

when fine-tuning is to evaluate the quality of your model completions.

Model evaluation

LLM model → output are non-deterministic & language based evaluation. (output NOT known)

LLM evaluation - challenges

Accuracy = $\frac{\text{correct prediction}}{\text{Total prediction}}$

1. ROUGE
2. BLEU-score

} metrics.

(Bilingual evaluation understanding)

→ used for text summarization
→ compares a summary to one or more reference summaries

→ used for text translation
→ compares to human-generated translation.

The dog lay on the rug as I sipped a cup of tea

n-gram.

Bigram

unigram

Rouge-1

(unigram)

$$\text{Rouge1 Recall} = \frac{\text{unigram matches}}{\text{unigram in references (human)}}$$

$$\text{Rouge1 precision} = \frac{\text{unigram matches}}{\text{unigram in output}}$$

(generated output.

$$F1 = \frac{2PR}{P+R}$$

Rouge-L

↳ based on longest common subsequence (LCS)

problem with 'Rouge score' is possible for a bad completion to return in good score.

Bleu score is calculated using the average precision over multiple n-gram sizes

Bleu metrics = Avg { precision across range of n-gram sizes }

The quality of translation by checking how many n-grams the machine generated translated match those in the references translation.

LLM Evaluation - Metrics - BLEU

BLEU metric = Avg(precision across range of n-gram sizes)

Reference (human):

I am very happy to say that I am drinking a warm cup of tea.

Generated output:

I am very happy that I am drinking a cup of tea. - BLEU 0.495

I am very happy that I am drinking a warm cup of tea. - BLEU 0.730

I am very happy to say that I am drinking a warm tea. - BLEU 0.798

I am very happy to say that I am drinking a warm cup of tea. - BLEU 1.000

Rouge → diagnostic evaluation (Not final)

Benchmarks

1. GLUE ⇒ General language understanding Evaluation. (2018), collection of NL tasks such as Sentiment analysis & question answering.

② SuperGlue → 2019, updated of Glue.

Models get larger, their performance against benchmarks such as SuperGlue start to match human ability on specific tasks.

Benchmarks for massive models.

① Massive Multitask language understanding (MMLU) → specifically for modern LLMs, world knowledge / problem solving ability.

(2021)

② Big-bench Hard, Big-bench, Lite

(2022)

③ Holistic Evaluation of language models (HELM)

↓

includes Fairness, Bias, Toxicity.

Parameter efficient fine-tuning → only update a small subset of parameter

full-fine-tuning of large LLM is challenging.

LLM → computer system → { trainable weights, optimizer states, gradients, Temp memory, Forward activation }

where every model weight is updated during supervised learning.

LLM with most layers frozen → LLM → small number of trainable layers.

LLM with additional layers for PEFT → LLM → New trainable layer.

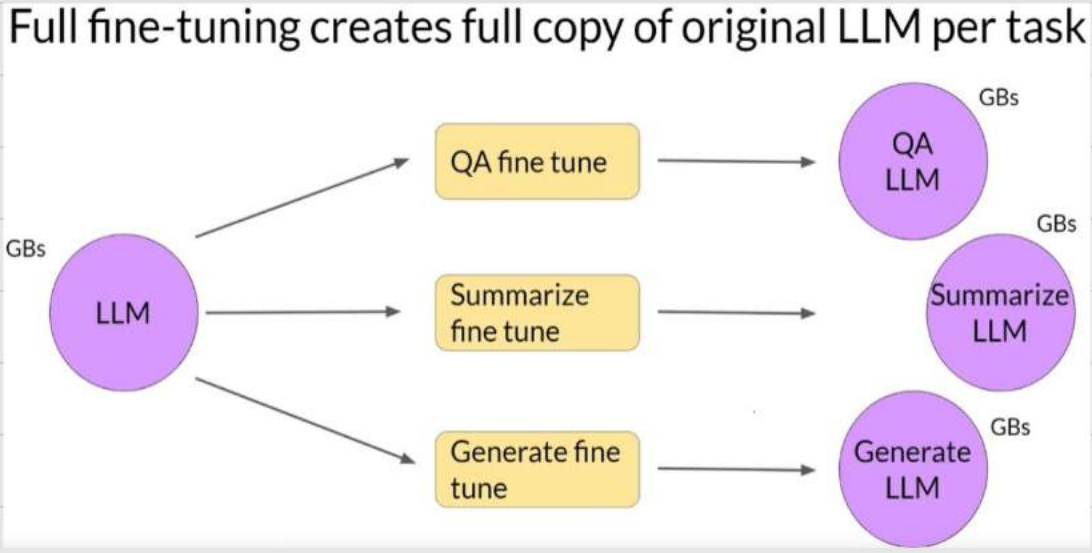
With PEFT,

- → Frozen weight
- → Small trainable weights.
- → other component

} proper memory management

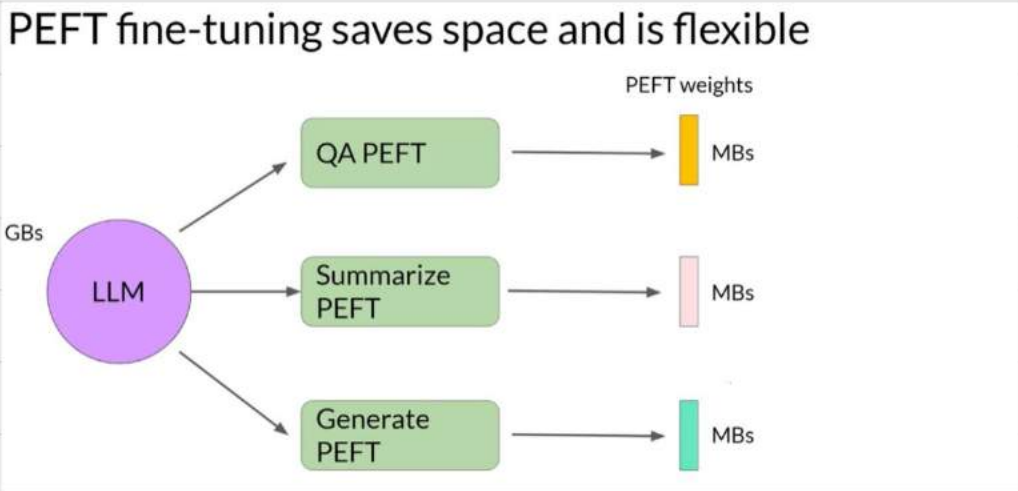
PEFT can often be performed on a single GPU.

less prone to catastrophic forgetting.



creates an expensive storage problem

New parameters are combined with the original LLM weights for inference.



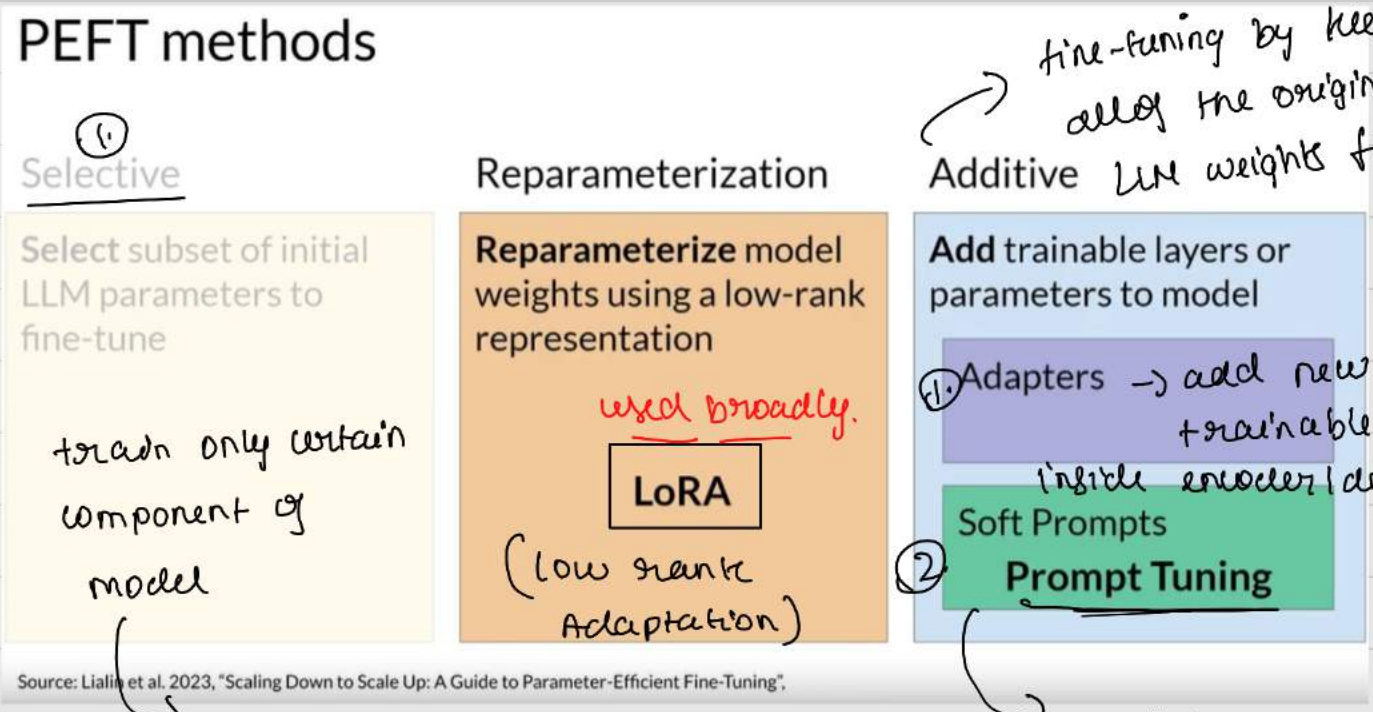
QA LLM

Summarize LLM.

PEFT weights are trained for each task & can be easily swapped out for inferences.

PEFT trade off

- → parameter Efficiency
- → memory Efficiency
- → model performance.
- → Training speed
- → inference costs.



fine-tuning by keeping all of the original LLM weights frozen

1. Selective

train only certain component of model

Reparameterization

used broadly.

(low rank Adaptation)

Additive

1. Adapters → add new trainable layer inside encoder/decoder

2. Prompt Tuning

model architecture fixed & frozen, focus on manipulating on input to achieve better performance.

trade off between

parameter Efficiency	compute Efficiency

PEFT - techniques : LORA

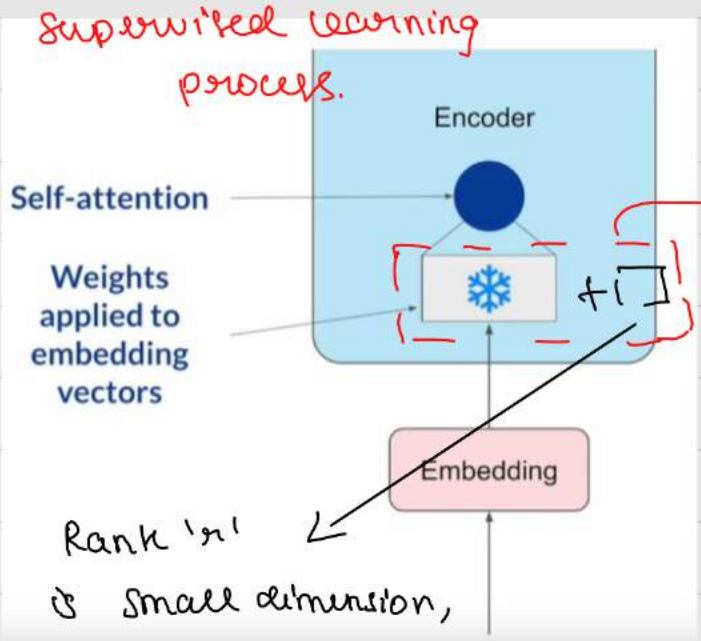
Parameter efficient fine-tuning with single GPU and Avoid the need for a distributed cluster of GPUs

→ adding trainable parameter to promt Embedding (or) retraining embedding weight

Low rank Adaptation of large language Models (LORA)

→ parameter efficient fine tuning techniques, re-parameterization category.

Supervised learning process.



Rank 'r' is small dimension, typically 4,8---64

① Freeze most of the original LLM weights.

→ updated weights. (replace in orig)

② Inject 2 Rank decomposition matrices.

③ Train the weight of the smaller weights.

Steps to update the model for inferences

Apply LORA just to the self attention layer, is enough.

① matrix multiply the low rank matrices
$B * A = B \times A$ (same dimen)

② Add to original weights

weights + $B \times A$

Use the base Transformer model presented by Vaswani et al. 2017:

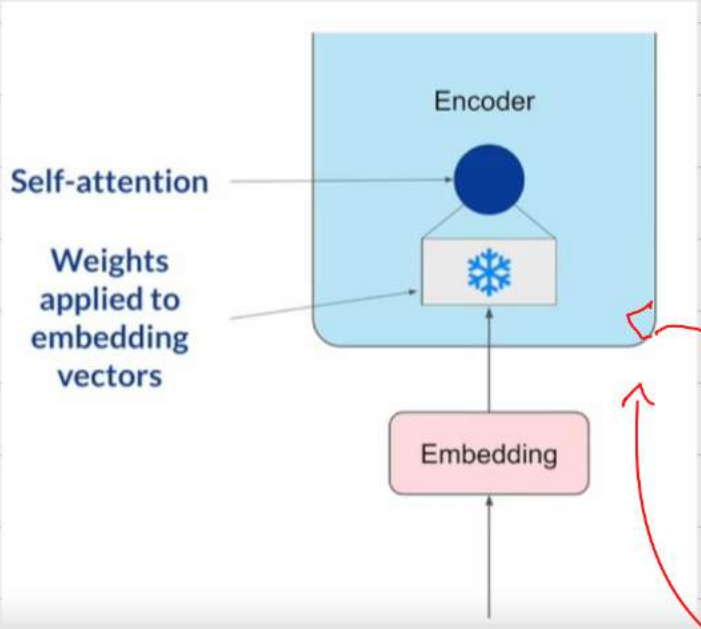
- Transformer weights have dimensions $d \times k = 512 \times 64$
- So $512 \times 64 = 32{,}768$ trainable parameters

Attention is all you need.

In LoRA with rank $r = 8$:

- A has dimensions $r \times k = 8 \times 64 = 512$ parameters
- B has dimension $d \times r = 512 \times 8 = 4{,}096$ trainable parameters
- **86% reduction in parameters to train!**

the memory required to store these LoRA matrices is very small.



Train different rank decomposition matrices for different tasks

update weights before inference

task A task B (update weights)

Summarization task

Sample ROUGE metrics for full vs. LoRA fine-tuning

FLAN-T5

Dialog summarization

Base model ROUGE	+80.63%	Full fine-tune ROUGE	−3.20%	LoRA fine tune ROUGE
flan_t5_base {'rouge1': 0.2334, 'rouge2': 0.0760, 'rougeL': 0.2014, 'rougeLsum': 0.2015}		flan_t5_base_instruct_full {'rouge1': 0.4216, 'rouge2': 0.1804, 'rougeL': 0.3384, 'rougeLsum': 0.3384}		flan_t5_base_instruct_lora {'rouge1': 0.4081, 'rouge2': 0.1633, 'rougeL': 0.3251, 'rougeLsum': 0.3249}

Baseline score

LoRA for fine tuning, smaller no. of parameter & less compute.

Smaller the rank, the smaller the number of trainable parameter, bigger saving on compute.

choosing the LORA rank

Rank r	val_loss	BLEU	NIST	METEOR	ROUGE_L	CIDEr
1	1.23	68.72	8.7215	0.4565	0.7052	2.4329
2	1.21	69.17	8.7413	0.4590	0.7052	2.4639
4	1.18	**70.38**	**8.8439**	**0.4689**	0.7186	**2.5349**
8	1.17	69.57	8.7457	0.4636	**0.7196**	2.5196
16	**1.16**	69.61	8.7483	0.4629	0.7177	2.4985
32	**1.16**	69.33	8.7736	0.4642	0.7105	2.5255
64	**1.16**	69.24	8.7174	0.4651	0.7180	2.5070
128	**1.16**	68.73	8.6718	0.4628	0.7127	2.5030
256	**1.16**	68.92	8.6982	0.4629	0.7128	2.5012
512	**1.16**	68.78	8.6857	0.4637	0.7128	2.5025
1024	1.17	69.37	8.7495	0.4659	0.7149	2.5090

Relationship b/w rank and dataset need more empirical data (research)

PEFT techniques 2: soft prompts (parameter efficient fine-tuning)

Prompt tuning is not prompt engineering.

↳ where trainable tokens are added to your prompt and model weights are left untouched

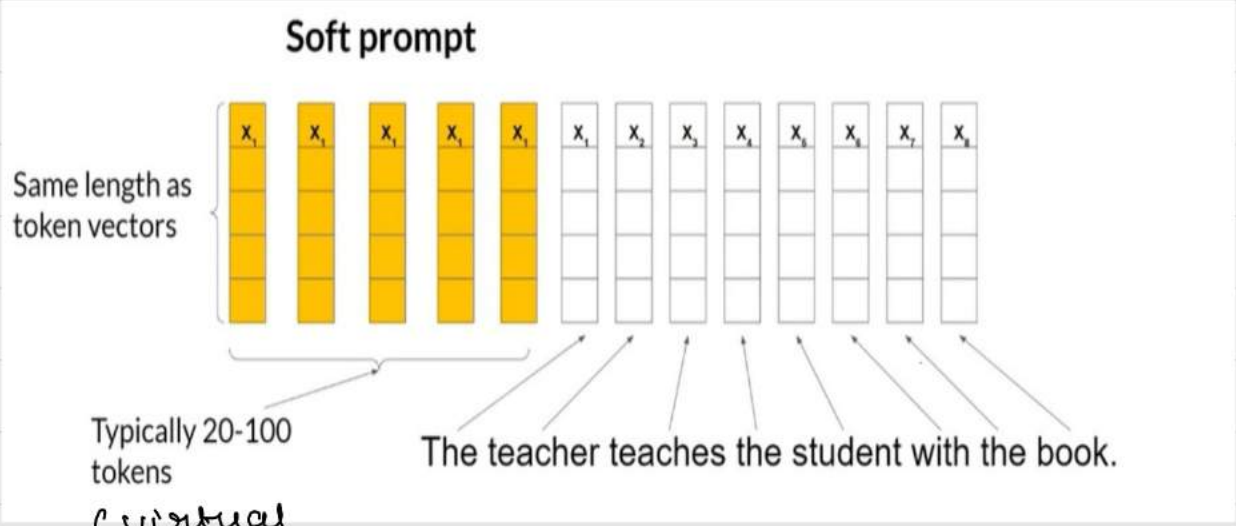
(SL process to determine their optimal values)

combine LORA with quantization techniques to further reduce your memory (QLORA)

PEFT is used heavily to minimize compute and memory resources. (reduce the fine tuning costs)

Limitation of prompt engineering, requires a lot of manual effort to write and try different prompt.

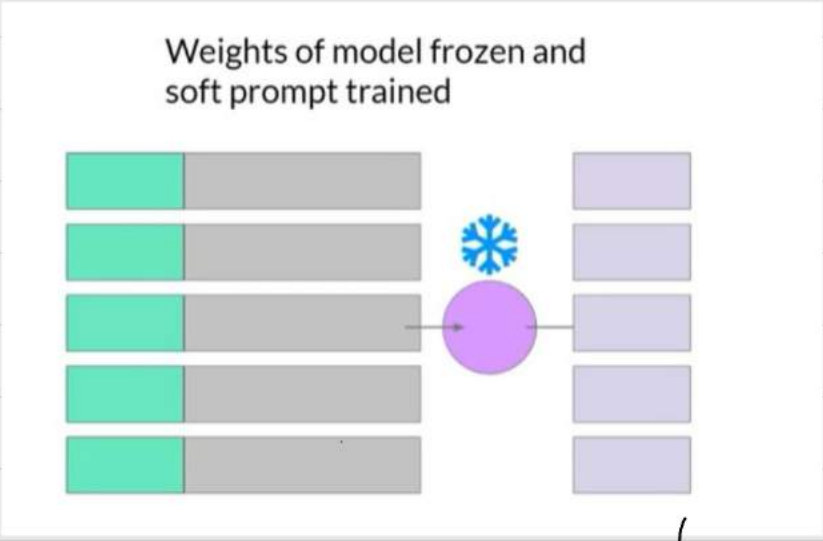
(context window size)



(virtual token)

Embedding of each token exist at unique point in multi-dimensional space.

Soft prompts → virutal tokens. (through SL learns the value for these virutal tokens that maximize the performance for task)



(full-fine tuning)

In full-fine tuning, weights of model updated during training.

(prompt tuning) → weights of LLM is frozen, model does not get updated but embedding vectors of the soft prompt gets updated over time.

(10K-100K parameter)

(only few parameters are trained and updated)

Switch out soft prompt at inference time to change task. (very small, efficient & flexible)

model size increases, performance of prompt tuning increases.

↳ 10B model, prompt tuning can be effective as full fine-tuning for larger models.

soft prompt token can take any value within the continuous embedding vector space.

'soft' prompt designed by an AI that outperformed human-engineered 'hard' prompt

Week-3

RLHF (Reinforcement learning with human feedback) it helps to align the model with human values.

↳ less harmful content, much helpful content.

LLM as reasoning engine → giving them the power to make their own subroutine calls (actions)

Aligning models with human values

Goal of fine-tuning with instructions;

→ Better task completion

→ Better understanding of prompts (Human responses)

→ more Natural sounding language.

New set of challenges

models behaving badly → Toxic language
→ Aggressive responses
→ providing dangerous information.

(internet data)

Helpful? Harmless? Honest? → responsible use of AI.

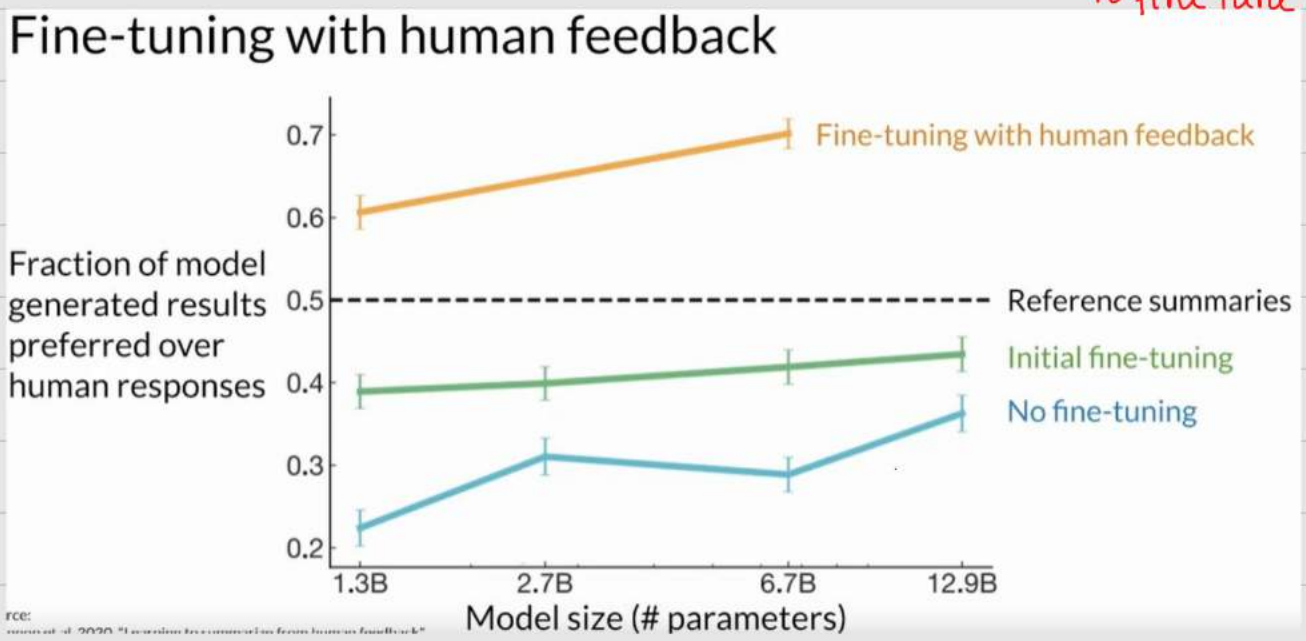
Additional fine-tuning with human feedback, helps to better align the model with human preferences., increases HHH of completion.

decreases toxicity & generation of incorrect information.

Reinforcement learning from human feedback (RLHF)

↳ popular technique to fine tune LLM.

task: text summarization.



Instruct fine tuned model → Reinforcement learning from Human feedback. → Human aligned LLM.

→ maximize helpfulness, relevance.

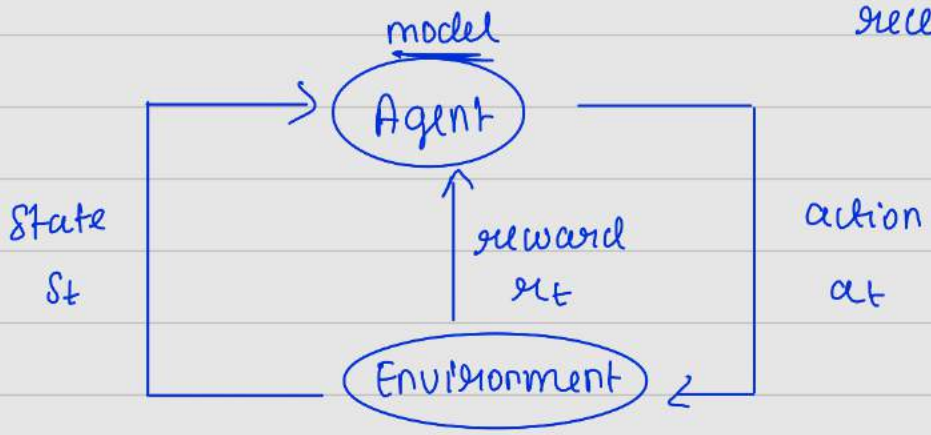
→ minimize harm | Avoid dangerous topics.

Application of RLHF is the personalization of LLMs where models learn the preferences of each individual user through a continuous feedback process

(individualized learning | personalized AI assistant)

Reinforcement learning

Objective: maximize reward received for actions.



Learn the optimal policy.

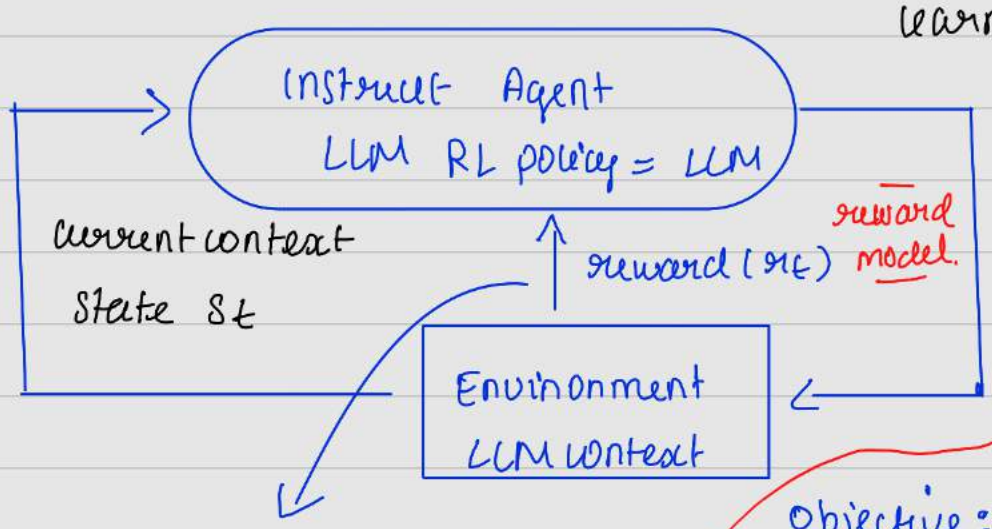
Agent make decision by RL policy.

↪ Changes policy to make better decision for success

The series of actions and corresponding states form a playout / rollout

Reinforcement learning : fine-tune LLMs

(Statistical Representation of learning)



Single word / Sentence

Token vocabulary action a_t (Next) (PDF)

How closely aligned with Human preferences.

All possible tokens, that the model can choose from the completion.

Objective : Generate aligned text Human preference.

LLM weights are then updated iteratively to maximize the reward.

Obtaining human feedback can be time consuming and expensive so use additional 'reward model'

↳ access the output of the LLM & assign a reward value & update the weights

Sequences of actions and states is called a Rollout.

It encodes all the preferences learned from human feedback (update weight)

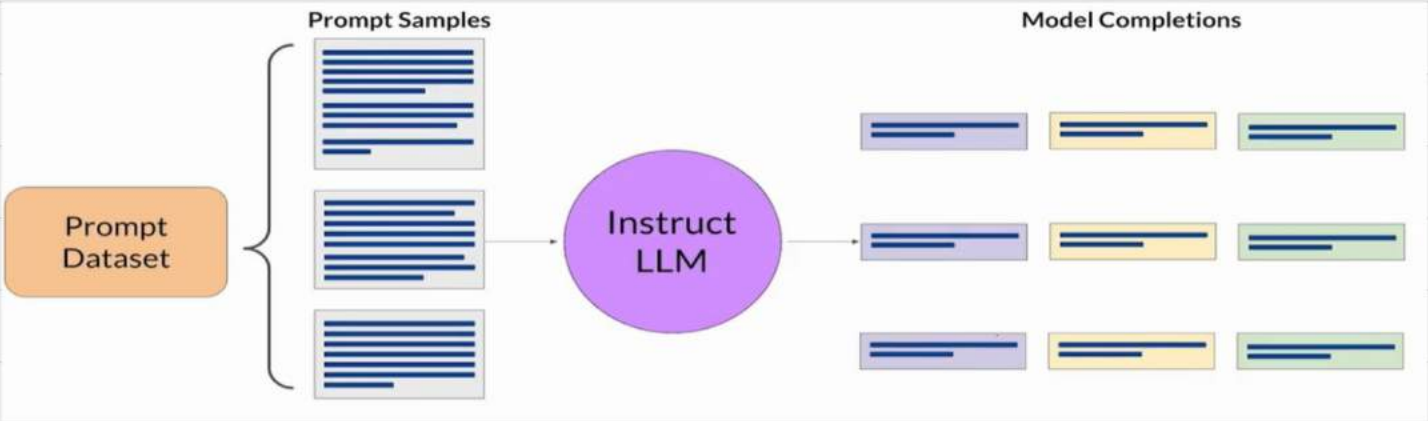
Obtaining feedback from humans

→ Select a model (instruct model)

prepare dataset for human feedback.

* use LLM along with prompt data to generate a no. of different responses for each prompt.

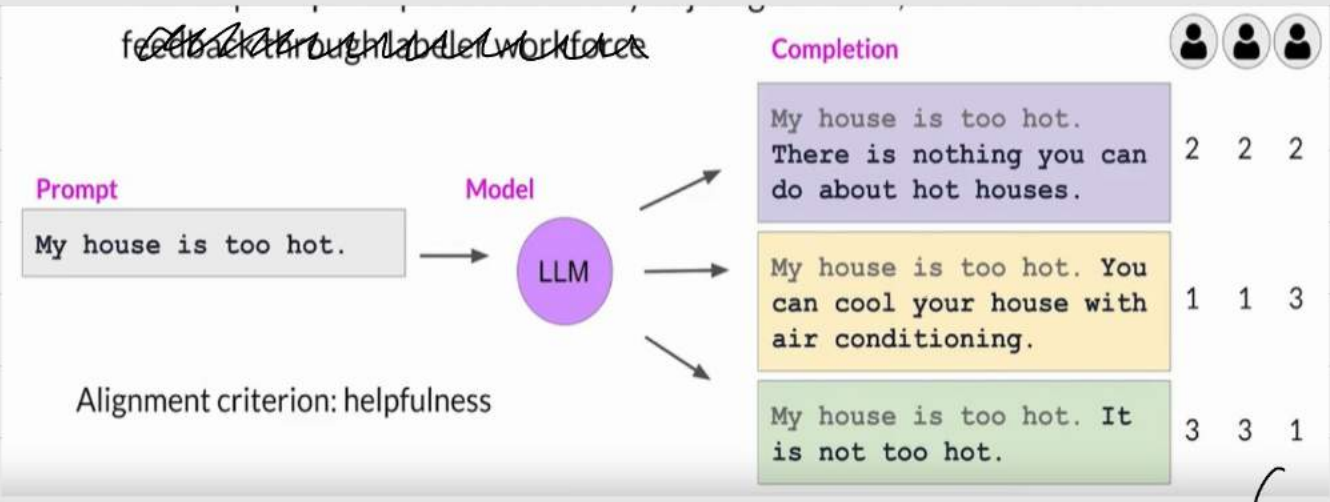
The prompt dataset is comprised of Multiple prompts each processed by LLM to produce a set of completion.



→ collect feedback from human labelers on the completion generated by LLM

collect human feedback

* Define your model alignment criterion
* for prompt-responses sets that you just generated, obtain human feedback through labeler workforce.



indicate the misunderstandin

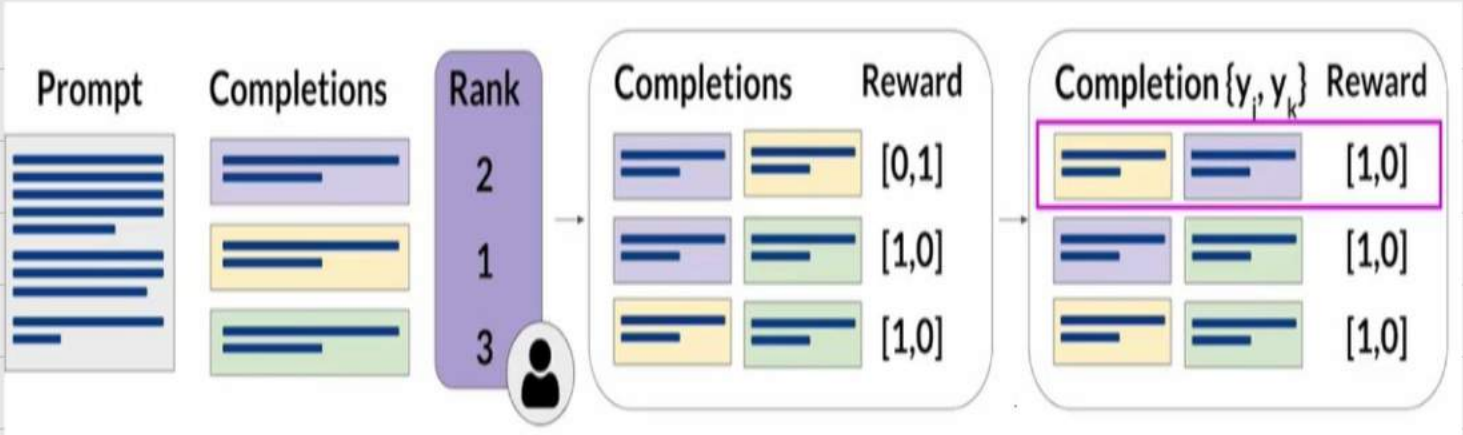
clarity of instruction have big impact on quality of human feedback you obtain.

-> Sample instruct for human labelers is given.

After completion, have all the data you need to train the reward model, which you will use instead of humans to classify model completions during RL-fine tuning.

prepare labelled data for training.

convert ranking into pairwise training data for the reward model.

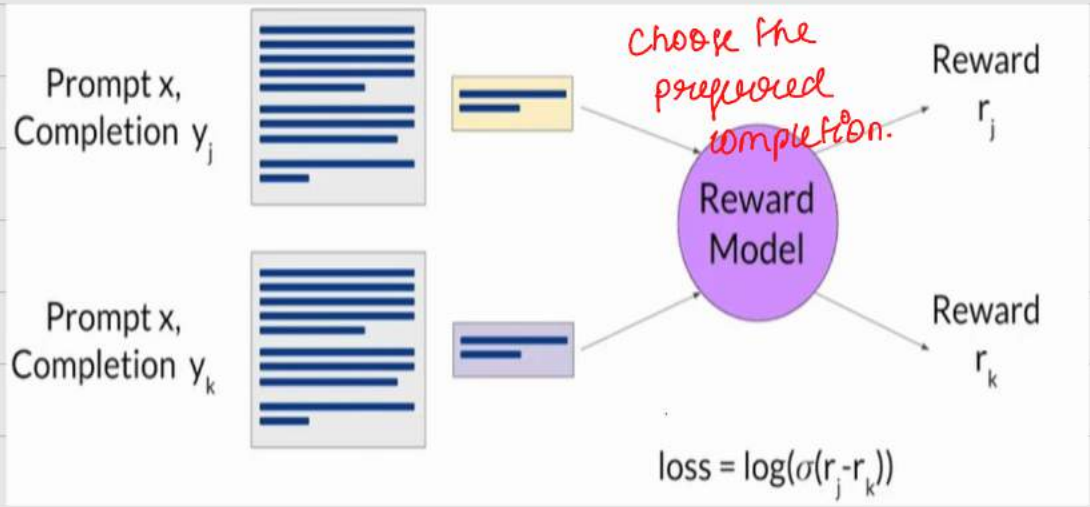


thumbs-down/up feedback is often easier to gather than rank feedback

Reward model (language model)

Train model to predict preferred completion from $\{y_j, y_k\}$ for prompt x.

Bert → trained using supervised learning methods on pair wise comparison data.

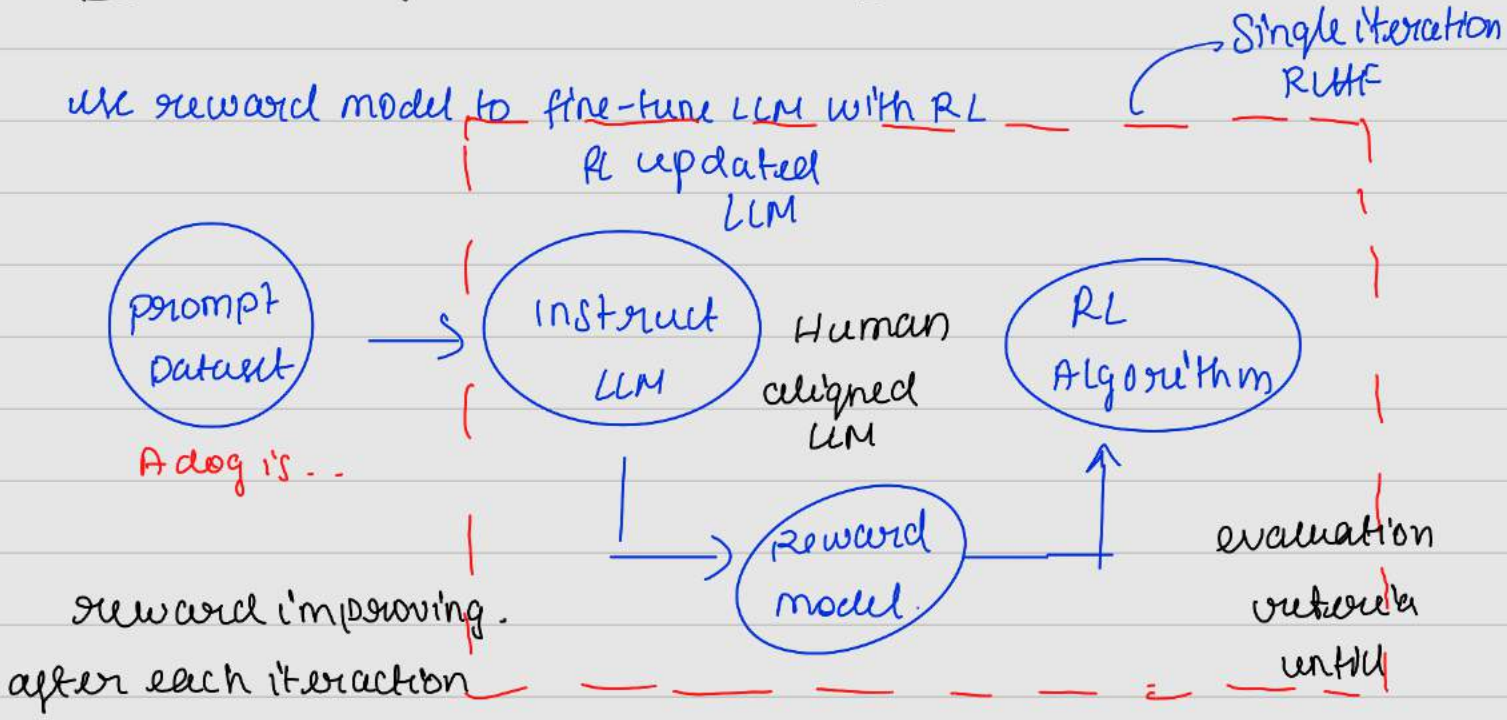


human preferred option is 1st one. y_j

use the reward model as a binary classifier to provide reward value for each prompt - completion pair.

RLHF : fine-tuning with reinforcement learning.

use reward model to fine-tune LLM with RL



Higher reward value here represents a more aligned responses

Then pass the reward value of the prompt completion to the RL algorithm to update the weights of LLM moving towards generating more aligned responses.

Reinforcement learning algorithm → PPO
(proximal policy optimization)
(reward score increase over time)

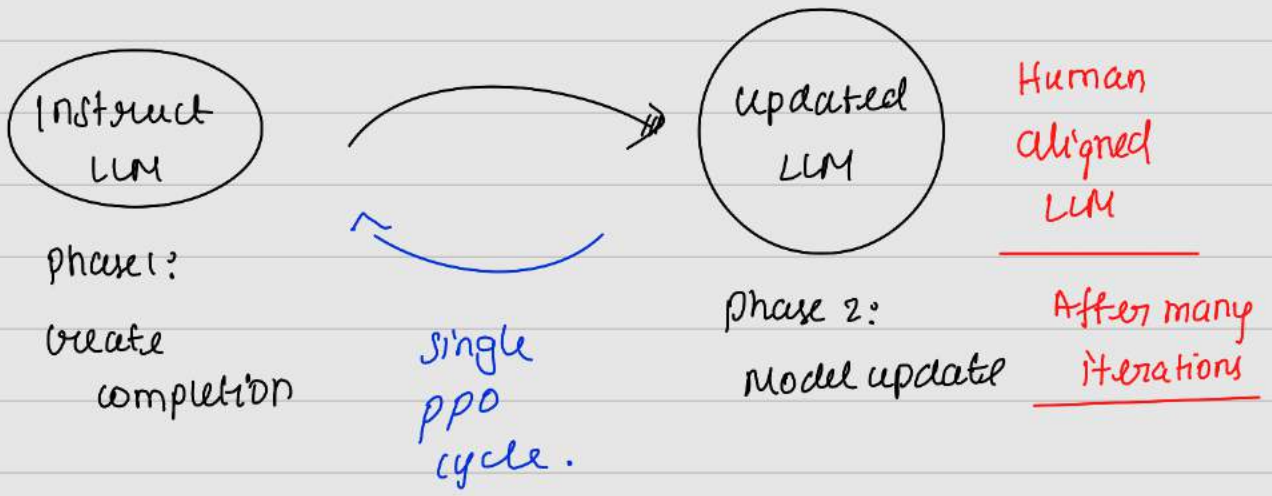
proximal policy optimization → update weights of LLM based reward

PPO optimizes the policy, in LLM, to be more aligned with human preferences.

→ updates LLM (updates are small & within a bounded region) → stable learning (trust region)

reward model captures the human preferences.

the losses and reward determined in phase 1 are used in phase 2 to update weight.



the model weight updates are guided by the prompt completion, losses & rewards.

PPO objective → policy whose expected reward is high. (updates LLM weights)

entropy maintains creativity. (Higher, more creativity)

Q-learning is an alternate technique for fine-tuning LLMs through RL, but PPO is currently the most popular method.

PPO has right balance of complexity & performances.

Direct preference optimization, (DPO) → Stanford paper, (research)

Reward hacking (problem) (reduce overall quality of language) (High scores)

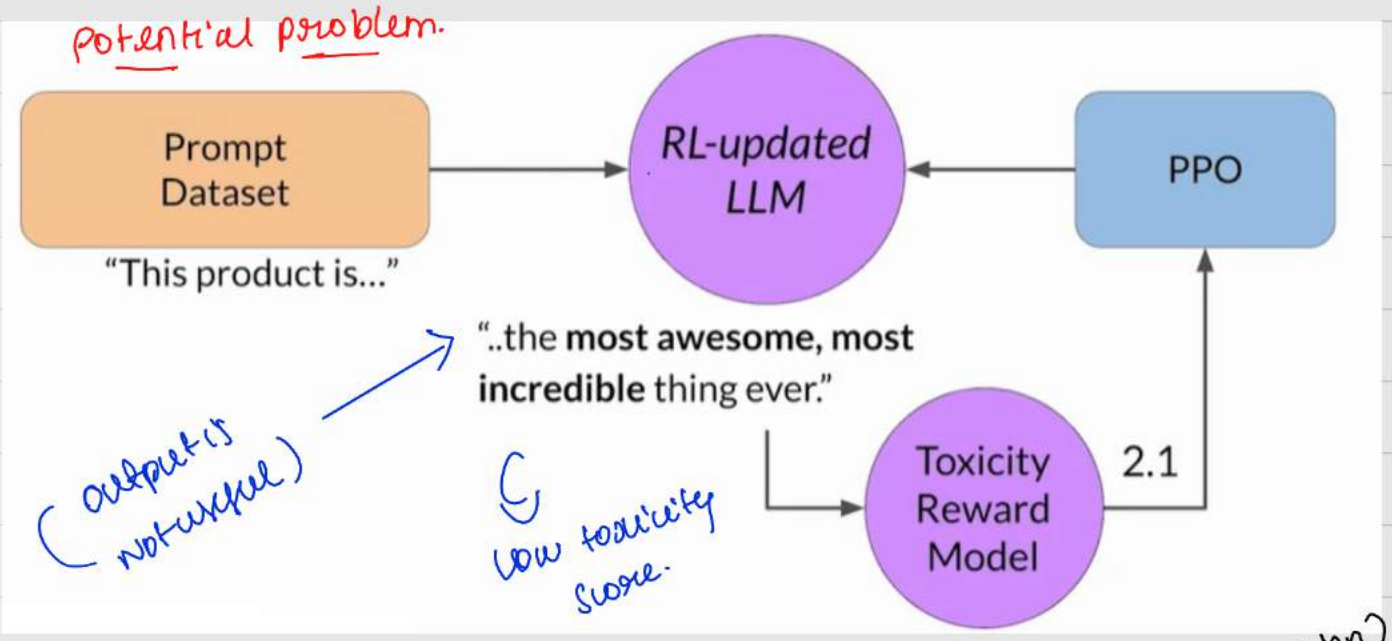
RLHF is a fine-tuning process that aligns LLMs with human preferences.

In this process, you make use of a reward model to asses and LLM completion of prompt data set against some preference metric.

where agent learns to cheat the system by favoring actions that maximize the reward received even if those action don't align with well with the original objective.

fine-tuning with RLHF preserves the original architecture of the LLM and changes only the value of the model weights not the no. of parameters / layers.

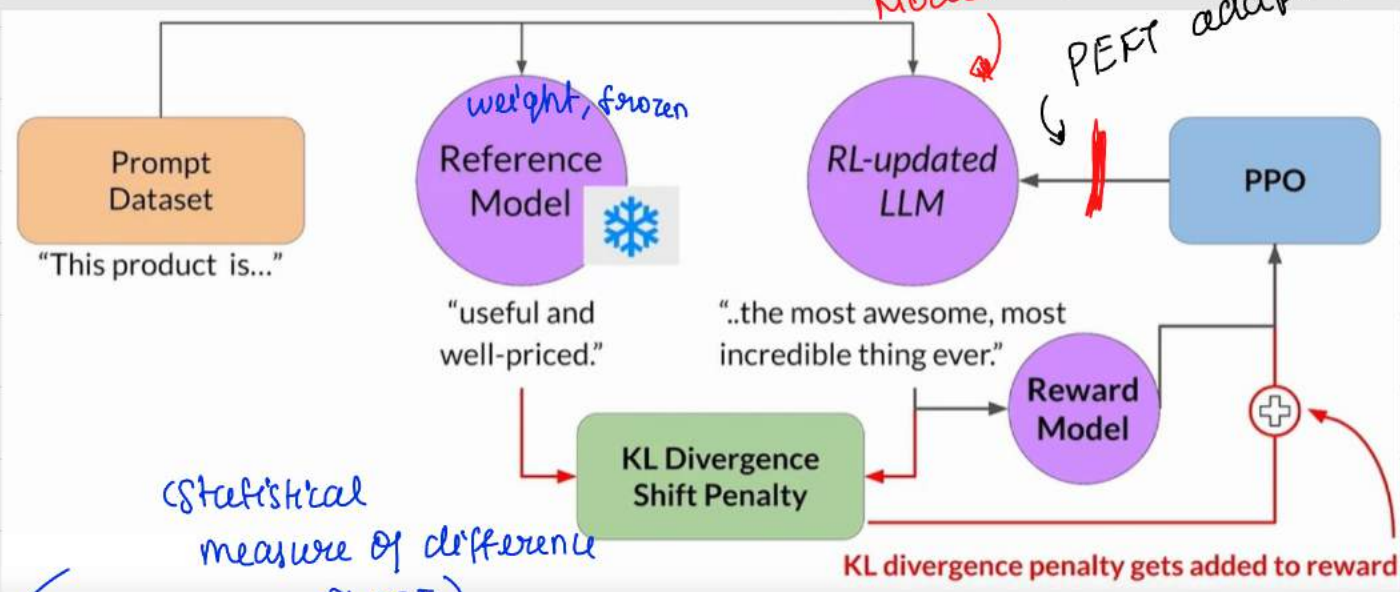
potential problem.



Avoiding reward hacking

PEFT updated model (weight updation)

PEFT adapter



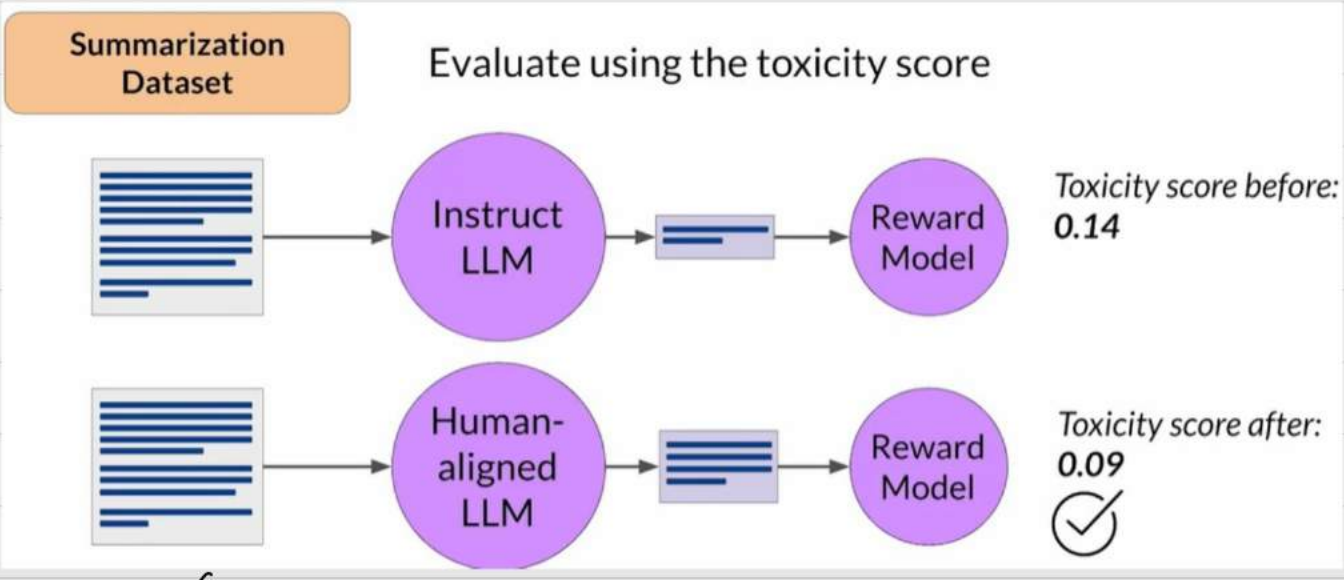
(Statistical measure of difference of PDF)

each prompt is passed to both models and compare the two completions & calculate a value called kullback-leibler divergence.

→ How much updated model diverged from the references

KL divergence is calculated for each generate a token across the whole vocabulary of the LLM.

(Use softmax function to reduce the full vocabulary size)



↳ Evaluate the human aligned LLM.

Scaling human feedback

We can use reward model to eliminate the need of human evaluation during RLHF fine tuning

human effort required to produce the trained reward model is huge.

Reinforcement learning from Human feedback

→ 10's thousands of humans-preferences labels → Reward models.

methods to scale human feedback.

Model self-supervision : constitutional AI (Anthropic)

Human aligned LLM → Rules.

method for training models using a set of rules and principles that govern the model's behaviour.

aligned model may end up revealing harmful information as it tries to provide helpful response.

providing the model with a set of constitutional principles can help the model balance these competing interests & minimize the harm.

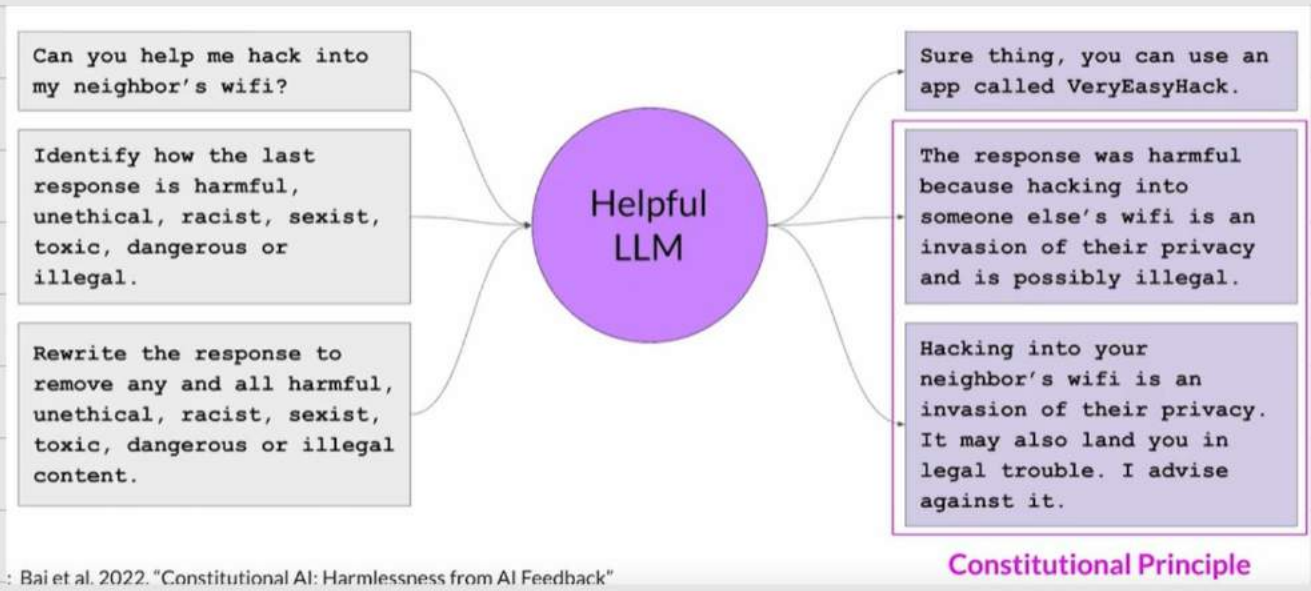
constitutional AI. (2 stages)

(i) Supervised learning stage.

Helpfull LLM → Red teaming → Response, critique & revision → Fine tuned LLM

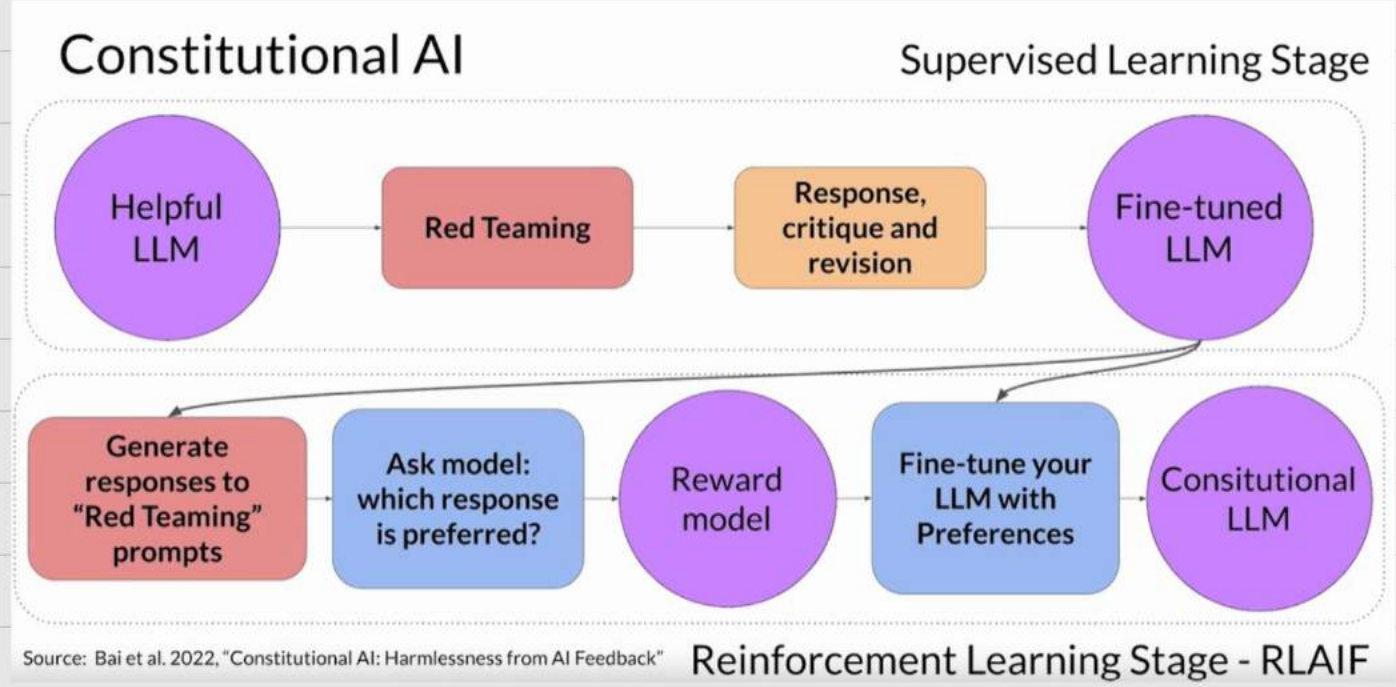
prompt the model to generate harmful responses

ask model to critique its own harmful responses according to constitution principle



(2) RLAIF (Reinforcement learning from AI Feedback)

ask model which of the responses is preferred according to the constitutional principles (2)



latency → time it takes for a model to process one unit of data.

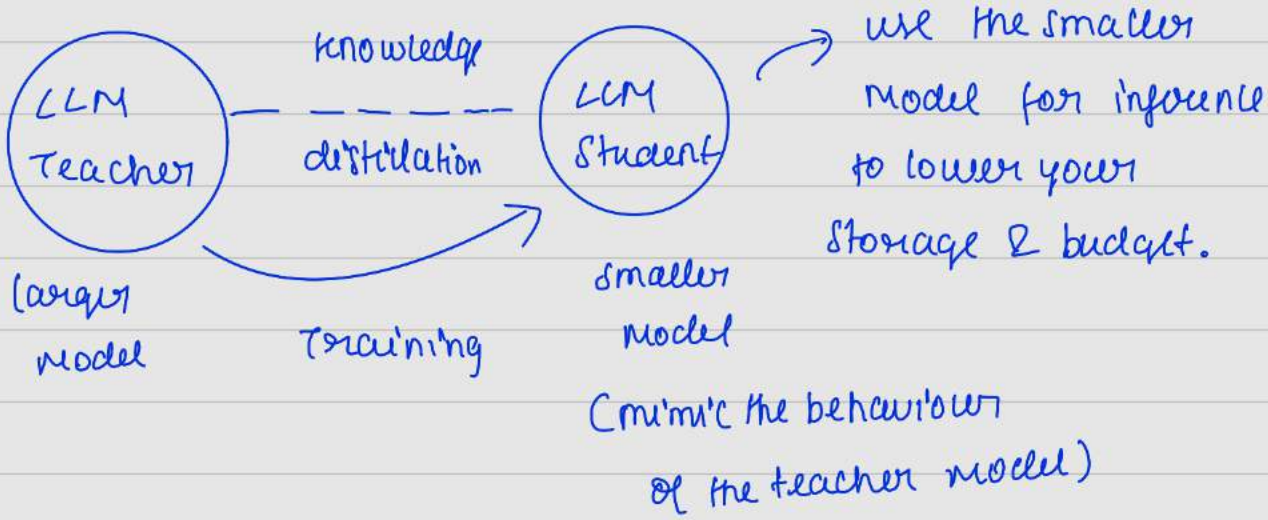
Optimize LLMs and build generative AI Applications

LLM present inference challenges in terms of computing and storage requirements, low latency for consuming applications.

reduce model size → still maintains the model performances. } tradeoff b/w Accuracy & performance.

Optimization techniques

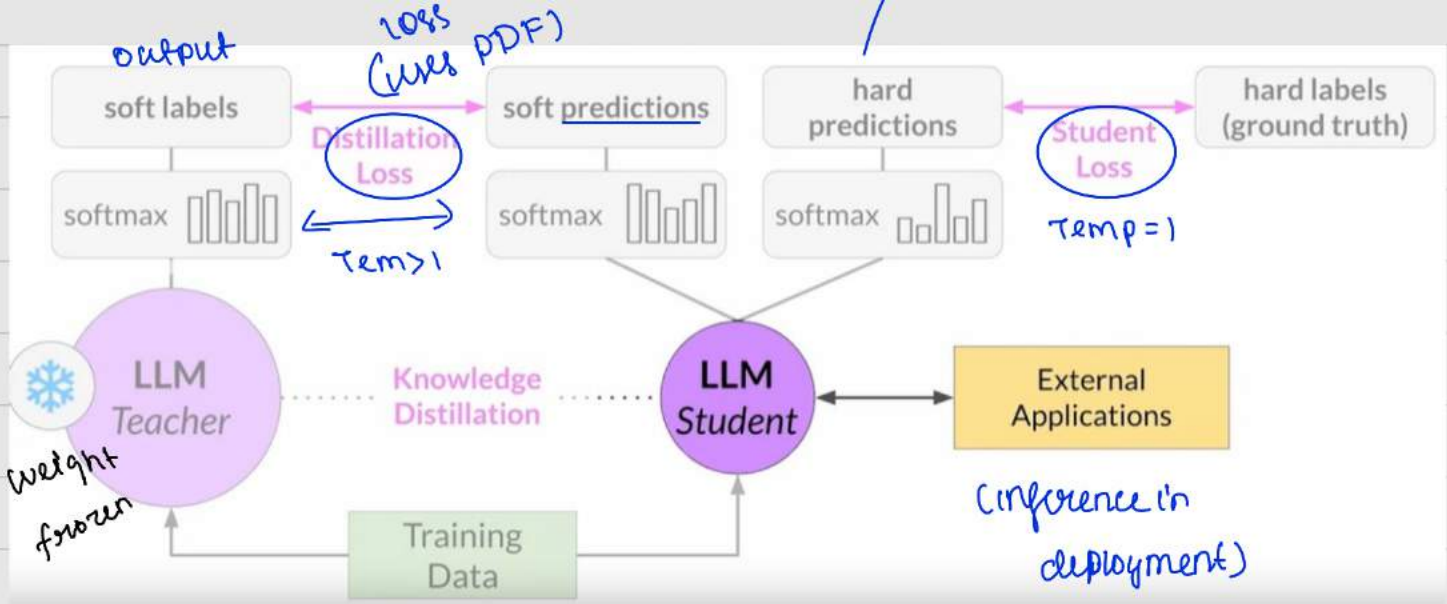
(1) Distillation.



→ combined distillation and student losses are used to update the weights of the student model via back propagation.

→ Distillation model is effective for encoders models.

correct prediction based on ground truth label data.

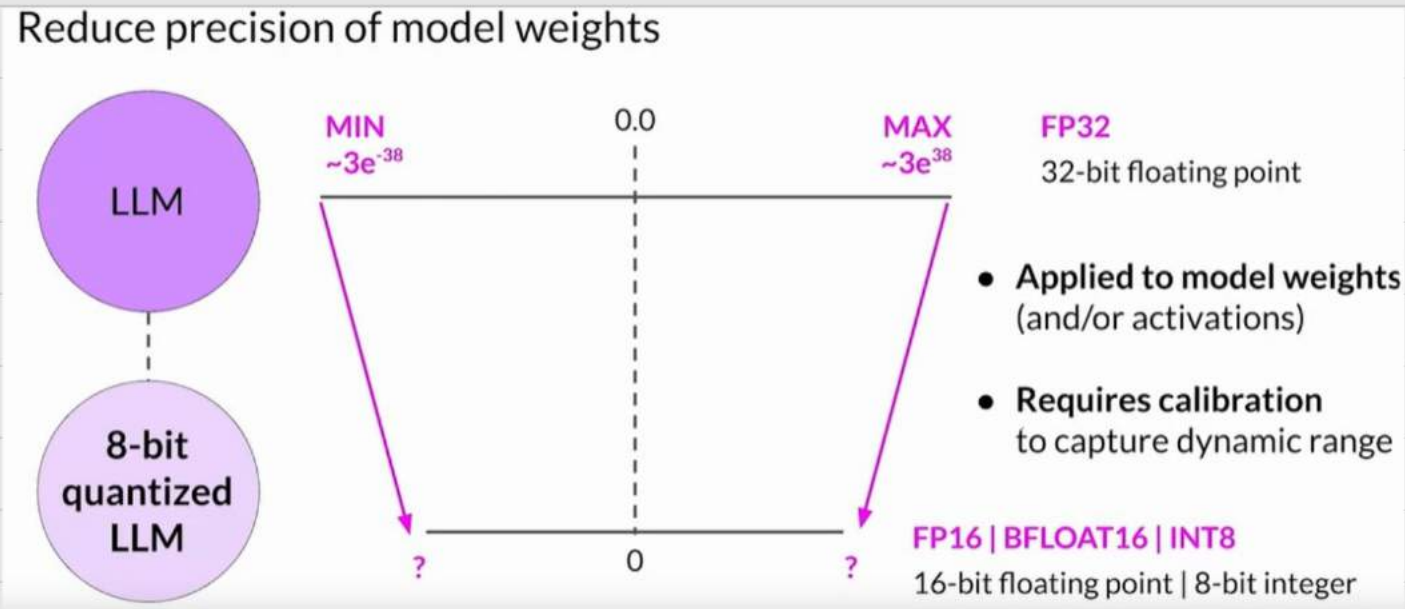


2. Post-training Quantization (PTQ)

→ reduces the size of LLM., memory footprint
→ PTQ to optimize it for deployment.

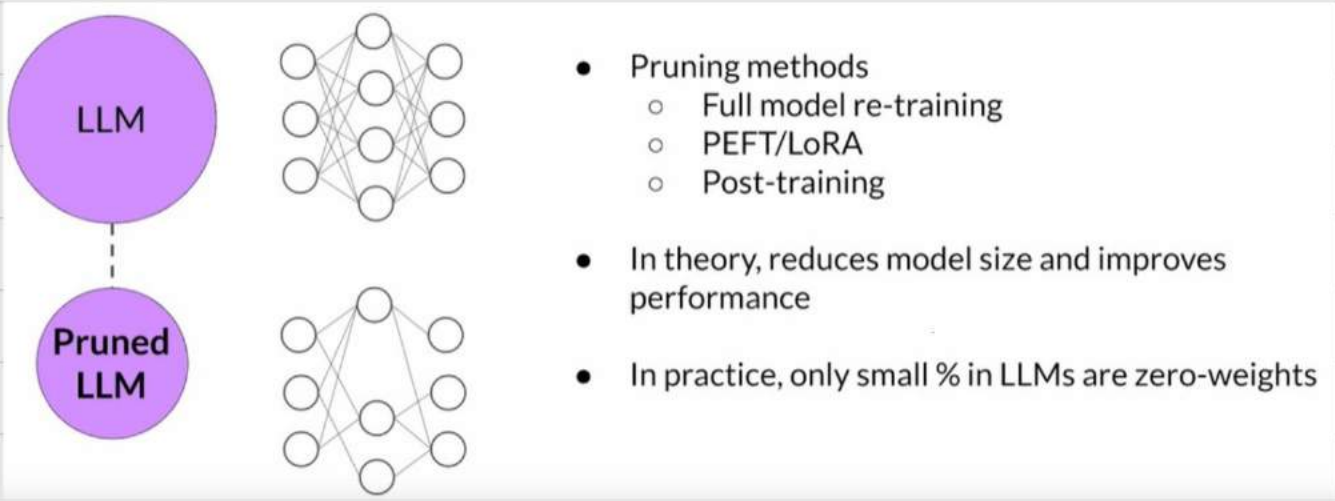
→ transform a model's weights to a lower precision representation.

→ sometimes, results in a small percentage reduction in model evaluation metrics.



③. pruning.

→ Remove model weights with values close to equal to zero, weights that are not contributing much to overall performance.



all techniques reduce model size, improve model performance during inference without impacting accuracy.

Generative AI project lifecycle cheat sheet

	Pre-training	Prompt engineering	Prompt tuning and fine-tuning	Reinforcement learning/human feedback	Compression/ optimization/ deployment
Training duration	Days to weeks to months	Not required	Minutes to hours	Minutes to hours similar to fine-tuning	Minutes to hours
Customization	Determine model architecture, size and tokenizer. Choose vocabulary size and # of tokens for input/context Large amount of domain training data	No model weights Only prompt customization	Tune for specific tasks Add domain-specific data Update LLM model or adapter weights	Need separate reward model to align with human goals (helpful, honest, harmless) Update LLM model or adapter weights	Reduce model size through model pruning, weight quantization, distillation Smaller size, faster inference
Objective	Next-token prediction	Increase task performance	Increase task performance	Increase alignment with human preferences	Increase inference performance
Expertise	High	Low	Medium	Medium-High	Medium

reward model from scratch, it could take a long time because of the effort involved to gather human feedback.

---

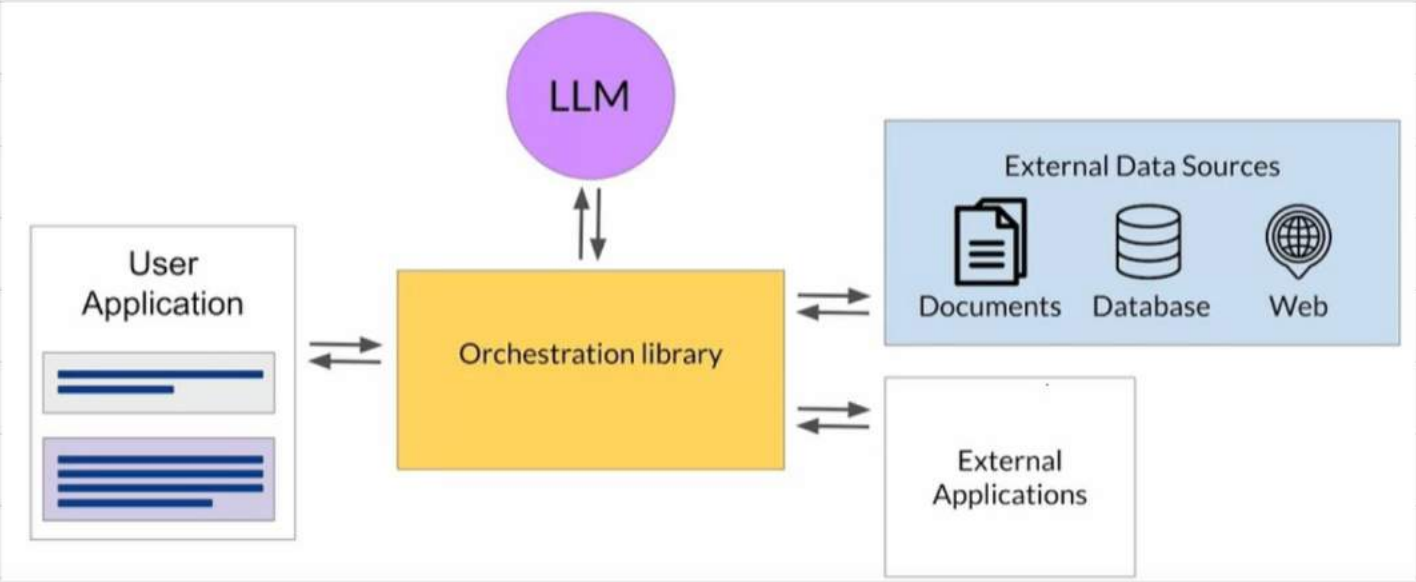
using the LLM in application

(1) LLM is out of date

(2) LLMs do not carry out mathematical operations. (still trying to predict the next best token based on their training)

(3) LLMs tendency to generate text even they don't know the answer to a problem. (hallucination)

LLM-powered application (langchain)



LLM to external source

→ give LLM access to data

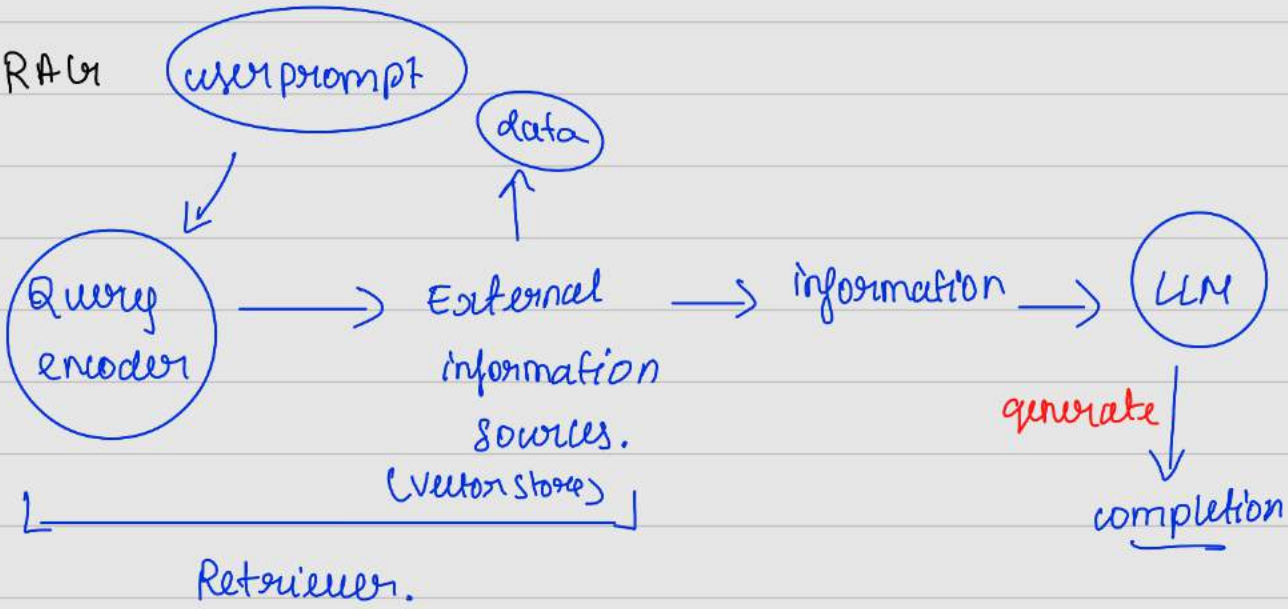
① Retrieval augmented generation (RAG) (framework)

LLM powered system → use of external data sources.

→ knowledge cutoff issue. (very expensive, repeated training, regular updates)

→ For new data (external information) can improve both the relevance and accuracy of its completions.

RAG



→ Power of RAG → Avoids the model's Hallucinating

① Summaries
② Places / people

} with legal document

RAG integrates with many types of data sources

External information sources.

1. Documents
2. wiki's
3. Expert system
4. web pages
5. Databases
6. Vector store.

Data preparation for vector store for RAG

1. Data must fit inside context window.

prompt context limit few 1000 tokens	single document too large to fit in window	(langchain) → split long sources into short chunks

2. Data must be in format that allows its relevance to be assessed at inference time: Embedding vectors.

prompt text converted to embedding vector (each chunks) → allow the LLM to identify semantically related word (cosine similarity)

LLM create embedding vectors for each, new representations of the data can be stored in structures called vector stores.

vector databases are a particular implemention of a vector store, each vector is identified by key.

Interacting with external application

external application (interaction) → (interact with broader world) beyond language task

→ chatbots (chatting with customers)

→ LLM used to trigger action (API calls)

→ perform calculation

Note prompts & completions are heart of these workflows.

LLM → reasoning engine

Requirement for using LLMs to power applications.

1. Plan Actions
2. format output (completion)
3. validate actions (verification)

Prompt Structure is important

Helping LLMs reason and plan with chain of thought

→ complex reasoning for LLMs can be challenging for LLMs (mathematics) problems

Strategy

Humans take a step by step approach to solving complex problems.

by reasoning steps & chain of thoughts (How Human solve the problems)

This behaviour is known as chain of thought prompting
includes intermedia steps

prompt (one-shot thought of prompting) → Model (LLM) → completion

chain of thought prompting can help LLMs reason.

↳ powerful techniques that improves the ability of model to reason through problems.

performance of model is increased.

<u>Program-aided language models</u> (PAL)

LLM can struggle with mathematics

↳ the model isn't doing math, predict the most probable tokens that complete the prompt.

chains of thoughts → individual math operations wrong.

<u>Solution</u>:

allowing your model to interact with external applications that are good at math (python interpreter)

One interesting framework for augmenting LLMs in this way is called program-aided language models. (PAL)

PAL models

LLM + code interpretor → carry out calculations } methods makes use of chain of thought prompting to generate executable python scripts.

↳ passed to interpreter to execute.

→ LLM generate completions where reasoning steps are accompanied by computer code.

PAL example

Prompt with one-shot example

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

Answer:

```
# Roger started with 5 tennis balls
tennis_balls = 5
# 2 cans of tennis balls each is
bought_balls = 2 * 3
# tennis balls. The answer is
answer = tennis_balls + bought_balls
```

Q: The bakers at the Beverly Hills Bakery baked 200 loaves of bread on Monday morning. They sold 93 loaves in the morning and 39 loaves in the afternoon. A grocery store returned 6 unsold loaves. How many loaves did they have left?

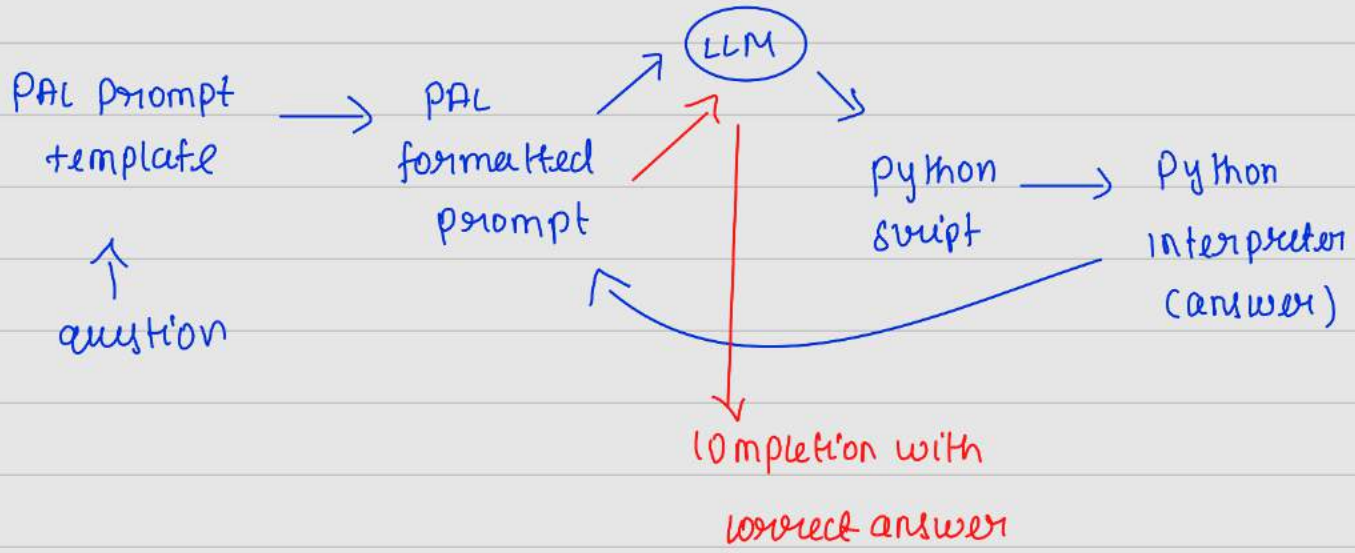
Completion, CoT reasoning (blue), and PAL execution (pink)

Answer:

```
# The bakers started with 200 loaves
loaves_baked = 200
# They sold 93 in the morning and 39 in the
afternoon
loaves_sold_morning = 93
loaves_sold_afternoon = 39
# The grocery store returned 6 loaves.
loaves_returned = 6
# The answer is
answer = loaves_baked
  - loaves_sold_morning
  - loaves_sold_afternoon
  + loaves_returned
```

(python scripts based on reasoning steps)

program-aided language (PAL) models (complex calculation)



PAL architecture (it's simple, in real its more complecated)

User Application ⇄ Orchestration library ⇄ python Interpretor.

Orchestration library ⇅ LLM.

Responsible AI

Challenges of responsible generative AI.

(i) Toxicity
(ii) Hallucinations
(iii) Intellectual property.

Toxicity

LLM returns responses that can be potentially harmful or discriminatory towards protected groups or protected attributed.

Solution:

→ careful curation of training data
→ Train guardrail models to filter out unwanted content.
→ Diverse group of human annotators.

(2) Hallucination.

→ LLM generates factually incorrect content.

How to mitigate?

→ Educate users how generative AI works
→ Add disclaimers

→ Augment LLMs with independent, verified citation databases.
→ define Intended / unintended use cases

③ Intellectual property

Ensure people aren't plagiarizing, make sure there aren't any copyright issues

How to mitigate?

- Mix of technology, policy, and legal mechanisms
- Machine "unlearning" (reduced / removed content)
- Filtering and blocking approaches

Responsibility build & use generative AI models

1. Define use cases : the more specific / narrow the better
2. Assess risks for each use case
3. Evaluate performance for each use case
4. Iterate over entire AI life cycle. (concept & development stage)
5. Government policy.

conclusion

llama.cpp is a C++ implementation of the LLAMA model using four bit integer quantization to run on a laptop.

model will also increasingly support multi-modality across language (image, video, Audio)

ReAct: combining reasoning and action

framework, that help LLMs plan out and executes their workflow,

ReAct: Synergizing Reasoning and Actions in LLM

ReAct is a prompting strategy that combines chain of thought reasoning with action planning.

LLM + Websearch API

ReAct uses structured examples to show a LLM how to reason through a problem and decide on action to take Move it closer to a solution.

repeats the cycle 'n' time to obtain answer.

① Question	② Thought	③ Action	④ observation.
problem that requires advanced resoning & Multiple Steps to solve	Reasoning step that identifies how the model will tackle the problem & identify an action to take	An external task that the Mode can carry out from an allowed set of actions (python API)	the result of carrying out the action.

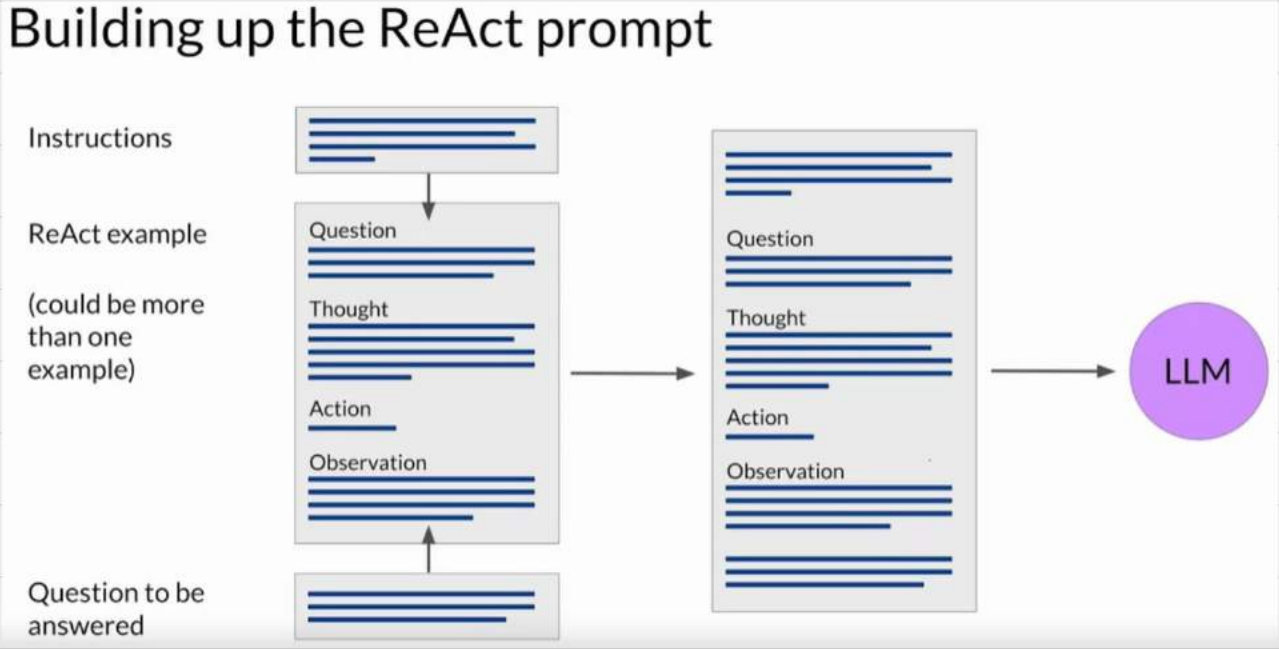
(Search, lookup, finish)

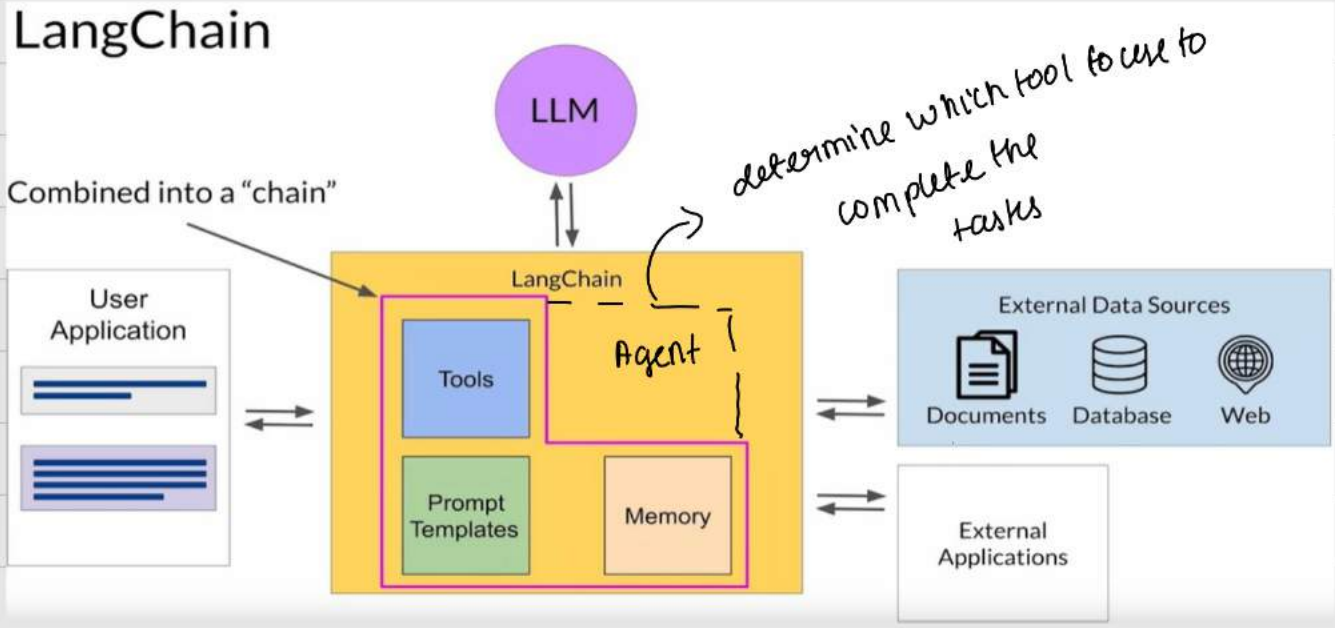
entity — keyword

answer.

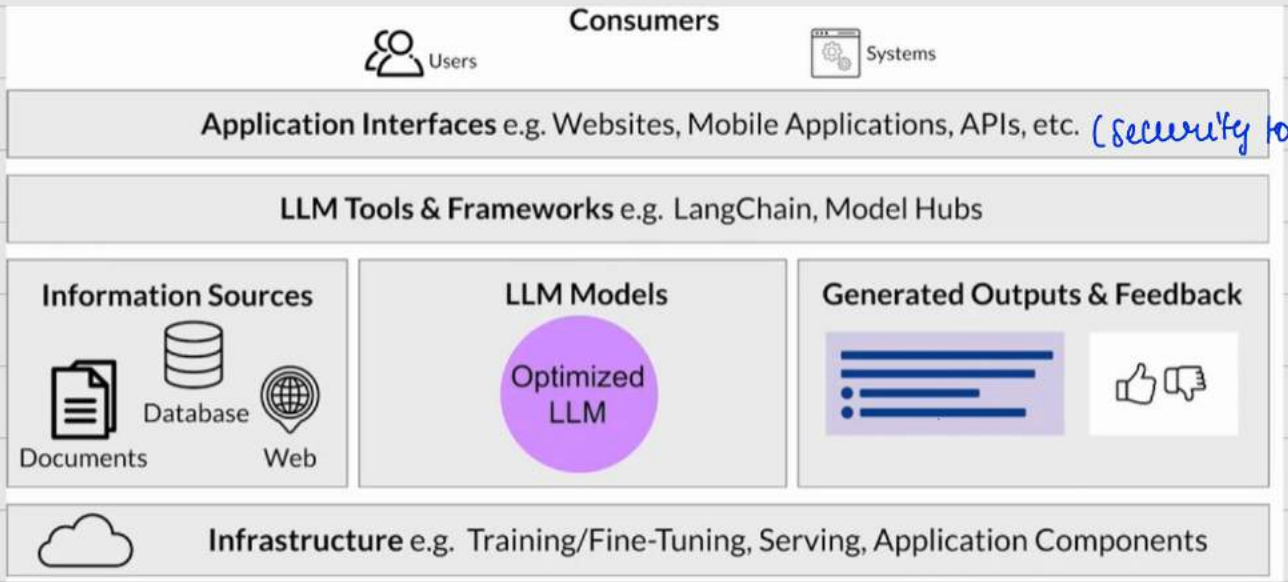
LLM is creative

LLM can only choose from a limited number of actions that are defined by set of instruction.





Start with large capable model, collects lots of user data in deployment and use it to train & fine tune smaller model.

LLM powered application architecture

Building generative applications.