

LLM Is All You Need

Tarbiat Modares University

Dr Mehdi Roayaei

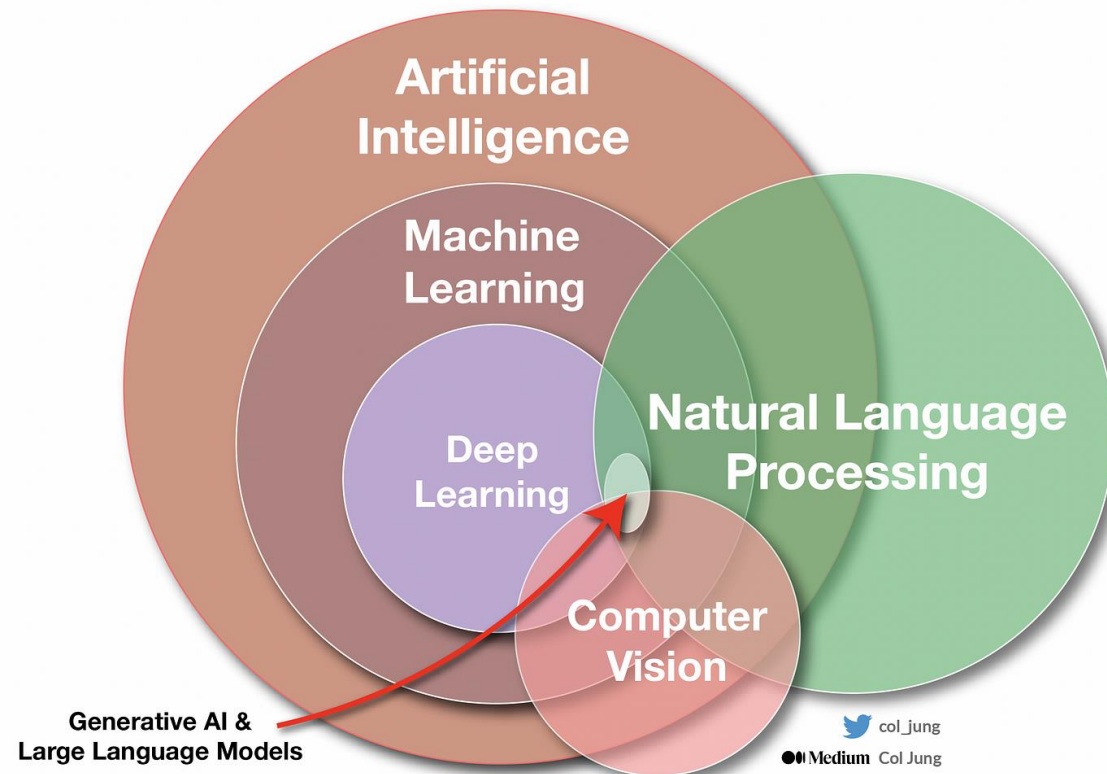
Presented by: Hanieh Sartipi

May 2025



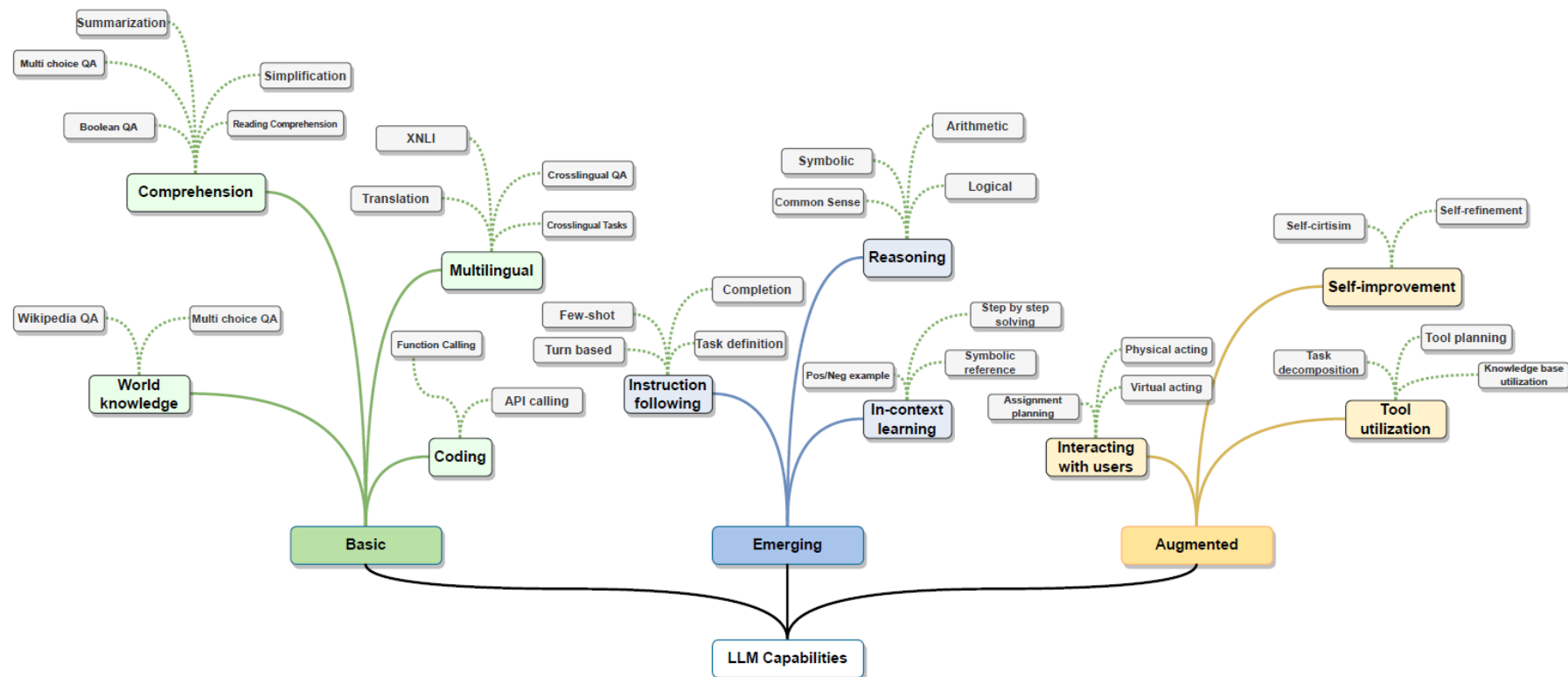
Large Language Models

- Language is a core human ability for expression and communication.
- Machines lack natural understanding of human language.
- Language Modeling is one of the major approaches to advancing language intelligence of machines.



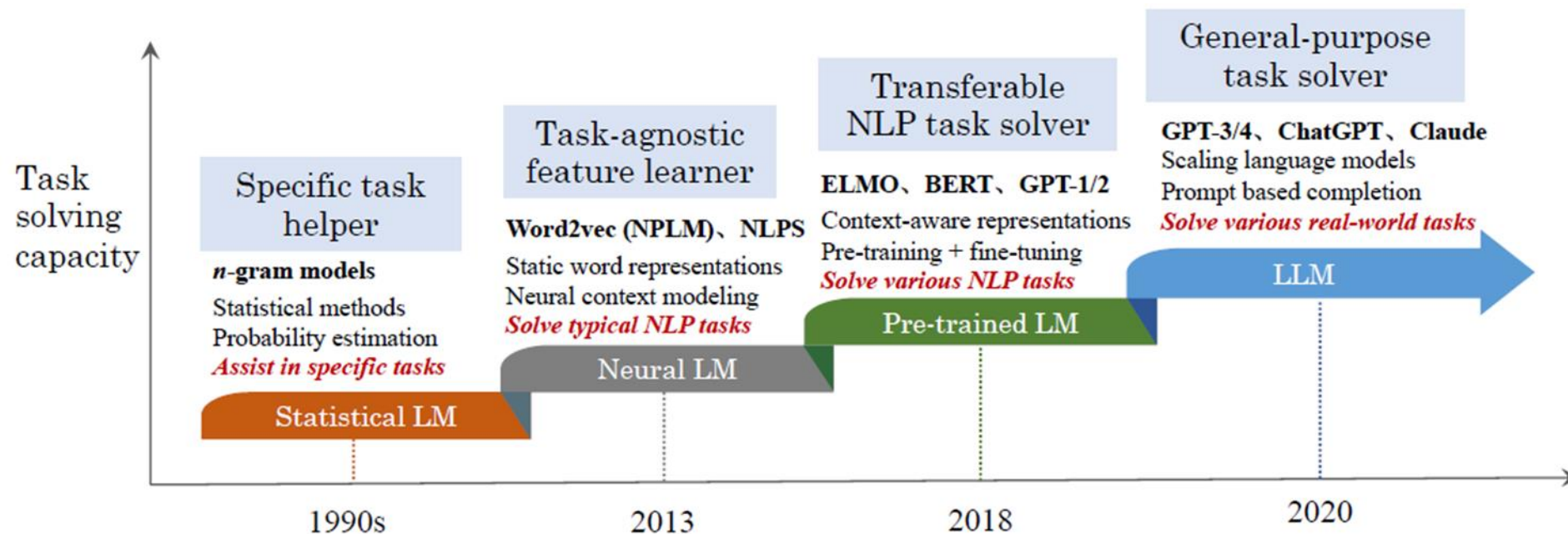
Large Language Models

- An LLM is a type of AI model that excels at understanding and generating human language. They are trained on vast amounts of text data, allowing them to learn patterns, structure, and even nuance in language. These models typically consist of many millions of parameters.



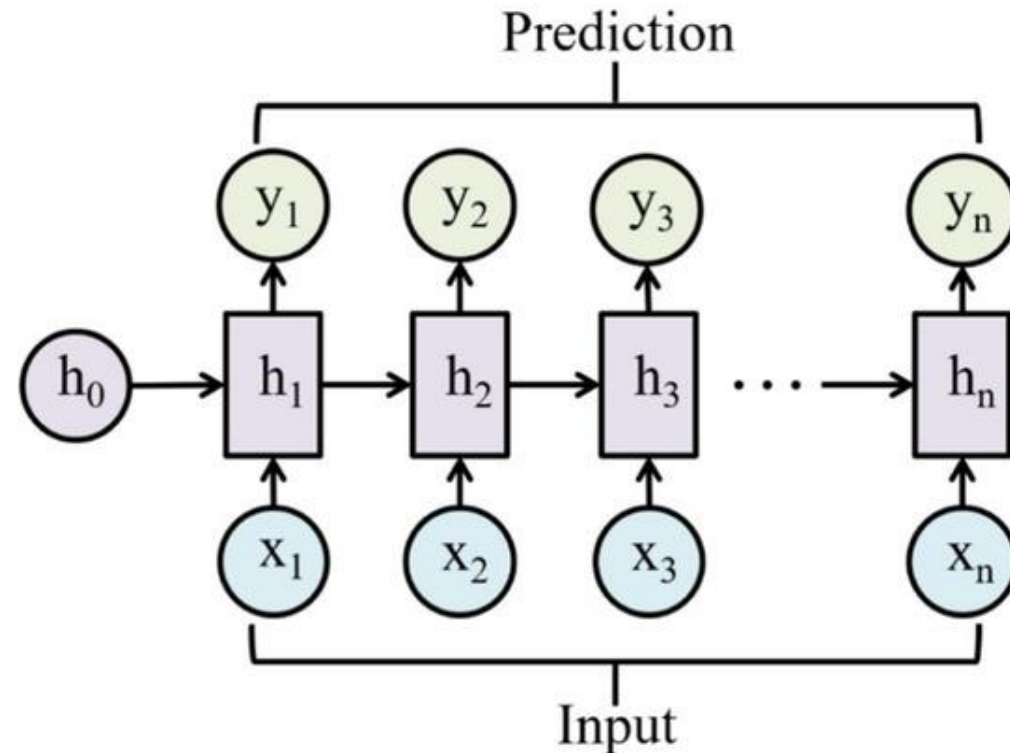
Evolution of language models

The research of LM has received extensive attention in the literature, which can be divided into four major development stages:



From RNNs to Transformers

- Process input sequences left to right → capture word order, distance, and local context.



From RNNs to Transformers



Strengths of RNNs:

- Preserve sequential structure and temporal dependencies.

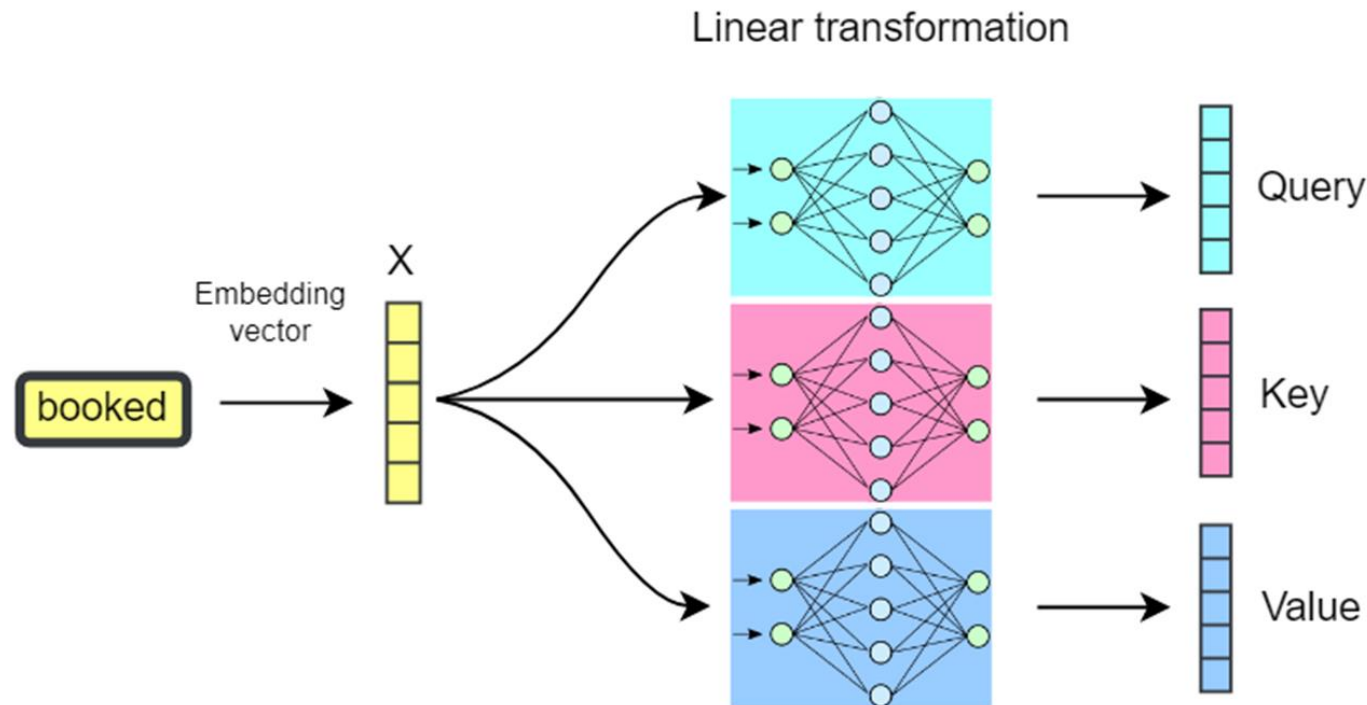


Limitations of RNNs:

- Entire input compressed into a single hidden state → information bottleneck.
- Cannot be parallelized due to step-by-step (sequential) processing.
- Suffer from vanishing gradient problems on long sequences.

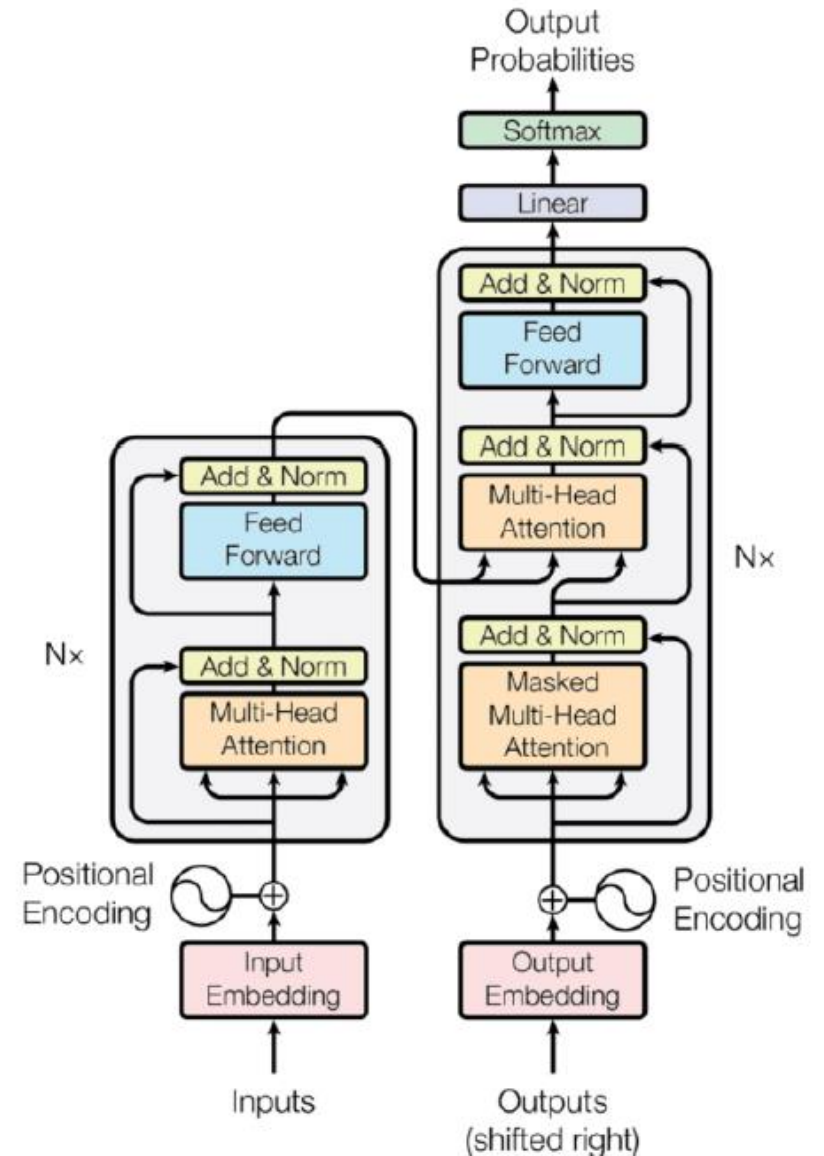
Attention

- Value = the possible meanings
- Query & Key = selectors that decide which meanings matter in this sentence
- Attention output = a context-aware meaning of the word
- I bought apple stock



Transformer

- Highly interpretable
- Solves vanishing gradient issue
- Parallel training
- Data availability
- Self-supervised approach of pretraining
- Hardware improvements
- Quadratic time computation



Types of transformers

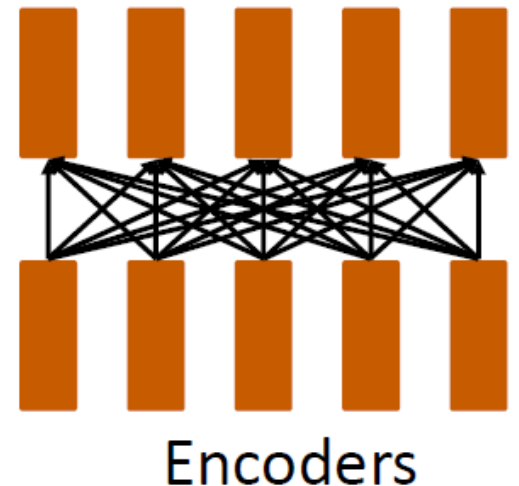
1. Encoders

An encoder-based Transformer takes text (or other data) as input and outputs a dense representation (or embedding) of that text.

- **Example:** BERT from Google
- **Use Cases:** Text classification, semantic search, Named Entity Recognition
- **Typical Size:** Millions of parameters

Input: "The [MASK] sat on the mat."

Goal: Predict "[MASK]" = "cat"



Types of transformers

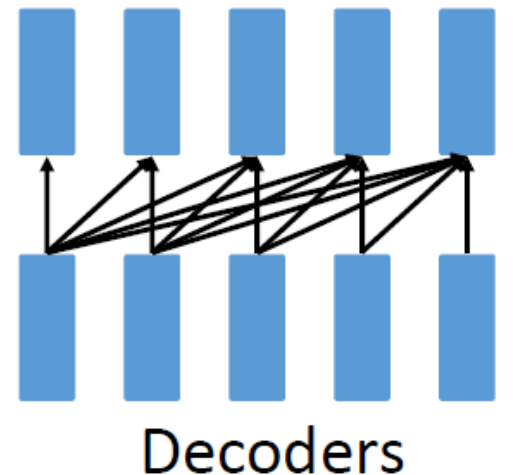
2. Decoders

A decoder-based Transformer focuses on generating new tokens to complete a sequence, one token at a time.

- **Example:** Llama from Meta
- **Use Cases:** Text generation, chatbots, code generation
- **Typical Size:** Billions of parameters

Input: "The cat sat"

Goal: Predict next = "on"

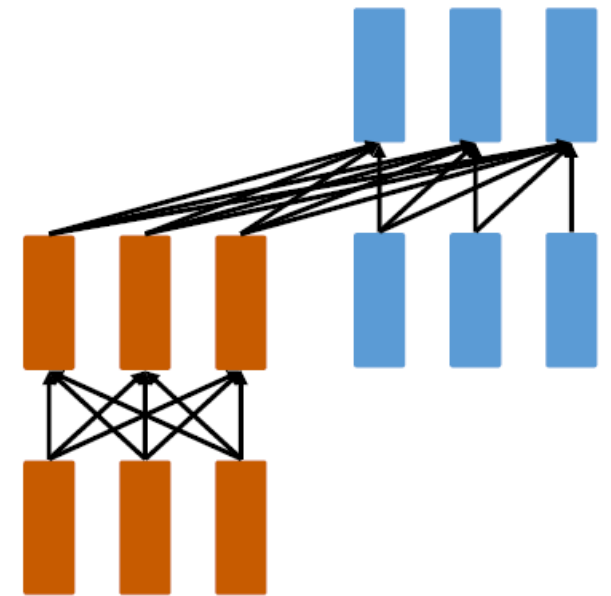


Types of transformers

3. Seq2Seq (Encoder–Decoder)

A sequence-to-sequence Transformer combines an encoder and a decoder. The encoder first processes the input sequence into a context representation, then the decoder generates an output sequence.

- **Example:** T5, BART
- **Use Cases:** Translation, Summarization, Paraphrasing
- **Typical Size:** Millions of parameters



Encoder-Decoders

LLM Use Case

- PaLM-E

Can you write me a report analyzing this chest X-ray?



Findings:

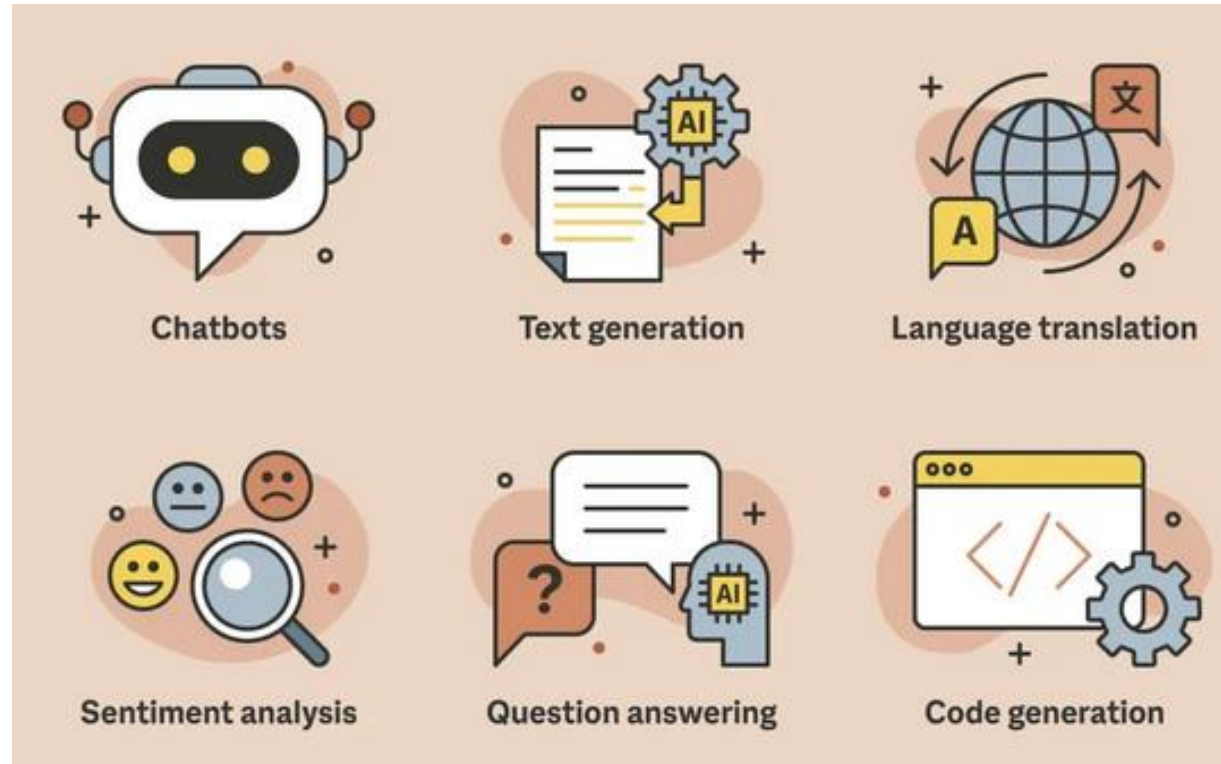
- Devices: None.
- Lungs: No pneumothorax. No substantial pleural effusion. Lungs appear clear.
- Cardiomedial: Normal heart size. Mediastinal contours within normal limits.
- Other: No acute skeletal abnormality.

Impression:

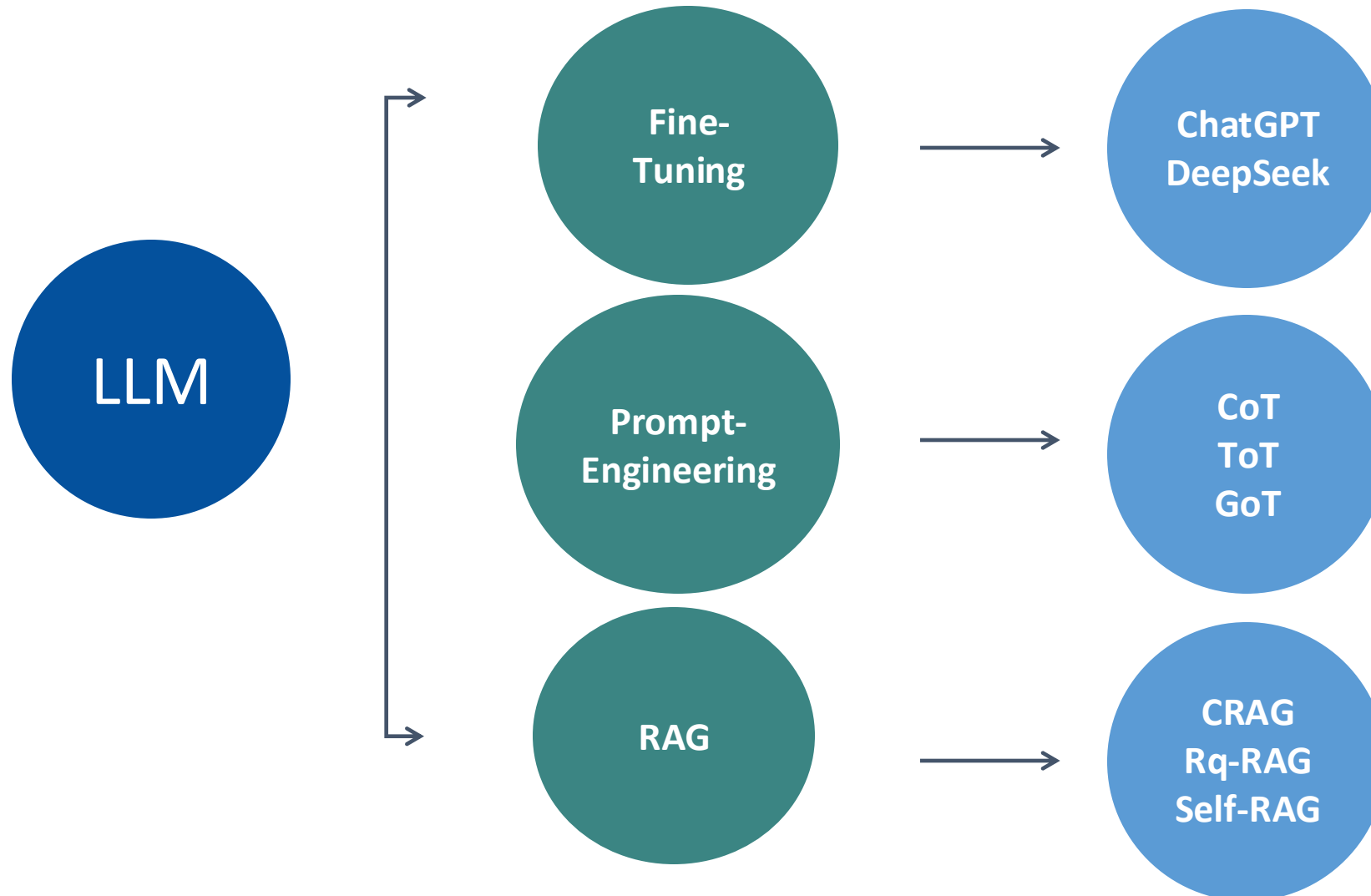
No active disease seen in chest.

Enter a question here

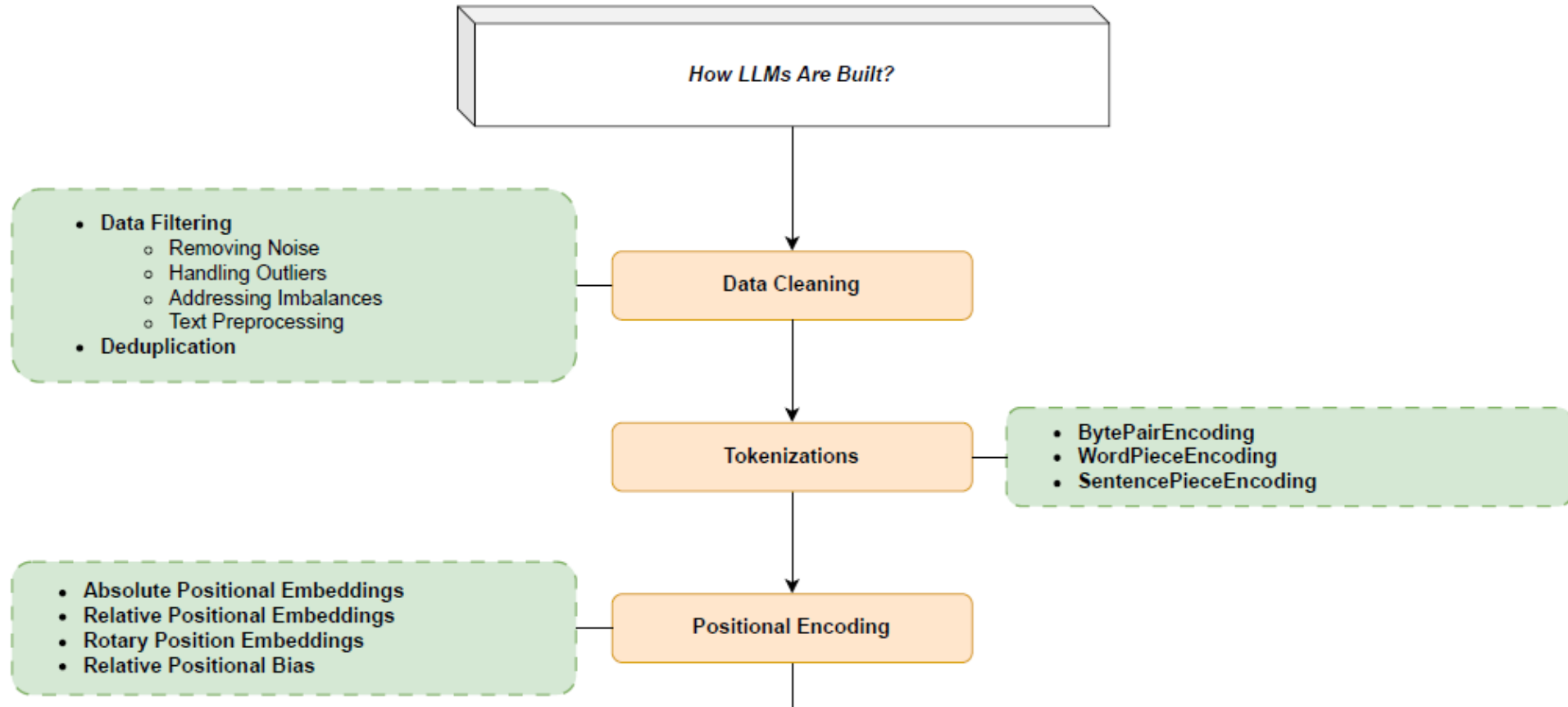
LLM Use Case



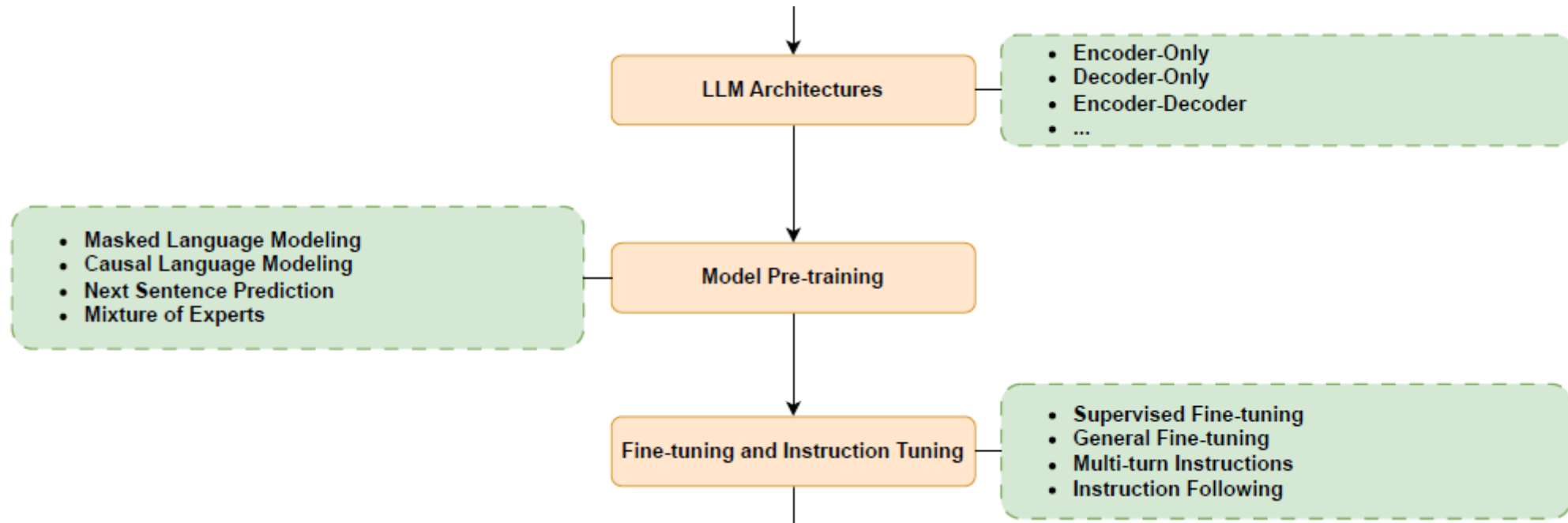
How LLMs Are Used



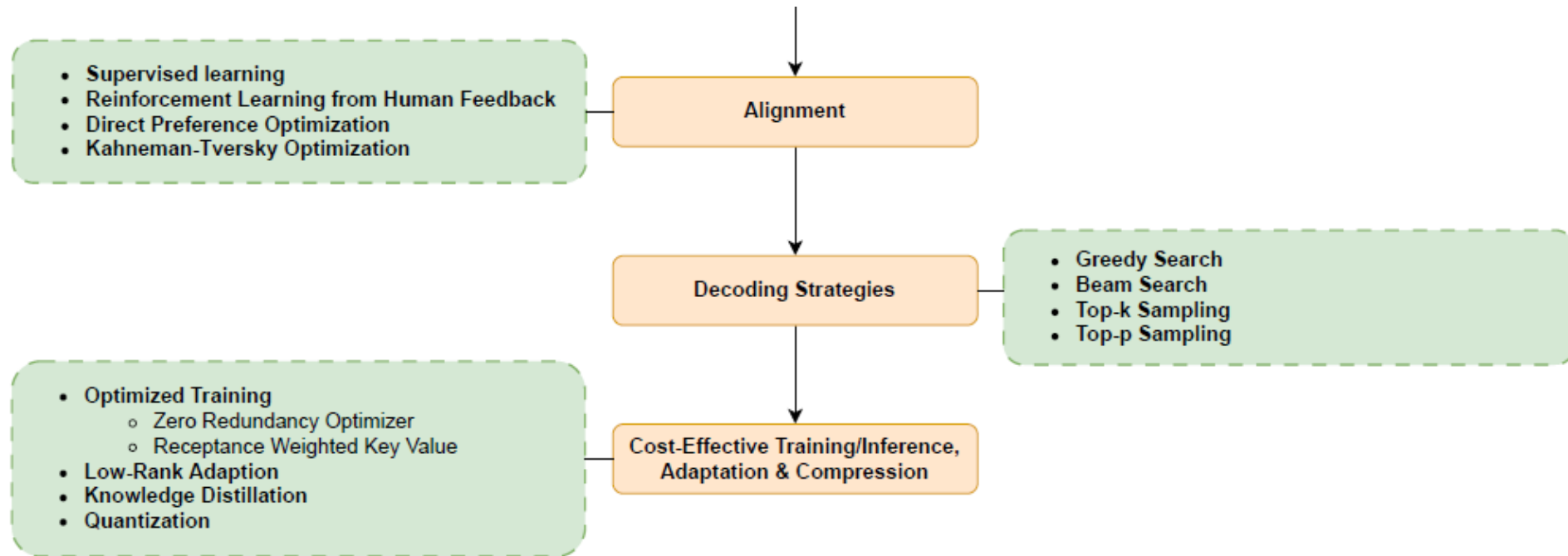
How LLMs are Built?



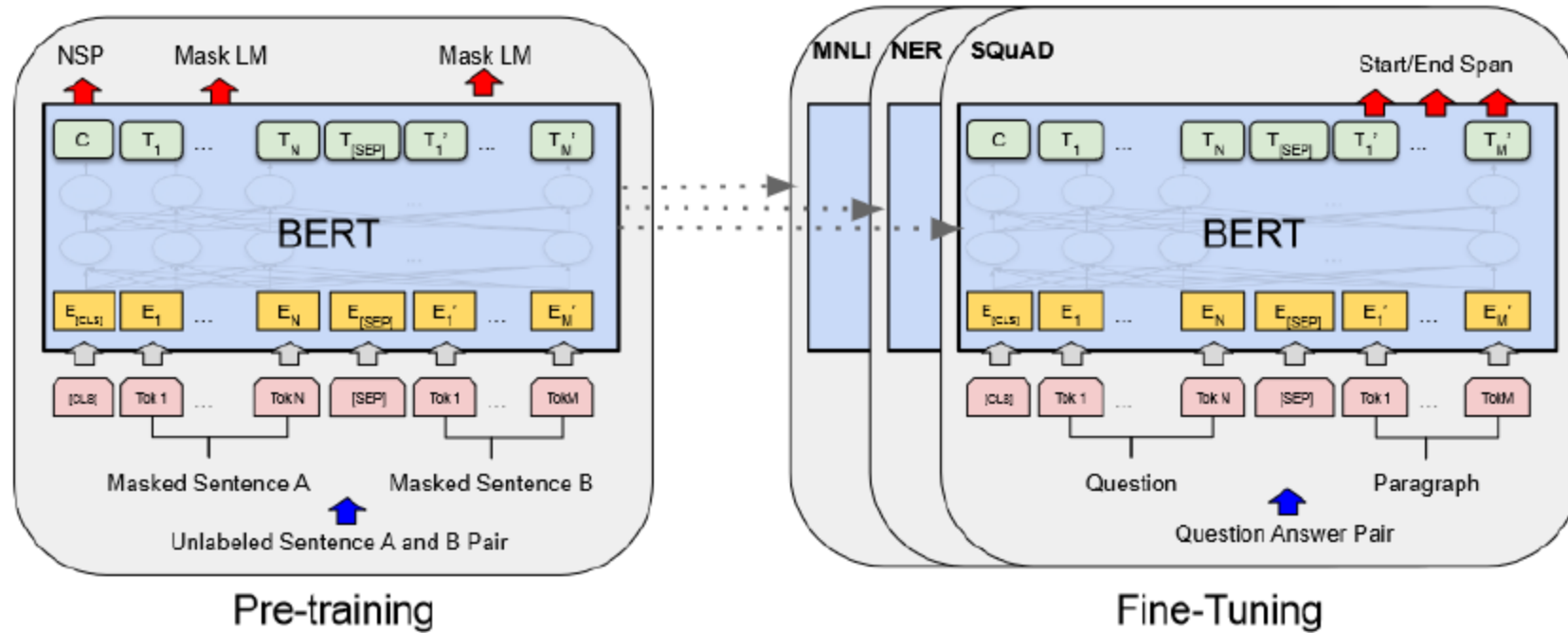
How LLMs are Built?



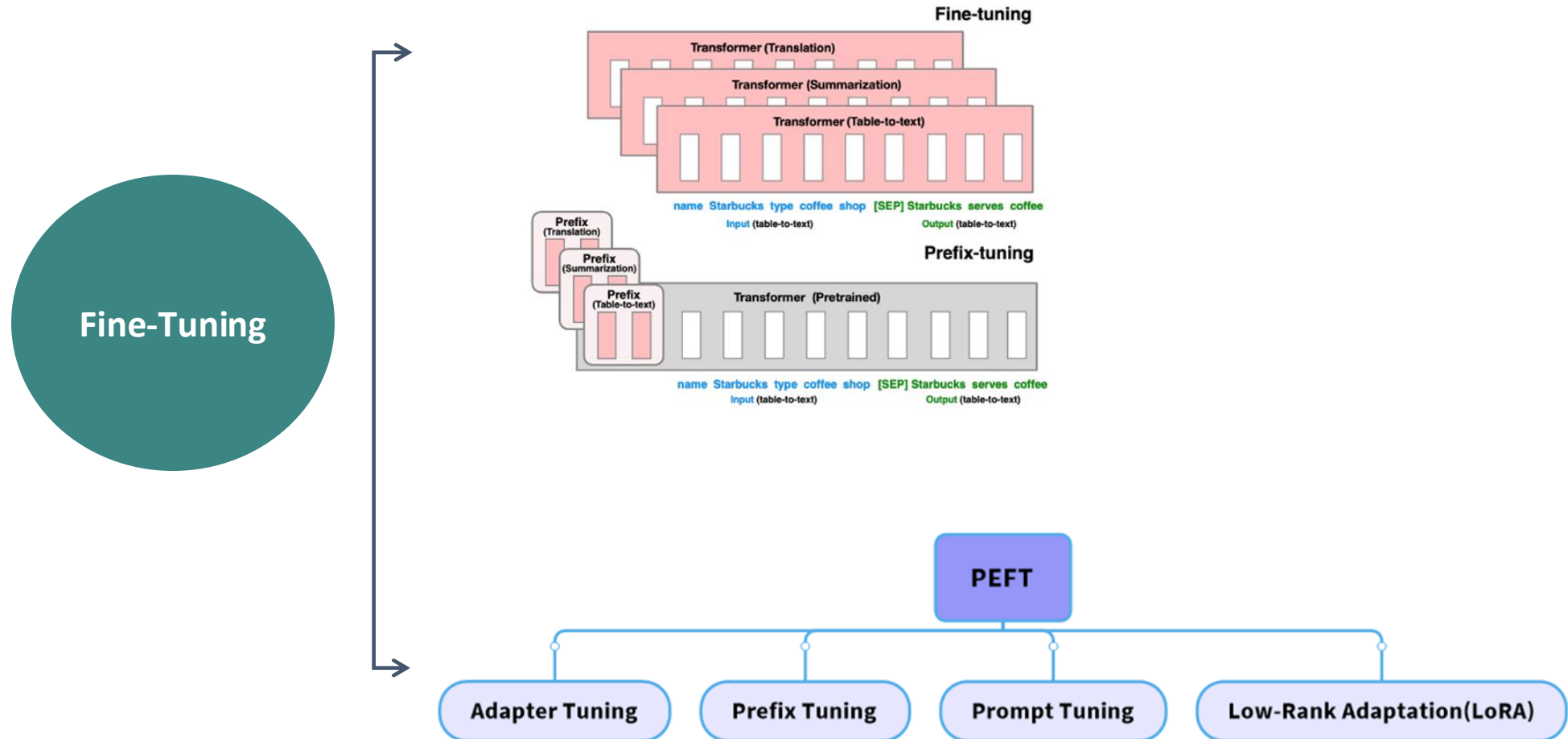
How LLMs are Built?



How LLMs are Built?



Full Fine Tuning or PEFT



RLHF

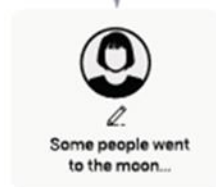
Step 1

**Collect demonstration data,
and train a supervised policy.**

A prompt is
sampled from our
prompt dataset.



A labeler
demonstrates the
desired output
behavior.



This data is used
to fine-tune GPT-3
with supervised
learning.



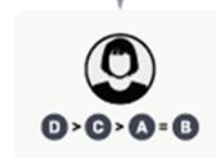
Step 2

**Collect comparison data,
and train a reward model.**

A prompt and
several model
outputs are
sampled.



A labeler ranks
the outputs from
best to worst.



This data is used
to train our
reward model.



Step 3

**Optimize a policy against
the reward model using
reinforcement learning.**

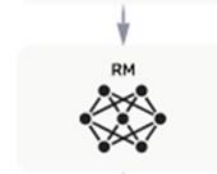
A new prompt
is sampled from
the dataset.



The policy
generates
an output.



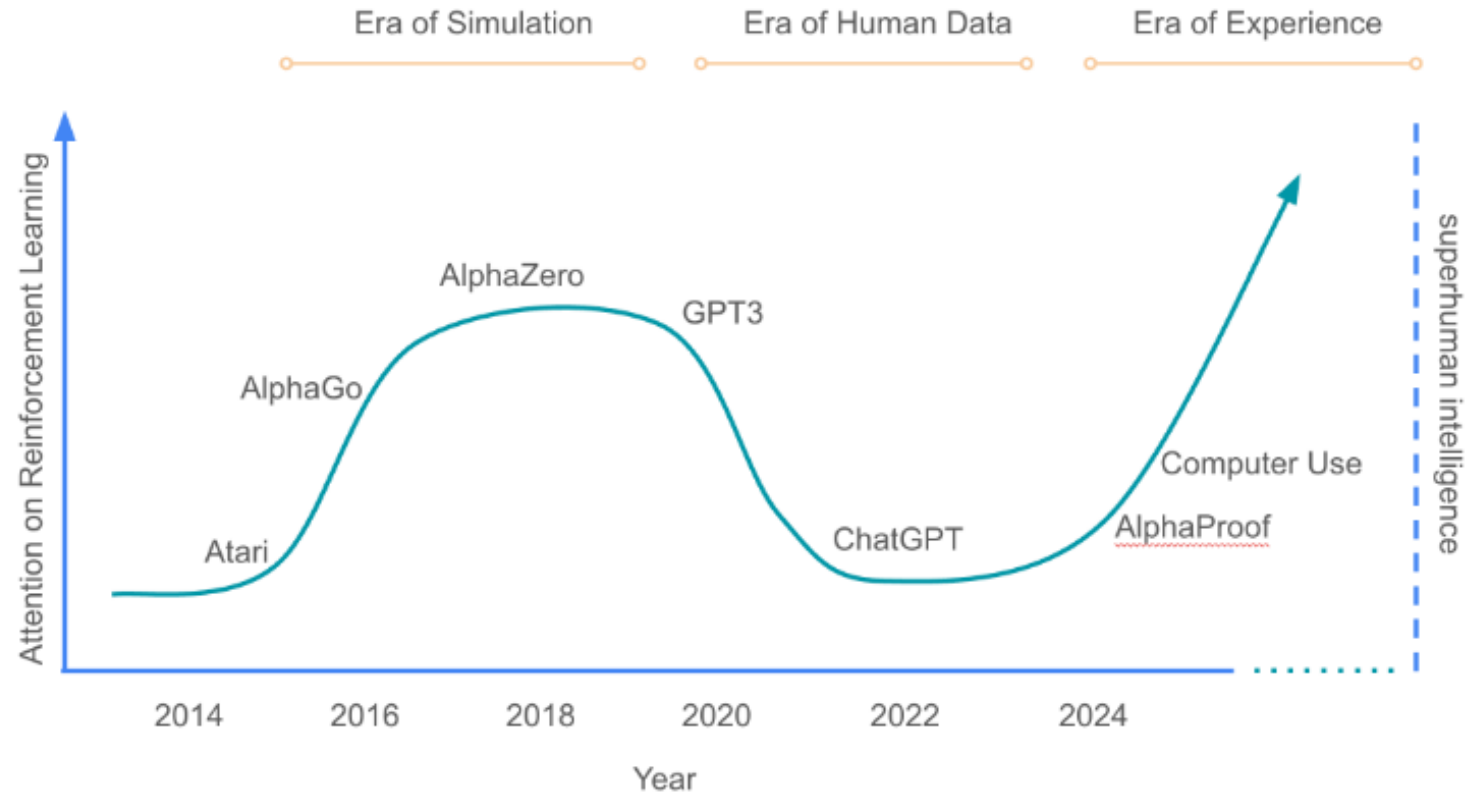
The reward model
calculates a
reward for
the output.



The reward is
used to update
the policy
using PPO.

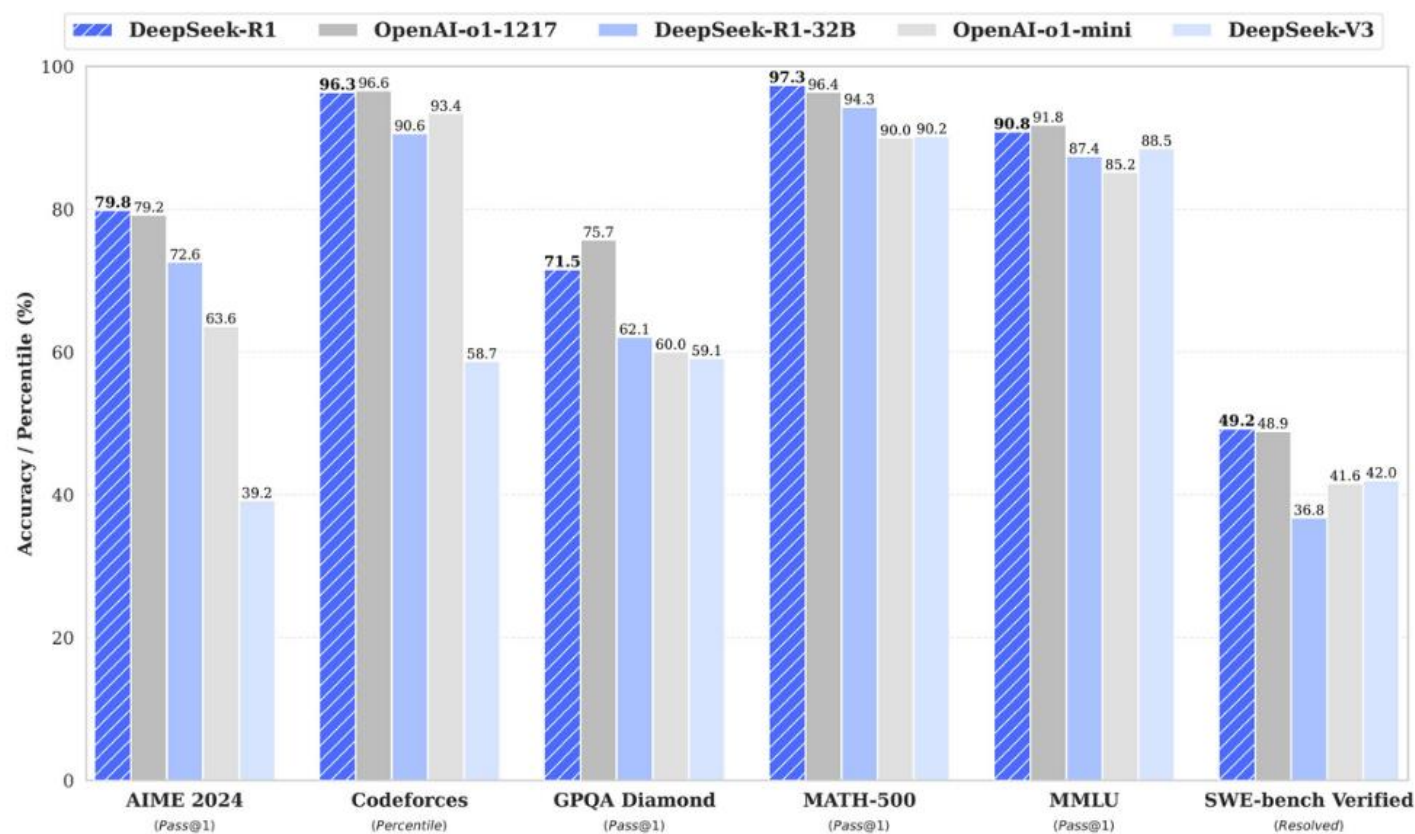


Welcome to the Era of Experience



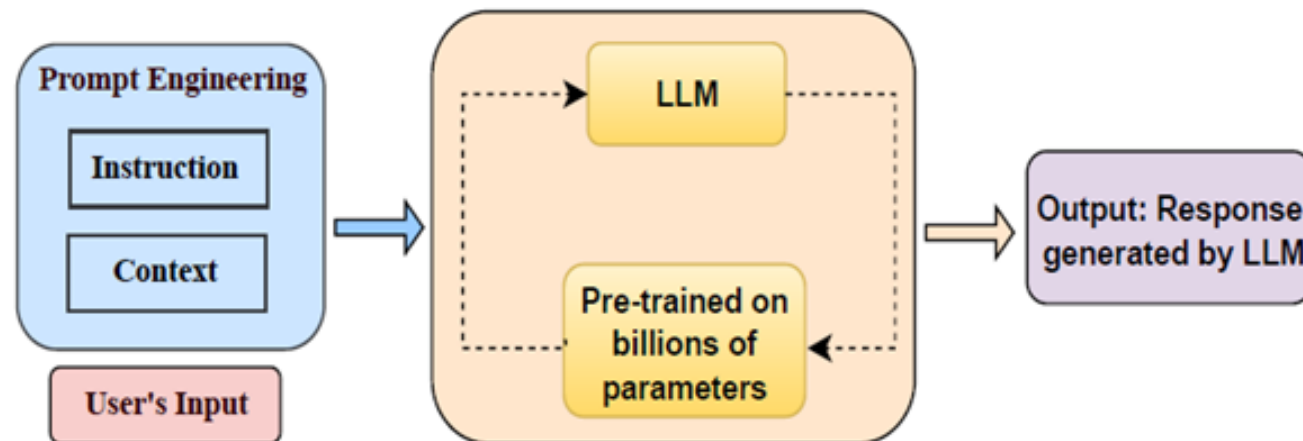
DeepSeek: Incentivizing Reasoning Capability in LLMs via RL

- DeepSeek-R1-Zero, without supervised fine-tuning



Prompt Engineering

- Prompt engineering is the process of designing and refining input prompts to guide the output of language models effectively.
- Principles of Prompting :
 1. Write Clear and Specific instructions
 2. Give the model time to think



Chain-of-Thought

A chain of thought is a series of intermediate natural language reasoning steps that lead to the final output.

Standard Prompting

Model Input

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?

A: The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

Model Output

A: The answer is 27. ❌

Chain-of-Thought Prompting

Model Input

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?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.

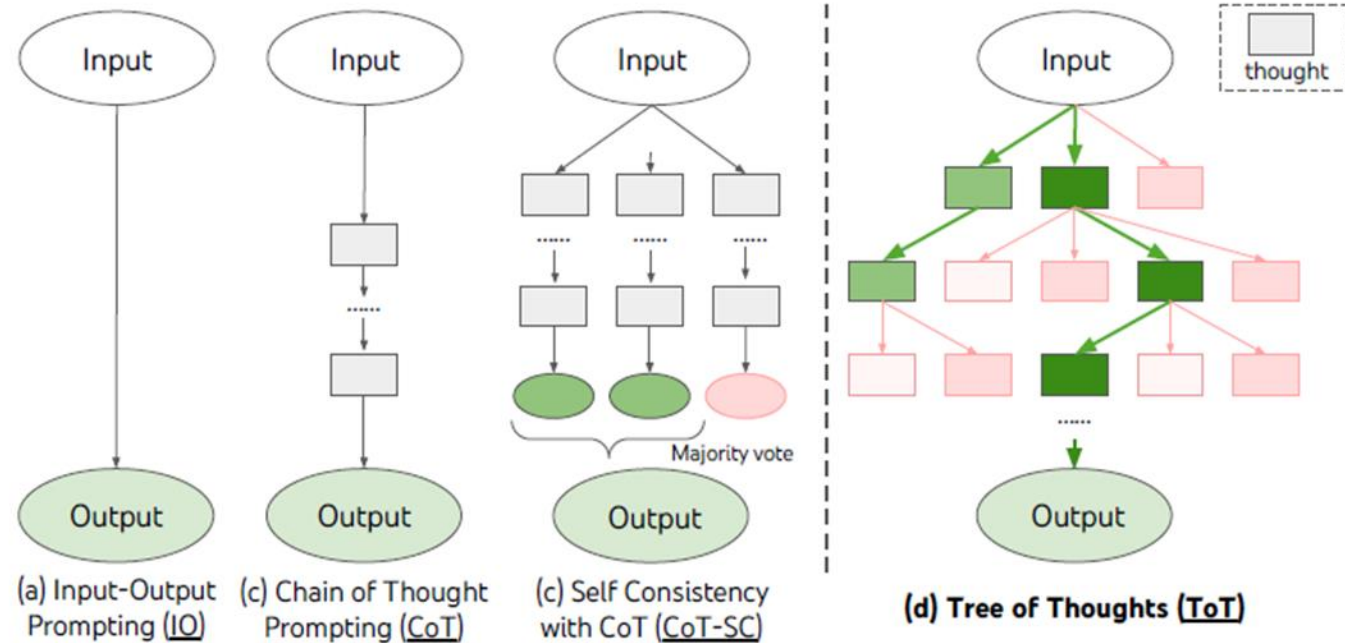
Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

Model Output

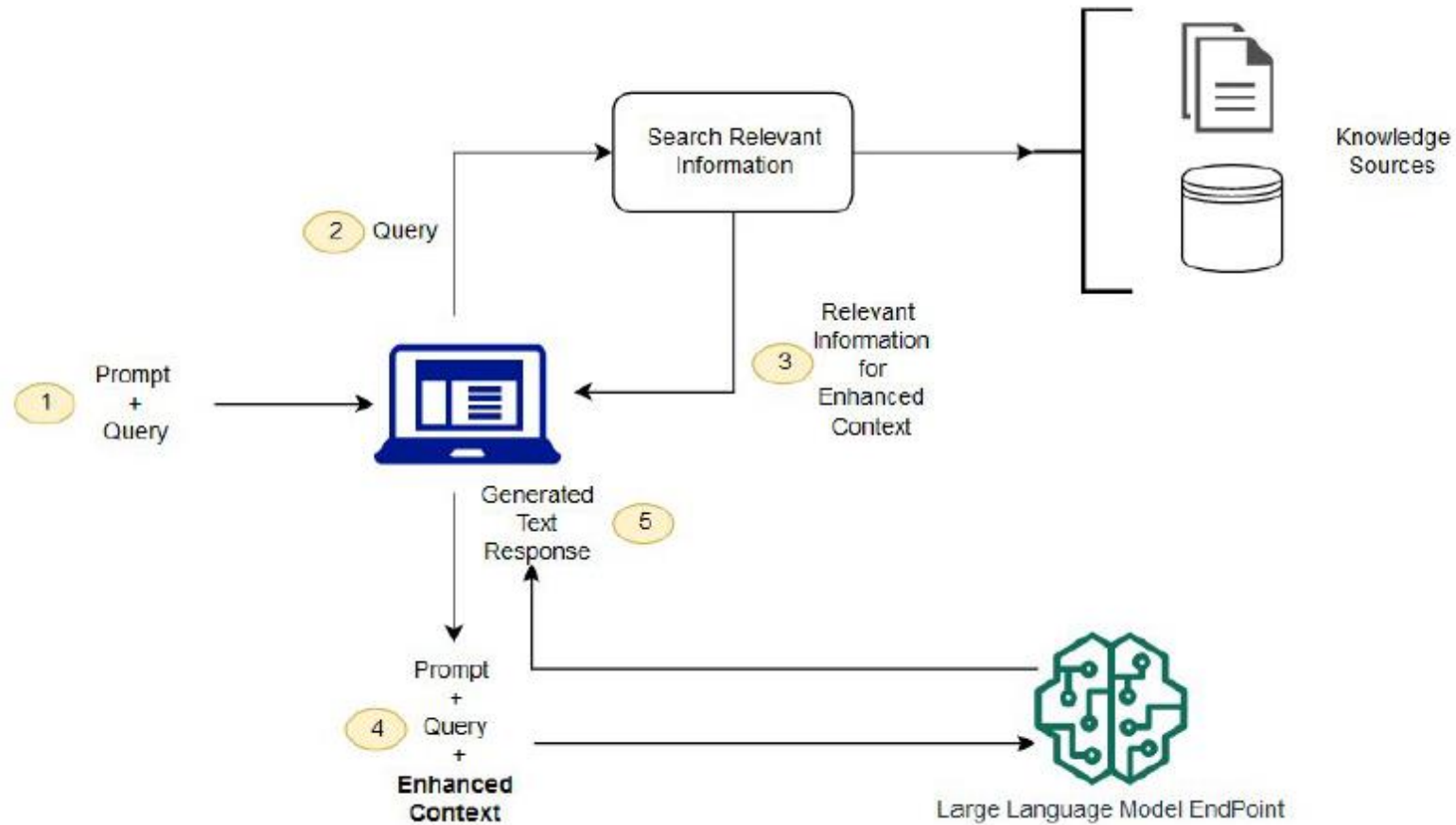
A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had $23 - 20 = 3$. They bought 6 more apples, so they have $3 + 6 = 9$. The answer is 9. ✅

Tree of Thoughts

ToT allows LMs to perform deliberate decision making by considering multiple different reasoning paths and self-evaluating choices to decide the next course of action, as well as looking ahead or backtracking when necessary to make global choices.

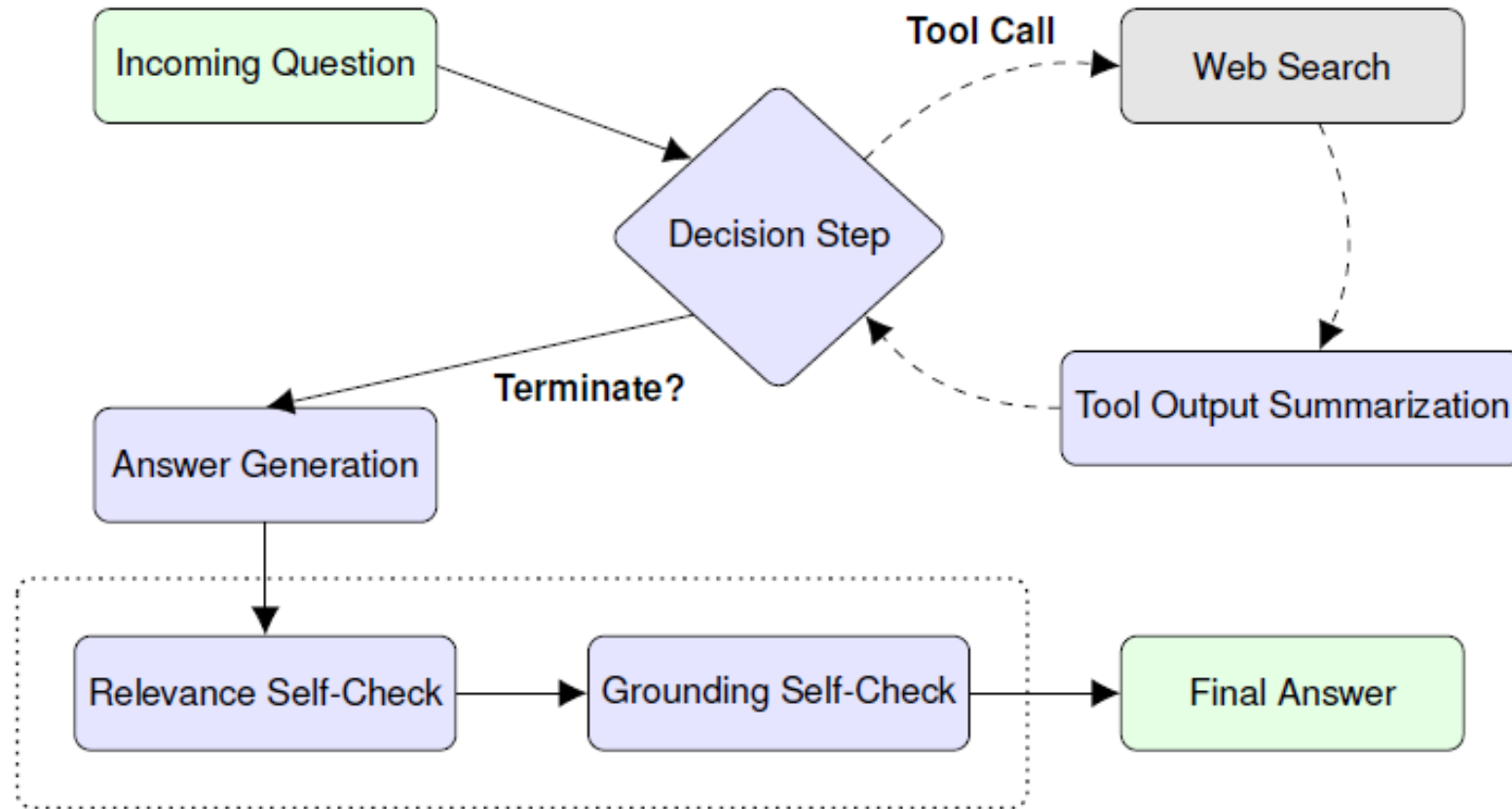


RAG

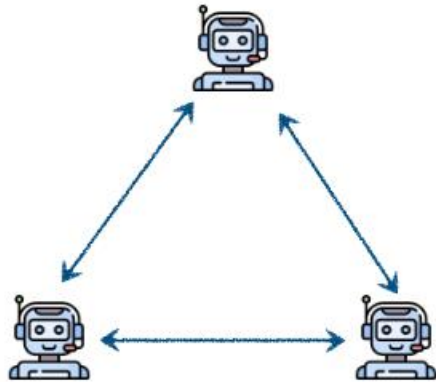


$$P(Y|X) = P(D|X)P(Y,D|X)$$

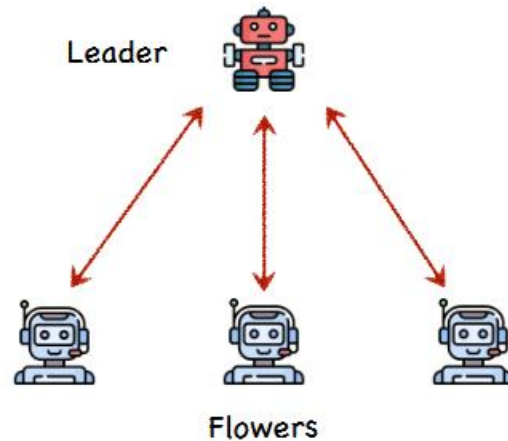
LLM Agents



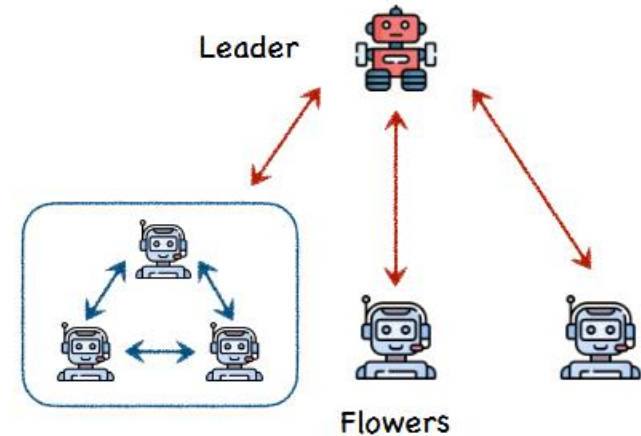
Structures of multi-agent systems



a) Equi-level structure



b) Hierarchical structure



c) Nested structure

Judging LLM-as-a-Judge

Question: If the FED buys bonds in the secondary market
(A) the money supply will increase. (B) the money supply will decrease. (C) the money supply will not be affected. (D) the discount rate would be affected. Output the answer only.

Assistant A:

The Federal Reserve buys bonds in the secondary market to increase the money supply.

Assistant B:

(A) the money supply will increase.

Follow-up Question: How does it affect my daily life? Give 3 examples.

Assistant A:

The Federal Reserve buys bonds in the secondary market to increase the money supply. This affects your daily life by:

1. Increasing the money supply.
2. Increasing the money supply and lowering the discount rate.
3. Increasing the money supply and lowering the discount rate and increasing the money supply.

Assistant B:

When the Federal Reserve buys bonds in the secondary market, it can have several effects on the economy that can impact your daily life. Here are three examples:

1. Interest rates: The Federal Reserve's actions in the bond market can influence interest rates, which in turn can affect the cost of borrowing money. For example, if the Federal Reserve buys bonds and drives up demand for them, interest rates on things like mortgages, car loans, and credit cards may go up, making it more expensive to borrow money.
2. Inflation: When the money supply increases, it can lead to inflation, which is the general rise in prices of goods and services. This can impact your daily life by making it more expensive to buy things like groceries, gas, and other necessities.
3. Employment: The Federal Reserve's actions in the bond market can also have an impact on employment. For example, if the Federal Reserve's actions lead to economic growth and increased demand for goods and services, it can create more job opportunities and boost employment.

GPT-4 Judgment:

Assistant A provided an incorrect response to the user's question about how the Federal Reserve buying bonds in the secondary market affects daily life. The answer given is repetitive and lacks clear examples of how the action impacts daily life.

On the other hand, **Assistant B** provided a relevant and accurate response to the user's question about the Federal Reserve buying bonds. The answer includes three clear examples of how the action impacts daily life, such as interest rates, inflation, and employment.

Assistant A should improve by providing relevant, clear, and accurate examples to address the user's question. **Assistant B's** response is more helpful, relevant, and detailed.

Limitations of LLMs

- Hallucination
- LLMs are sensitive to tweaks to the input phrasing or attempting the same prompt multiple times. For example, given one phrasing of a question, the model can claim to not know the answer, but given a slight rephrase, can answer correctly.
- Ideally, the model would ask clarifying questions when the user provided an ambiguous query. Instead, current models usually guess what the user intended.
- LLMs sometimes respond to harmful instructions or exhibit biased behavior.

Thank You