

智能问答系统实践

第六课：答案生成



姜文斌

北京师范大学人工智能学院

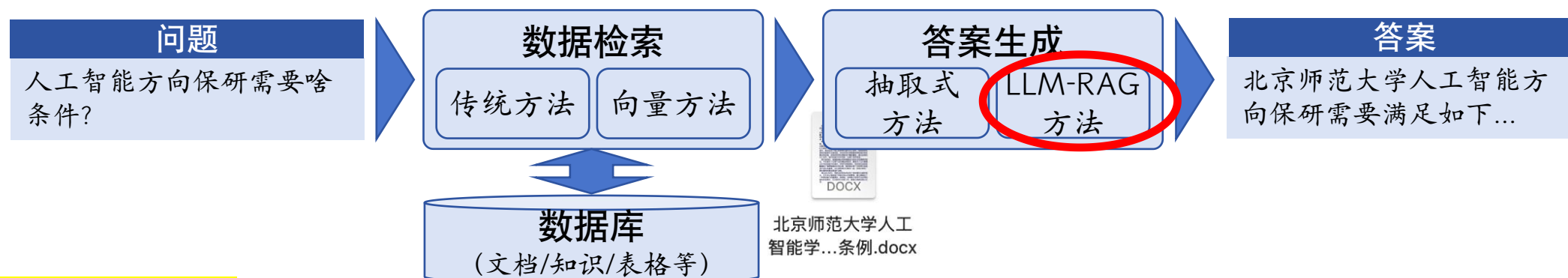
2025.04.03

我的位置



智能问答系统

针对用户提出的自然语言问题，从数据库中检索相关信息，并依据相关信息作出回答



智能问答线上处理流程

智能问答线下处理模块

问答数据库构建

基于传统方法的数据建库

基于向量方法的数据建库

数据检索模块构建

传统语义匹配模型构建

向量语义匹配模型构建

答案生成模块构建

抽取式答案生成模型构建

RAG式答案生成模型构建

效果评估模块构建

文档检索效果评估

问答整体效果评估

目录

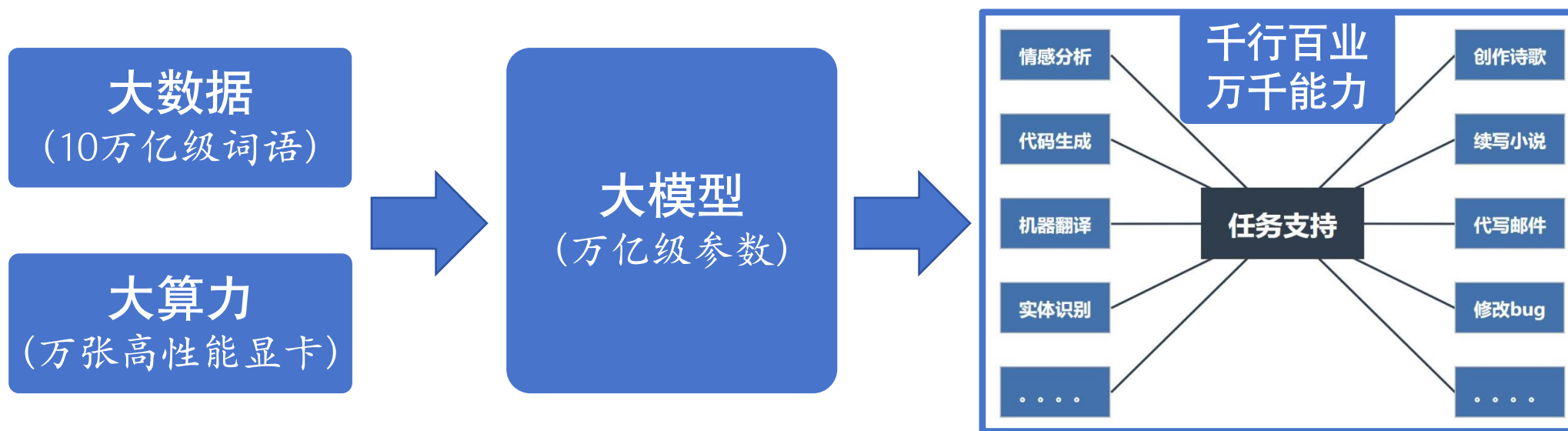


- LLM基础
- LLM原理
- RAG方法
- 总结

大模型时代



- OpenAI于2022年底发布的ChatGPT，在众多NLP任务上的表现令人惊叹
 - ChatGPT支持多轮人机对话，以统一的对话形式提供对多种任务的支持
 - 此后相继发布GPT-4，以及GPT-4o（多模态）和OpenAI-o1（推理）



GPT3成本约460万美元（万张显卡3个月），GPT4成本约6300万美元

大模型与AGI



■ 大模型技术近年来蓬勃发展，成为通向通用人工智能（AGI）的可能路径

ChatGPT生成文本、代码

明钰 请问你背后的技术原理是什么？

我是一种大型语言模型，使用了深度学习技术来学习和理解语言。具体地，我是由一个名为Transformer的神经网络架构训练出来的。在训练过程中，我接受了大量的文本数据，并尝试预测文本中的下一个单词或下一个句子。这样的训练使我能够理解语言的语法、语义和上下文，并生成自然语言响应。同时，我还使用了一些技术来帮助我生成高质量的响应，如beam search、attention机制等。

明钰 只有这些吗？那你能介绍一下什么是基于人类反馈的强化学习（Reinforcement Learning from Human Feedback, RLHF）吗？

当然，除了上述的深度学习技术外，RLHF 是另一个非常有趣的机器学习技术。RLHF 是一种强化学习方法，其目的是通过人类反馈来训练一个智能体，使其在交互式任务中表现得更好。

在 RLHF 中，人类提供了正面或负面的反馈信号，用于指导智能体的决策。通过不断接收人类反馈信号并根据这些信号改进自身的策略，智能体可以逐渐学会如何在特定任务中表现得更好。

相对于其他强化学习技术，RLHF 具有一些优势，例如更快的学习速度、更好的稳定性和更高的任务效率。然而，RLHF 的一个主要挑战是如何有效地融合人类反馈和自主学习的能力。目前，研究人员正在积极探索 RLHF 技术在各种领域的应用，例如游戏、机器人控制和自然语言处理等。

Stable Diffusion生成图像



SORA生成分钟级视频



文本生成大模型

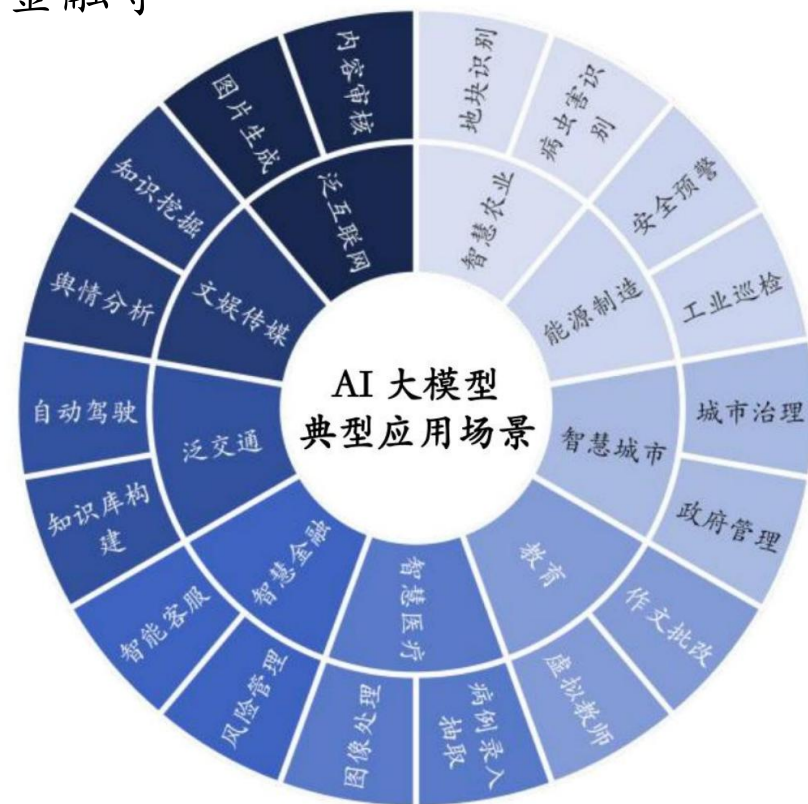
■ 几乎所有AI任务，只要能将输出表示为文本，即可用文本生成大模型求解

■ 国内企业机构非常重视ChatGPT引发的AIGC浪潮，积极布局生成式AI，百模大战

■ 大模型从通用领域向行业领域扩展，如教育、医疗、金融等

 百度 文心一言	 阿里巴巴 通义千问	 360 360智脑	 腾讯 混元	 华为 盘古
 商汤科技 日日新	 润舟科技 孟子	 智源研究院 悟道2.0	 科大讯飞 星火认知	 昆仑万维 天工3.5
 清华大学 ChatGLM-6B	 复旦大学 MOSS	 中科院自动化所 紫东太初	 面壁智能 CPM-Bee	 达观数据 曹植

“百模大战”时的代表性大模型



图像生成大模型



- 图像生成大模型能够根据输入文本信息，生成不同内容、结构、风格的图
 - 文生图的分辨率和逼真度有了很大提升，但复杂结构刻画和物理规律遵循有待加强



视频生成大模型



- 视频生成根据文本、图像和视频片段等输入，生成不同内容、风格的新视频
 - 2024年2月 OpenAI 发布文本生成视频模型 Sora，将视觉生成推到新的高度



- **画质突破**：视频非常高清，细节极其丰富
- **帧率和连续性突破**：视频帧率高、连续性好、一致性高
- **时长突破**：相比之前模型仅能生成几秒的时长，Sora 可以生成长达1分钟的视频
- **物理世界规律未突破**：整个视频看上去非常自然和逼真，但是视频中物体的运动、光影等不一定符合自然世界的物理规则

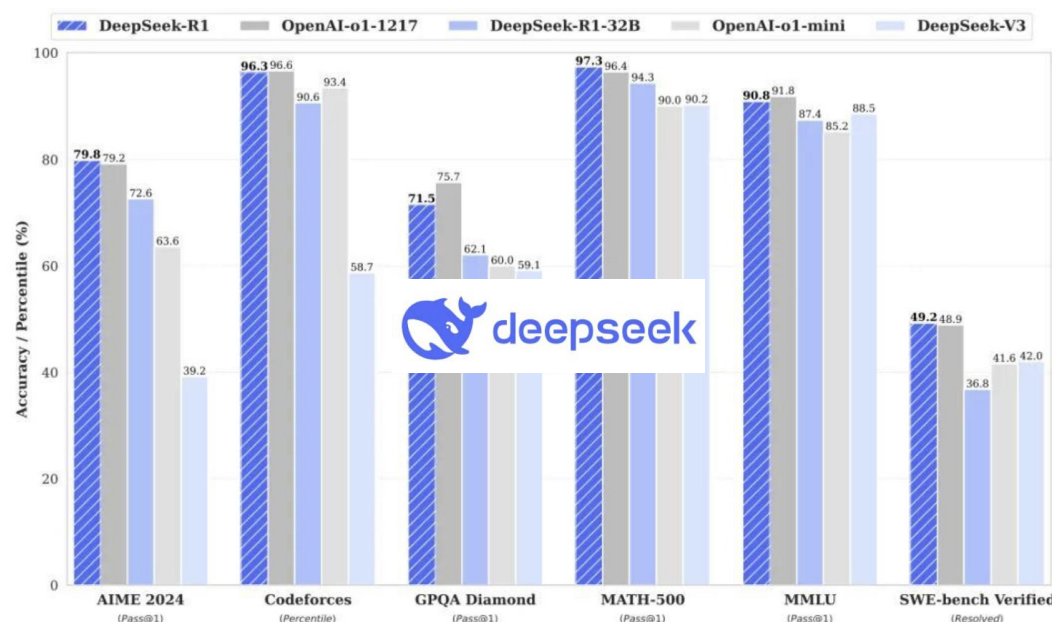
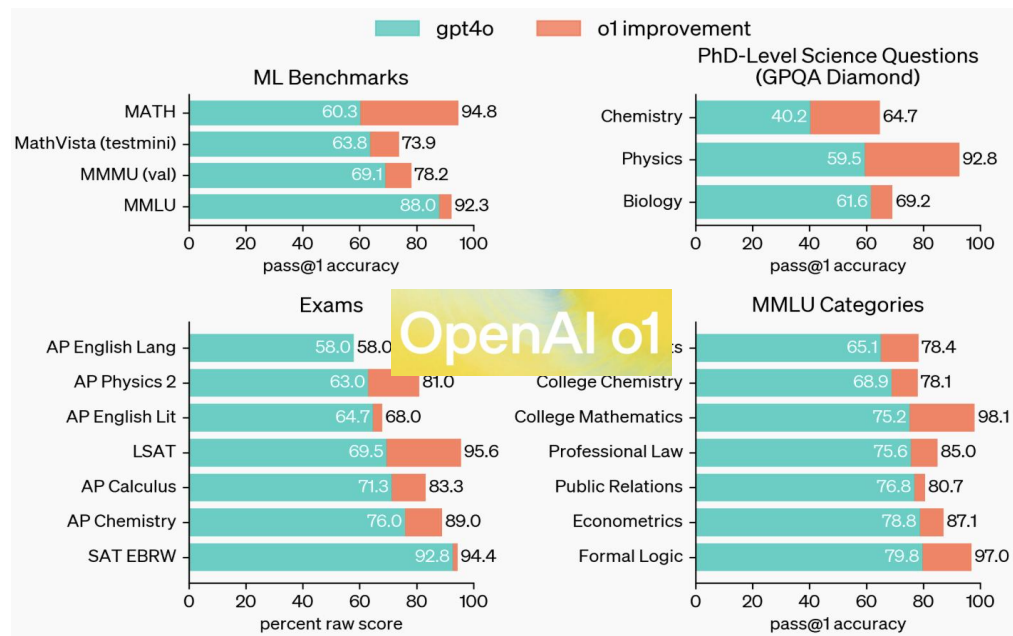
深度推理大模型



■ 通过精细思维链和强化学习，自动学习更好的问题求解过程

■ **精细思维链**：提升思维过程精细度，并且带反思和纠正操作，边推进边反思纠正

■ **强化学习**：以最终目标驱动的问题求解策略优化，从而找到更优的思维过程



DeepSeek-R1的训练成本 (~560万美元) 相比OpenAI-o1 (>1亿美元) 降低95%

DeepSeek意义

- 技术优化 vs 算力堆砌
 - 通过极致工程技术优化，破解美国算力扼制
- 开源模型 vs 闭源模型
 - 开源模型效果超过闭源，剧烈改变业界格局
- 中国技术 vs 美国技术
 - 冲击美国AI技术垄断，彰显中国AI创新实力

春节期间两大热点：DeepSeek和哪吒2

- 证明了沉下心专注技术的重要性
- 在技术和艺术领域冲击美国神话



目录



- LLM基础
- LLM原理
- RAG方法
- 总结

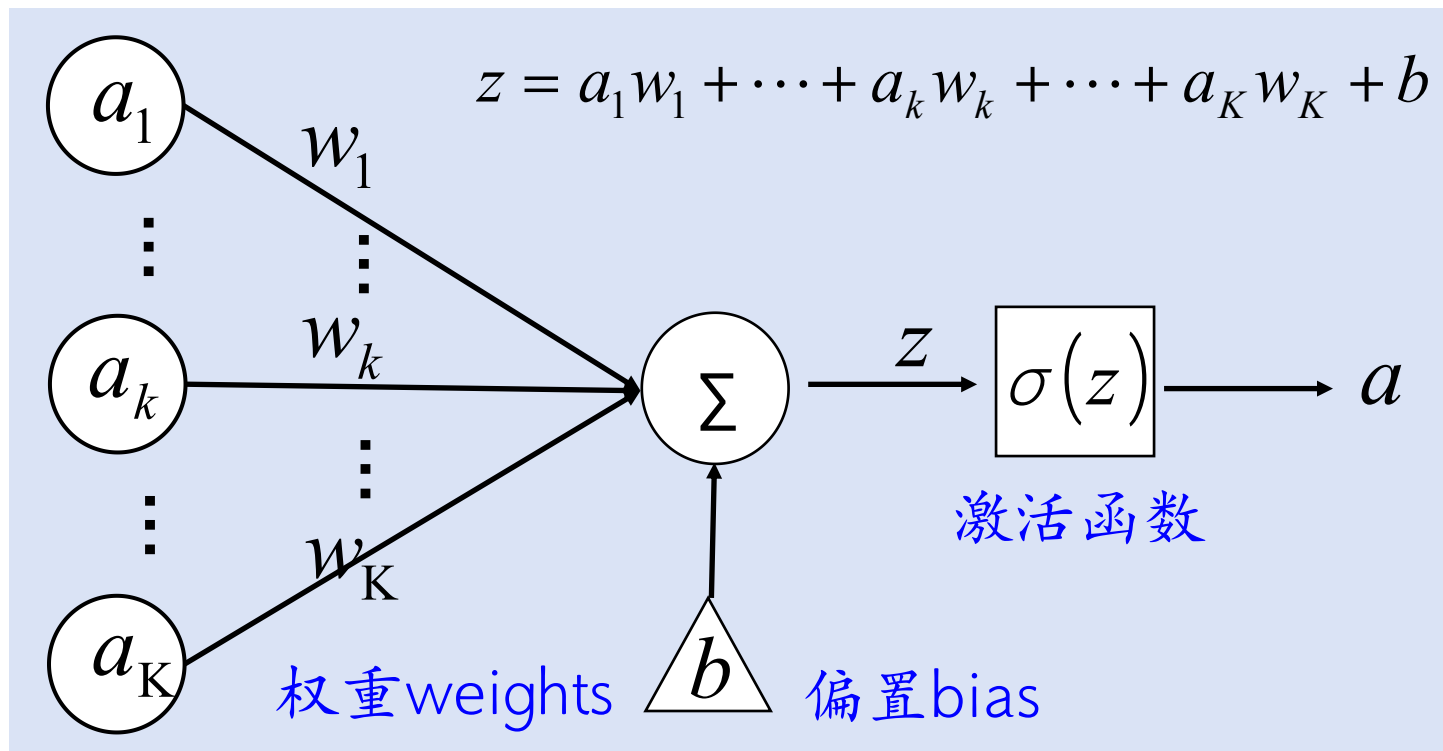
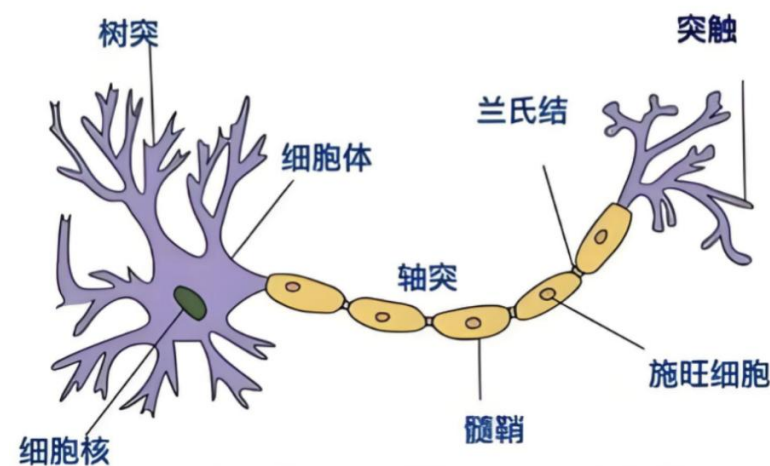
神经元



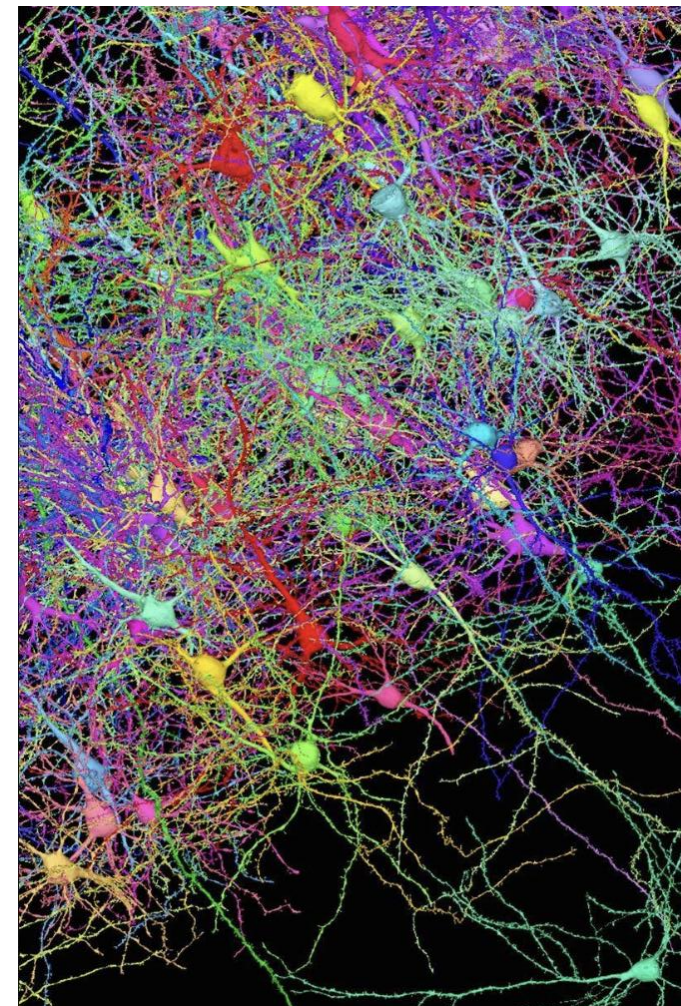
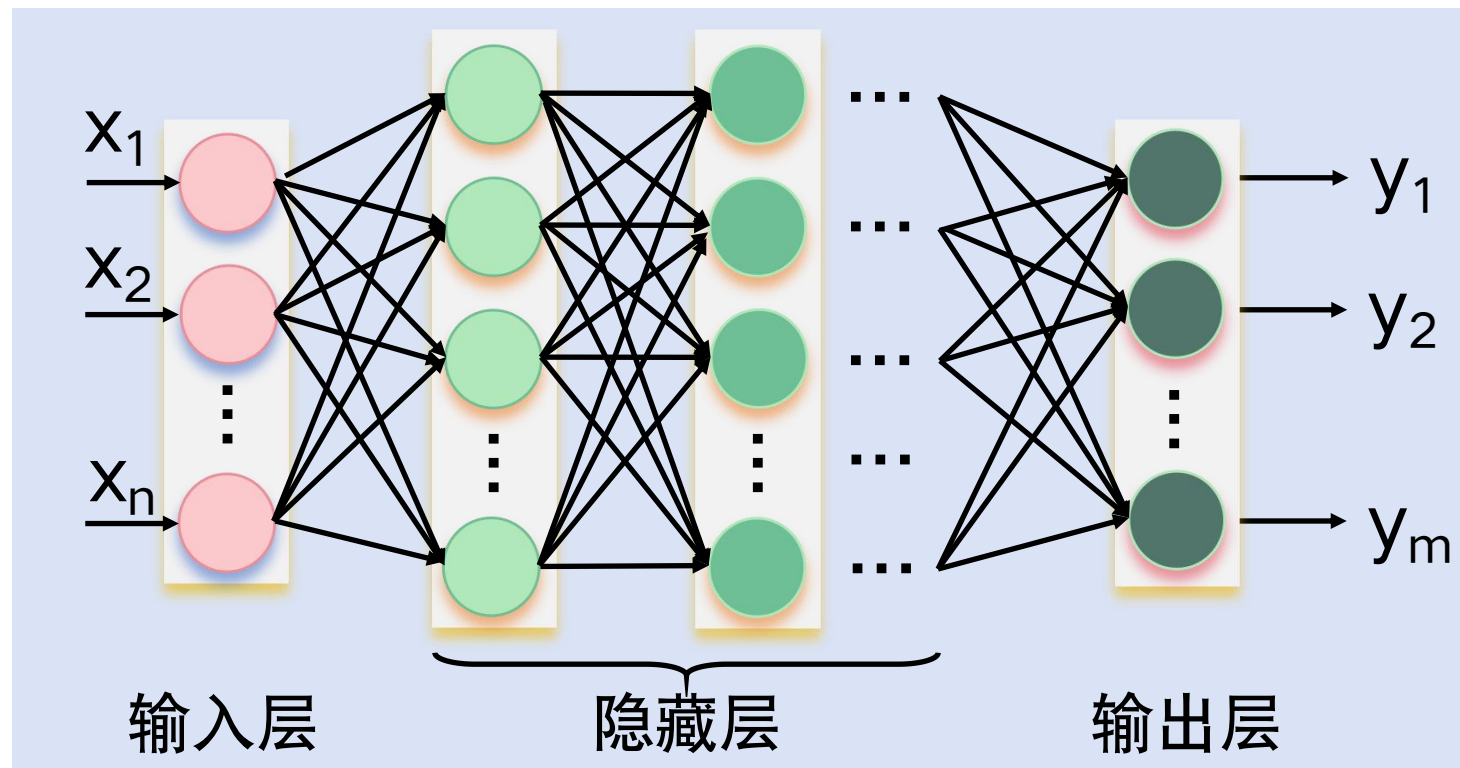
1、**胞体**：内含细胞核和众多细胞器，负责维持神经元的生命活动并提供能量。

2、**树突**：接收来自其他神经元的信号。这些信号可以是感觉信息、化学信号或其他神经元的电信号。

3、**轴突**：一根长长的、细长的纤维状结构，负责将胞体整合后的信号快速传递到下一个神经元或效应器。



神经网络

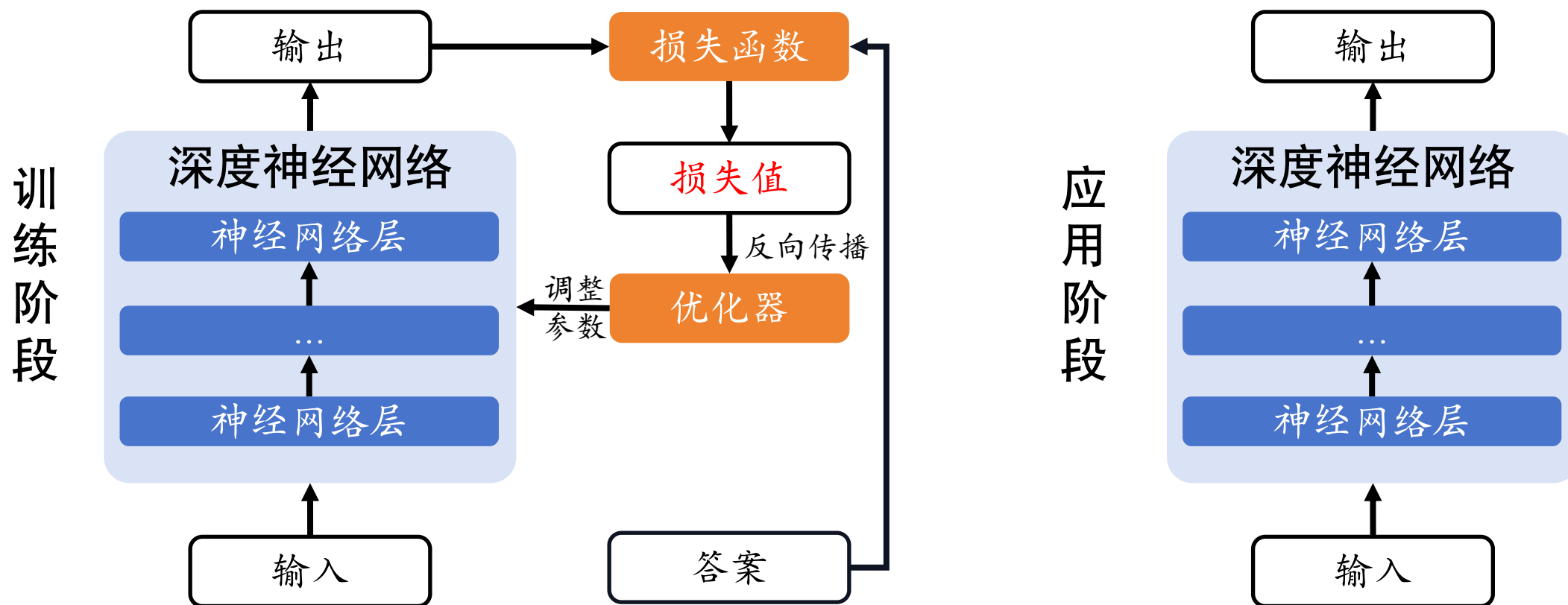


深度学习



■ 深度学习本质是通过大规模神经网络，学习从输入到输出的映射函数

■ 神经网络是海量的非线性函数的组合，拟合能力极强，但极难分析



■ 物理意义上的大

- 大参数：（数十亿 ~ 数万亿）的参数
- 大算力：（数千卡 ~ 数万卡）训练（数天 ~ 数月）
- 大数据：（数千亿 ~ 十万亿）的训练token
- 大资金：（数百万 ~ 数亿美元）的训练成本

■ 逻辑意义上的大

- 广泛能力：理解/推理/决策/生成...
- 广泛领域：覆盖各行各业
- 广泛任务：支持各种任务

关于token

英文：1token 约为0.75个单词
中文：1token 约为1~1.8个汉字

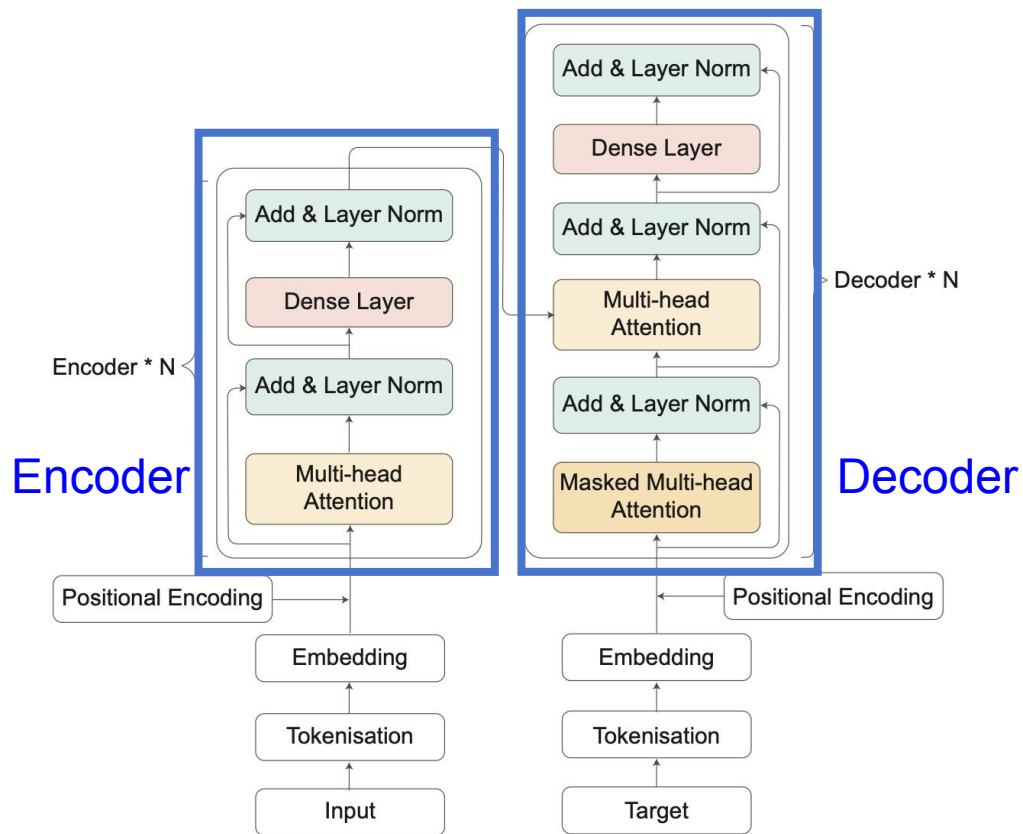
示例：

1000亿token，对应约1000亿汉字；一部教材，按50万字算；因此，1000亿token约合**20万**部教材

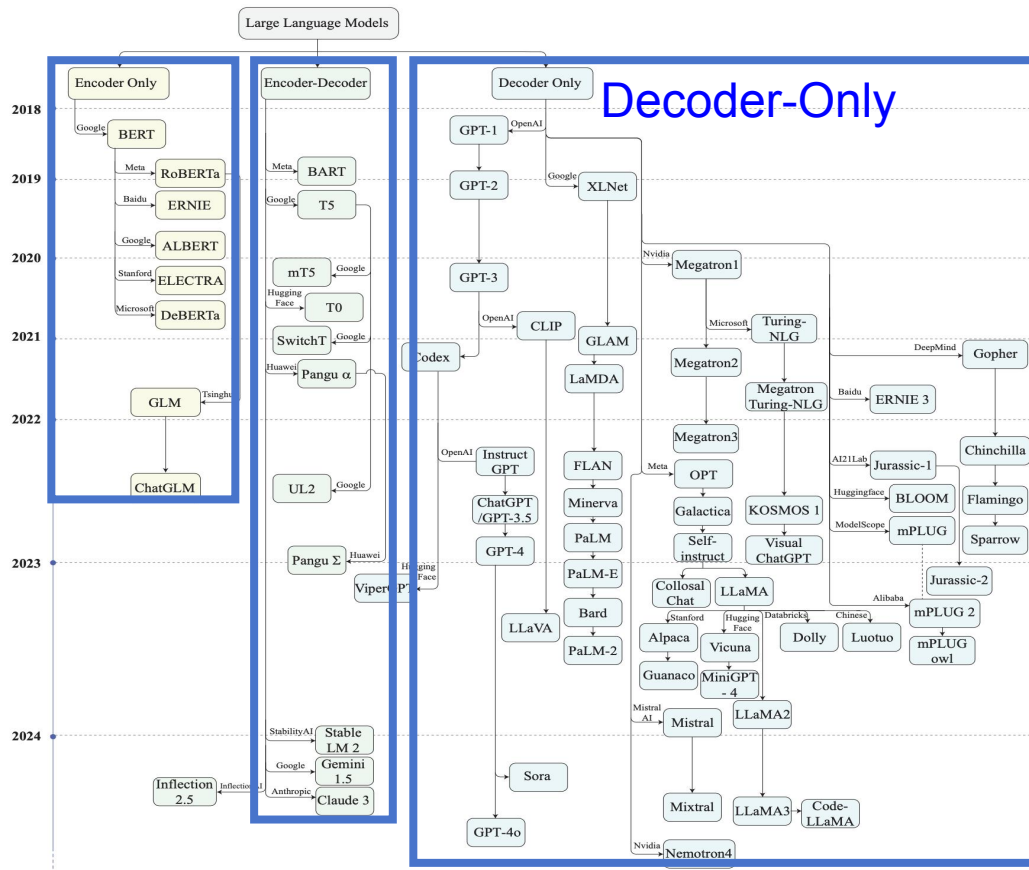
将万千任务的求解能力，训练在了同一个**自回归生成式**的求解器中

大模型架构

- 大语言模型将众多任务统一为文本生成，多任务学习带来新任务求解能力

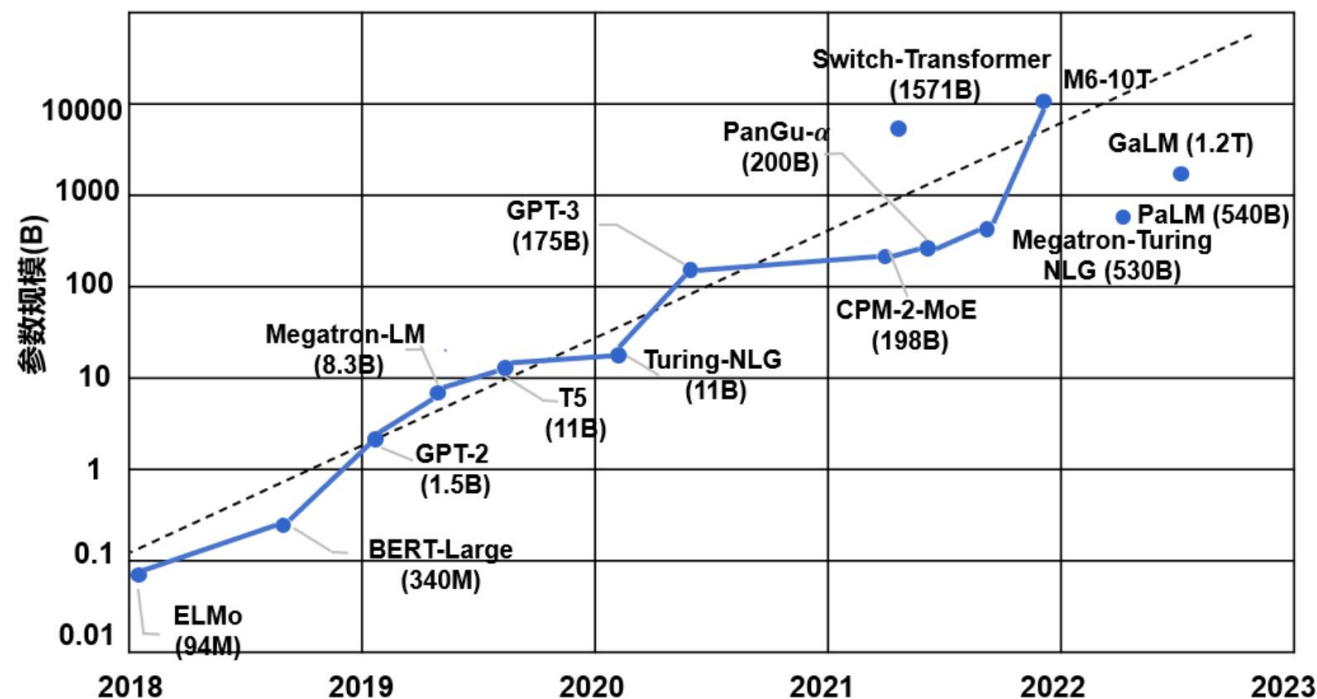


经典Transformer架构(Encoder+Decoder)



大模型构建：预训练

- ChatGPT等大模型成功的关键在于海量数据上的预训练，例如GPT-3的预训练语料规模达到了3000亿单词



2024年之前，模型参数规模疯狂的增长

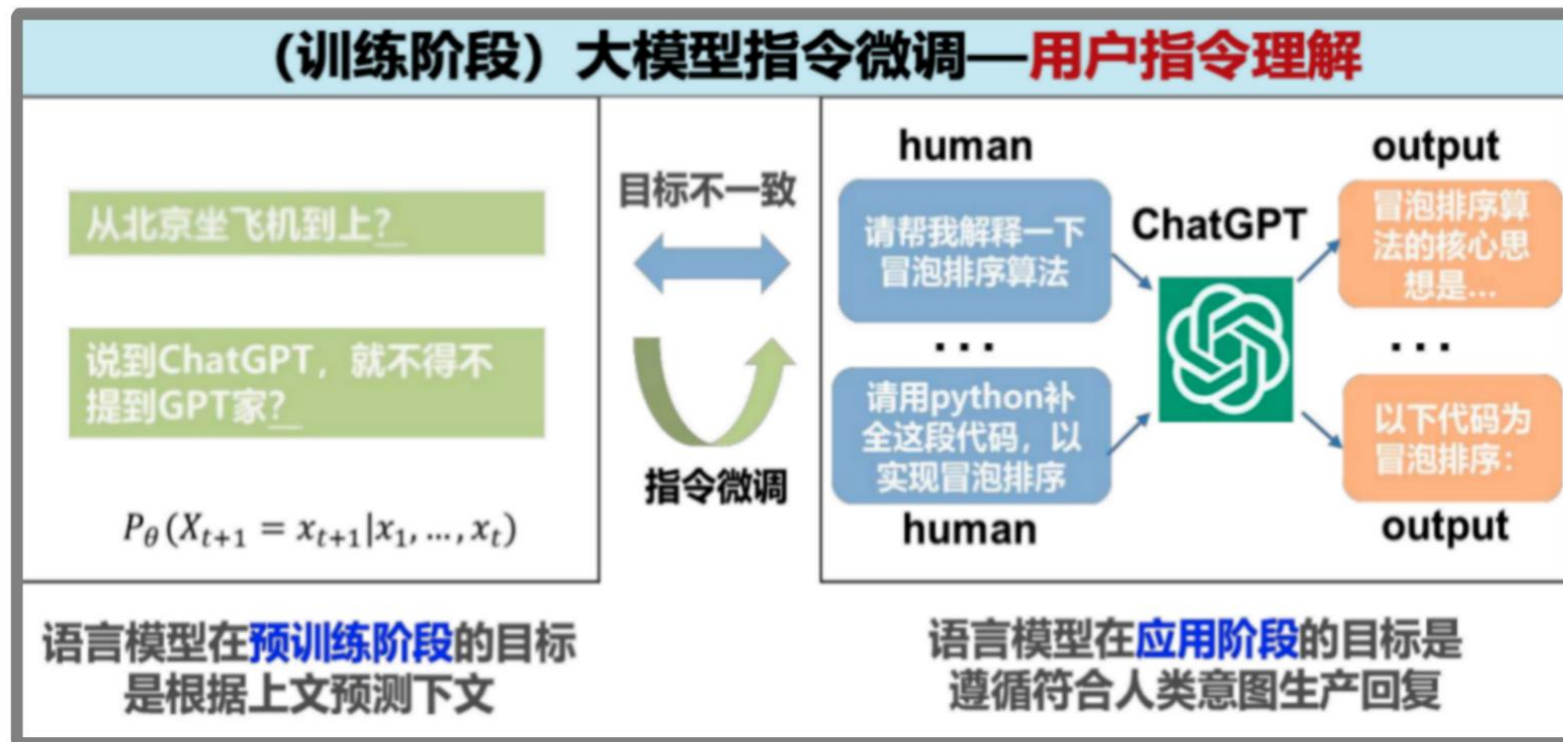
读书破万卷

- 自然语言的理解与生成能力
- 多任务的基本理解与求解能力

高中生 基础教育

大模型构建：指令微调

- 用高质量的有监督数据 <输入指令, 输出> 指导大模型理解复杂的人类指令, 使得大模型更好地理解 and 执行指令



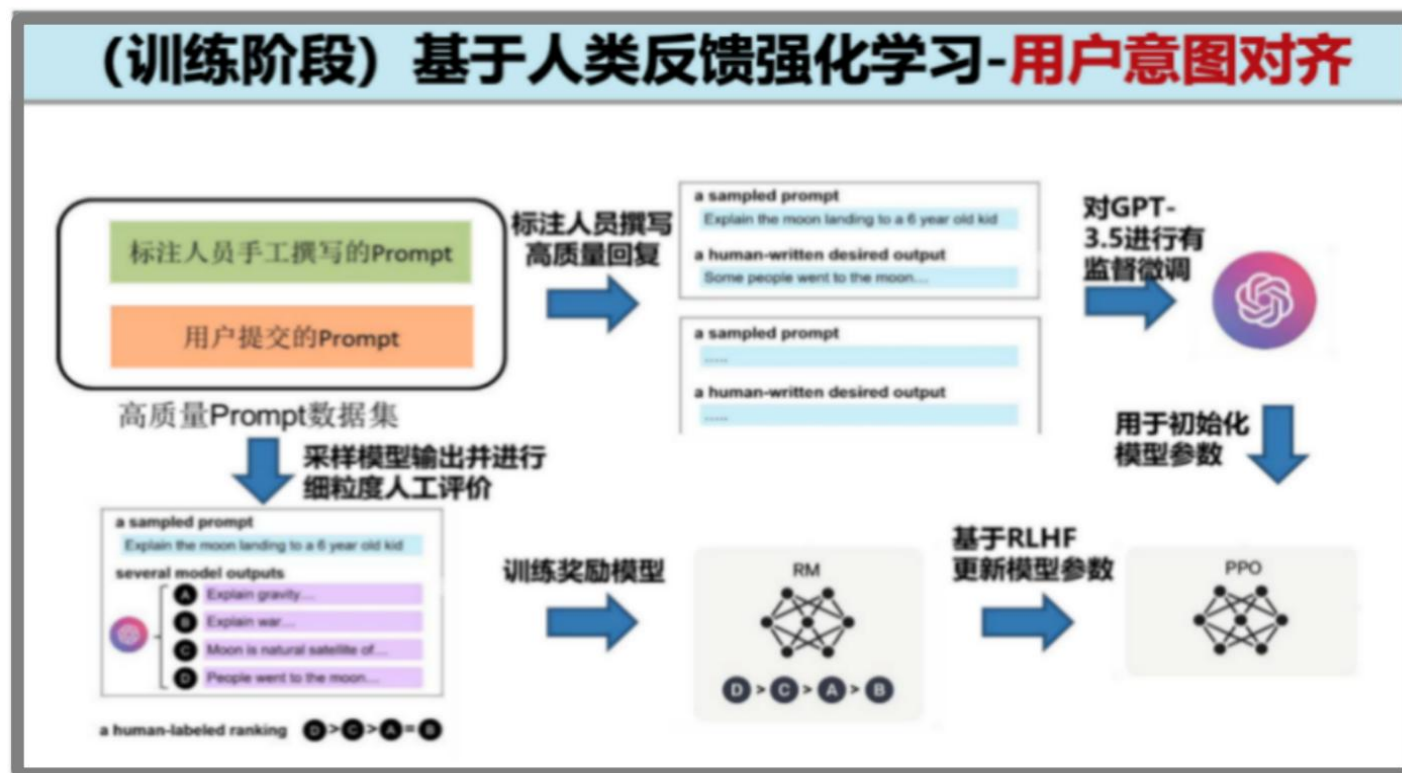
专业技能学习

- 多任务较为准确的理解与求解能力
- 新任务的快速学习能力

大学生
高等教育

大模型构建：意图对齐

- 采用基于人类反馈的强化学习方法更新模型参数，利用人类反馈指导模型生成内容更加符合人类意图和价值观



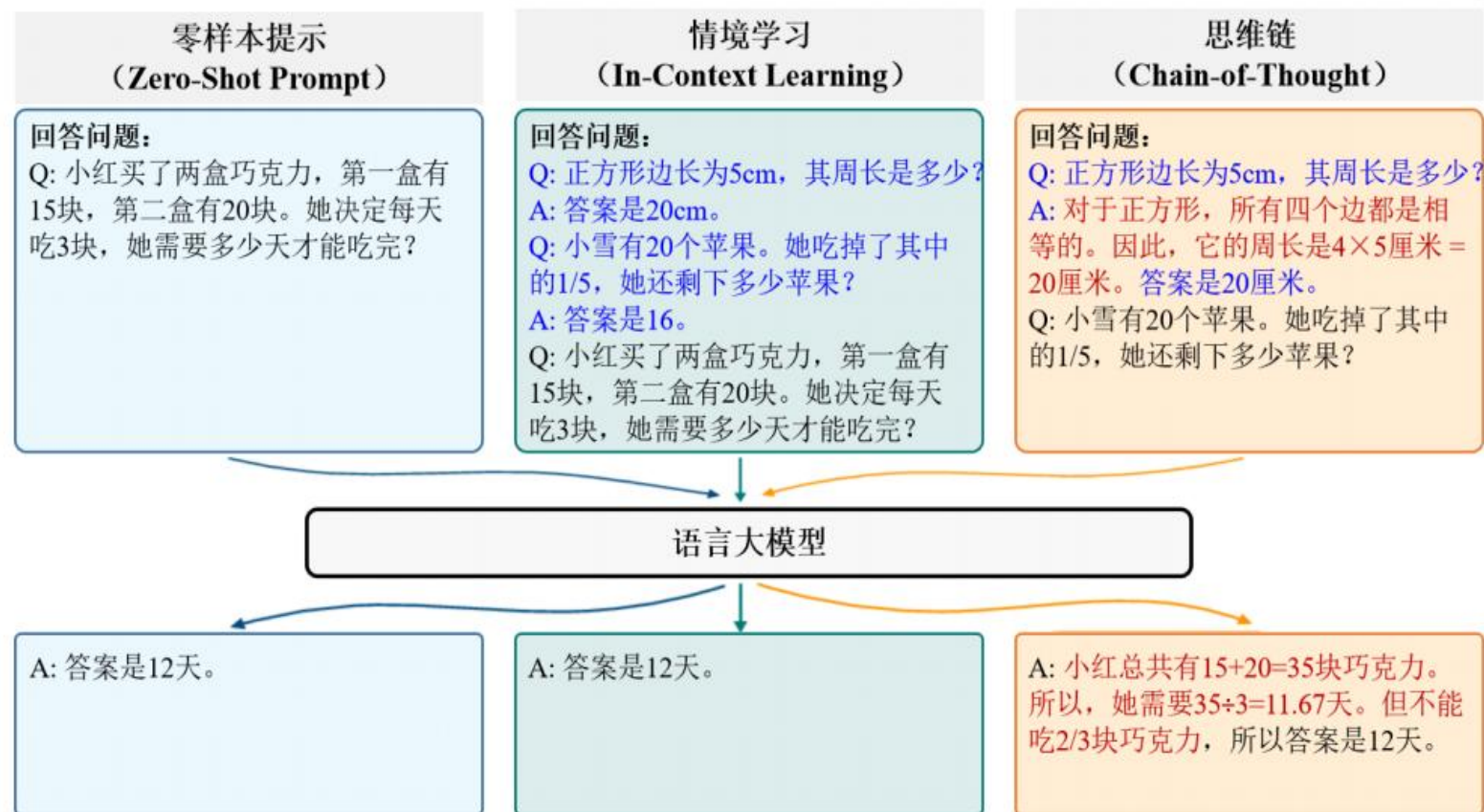
意图与价值遵循

- 更符合人类意图和价值观
- 更优质更有用的求解结果

熟练工
走向社会

大模型使用：提示技术

- 通过设计提示词与大模型进行交互，包括明确的任务类型、输出内容、输出格式等要求，大模型生成满足提示指令的输出



照葫芦画瓢

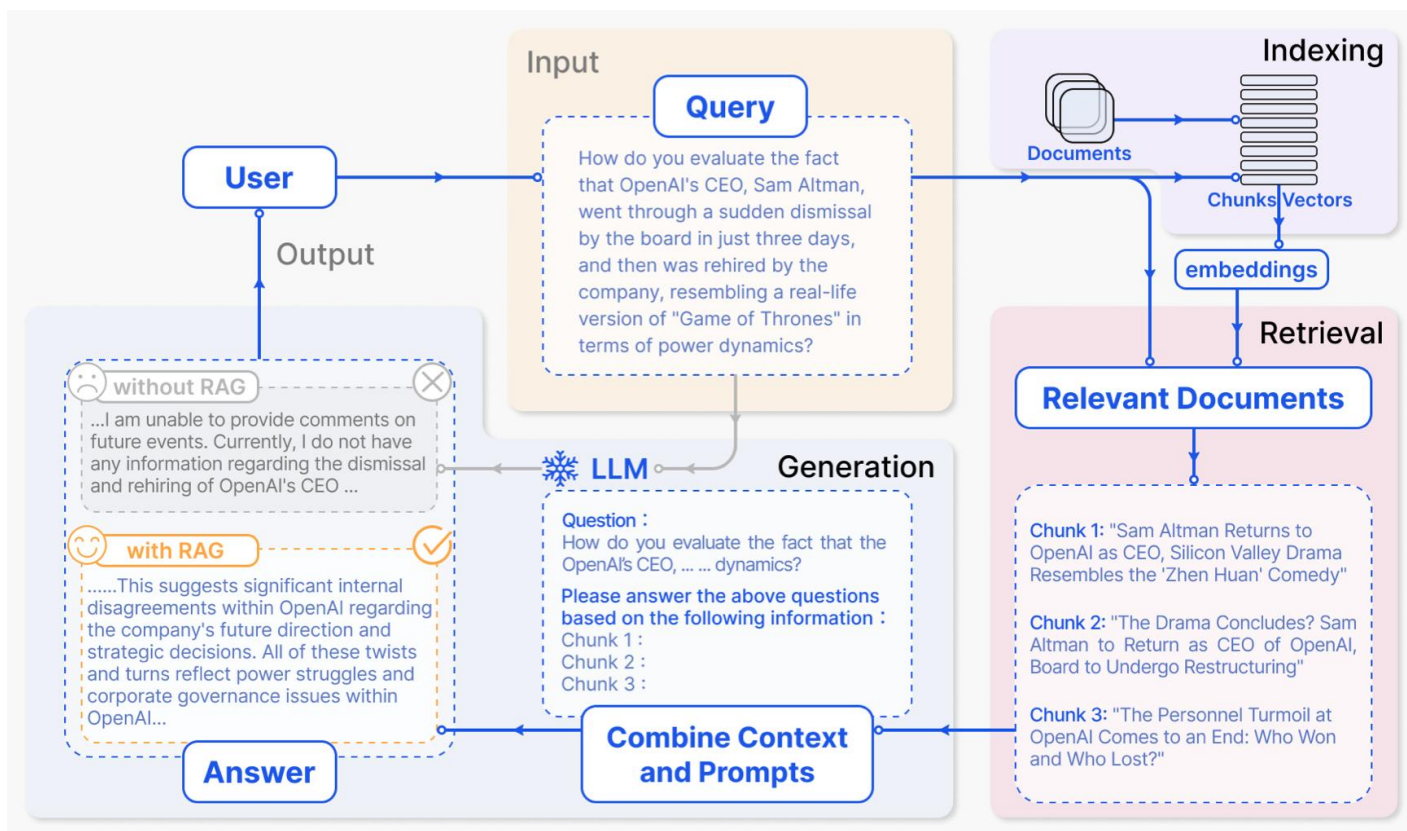
- 从用户提供的样例中现场学习问题的求解
- 样例的选择和组织很重要

会模仿
现学现卖

大模型使用：检索增强

■ 大模型难以快速地更新知识，且存在“一本正经胡说八道”的幻觉现象

■ 检索增强的生成方法，能够有效环节幻觉，提升信息时效性、结果可信性



边查材料边解问题

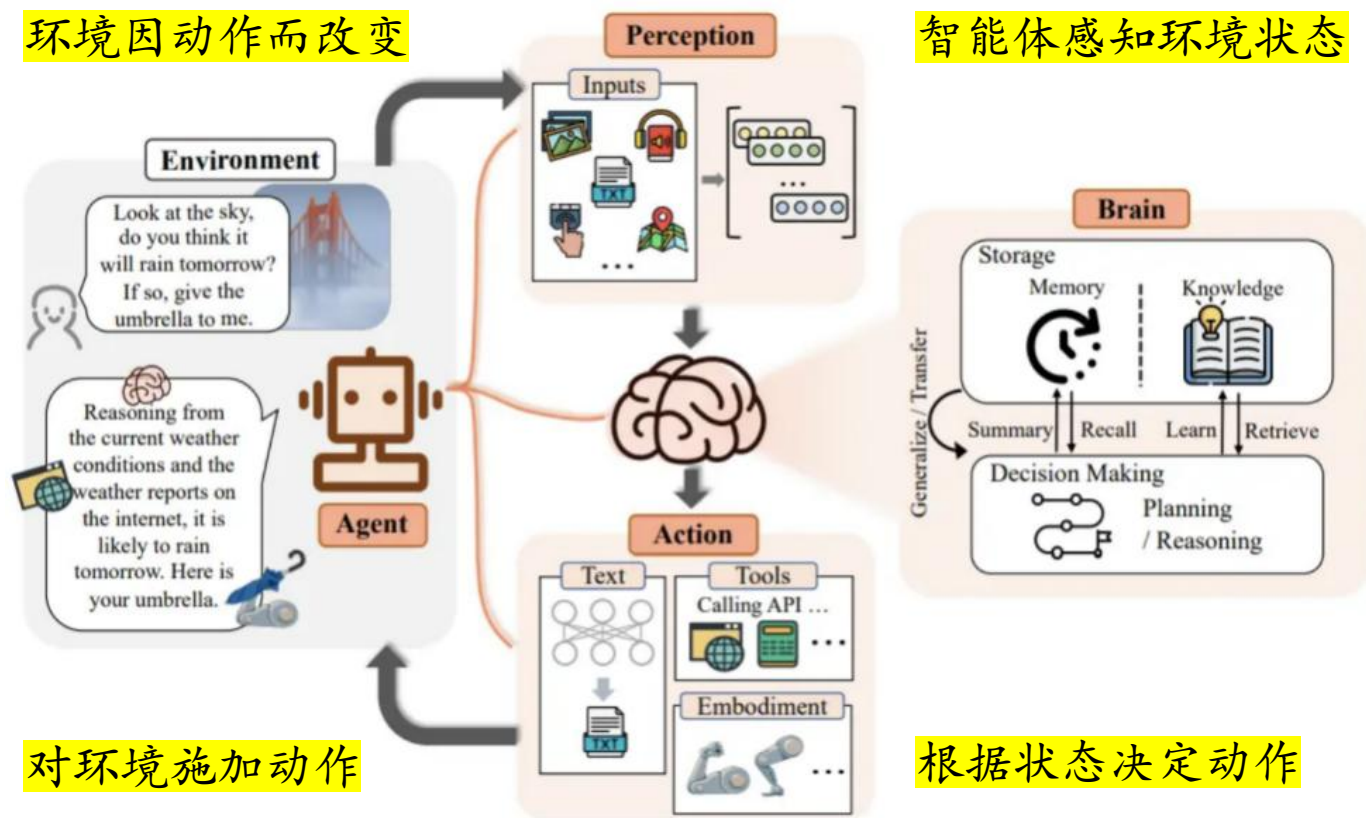
- 借助外部知识库解决了大模型知识陈旧的问题
- 促成了大模型求解器和外部知识库分离的模式

会摇人
求助外援

大模型使用：智能体

■ 智能体是能够自主感知和理解环境，进行规划决策和执行动作的智能体主体

■ 智能体具备任务规划、调用工具，逐步推理，从而完成给定复杂任务的能力



仔细思考规划

- 借助外部记忆和规划机制实现复杂问题的求解能力
- 求解模式顺便具有了可解释性和可干预性

会规划
能力升级

目录



- LLM基础
- LLM原理
- RAG方法
- 总结

LLM问题



■ 知识更新问题

- 大模型的参数所蕴含的知识，其时效性停留在训练结束的那一刻
- 大模型训练成本高昂，难以实时便捷地更新其参数中内置的知识
- 有监督微调方法更多是激发大模型已有能力，难以根本性更新知识

■ 幻觉生成问题

- 生成机制：大模型采用自回归生成方式生成答案，并不遵循上层业务的求解逻辑
- 能力边界：大模型难以知悉和遵循自己的能力边界，往往“一本正经胡说八道”
- 幻觉抑制：幻觉抑制策略通常采用强化学习等手段，难以从根本上消除幻觉

RAG理由



■ 检索增强生成 (RAG)

- 检索阶段：根据输入问题，从资料库中查找有助于回答问题的资料
- 生成阶段：根据输入问题和检索得到的资料，借助资料更好地生成答案

■ RAG本质

- 知识存储与推理引擎分离，推理引擎在任务维度和时间维度具有通用性
- 类比开卷考试，根据问题动态检索资料，然后根据资料回答问题

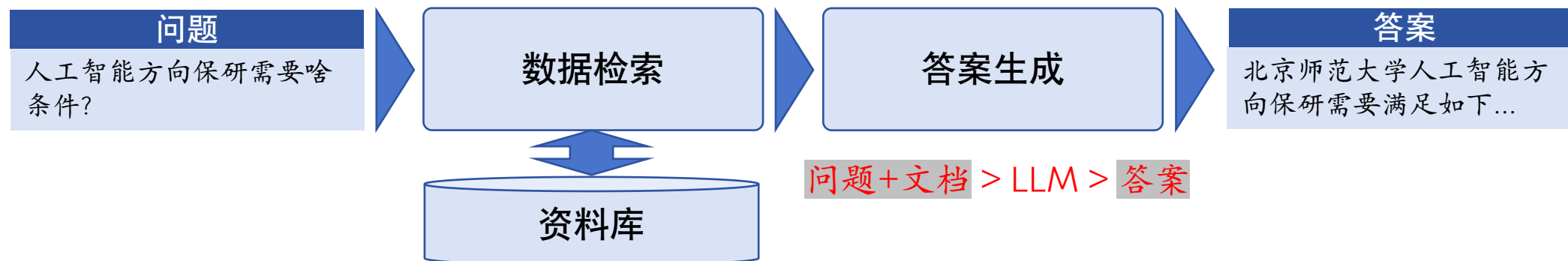
■ RAG优势

- 知识更新：通过对知识库进行更新，随时供大模型获取使用最新的知识
- 幻觉抑制：根据检索的知识来回答问题，降低胡说八道的可能性

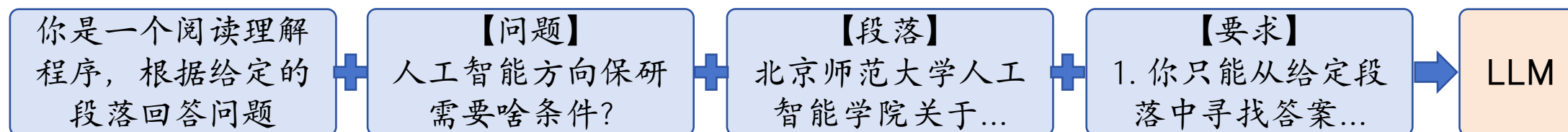
RAG流程



■ 基于大模型的“检索-生成”式的固定 workflow



■ 设计合理的提示引导LLM根据文档生成答案



RAG 优化



■ 数据优化

- 对文档资料库进行更好的切片处理，让资料片段长度处于合理的区间

■ 单步优化

- 更好的检索：传统检索&向量检索融合；对检索结果进行大模型校验
- 更好的生成：构造<问题，段落，答案>样本进行SFT；对生成结果进行大模型校验

■ 整体优化

- 流程容错：保留多个检索结果和答案候选然后投票；在整个流程中引入反思纠正
- 强化学习：端到端的强化学习，同时优化检索环节和生成环节

目录



- LLM基础
- LLM原理
- RAG方法
- 总结

总结



- 大模型具有广泛的知识 and 能力，具有支持复杂任务的潜质

- 掌握海量事实和常识知识，具有基础的理解与推理能力，可求解多种多样的任务

- 大模型难以明确遵循任务求解机理，且内部知识难以更新

- 能求解复杂任务但难以保证正确性，存在幻觉生成即“一本正经胡说八道”问题

- 通过参考外部知识库，可以极大提升复杂问题求解的效果

- 开卷考试，知识与推理分离，知识可以实时更新，让大模型专注于推理求解本身

谢谢大家！

