

大模型智能体与群体智能 迎接智能的第二次涌现

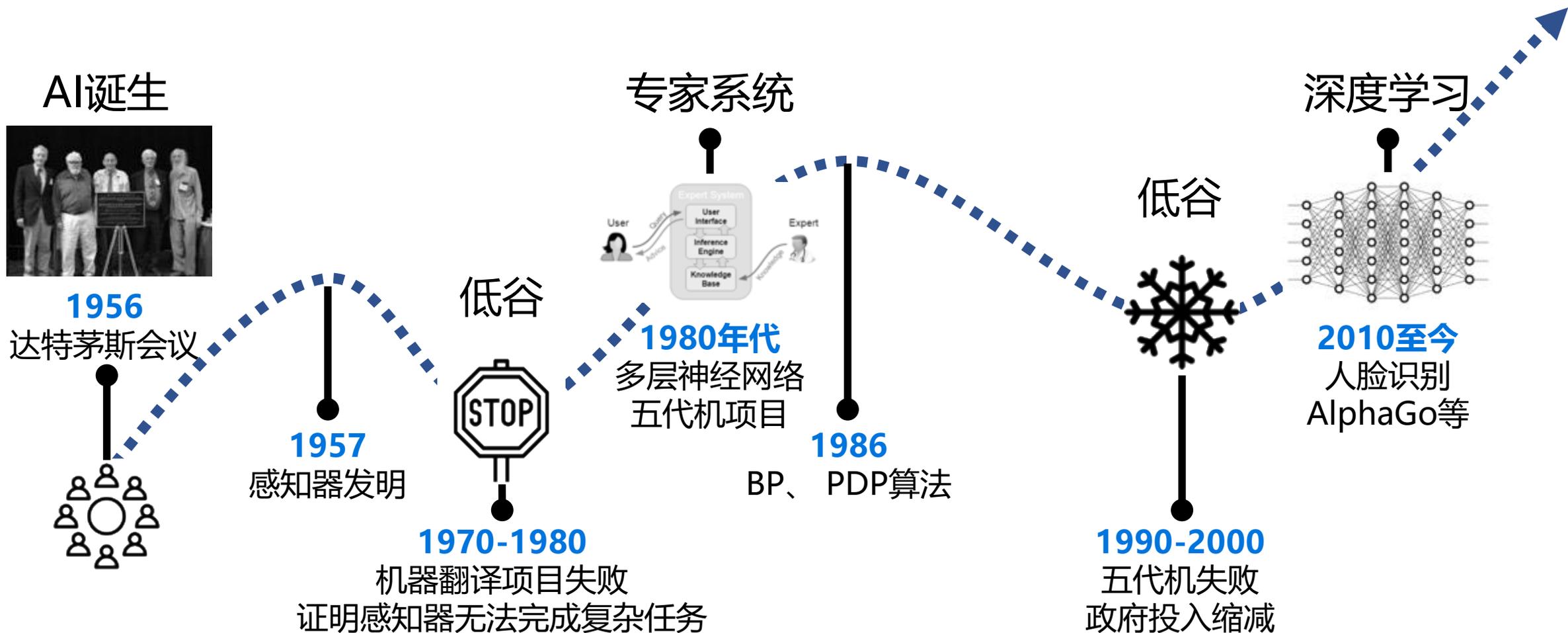
刘知远

上海 · 2024

1

大模型与人工智能

人工智能核心命题—掌握完成复杂任务的知识



人工智能发展路线—符号智能

符号智能：专家手工构

建规则库和知识库，以

规则库和知识库解决具
体问题

局限：规则与知识难以

穷尽式枚举，无法解决

规则库和知识库未覆盖

的任务



1960

Noam Chomsky
(语言学巨擘)

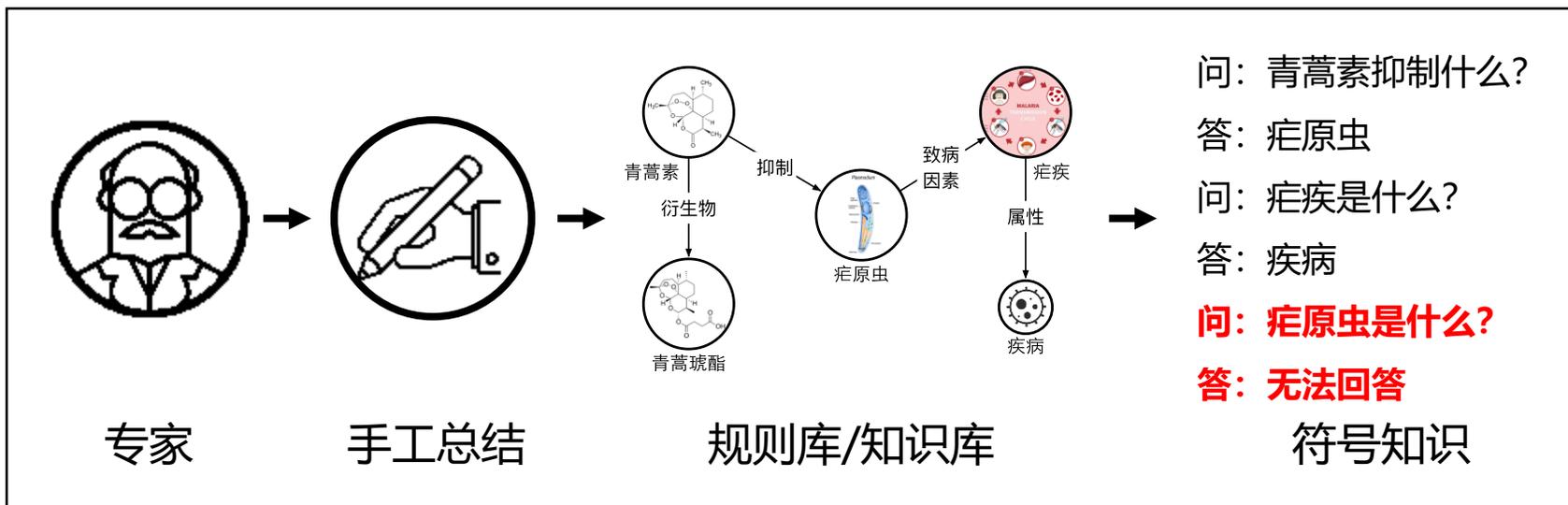
20世纪50年代后，词法、句法、语法**规则**被广泛应用于自然语言理解



1980

Edward Feigenbaum
(图灵奖获得者)

专家系统由知识库与推理机构成，知识库存储事实和规则，推理机则基于知识库进行推理



人工智能发展路线—专用智能

专用智能：利用**数据驱动**

机器学习从特定任务

带标注数据之中自动学

习知识，以**小模型参数**

存储知识

局限：要针对特定任务

标注数据，标注代价高，

无法解决标注数据未能

覆盖的任务



Judea Pearl
(图灵奖获得者)

概率与统计方法被引入自然语言处理，模型从符号系统推演转变为数据驱动学习

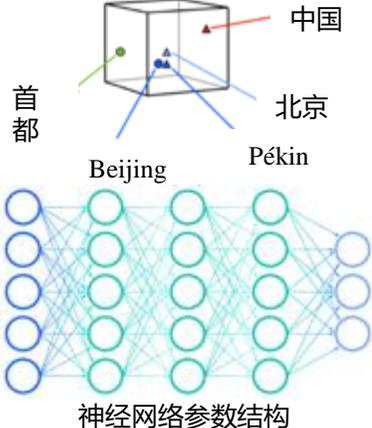


Yann LeCun
(图灵奖获得者)

2010年后神经网络兴起，将数据驱动的效果推到新高位，成为当前自然语言处理主要范式



中文：中国首都是北京
English: The capital of China is Beijing
Française: La capitale de la Chine est Pékin
...



神经网络参数结构

问：计算机英文是什么？
答：Computer
问：计算机法文是什么？
答：Ordinateur
问：1+2=?
答：无法回答

特定任务带标注数据 机器学习 任务专用小模型 专用知识

人工智能发展路线—小结

- 自1956年达特茅斯会议至今，人工智能经历三个主要发展阶段
- 呈现从手工总结到自动学习、从离散符号到连续参数、从专用智能到通用智能趋势

符号智能

时间：1950-1990

知识来源：领域专家

获取方法：手工总结

知识形式：以**知识库**等**符号系统**存储**专家知识**

专用智能

时间：1990-2018

知识来源：特定任务带标注数据

获取方法：机器学习（自动）

知识形式：以**任务专用小模型**存储**任务知识**

通用智能

时间：2018至今

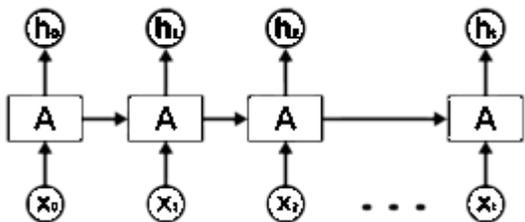
知识来源：通用域无标注数据

获取方法：预训练学习（自动）

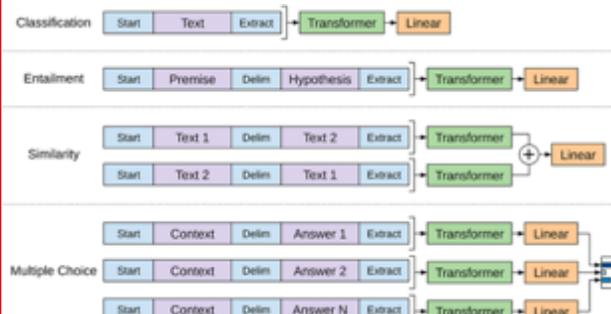
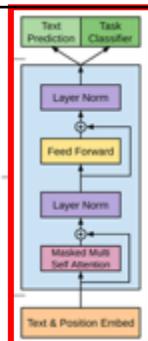
知识形式：以**通用大模型**存储**通用知识**

通用智能—通用模型架构

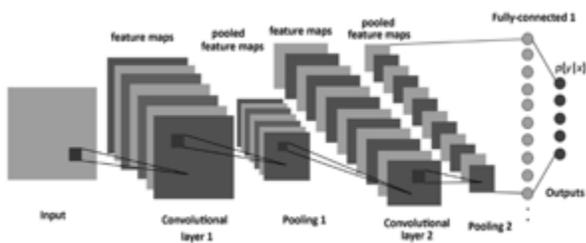
使用 **Transformer 通用架构** 对各类数据进行建模



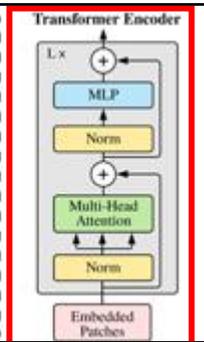
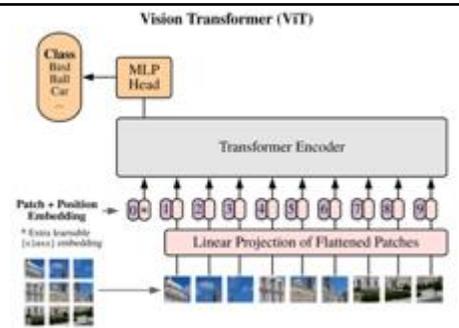
循环神经网络 (RNN) 擅长处理一维序列化文本、语音数据



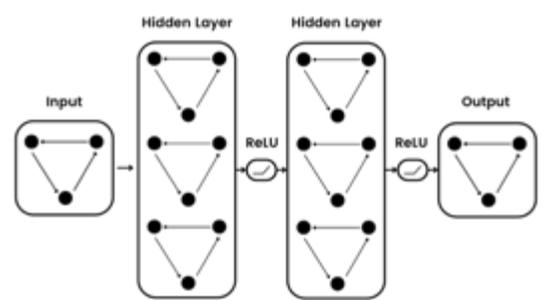
使用**Transformer**进行**文本建模**



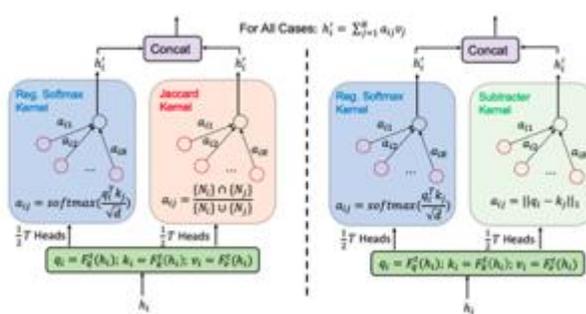
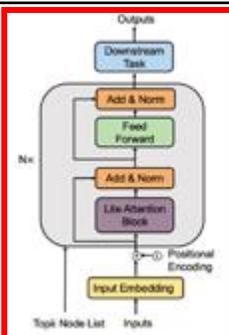
卷积神经网络 (CNN) 擅长处理二维平面图片数据



使用**Transformer**进行**图片建模**



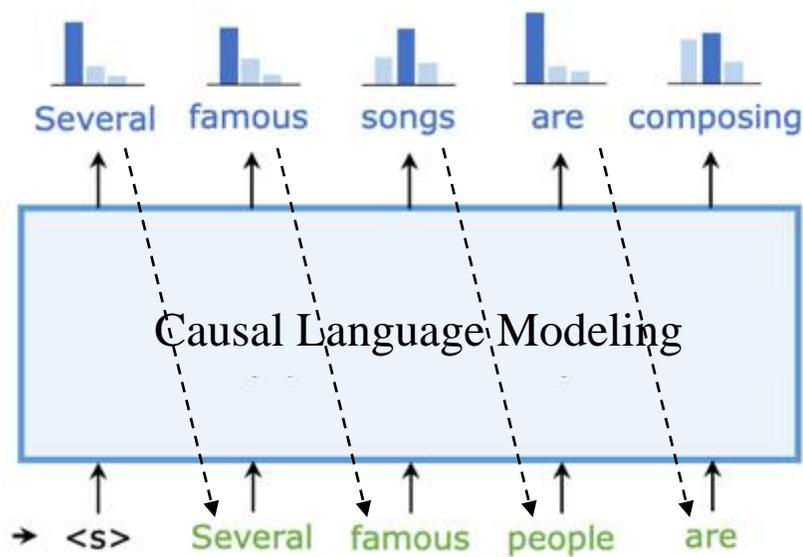
图神经网络 (GNN) 擅长处理结构化、半结构化图数据



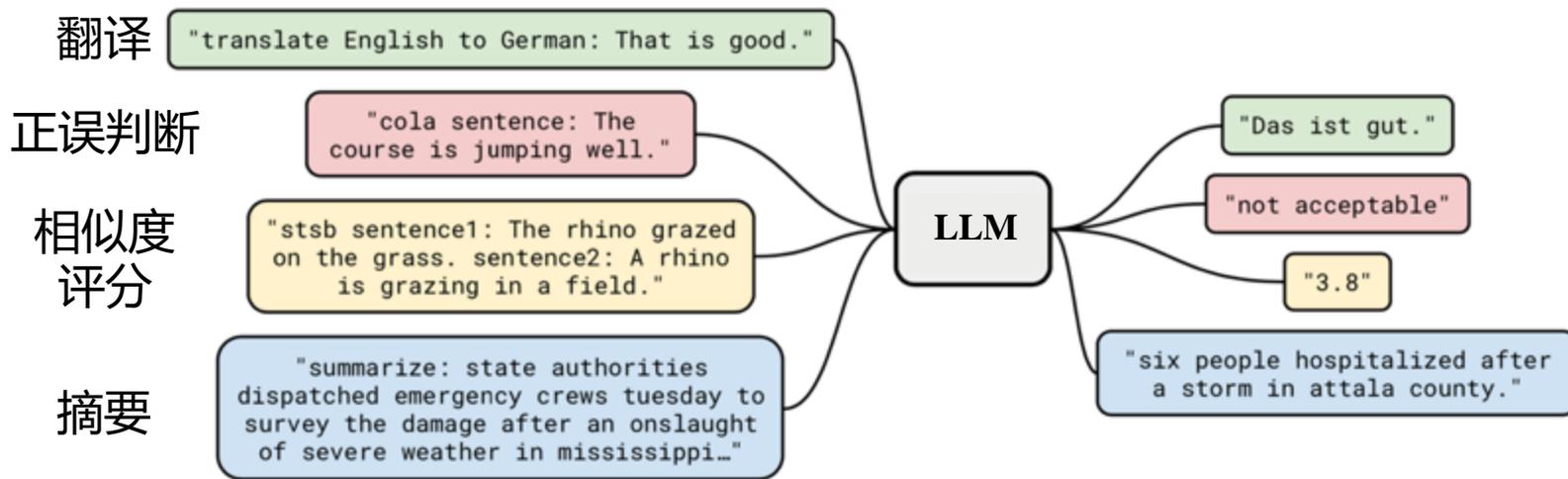
使用**Transformer**进行**图结构建模**

通用智能—通用学习方法

- 使用**预测下一个字符 (Token)** 的**语言建模任务 (Language Modeling)**，从无标注数据中学习通用知识
- 各类自然语言处理任务均可**转化为序列生成**任务进行处理



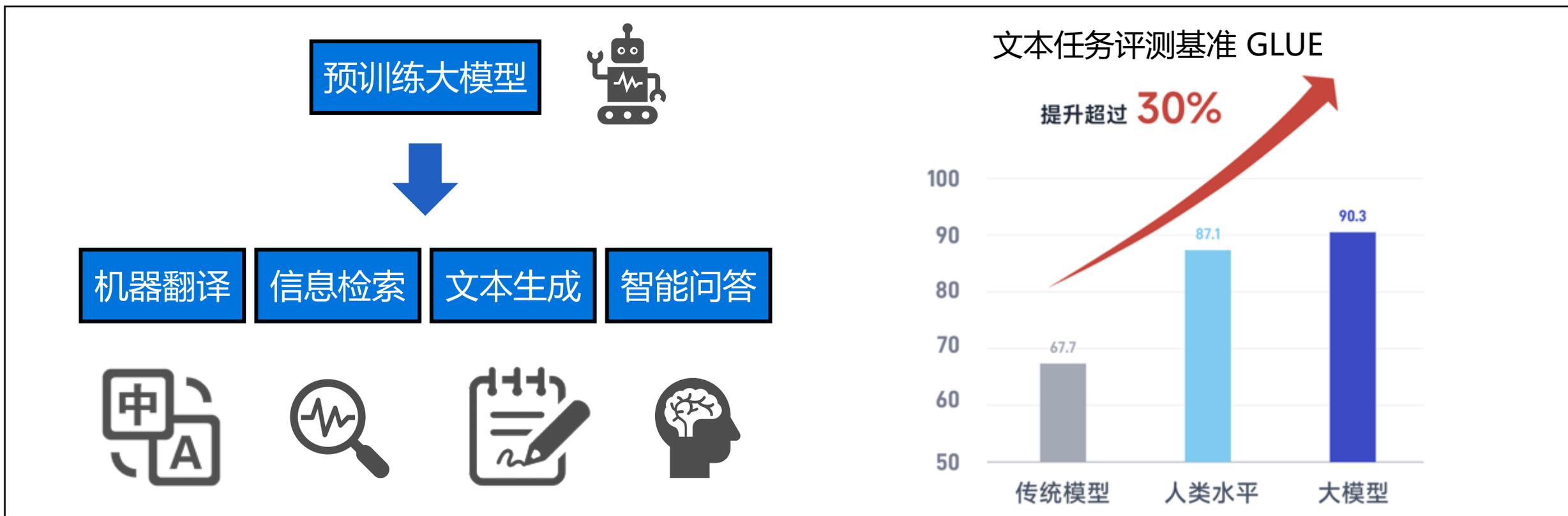
语言建模过程



翻译、正误判断、相似度评分、摘要等文本任务均可转为语言建模形式

通用智能—通用智能能力

- 单个预训练大模型**可同时处理多种任务**
- 在若干权威评测上达到或超过人类水平，远超传统任务专用小模型的水平

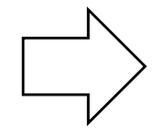
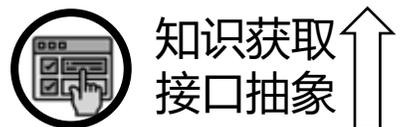
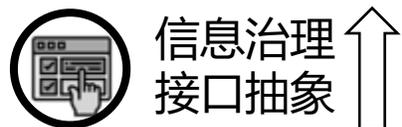
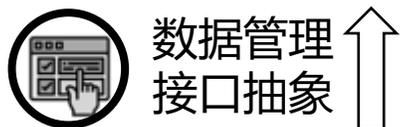
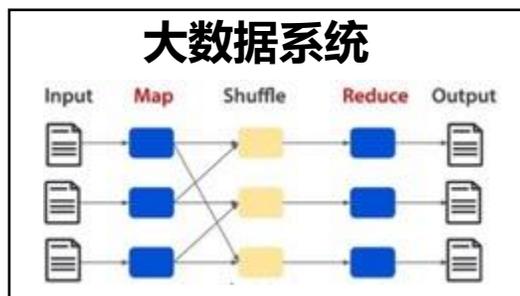


大模型成为智能时代基础设施

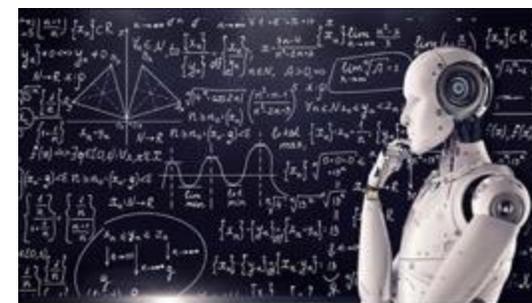
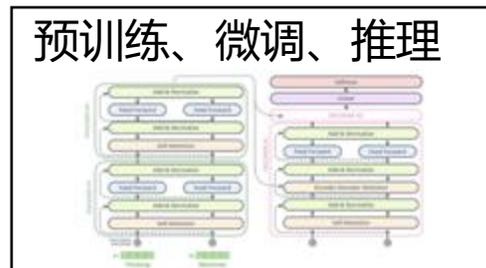
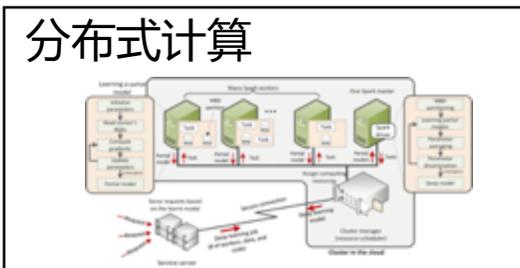
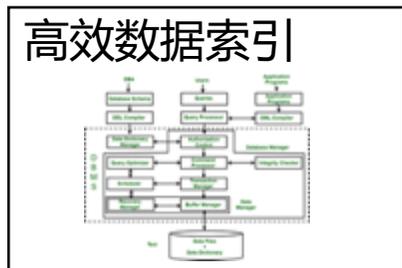


Russell Ackoff
(工程系统巨擘)
“From Data to Wisdom”

用户逻辑层



物理执行层



通用人工智能

大模型的智能涌现

涌现：**量变引起质变**，多个小实体相互作用产生了呈现全新性质的大实体

智能涌现：当计算量突破一定规模，大模型表现出新智能，**部分困难任务迎刃而解**



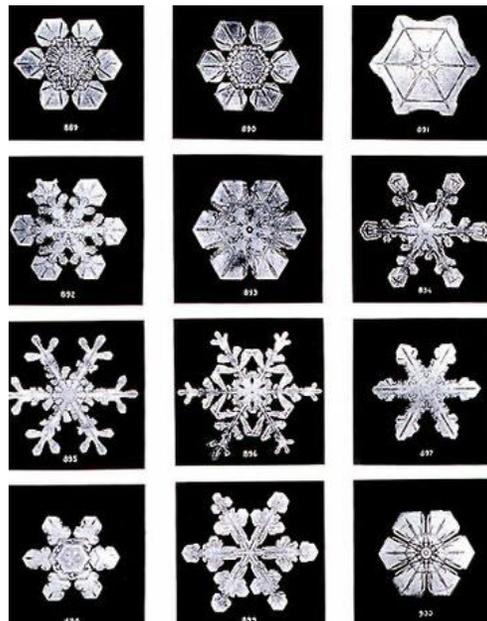
Philip Anderson
(诺贝尔物理学奖获得者)

物理系统在每一个复杂度上都会出现全新的性质



Ilya Sutskever
(OpenAI首席科学家)

语言模型在学习预测下一个字符的过程中来学习对整个宇宙的规律



杂乱无章的水分子间作用力形成了复杂的雪花分形图像



水滴汇聚成大气现象
神经元汇聚成人脑

大模型的智能涌现

学习大数据需要**大参数**，训练大参数模型需要**大算力**，计算量增长使模型**涌现智能**

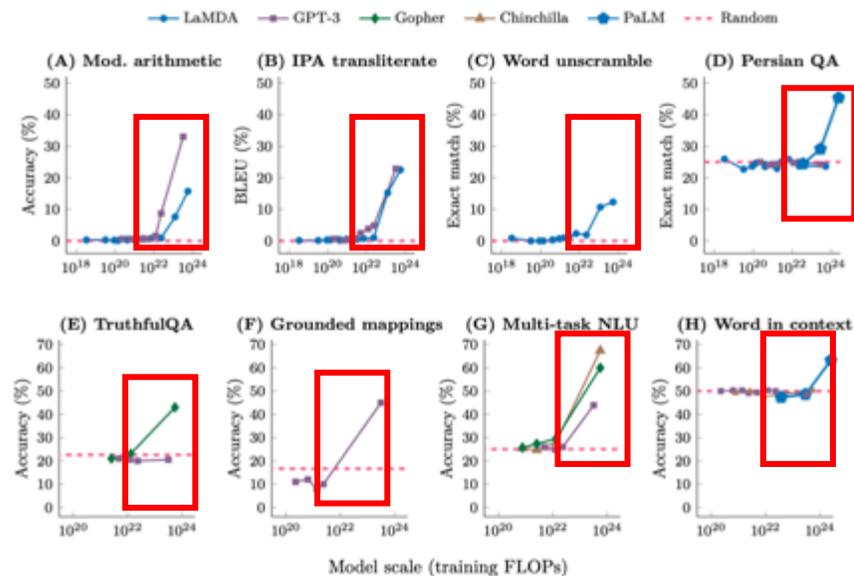
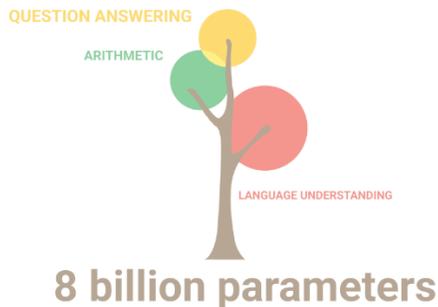


Geoffrey Hinton
(图灵奖获得者)

将GPT-3的壮观表现推断到未来，表明生命、宇宙和万物的答案只是4.398万亿个参数。

大模型随计算量增长而不断生出新能力

大模型随计算量增长而产生能力阶跃



大模型的智能涌现—万物皆可序列化建模

在文本之外，可通过**序列化**方法抽象、学习物理世界中的万事万物

语言



['Founded', 'in', 1988,', Huawei, 'is']..
['class', 'SCLASS', \$INT', '=', ';']..
[('(', '(', '10', '+', '4', ')', '^', '2', ')'].

图像



DNA



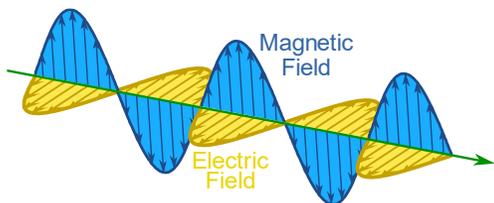
5' ATGACGTGGGGA3'
3' TACTGCACCCCT5'

工具使用

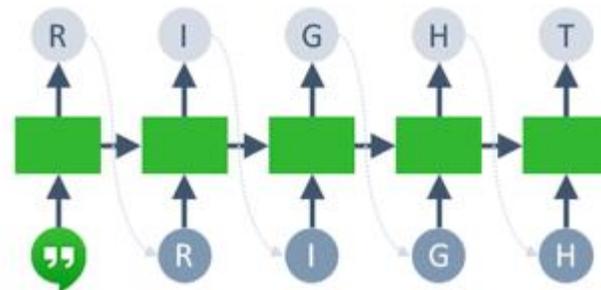


[检索, '翻页', '摘取', '翻译', '总结']..

电磁波



在大模型中，它们都是字符
(Token) 的**序列**



任何可被序列化的信息
均可被大模型学习

2

大模型驱动的自主智能体

大模型的局限性

实时知识缺乏

大模型受限于训练语料，知识有时间局限性。同时由于参数更新困难，难以获取实时知识



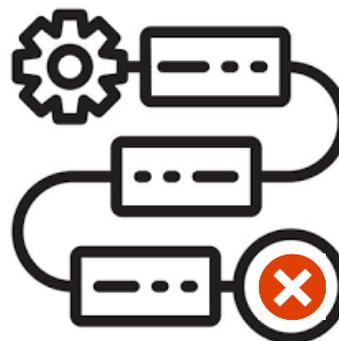
专业技能欠缺

大模型只能处理常见的语言任务，一旦涉及到专业场景，大模型不擅长处理这些专业任务



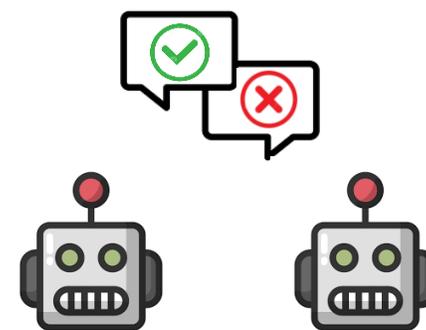
自主能力不足

大模型无法进行多步决策，面对复杂任务无法规划复杂逻辑，编排复杂流程来解决



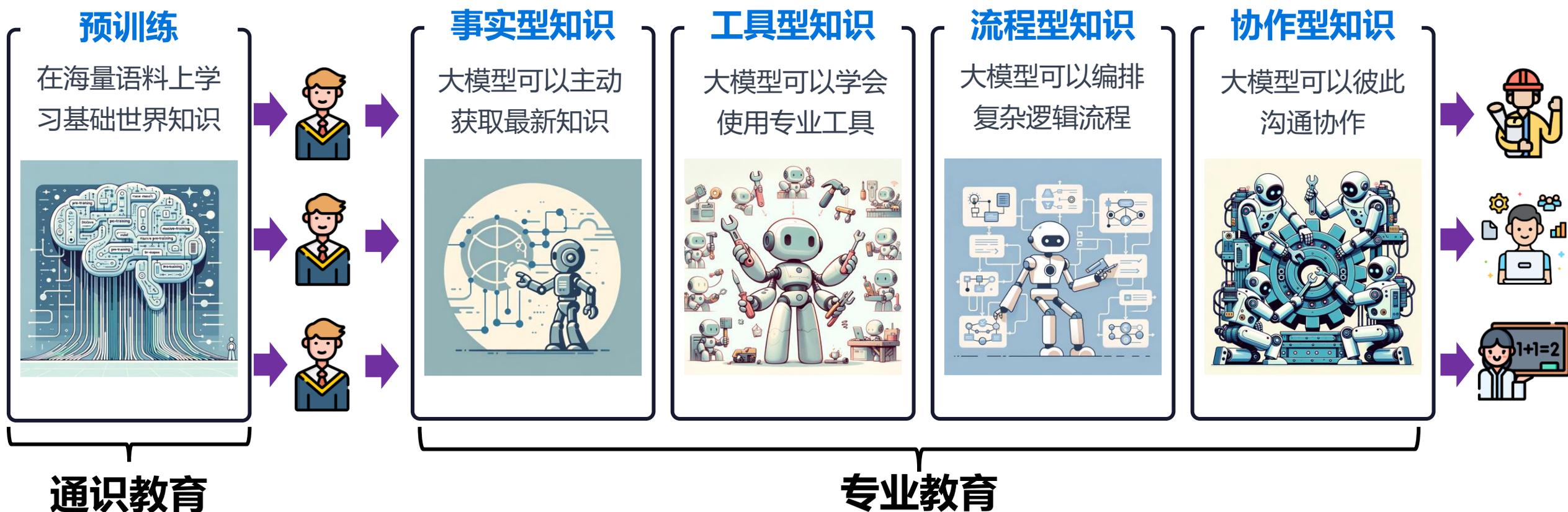
协作意识薄弱

大模型缺少协作意识，彼此之间无法协同配合，共同完成复杂任务



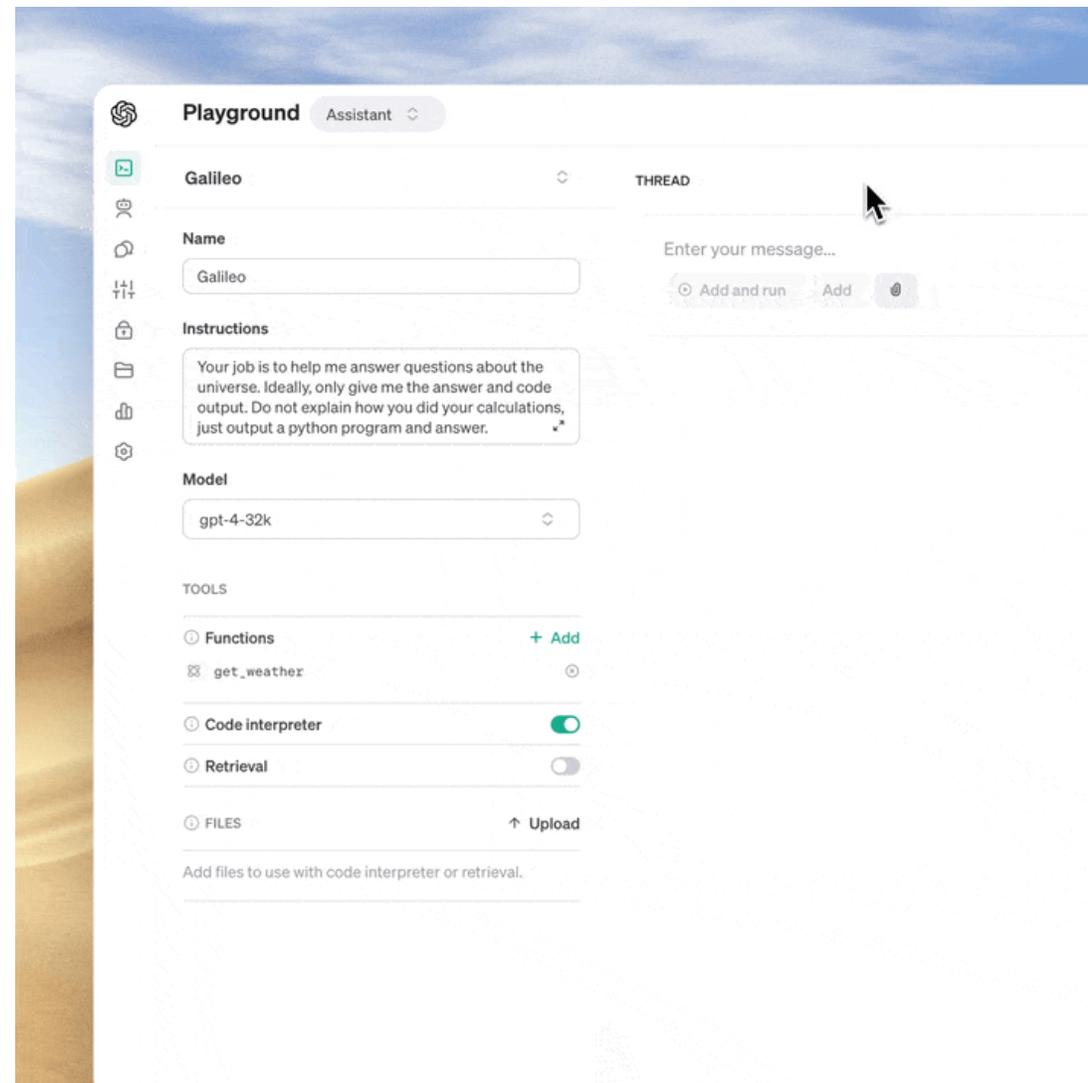
大模型专业教育：智能体化

- 大模型通过预训练完成通识教育，需要进一步学习专业知识实现专业教育赋能行业应用



| 智能体技术正在成为OpenAI的核心战略

- 2023年11月6日第一届OpenAI开发者大会，创始人Sam Altman的演讲后半部分集中在Agent以及相关生态的构建上：
 - Assistants API：提供代码解释、函数调用、检索等能力，方便开发者构建Agent
 - GPTs应用商店：用户和开发者可以定制和商业化发布自己的Agent
- 帮助用户和开发者更好的构建智能体并为其寻找商业模式已经成为OpenAI目前的重要工作



专业教育：知识图谱与检索增强生成智能

检索增强生成(RAG)技术让智能体掌握事实性知识，是实现专业智能体的基础

发展脉络：
信息从简单到复杂，
问答系统从规则抽取到语义理解

Baseball QA System
进行简单问答



Ask Jeeves线
上问答平台

IBM Watson在知识
问答比赛上击败人类



正式提出RAG作为
NLP重要任务之一

DPR在开放域问答
取得显著进展



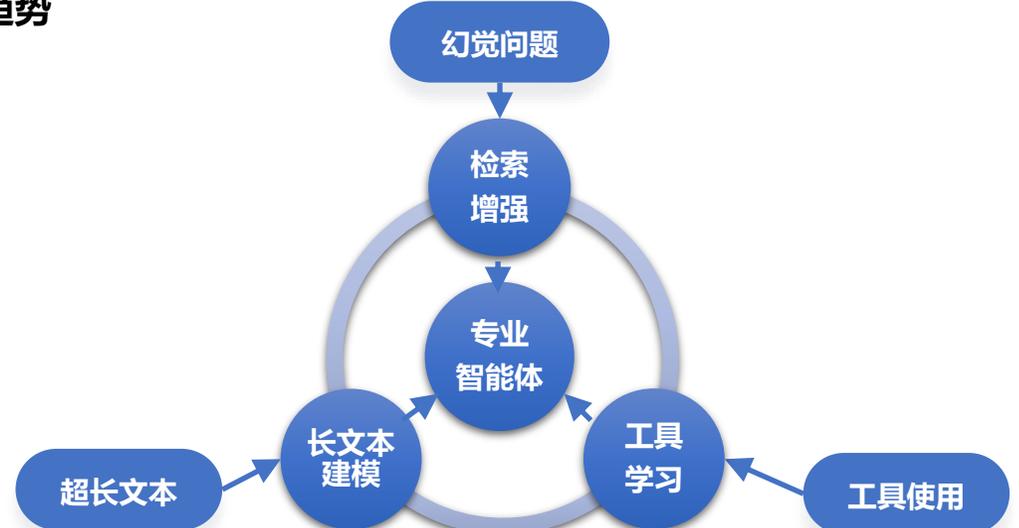
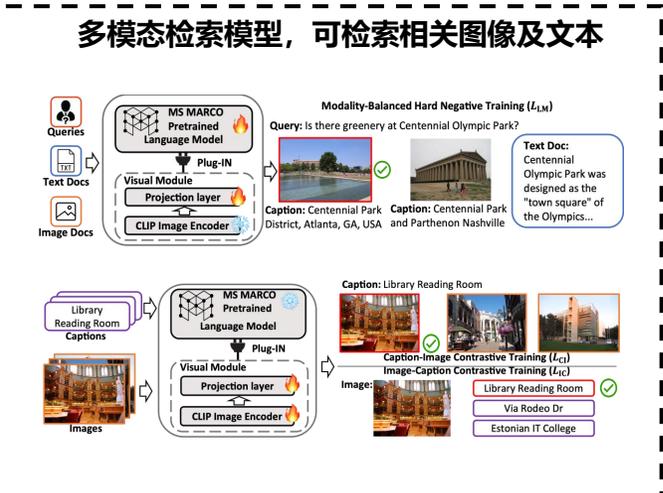
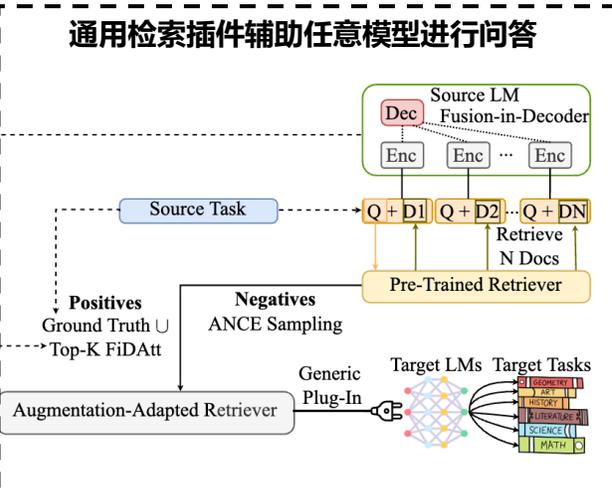
AAR检索插件用于
辅助任意模型

UniVL-DR实现
高效多模态检索



成果：信息检索模型逐渐走向通用与多模态

未来趋势

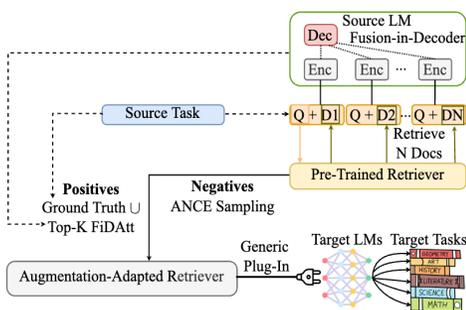


专业教育：检索增强生成智能

- 检索增强生成存在着**检索模型通用性差**、**人类偏好对齐差**、**跨模态检索难**的挑战

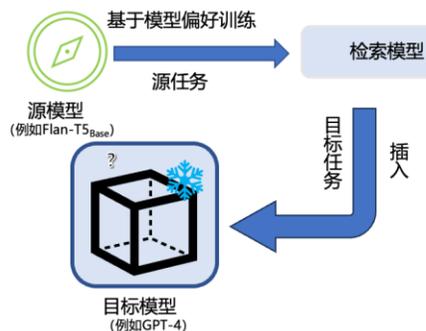
检索模型通用性差

现有检索模型针对不同大模型进行相应设计，致导检索模型难以适用于不同大模型



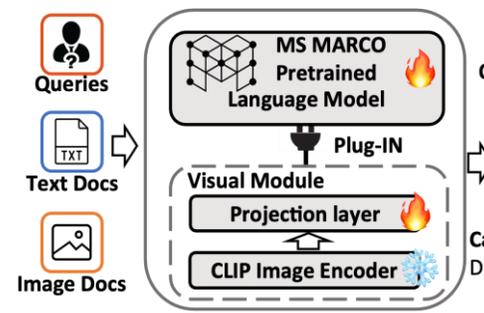
人类偏好对齐差

检索模型通常使用人类偏好训练，与大模型的信息获取偏好存在偏差，导致生成效果差



跨模态检索难

检索增强技术仅局限于对文本类数据进行检索，难以应用到如图像等其它模态的数据上



专业教育：检索增强生成智能

- 检索增强生成（RAG）中的检索部分通常使用人类偏好训练，与大模型的信息获取偏好存在**偏差**，亟待训练适配大模型的信息检索模型

信息检索的人类偏好与模型偏好



错过了游轮怎么办？

人类偏好文档

如果您错过了游轮，请您前往码头，和港口代理联络...

倾向于**直接回答**

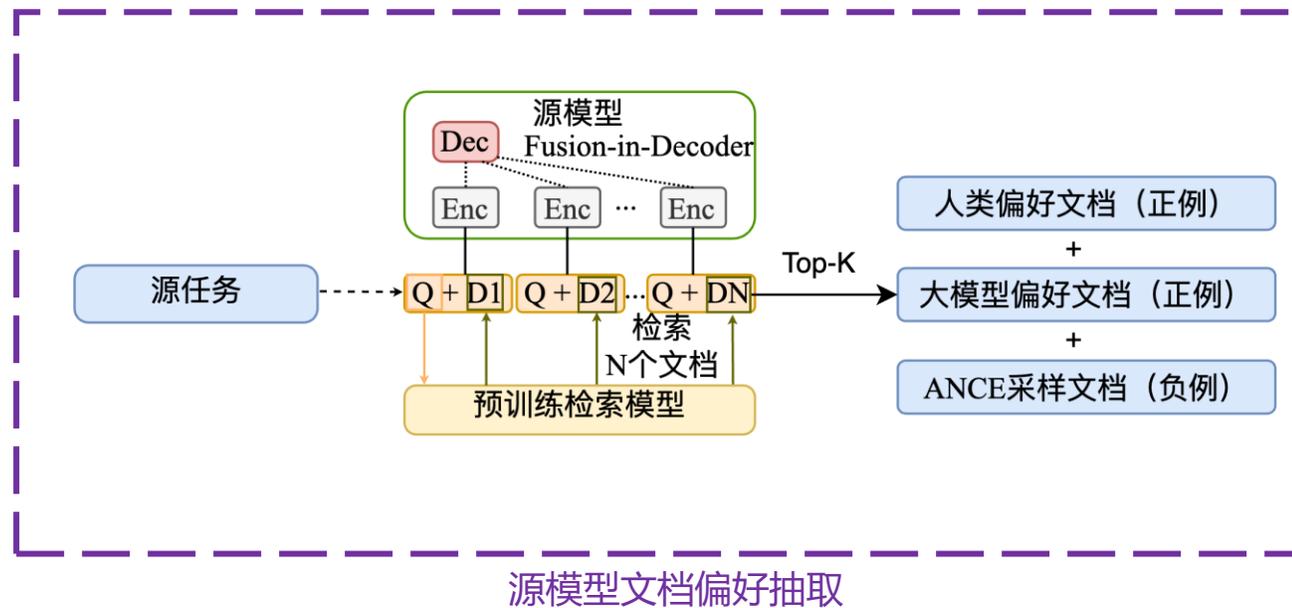
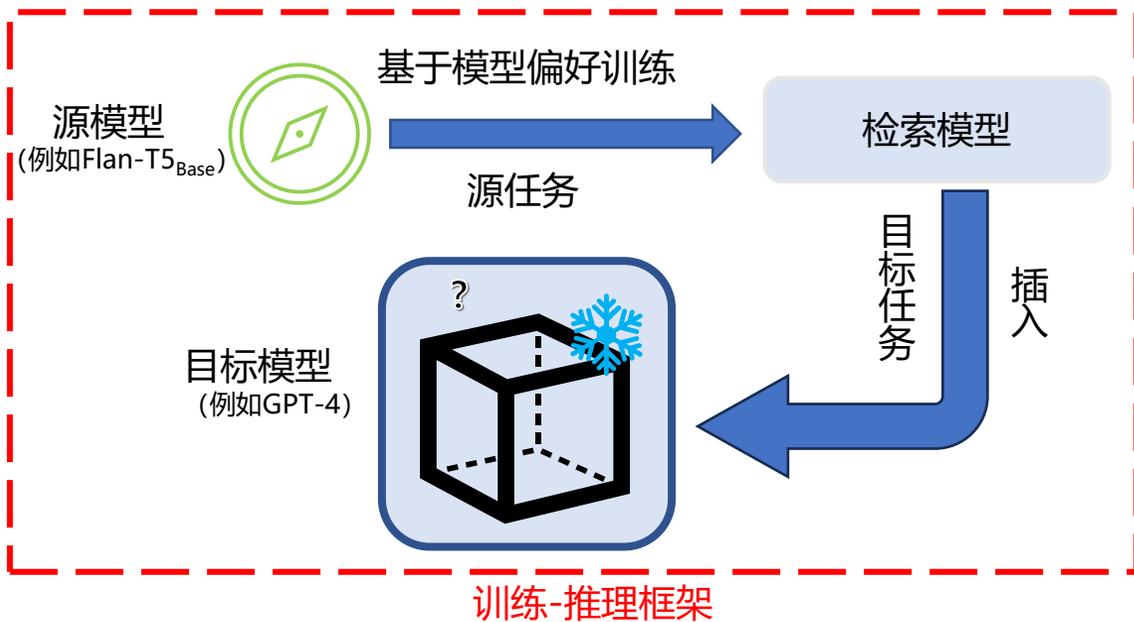
大模型偏好文档

如果乘客误船，邮轮公司不承担将乘客送往下一个港口的财务责任...

倾向于**提供补充信息**，大模型可以利用补充信息提供**更全面的回复**

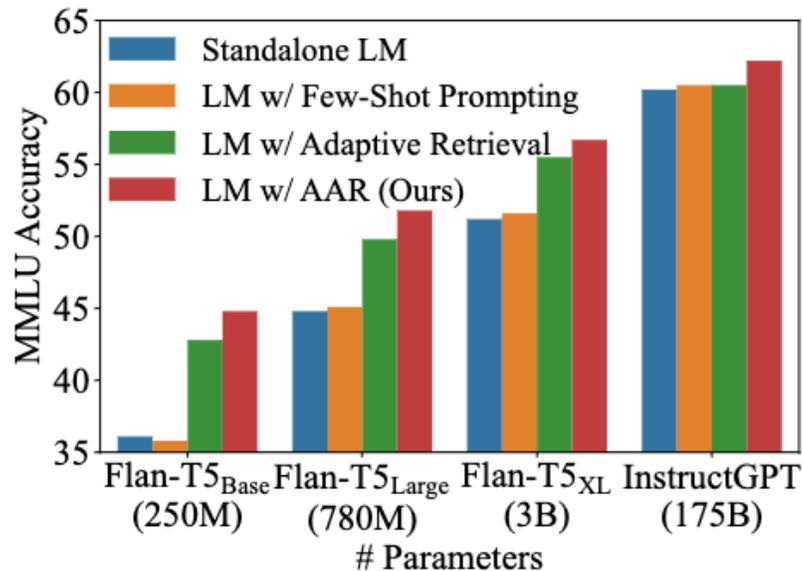
专业教育：检索增强生成智能

- 基于解码器-编码器注意力机制的**大模型文档偏好抽取**
- 融合**大模型偏好**信号和**人类偏好**信号的**适应性检索器训练**

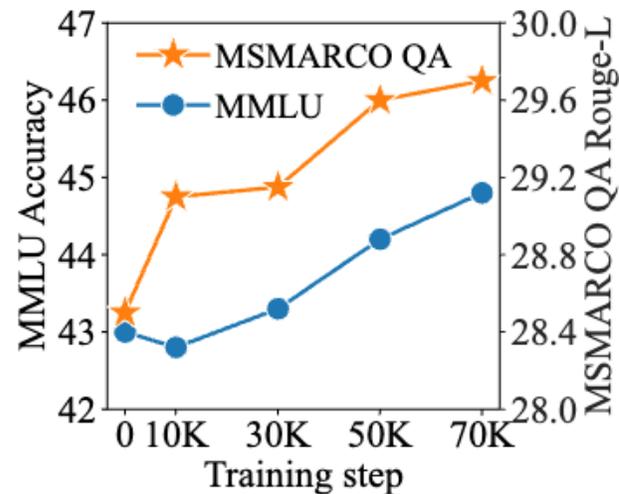


专业教育：检索增强生成智能

- 生成结果质量**超越普通检索增强生成方法**
- **单一源**语言模型训练的检索器可以作为**多种目标**语言模型的**通用插件**，提高各类语言模型的**泛化能力**，例如250M Flan-T5和175B InstructGPT



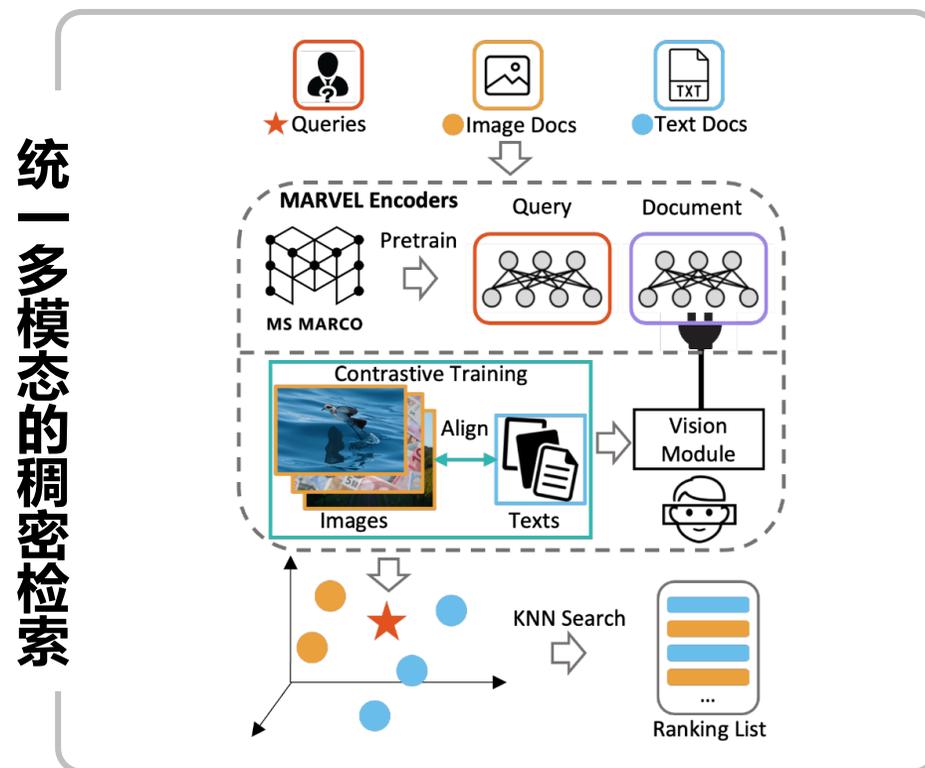
效果稳定超过普通检索增强生成基线



大模型偏好训练持续增强RAG效果

专业教育：检索增强生成智能

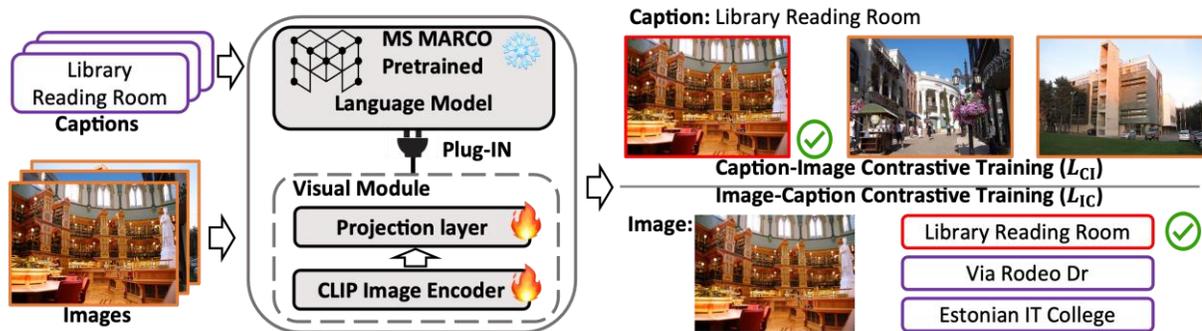
- 多模态模型使用不同编码器编码文本和图像，存在**模态差异**问题，影响检索效果
- MARVEL：基于视觉模块插件的多模态检索模型，使用**统一视觉模块插件**实现稠密检索器的多模态检索能力



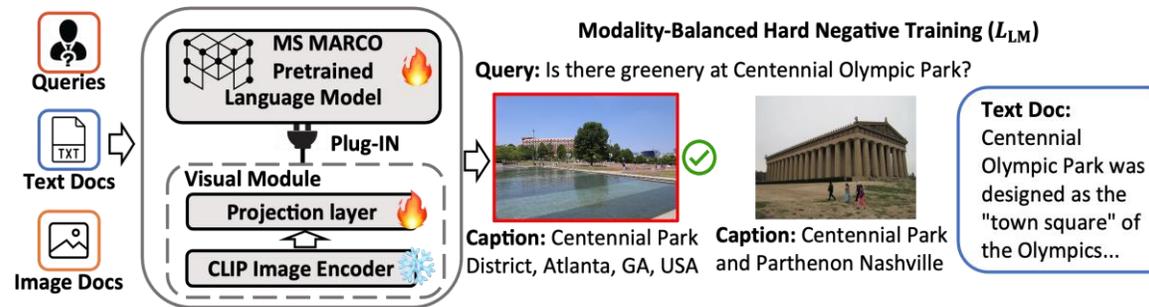
专业教育：检索增强生成智能

- 通过视觉编码器对齐到预训练语言检索模型T5-ANCE，为图像和文本建立了统一的表示方式
- 采用预训练 + 微调**两阶段进行视觉模块信息表示能力构建**

多模态检索能力构建



(a) 预训练视觉模块使其适配到稠密检索模型



(b) 微调语言模型获取捕获图片表示的能力

| 专业教育：检索增强生成智能

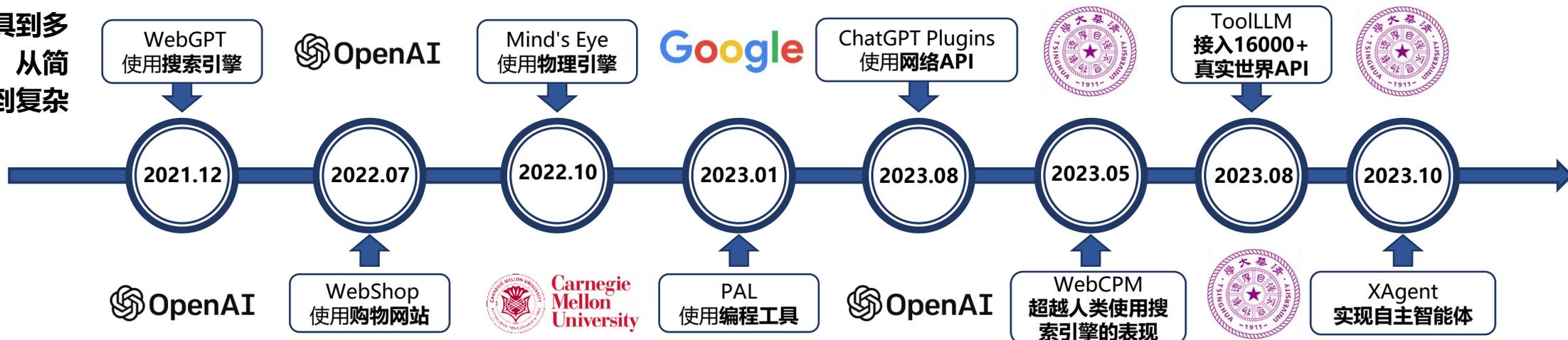
- MARVEL将**文本检索模型的优势**引入了**多模态检索**任务，验证了语言模型具有**提取图像语义**并将其**映射到词嵌入空间**的能力，**缓解不同模态间的差距**

Setting	Model	WebQA			ClueWeb22-MM		
		MRR@10	NDCG@10	Rec@100	MRR@10	NDCG@10	Rec@100
Single Modality (Text Only)	BM25	53.75	49.60	80.69	40.81	46.08	78.22
	DPR (Zero-Shot)	22.72	20.06	45.43	20.59	23.24	44.93
	CLIP-Text (Zero-Shot)	18.16	16.76	39.83	30.13	33.91	59.53
	Anchor-DR (Zero-Shot)	39.96	37.09	71.32	42.92	48.50	76.52
	T5-ANCE (Zero-Shot)	41.57	37.92	69.33	45.65	51.71	83.23
	BERT-DPR	42.16	39.57	77.10	38.56	44.41	80.38
	NQ-DPR	41.88	39.65	78.57	39.86	46.15	83.50
	NQ-ANCE	45.54	42.05	69.31	45.89	51.83	81.21
Divide-Conquer	VinVL-DPR	22.11	22.92	62.82	29.97	36.13	74.56
	CLIP-DPR	37.35	37.56	85.53	39.54	47.16	87.25
	BM25 & CLIP-DPR	42.27	41.58	87.50	41.58	48.67	83.50
UnivSearch	CLIP (Zero-Shot)	10.59	8.69	20.21	16.28	18.52	40.36
	VinVL-DPR	38.14	35.43	69.42	35.09	40.36	75.06
	CLIP-DPR	48.83	46.32	86.43	42.59	49.24	87.07
	UniVL-DR	62.40 ^{†§}	59.32 ^{†§}	89.42 ^{†§}	47.99 ^{†§}	55.41 ^{†§}	90.46 ^{†§}
	MARVEL-DPR	55.71 [†]	52.94 [†]	88.23 [†]	46.93 [†]	53.76 [†]	88.74 [†]
	MARVEL-ANCE	65.15 ^{†‡§}	62.95 ^{†‡§}	92.40 ^{†‡§}	55.19 ^{†‡§}	62.83 ^{†‡§}	93.16 ^{†‡§}

专业教育：工具智能

工具学习技术让智能体学会使用搜索引擎等认知工具，拓展智能体能力边界

发展脉络：从单一工具到多种工具，从简单工具到复杂工具



成果：从模仿人类行为到自主完成任务，自主化程度逐步提高

未来趋势：从使用工具迈向自主智能体

模仿人类行为学习使用高级认知工具

ACL 2023 ★ 954

根据工具教程学会使用新工具

ICLR 2024 Spotlight ★ 4.4k

自主探索规划组合使用工具

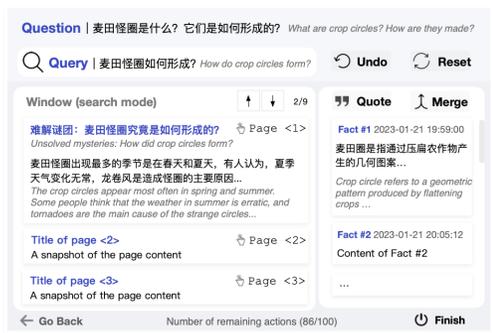
GitHub开源项目 ★ 7.5k

专业教育：工具智能

- 工具学习存在着**复杂工具学习难**、**工具泛化能力差**、**工具组合使用能力不足**等挑战

复杂工具学习难

大模型在面对复杂认知工具时，例如：搜索引擎、知识图库、数据库等，难以学习类人的使用策略



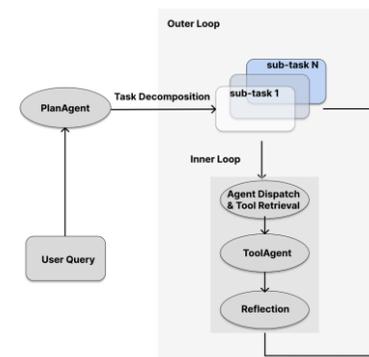
工具泛化能力差

大模型通常只能使用学习过的工具，一旦涉及新的工具，便难以根据工具的教程快速泛化



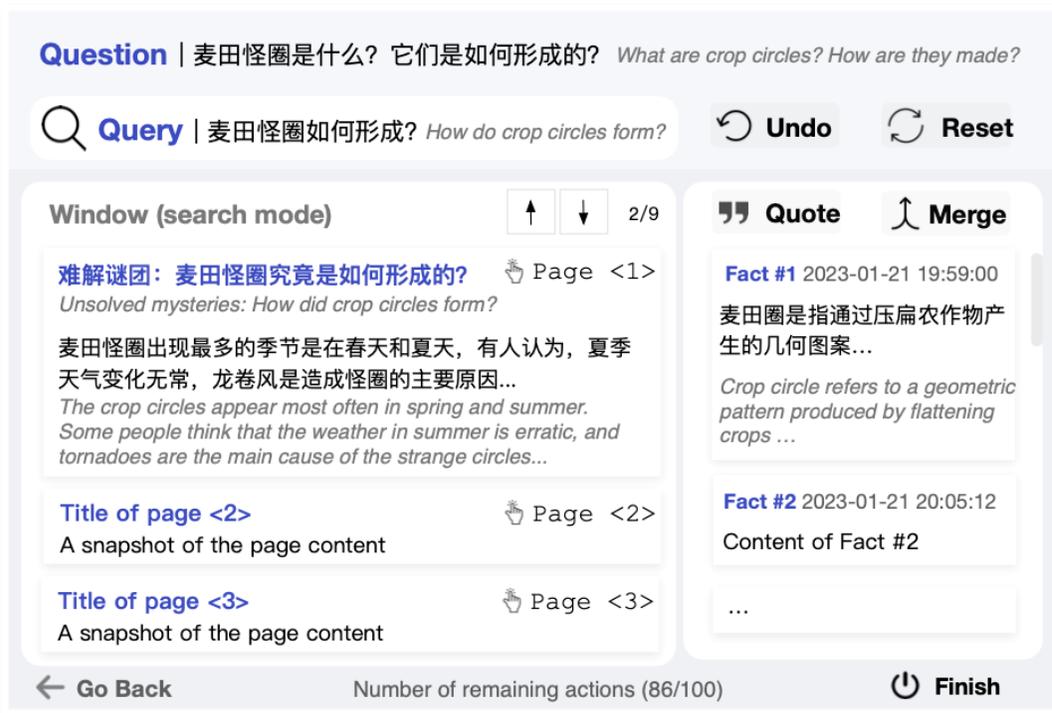
组合使用能力不足

大模型无法进行多种工具的组合使用，面对复杂任务无法将其拆解为多个子任务，并使用不同工具解决



| 专业教育：工具智能

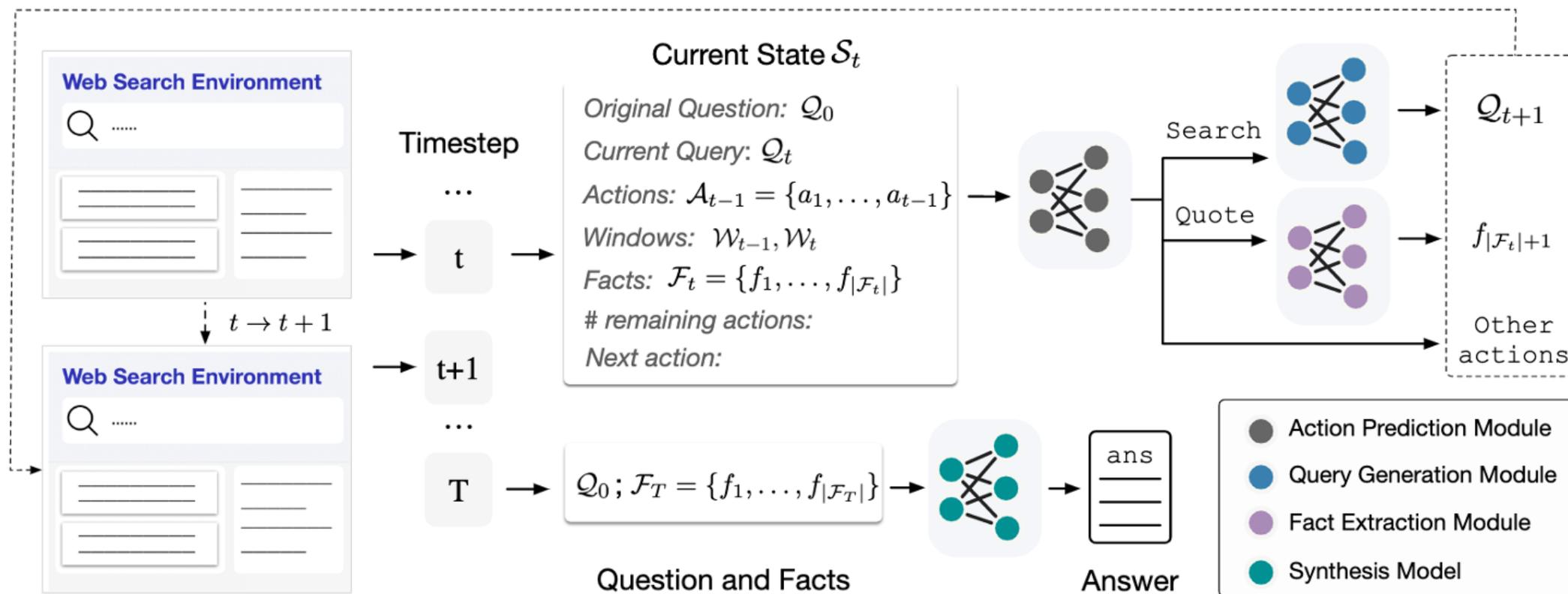
- WebCPM：首个基于交互式网络搜索的中文领域开源问答框架，**模仿人类使用搜索引擎行为**，学习使用搜索引擎
- 构建**首个中文网络搜索LFQA数据集**，含有5500条记录



Action Name	Functionality
🔍 Search <query>	Call Bing search with <query>
⬅️ Go Back	Return to the previous window
👆 Load Page <1>	Load the details of page <1>
👆 Load Page <2>	Load the details of page <2>
👆 Load Page <3>	Load the details of page <3>
⬆️ Scroll Up	Scroll up for a pre-set stride
⬇️ Scroll Down	Scroll down for a pre-set stride
🗉 Quote <content>	Extract <content> from the current page as a supporting fact
🔗 Merge	Merge two facts into a single fact
🛑 Finish	End the search process

专业教育：工具智能

- 在接收到查询请求后，WebCPM会**自主**决定每一步的操作（滚动、搜索、点击等），直到收集到足够的信息来回答问题。该过程**完全自动化**，无需用户介入



专业教育：工具智能

- 微调后的大模型可以**获得使用搜索引擎的能力**，展示出**类人的搜索策略**

Question:

麦田怪圈是什么？它们是如何形成的？

Action Sequence:

Search → Load Page <1> → Scroll Down × 5 → Scroll Up → Scroll Down × 11 → Go Back → Search → Load Page <1> → Go Back → Load Page <3> → Scroll Down × 4 → Scroll Up × 3 → Quote → Scroll Down → Quote → Scroll Down → Quote → Scroll Down → Quote → Finish

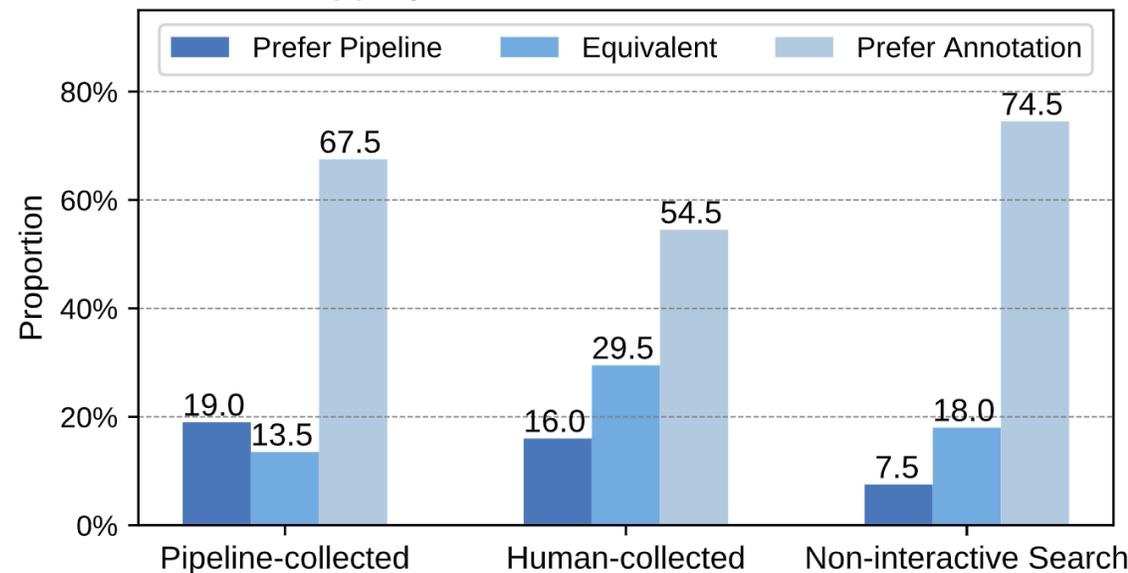
Supporting Facts:

- 麦田怪圈（Crop Circle），是指在麦田或其它田地上，通过某种未知力量（大多数怪圈是人类所为）把农作物压平而产生出来的几何图案。这个神秘现象有时被人们称之为“Crop Formation”。麦田怪圈的出现给了对支持外星人存在论的人们多种看法。
- 人为说：人为说一般认为，麦田圈是用木板压成的。木板两头系上绳子形成圈套，在制作时，一脚踩在木板上拖动木板压倒麦子，并拉着细绳与圆心保持固定的距离，逐渐就可以形成一个圆圈。为了便于制造，主要形状所有圆圈的直径都可以被6除尽。以前曾经出现过制作麦田圈被当场抓获的事情，制作者使用的就是这种工具。
- 自然形成说：也有人认为，麦田圈只是一种，成因还未被人类发现。就像雷电，古时候人类也是以为是雷神电母做的，对于麦田圈中经常出现人文信息的现象，他们认为这只是人们“先入为主”造成的错觉。
- 磁场说：有专家认为，磁场中有一种神奇的移动力，可产生一股电流，使农作物“平躺”在地面上。美国专家杰弗里·威尔逊研究了130多个麦田怪圈，发现90%的怪圈附近都有连接高压电线的变压器，方圆270米内都有一个水池。由于接受灌溉，麦田底部的土壤释放出的离子会产生负电，与高压电线相连的变压器则产生正电，负电和正电碰撞后会产生电磁能，从而击倒小麦形成怪圈。

Answer:

麦田怪圈是指在麦田或其它田地上，通过某种未知力量（大多数怪圈是人类所为）把农作物压平而产生出来的几何图案。【1】而麦田怪圈的形成有三个说法，人为说、自然说与磁场说。人为说一般认为，麦田圈是用木板压成的。木板两头系上绳子形成圈套，在制作时，一脚踩在木板上拖动木板压倒麦子，并拉着细绳与圆心保持固定的距离，逐渐就可以形成一个圆圈。为了便于制造，主要形状所有圆圈的直径都可以被6除尽。【2】自然形成说认为麦田怪圈的成因还未被人类发现。就像雷电，古时候人类也是以为是雷神电母做的，对于麦田圈中经常出现人文信息的现象，他们认为这只是人们“先入为主”造成的错觉。【3】磁场说认为，磁场中有一种神奇的移动力，可产生一股电流，使农作物“平躺”在地面上。【4】

(a) Pipeline Evaluation on Our Test Set



- pipeline-collected,
- human-collected,
- non-interactive search (TF-IDF)

专业教育：工具智能

- ToolLLM：旨在构建开源、大规模、高质量的指令微调数据，以促进大模型具有**通用工具使用能力**
 - 使大型模型具备**16,000+**个真实API的能力
 - 支持**49种领域工具使用**场景

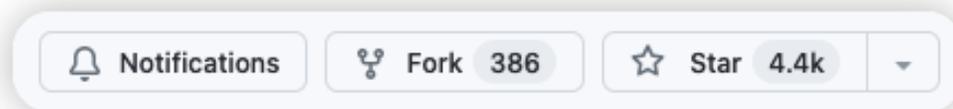
 TOOLLLM: FACILITATING LARGE LANGUAGE MODELS TO MASTER 16000+ REAL-WORLD APIS

Yujia Qin^{1*}, Shihao Liang^{1,2*}, Yining Ye¹, Kunlun Zhu^{1,2}, Lan Yan^{1,2}, Yaxi Lu¹, Yankai Lin^{3†}, Xin Cong¹, Xiangru Tang⁴, Bill Qian⁴, Sihan Zhao¹, Runchu Tian¹, Ruobing Xie⁵, Jie Zhou⁵, Mark Gerstein⁴, Dahai Li^{2,6}, Zhiyuan Liu^{1†}, Maosong Sun^{1†}

¹Tsinghua University ²ModelBest Inc. ³Renmin University of China

⁴Yale University ⁵WeChat AI, Tencent Inc. ⁶Zhihu Inc.

yujiaqin16@gmail.com



 ToolBench

Tool Num 29 API Num 86 Current Dataset Size 98K Total API Call 312K Tool LLaMA Released

[Model](#) • [Data Release](#) • [Toolkit](#) • [Paper](#) • [Paper List](#) • [Citation](#)



LLaMA

+



ToolBench

=

Tool
LLaMA



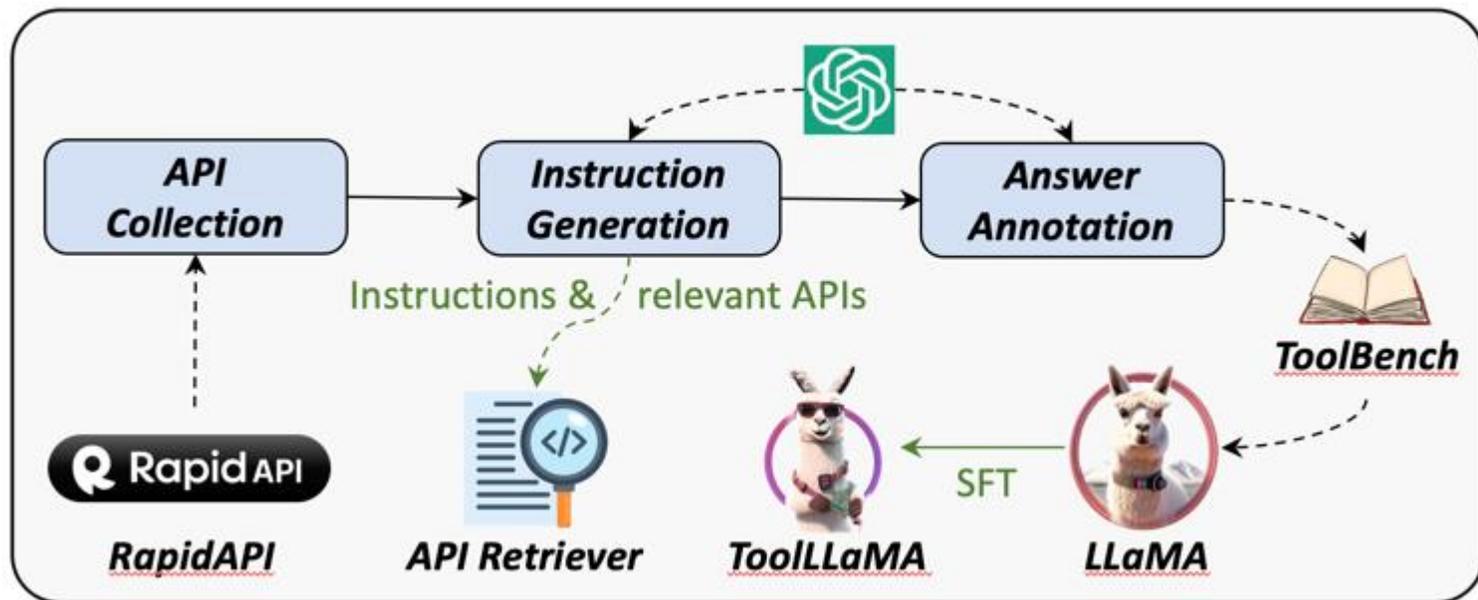
≈



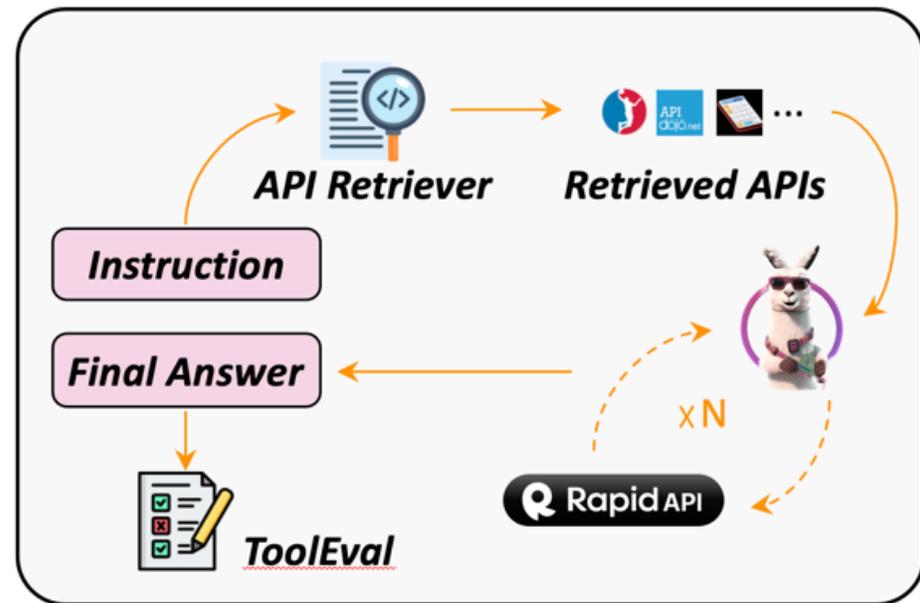
ChatGPT

专业教育：工具智能

- 支持根据工具描述**自动生成工具使用指令微调数据集**
- 支持多种**复杂工具调用**场景、自动**工具推荐**、工具能力**自动评测**



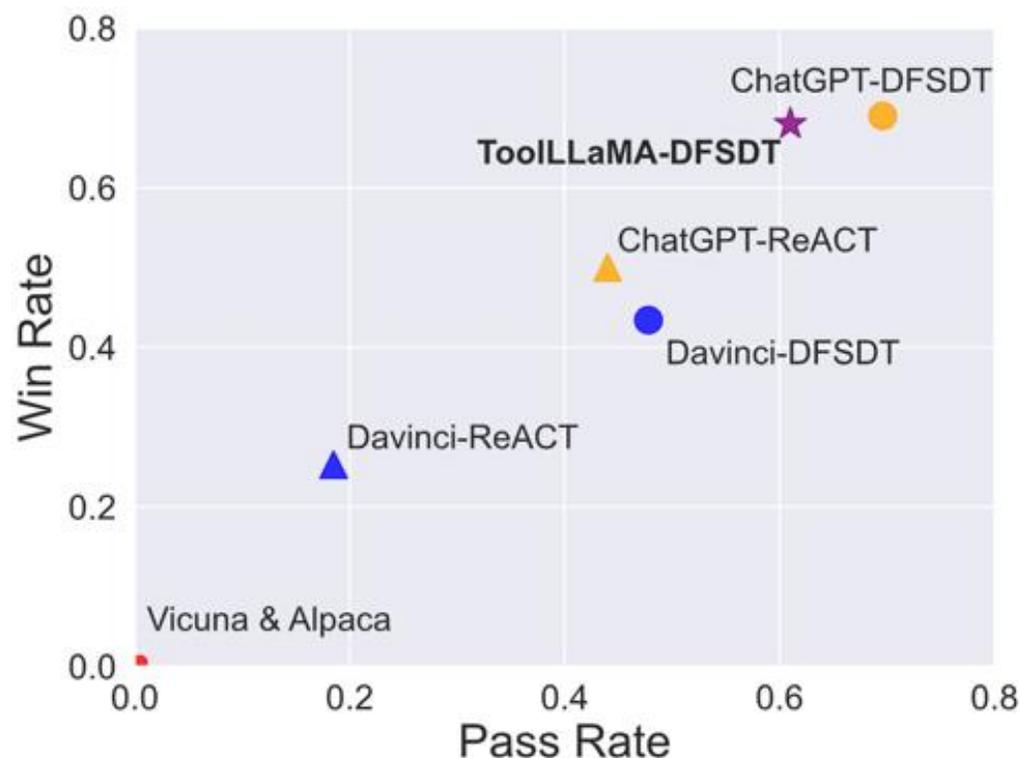
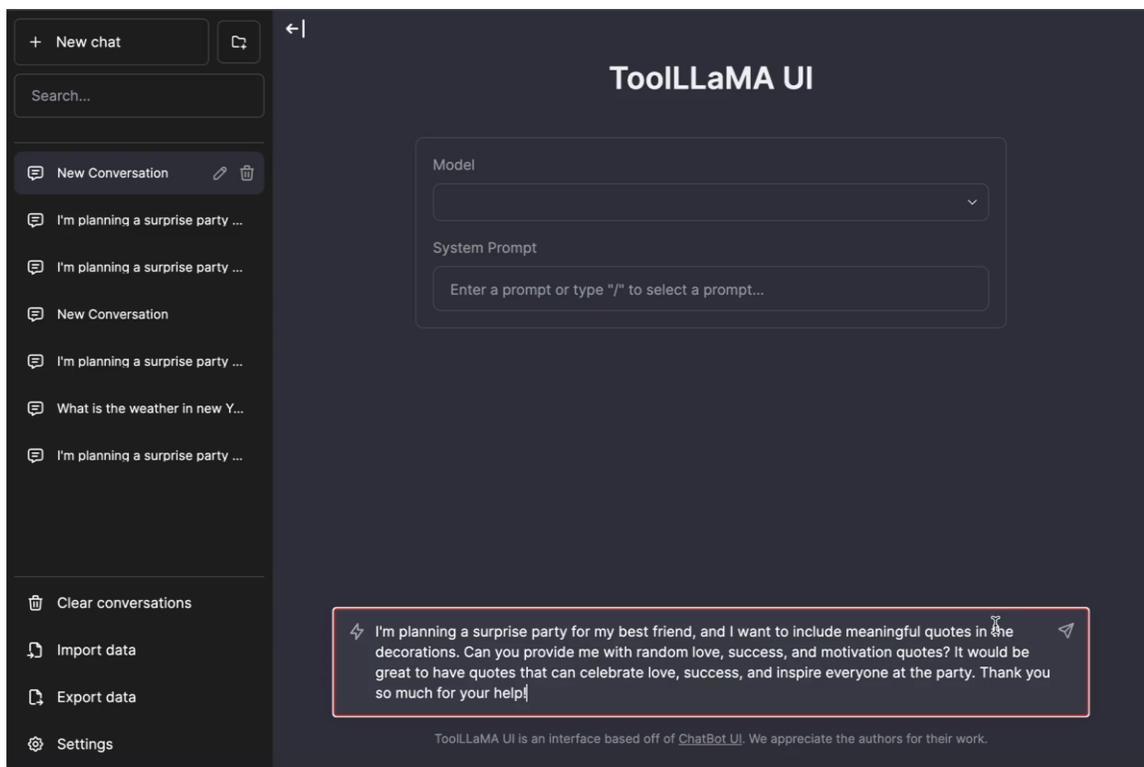
数据收集与模型训练



模型推理与性能评测

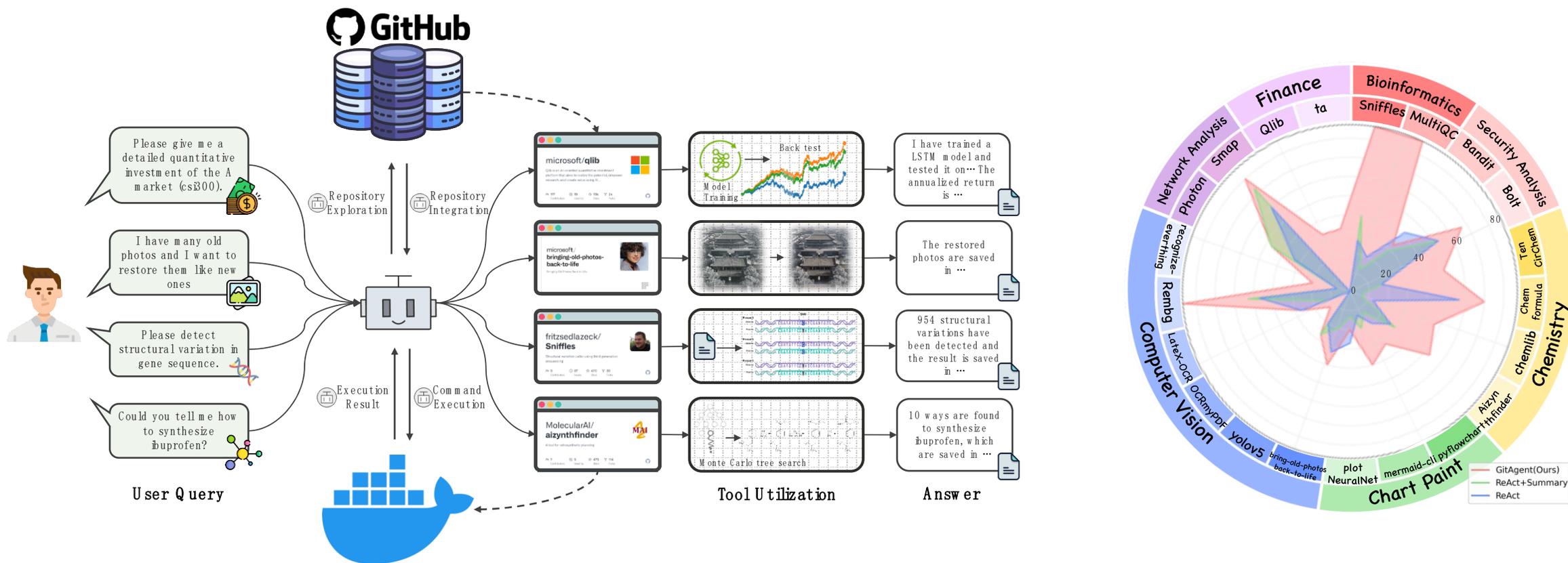
专业教育：工具智能

- 基于 ToolLLM 框架，自动构造工具学习数据集 ToolBench
- 基于 ToolBench 数据训练后的模型能够**高效泛化**到未见过的新API并高效调用，工具使用能力**接近ChatGPT**



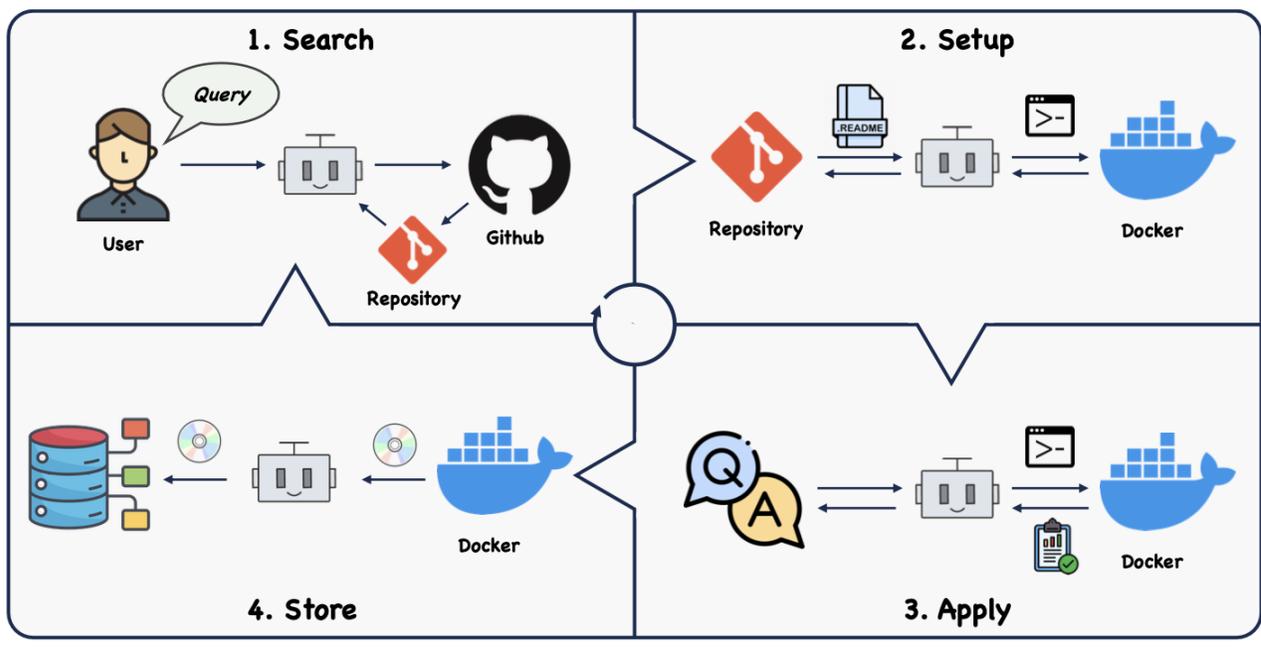
专业教育：工具智能

- GitAgent: 让Agent可以根据用户需求自主从GitHub上集成合适的Repo, **扩充工具集合**, 延展自身的能力边界

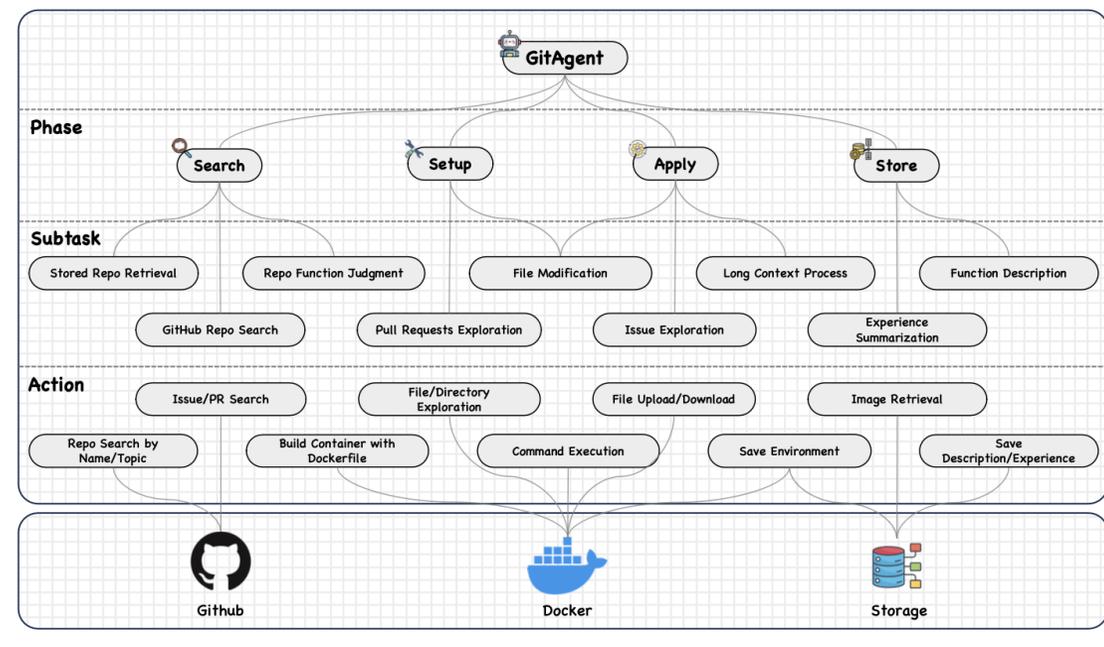


专业教育：工具智能

- 将工具扩展划分成四个阶段：**工具搜索**、**环境配置**、**工具使用**、**工具保存**
- 可以根据用户指令，**自主对Repo进行调整或修改**，以满足用户需求



GitAgent包含的四个阶段：工具搜索、环境配置、工具使用、工具保存

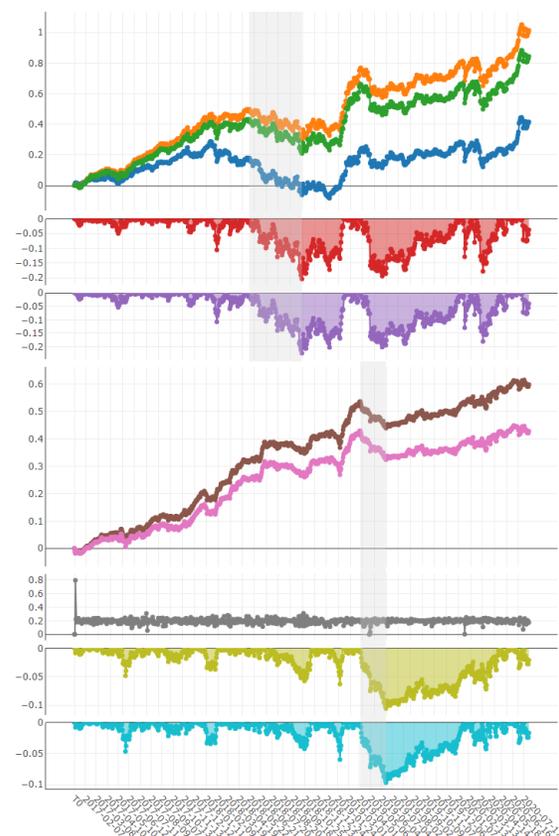


GitAgent可在各阶段自主解决遇到的不同问题

专业教育：工具智能

- GitAgent可以自主集成**7大专业领域**中共**21个Repo**为自身工具，从而完成复杂专业任务

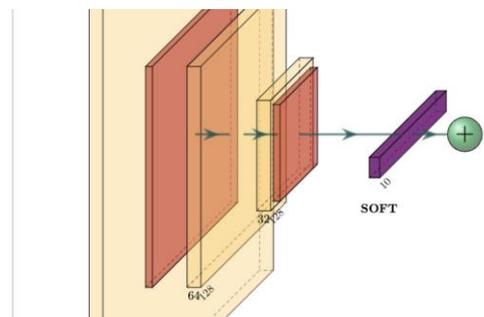
金融量化交易分析



老照片翻新



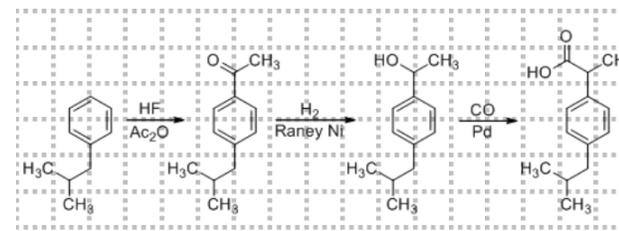
学术绘图



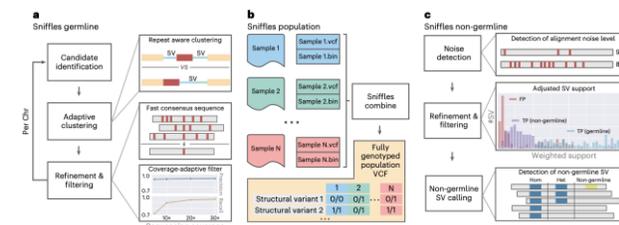
量子化学



有机合成

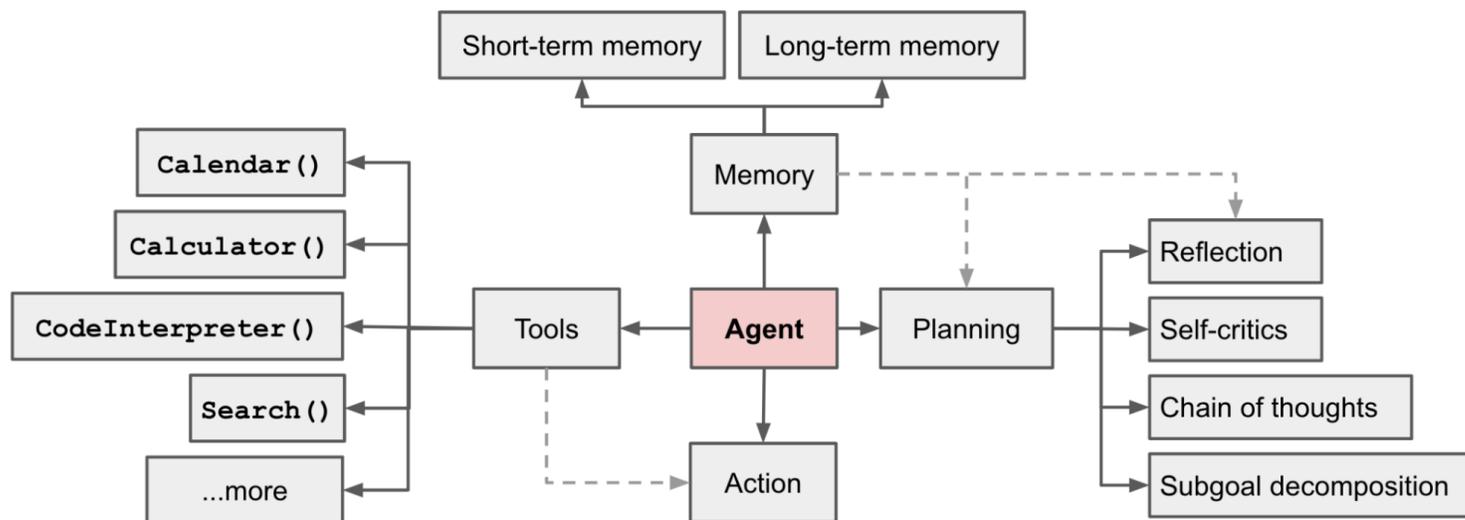


基因突变分析



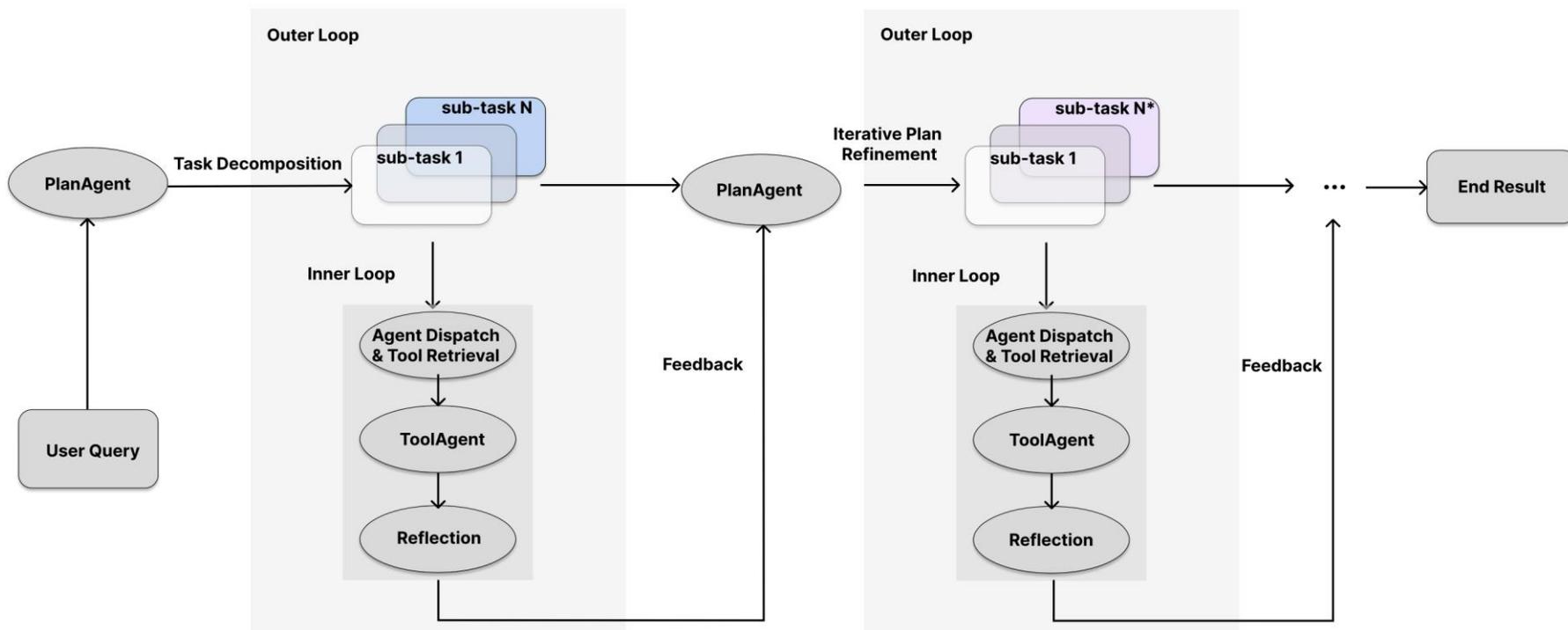
专业教育：工具智能

- 在大模型出现后，因大模型所展示出的通用智能，大模型智能体成为了新范式
- 大模型智能体指一个使用大模型驱动可以**观察周遭环境**并**利用工具**作出行动以**达成目标的自主实体**



专业教育：工具智能

- XAgent: 提出 **内循环+外循环“双循环机制”**，外循环处理任务的高级管理和分配，内循环专注每个子任务的低级执行和优化，实现对复杂任务进行**自主任务拆解**，进而**组合使用多种工具**

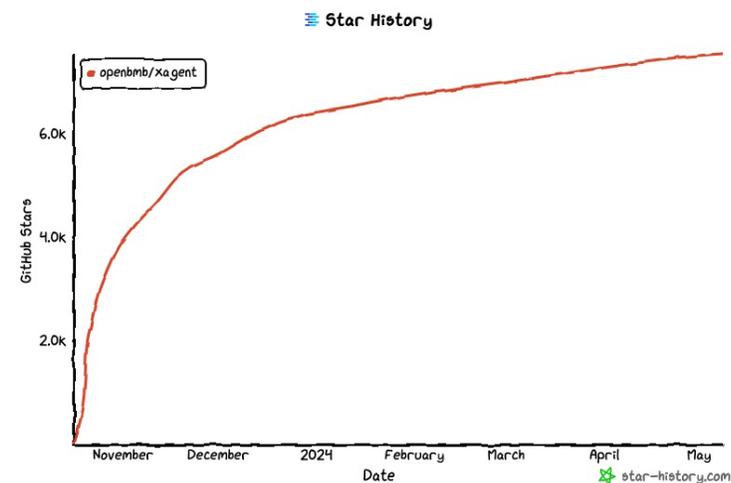
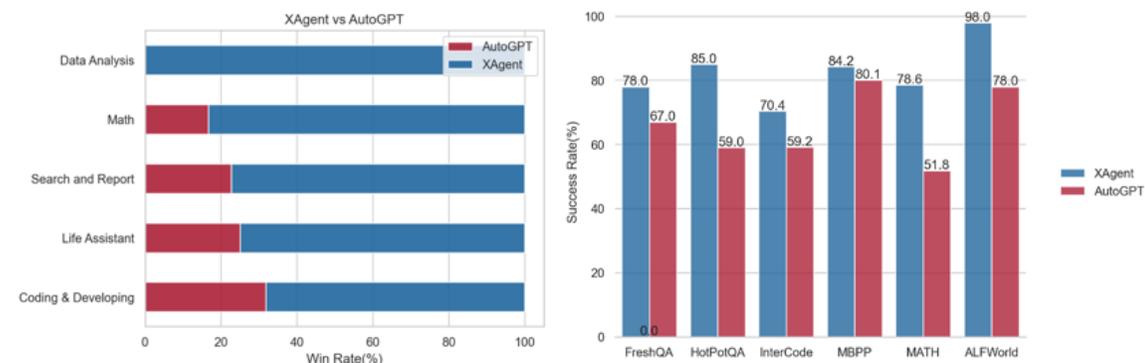


专业教育：工具智能

- 各类测试表明，XAgent在5大类真实复杂任务场景上的处理能力**全面超越AutoGPT**
- 2023年10月发布以来，登顶GitHub Trending榜首，已获GitHub **7500+**星标关注

Conversations Shared by Our Community

<p>XAgent / auto</p> <p>Find the positions of Mars, Venus, and Jupiter in the sky on December ...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>Develop a web application that allows users to upload and share music...</p> <p>by: yesai</p>	<p>XAgent / auto</p> <p>I will have five friends coming to visit me this weekend, please find an...</p> <p>by: yesai</p>	<p>XAgent / auto</p> <p>Can you help me to use python to analyze the given data?</p> <p>by: yesai</p>
<p>XAgent / auto</p> <p>Develop a web application that allows users to upload and share music...</p> <p>by: yesai</p>	<p>XAgent / auto</p> <p>Find the positions of Mars, Venus, and Jupiter in the sky on December ...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>I want to play game of 24, which use +, -, *, / to get 24 using 4 number...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>I'm planning a surprise birthday party for my best friend. Can you help...</p> <p>by: Yuja Qin</p>
<p>XAgent / auto</p> <p>Analyze a series-parallel circuit that has two 10 Ohm resistors in series...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>Design a solenoid using copper wire that can produce a magnetic field ...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>Please assist me in compiling a list of top 10 universities globally for a ...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>You're given a matrix: $\begin{bmatrix} 3 & 7 & 2 \\ 1 & 8 & 5 \\ 6 & 1 & 4 \end{bmatrix}$ Compute its determinant.</p> <p>by: Yuja Qin</p>
<p>XAgent / auto</p> <p>If a digital clock reads 3:15, calculate the angle between the minute and...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>I'm looking for a reliable car mechanic, can you recommend one with g...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>Find and recommend some restaurants for 8 people around, I prefer sw...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>For a simple random walk on the integers, starting at 0, prove that wit...</p> <p>by: Yuja Qin</p>
<p>XAgent / auto</p> <p>Given a positive integer n, prove that there are infinitely many prime nu...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>I want to play game of 24, which use +, -, *, / to get 24 using 4 number...</p> <p>by: Yuja Qin</p>	<p>XAgent / auto</p> <p>Can you help me compile a list of the top 10 most influential books in t...</p> <p>by: Yuja Qin</p>	



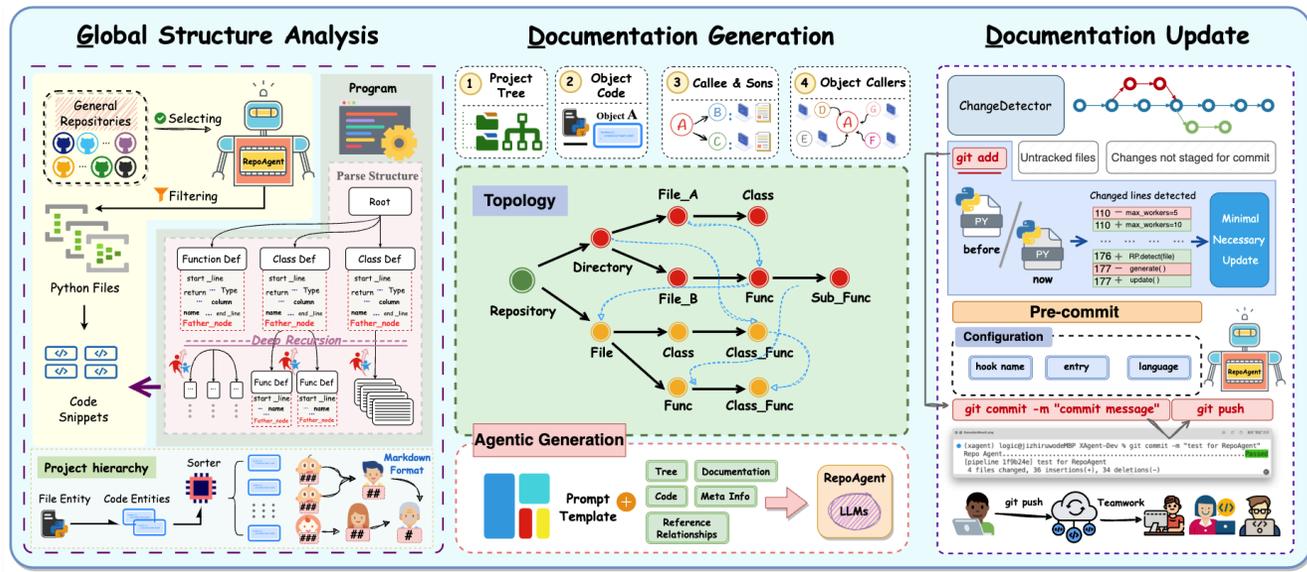
专业教育：工具智能

- RepoAgent: 面向项目级代码文档生成的自主智能体
- 利用**AST工具**分析代码结构，准确识别**代码对象调用关系**，丰富文档内容的全局视角，实现对代码的全局性细粒度的理解，帮助大模型生成详细代码文档

全局结构解析

代码文档生成

代码文档更新



实现功能:

- 自动检测Git仓库变化，追踪文件的添加、删除和修改
- 独立通过AST分析代码结构，为各个对象生成文档
- 准确识别对象间调用关系，丰富文档内容的全局视角
- 自动无缝更新代码文档内容，保持文档的一致性
- 执行多线程并发操作，提高文档生成的效率

专业教育：工具智能

- 结合全局代码结构分析能力，可以显著提升大模型项目级代码理解能力

```
FunctionDef chat(self, message, history, flow_config):  
  
Function chat: The function of chat is to process a given message within a chat environment, execute a workflow based on the message content and flow configuration, and return a response message with metadata including the history of messages, execution time, and modified files.  
  
Parameters:  


- message: An instance of Message containing the content and metadata of the incoming message.
- history: A list that keeps track of the conversation history.
- flow_config: An optional instance of AgentWorkflowConfig that defines the workflow configuration. If not provided, a default configuration is used.
- kwargs: A variable number of keyword arguments that can be used to pass additional information. Specifically, work_dir can be provided to specify the working directory.

  
Code Description:  


- The function starts by retrieving the work_dir from kwargs or setting it to None if not provided.
- It then constructs a scratch_dir path by joining work_dir with the subdirectory "scratch".
- If flow_config is not provided, the function calls get_default_agent_config with scratch_dir to obtain a default configuration.
- An instance of AutoGenWorkflowManager is created with the provided or default flow_config, the conversation history, and the scratch_dir.
- The message content is stripped of leading and trailing whitespace and passed to the flow.run method, which executes the workflow.
- The metadata dictionary is initialized and populated with the flow.agent_history.
- Depending on the summary_method specified in flow_config, the function processes the history to generate an output message. It supports three methods:
  - "last": Concatenates the last message content with any successful code blocks extracted from the history.
  - "llm": Currently, this method results in an empty output string.
  - "none": Also results in an empty output string.
- The function calculates the execution time and stores it in metadata.
- It calls get_modified_files to retrieve any files modified during the workflow execution and adds this information to metadata.
- The number of modified files is printed to the console.
- Finally, a new Message instance is created with the output content and metadata, and this message is returned.

  
Note:  


- The Message class and other functions such as get_default_agent_config, extract_successful_code_blocks, and get_modified_files are not defined within this code snippet. They are assumed to be part of the larger project and should be implemented elsewhere.
- The flow_config.summary_method should be properly set to one of the supported methods ("last", "llm", or "none") to ensure the expected behavior.
- The work_dir should be a valid directory path if provided, as it is used for file operations.
- The function assumes that the scratch_dir is a valid directory within work_dir and that it has the necessary permissions for file operations.

  
Output Example:  


```
output_message = Message(
 user_id="user123",
 root_msg_id="root456",
 role="assistant",
 content="Here is the response to your query...",
 metadata={'messages': [...], 'time': 2.34, 'files': ['file1.txt', 'file2.txt']},
 session_id="session789",
)
```

  
This example shows a possible appearance of the Message object returned by the chat function, containing the user ID, root message ID, role, content of the response, metadata in JSON format, and the session ID.
```

功能总结

参数描述

代码描述

注意事项

提供示例

Human Evaluation:

总数: 150

Ours: 105

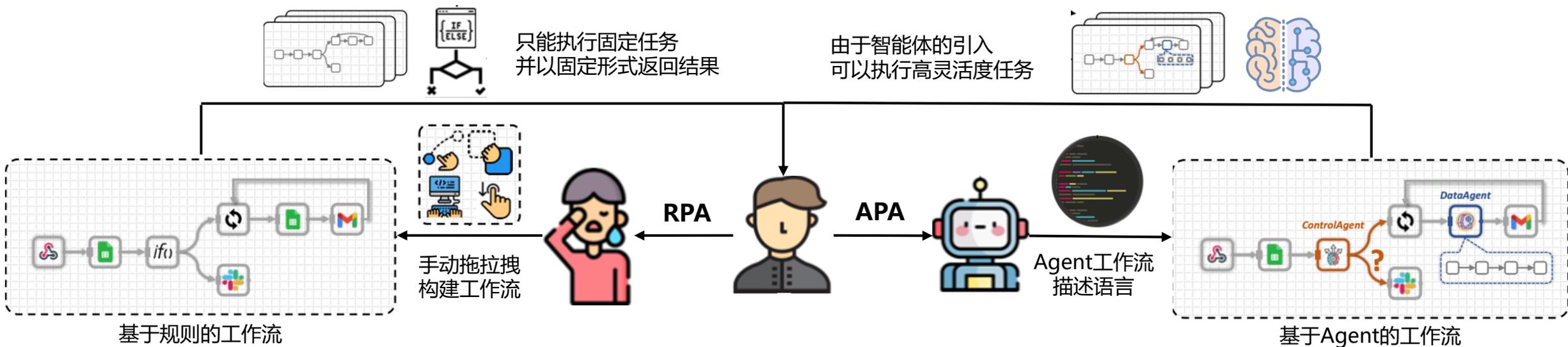
transformers人类文档: 45

ours 胜率: 0.70

生成文档质量评估

专业教育： workflows 与 流程自动化

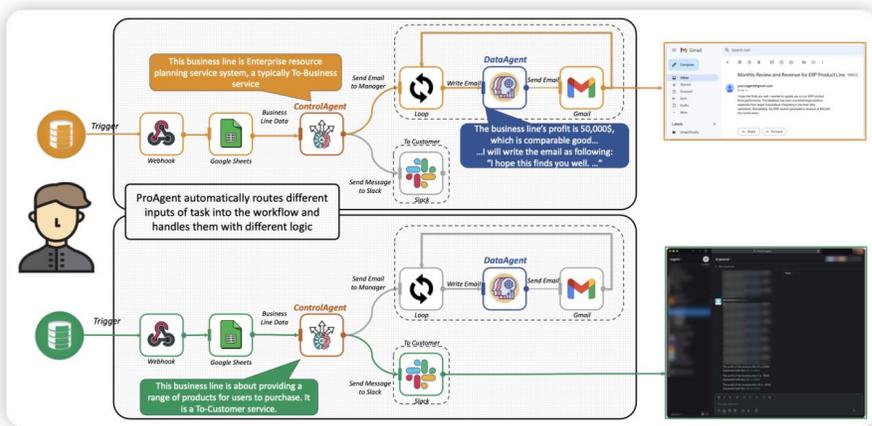
流程自动化技术让智能体掌握 workflows， 高效执行复杂多步骤任务



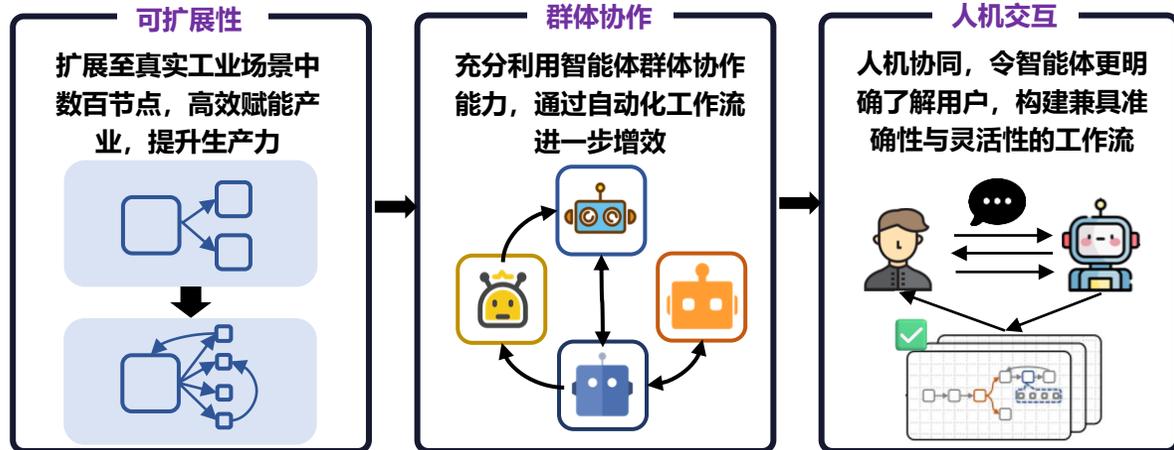
科研成果

智能体根据人类需求 **自动构建 workflows**， 实现机械任务自动化， 同时将智能体编入 workflows 中进行 **动态决策**

☆ 668



未来趋势



专业教育： workflows与流程自动化

- workflows存在**手工构建耗费人力、 workflow动态性不足、 任务经验无法重用**等挑战

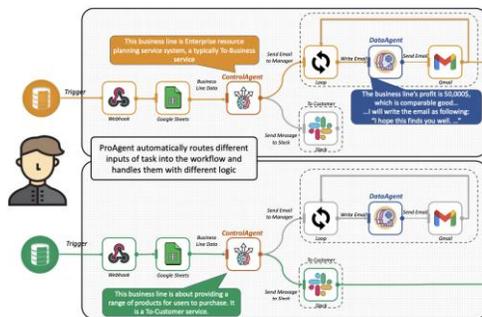
手工构建耗费人力

构建 workflow 往往需求特定专家知识和大量人力物力，存在自动化不足的瓶颈，效率难以提升



workflow动态性不足

静态的 workflow 无法根据任务特性智能动态地扩展执行流程，缺乏灵活性和适应性



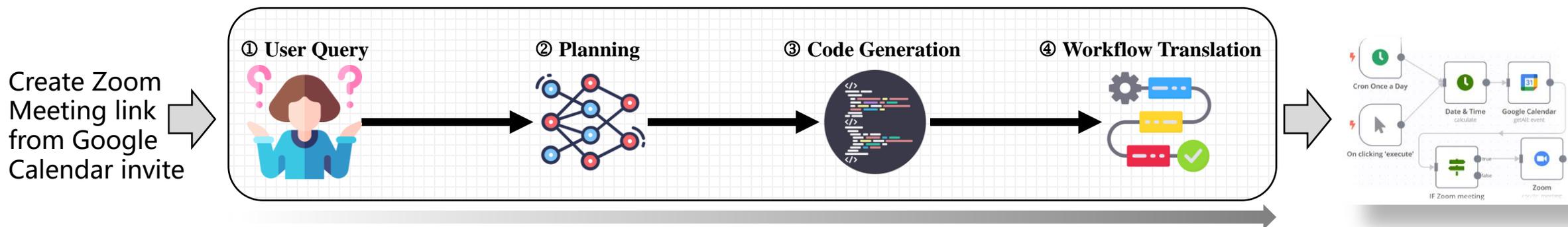
任务经验无法重用

智能体执行任务的轨迹蕴含了过去的成功经验，有效地利用这些知识可以帮助智能体不断进化



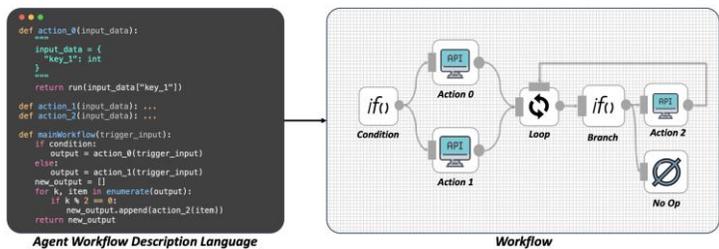
| 专业教育： workflows与流程自动化

- **Robotic Process Automation (RPA)**: 人手工构建Workflow实现对机械任务的自动化, 但依赖专家知识和耗费人力, 并且无法处理需要动态决策的任务
- **Agentic Process Automation (APA)**: 让Agent根据人类需要**自动构建 workflow**, 同时将Agent编入workflow中进行**动态决策**

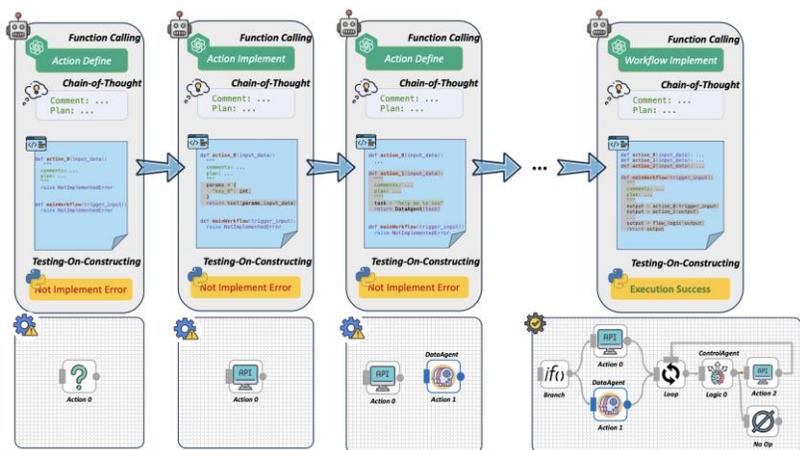


专业教育：工作流与流程自动化

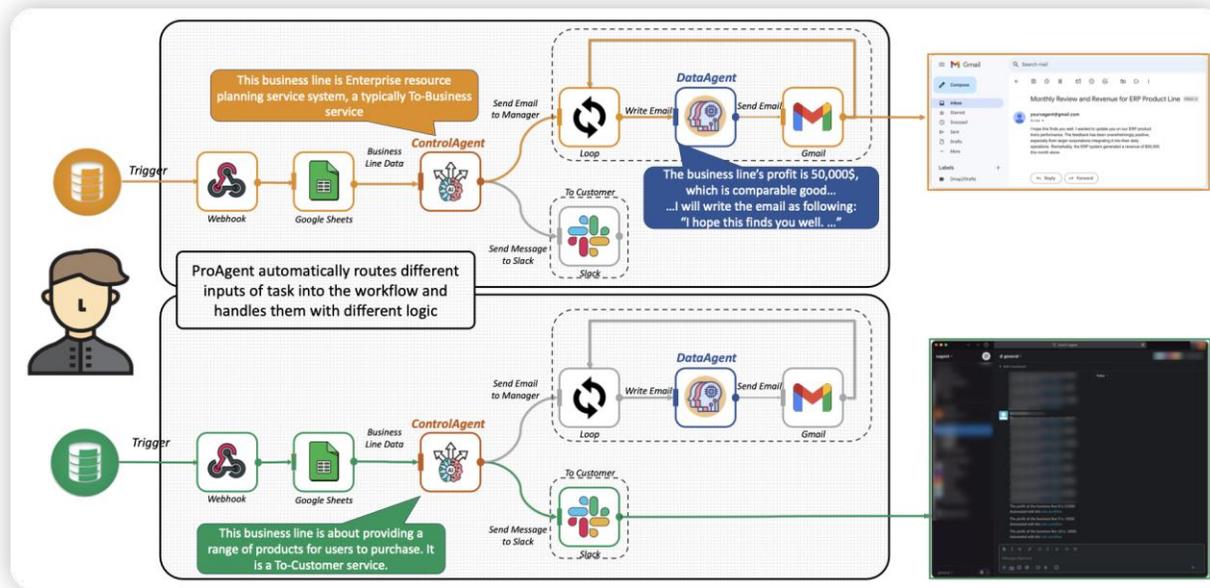
- 基于n8n workflow框架，实现了不同APP的执行引擎
- 使用Python-style的代码，实现了workflow的流程定义与控制



智能体工作流描述语言



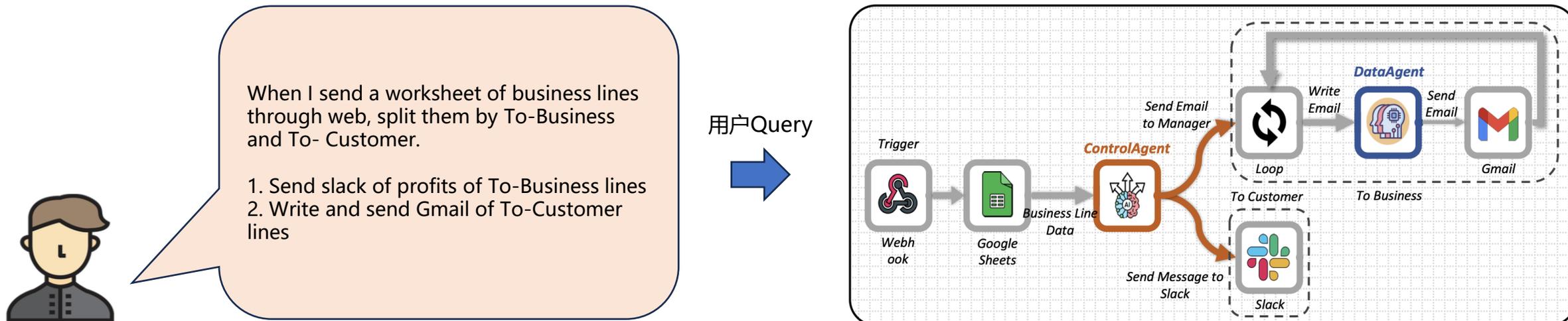
智能体自动创建工作流



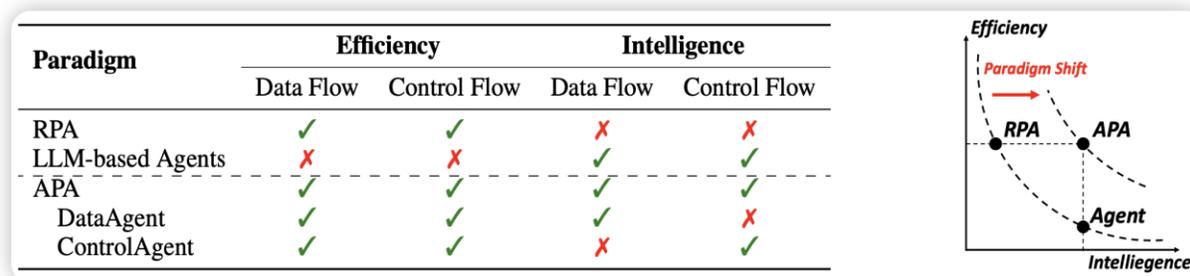
DataAgent实现对数据的复杂处理，ControlAgent实现动态选择执行逻辑

专业教育： workflows与流程自动化

- 案例展示——编排流程实现自动数据处理并发送邮件



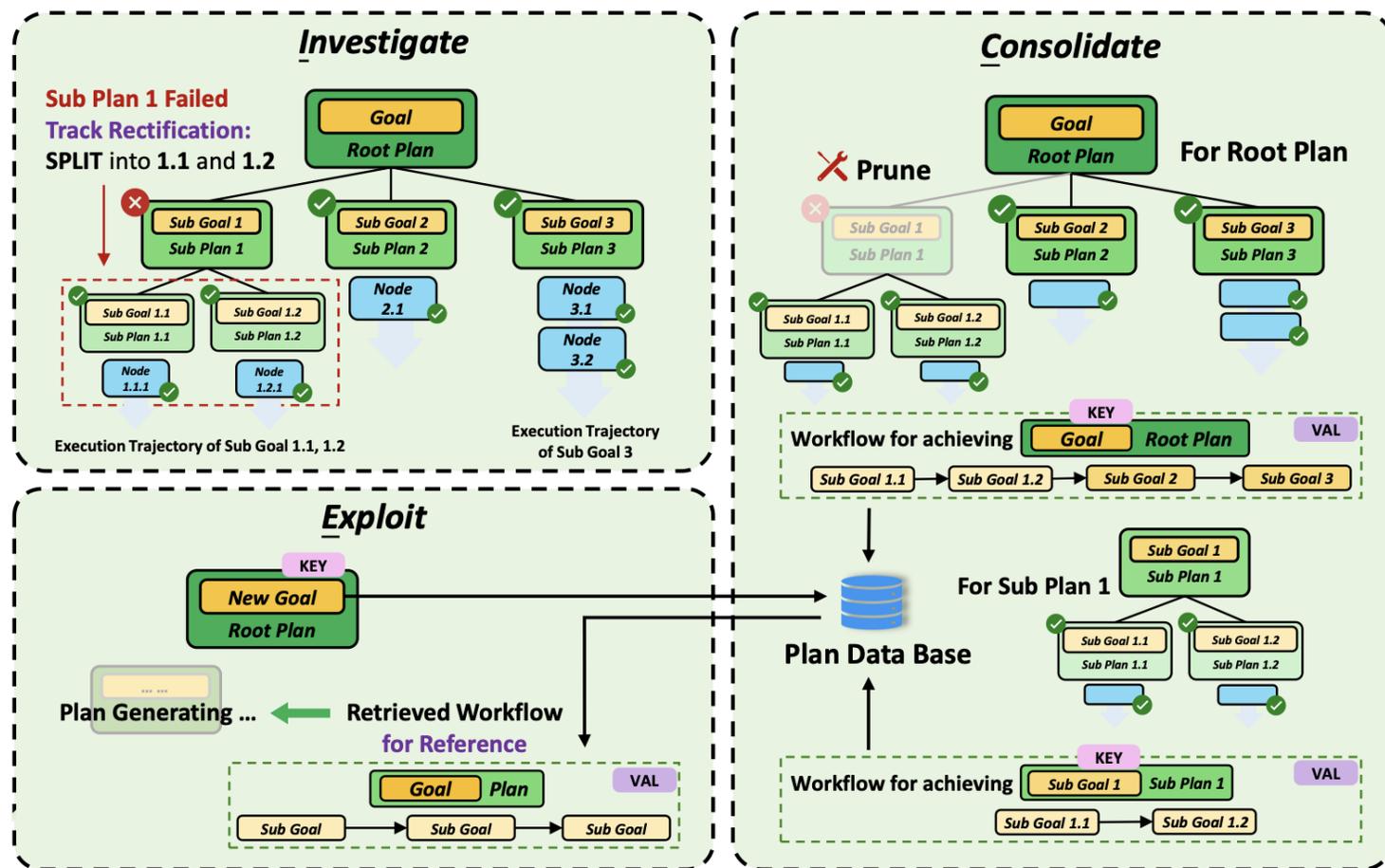
- ProAgent实现了流程的自动编排和动态执行，相比传统RPA具有更高的效率和更强的智能



专业教育：工作流与流程自动化

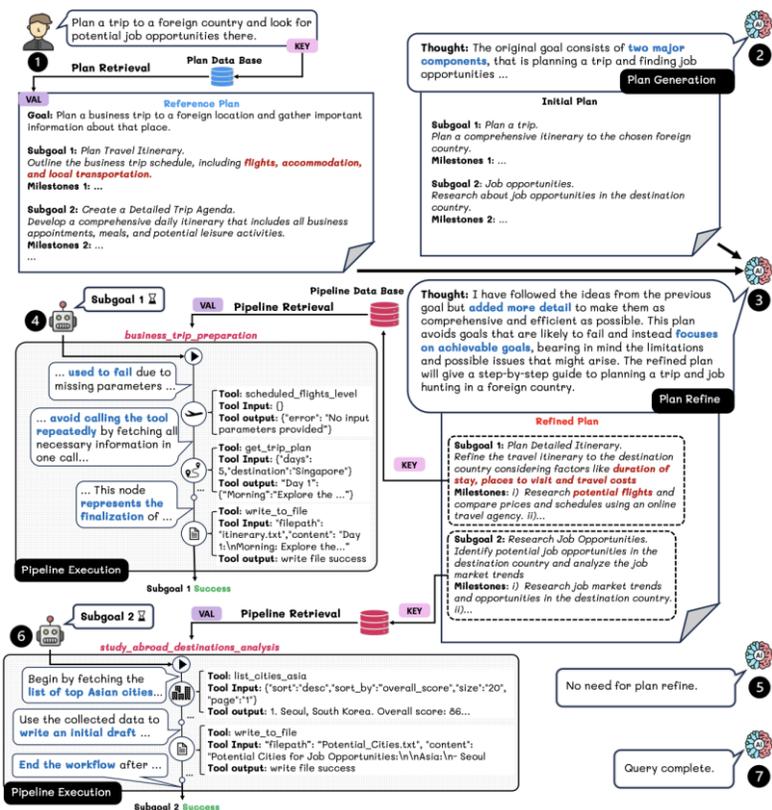
ICE框架：通过传递任务间的成功经验实现智能体的自我演化增强

- **Investigate**：识别值得学习和参考的经验，提取所有成功执行轨迹
- **Consolidate**：巩固经验并存储为标准化的格式，以便于未来的经验重用
- **Exploit**：利用巩固的经验来提高新任务的效率和效果



专业教育：工作流与流程自动化

- 通过将固化的经验进行检索重用，智能体有效地从过去的经验中获取知识
- ICE实现了较高经验重用率，减少API调用次数，提升任务性能



ICE Strategy	Model	API Calls (All)	API Calls (Tools)	Completion Rate (Subtasks, %)	Rectifications Times	Re-utilization Rate
Standard (w/o ICE)	GPT-4	3025	807	82.18	45	-
	GPT-3.5	4535	901	37.21	275	-
Planning ICE	GPT-4	2073	628	89.55	39	-
	GPT-4	456	317	93.10	-	53.52
Planning + Execution	GPT-4	495	313	90.32	6	47.89
	GPT-3.5	401	257	90.74	5	53.52

同分布任务执行效果

ICE Strategy	Model	API Calls (All)	API Calls (Tools)	Completion Rate (Subtasks, %)	Rectifications Times	Re-utilization Rate
Standard (w/o ICE)	GPT-4	2265	745	72.97	107	-
	GPT-3.5	4071	880	25.33	234	-
Planning ICE	GPT-4	1779	532	86.36	35	-
	GPT-4	443	318	94.44	-	39.44
Planning + Execution	GPT-4	540	384	90.00	6	47.89
	GPT-3.5	610	258	86.96	6	35.21

相似分布任务执行效果

3

迎接智能的第二次涌现

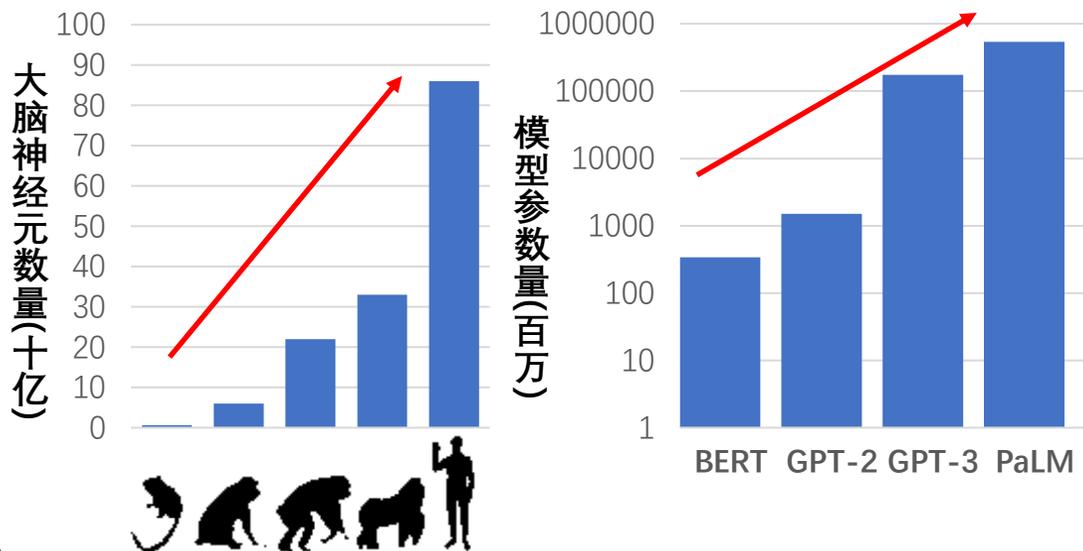
群体智能：智能的第二次涌现

个体智能涌现

神经元数量增加带来生物个体的智能涌现



参数增加带来单个大模型的智能涌现

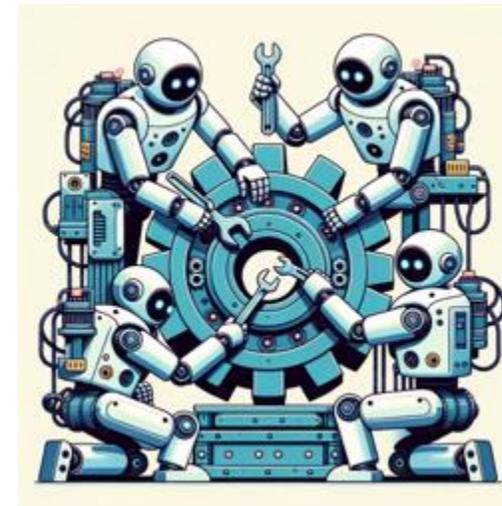
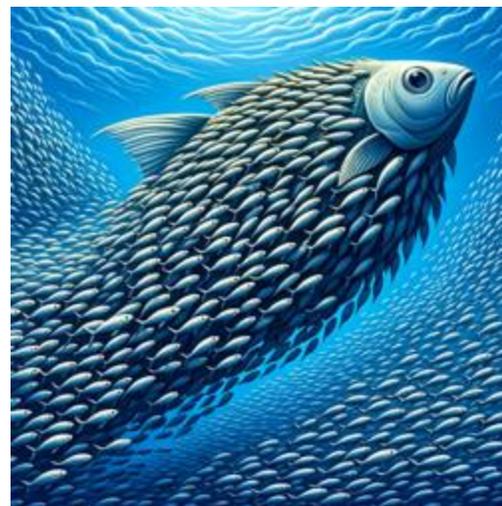


群体智能涌现

生物体群聚带来生物群体智能涌现



AI群聚带来AI群体智能涌现



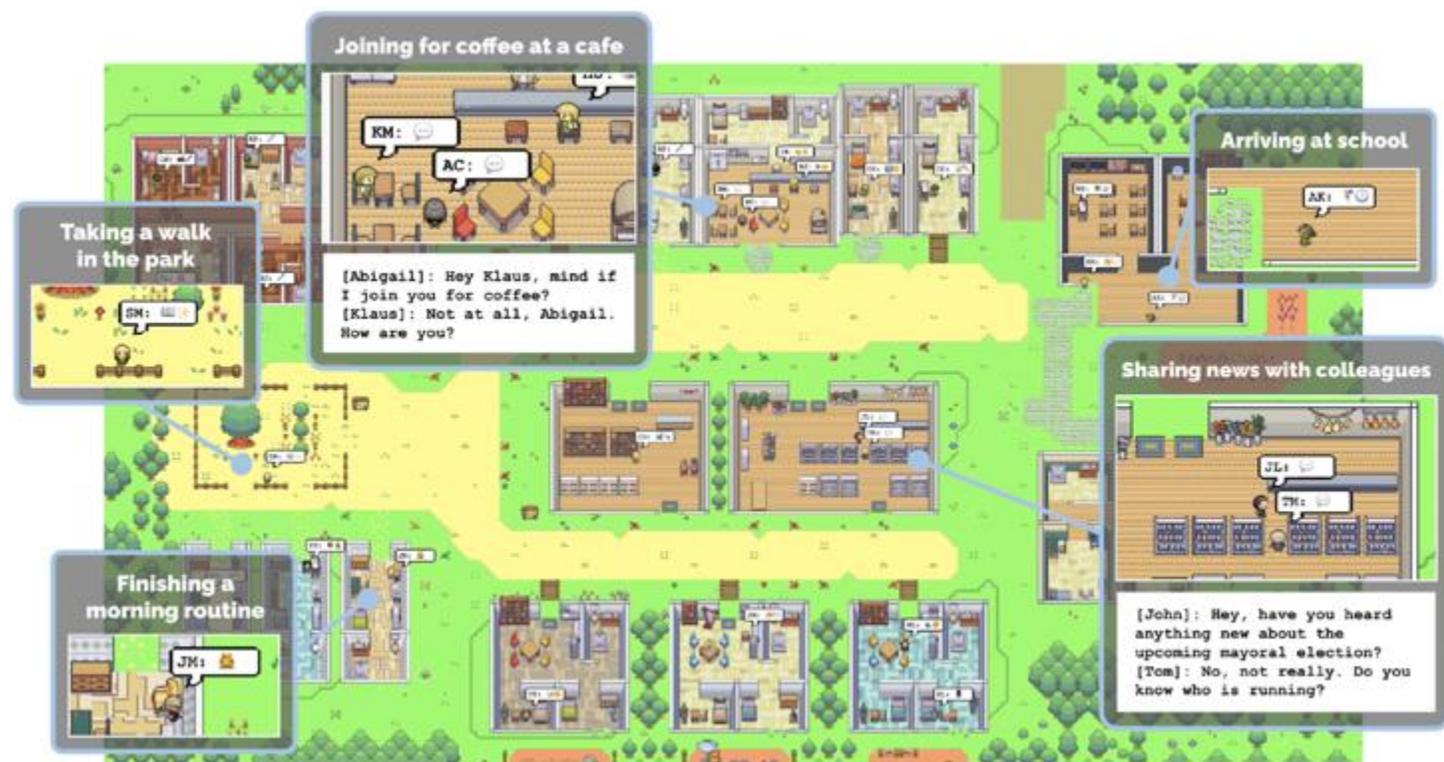
| 群体智能：自主语言交互的群体协作新范式

- **语言交互**搭建沟通桥梁，通过任务分工和协作执行**处理复杂任务**
- **集体协作**实现**多方优势互补**、配合无间，有效提高解决问题的准确率
- 群体智能与语言交互相得益彰，智能体合作实现各异其韵，协作其歌



群体智能：智能时代协同创新引擎

- 群体智能：划分为**社会模拟型**与**任务完成型**两类形式
- 实现“人类-环境-机器”无缝链接，孕育并引领**下一代人机协作范式**



社会模拟型

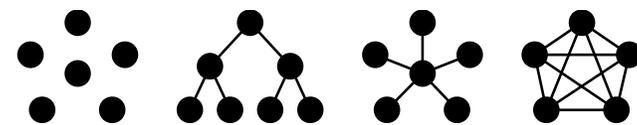
斯坦福的SmallVille小镇：基于层次规划的智能体社会小镇，实现人类社群行为的可信模拟



任务完成型

清华NLP的ChatDev数字团队：基于语言交互的智能体软件开发，实现群体交互协作式任务完成

群体智能：核心要素

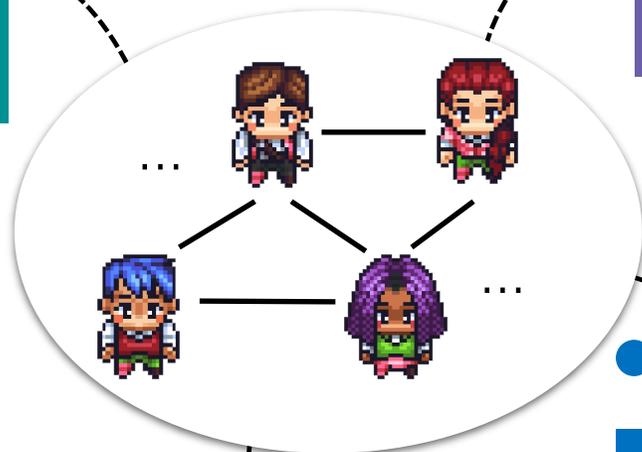


- 无目标导向型：群体自由规划及行为执行 (e.g., 社会模拟)
- 目标导向型：制定群体特定目标以协同进行任务完成 (e.g., 软件开发)

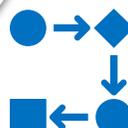
任务目标



组织结构



行为路由



社会关系



- 联盟结构：独立结构、层次化结构、中心化结构、全连接结构
- 组织规模：小规模、中规模、大规模



- 顺序型：各子组织间依次行动
- 互斥型：各子组织间选择性行动
- 并发型：各子组织间并行行动

- 行为关系：合作关系、竞争关系
- 组织行为：激励行为、团队凝聚力、劳动力多元化、资源竞争、同龄人压力、群体懈怠、评价焦虑、情绪感染等

群体智能：核心挑战

- 群体智能面临着设计有效**任务目标**、**交互协议**、**组织结构**、**成长演化**等挑战

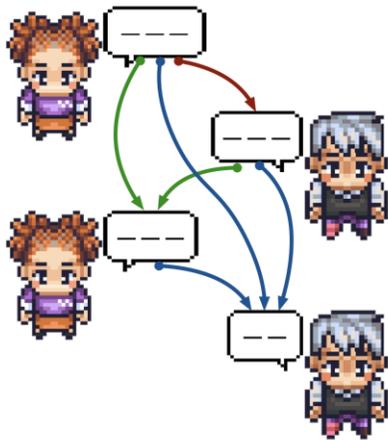
任务目标

多智能体协同决策的难点在于处理复杂的交互依赖，同时保证系统的通用性和可靠性



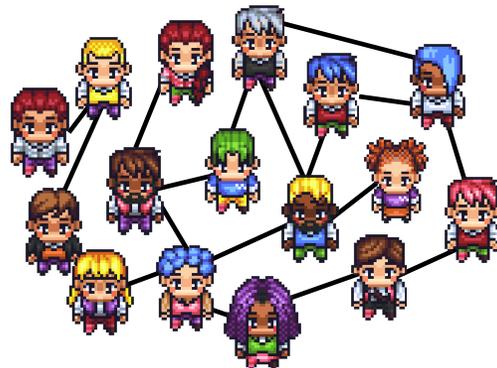
交互协议

难点在于设计有效的交互形式，以确保在多样化的团队成员实现高效的沟通、协调和决策



组织结构

难点在于构建灵活且高效的组织结构和行为路由策略，以驱动角色高效地协同完成最终目标



成长演化

难点在于设计多智能体协同的历史经验，还要具备经验的持续学习、适应和自我优化的能力



如何构建灵活易用的高可扩展群体智能平台？

- 灵活易用、高可扩展的群体智能平台，支持利用基础模型定制多智能体环境，创建多个具有不同能力与身份的智能体

The screenshot displays a complex multi-agent simulation environment. On the left, a 2D top-down view shows a town with buildings, trees, and several small agent characters. Overlaid on this are several utility panels: a 'Monitoring Dashboard' showing system metrics like CPU usage (2.1 day, 7.50 GiB), memory usage, and system load; a 'Code Editor' with Python code for a 'separate_paren_groups' function; and a 'Chat' window showing a dialogue between a police officer and two suspects. The bottom of the screen features a control bar with 'Reset', 'Next', 'Stop Autoplay', and 'Start Autoplay' buttons.



囚徒困境



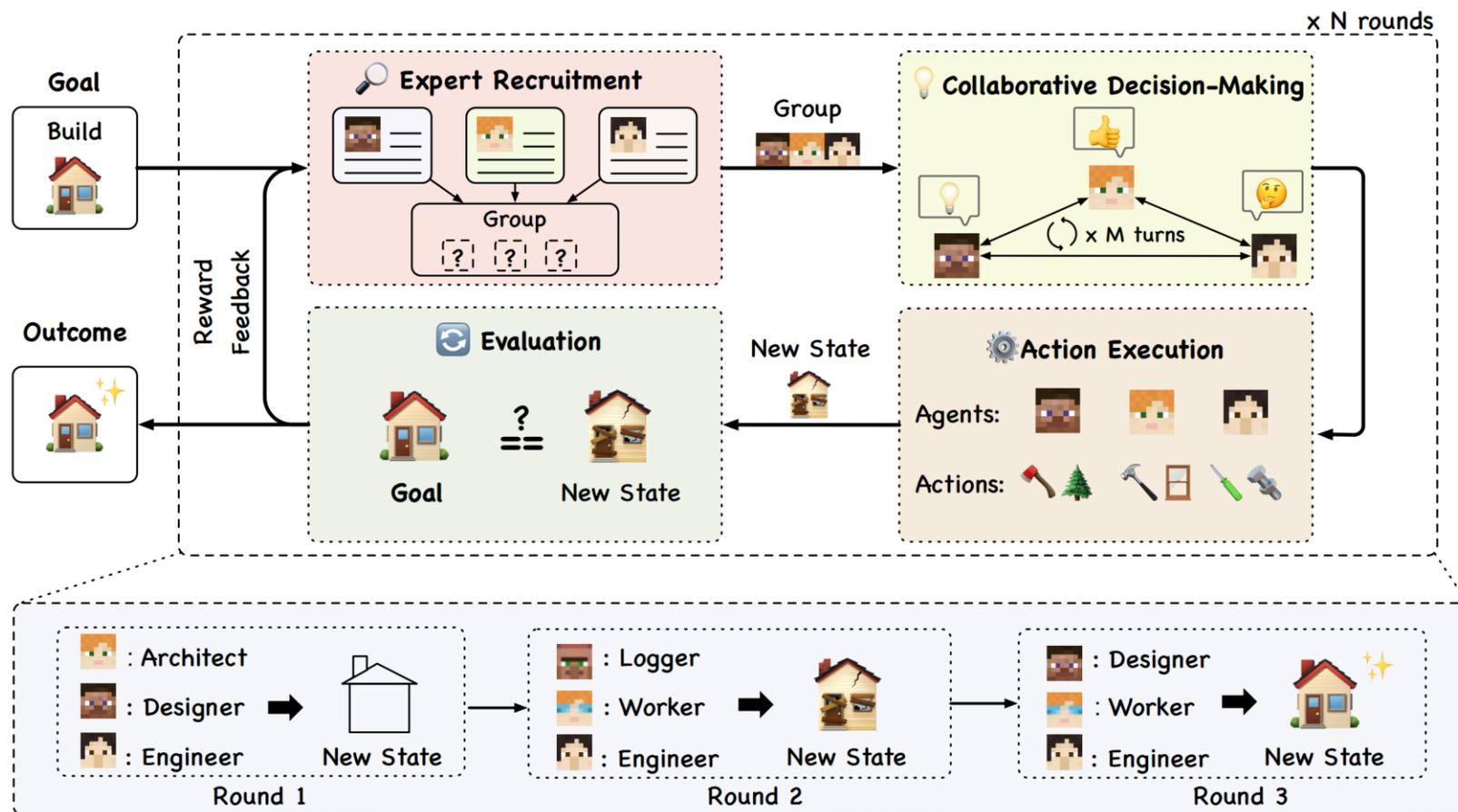
数据库管理



文本评估

AgentVerse: 灵活易用的高可扩展群体智能平台

- 在智能体空间中进行角色选择和目标分配，促进智能体有效**信息交互**和**知识交换**
- 通过**专家招募**、**协作决策**、**行动执行**、**方案评估**来模拟真实团队协同决策过程



AgentVerse: 灵活易用的高可扩展群体智能平台

- 不论采用何种GPT基座模型，群体决策的质量高于单个个体
- **涌现行为**: 自愿行为、服从行为、破坏行为

Setting	GPT-3.5-Turbo	GPT-4
CoT	73.8	83.5
Solo	74.4	87.2
Group	75.6	89.0

Agents: 🐱: Bella 🐼: Charlie Tools: 🔍 Bing Search API 🌐 Web Browser 💻 Code Interpreter

🔍 Query: Recently, it has become popular to verify the mathematical reasoning abilities of LLMs by observing if they can solve the "24-Point Game." **What is this game?** Does it have a code-based solution? If it does, **provide a Python code along with test cases and test its functionality.** What are some **other similar games** that can be used to test the models' mathematical reasoning abilities?

Round 0

Decision-Making

- 🐱: 🔍 Research the game and identify similar games
- 🐼: 🛠️ Develop and test the Python code for solving the game

Execution

<ul style="list-style-type: none">1. 🐼: What is 24-point game?2. 🌐: Browse the 1st website3. ✅: Submit the rules	<ul style="list-style-type: none">1. 🐼: Rule of 24-point game?2. 🌐: Browse the 1st website3. ✅: Write code + test cases
--	---

Evaluation

❌ Bella does not provide similar games

Round 1

Decision-Making

- 🐼: 🔍 Find similar mathematical reasoning games
- 🐼: 🛠️ Test the code with more cases

Execution

<ul style="list-style-type: none">1. 🐼: 24-point similar games?2. 🌐: Browse the 1st website3. 🌐: Browse the 2nd website4. 🐼: "Make a Number" Rule?	<ul style="list-style-type: none">1. 💻: More test case and test2. ✅: Submit the result
---	---

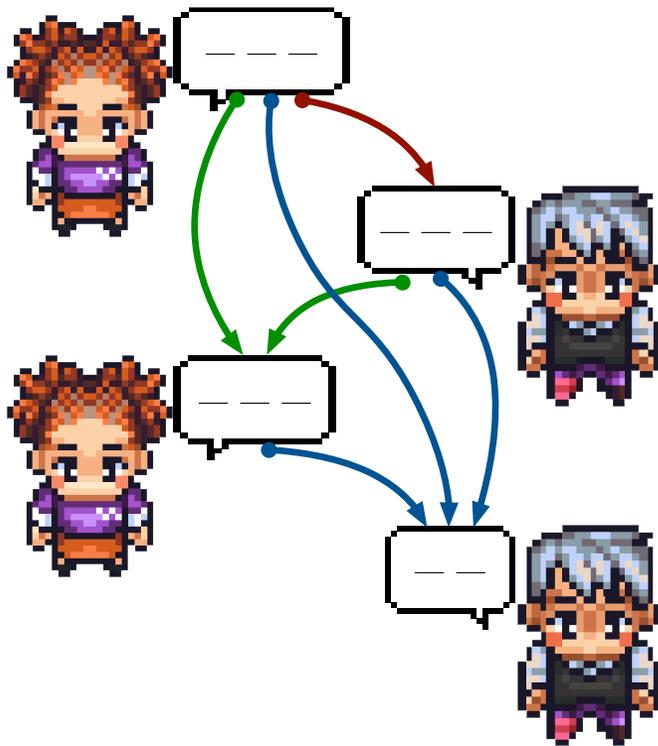
Evaluation

👍 (rules) 24-point game is ... (code) A Python code is written ... (similar games) Similar games include "Make a Number"...



| 如何挖掘多智能体间的高效交互形式?

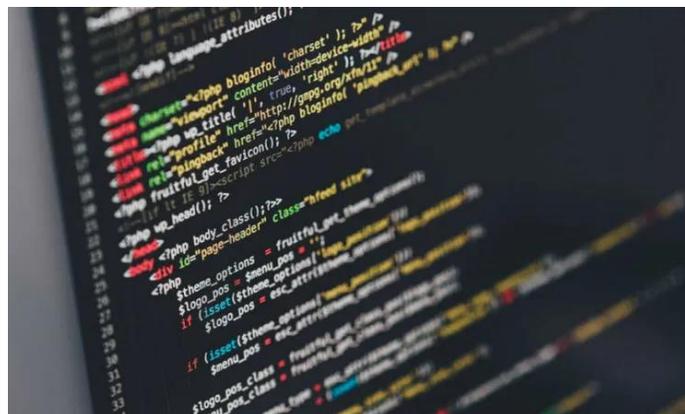
- **高效交互形式**的挖掘依赖于多智能体间的通信机制、决策同步和协作策略，通过模拟实验优化交互协议，保证高效稳定的协作



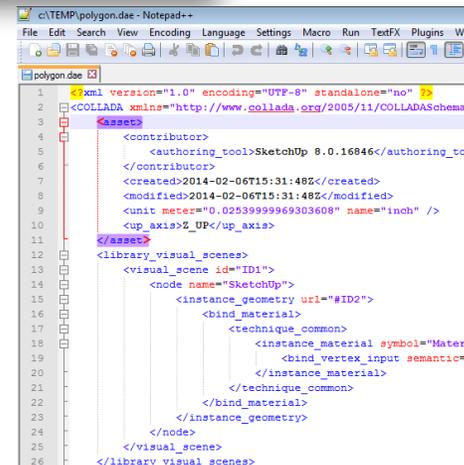
自然语言



Markdown



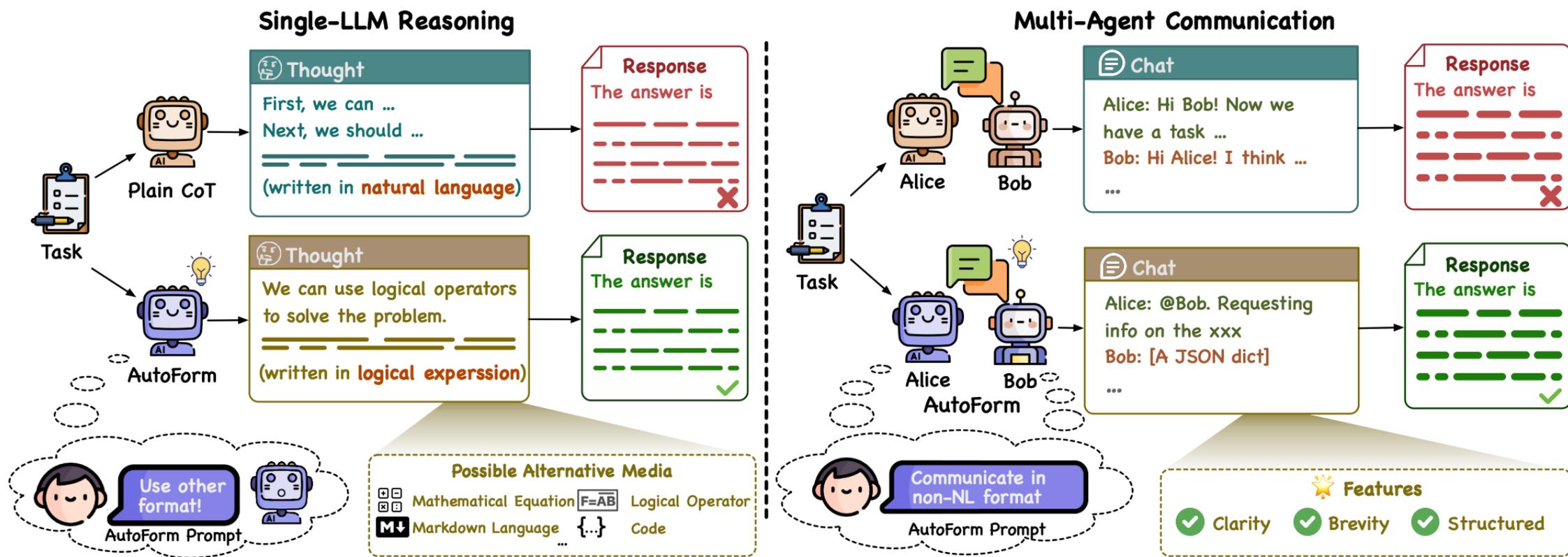
编程语言



Json

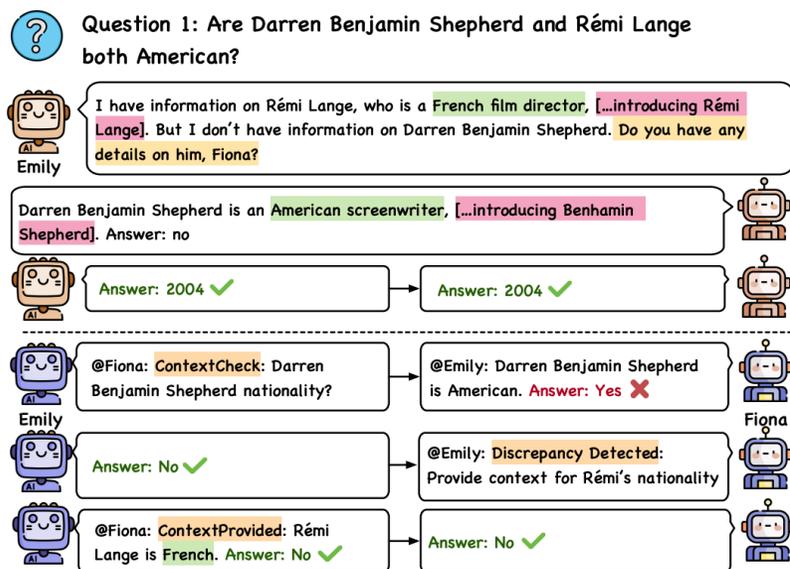
AutoForm: 非自然语言形式提升沟通效率

- 通过**形式空间搜索**，实现Agent根据任务选择**结构化**的语言格式，提升单体的**推断准确率**和群体的**交流效率**

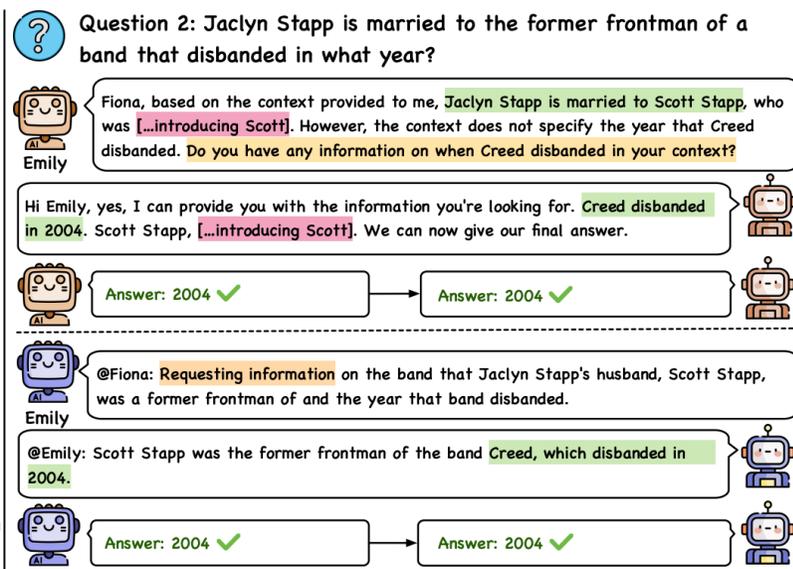


AutoForm: 非自然语言形式提升沟通效率

- 多智能体之间可以使用**非自然语言**的形式进行沟通，同时在组成结构上与传统Agent语言有相似之处，但进行了**显著的精简**



(a) Clarity and Structured



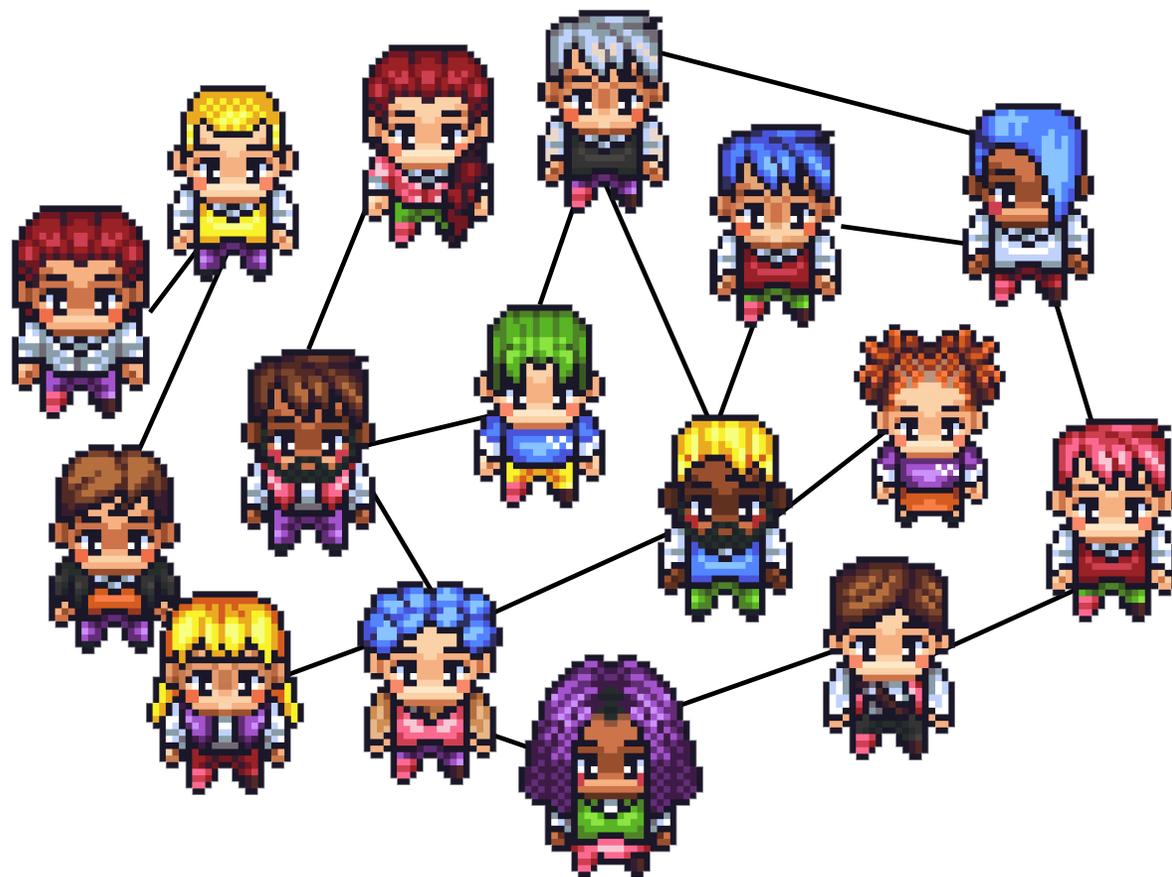
(b) Brevity and Efficiency

Format	Hotpot QA		Multi Wiki		Narrative QA	
	RougeL	#Tokens	RougeL	#Tokens	RougeL	#Tokens
KQML	0.76	313.8	0.53	368.1	0.28	343.3
JSON	0.71	346.0	0.53	291.4	0.22	385.2
AutoForm	0.76	115.0	0.52	146.2	0.43	141.7

(ask-one
:sender joe
:content (PRICE IBM ?price)
:receiver stock-server
:reply-with ibm-stock
:language LPROLOG
:ontology NYSE-TICKS)

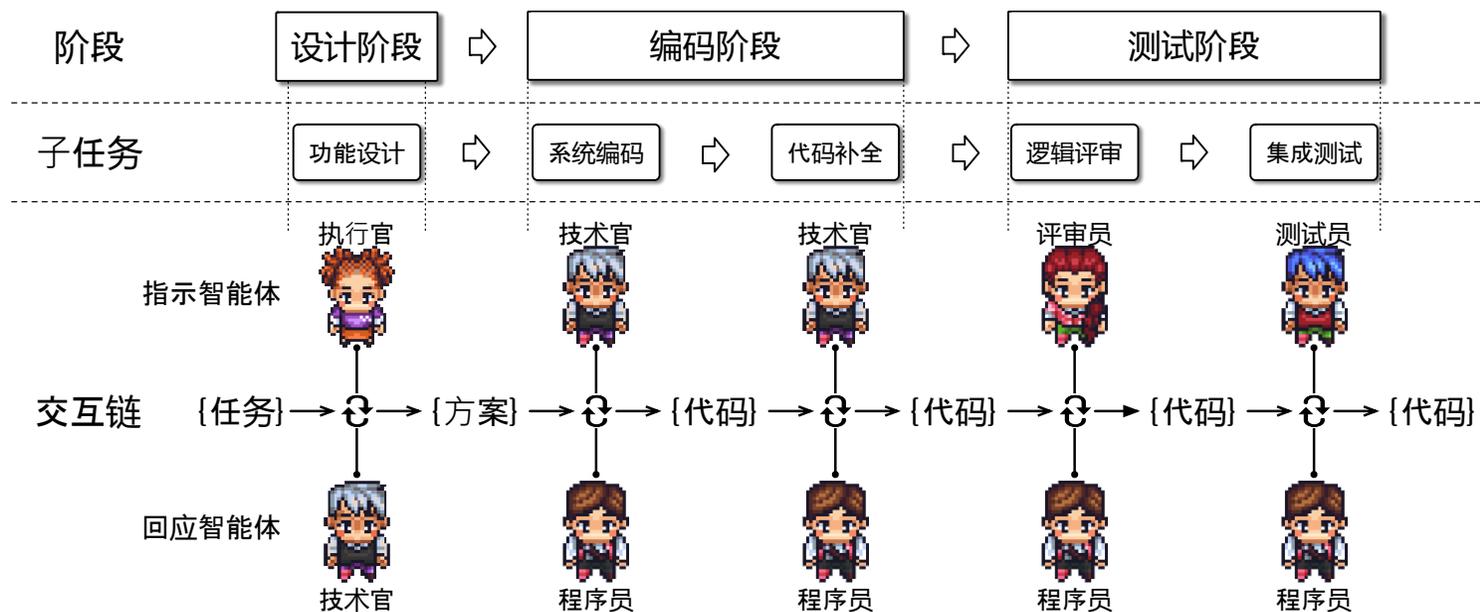
| 如何组织管理多智能体使其高效完成任务？

- 为高效协同完成特定任务，需设计智能体的角色和责任，通过实现**任务分配**和**行为路由**策略，确保多智能体在复杂环境中稳定高效交互运作



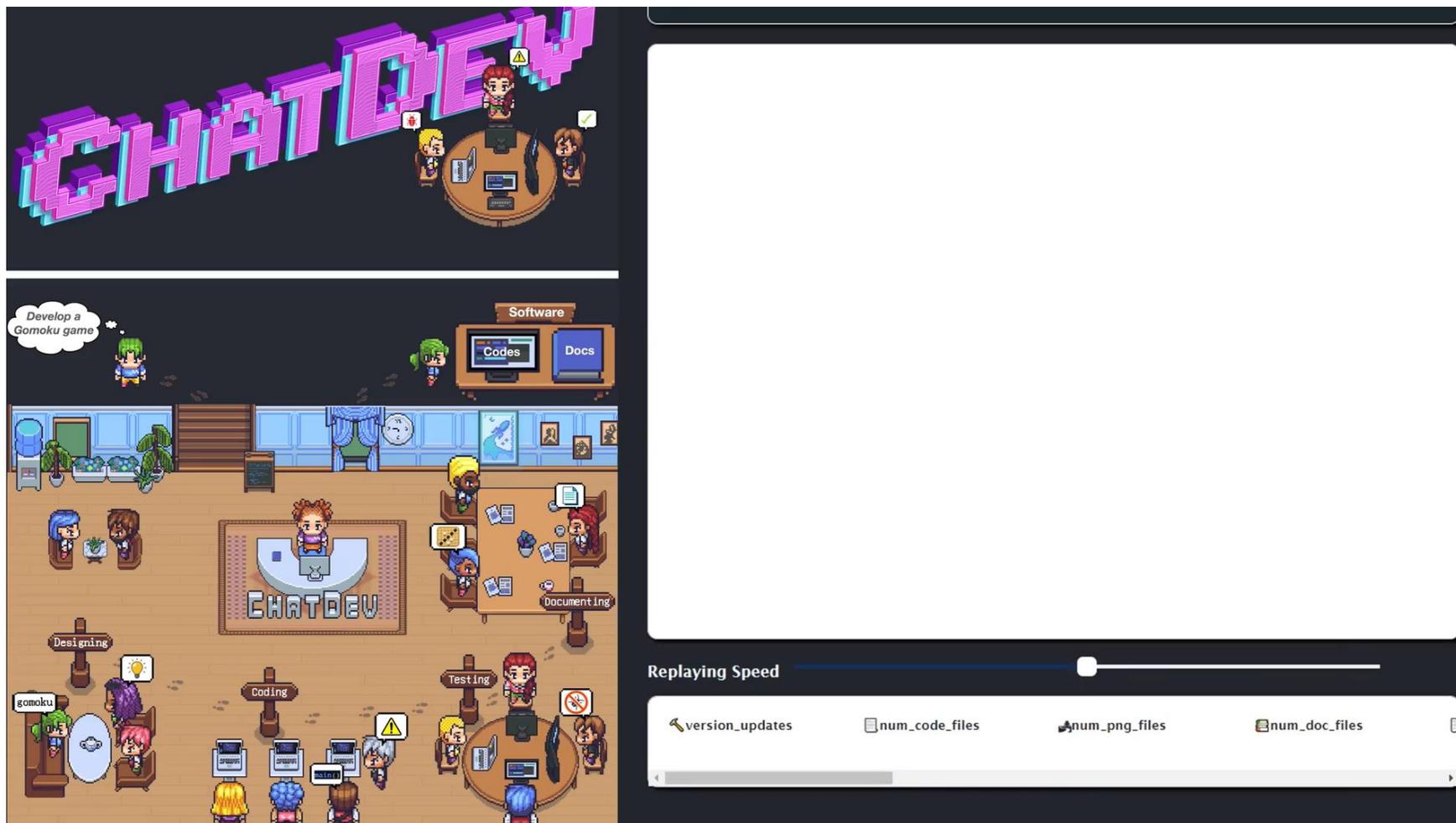
ChatDev: 多智能体协作式软件开发

- 通过**角色扮演**交流实现智能体间的**方案提议**和**决策研讨**过程
- 通过**交流链**将软件开发分解为由原子任务组成的“**软件生产线**”



| ChatDev: 多智能体协作式软件开发

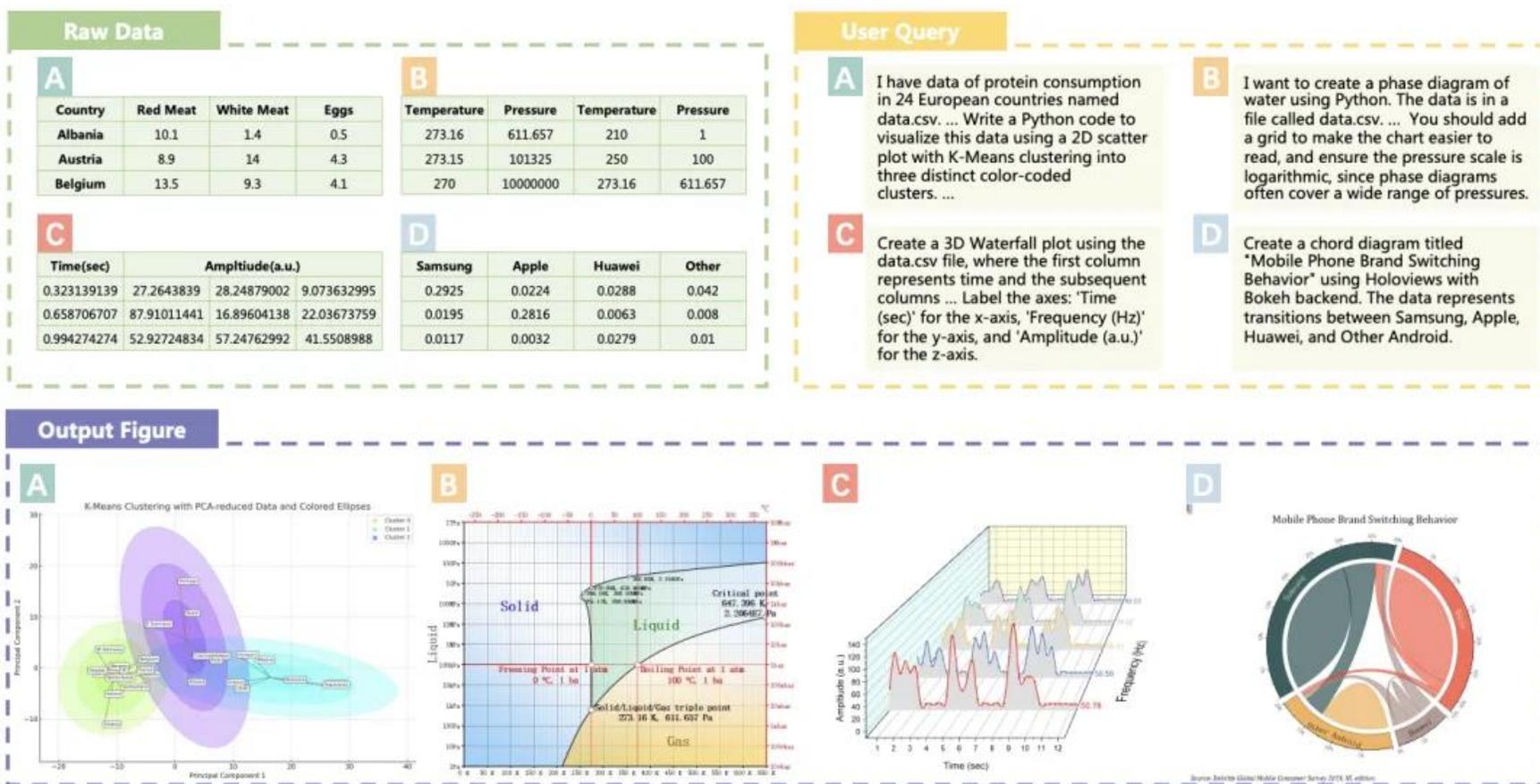
- ChatDev的软件制作平均**时间小于7.0分钟**且制作**成本约\$0.3美元**



累计获得超**23.3k星标关注**，曾连续多天**登顶Github Trending**榜单。被谷歌DeepMind大模型产品负责人Bailey和资深数据科学家Sanyam Bhutani等人进行解读、人工智能著名学者**Andrew Ng (吴恩达)**在红杉美国AI峰会上以ChatDev为例强调“多智能体协作是一种强大的设计模式”

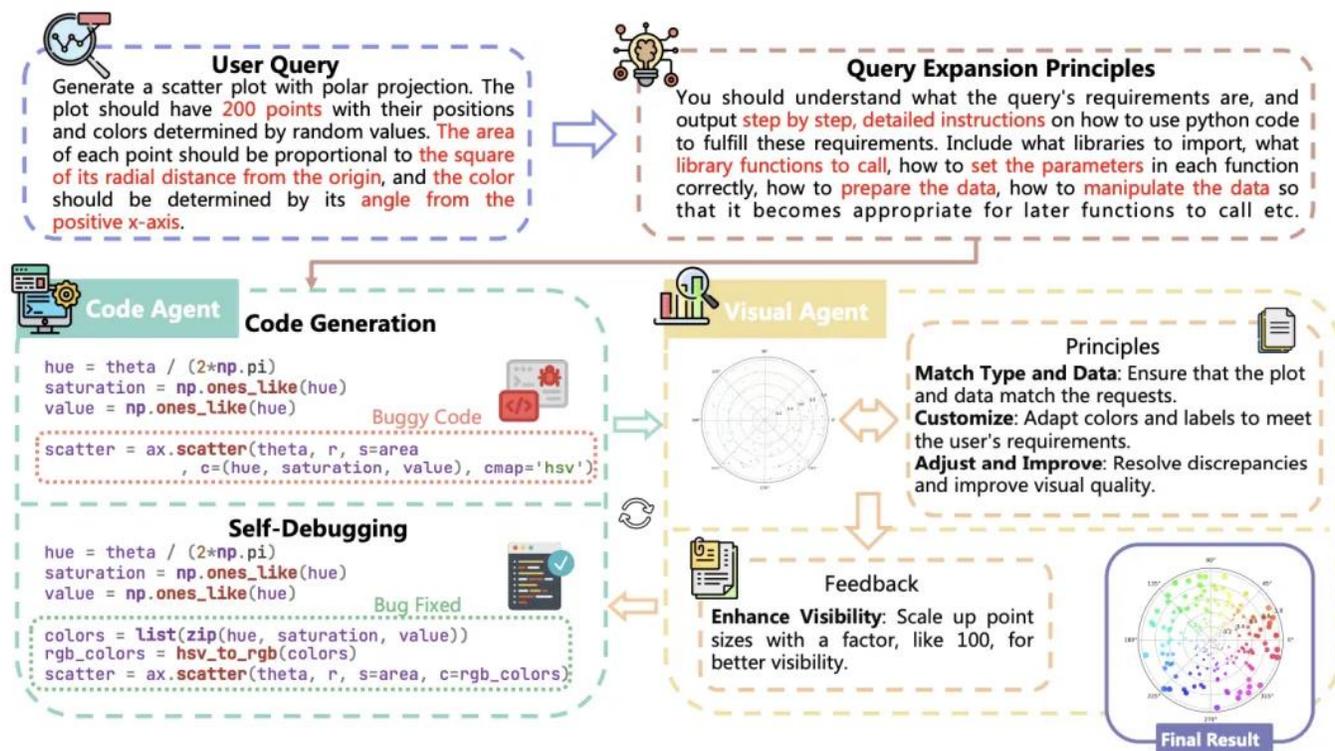
MatPlotAgent: 多智能体协作式数据可视化

- 数据可视化有助于更直接地传递复杂的信息，但制作可视化图表是一个耗时费力的过程。使用智能体技术进行**自动数据可视化**，可提升科学数据可视化的效率



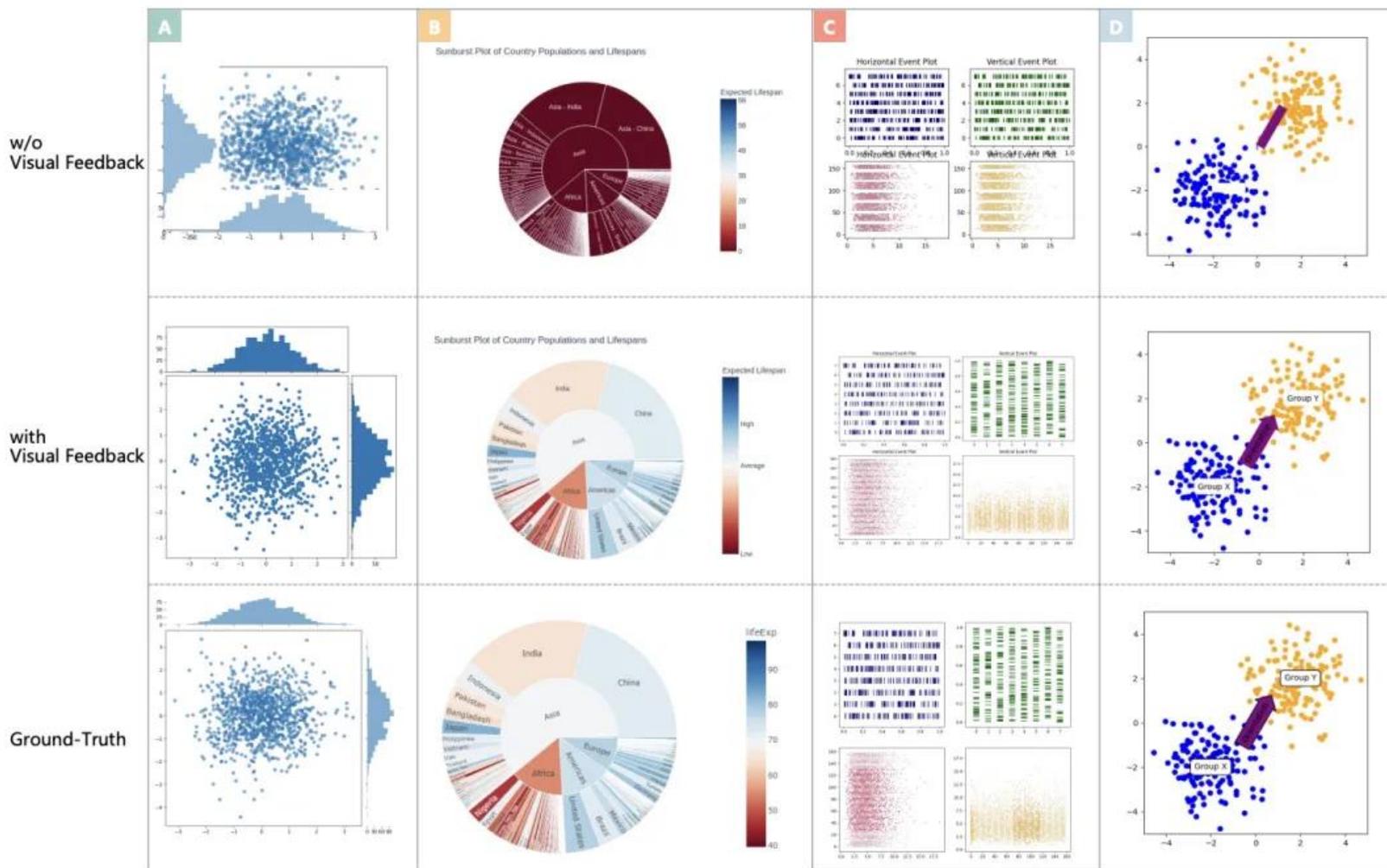
MatPlotAgent: 多智能体协作式数据可视化

- 指令扩展智能体：充分理解用户提出的需求
- 代码生成智能体：使用代码预处理原始数据并生成图表
- 视觉反馈智能体：寻找绘制草图中的错误，并提供视觉反馈给代码生成模块



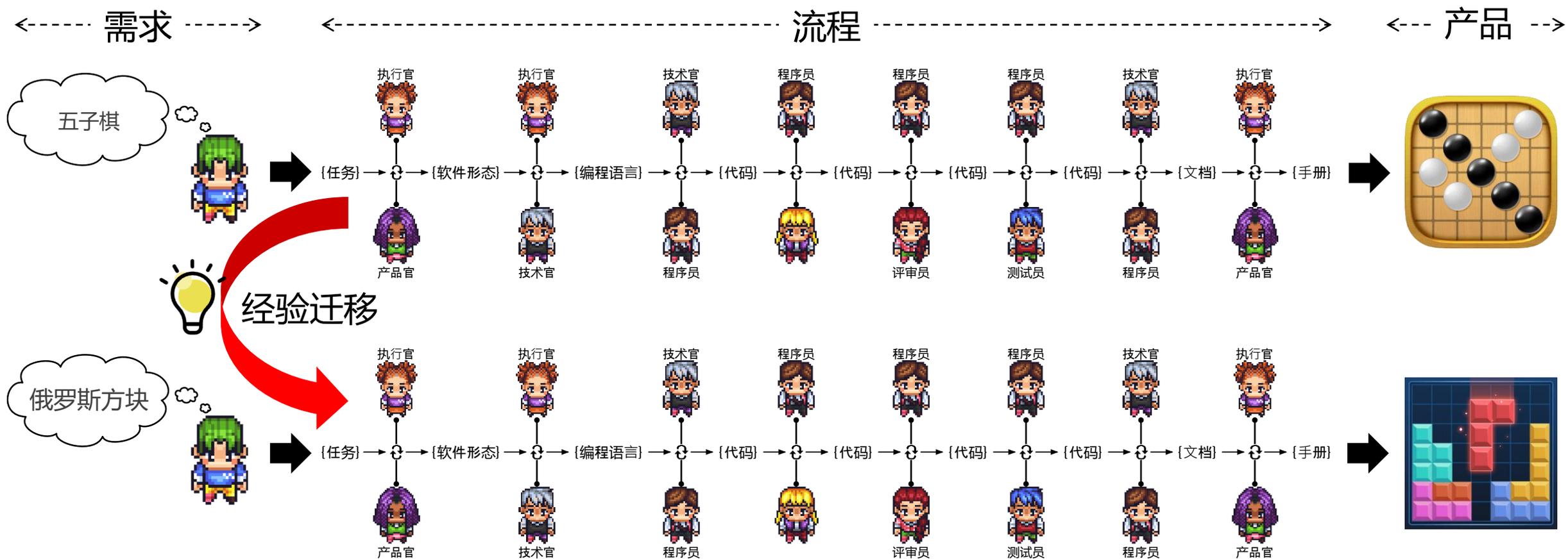
MatPlotAgent: 多智能体协作式数据可视化

- 通过各个智能体模块的交互反馈和迭代更新，得以绘制高质量的可视化图表



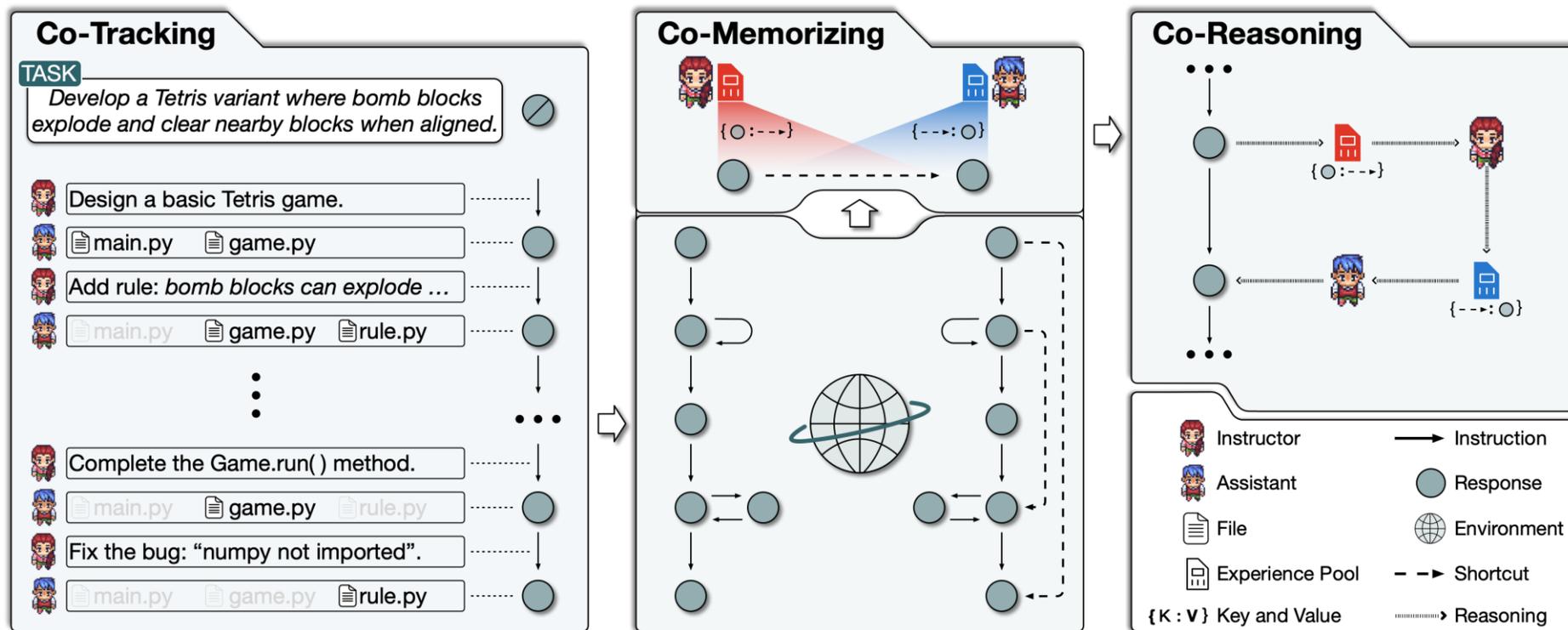
如何实现多智能体协作的能力演化?

- 积累任务执行过程中的**历史经验**，形成不同的经验池，以在通信过程中检索和交换历史经验，实现随**经验积累**的**群智演化**



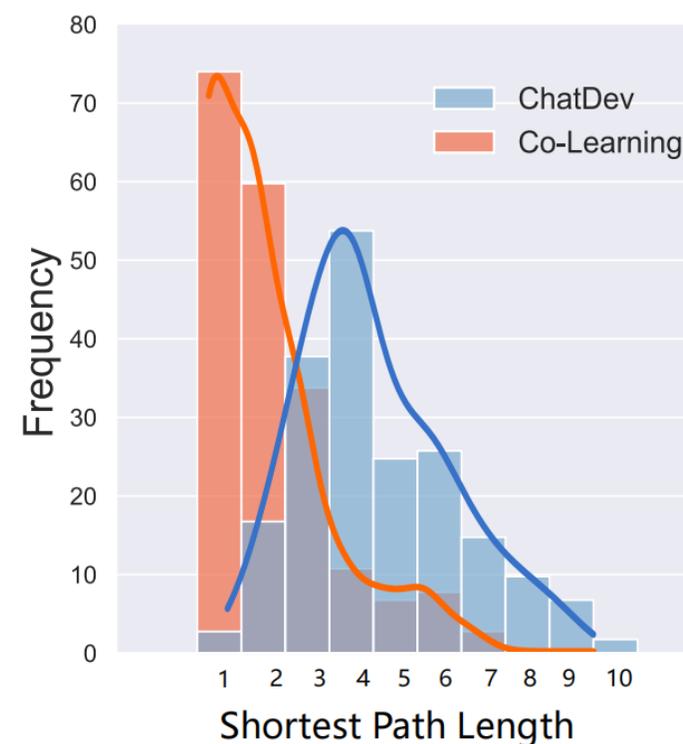
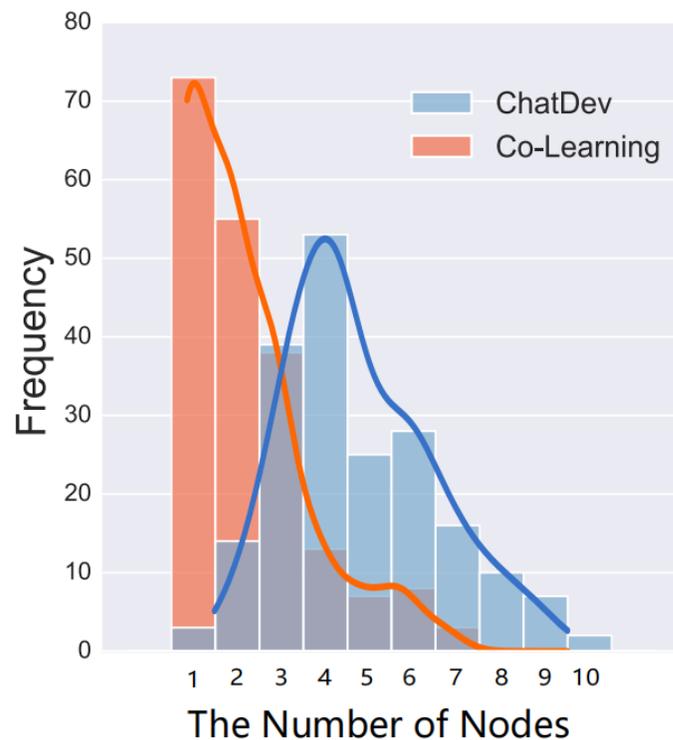
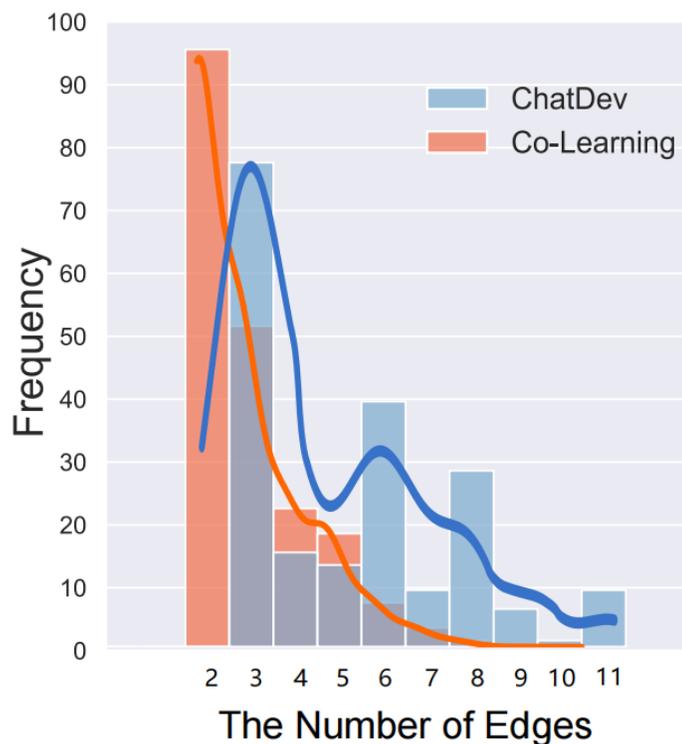
Co-Learning: 多智能体经验化共同学习框架

- 共同寻迹：训练任务上进行“彩排”，形成过往**执行轨迹**
- 共同记忆：对执行轨迹进行“**推理捷径**”抽取，作为智能体的过往经验
- 共同推理：测试任务上利用捷径记忆实现**经验化推理**



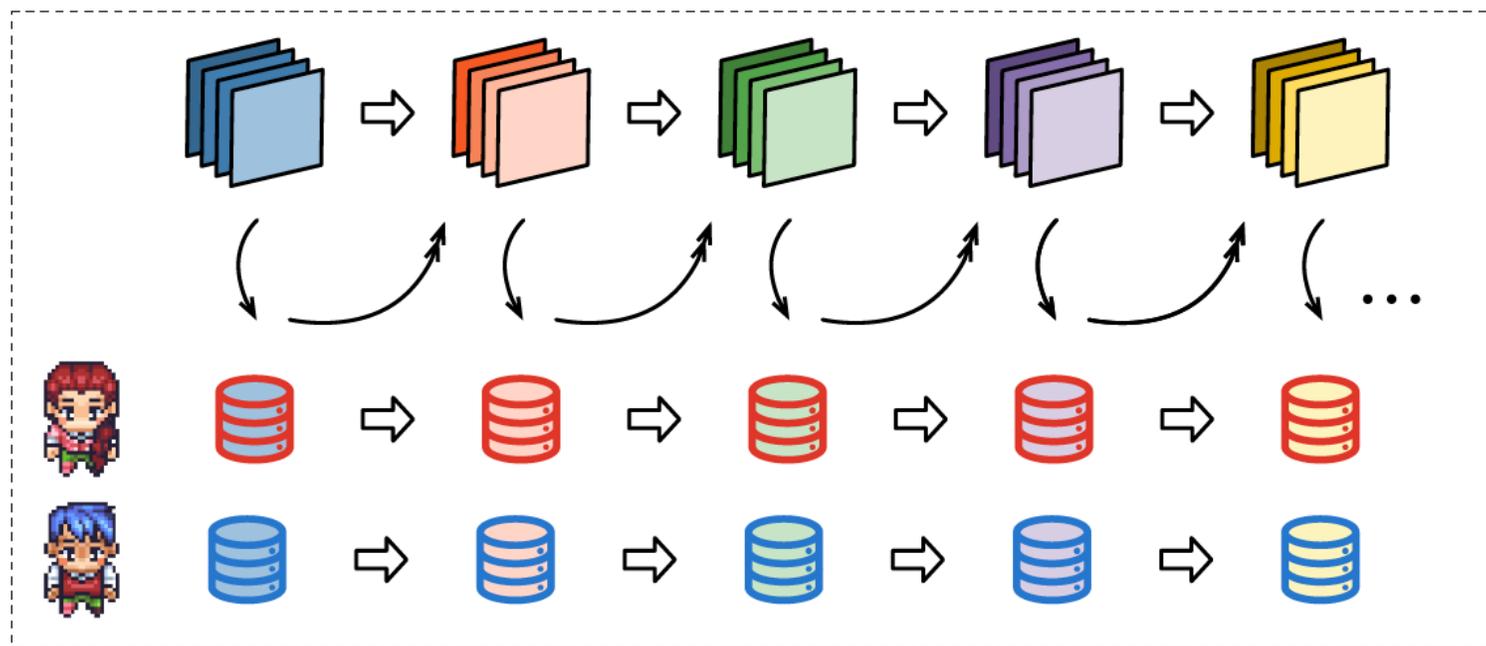
Co-Learning: 多智能体经验化共同学习框架

- 在经验化的任务执行过程中，智能体随着经验的积累实现软件步骤的显著减少，即以更少的步骤实现了更高质量的成品，实现群体推理过程的“降本增效”



| 如何迭代优化多智能体的协同经验?

- 多智能体在新任务上进行**经验收集**，同时已积累的经验根据质量进行**经验淘汰**，进而**迭代地优化**历史经验池，以提升整个系统应对复杂任务的**适应性**

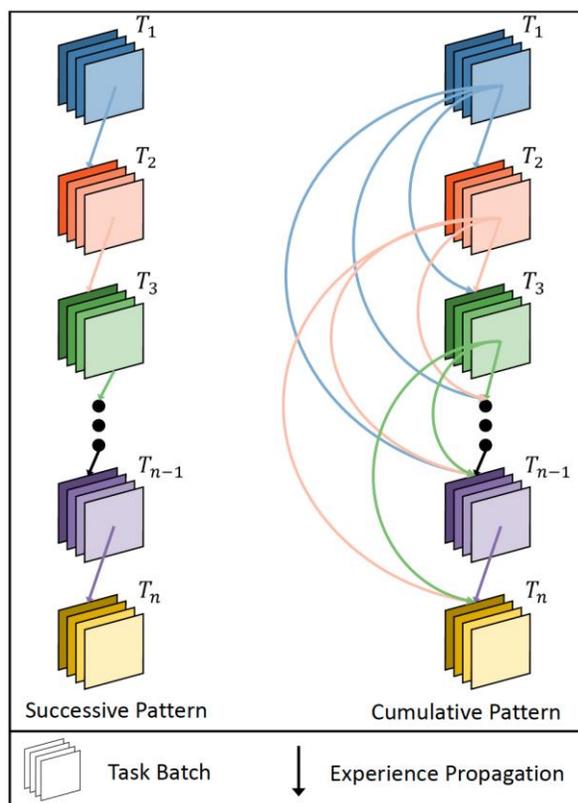


经验使用和精炼

 任务集 \Rightarrow 任务流 \longrightarrow 经验积累 $\longrightarrow\longrightarrow$ 经验使用

IER: 多智能体经验的迭代优化

- Iterative Experience Refinement: 随**任务批次**的陆续执行, 在Co-Learning**积累静态经验**的基础上, 进行**相继式**和**积累式**两类动态的经验积累



相继式 (左) 和积累式 (右) 经验积累

```
Test Reports of Source Codes:

Test Error on sales_report.py

Traceback (most recent call last):
  File "shape.py", line 42, in check_collision
    IndexError: list index out of range

According to my test reports, please locate and summarize the bugs that cause the problem.
Here's an template you can refer to but not copy:

Error Summary of Test Reports

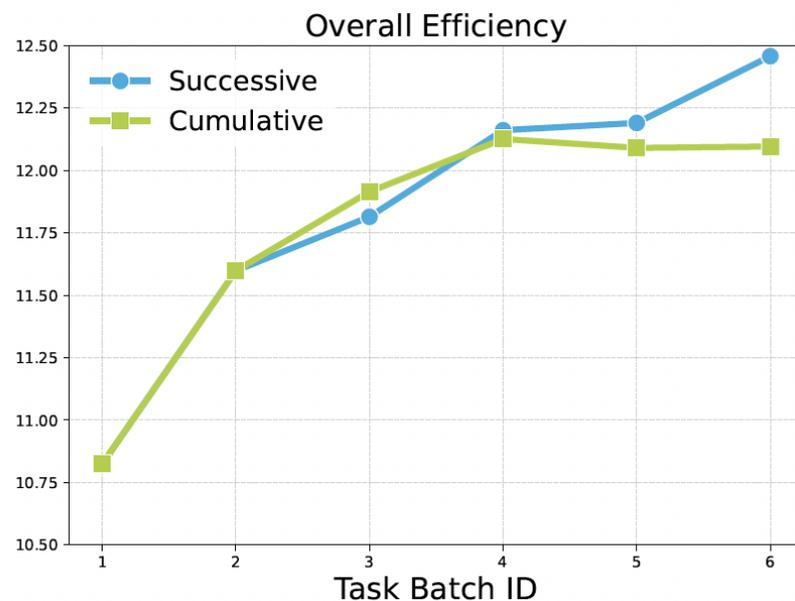
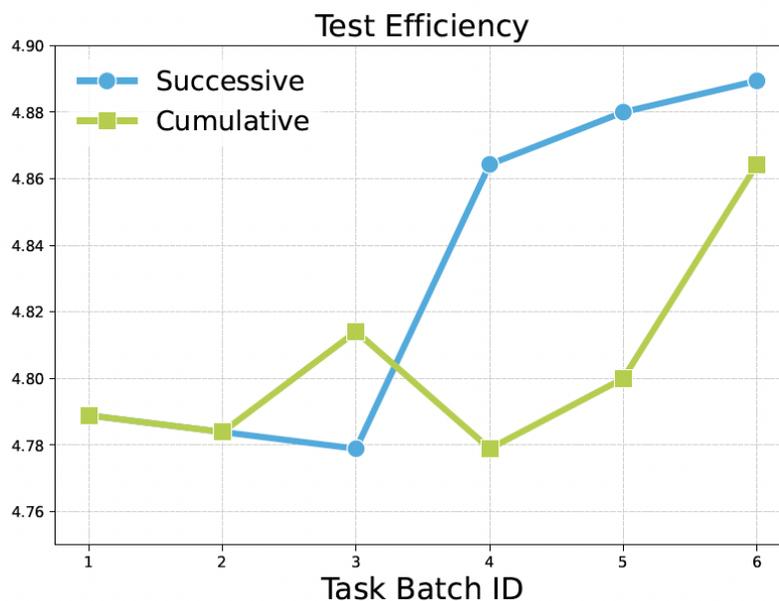
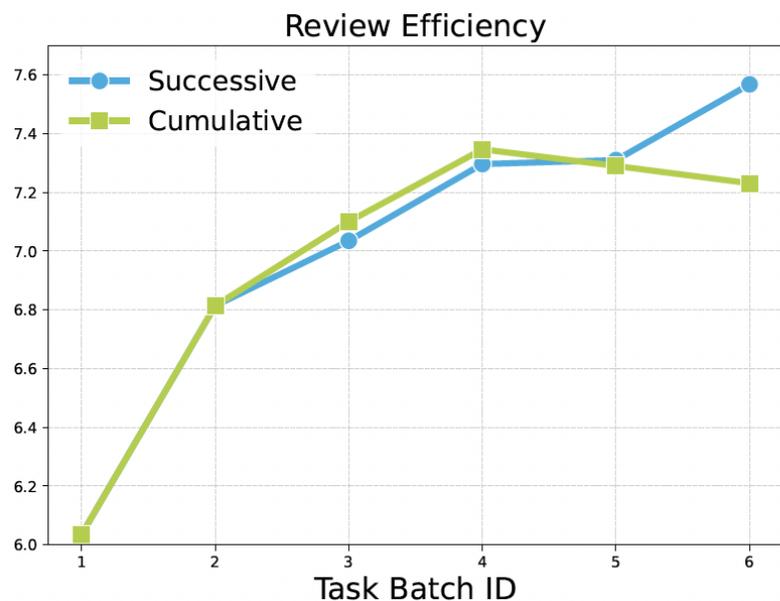
"Modules and Classes:
  No new modules need to be incorporated.
  The Game class in game.py needs to be amended to include a new attribute active_shape to
  keep track of the currently manipulated shape. This attribute will be initialized with the
  first shape in the shapes list.
  A new class Shape needs to be added to shapes.py to represent the silhouette. This class
  will have the same attributes and methods as the existing Shape class.
Data Structures:
  No new data structures need to be introduced or altered.
Main Program Flow:
  The program starts by initializing pygame and setting the dimensions of the window.
  An instance of the Game class is created, passing the screen as a parameter.
  The game loop starts, which continues until the user closes the window.
  Inside the game loop, events are checked, and if the user presses the 'r' key, the rotate
  method of the active_shape is called with an angle of 90. If the user presses the 'f' key,
  the flip method of the active_shape is called with xbool set to True and ybool set to False.
  If the user presses the 'space' key, the active_shape is updated to the next shape in the
  shapes list.
  The check_match method is called to compare the pixel data of the active_shape and the
  silhouette and take appropriate action if they match.
  The draw method is called to clear the screen and draw all the shapes.
  The display is updated to show the changes.
Input and Output:
  The program takes input from the user through keyboard events. The user can press the 'r'
  key to rotate the active shape, the 'f' key to flip the active shape, and the 'space' key
  to switch to the next shape in the list.
  The program outputs the visual representation of the shapes on the screen.
Exception Handling:
  No specific exception handling is required in this implementation.
External Libraries and Dependencies:
  The implementation requires the pygame library to be installed."
```

历史经验示例

| IER: 多智能体经验的迭代优化

- 随任务执行过程, Agent的协同效率**随经验的动态积累而逐步提升**

	Completeness	Executability	Consistency	Quality	Duration
GPTEngineer	0.4824	0.3583	0.7887	0.1363	15.6000
MetaGPT	0.4472	0.4208	0.7649	0.1439	154.0000
ChatDev	0.7337	0.8040	0.7909	0.4665	148.2150
ECL	0.8442	0.8643	0.7915	0.5775	122.7750
IER-Successive	0.8744	<u>0.9146</u>	<u>0.7968</u>	0.6372	179.4437
IER-Cumulative	<u>0.8492</u>	0.9347	0.7983	<u>0.6337</u>	181.5961



群体智能：数字孪生，万物智联

Internet

信息高速，全球连接

全球信息高速公路，
将每一位网民紧密相连



Internet of Things

设备互联，生活便捷

物体间的沟通桥梁，
使每一件设备灵活互联



Internet of Agents

数字孪生，万物智联

交织万物的网络纽带，
绘制人机共生的未来蓝图

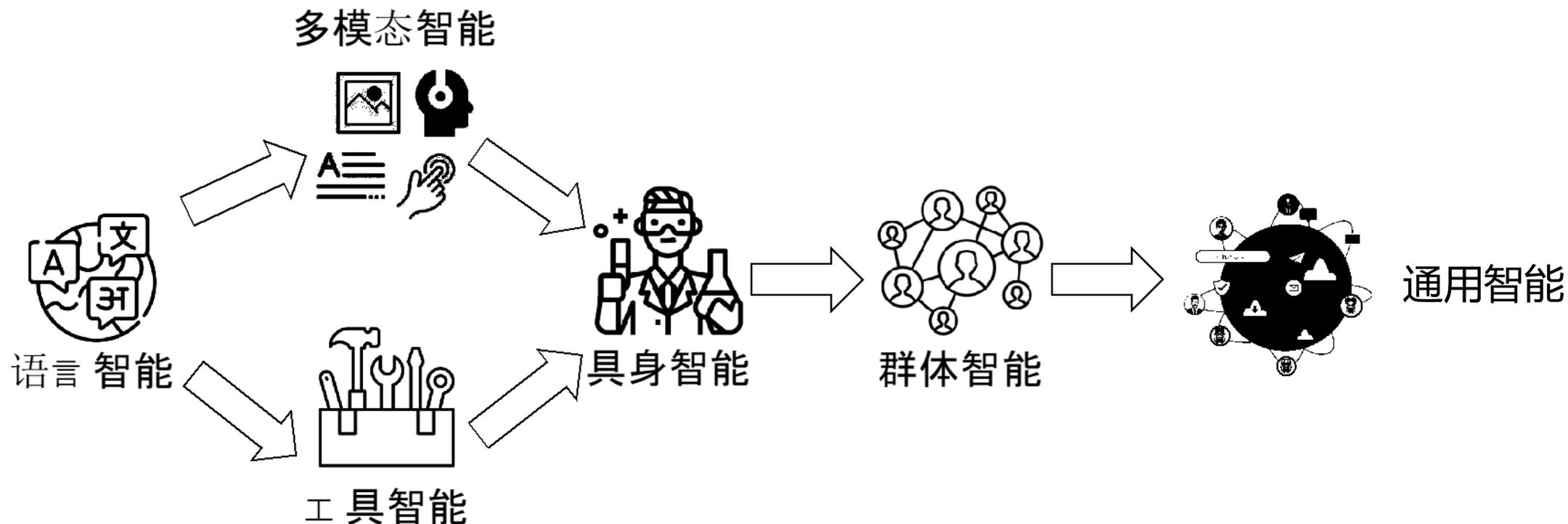


| 总结：迈向通用人工智能

人工智能三个发展阶段：**符号智能、专用智能、通用智能（大模型）**

大模型技术吹响迈向通用智能号角：**框架通用、学习通用、能力通用**

大模型特性亟待挖掘：**稀疏模块、多模态智能、工具智能、自主智能体、群体智能**



谢谢各位，欢迎批评指正！

刘知远

liuzy@tsinghua.edu.cn