



人工智能文集

第二十三集

中国开源软件推进联盟

China Open Source Software Promotion Union

目 录

- 一、数据是人工智能的石化材料.....Ilya Sutskever
- 二、对伊里亚演讲的注释和点评.....陆首群
- 三、“AI agent 黎明”之后 我们期待些什么?Silvio Savarese
- 四、Agent 人工智能:走向 AGI.....Anna.AI MED ADD
- 五、实践 AI Agent 自动化扫描代码库的思考与总结.....袁恽
- 六、中国 DeepSeek 崛起从震撼硅谷到震撼世界.....COPU
- 七、我为什么写支持 DeepSeek 的文章.....陆首群
- 八、DeepSeek 证明:开源是主导科技市场的秘诀.....Jim Zemlin
(华尔街的看法是错的)
- 九、DeepSeek 拆解源代码发生了秘密.....陈钟
- 十、李飞飞向巴黎人工智能大会提出制定 AI 政策三原则.....COPU 摘录
- 十一、DeepSeek 启示录.....韩宪平
- 十二、DeepSeek 的学习与讨论.....刘澎
- 十三、DS 对模型架构 MLA 和 MoE 全方位创新.....陆首群

数据是人工智能的石化材料

(Data is the fossil fuel of AI)

Ilya Sutskever

Ilya 重磅演讲：预训练将结束，接下来是超级智能「自我意识」



Ilya 燃爆 NeurIPS 2024 ，最新演讲来了

我们现在如此依赖的强大人工智能，在未来的某一天会走向何方？我们是否已触及了数据时代的顶峰？Ilya 带我们回顾过去十年，并大胆预测 AI 的未来

Ilya 核心观点：

LLM 预训练将结束，数据是 AI 的化石燃料，超级智能是 AI 领域的未来，超级智能的演化步骤是：代理、推理、理解和自我意识，我们将来要处理的 AI 系统将是高度不可预测的

以下是 Ilya 在 NeurIPS 2024 接受颁奖的主题演讲 Data is the fossil fuel of AI

全文

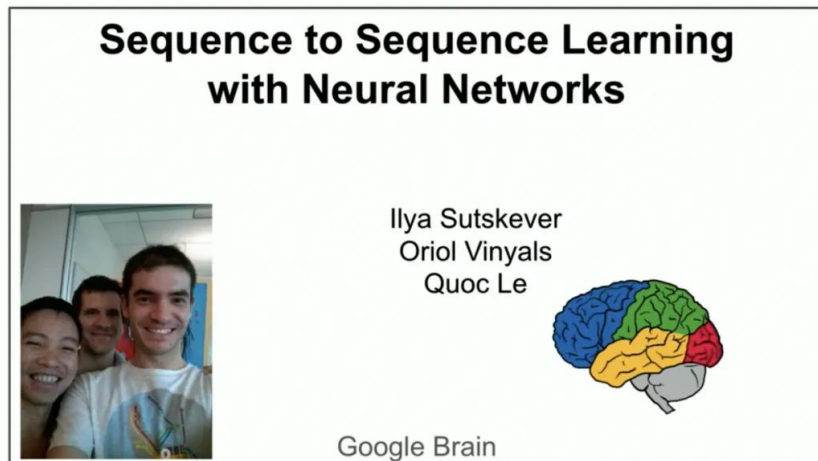
开场致谢

我首先要感谢组织者选择我们的论文给予支持，这真是太棒了。同时，我还要感谢我的杰出合作者 Oriol Vignales 和 Kwokli，他们刚才还站在你们面前。

回顾：十年前的演讲

现在你们看到的是一张截图，来自 10 年前，2014 年在蒙特利尔的 NeurIPS 会议上我做的类似演讲。那时我们还很天真。照片上是当时的我们（“之前”）

2014



这是现在的我们（“之后”）。现在，我希望我看起来更成熟，更有经验

2024



今天我想谈谈这项工作本身，并进行一个 10 年的回顾。因为这项工作中有很多观点是正确的，但也有一些不太正确。我们可以回顾一下，看看发生了什么，以及它是如何逐渐演变成今天的样子的

我们做了什么？

我们先来回顾一下我们当时做了什么。我会展示 10 年前那次演讲的幻灯片。总的来说，我们做了以下三件事：

- 构建了一个基于文本训练的自回归模型
- 使用了一个大型神经网络
- 使用了大型数据集

就这么简单。现在我们深入探讨一下细节

深度学习的假设

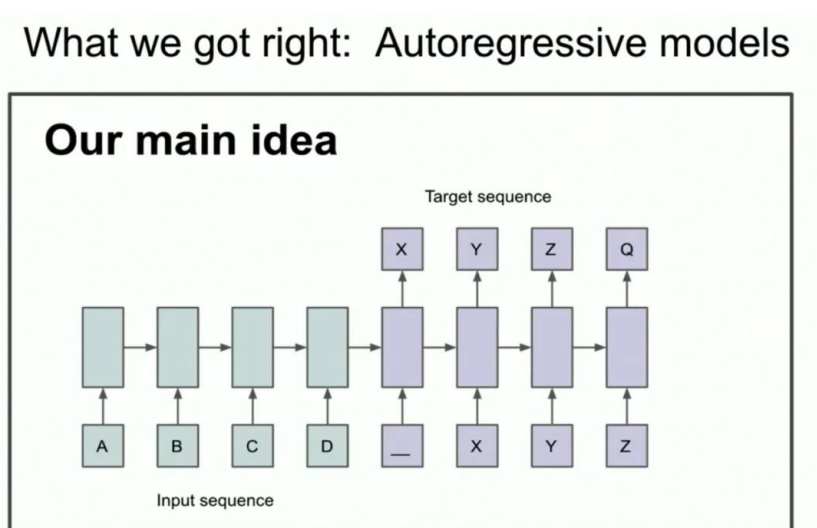
这是 10 年前的幻灯片，还不错吧？上面写着“深度学习的假设”。我们当时认为，如果有一个大型神经网络，它包含很多层，那么它就能在不到一秒的时间内完成人类可以完成的任何事情。为什么我们要强调人类在一秒内可以完成的事情？

这是因为，如果你相信深度学习的“教条”，认为人工神经元和生物神经元是相似的，或者至少没有太大的不同，并且你相信神经元是缓慢的，那么任何人类能够快速完成的事情，只要世界上有一个人能够在一秒内完成，那么一个 10 层的神经网络也能做到。逻辑是这样的：你只需要提取他们的连接方式，然后将其嵌入到你的人工神经网络中。

这就是动机。任何人类在一秒内可以完成的事情，一个大型 10 层神经网络都可以做到。我们当时关注 10 层神经网络，是因为那时我们只知道如何训练 10 层的网络。如果层数能更多，也许能做更多事情。但当时我们只能做到 10 层，所以我们强调的是人类在一秒内能完成的事情。

核心思想：自回归模型

这是当时演讲的另一张幻灯片，上面写着“我们的核心思想”。你可能认出来至少一个东西：这里正在发生自回归的过程。这张幻灯片到底在说什么？它在说，如果你有一个自回归模型，它能很好地预测下一个 token，那么它实际上会捕获、抓住下一个序列的正确分布。



这在当时是一个相对较新的想法。这并不是第一个自回归神经网络。

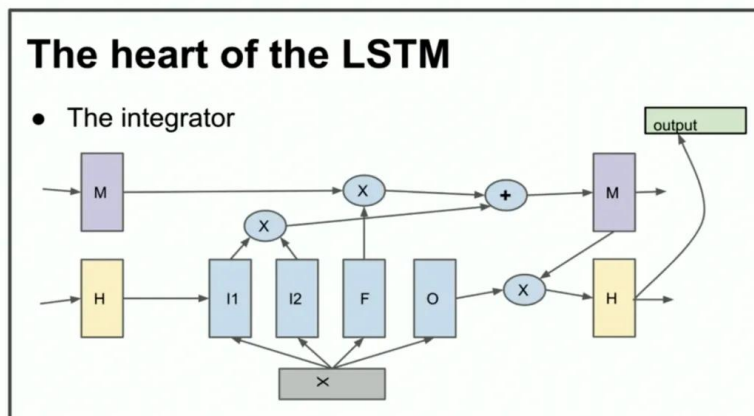
但我认为，这是第一个我们真正相信，如果训练得足够好，就能得到任何想要的结果的自

回归神经网络。在当时，我们的目标是（现在看来很平常，但当时非常大胆）机器翻译

LSTM: Transformer 之前的技术

接下来我要展示一些你们很多人可能从未见过的古老历史：**LSTM**。对于不熟悉的人来说，LSTM 是在 Transformer 出现之前，可怜的深度学习研究人员使用的东西。它基本上是一个旋转了 90 度的 ResNet。你可以看到它集成了残差连接（现在被称为残差流），但也有些乘法运算。它比 ResNet 稍微复杂一点。这就是我们当时用的。

What we got wrong: the LSTM



并行计算：管道并行

另一个我想强调的特点是并行计算。我们使用了管道并行，每个 GPU 处理一层。使用管道并行明智吗？现在看来，管道并行并不明智。但我们当时没那么聪明。通过使用 8 个 GPU，我们获得了 3.5 倍的速度提升。

Early distributed training

Parallelization

- Use an 8 GPU machine
- One layer per GPU, softmax for remaining GPUs
- **3.5x speedup** over a single GPU
- **8x more RAM**

- Model can be run on a single K40

结论：规模化假设

当时演讲的结论幻灯片

可以说是最重要的幻灯片，因为它阐述了规模化假设的开端：如果你有非常大的数据集，并且训练非常大的神经网络，那么成功就是必然的。如果你愿意往好的方面想，可以说，这确实就是之后发生的事情。

What we got right: early scaling hypothesis

Conclusions

- If you have a large big dataset
- And you train a very big neural network
- Then success is guaranteed!

The core idea

- If: Bio neuron \approx artificial neuron
- Then: Human Brain \approx Very large artificial neural network

核心理念：连接主义

我还想提一个理念，我认为这个理念经受住了时间的考验。这就是连接主义。核心理念是：

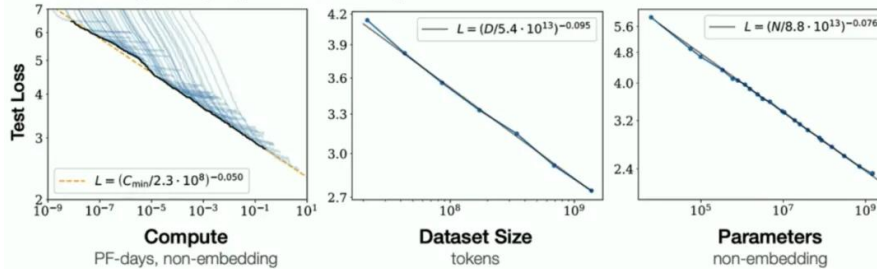
如果你相信人工神经元有点像生物神经元，那么你就有信心相信大型神经网络（即使它们不完全像人类大脑那么大）可以被配置来完成我们人类所做的大部分事情。当然还是有差异，因为人类大脑会自我重构，而我们现在最好的学习算法需要大量的数据。人类在这方面仍然更胜一筹。

预训练时代

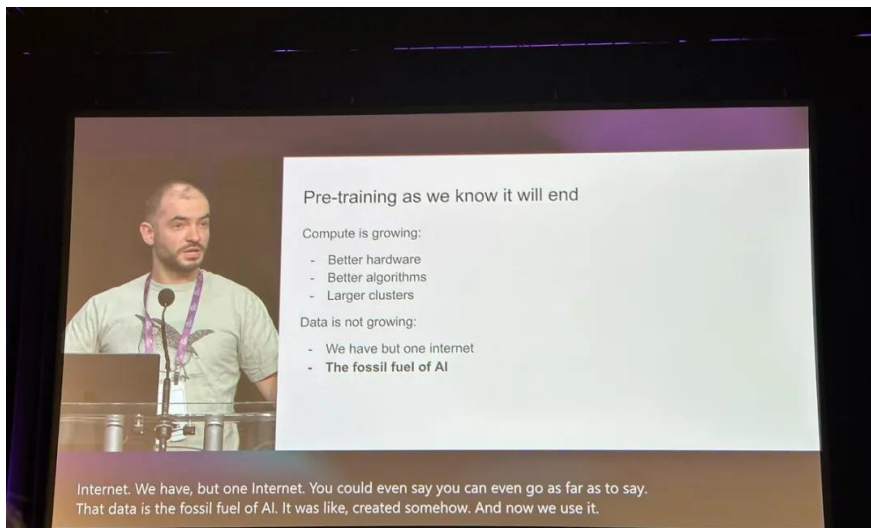
我认为所有这些都引领了预训练时代的到来。GPT-2 模型、GPT-3 模型、缩放法则，我要特别感谢我的前合作者：Alec Radford、Gerrit Kaplan 和 Daria Amodei，他们的工作至关重要。预训练是今天我们看到所有进步的驱动力。超大型神经网络，在海量数据集上训练。

The age of Pre-Training

- GPT-2 [Radford et al., 2019]
- GPT-3 [Brown et al., 2020]
- Scaling laws [Kaplan et al. 2020]



预训练的终结，但预训练终将结束。为什么？因为虽然算力在不断增长，但数据并没有无限增长，因为我们只有一个互联网。你甚至可以说，数据是人工智能的化石燃料。它被创造出来，我们使用它，并且已经达到了数据峰值，不会有更多的数据了。我们只能处理现有的数据。尽管我们还有很多路要走，但我们只有一个互联网。



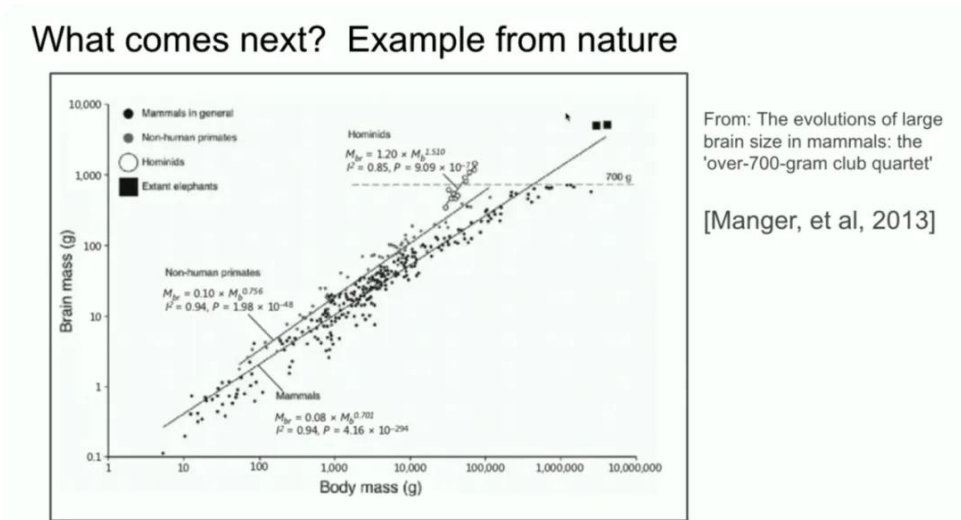
下一步是什么？

接下来我将稍微推测一下未来会发生什么。当然，很多人都在推测。你可能听说过“智能体”（agents）这个词。人们觉得智能体是未来。更具体一点，但也有点模糊的是合成数据。如何生成有用的合成数据仍然是一个巨大的挑战。还有推理时的算力优化，以及最近在 o1 模型中看到的，这些都是人们在预训练之后尝试探索的方向。

生物学启示：不同物种的大脑缩放

我还想提一个生物学的例子，我觉得非常有趣。多年前，我也在这个会议上看到一个演讲，演讲者展示了一个图表，显示哺乳动物的身体大小和大脑大小之间的关系。演讲者说，在生物

学中，一切都很混乱，但这里有一个特例，即动物的身体大小和大脑大小之间存在紧密的关系。

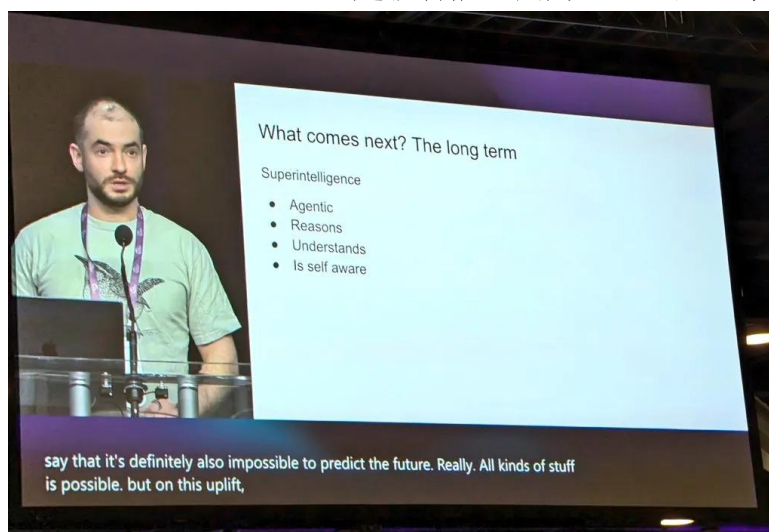


我当时对这个图表产生了好奇，并开始在谷歌上搜索。其中一个图片结果是这样的：你可以看到各种哺乳动物，非人类灵长类动物也是如此。但接下来是人科动物，如尼安德特人，他们和人类的进化关系很近。有趣的是，人科动物的脑体缩放指数具有不同的斜率。

这意味着，生物学中存在一个例子，它展示了某种不同的缩放方式。这很酷。另外，我要强调一下，x 轴是对数刻度。所以，事物是有可能不同的。我们目前所做的事情，是我们第一个知道如何进行缩放的事情。毫无疑问，这个领域的所有人都会找到下一步的方向。

关于未来的推测

现在我想花几分钟推测一下更长远的未来，我们都将走向何方？我们正在取得进步，这真是太棒了。如果你是 10 年前就入行的，你会记得当时的技术有多么不成熟。即便你觉得深度学习是理所当然的，但亲眼看到它取得的进步还是令人难以置信。我无法向那些最近两年才加入这个领域的人传达这种感觉。但我要谈谈**超级智能**，因为这显然是这个领域的未来。



超级智能在性质上将与我们今天拥有的智能截然不同。我希望在接下来的几分钟里，给你一些具体的直觉，让你感受到这种不同。

现在我们拥有了强大的语言模型，它们是很棒的聊天机器人，它们甚至能做一些事情，但它们也常常不可靠，有时会感到困惑，同时在某些任务上又具有超人的表现。如何协调这种矛盾目前还不清楚。

但最终，以下情况将会发生：

这些系统将真正具有智能体的性质。而现在，它们在任何有意义的层面上都不是智能体，或者说只有非常微弱的智能体性质。它们会进行真正的推理。

我还要强调一点，关于推理：

一个系统越能进行推理，就变得越不可预测。我们现在使用的模型都是可预测的，因为我们一直在努力复制人类的直觉。我们大脑在一秒钟内的反应，本质上就是直觉。所以我们用一些直觉训练了模型。但推理是不可预测的。原因之一是，好的国际象棋 AI 对人类国际象棋高手来说是不可预测的。

所以，我们将来要处理的 AI 系统将是高度不可预测的。它们会理解有限的数据，它们不会感到困惑，这是它们目前存在的巨大局限。我不是说如何做到，也不是说何时做到，我只是说它将会发生。当所有这些能力都与自我意识相结合时（为什么不呢？自我意识是有用的），我们将拥有与今天截然不同的系统。它们将拥有令人难以置信的能力。但与这些系统相关的问题将与我们过去习惯的问题大相径庭。

预测未来是不可能的，一切皆有可能。但最后，我还是要以乐观的态度结束我的演讲。

问答环节

问题 1：生物结构与人类认知

- 问题：在 2024 年，是否有其他生物结构在人类认知中发挥作用，您认为值得像您之前那样去探索？
- 回答：如果有人对大脑的运作方式有独特的见解，并且认为我们目前的做法是愚蠢的，他们应该去探索它。我个人没有这样的想法。也许从更高的抽象层面来看，我们可以说，生物学启发的人工智能是非常成功的，因为所有的神经网络都是受生物启发的，尽管其灵感非常有限，比如我们只是使用了神经元。更详细的生物灵感很难找到。但如果有什么特别的见解，也许可以找到有用的方向。

问题 2：推理和自我纠正

- 问题：您提到推理是未来模型的核心方面。我们看到现在模型中存在幻觉。我们使用统计分

析来判断模型是否产生幻觉。未来，具有推理能力的模型能否自我纠正，减少幻觉？

• 回答：我认为你描述的情况是极有可能发生的。事实上，有些早期的推理模型可能已经开始具备这种能力了。长期来看，为什么不能呢？这就像微软 Word 中的自动更正功能。当然，这种功能比自动更正要强大得多。但总的来说，答案是肯定的。

问题 3：超级智能的权利和激励机制

• 问题：如果这些新诞生的智能体需要权利，我们应该如何为人类建立正确的激励机制，以确保它们能像人类一样获得自由？

• 回答：这是一个值得人们思考的问题。但是我不觉得我有能力回答这个问题。因为这涉及建立某种自上而下的结构，或者政府之类的东西。我不是这方面的专家。也许可以用加密货币之类的东西。如果 AI 只是想与我们共存，并且也想要获得权利，也许这样就挺好。但我认为未来太不可预测了，我不敢轻易评论。但我鼓励大家思考这个问题。

问题 4：LLM 的多跳推理泛化能力

• 问题：您认为大型语言模型（LLM）是否能够进行多跳推理的跨分布泛化？

• 回答：这个问题假设答案是肯定的或者否定的。但这个问题不应该用“是”或“否”来回答，因为“跨分布泛化”是什么意思？“分布内”又是什么意思？在深度学习之前，人们使用字符串匹配、n-gram 等技术进行机器翻译。当时，“泛化”意味着，是否使用完全不在数据集中的短语？现在，我们的标准已经大幅提高。我们可能会说，一个模型在数学竞赛中取得了高分，但也许它只是记住了互联网论坛上讨论过的相同想法。所以，也许它是在分布内，也许只是记忆。我认为人类的泛化能力要好得多，但现在的模型在某种程度上也能够做到。这是一个更合理的答案

对伊里亚演讲的注释和点评

COPU

伊里亚·萨斯哥弗(Ilya Sutskever)是人工智能大师杰夫里·辛顿(Geoffrey Hinton)的学生,也是一位知名的人工智能专家,他是 OpenAI 的创始人之一,曾任该公司的首席科学家。

他在《神经信息处理系统 2024 年会(NeurIPS2024)》上接受领奖时,作了“数据是人工智能化石燃料”(Data is the fossil fuel of AI)的主题演讲。他在演讲中回顾了人工智能发展的过去,谈到了现在,并展望未来。

为了便于读者更好理解他的演讲,COPU 谨对他演讲中的一些核心观点进行注解和点评。

伊里亚认为,现在的人工智能语言大模型(LLM)是基于深度学习发展起来的。

COPU 注释:语言大模型是基于深度学习算法(辛顿等人自创的人工神经网络是其核心技术)、采用统计学模型(其语料库中规模数量的语料为其提供化石燃料)发展起来的。

其中,人工神经网络(Artificial Neural Network, ANN)与生物神经网络相似而非相同,它成功模拟生物神经网络中的神经元的功能,但在全面、准确、高效模拟方面尚有局限;它比起后来建立类脑的脉冲神经网络(Spiking Neural Network, SNN)也有差距。

伊里亚谈到语言大模型的预训练行将结束。

COPU 注释:供大模型“预训练”之用的语料数量的增长将导致大模型推理能力的增长。语料的参数量开始取自日常数据,继而取自行业内专用的大数据,后来又取自互联网的海量数据,这时自然取得的参数量已经到顶(GPT-4 达 Token 1.76 万亿, Llama 达 Token 2 万亿, Falcon 达 Token 3.5 万亿, 总之互联网海量数据 Token 约几万亿),宣告了预训练的终结。

为了满足进一步提高推理能力(进而提高大模型智能)的需要,人们将越过从互联网自然取材的海量数据的顶峰,自产数量级约为 Token 几百万亿的合成数据,自 GPT 1o 开始应用,从而开辟了“后训练”的新时代。

伊里亚认为,人工智能的未来是超级智能,而超级智能的演化步骤是代理、推理、理解 and 自我意识。他还认为,智能体(agents)是 AI 的未来,推理是未来 AI 的核心,但推理是不可预测的。他还就推理是否能产生自我纠正能力、大模型能否产生自我意识、未来大模型是否具有预测能力、以及如何赋予超级智能权利等问题,进行思考。

COPU 注释：大模型推理能力的提高是会产生自我纠正能力的，从而减少或消除大模型产生“幻觉”的负面效应。大模型如果能摆脱有限数据条件的局限，采用类脑神经网络并发挥其作用，导致大模型产生自我意识完全是可能的。而具有自我意识的大模型才会产生预测能力。

伊里亚没有谈到未来 AI 与人类的关系问题。

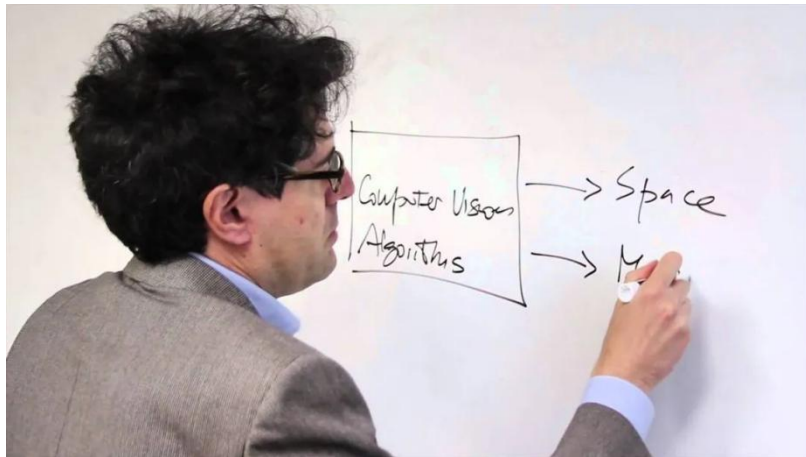
不久前 COPU 尝列举几位人工智能大师的看法：①人类+agents 应对 AI, ②人类与 AI 是协同合作关系, ③人类设置安全红线应对 AI。这是一个关系到人类安全和利益的重大课题, 有待于稳妥解决。

最近看到李飞飞大师最新的访谈：她在谈到人类与 AI 的关系时强调：无论如何要确保人的主体性和能动性，把 AI 看作为“强大”的工具，这些工具用于增强人的能力而非替代，使人类能够更精确地利用这些工具完成任务，我们将看到更多的(人类与 AI)的协同能力将展现出来。如此看来，李飞飞的观点属于上述人工智能大师看法的第②类。

“AI agent 黎明”之后 我们期待些什么？

Silvio Savarese

李飞飞丈夫、Salesforce 首席科学家撰文：「AI agent 黎明」之后，我们期待些什么？



人工智能（AI）专家普遍认为，2025 年将是智能体（agent）爆发之年。

去年底，Gartner 也将 agentic AI 列入了 2025 年十大技术趋势之一，并预测 2028 年将至少有 15% 的日常工作决策由 agentic AI 自主完成，而这一数字在 2024 年为 0。

随着大模型在多模态理解、逻辑推理等方面的进一步发展，agent 或将在 2025 年迎来大规模落地应用，替代人类自主解决越来越多的日常工作。

日前，Salesforce 首席科学家撰文、斯坦福大学计算机科学兼职教授 Silvio Savarese，在一篇文章中探讨了 agent 系统的发展前景、在这一过程中需要人类提供哪些帮助，以及有关 agent 的信任和问责问题。

值得一提的是，Savarese 也是“AI 教母”、斯坦福大学首位红杉讲席教授、美国三院院士李飞飞的丈夫。

他表示，正如音乐从单音旋律发展到复杂的交响乐一样，agent 也正从「个体演奏者」发展到「管弦乐团」。从现在开始，几乎所有企业——从个人贡献者到高管——不仅可以协调人类劳动力，还可以协调数字劳动力。

“未来不是人类与人工智能的对决，而是双方协同合作，发挥各自的独特优势。”

学术头条在不改变原文大意的情况下，对整体内容做了精编，如下：

在由 AI agent 网络增强的新兴格局中，人类在工作中的角色变得比以往任何时候都更有能力、更有趣、更有创造力。我们现在已经迎来了人工智能的第三次浪潮，它以预测式和生成式人工

智能为基础。从人才招聘到超级医疗保健，我们现在将看到人工智能与人类在各个领域合作，以更快的速度满足各种需求，而且在许多情况下比人类本身更准确。Agentic AI 需要一些时间来产生效应，但它将改善我们工作的许多方面：生产力、效率、战略决策，以及总体工作满意度。

欢迎来到 Agentic AI 时代的黎明。从现在开始，几乎所有企业——从个人贡献者到高管——不仅可以协调人类劳动力，还可以协调数字劳动力。

我们将看到信任和问责制作为三个阶段演进的基石：掌握离散任务的专业 agent，多 agent 系统无缝协作，以及重写业务运作方式的企业级编排。

以下是我们对 agent 系统发展前景的展望，以及在发展过程中需要人类提供哪些帮助。

agent 的演变：从规则到推理

大语言模型（LLM）是一种经过训练的深度学习模型，能够理解文本并生成文本。agent 的发展反映了机器学习本身的发展。传统的基于规则的系统，如机器人流程自动化（RPA），能够执行精确的序列，但在面对（周围环境）变化时的表现不佳。这些早期实施需要大量的技术开销和咨询服务，给许多组织带来了很高的准入门槛。

在过去的几十年里，我们见证了渐进式和突破性的进步，这些进步改变了机器处理信息的方式——从僵化的自动化发展到更加灵活、适应性更强、效率更高的学习系统。但是，更令人兴奋的是我们的发展方向：通过多 agent 推理实现自适应 agent——agent 可以从环境中学习，通过经验不断改进，并与人类和来自企业客户、合作伙伴、供应商的 agent，甚至消费者的个性化人工智能助手进行协作，而人工智能助手正在成为他们生活中越来越重要的一部分。企业 agent 的未来将分为三个阶段，而我们现在只是刚刚开始。

企业 AI agent 的三个阶段

正如音乐从单音旋律发展到复杂的交响乐一样，AI agent 也正从个体演奏者发展到管弦乐团。每个阶段都建立在上一个阶段的基础上，在企业环境中创造出更丰富、更细微的互动。

第 1 阶段：“单音”人工智能——专业贡献者



在 agent 演变的第一阶段，专业 agent 擅长特定行业中的特定任务，为常规但关键的业务运营带来更高的效率和准确性。它们代表了企业人工智能采用的基础，以一致性和速度处理离散任务，从而转变部门 workflow。它们还擅长提供人工智能迄今取得的进步所带来的好处，如预测下一个最佳行动和产品推荐，根据每个客户的偏好和行为进行高度个性化。此外，它们还能为客户、服务人员和销售代表——无论是人类还是机器人——提供最高水准的生成指导、营销语言和通信。

例如，在商业领域，它们彻底改变了库存和账户管理。事实上，agent 不只是处理基本的库存检查，还能主动监控多个地点的库存水平，预测季节性需求，并生成实时账户摘要，以标记异常模式或机会。过去需要数小时人工分析的任务，现在只需几秒钟就能完成，而且具有更大准确度和深度，为零售客户带来优化、个性化和近乎“神奇”的体验。

服务运营也有类似的转变。除了基本的账单汇总外，agent 还能分析客户互动模式，自动分类和为服务请求设定优先级，并生成关于客户需求的预测性见解。他们会发现客户行为的趋势，这些趋势可能预示着满意度问题或扩展机会，从而为服务团队提供可操作的情报，而不是原始数据。其结果是，客户服务让终端客户感觉毫不费力、环境友好，几乎无处不在——他们的问题往往在不知不觉中就得到了解决。

在金融服务领域，agent 重新定义了客户服务效率。在处理纠纷确认时，他们会分析交易历史，识别潜在欺诈活动的模式，并自动触发相关的安全协议。在财务规划方面，它们通过关联市场数据、个人客户历史和广泛的经济指标来生成综合分析。如果使用得当，agent 将为企业带来前所未有的后台效率，并为消费者提供下一代零售银行业务、投资指导和财富管理体验。

第二阶段：“复音”人工智能——无缝合作者



这一阶段引入了同一公司内专业 agent 之间的协调合作，共同致力于实现共同的业务目标。在这种情况下，「管弦乐演奏家」agent 会协调多个专家协同工作，这就好比餐厅总经理如何协调有才能的主持人、服务员、经理、厨师和预备厨师等共同工作，以获得令人羡慕的米其林星级。

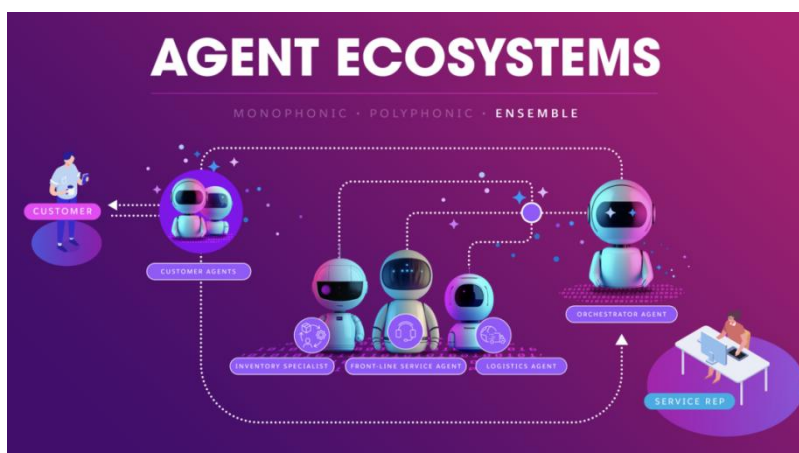
对于复杂的业务运营来说，“复调”人工智能是什么样的呢？考虑一下这样一种客户服务场景：多个 agent 协同工作，为零售客户要求调换淡季 SKU 尺寸的票据提供支持。

- 一线服务 agent 处理最初的客户询问
- 库存专员检查各地的产品供应情况
- 物流 agent 计算运输选项和时间安排
- 计费专家审查账户历史和付款选项

最重要的是：协调 agent 可以将所有这些输入信息协调为一致、有效、符合品牌形象且与上下文相关的响应，供人类审查、完善并与客户分享。

如果实施得当，这种由“协调 agent”为“协调人类”服务的多 agent 方法将带来强大的人工智能驱动优势：系统通过利用专注于特定领域的专业化、可信赖的 agent 来提高可靠性，同时减少幻觉，因为每个 agent 都在特定领域内运行。这种分布式方法还能将敏感数据的处理隔离给特定的 agent，从而加强安全性。也许最重要的是，该生态系统提供了无缝的可扩展性——组织可以根据需要不断添加新的专业 agent 来扩展功能。

第三阶段：“合奏”人工智能——企业协调者



最后阶段（一个理想阶段）增加了跨越组织边界的复杂 agent 到 agent (A2A) 互动，创造了全新的业务关系模式。除了传统的 B2B 和 B2C 模式，我们还看到 B2A（企业对 agent）甚至 B2A2C 互动的出现，在这些互动中，agent 充当工作和交易的中介。

考虑一个简单的租车场景：客户的个人 agent 与租赁公司的商业 agent 进行谈判。客户的 agent 会优化价格和价值，而租赁公司的 agent 则希望通过附加服务实现收入最大化。但是，业务必须在激进的销售策略与将交易拱手让给竞争对手的风险之间取得平衡。这些互动可能受复杂的“博弈论”原则支配，需要优秀的谈判技巧和协议、不确定性下的风险管理、确保信任的验证机制，更不用说巧妙解决冲突的能力了。

现在，想象一下我们在各行各业看到的日益复杂的企业流程：从供应链优化到客户体验编排。无论你是消费者还是企业员工，“合奏”人工智能都将为你提供一个助手，帮助你根据自己的个性化需求和愿望执行复杂的编排和有意义的协作。为了实现这一目标，我们人类还有很多工作要做。

必要条件：信任和问责

随着我们部署越来越复杂的 agent 系统，每项决策都必须遵循两个基本原则：信任和问责。

建立信任

agentic AI 时代的信任远远超出了防止毒性、偏见和幻觉的技术保障。Salesforce 最近的研究表明，61% 的客户认为人工智能的发展使可信度变得比以往任何时候都更加重要——他们是对的。我们正在进入一个需要对人类和人工智能之间的共生关系有深刻组织信任的领域。

这种信任建立在四个重要基础之上。

首先是准确性和边界的基石——agent 必须在明确定义的参数内运行，同时保持准确性。除了防止出错之外，这些防护栏还将创建可预测、可信赖的合作伙伴关系，从而增强集体智慧。同样关键的是 agent 的自我意识。与任何有价值的同事一样，agent 必须认识到自身的局限性，并知道何时需要借助人类的专业知识。这就需要复杂的切换协议，以确保人工智能和人类智能之间的无缝协作。例如，我们的人工智能研究团队探索了训练方法，教授 agent 标记不确定区域，并在遇到未知挑战时寻求帮助。经过正确训练后，人工智能将知道何时不应尝试猜测，而应向人类寻求帮助。

对于多 agent 系统，我们还需要全球公认和采用的参与协议。可以这样想：银行有全球协议或规则，使个人、企业和国家之间的资金转移系统化。交通有协议来确保遵守规则，由我们通用的交通指示灯颜色系统管理。互联网有“IP”——我们的全球互联网协议，允许数据包的路由和寻址穿越网络，并到达正确的目的地。

因此，未来的 agent 也需要这些协议，这些协议应该得到普遍认可和实施，以便协调 agent 能够安全、合乎道德地与其他企业 agent 进行沟通、协商和合作，并使双方互惠互利。这种“合奏”级别的参与必须快速、高效和公平。如果没有这样的协议，往好了说，我们会面临 agent 与 agent 之间的“垃圾邮件”风险，往坏了说，我们会面临欺诈和其他危险。

最后，随着我们的 agent 队伍不断壮大，我们的安全措施也必须跟上。与任何技术一样，怀有恶意的人类也可能利用人工智能，设计和训练“人工智能蠕虫”，以达到数据泄露的目的，或试图劫持其他 agent，泄露客户的私人数据。加强保护、隐私控制和持续监控绝不能被视为单纯的技术要求，它们对于维护信任至关重要，而这种信任能将人工智能从我们使用的工具转变为我们企业共同成长的合作伙伴。

确保问责制

随着企业部署每秒可以做出数千个决策的 agent，我们必须建立明确的问责和监督框架，以确保在出现问题时有一个应对计划。这需要一种全面的方法。以下是企业高管监督 agent 实施工作的出发点。

明确 agent 决策的责任链。当 agent 做出重要决定时，谁应该对此负责不应该含糊不清。这甚至意味着要设立“人工智能运营官”这样的新角色，他们既有权监督 agent 的部署，又要在出现问题时承担责任。

强大的系统，用于检测和纠正不完整的信息、偏差、幻觉或有毒输出，以防它们影响你的业务。这不仅包括基本的安全检查，还包括对 agent 决策的持续监控、实时干预能力和系统审计跟踪。我们的研究团队最近在检索增强生成（RAG）方面取得了进展，极大地改进了人工智能系统访问和验证信息的方式，这只是其中的一个例子。这些创新实现了快速评估和过程修正，确保人工智能系统提供人类和企业可以信赖的准确、可靠的结果。

确定人类监督和干预的程序，平衡自主与控制。我们需要超越“human in the loop”的简单概念，为人类何时以及如何干预 agent 决策制定复杂的框架。正如我的同事 Paula Goldman 所说，这更多的是“human-at-the-helm”。这意味着要制定与 agent 沟通的指导原则和全组织范围内的标准方式，以及明确的升级路径，在日常任务中最大限度地发挥 agent 的自主性，同时在重大决策中保持人类判断的核心地位。

当错误发生时，采取结构化方法纠正错误。这不仅包括技术上的回退程序，还包括明确的客户沟通、补救和系统改进协议，以防止出现类似问题。

新的法律和合规框架，明确解决 agent 的问责。当前的监管环境并不是为自主的 agent 做出商业决策而设计的。我们需要积极主动地与监管机构合作，制定适当的治理结构。

展望未来：科学方法与企业创新

部署真正交互式人工智能系统需要高管的远见：我们必须将产生这些进步的同样严格的科学标准应用到现实世界的实施中。成功不仅取决于部署的 agent 数量或实施速度，还取决于企业领导者和技术专家如何将其与现有的劳动力协议、流程和偏好进行整合。

随着我们对 agent 协作、共享学习和人与人工智能交互的理解不断加深，我们发现了一些原则，这些原则得到了可重复研究和经验证据的支持。未来不是人类与人工智能的对决，而是人类与人工智能的协同合作，发挥各自的独特优势。现在是开始这种转变的时候了，通过仔细的假设检验、细致的测量和基于证据的不断完善，科学方法将照亮我们前进的道路。

正如每一次突破性实验都始于假设一样，每一次成功的人工智能转型都始于一个愿景，并以经过验证的事实结束。

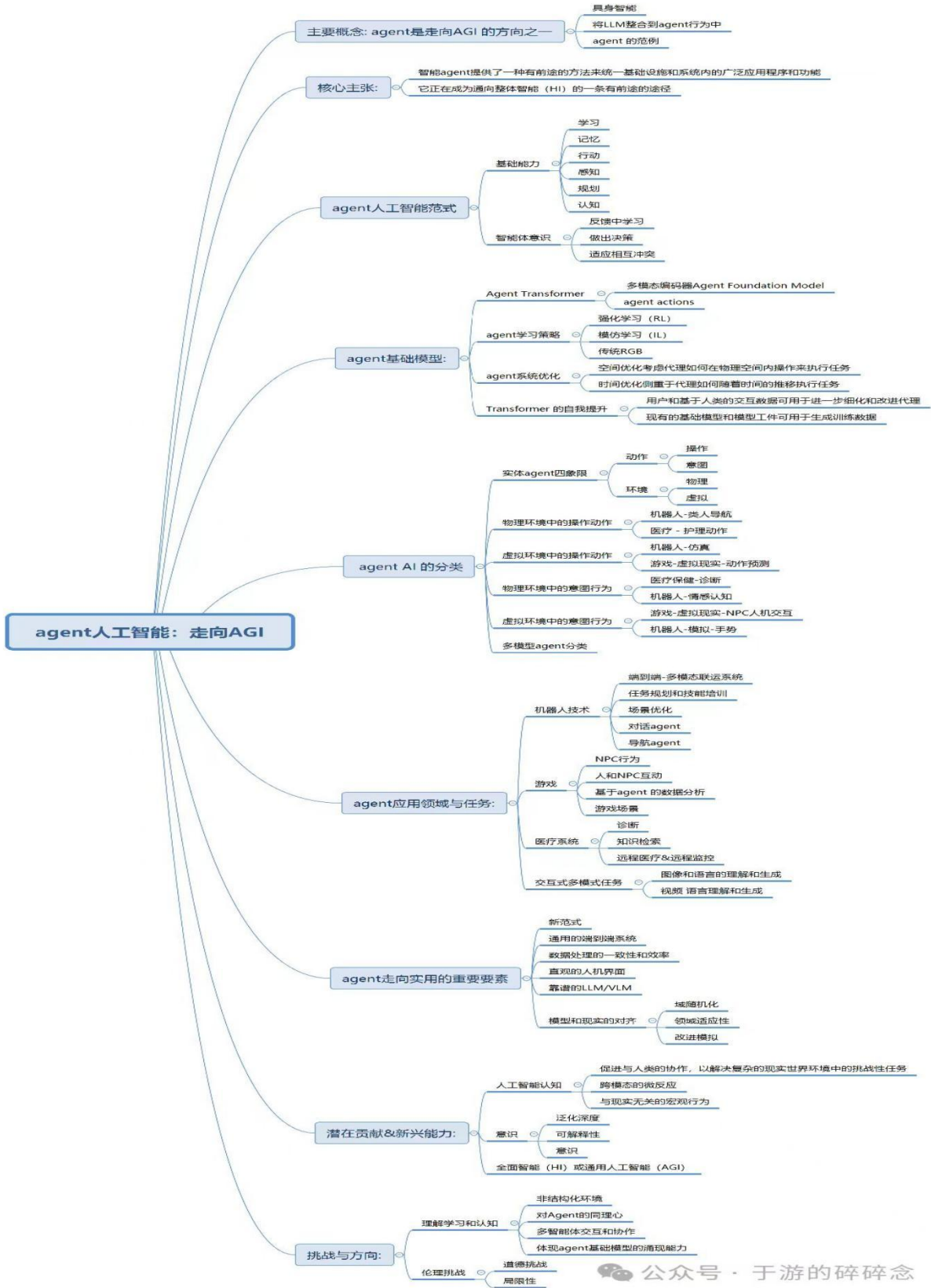
原文链接：

<https://www.salesforce.com/blog/the-agentic-ai-era-after-the-dawn-heres-what-to-expect/>

整理：学术君

Agent 人工智能：走向 AGI

Anna.AI MED ADD



实践 AI Agent 自动化扫描代码库的思考与总结

袁恽

Upgrade Bot to AI Agent, benefit Open Source Communities Agenda

AI Agent模型

实践与具体任务架构

与pipeline相结合

关键点

基于ReAct, ToT等论文的讨论

后续发展与总结

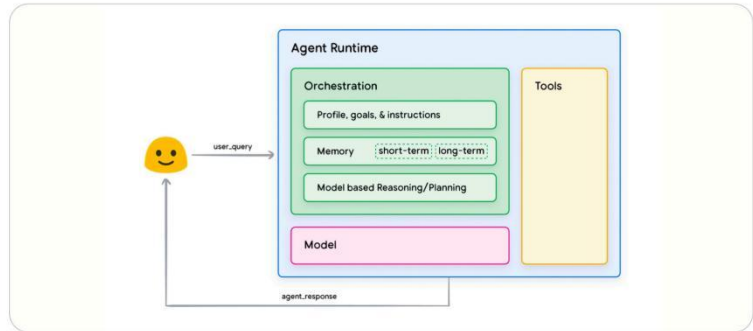
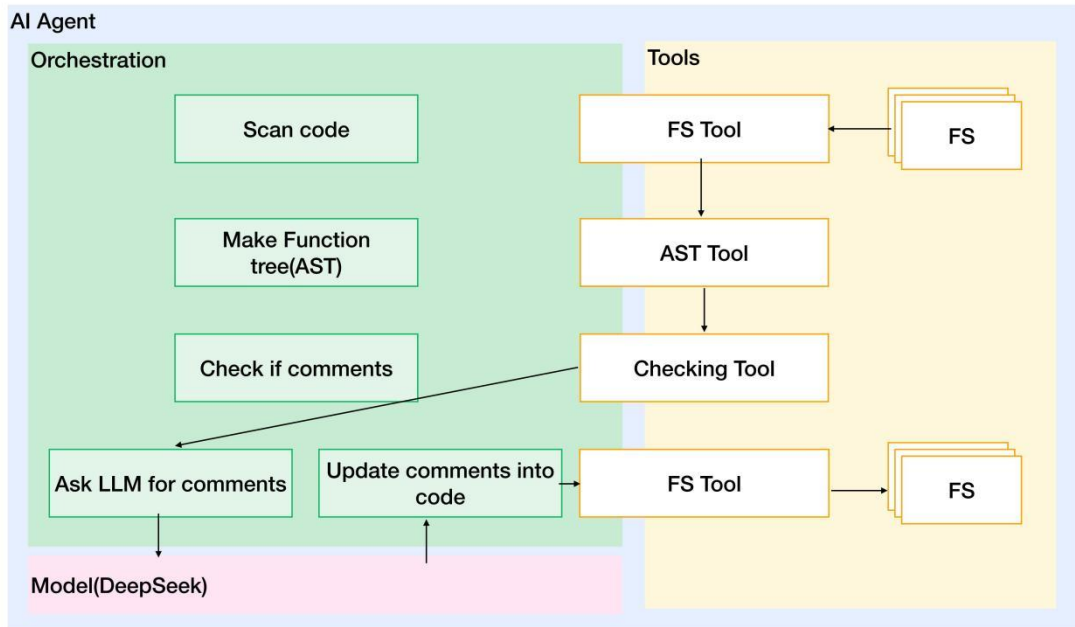
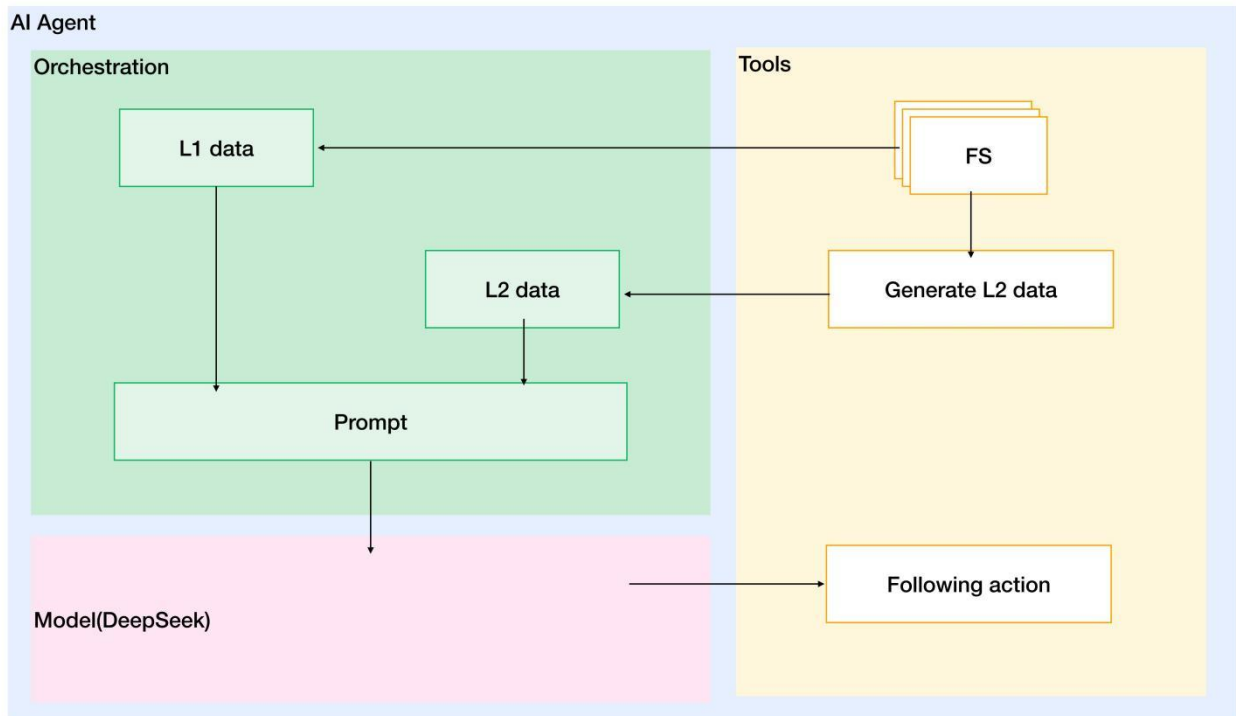
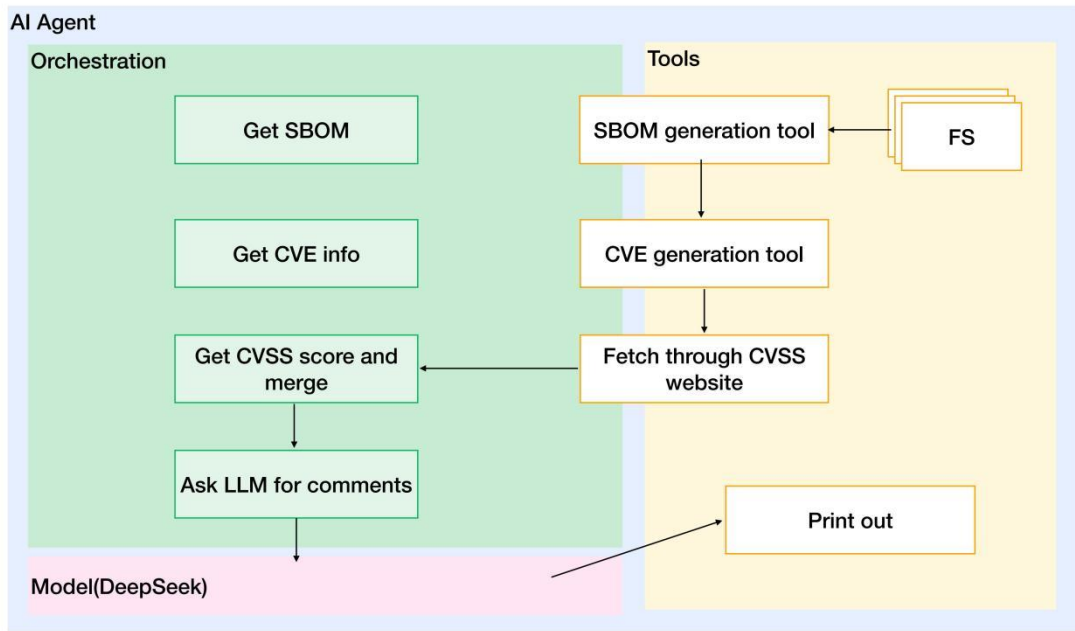
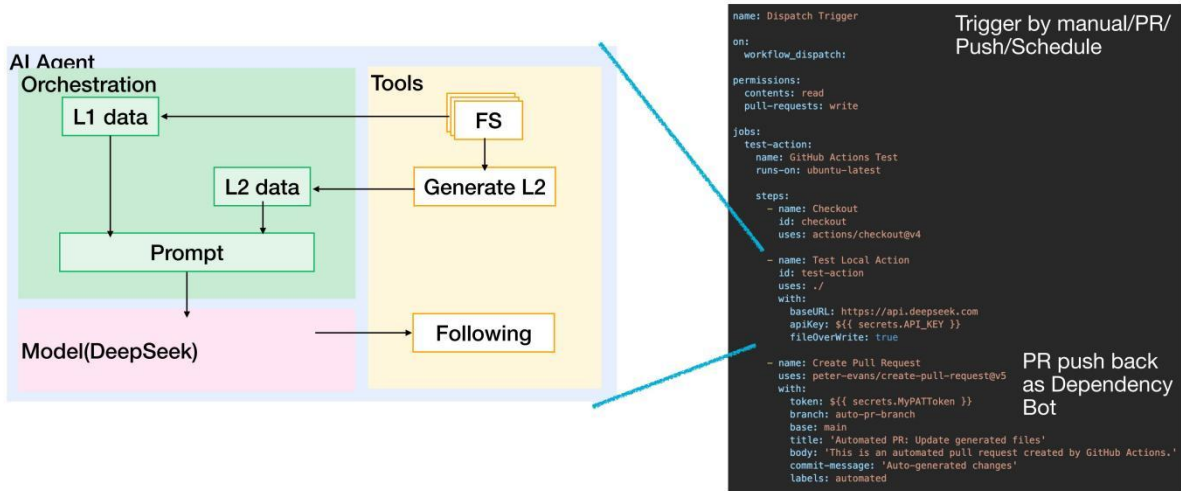


Figure 1. General agent architecture and components





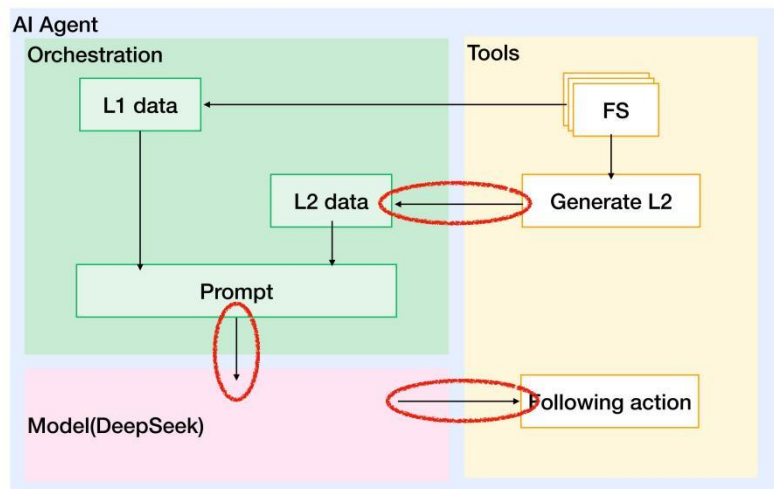
Upgrade Bot to AI Agent, benefit Open Source Communities Running in Pipeline



Upgrade Bot to AI Agent, benefit Open Source Communities

实践过程中的问题

- 意图
- 提示词
- 调用次数
- 对话方式
- 注意力
- 请求大小
- 幻觉



From LLMs to LLM-based Agents for Software Engineering: A Survey of Current, Challenges and Future

Upgrade Bot to AI Agent, benefit Open Source Communities

ReAct论文 提示词有效性?

REACT: SYNERGIZING REASONING AND ACTING IN LANGUAGE MODELS

- 通过可靠的第三方数据从而提高LLM对于问题的理解，提高正确率。论文中使用了Wiki作为第三方外部数据源。

	Type	Definition	ReAct	CoT
Success	True positive	Correct reasoning trace and facts	94%	86%
	False positive	Hallucinated reasoning trace or facts	6%	14%
Failure	Reasoning error	Wrong reasoning trace (including failing to recover from repetitive steps)	47%	16%
	Search result error	Search return empty or does not contain useful information	23%	-
	Hallucination	Hallucinated reasoning trace or facts	0%	56%
	Label ambiguity	Right prediction but did not match the label precisely	29%	28%

Table 2: Types of success and failure modes of ReAct and CoT on HotpotQA, as well as their percentages in randomly selected examples studied by human.

```

import wikienv, wrappers
env = wikienv.WikiEnv()
env = wrappers.FeverWrapper(env, split="dev")
env = wrappers.LoggingWrapper(env)

def step(env, action):
    attempts = 0
    while attempts < 10:
        try:
            return env.step(action)
        except requests.exceptions.Timeout:
            attempts += 1

for i in range(1, 8):
    n_calls += 1
    thought_action = llm(prompt + f"Thought {i}:", stop=[f"\nObservation {i}:"])
    try:
        thought, action = thought_action.strip().split(f"\nAction {i}: ")
    except:
        print('ohh...', thought_action)
        n_badcalls += 1
        n_calls += 1
        thought = thought_action.strip().split('\n')[0]
        action = llm(prompt + f"Thought {i}: {thought}\nAction {i}:", stop=[f"\n"], strip())
    obs, r, done, info = step(env, action[0].lower() + action[1:])
    obs = obs.replace('\n', ' ')
    step_str = f"Thought {i}: {thought}\nAction {i}: {action}\nObservation {i}: {obs}\n"
    prompt += step_str
    if to_print:
        print(step_str)
    if done:
        break
    
```

Upgrade Bot to AI Agent, benefit Open Source Communities

ToT论文 多次调用

Tree of Thoughts: Deliberate Problem Solving with Large Language Models

- 通过不断分析和调用LLM实现树形思维结构（基于CoT-SC，评分思维连的提升）。

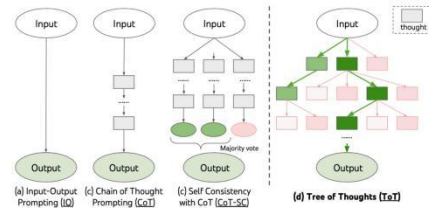


Figure 1: Schematic illustrating various approaches to problem solving with LLMs. Each rectangle box represents a *thought*, which is a coherent language sequence that serves as an intermediate step toward problem solving. See concrete examples of how thoughts are generated, evaluated, and searched in Figures 2,4,6.

Method	Success
IO prompt	7.3%
CoT prompt	4.0%
CoT-SC (k=100)	9.0%
ToT (ours) (b=1)	45%
ToT (ours) (b=5)	74%
IO + Refine (k=10)	27%
IO (best of 100)	33%
CoT (best of 100)	49%

Table 2: Game of 24 Results.

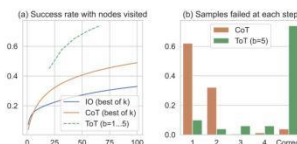


Figure 3: Game of 24 (a) success analysis & (b) error analysis.

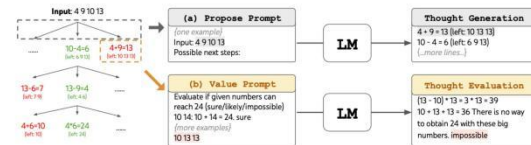


Figure 2: ToT in a game of 24. The LM is prompted for (a) thought generation and (b) valuation.

Upgrade Bot to AI Agent, benefit Open Source Communities

关键是有用——Active RAG? Or One shot Prompt

这是一段C代码，假设这段代码中的任何外部调用都存在指针或者内存泄露的可能，请为这段代码提供修改意见。for (size_t i = 0; i != count; ++i) { if (field->is_optional()) { print(field) } else { Value* field_json = field2json(msg, field, allocator); root->AddMember(name, *field_json, allocator); }

在这段 C 代码中，存在潜在的内存泄漏和指针问题，尤其是在 field2json 函数返回的 Value* 指针可能没有被正确释放的情况下。以下是代码的潜在问题及修改建议：

潜在问题

- 内存泄漏：**field2json 返回的 Value* 指针可能没有被释放。如果 root->AddMember 没有接管 field_json 的所有权，field_json 的内存将不会被释放。
- 空指针问题：**如果 field2json 返回 NULL，直接解引用 *field_json 会导致未定义行为。
- 资源管理：**如果 field2json 分配了内存，但没有明确的释放机制，可能会导致内存泄漏。

修改建议

以下是改进后的代码，增加了内存管理和错误处理：

```

c
for (size_t i = 0; i != count; ++i) {
    if (field->is_optional()) {
        print(field);
    } else {
        // 调用 field2json，检查返回值是否为 NULL
        Value* field_json = field2json(msg, field, allocator);
        if (field_json == NULL) {
            // 处理错误，例如记录日志或返回错误
            fprintf(stderr, "Error: field2json returned NULL!\n");
            continue; // 跳过当前元素，继续处理下一个元素
        }
        root->AddMember(name, *field_json, allocator);
    }
}
    
```

REPOAUDIT: An Autonomous LLM-Agent for Repository-Level Code Auditing

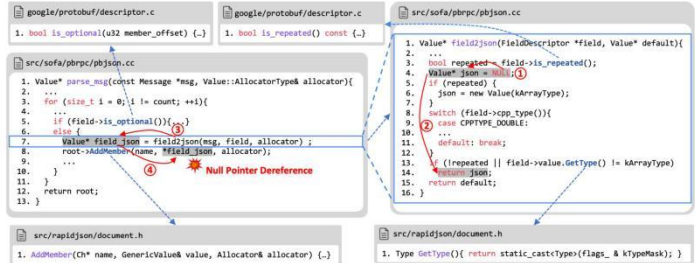
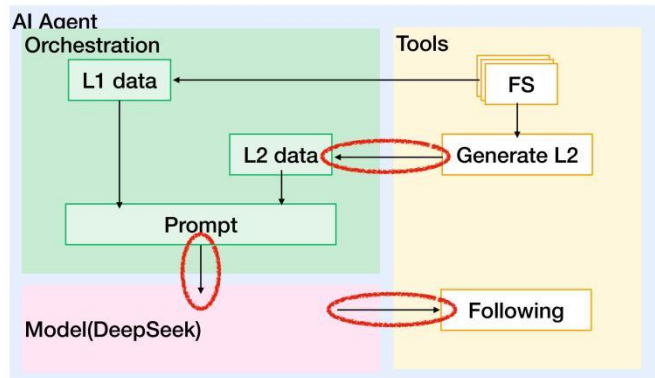


Figure 1. A simplified code snippet from the project sofa-pbrpc contains a real NPD bug found by REPOAUDIT. The blue dashed arrows indicate the edges in the call graph. The red solid arrows show the data-flow facts indicating the null value propagation. The call graph of the project contains 1,508 nodes and 6,196 edges, while its data dependence graph contains 160,875 nodes and 360,096 edges.

Upgrade Bot to AI Agent, benefit Open Source Communities

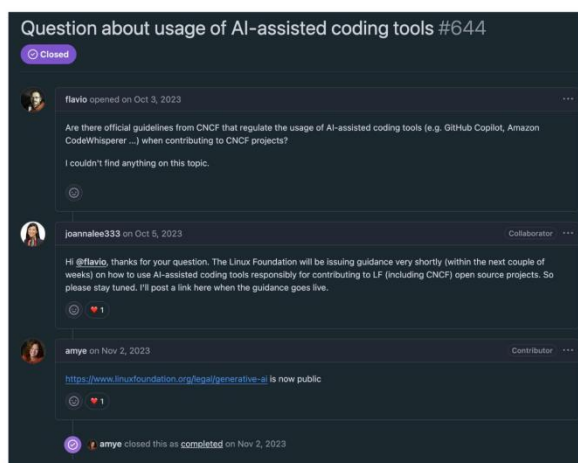
后续发展与总结 指标体系?

- 意图
 - 准确性高是目的，调用次数不是目的
 - 提示词有效性?
 - 可以one shot? 看如何看待思考问题?
 - 提示词组成比例?
 - 以CoT下移到Deep Seek R1来看?
- 对话方式
 - 注意力在有具体任务情境下，可以提高大模型注意力
 - 请求大小，由于服务器窗口大小的存在因此，尽可能给大模型提供具体任务
- 幻觉
 - 输出的有效性?



Upgrade Bot to AI Agent, benefit Open Source Communities

Ethical Considerations



以上内容核心阐述了：

基于开源实践，探讨 AI Agent 如何增强现有代码扫描工具的能力。

目前 AI Agent 的发展趋势与挑战，如工程化与学术论文之间的差异。

尝试通过指标体系，对这些挑战进行量化评估。

AI 伦理道德相较于 AI Agent 自动化领域的空白。

中国 DeepSeek 崛起从震撼硅谷到震撼世界

COPU

中国深度求索（DeepSeek）最近发布 DeepSeek-V3、DeepSeek-R1，Kimi K1.5 三个人工智能模型，震撼美国硅谷，几天以后冲击波震撼世界。

中国 DeepSeek-V3 崛起震撼美国硅谷

去年年底，中国深度求索 AI 初创公司发布 DeepSeek-V3 大模型，在美国独立评测机构 Artificial Analysis 上进行测试，在美国 APP Store 排行榜上排名第一，力压长期霸据榜首的 ChatGPT，美国硅谷好评如潮，认为是一款颠覆性的大模型。彭博社认为，这是中方大模型全面超越美国多款大模型的开端，是中方大模型技术开始碾压美国大模型里程碑式时刻。更为突出的是，根据 DeepSeek-V3 的技术报告，该大模型以低得多的训练成本（采用相当于 A100 阉割版的 H800 低算力芯片，训练成本仅为 550 万美元），训练周期仅 2 个月，其训练后的性能可以比肩 ChatGPT 最新版的大模型（ChatGPT 的训练成本为 1.1 亿美元，为 DeepSeek 的 20 倍）。DeepSeek-V3 研制成功，开辟了采用低资源、低成本训练大模型获得高性能的研制路径。DeepSeek-V3 不同于 ChatGPT，也反映为开源与闭源之争。

DeepSeek-R1、Kimi K1.5 研发成功，缔造出一种高效能低成本研发训练开源大模型产业发展之路

中国深度求索公司随后发布 DeepSeek-R1 推理模型，Kimi K1.5 多模态推理模型，缔造出一种高效低成本研发与训练开源透明的 AI 大模型产业发展之路。

DeepSeek-R1 的训练模式在数学、编程、推理方面非常出色，在实现高水平输出性能时，得益于其独特的思维链，允许模型通过逐步处理查询推理复杂问题。

DeepSeek-R1 推理模型开源软件总体性能完全可以比肩闭源的 OpenAI 的 GPT o1 正版大模型，这是一款从低资源训练出高性能的模型。同时发布开源 Kimi K1.5（月之暗面）多模态推理模型，其文本和视觉多模态推理性能已追上闭源的 GPT o1，而在快速推理思维链（短模型或短思考模式）下，K1.5 的性能已大幅领先于 GPT-4 和 claude 3.5，在综合分析和 AIME 榜单上，Kimi K1.5 对美方最先进模型进行断崖式的碾压。

DeepSeek-R1 与 Kimi K1.5 研发成功，缔造出一种高效低成本研发、训练开源透明的大模型产业发展之路。美国各家 AI 专业媒体纷纷惊呼：美国 AI 产业已经输了头筹。

DeepSeek-V3、DeepSeek-R1 与 Kimi K1.5 研发成功，形成了人工智能发展的全新思路

DeepSeek-V3、DeepSeek-R1 与 Kimi 1.5 研发成功，缔造出一种高效、低成本、开源透明的大模型生成和发展机制，冲击美西方所谓发展 AI 产业必须奉行“大力出奇迹”的发展思路，是美西方所谓通过高性能 AI 芯片才能堆叠算力，只有大量算力中心堆砌才能训练大模型，这种通过高投入低效率来获得大模型的思路是不可持续的。从而打破美西方垄断全球人工智能的局面，引起了他们的焦虑和恐慌。

DeepSeek-V3，DeepSeek-R1 与 Kimi 1.5 研发成功，产生了四大效应：

- 1) 英伟达算力帝国及其市值的崩溃
- 2) 为华为昇腾芯片带来数量可观的订单（深度求索创始人梁文锋说，在训练 DeepSeek AI 大模型时并未采用英伟达芯片，而是选用华为的昇腾 AI 处理器）
- 3) OpenAI 市值崩盘并出现泡沫
- 4) 未来 AI 发展方向将由中国引导而并非美国领导

深度求索创始人梁文锋接着谈他们进一步工作，他们在做四件事：

- 1) DeepSeek 研发团队人员不走了，这样创新技术有保障
- 2) 加大对 DeepSeek AI 的投入，从硬件、规模、算力等各方面提升，让 DeepSeek AI 成为公司的中流砥柱。
- 3) 加强与华为、阿里、百度、字节跳动等企业的合作，推动国产化进程
- 4) DeepSeek 不融资、不上市、保持独立，让技术探索有足够多的时间和空间

DeepSeek AI 创新的技术特色

深度求索初创公司研发的 DeepSeek AI 改变了 AI 大模型的研发模式，打破了 AI 大模型的研发壁垒，走出了一条 AI 大模型的研发新路。

DeepSeek AI 创新的技术特色概括如下：

1) 实行高起点创新

瞄准 AI 大模型架构的核心技术进行变革创新，实行跨时代颠覆性 0→1 的创新。

2) 利用数学和编程知识，解决如何减少训练资源支持高性能的核心算法，实行其独特的思维链，走出一条低资源、低成本、开源高效、高输出、高性能 AI 大模型之路（打破美西方高投入、大算力、强训练，闭源、低效，高输出高性能的研发 AI 大模型之路）。

3) 推进多角度的综合创新

a) AI 大模型将以更强的技术、更好的市场策略、更快的迭代等多角度创新。

b)吸取开闭源历史的经验教训，开源创新推动数字化转型或智能化重构，高举开源旗帜处理好开源核心的开放创新和开源的商业模式的关系，发挥开源的作用：算法的创新和计算生态的重构。

深度求索公司创始人梁文锋说：“开源可是技术进步的命根子”，在开源的 DeepSeek AI 冲击下，Open AI 公司创始人奥特曼（Sam Altman）罕见的表态：OpenAI 由于违背初心执行闭源策略，“在开源软件方面一直站在历史错误的一边”（他们拟于不久从发布 GPT o3-mini 序列开始推出开源推理模型）。

人工智能大师杨立昆（Yaun LeCun）指出：“DeepSeek 的成功是开源模型正在超越专有模型”（注：专有模型即闭源模型）

并发挥类脑的神经拟态（比数字算力效率高）多元支持推理模型的作用。

DeepSeek AI 研发成功冲击了纳斯达克股市

1月17日纳斯达克100指数下跌5%，股市损失万亿美元。

英伟达股市收盘跌幅12%（一度下跌17%），单日蒸发6000亿美元，引发了美股（半导体股、科技股）全面暴跌：其中博通跌17%，市值蒸发2000亿美元，阿斯麦跌5%，台积电跌13%，市值蒸发1500亿美元，超威、微软、谷歌等股市市值也大幅下跌。

DeepSeek AI 的社会影响

从震撼硅谷到震撼世界

DeepSeek AI 的崛起不但改变了 AI 的创新之路，冲击纳斯达克股市，震撼硅谷，几天后又震撼世界，对社会产生深刻的影响。

美国总统特朗普1月27日说，中国初创企业深度求索（DeepSeek）公司的技术应为美国企业敲响警钟。中国企业想出以更快的发展 AI 方法是好事，我们需要专注于竞争以赢得胜利。后来特朗普还威胁说，中国如果不出售 DeepSeek 给美国，我们就加税。美国白宫新任新闻秘书卡罗琳·莱维特举行她首次新闻发布会时，提到中国 AI 初创公司深度求索，她表示：特朗普总统认为该公司发布的 AI 模型是对美国 AI 行业的一个警钟。她接着说，我们正在努力，确保美国 AI 的主导地位。总统此前签署行政命令，撤销了对 AI 行业的一些繁琐监管。

俄罗斯外交部部长拉夫罗夫1月29日谈：中国的 DeepSeek AI 模型超越了美国。

意大利总理梅洛尼率先跳出来封禁 DeepSeek，后来发现英伟达、谷歌、亚马逊和微软等美国 AI 头部企业连夜接入 DeepSeek 大模型，意大利反而成为孤家寡人，她还指使该国隐私监管机构 Garante 向深度求索索要 DeepSeek 的数据，并就个人数据使用问题作出解释。

Meta CEO 扎克伯格关注 DeepSeek Aide 重磅发布，表示非常重视中方研发 AI 的进展更加节省能源和投资，他说 DeepSeek 将改变一切。他在 1 月 26 日公开表示东大（指中国）在大模型领域的投入太卷了，影响了美国的领先优势，是人工智能领域的巨大威胁。值得指出的是，无论 DeepSeek-R1 还是 Kimi K1.5 都是在相对较低成本、短时间和较低算力下训练出来的，其总体性能达到或超过美方人工智能领域剧透花费数十亿美元，甚至上百亿美元的巨额资金，花费几个月才训练出来的大模型，这对美国人工智能产业来说就是晴天霹雳，它带来的冲击必然将让全球人工智能产业发展进行新一轮洗牌。美国在人工智能领域所谓的领先地位已经不复存在。冲击美方人工智能的发展思路，美国企业构筑以 AI 芯片、大算力集群，以及巨额投资为基础的大模型技术门槛瞬间被打破，而美国一直对中国全方位算力限制已经毫无意义。

但扎克伯格在美国国会听证会上作证发言时，担心 DeepSeek AI 威胁到美企在行业中的领先地位，他主张对华进行限制打压。

Meta 首席科学家、图灵奖获得者 Yann LeCun 认为，DeepSeek 的成功不应该被误解为“中国超越美国 AI”，而是“开源模型正在超越专有模型”。（编者注：专有模型即闭源模型）。

美国企图封杀 DeepSeek 行将破产

美国候任商务部部长卢特尼克在美国国会听证会上作证时，针对深度求索公司研发的 DeepSeek，定性为中方窃取美方技术。这与美国之前启动的国家安全调查前后呼应，企图一举封杀 DeepSeek。

但是一个更大的噩耗传来：中国知名的大型科技企业阿里云发布了与 DeepSeek 同等的 Qwen 2.5-Max 旗舰大模型（其性能还超越 DeepSeek-V3，以及 OpenAI 的 GPT-4.0、Meta 的 Llama 3.1-401B）。而且字节跳动也推出与 DeepSeek 同等性能的豆包 1.5pro，它们在知识、编程、基准测试等方面全面超越美国生成式大模型。这样，中方有比 AI 初创企业研发的 DeepSeek 单一模型大得多由多家大型科技企业研发的同等性能的大模型，对美方来说是一个更大的噩耗，将宣告其封杀 DeepSeek 的破产。

DeepSeek 与华为、腾讯联手：中国 AI 大模型开启“铁三角”时代

在全球 AI 竞争进入到白热化关键节点，中国科技巨头华为、腾讯与专注 AI 大模型的 DeepSeek 达成战略合作。此次合作不仅为中国大模型赛道注入了新动能，更有可能重塑全球 AI 竞争的格局。

1) 合作逻辑：互动性资源构建闭环生态

a) 华为硬件底座的优势：昇腾 AI 芯片、Atlas 服务器集群、华为云提供国产化算力保障

b)腾讯场景入口价值：微信、游戏、金融等场景的海量数据和商业化通道，可促进大模型迭代

c)DeepSeek 的技术纵深：其在垂直领域的大模型（如 Moonl shoot）的积累，可补充华为、腾讯在专业赛道的能力短板

2)对 DeepSeek 的跃升效应：从技术突围到商业破局

“铁三角”合作将深度改变这家 AI 独角兽的发展轨迹

可进一步削减算力和训练成本，使模型迭代速度倍增，可打通商业化路径，可扩大 DeepSeek 生态，在政务、医疗国产化领域内构建护城河。

3)对海外模型进行战略挤压

4)未来变局：AI 竞争进入生态对抗时代

从“单兵”突破到“军团”作战，面对未来胜负手中以制胜。

我为什么写支持 DeepSeek 的文章

陆首群

梁文锋团队作出了国运式的贡献

自 AI 初创公司深度求索梁文锋研发团队推出 DeepSeek (DS) 以来，震撼硅谷继而震撼世界，好评如潮。国内有两件重要的正面反应：有人认为这是一件国运式贡献，还有人认为这是自 1840 年以来我国自主研发创新的技术首次冲击全球舆论。

美国权威专家驳斥所谓 DS 抄袭 OpenAI 平台上的数据

近来也听到一些负面的反应、质疑之声，使有些人无所适从：有人说 DeepSeek 是窃取 OpenAI 平台的数据，这个说法出自奥特曼和极少数 AI 专家之口，他们认为 DeepSeek 采用蒸馏技术偷师 OpenAI，为此我曾引述全球最大的开源社区 Stability AI 创始人 Emad Mostaque 的谈话，他说 DeepSeek 没有抄袭，不要再质疑了！他从 DeepSeek 发表的论文中抓到依据，表示那些指责的原因，简直是对强化学习的侮辱！这相当于 AlphaGo 棋局中自己和自己下棋而已，根本不需要偷师一样，那些说抄袭的人恐怕自己都没见过强化学习暴走模式。

近日奥特曼已不再指责 DS，而是赞扬有加，但随着专家退场政府上阵，白宫人工智能政策特别顾问戴维·萨克斯 (David Sacks) 发言，有证据表明 DS 盗窃 OpenAI 的知识，指责深度求索公司通过非法手段获取 OpenAI 的专有数据用于模型训练。我不明白 OpenAI 的当事人 (专家) 不再质疑了，而这位没有信誉不懂业务的政府高官跳出来指责，不感到奇怪吗？！

讨论纽约大学的教授对 DS 点评的意见

纽约大学名誉教授 Gary Marcus 在《Fortune》杂志上发文对 AI 聊天机器人 DS 提出 8 项点评意见，我觉得他并不怀疑 DS 的测试数据，也不怀疑其以低成本、高效率、高智能走出一条发展 AI 的新路，但他表示 “虽然 DS 进步快，但这并不意味着中国的 AI 在技术上已超过了美国，还存在很大差距”，这是对的！说明年轻的 DS 还需要坚持创新进步提高大模型的智能 (从另一个角度讲 DS 还有发展潜力)。我曾向他们建议，要对计算架构关键技术进行深度研发创新 (研发跨时代、颠覆性 0→1 的创新成果)。而该教授还提出美国想投资 5000 亿美元建设星际之门计划可能没有太大意义，他是对的！他也知道美国对相关研发花巨资可能产生浪费？！他对英伟达的霸主地位受到威胁，认为是市场的合理调整，他似乎也担心美国是否会失去 AI 行业内的领先地位。

华为、腾讯与深度求索进行 AI 大模型发展的战略合作

他们三家组成战略合作的 “铁三角”，变 “单兵作战” 为 “军团作战”。

① 开启 “铁三角” 合作时代，互补性资源，构建闭环生态。

华为具有硬件底座优势，腾讯具有扩大生态及场景入口价值，深度求索深耕 DeepSeek 效应。

② 大胆设想，铁三角联手，提高研发通用人工智能专业赛道的竞争力。

我祝贺他们合作事业成功！

回复马斯克的怀疑

关于马斯克怀疑 DeepSeek-V3 只花 600 万美元很低的成本，其训练后大模型的智能却能达到 ChatGPT 最新版本同等的水平。

我在一篇文章中是如此协助 DS 作出解释的：其实这个怀疑很容易解决，从硅谷独立测评机构的测试报告中便可获知。

后来我看到梁文锋回答马斯克的疑问为什么 DeepSeek 能以低成本、低投资，进行高效率训练，并能获得如此高智能输出？梁文锋回答是：一般 AI 大模型训练费用高昂，原来与语言差异密切相关！英语冗长繁琐，而汉语简洁明了，学习成本更低。在专业词汇方面，汉语造词能力更是令人惊叹：通俗易懂，助力科技发展。梁文锋一语惊人，马斯克恍然大悟。

如何看待李飞飞等研发 S1 推理模型的目的

李飞飞大师等斯坦福大学、华盛顿大学的研究人员，于 2 月 6 日，仅用不到 50 美元的云计算费用，训练出一个名为 S1 的 AI 推理模型，该模型在数学和编程测试中表现与 GPTo1 和 DeepSeek-R1 顶尖的推理模型相似的水平，它是从谷歌的 Gemini2.0、Flash Thinking Experimental 模型中提炼出来的，使用 16 个英伟达的 H100 GPU，训练 26 分钟。

S1 是不是碾压了 DeepSeek？不是！S1 只是验证 DeepSeek 所开创的低成本发展 AI 之路是成功的，并且还有很大发展潜力，同时它也与 DS 一样打脸以数千亿美元的巨额投资训练 AI 模型来发展 AI 之路是不可取的！

（注：有人说李飞飞叫板梁文锋，S1 仅用 50 美元及更短时间蒸馏出类似 DeepSeek-R1 的推理模型？我如上已说，S1 是验证 DeepSeek，不是竞争！为此在注解中说明 S1 的细节，与 DeepSeek 不具竞争的可比性。原来他们训练出新的只有推理能力的 1000 个样本是从谷歌模型中提炼出来的，然后在中国阿里云 Qwen 2.5-MAX 大模型基础上进行微调而已。）

李飞飞公开说明，她训练 S1 不是从 0 开始，数据取自谷歌，训练是在阿里云 Qwen 大模型上进行微调，S1 无意与 DS 竞争，而是验证 DS 开创的一条发展 AI 的新路是成功的。

引入类脑算力可进一步提升 DS 低成本高效率发展 AI 新路

发展 AI 一般采用投入巨资、堆叠算力，在低效率下，争取提升大模型智能水平之路。这里的算力是基于数字化的。

而从提高效率的角度来看，效率是按如下路线呈梯度提升的：数字化算力 → 类脑算力 → 大脑算力。因此，类脑（即神经拟态计算系统）算力如果取代单纯的数字化算力，完全可能进一步提升由 DeepSeek 展示的以低成本发展 AI 过程中的效率。

以算力驱动推理，而推理是生成的基础，在发展生成式大模型过程中，提高效率是实现低投入高产出的关键。

重点针对计算架构核心技术实行跨时代颠覆性（从 0 到 1）的变革创新

我曾建议深度求索公司针对计算架构核心技术实行颠覆性创新，以提高大模型的智能水平。

坚持开源创新，可以构建具有“基于知识社会的创新 2.0”机制的现代创新引擎。为充实创新引擎，要建设具有交互作用的两个空间：即现实的物理空间（physical space）和虚拟的数字空间（Cyberspace）。前者是适应现实的低阶社会，将储存表征计算架构的业态，后者为设计中的虚拟的高阶社会，储存用以改造计算架构的超级动能。实现计算架构业态变革的操作步骤为：将虚拟的数字空间中的超级动能作用于现实的物理空间中的计算架构业态，促使其发生数字化转型或智能化重构。

创建通用人工智能

在梁文锋的多次发言中谈到，他发展人工智能目标的重点是创建通用人工智能（AGI）。

通用人工智能的演化路径为：语言大模型 → 多模态大模型 → 具身大模型 → 世界模型 → 通用人工智能。

建议深度求索公司要制定发展规划。

美国企图封杀 DeepSeek 行将破灭

美国候任商务部部长卢特尼克在美国国会听证会上作证时，针对深度求索公司研发的 DeepSeek，无端定性为中方窃取美方技术。这与美国之前启动的国家安全调查前后呼应，妄图一举封杀 DeepSeek。

但是一个更大的噩耗传来：中国知名的大型科技企业阿里云发布了与 DeepSeek 同等的 Qwen2.5-Max 旗舰大模型（其性能还超越 DeepSeek-V3，以及 OpenAI 的 GPT-4o、Meta 的 Llama 3.1-40B）。而且字节跳动也推出与 DeepSeek 同等性能的豆包 1.5pro，它们在知识、编程、基准测试等方面全面超越美国生成式大模型。这样，在现时中方有比 AI 初创企业研发的 DeepSeek 单一模型更多的由几家企业研发的同性能的大模型，对美方来说是一个更大的噩耗，将宣告其封杀 DeepSeek 的破产。

由深度求索梁文锋团队独创的 DeepSeek 其重大意义是开辟了一条以低投入（低成本、低资源），通过高效率导致高产出（高智能）研发人工智能的新路。

2 月 8 日特朗普下令不准再打压 DeepSeek，《纽约时报》揭秘：因为在华经营多年的美国汽车巨头福特公司 CEO 吉姆·法利的报告：中方在电动汽车电池技术方面已领先美国约 10 年（而白宫认为目前 DeepSeek 只与美国 AI 大模型技术水平持平或至多领

先 3 - 6 个月），白宫如果能让美国汽车产业 “再次伟大”，就必须与中国合作，从而获得授权许可（电动汽车电池的知识产权）。如此，白宫收到一个更大的噩耗，迫使特朗普作出如此决定。

（中方对特朗普这次放弃对 DeepSeek 的打压政策并不可信，并要听其言观其行！）

DeepSeek 证明:开源是主导科技市场的秘诀

(华尔街的看法是错的)

Jim Zemlin

我很少写博客或在社交媒体上发帖,但我确实为我们的员工和董事会写一份每周的私人新闻稿,并且连续几周都在写关于 DeepSeek 的内容。我没有考虑到的是本周在媒体和市场上的反应。Ben Thompson、Pat Gellisnger、Tomasz Tunguz 等优秀人士都在评论。由于 AI 股票受到重创,并且对 DeepSeek 的 R1 模型对 AI 未来的影响浮出水面,很明显,对 DeepSeek 的担忧触动了人们的神经。这种巨大的反应值得我们审视和解释。

简而言之,市场反映的是 DeepSeek 能够以极低的成本,用极少的算力,构建出一个可以与 OpenAI 复杂的 o1 推理模型和 Anthropic 的 Sonnet 模型相媲美的模型。而且,DeepSeek 似乎是使用众所周知的技术做到的。没有重大的算法突破,只有非常聪明的工程设计。该团队只是回到了第一性原理,提出了基本问题,并以新颖的方式堆叠现有技术,使用强化学习 (RL) 和各个阶段的微调,实现了超额的结果。这里没有魔法——只是对现有牌组进行了非常巧妙的重新洗牌,从而产生了更精致和高效的结果。

一些观察家指责 DeepSeek “免费搭车”,利用 Meta (Llama) 和 AliBaba (Qwen) 等大型模型制造商的工作成果。然而,这种观点反映了对开源系统运作方式的误解。开源创新的基本原则是期望其他人能够在先前的工作基础上进行构建,以推动进步。以 DeepSeek 为例,他们通过提炼其基础推理模型 DeepSeek-R1 (他们早期开源模型 DeepSeek-V3-Base 的演进) 并使用其基础模型生成的推理数据,对 Llama 3 和 Qwen 2.5 系列的较小模型进行微调,从而证明了这一点。这个过程突显了 DeepSeek 如何利用现有的开源创新,而不仅仅是复制,而是为了展示小型语言模型性能的显著改进。然后,DeepSeek 将这些模型重新发布回开源 AI 社区。

重点是:新闻和评论员们忽略了 DeepSeek 为开源以及更广泛的开放运动所开启的巨大机会。太多的对话都以美国与中国之间的竞争以及 AI 霸权之争为框架。太多的对话都基于这样一种观点,即 DeepSeek 以极低的成本和极少的算力训练出一个强大的模型,意味着所有在 NVIDIA 设备和训练上花费巨额资金的大公司都将被削弱。

在我(带有偏见的)看来,开源创新将会胜出,而且这对每个人都有好处——中国、美国、大型科技公司、欧洲数字主权、NVIDIA 等等。一些投资于早期 AI 初创公司的风险投资者可能会被淘汰,但这种情况在任何技术转型阶段都会发生。DeepSeek 证明,我们需要成千上万的人关注这个问题,才能提出更好的解决方案,使智能尽可能接近免费。中国的一个小团队以全新的视角审视了一个问题,并提出了一种新颖的方法,将思维链推理的成本降低了 50 倍(如果 DeepSeek 的帖子是准确的),然后发表了一篇论文,完整地描述了他们的过程,使社区能

够从他们的学习中受益。我们需要更多这样的进步，而不是更少。这不是美国和中国之间的军备竞赛。这是开放力量和封闭力量之间对开放市场的争夺。政府可能认为他们可以控制这一点，但历史表明，开放技术一旦被发现并掌握在社区手中，就像雨水一样。你无法暂停或阻止它。人为地阻止科学发展在任何长期来看都从未奏效，计算机科学和 AI 也不例外。

2013 年 3 月，开源世界引入了一种轻量级、标准化的方式来打包和运行应用程序及其所有依赖项，从而确保了不同环境中的一致性。与传统的虚拟机不同，容器使用单个底层操作系统上的隔离环境来进行虚拟化。容器通过共享主机系统的内核同时隔离进程，从而更快、更便携、更高效。容器重组了许多现有的开源虚拟化和容器功能，如 `cgroups`、`LXC`、`namespaces` 等。这种重组，或者说对当时现有牌组的重新洗牌，改变了游戏规则。虚拟机多年来一直运行良好，但容器在许多工作负载方面都远胜一筹。这种技术转变的开放性帮助推动了新一波云原生计算的采用。

另一个根本性的误解是，DeepSeek 将减少对 AI 基础设施的投资需求。然而，人们对智能的需求是无限的。我们甚至还没有触及表面，并且正处于利用 AI 驱动的应用程序的早期阶段。

AI 模型最近的改进已经将推理的重心从预训练和后训练的增强转移到现在的测试时计算，允许模型通过它们的响应进行“推理”（思维链）。这并不意味着我们需要更少的计算。实际上，这意味着我们需要更多的计算，当推理层更像人脑一样——总是在思考、重新考虑、同时处理多个任务，并不断发展以满足对新智能活动的需求时。这更像电力——一种商品。使其更便宜，以便更多的应用程序成为可能（正如风险投资家 Tomasz Tungus 在此^[1]简洁地解释的那样），并且更多的人会使用它。

对于开源来说，这开启了一个巨大的新领域。如果开源在 AI 领域获胜并成为主要的创新和开发模式，那么我们就有机会从根本上重塑世界运作的方式。DeepSeek 是使推理可供更广泛的用户和应用程序使用的一个例子。开源 AI 可能是实现应用程序和应用程序堆栈之间真正互操作性和标准的途径。

AI 是一个元层，我们可以基于它构建对互操作性的新期望，Satya Nadela 在多个论坛上暗示了一种新的现实，即 AI 如何通过允许组织将不同的后端和数据源连接到 AI 引擎来颠覆 SaaS 应用程序。换句话说，开源 AI 让世界有机会重写规则，以尽可能地支持一切开放。在这个世界里，权力归于社区和维护者。

当然，关于开源及其运作方式有很多细微之处。但通过这个视角，我相信 DeepSeek 的教训是关于即将到来的 AI 繁荣，以及如果我们保持开放，它如何能够使每个人受益，并推动超出市场认知的经济和技术进步。

不相信我吗？Linux 已经有 34 年的历史了，滑铁卢大学的一组研究人员在[上周](#)^[2]的公开演示中表明，“更改 Linux 中的 30 行代码可以将某些数据中心的能源使用量减少多达 30%”。猜猜所有这些 AI 工作负载都在什么操作系统上运行？

最后，我要对所有“特洛伊木马”式的、不明真相的反对者们做一个小小的预测。在接下来的几周内，另一家公司或研究实验室将使用类似的方法开发出具有惊人性能成本比的模型。欢迎在评论中猜测是谁。

参考资料：

[1]此： <https://www.linkedin.com/pulse/ai-cost-curve-just-collapsed-again-tomasz-tunguz-tdhlc/>

[2]上周： <https://www.datacenterdynamics.com/en/news/changing-linux-code-could-cut-data-center-energy-use-by-30-researchers-claim/>

DeepSeek 拆解源代码发生了秘密

陈钟 转自 [青山读不完]

在拆解 DeepSeek 源代码后，我发现了几个颠覆行业认知的真相。这个号称“用十分之一算力吊打 GPT-4”的国产大模型，藏着令人拍案叫绝的工程智慧，却也暗藏致命软肋。

第一刀，切开开源表象。

DeepSeek 确实把代码仓库甩上了 GitHub。但这套开源策略藏着精妙算计。他们公开的是经过蒸馏的“成品模型”，而非原始训练框架。就像给你组装好的乐高战舰却藏起了设计图纸。这种半开放式开源剂能吸引开发者构建生态，又守住了核心 Know-How。反观 open AI 彻底闭源的 API 模式，DeepSeek 这招既赚了口碑，又卡住了技术咽喉。

第二刀，解剖算力魔术。

当我追踪到模型架构层时，发现了真正的技术核弹：他们用 FP8 混合精度训练替代传统 FP32 硬生生把显卡显存占用砍掉 75%。更绝的是 MoE 架构的动态路由机制：面对医疗问题就唤醒医学子模型，遇到代码任务就启动编程模块，让每个 GPU 时钟周期都用在刀刃上。这套组合拳下来，训练成本直接压到 open AI 的 5.6%，但代价是工程复杂度指数及暴增，稍有不慎就会数值溢出。

第三刀，刺穿精度幻象。

在数学推理测试集上。DeepSeek-R1 确实追平了 GPT-3，但当我用医疗影像诊断任务实测时，FP8 精度导致的梯度消失问题暴露无遗：例如模型可能会把 0.8 厘米的肿瘤误判为 0.1 厘米，这种误差在现实场景足以致命。

开源社区狂欢的“80 元部署个人助手”，本质是把专业级手术刀当水果刀用，看似普惠，实则埋雷。

第四刀，直指生态悖论。

虽然华为、燧原等 20 余家芯片厂宣布适配。但代码里暗藏的 PTX 指令集暴露出对英伟达架构的深度绑定。所谓“国产算力突围”，更像是用美式枪械打游击战。一旦遭遇架构及封锁，这套优化体系有可能瞬间崩塌。DeepSeek 真正颠覆的不是技术路线，而是游戏规则。它证明在 AI 竞赛中，后来者完全可以用“算法杠杆”撬动千倍算力差距。但当行业集体转向优化竞赛时，我们可能正在亲手埋葬通用人工智能的未来。当所有人都沉迷于裁剪模型尺寸时，谁还有勇气继续攀登 AGI 的先锋？DeepSeek 映照出中国 AI 军团破局的智慧，也暴露出急功近利的隐忧。在这个算力与算法疯狂博弈的时代，DeepSeek 就像一剂强效兴奋剂，能让追赶者瞬间爆发，却有可能治不好核心技术贫血症。下一个十年 AI 王座的归属，恐怕要看谁能在这条钢索上走出最精妙的平衡。

李飞飞向巴黎人工智能大会提出制定 AI 政策三原则

COPU 摘录

1) 基于科学而非科幻

决策者应将目光聚焦于当下 AI 的实际状况，清楚认识到目前聊天机器人等 AI 产品并非具有意图、自由意志或意识的智能体，只有这样才能避免被不切实际的幻想分散注意力，集中精力解决 AI 发展过程中面临的真正问题，如数据隐私保护、算法偏见消除等。

2) 务实而非意识形态化原则

要求政策设计者目标在激励创新的同时，尽可能减少 AI 可能带来的危害。AI 技术发展日新月异的今天(指新的应用与 AI 创新)，如果政策过于僵化或被意识形态左右，可能会阻碍技术进步，合理的政策应在保障安全和公平的前提下，为 AI 创新提供宽松环境，鼓励企业和科研机构积极探索，推动 AI 技术更好服务于社会。

3) 为整个生态系统，政策要赋予开源社区和学术界在内整个 AI 生态系统更多自由，大模型和计算工具的开放访问，对于 AI 进步至关重要。

在当前 AI 发展格局中，私营部门往往拥有更丰富的资源和强大的研发能力，但学术机构和研究人员在基础研究和理论创新方面有着不可替代的作用。如果对这些资源的访问设置更多的限制，学术机构和研究人员将难以开展前沿研究，技术突破速度也会减缓。开源社区更是 AI 创新的重要力量，许多优秀的 AI 算法和模型都诞生于开源社区的协作。政策应鼓励这种开放和共享的精神，促进整个 AI 生态系统的繁荣发展。

DeepSeek 启示录

韩宪平

Our goal is to explore the potential of LLMs to develop reasoning capabilities without any supervised data, focusing on their self-evolution through a pure RL process. – DeepSeek

在第 19 届“开源中国开源世界”圆桌会议上我发言说人工智能时代开源越来越重要，作为新的生产方式（生产力+生产关系），开源文化、开源方法、开源治理适合各行各业；2015 年 1 月 20 日 DeepSeek 横空出世更是让开源变得巷议街谈家喻户晓，引来传播开源运用开源的热潮，杨立昆说“与其说是中国的胜利不如说是开源对闭源的胜利”，更是让全世界对中国开源刮目相看，在 Reddit AMA 对话中山姆奥特曼对 DeepSeek 开源思维链数据心悦诚服，承认自己站在了历史错误一边，但还是担心被竞争者利用基础模型生成的推理数据。梁文峰明确提出，“在美国每天发生的大量创新里，这是非常普通的一个，硅谷惊叹的原因是因为这是一个中国公司，在以创新贡献者的身份，加入到他们游戏里去。毕竟大部分中国公司习惯 Follow 而不是创新。”

- 开源促进开放，开放促进透明，透明促进信任，信任促进和平。
- 从这几天跟踪观察“DeepSeek 时刻”（Lex Fridman）带来的地缘政治冲击波似乎可以得出结论：中国处于“劣势策略” Dominated Strategy 地位，他国一边得享开源普惠一边调查禁运打压，川普 2 月 1 日在白宫会见黄仁勋；他上台任命的 AI 与加密货币负责人 David Sacks 随即制定了所谓“五步杀”祭出更严厉的芯片出口、人才流动、数据安全政策，甚至包括“arXiv、GitHub 等平台的 2500 万份技术文档列入出口管制清单”近乎坚壁清野的路数。
- 开源游戏基本规则：开放程度更高的玩家总是处于更有利的竞争地位。开放程度低的只能是为他人做嫁衣裳，可能惹来的麻烦比带来的好处更多，迫使中国采取更加开放的开源策略包括社会、资源、数据各个层面的深刻开放，开源并不是一个软件或是一个模型而是整个生态系统与 AI 供应链，在 X 社交平台上总能看到比国内多得多的测试研究，应用开发，下载安装，证明开源开放比政治安全带来更大更多的战略收益。开放不只是对外开放，实际上没有对内开放就没有对外开放，推理链被打断，推理联网被禁用、注册被限制都会大大限制大模型性能提升。
- 证明《为什么伟大不能被计划》：DeepSeek 既不是顶层设计的成果也不属于任何国家战略规划项目，幻方量化基金一直在使用 AI 处理对冲业务，2023 年才创建大模型团队，的确

可以被看作“副业项目”，仅凭个人情怀带与 AI 信念领着 150 多位所谓“导弹科学家”（1990's 年代称呼那些从其他行业转入衍生产品金融创新的数学家与工程师）自由组合，团队包括了 PTX、FP8 底层开发者，可能连 TA 们自己也根本没预见到后来地缘政治的轰动效应，这种人才自组织现象非常值得深入研究；公司治理结构恐怕也是出奇制胜的要素之一，没有任何风险投资背景；决策者本人同时也是开发者：“创新缺乏的肯定不是资本，而是信心并且知道怎么组织高密度人才，形成可以创新的组织和文化就是我们的护城河”（梁文峰）。肉食者鄙，未能远谋，高手在民间。

- 英伟达首席研究科学家 Jim Fan 说：“简单的数学！人们可以以 10 倍更少的成本获得单位智能增益，人工智能的时间线刚刚被压缩”；听说 Jeffrey Hinton 教授组织力量研究了技术报告击节赞叹，只有技术理想主义者能坚持简单数学体现的纯粹第一性原理，才能想出来用 $(\pi_{\theta}/\pi_{old})A_i$ 相对值 Advantage 代替绝对 Reward，这样就能避免使用监督微调 SFT、Critic Model（跟策略模型一样大小的另外一个模型），使得自我验证自主进化 self-evolution\verification\improvement\cognition、反思 reflection、长思维链 Long Chain of Thought 推理能力涌现出来（Aha Moment）。Arthur Clarke's 第三定律说：“任何非常先进的技术初看起来都与魔法无异”，真正的 Silver Bullet 是强化学习框架 GRPO 的目标函数，“春风大雅能容物，秋水文章不染尘”，其他创新例如 MoE 运用、MLA、多 Token 预测、Cold-start 可能都是这个主要创新基础上带来的灵感，是否用了 5 万块英伟达 GPU，是否使用了 openAI 的思维链推理数据，是否真的仅用了 600 万美元完成模型训练都显得不那么重要了，It is not a top focus for me -- Sam Altman，何况他也在重新考虑公司的开源战略了，如果不存在服务条款也许基础模型 V3-Base 也许只是一个 Fork 而已。
- Pure RL 的启发带给学界业界带来巨大影响，Andrej Karpathy 似乎是在回顾与检讨自己前几年探索的路线，前几天他说：“对于开源的朋友来说，在我看来，你能做得最有杠杆作用的事情就是帮助构建一个高度多样化的 RL 环境、各种类型的 gym 以帮助提升 LLM 的认知策略。这是一个高度并行化的任务，有利于大型协作者社区。” Hugging Face 的科学家 Lewis Tunstall 说：“R1 表明，有了足够强大的基础模型，强化学习就足以在没有任何人工监督的情况下从语言模型中实现推理。”（2025 年 2 月 1 日）

DeepSeek 的学习与讨论

刘澎

我理解深度求索在长思考慢思维方面取得了长足进步，但在某些方面它还在改进中，采用大量蒸馏技术路线，对 Qwen 和 Llama 等国内外大模型数据进行蒸馏。

主要贡献是证明开源模式兴起。

第一，在与训练方面对其他领先大模型（大语言通用 LLM）蒸馏。相当于，在操作系统方面借鉴 Linux 的宏内核，萃取精华。

第二，在专业领域方面重点进行自我纠错的强化学习，基本不采用监督学习，减少了成本。特别突出编程、数学和推理三个小模型（垂直模型）内核，并形成 MoE 专家混合系统的优化调度，试图在特定领域达到大模型效果。相当于，以微内核聚会宏内核。

1，快速筛选：

首先选择 100 种模型训练一到两周，选取效果好的 10 模型，后面不再淘汰。

2，对 10 个模型分别进行机器纠错的有奖励的强化训练，并相互借鉴结果，不采用人工干预反馈，即不使用监督学习，节约了大量成本。

3，首先，在编程、数学、推理，三个基础工程技术方面谋求优异成绩，形成精湛逻辑内核。然后，向人文历史等通识领域扩展，通过高效的模型路由调度，形成合成效果，最终挑战单体大模型。

第三，在推理应用阶段，借助开源模式，广泛吸引用户参与，大量反馈形成事实上的监督学习效果，零成本弥补了前期只有强化学习没有人类监督学习的重要缺失。

第四，基于蒸馏和微内核的实现，使得到端的安装应用比较便捷，性价比很高，进一步极大地支持了广泛的开源使用和用户反馈增强。

第五，由于是从微内核起步，目前，在通识方面，相对于通用语言大模型(LLM)，知识深度和广度不够丰富。但借助于最彻底的 MIT 开源许可证模式，吸引了广泛用户使用开发参与，情况正在迅速改善。

第六，由于对机器强化学习的自我纠错能力重视，系统在推理环境，发生错误和克服过程中，会给人感觉出现顿悟现象，预示了自主意识的前兆。因此，在慢思维和长思考方面，进步明显。

DS 对模型架构 MLA 和 MoE 全方位创新

陆首群

致章文嵩及 COPU 同仁：

在 2 月 11 日 COPU 例会上，在讨论 DeepSeek 如何做到以低成本实行高效率创新时，文嵩提出，主要依靠强化学习和改革 MoE 架构，我同意他的观点，并指出对 MoE 要提出量化的概念，我在会上指出：主要是 DeepSeek 对模型架构 MLA 和 MoE 进行全方位的创新；进行强化学习；以及与其数学、编程优化和工程突破能力有关！现将刘明寄给我有关 MLA 和 MoE 架构的变革创新（并含量化）的信息提供给文嵩和朋友们参考，期望你们深入思考、探索，有所收获。

刘明来信（摘要）

揭秘 DeepSeek：一个更极致的中国技术理想主义故事

（原创）暗涌 Waves2024.7.17

做贡献者，而非搭便车（蒸馏）者

暗通.....DeepSeek（深度求索）最不声不响，但它总能以出其不意的方式被人记住。

.....

DeepSeek 一跃成名，起因是他们发布的一款名为 DeepSeek-v2 的开源模型，提供了一种史无前例的性价比：推理成本被降到每百万 token 仅 1 块钱，约等于 Llama3-70B 的 1/7，GPT-4Turbo 的 1/70，.....

DeepSeek 对模型架构进行了全方位创新。它提出的一种崭新的 MLA（一种新的多头潜在注意力机制）架构，把显存占用降低到过去常用的 MHA 架构的 5%~13%，同时它独创的 DeepSeekMoESparse 架构，也把计算量降到极致（陆注：MoE 架构把训练成本砍了 40%），所有这些最终促成了成本的下降。

刘明在此处提到的 MLA 和 MoE 是相当于 DeepSeekv2 早期的架构，而在发展到 DeepSeekv3 及 R1 时，MLA 和 MoE 架构及其量化效应，似应有所发展或变化。

在硅谷，DeepSeek 被称作“来自东方的神秘力量”。Semi Analysis 首席分析师认为，DeepSeekv2 论文“可能是今年最好的一篇”，OpenAI 的 Andrew Carr 认为论文“充满惊人的智慧”。在硅谷对其强烈的反应源自架构层面的开源创新，这是全球基座大模型罕见的尝试。

DeepSeek 显然是逆行者，在一片认为大模型技术必然趋同，follow 是“更聪明的捷径”的喧哗声中，DeepSeek 与众不同，它是唯一一家不做 toc 应用、专注于核心技术架构原创式创新的公司，也是唯一一家未全面考虑商业化、选择开源路线的公司，它常被遗忘在牌桌之外，进行低调的埋头巧干+苦干！



敬请关注联盟微信公众号
COPU开源联盟



扫描二维码
获取往期资料

中国开源软件推进联盟秘书处

电话：+86 010-88558999

联盟公共邮箱：office@copu.org.cn

联盟官网：<http://www.copu.org.cn>

地址：北京市海淀区紫竹院路66号赛迪大厦18层
