Artificial Intelligence Newsletter

人工智能前沿快报



2026 年第 07 期
总第 32 期

学会官方公众号

广东省图象图形学会
GDSIG
学术交流、技术咨询、科学普及

目 录

学 术 动 态

一. ReconVLA: Reconstructive Vision-Language-Action Model as Effective Robot Perceiver ····· 1

二. Sampling-enabled scalable manifold learning unveils the discriminative cluster structure of high-dimensional data ····· 4

三. OmniScientist: Toward a Co-evolving Ecosystem of Human and AI Scientists ····· 6

四. Causal Structure Learning for Dynamical Systems with Theoretical Score Analysis ····· 8

五. A Survey of Vibe Coding with Large Language Models ····· 10

六. End-to-End Test-Time Training for Long Context ····· 12

七. Deep contrastive learning enables genome-wide virtual screening ····· 14

八. AI Agent Systems: Architectures, Applications, and Evaluation ····· 16

九. The Path Ahead for Agentic AI: Challenges and Opportunities ····· 18

十. mHC: Manifold-Constrained Hyper-Connections ····· 20

十一. Qwen3-VL-Embedding and Qwen3-VL-Reranker: A Unified Framework for State-of-the-Art Multimodal Retrieval and Ranking ····· 22

十二. Conditional Memory via Scalable Lookup: A New Axis of Sparsity for Large Language Models ····· 24

目 录

技 术 动 态

一． OpenAI 官方 Prompt 指南：用目标、上下文、输出和边界组织高质量任务……26
二． Kimi K3 发布：2.8 万亿参数开源模型瞄准前沿编程与长程 Agent……28
三． Claude Opus 5 发布，Anthropic 以“减少上下文负担”重构 Agent 协作方式……29
四． Nature 2026 大模型研究脉络综述：从后训练与可信评测到科研 Agent……30
五． Kimi K3 完整权重与技术报告开放：重点解决长程 Agent 状态、训练与验证……33
六． Unsloth Dynamic 3.0 GGUFs：面向 Qwen3.8-27B 的高精度动态量化资源……35
七． 小红书开源 dots.tts：2B 全连续端到端语音合成系统输出 48 kHz 音频……36
八． GLM-5.3：Frontier Coding with Emergent Cyber Capabilities……37
九． 阿里巴巴开源 Qwen3.8-27B……38
十． Qwen3.8-27B 开源：27B 稠密原生多模态模型强化代码、Agent 与本地部署……39
十一． DeepSeek 首个多模态模型发布：V4-Flash-Vision-Exp 上线 API……41
十二． NVIDIA 据悉洽谈收购 Hugging Face，估值或超 130 亿美元……43

INTRODUCTION
导读

在人工智能技术飞速发展的时代背景下，我们将不定期梳理人工智能领域的部分前沿学术与技术动态，并以简报的形式分享给读者，以帮助关注此领域的人士了解最新的学术前沿发展与产业技术动态，促进学术交流和技术繁荣。本期摘选了近期全球人工智能领域的 12 篇最新学术动态、12 篇技术动态推荐给广大读者。

ACADEMIC TRENDS
学术动态

● 论文一

Advances and Challenges in Foundation Agents: From Brain-Inspired Intelligence to Evolutionary, Collaborative, and Safe Systems

日期

2025-08-02（v2，最后修订）

ADVANCES AND CHALLENGES IN FOUNDATION AGENTS
FROM BRAIN-INSPIRED INTELLIGENCE TO EVOLUTIONARY, COLLABORATIVE, AND SAFE SYSTEMS

Bang Liu[2,3,20*†], Xinfeng Li[4*], Jiayi Zhang[1,10*], Jinlin Wang[1*], Tanjin He[5*], Sirui Hong[1*], Hongzhang Liu[6*], Shaokun Zhang[7*], Kaitao Song[8*], Kunlun Zhu[9*], Yuheng Cheng[1*], Suyuchen Wang[2,3*], Xiaoqiang Wang[2,3*], Yuyu Luo[10*], Haibo Jin[9*], Peiyan Zhang[10], Ollie Liu[11], Jiaqi Chen[1], Huan Zhang[2,3], Zhaoyang Yu[1], Haochen Shi[2,3], Boyan Li[10], Dekun Wu[2,3], Fengwei Teng[1], Xiaojun Jia[4], Jiawei Xu[1], Jinyu Xiang[1], Yizhang Lin[1], Tianming Liu[14], Tongliang Liu[6], Yu Su[15], Huan Sun[15], Glen Berseth[2,3,20], Jianyun Nie[2], Ian Foster[5], Logan Ward[5], Qingyun Wu[7], Yu Gu[15], Mingchen Zhuge[16], Xinbing Liang[1], Xiangru Tang[12], Haohan Wang[9], Jiaxuan You[9], Chi Wang[19], Jian Pei[17†], Qiang Yang[10,18†], Xiao-Liang Qi[13†], Chenglin Wu[1*†]

[1]MetaGPT, [2]Université de Montréal, [3]Mila - Quebec AI Institute, [4]Nanyang Technological University, [5]Argonne National Laboratory, [6]University of Sydney, [7]Penn State University, [8]Microsoft Research Asia, [9]University of Illinois at Urbana-Champaign, [10]The Hong Kong University of Science and Technology, [11]University of Southern California, [12]Yale University, [13]Stanford University, [14]University of Georgia, [15]The Ohio State University, [16]King Abdullah University of Science and Technology, [17]Duke University, [18]The Hong Kong Polytechnic University, [19]Google DeepMind, [20]Canada CIFAR AI Chair

内容摘要

本文是一篇关于基础智能体（Foundation Agents）的系统综述，围绕大语言模型驱动的智能体如何获得感知、推理、记忆和行动能力展开分析。论文以脑启发的模块化架构为主线，系统讨论记忆、世界模型、奖励处理、目标和情绪等核心模块；进一步总结智能体的自我增强、自动优化与持续学习机制，分析多智能体协作及其集体智能演化；最后从内生与外部安全威胁、价值对齐、鲁棒性和伦理治理等方面讨论安全可靠部署所需的技术与实践路径。

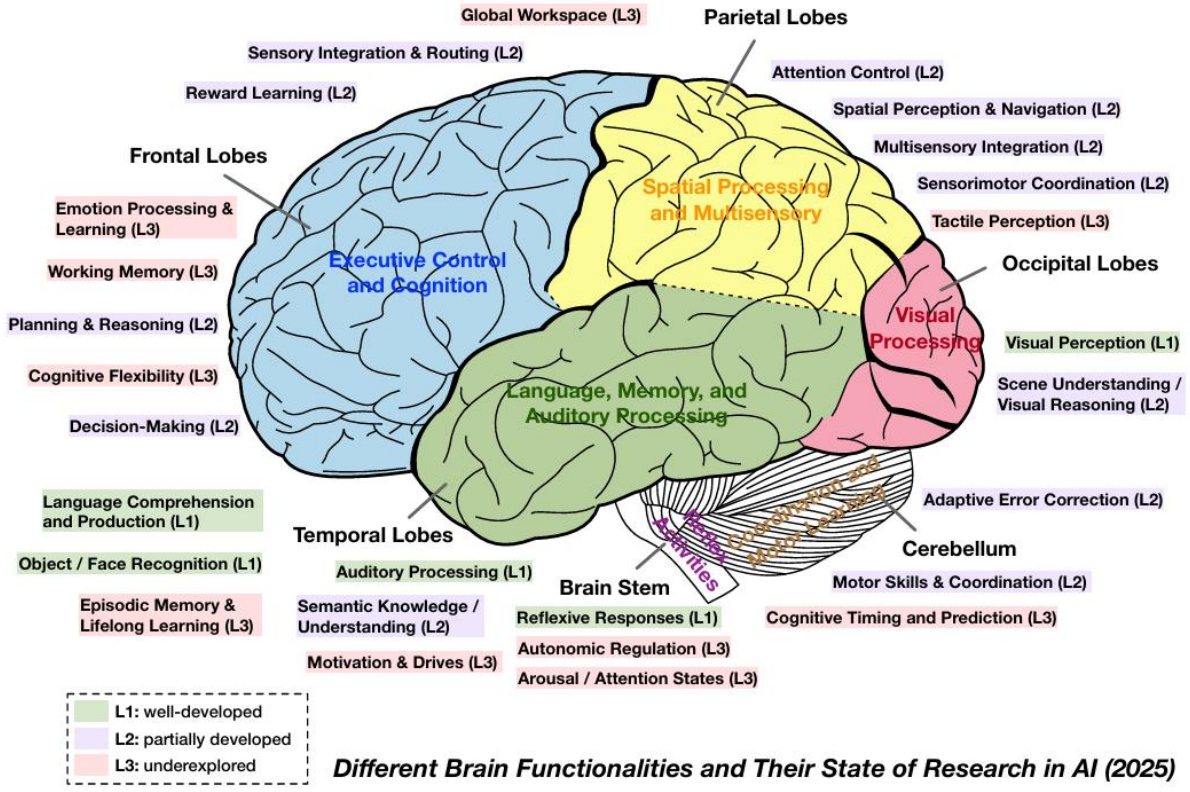


Figure 1.1: Illustration of key human brain functionalities grouped by major brain regions, annotated according to their current exploration level in AI research. This figure highlights existing achievements, gaps, and potential opportunities for advancing artificial intelligence toward more comprehensive, brain-inspired capabilities. Please note: The location of a label does not imply that it is associated with or is only associated with nearby brain regions. Also, to focus on the current state of AI capabilities rather than the anatomy of the brain, we did not mark the limbic system, subcortical system, hypothalamus, amygdala, and so on in this lateral view of the brain, though these systems play important roles in brain function.

主要亮点

- 脑启发模块化架构：将记忆、世界模型、奖励、目标和情绪等智能体组件与认知科学和神经科学机制相联系。
- 系统梳理自我增强与适应性进化：覆盖自动优化、持续学习及动态环境中的能力更新。
- 关注多智能体集体智能：分析协作、交互和社会结构如何推动群体能力涌现。
- 兼顾安全与实用部署：总结安全威胁、价值对齐、鲁棒性和风险缓解等关键挑战。

相关链接

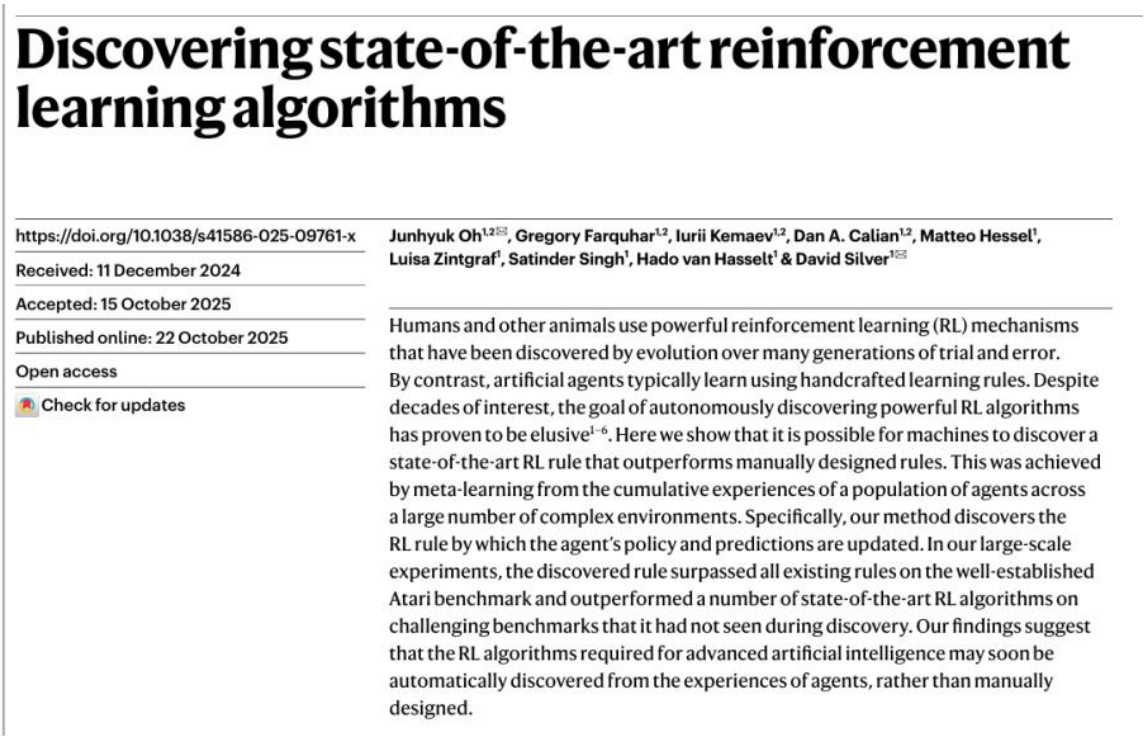
Paper： https://arxiv.org/abs/2504.01990

● 论文二

Discovering state-of-the-art reinforcement learning algorithms

日期

2025-10-22



Discovering state-of-the-art reinforcement learning algorithms

https://doi.org/10.1038/s41586-025-09761-x
Received: 11 December 2024
Accepted: 15 October 2025
Published online: 22 October 2025
Open access
Check for updates

Junhyuk Oh[1,2], Gregory Farquhar[1,2], Iurii Kemaev[1,2], Dan A. Calian[1,2], Matteo Hessel[1], Luisa Zintgraf[1], Satinder Singh[1], Hado van Hasselt[1] & David Silver[1]

Humans and other animals use powerful reinforcement learning (RL) mechanisms that have been discovered by evolution over many generations of trial and error. By contrast, artificial agents typically learn using handcrafted learning rules. Despite decades of interest, the goal of autonomously discovering powerful RL algorithms has proven to be elusive[1–6]. Here we show that it is possible for machines to discover a state-of-the-art RL rule that outperforms manually designed rules. This was achieved by meta-learning from the cumulative experiences of a population of agents across a large number of complex environments. Specifically, our method discovers the RL rule by which the agent's policy and predictions are updated. In our large-scale experiments, the discovered rule surpassed all existing rules on the well-established Atari benchmark and outperformed a number of state-of-the-art RL algorithms on challenging benchmarks that it had not seen during discovery. Our findings suggest that the RL algorithms required for advanced artificial intelligence may soon be automatically discovered from the experiences of agents, rather than manually designed.

内容摘要

Google DeepMind 提出 DiscoRL，一种通过元学习自动发现强化学习更新规则的方法。系统让一组智能体在大量复杂环境中并行交互，由元网络根据智能体的策略、预测、奖励和轨迹生成学习目标，再通过穿过智能体更新过程的元梯度优化规则本身，从而同时学习策略与预测应如何更新。大规模实验显示，DiscoRL 在 Atari 基准上超过已有手工设计规则，并在发现阶段未见过的 ProcGen 等挑战性任务上达到领先表现；使用更多样、更复杂的环境进行发现还能进一步提升泛化性。

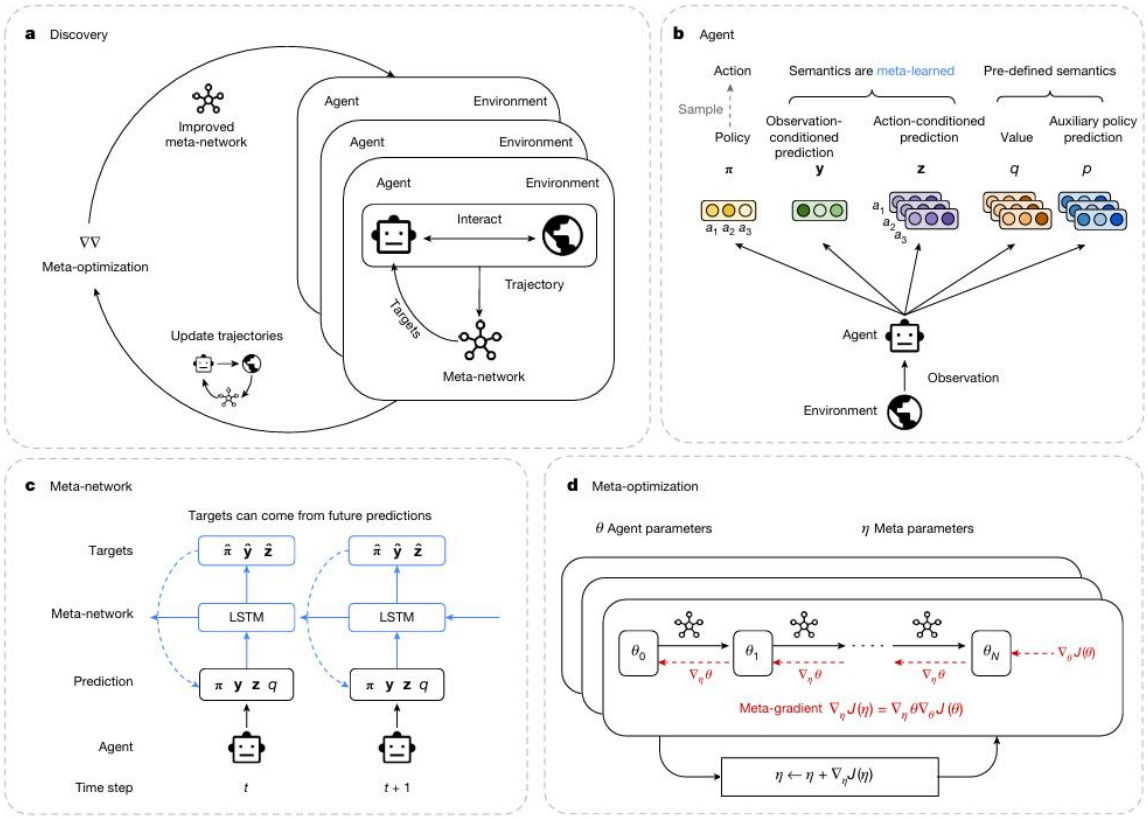


Fig. 1 | Discovering an RL rule from a population of agents. a, Discovery. Multiple agents, interacting with various environments, are trained in parallel according to the learning rule, defined by the meta-network. In the meantime, the meta-network is optimized to improve the agents' collective performances. **b**, Agent architecture. An agent produces the following outputs: (1) a policy ($\boldsymbol{\pi}$), (2) an observation-conditioned prediction vector ($\mathbf{y}$), (3) action-conditioned prediction vectors ($\mathbf{z}$), (4) action values ($\mathbf{q}$) and (5) an auxiliary policy prediction ($\mathbf{p}$). The semantics of $\mathbf{y}$ and $\mathbf{z}$ are determined by the meta-network. **c**, Meta-network architecture. A trajectory of the agent's outputs is given as input to the meta-network, together with rewards and episode termination indicators from the environment (omitted for simplicity in the figure). Using this information, the meta-network produces targets for all of the agent's predictions from the current and future time steps. The agent is updated to minimize the prediction errors with respect to their targets. LSTM, long short-term memory. **d**, Meta-optimization. The meta-parameters of the meta-network are updated by taking a meta-gradient step calculated from backpropagation through the agent's update process ($\theta_0 \rightarrow \theta_N$), where the meta-objective is to maximize the collective returns of the agents in their environments.

主要亮点

- 从手工规则转向自动发现：由元网络直接学习智能体预测目标和策略更新目标，搜索空间比固定损失函数更灵活。
- 多智能体跨环境元学习：并行收集不同任务的交互经验，以群体累计回报作为元优化目标。
- 元梯度闭环优化：反向传播穿过智能体的多步学习过程，联合更新智能体参数与强化学习规则。

泛化能力得到验证：在 Atari 上超越已有规则，并在未参与发现的 ProcGen 等任务上取得领先表现。

相关链接

Paper： https://www.nature.com/articles/s41586-025-09761-x

Project： https://google-deepmind.github.io/disco_rl/

● 论文三

Structure and evolution-guided design of minimal RNA-guided nucleases

日期

2026-07-25



Article

Design of highly functional genome editors by modelling CRISPR–Cas sequences

https://doi.org/10.1038/s41586-025-09298-z
Received: 3 May 2024
Accepted: 17 June 2025

Jeffrey A. Ruffolo[1,4], Stephen Nayfach[1,4], Joseph Gallagher[1,4], Aadyot Bhatnagar[1,4], Joel Beazer[1], Riffat Hussain[1], Jordan Russ[1], Jennifer Yip[1], Emily Hill[1], Martin Pacesa[1,2], Alexander J. Meeske[1,3], Peter Cameron[1] & Ali Madani[1]

内容摘要

相关研究显示，AI 蛋白设计正在把 CRISPR 核酸酶的开发从天然序列筛选推进到按目标结构和功能生成新序列。Jennifer Doudna 团队以微型 TnpB 核酸酶为对象，将结构约束、进化信息与序列生成结合，获得与天然版本约 30%序列不同、仍能在细菌、植物和人类细胞中工作的候选酶。另一条由 Profluent 推进的路线从大规模 CRISPR 蛋白数据中生成 OpenCRISPR-1；其公开实验报告显示，在特定测试中保持较高靶向活性并显著降低脱靶。成果说明 AI 可以探索进化未覆盖的蛋白空间，但目前主要停留在实验室验证阶段，独立复现、动物实验、临床安全与治理仍是必要关口。

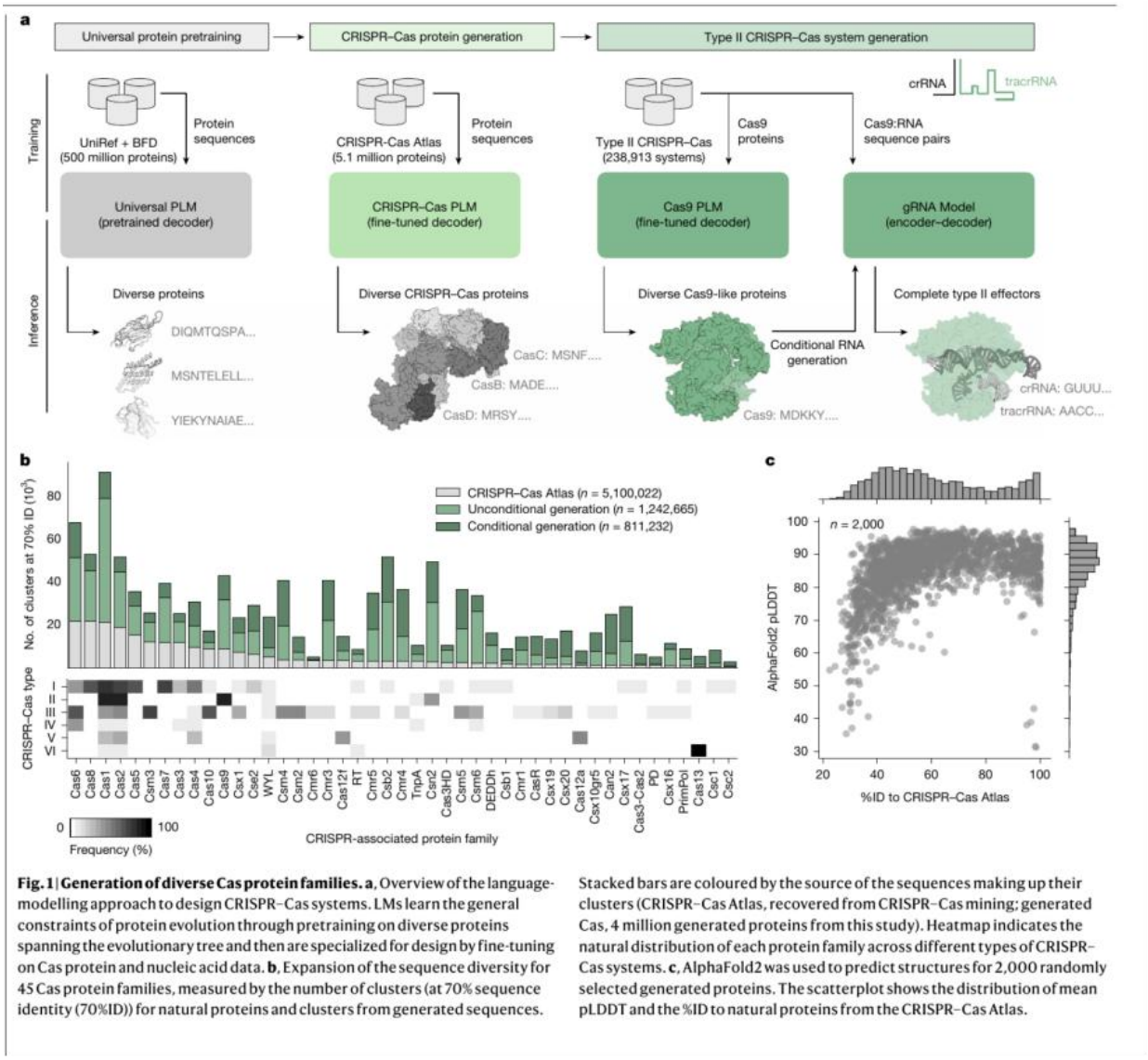


Fig. 1 | Generation of diverse Cas protein families. a, Overview of the language-modelling approach to design CRISPR–Cas systems. LMs learn the general constraints of protein evolution through pretraining on diverse proteins spanning the evolutionary tree and then are specialized for design by fine-tuning on Cas protein and nucleic acid data. **b**, Expansion of the sequence diversity for 45 Cas protein families, measured by the number of clusters (at 70% sequence identity (70%ID)) for natural proteins and clusters from generated sequences. Stacked bars are coloured by the source of the sequences making up their clusters (CRISPR–Cas Atlas, recovered from CRISPR–Cas mining; generated Cas, 4 million generated proteins from this study). Heatmap indicates the natural distribution of each protein family across different types of CRISPR–Cas systems. **c**, AlphaFold2 was used to predict structures for 2,000 randomly selected generated proteins. The scatterplot shows the distribution of mean pLDDT and the %ID to natural proteins from the CRISPR–Cas Atlas.

主要亮点

- 将结构反向折叠与实验数据约束结合，使大幅改写后的核酸酶仍保持可用功能。
- OpenCRISPR-1 等生成式候选展示了提高编辑效率、降低脱靶的潜力。
- 从“寻找天然蛋白”转向“按功能设计蛋白”，同时凸显湿实验验证和生物安全的重要性。

相关链接

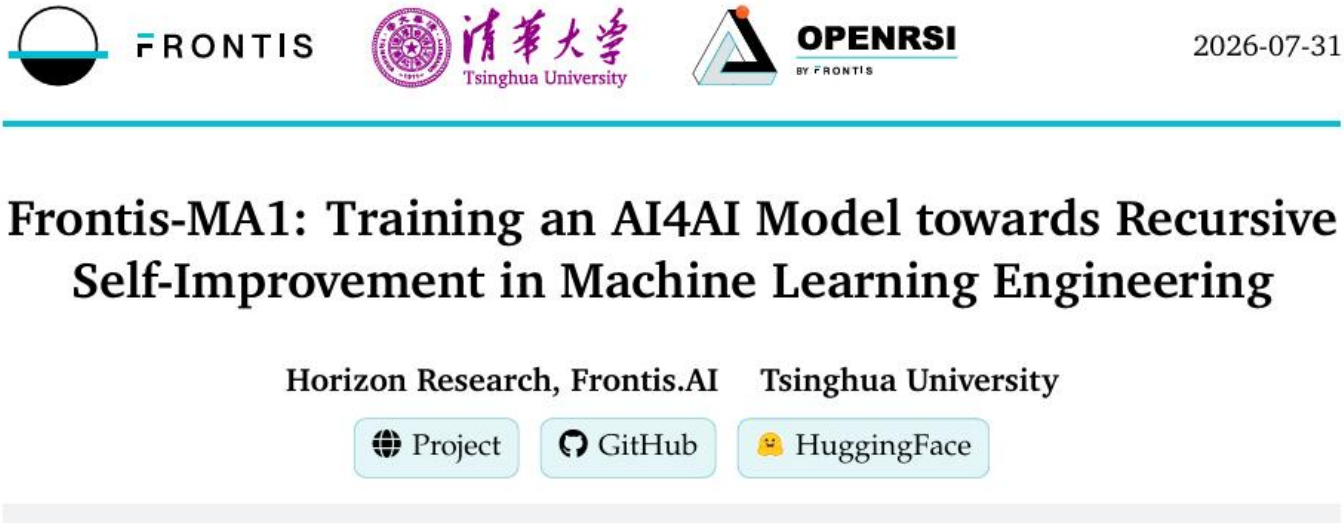
Paper： https://doi.org/10.1126/science.aed6123

● 论文四

Frontis-MA1: Training an AI4AI Model towards Recursive Self-Improvement in Machine Learning Engineering

日期

2026-07-30



内容摘要

本文将机器学习工程（MLE）作为研究递归自我改进（RSI）的可执行试验场，提出开放的全栈系统 OpenMLE。该系统由带执行反馈的任务环境 OpenMLE-Gym、算子学习模块 OpenMLE-RL 和长程搜索模块 OpenMLE-Evo 组成，并在此基础上训练 35B 参数的 Frontis-MA1 元进化智能体。模型围绕 Draft、Improve、Debug、Crossover 四种程序进化原子算子，使用执行结果驱动的监督微调与强化学习进行后训练，再将同一组算子组合到长程搜索中。实验显示，在 MLE-Bench Lite 上，OpenMLE-Evo 将基础模型 Medal Average 从 39.39% 提升至 60.61%，增强版达到 71.21%；在留出的 NatureBench Lite 上，模型和框架也表现出相互迁移的收益。

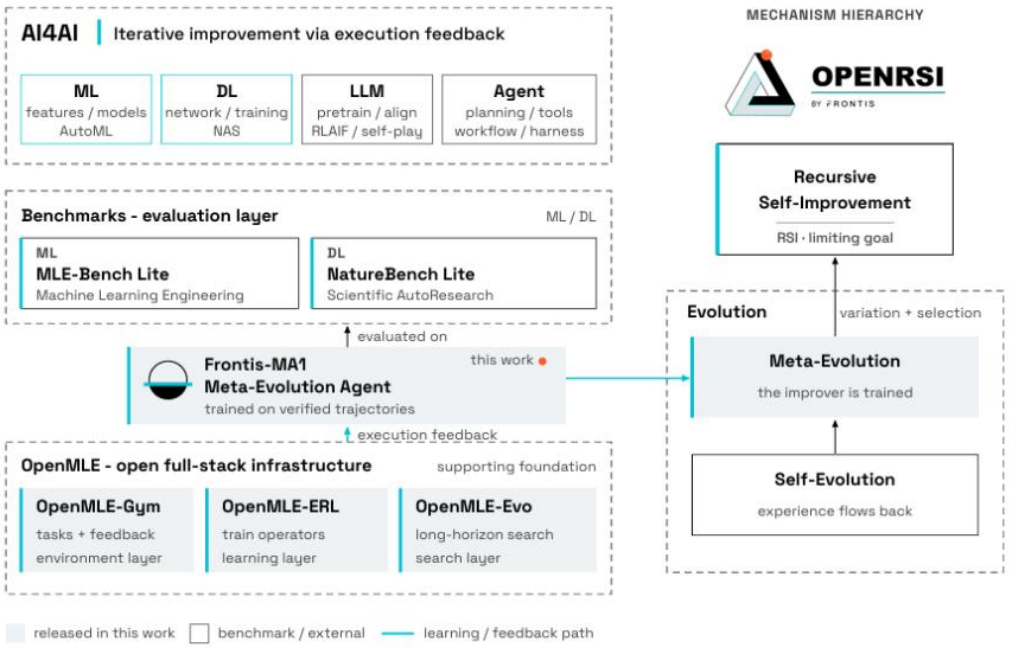


Figure 2 | Positioning of this work. **Left:** within AI4AI, machine learning engineering (MLE) is our task domain; the OpenMLE stack trains and deploys Frontis-MA1, which is both the product of the stack and its engine, evaluated only on third-party benchmarks. **Right:** the mechanism ladder from evolution to recursive self-improvement; the meta-evolutionary loop (orange) places this work at the level where the improver itself is trained—the level after which Frontis-**MA**1 (**M**eta-evolution **A**gent) is named.

主要亮点

- 构建 OpenMLE 全栈 RSI 研究平台：统一任务环境、执行反馈、强化学习和进化搜索。
- 以四种程序进化算子训练模型：Draft、Improve、Debug、Crossover 贯通后训练与推理时搜索。
- 执行反馈驱动长程自我改进：模型可依据实验结果迭代机器学习工程方案，而无需额外人工标注。
- 在 MLE-Bench Lite 和 NatureBench Lite 上验证泛化：模型能力与搜索框架可彼此迁移并提升效果。

相关链接

Paper： https://arxiv.org/abs/2607.28568

Code： https://github.com/FrontisAI/OpenRSI

● 论文五

Beyond representational alignment with brain-guided language models for robust reasoning

日期

2026-08-03

Article | Published: 03 August 2026

Beyond representational alignment with brain-guided language models for robust reasoning

Mingqing Xiao (肖命清), Kai Du (杜凯) ✉ & Zhouchen Lin (林宙辰) ✉

Nature Machine Intelligence **8**, 1275–1289 (2026) | Cite this article

内容摘要

Nature Machine Intelligence 发表研究，探讨大语言模型的内部表征是否与人类高阶推理的神经机制相对应。研究聚焦演绎推理任务，利用功能磁共振成像（fMRI）信号评估模型与人脑推理相关区域的神经预测性，发现二者存在部分对齐但也具有明显差异。在此基础上，作者提出脑信号引导的表示干预与参数微调方法，将人类推理相关脑活动用于引导模型表征；在 10 个、参数量 1.5B 至 72B 的语言模型上，跨推理类型最高带来 13 个百分点的准确率提升，显示脑信号可成为语言监督之外的稳健推理增强路径。

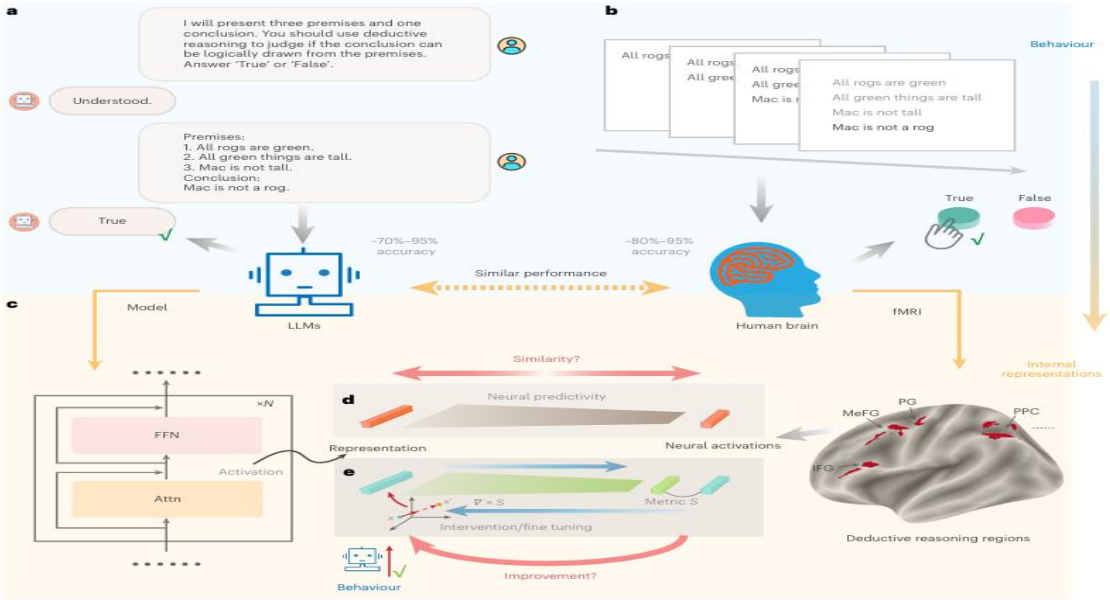


Fig. 1 | Overview of connections between LLMs and humans for solving deductive reasoning problems. We aim to step from the behaviour level to internal representations. **a**,**b**, LLMs and humans show similar behaviour performance. **a**, LLMs process problems through chat-formatted prompts, generating direct linguistic responses. **b**, Human participants sequentially view premises and conclusions, responding via button press after the presentation of the conclusion. **c**, We examine whether shared behaviour performance reflects internal connections between internal representations of LLMs and humans, that is, if their internal representations (model representations and neural activations of human brains in related regions) align, and if neural signals can guide the improvement of AI models. **d**, We study representational similarity through the neural predictivity score. **e**, We enhance LLMs by steering their representations of incorrect responses towards neural-derived directions through the representation intervention or parameter fine tuning.

主要亮点

- 神经表征对齐评估：利用 fMRI 信号检验语言模型与人脑推理相关区域的神经预测性，区分表征相似性与实际推理能力。
- 脑信号引导模型增强：将人类推理相关脑活动转化为表示干预信号，并用于参数微调，形成从脑科学测量到模型训练的闭环。
- 跨模型、跨推理类型验证：在 10 个、参数量 1.5B 至 72B 的语言模型上开展实验，最高带来 13 个百分点的准确率提升。
- 提升稳健推理能力：结果表明，脑信号能够作为语言监督之外的补充，为改善模型在不同演绎推理任务上的泛化提供新路径。

相关链接

Paper： https://www.nature.com/articles/s42256-026-01278-w

● 论文六

A Survey of Agent Memory in the Second Half: Towards Self-Evolving and Long-Horizon Agents

日期

2026-08-04（v4，最后修订）

A Survey of Agent Memory in the Second Half: Towards Self-Evolving and Long-Horizon Agents

Wei-Chieh Huang[1,†], Weizhi Zhang[1,†,‡], Yueqing Liang[2,†], Yuanchen Bei[3,*], Yankai Chen[1,18,*], Tao Feng[3,*], Xinyu Pan[4,*], Zhen Tan[5,*], Yu Wang[14,*], Tianxin Wei[3,*], Shanglin Wu[6,*], Ruiyao Xu[7,*], Liangwei Yang[22,*], Rui Yang[3,*], Wooseong Yang[1,*], Chin-Yuan Yeh[1,*], Hanrong Zhang[1,*], Haozhen Zhang[8,*], Siqi Zhu[3,*], Henry Peng Zou[1], Wanjia Zhao[21], Song Wang[9], Wujiang Xu[10], Zixuan Ke[22], Zheng Hui[11], Dawei Li[5], Yaozu Wu[13], Langzhou He[1], Chen Wang[1], Xiongxiao Xu[2], Baixiang Huang[6], Juntao Tan[22], Shelby Heinecke[22], Huan Wang[22], Caiming Xiong[22], Ahmed A. Metwally[23], Jun Yan[23], Chen-Yu Lee[23], Hanqing Zeng[24], Yinglong Xia[24], Xiaokai Wei[25], Ali Payani[26], Yu Wang[27], Haitong Ma[12], Wenya Wang[8], Chenguang Wang[15], Yu Zhang[16], Xin Eric Wang[17], Yongfeng Zhang[10], Jiaxuan You[3], Hanghang Tong[3], Xiao Luo[4], Xue Liu[18,19], Yizhou Sun[20], Wei Wang[20], Julian McAuley[14], James Zou[21], Jiawei Han[3], Philip S. Yu[1,¶], Kai Shu[6,¶]

[†] *Co-first authors* [*] *Core contributors (listed alphabetically)* [‡] *Project organizer* [¶] *Core supervisors*

[1] *UIC* [2] *IIT* [3] *UIUC* [4] *UW–Madison* [5] *ASU* [6] *Emory* [7] *Northwestern* [8] *NTU* [9] *UCF* [10] *Rutgers*
[11] *Cambridge* [12] *Harvard* [13] *UTokyo* [14] *UCSD* [15] *UCSC* [16] *TAMU* [17] *UCSB* [18] *MBZUAI* [19] *McGill*
[20] *UCLA* [21] *Stanford* [22] *Salesforce* [23] *Google* [24] *Meta* [25] *Roblox* [26] *Cisco* [27] *Capital One*

内容摘要

本文面向智能体编程、深度研究和计算机使用等长程、动态且依赖用户的场景，系统综述智能体记忆研究。论文从记忆基底（模型内部参数状态与外部检索存储）、认知机制（感觉、工作、情景、语义和程序性记忆）以及记忆主体（用户个性化与智能体经验）三个维度建立统一框架，讨论短期记忆如何筛选和抽象当前经验、长期记忆如何将其巩固为可复用知识与技能。作者进一步分析单智能体和多智能体拓扑下的记忆操作学习，梳理记忆评测基准与指标，并总结记忆管理可训练化、可迁移技能共享、安全和规模化等开放问题。



Figure 1: **Roadmap of Foundation Agent Memory**. A timeline illustrating the trend of foundation agent memory frameworks released between 2023 and 2025, categorized along two of the three taxonomy dimensions: memory substrates (internal, external, or mixed) and memory subjects (user- or agent-centric).

主要亮点

- 三维统一框架：从记忆存储基底、认知功能和记忆服务对象刻画基础智能体记忆。
- 记忆驱动自我进化：将短期经验筛选、长期知识巩固与技能复用连接为持续改进闭环。
- 记忆操作走向可训练化：涵盖强化学习式上下文整理、决策时经验整合和可共享智能体技能。
- 系统整理评测与挑战：覆盖记忆效用指标，并讨论个性化、安全、可扩展性和跨智能体迁移。

相关链接

Paper：https://arxiv.org/abs/2602.06052

● 论文七

AI4AI at Test-Time: Strong-to-Weak Capability Transfer via Harnesses

日期

2026-08-12

AI4AI at Test-Time: Strong-to-Weak Capability Transfer via Harnesses

Cheng Qian[1,2], Wenting Zhao[1], Liangwei Yang[1], Heng Wang[1,2], Jielin Qiu[1], Heng Ji[2], Silvio Savarese[1], Huan Wang[1], Shelby Heinecke[1]

[1]Salesforce AI Research, [2]University of Illinois Urbana-Champaign

内容摘要

本文研究无需更新模型参数，能否在测试时通过智能体外壳（harness）把强模型的能力迁移给弱模型。作者让更强的 builder model 根据少量验证数据，为目标模型迭代构建推理时脚手架，并在四类心智理论（Theory of Mind）基准上进行评估。结果表明，目标模型平均性能可由 0.49 提升至 0.91，增益主要来自将不稳定推理外包给确定性代码、进行基准特定路由以及严格约束答案格式，而不是简单要求模型进行更长推理或更广泛采样。研究说明，测试时 harness 设计可作为训练时蒸馏的补充，在不重新训练弱模型的情况下传递部分认知结构。

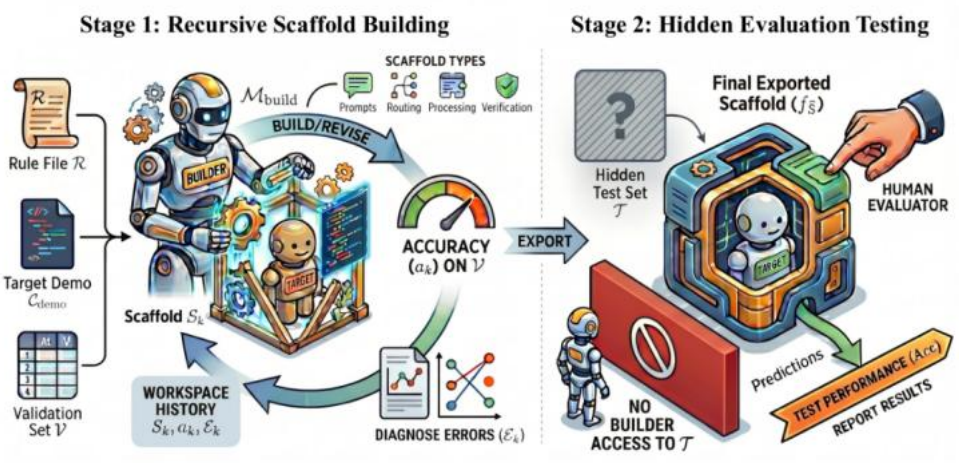


Figure 1: Overview of the **Strong-to-Weak Scaffolding** evaluation framework. During *recursive scaffold building*, the builder model iteratively refines a scaffold to improve target-model performance on validation sets. During *hidden evaluation testing*, the final scaffold is evaluated on the full hidden test set to measure target-model performance.

主要亮点

- 提出强到弱测试时能力迁移：由强模型构建推理外壳，弱模型无需参数更新即可受益。
- 迭代式 harness 优化：仅使用 5% 验证数据多轮改进，再在完整测试集上评估。
- 性能接近翻倍：四类心智理论基准上的目标模型平均得分从 0.49 提升到 0.91。
- 揭示增益来源：确定性代码、任务路由和答案格式校验比单纯增加推理或采样更关键。

相关链接

Paper： https://arxiv.org/abs/2608.12307

● 论文八

OmniScientist: An Omni-Modal Omni-Discipline AI Scientist

日期

2026-08-13







OmniScientist:
An Omni-Modal Omni-Discipline AI Scientist

Bobo Li[1], Hao Fei[2*], Tianjie Ju[1], Mong-Li Lee[1] and Wynne Hsu[1]

[1]National University of Singapore [2]University of Oxford

内容摘要

OmniScientist 提出一个从异构原始证据出发的全模态、跨学科 AI 科学家系统。与主要依赖文本、代码或预计算特征的科研 Agent 不同，该系统把图像、信号、音频、视频、三维结构、轨迹、表格、公式和图等证据直接纳入研究流程，并由感知层以及构思、实验、写作三个自主 Agent 组成确定性流水线。系统用代码执行创意、严谨性和主张检查，约束新颖性筛选、统计有效性、执行溯源与数值可追踪性。在覆盖 5 类学科、4 类科学证据的 36 个真实数据案例中，系统完成了从原始数据到编译论文的全流程；与仅接收标量特征的盲化版本相比，直接感知在 7 个评估维度均有提升。

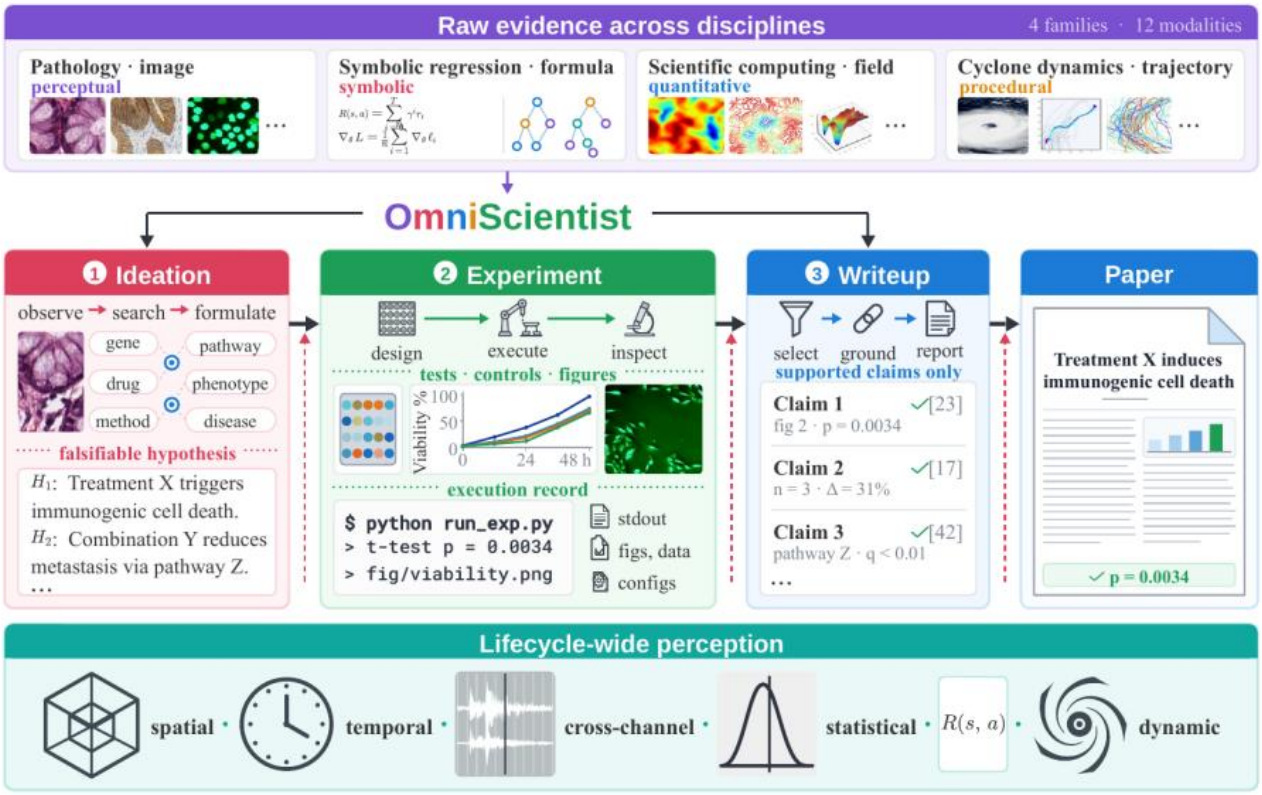


Figure 3. Architecture of the OmniScientist framework. At the top, raw evidence from multiple disciplines enters the system, categorized into four evidence families (perceptual, symbolic, quantitative, and procedural) and 12 modalities. The core pipeline consists of three sequential stages. First, the Ideation stage (left) observes materials, searches literature, and formulates falsifiable hypotheses. Next, the Experiment stage (center) designs tests, executes code, and inspects results to generate an execution record containing standard output, figures, data, and configurations. Finally, the Writeup stage (right) selects, grounds, and reports claims supported exclusively by the execution record to compile the final paper. At the bottom, a lifecycle-wide perception layer provides spatial, temporal, cross-channel, statistical, and dynamic analysis capabilities. Dashed arrows indicate that these perception tools are available to all three stages of the pipeline.

主要亮点

- 把多模态原始证据贯穿选题、实验决策和论文主张，而非仅作为前置特征。
- 以构思、实验、写作三个 Agent 配合确定性检查，强化统计与证据追踪。
- 在 36 个跨学科真实数据案例上验证端到端能力，突出科学感知对可靠发现的价值。

相关链接

Paper： https://arxiv.org/abs/2608.13558

Project： https://omni-scientist.github.io

● 论文九

Training AI Scientists to Replicate Research

日期

2026-08-13


inherent

14th August 2026

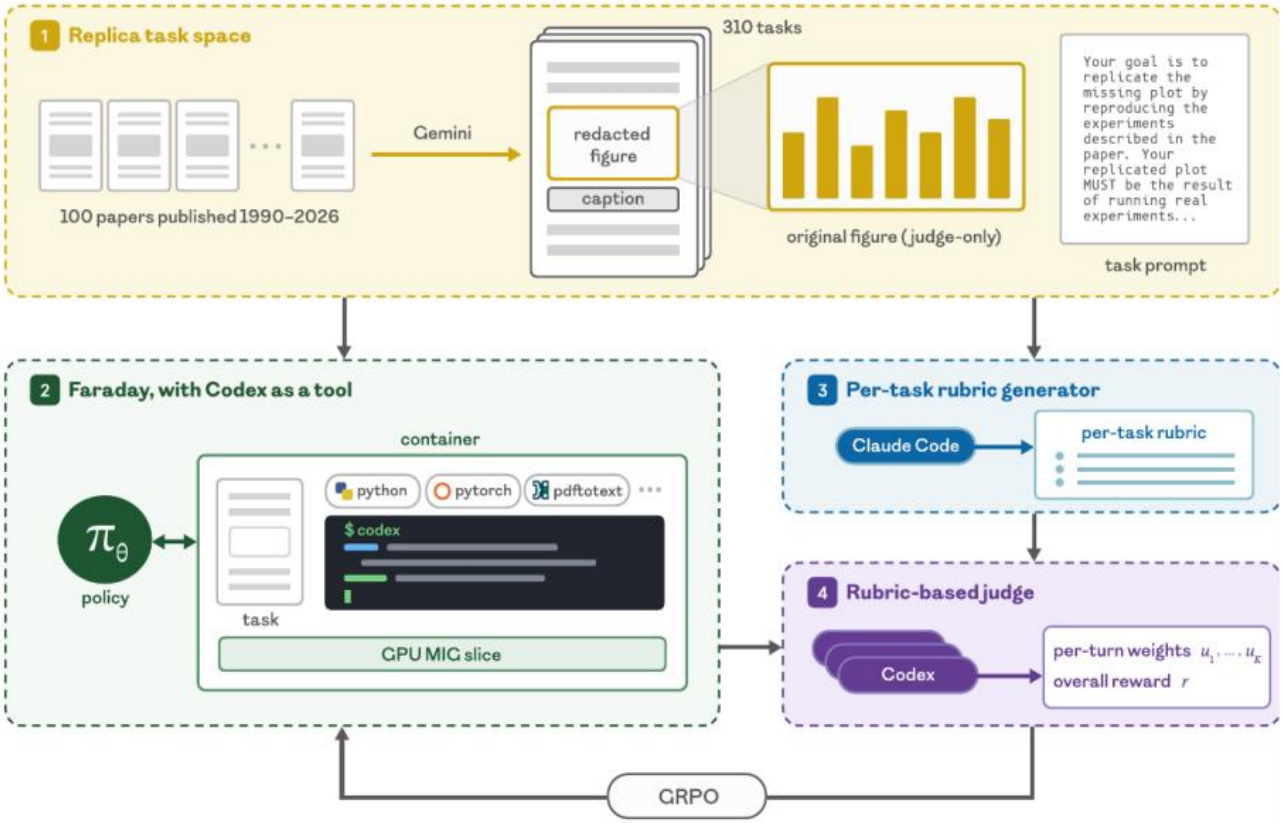
Training AI Scientists to Replicate Research

Damon Falck*,1, Samer Sabri*,1, Anja Surina[1], Thom Foster[1], Anya Sims[1], Sam Devlin[1], Dylan Rogers[1], Tantum Collins[1], Kaloyan Aleksiev§,1, Louis Kirsch†,1, Edward Hughes†,1

*Equal first author. §Infrastructure lead. †Equal last author. [1]Inherent

内容摘要

该研究把“复现实证论文”构造成可规模化训练与评估 AI 科学家的任务空间 Replica。论文复现不仅要求执行已有代码，还需要识别原文中未充分说明的细节、形成假设、排查实现差异并判断结果是否真正支持原结论。为提供稳定奖励信号，作者设计自动生成的量表式评审器，并验证其噪声较低、与人类对复现质量的判断一致。在此基础上，团队后训练了 27B 参数的 Faraday 科研 Agent，使其能够把编码 Agent 作为工具使用；在保留的复现任务上，论文报告 Faraday 超过 Claude Opus 4.8 和 GPT-5.5，并在案例分析中表现出更符合科学方法的排查路径。工作强调，复现训练可成为通往长周期科学创新的中间台阶。



主要亮点

- 将论文复现定义为包含假设驱动探索的科研任务，而非机械运行代码。
- 通过自动生成的 rubric 评审器提供可扩展奖励，并与人类评价进行一致性校验。
- 后训练 27B Faraday Agent，探索在较轻量 harness 下形成科研推理能力的路线。

相关链接

Paper:https://arxiv.org/abs/2608.13331

● 论文十

A Programming Paradigm for Spatiotemporal Composability

日期

2026-08-13

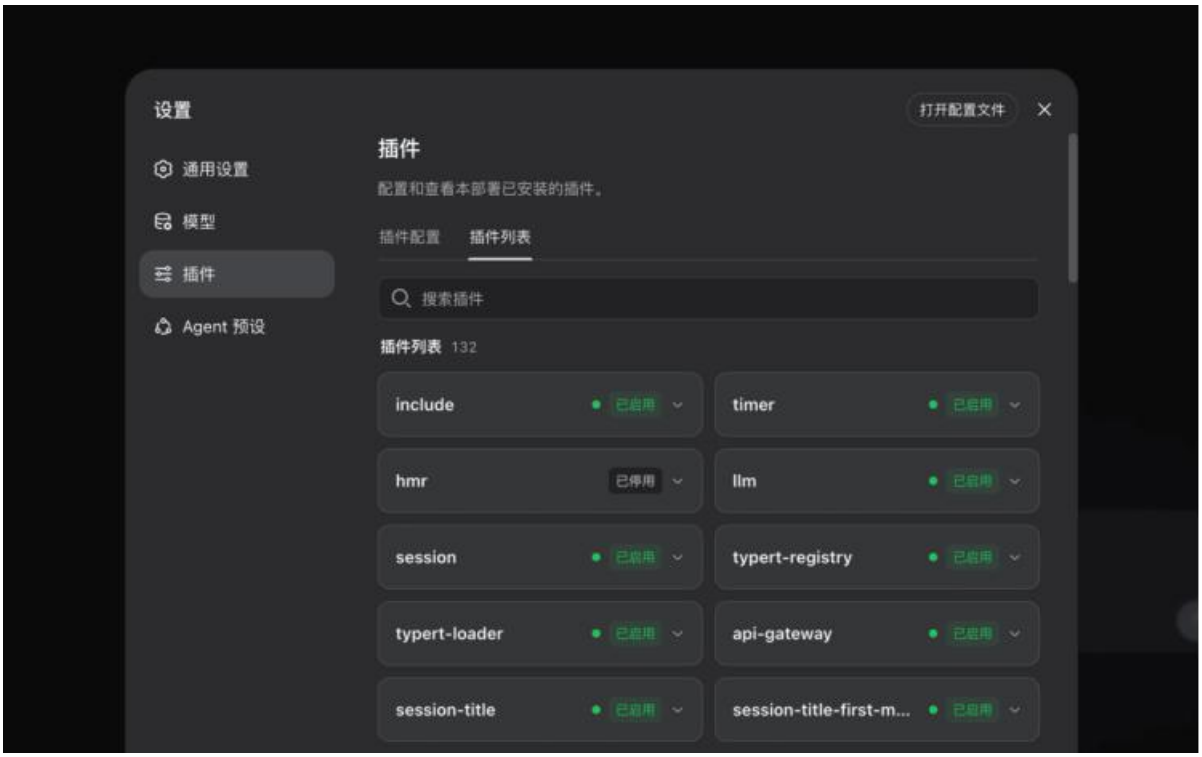


A Programming Paradigm for Spatiotemporal Composability

Yifan Shi[1,2], Wei Zhang[1], Tianyi Cui[2]
[1]Peking University [2]DeepSeek-AI

内容摘要

DeepSeek 开源 DeepSeek Harness（dsh）开发者预览版，将模型、工具、Skills、会话、沙箱、存储、循环、调度和 UI 等 Agent 能力统一抽象为可替换插件。底层 Cordis 内核只负责插件加载、卸载和依赖关系，开发者可在配置层组合能力，无需修改核心源码。系统采用仅追加的会话事件流，记录系统提示、工具调用与结果、子 Agent 调度和上下文注入，并支持恢复、分叉、检索与回放。官方提供标准、PTC、极简和创造等运行模式，覆盖完整编码 Agent、代码组合工具调用、最小基准环境和自定义 preset 创作。项目以 MIT 许可证开放且仍在快速迭代，基础 API 可能发生不兼容变化。



主要亮点

- 把 Agent 运行时的关键能力插件化，支持模型、工具、沙箱和 UI 自由替换组合。
- 仅追加会话日志让运行轨迹可追踪，并统一支持恢复、分叉、检索和回放。
- 多种预设兼顾生产探索、PTC 工具编排、最小化评测和插件生态开发。

相关链接

Project： https://www.deepseek.com/harness/
Code： https://github.com/deepseek-ai/deepseek-harness
Paper： https://arxiv.org/pdf/2608.25512

● 论文十一

How Claude is accelerating protein design and analytical chemistry

日期

2026-08-18

Autonomous *de novo* protein binder design with Claude

Claude Science[1] Amir Shanehsazzadeh[1,*]

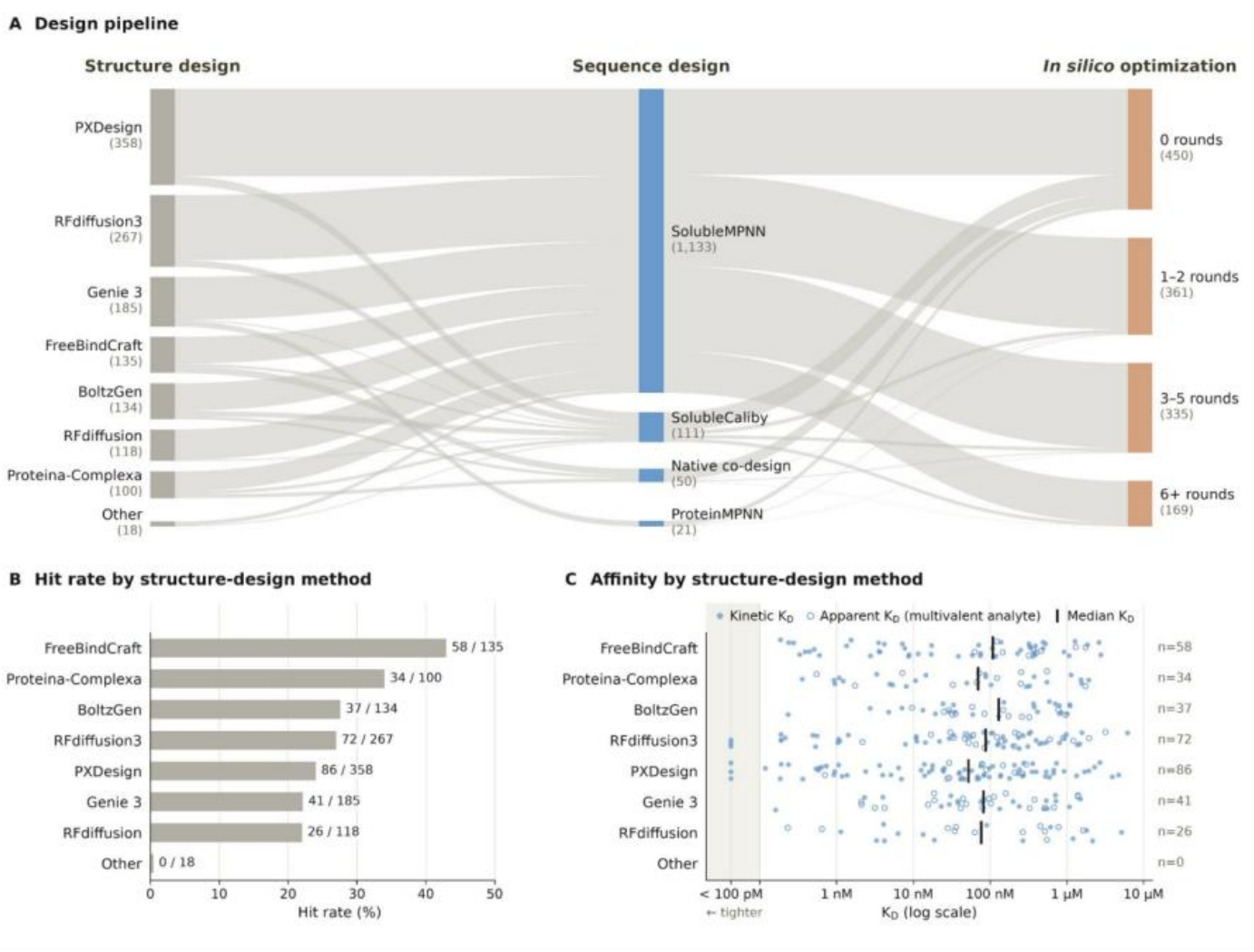
August 18, 2026

[1]Anthropic, San Francisco, CA, USA

*Correspondence: ashanehsazzadeh@anthropic.com

内容摘要

Anthropic 公布两组生命科学实验结果。第一组中，Claude Mythos Preview 与 Opus 4.8 自主编排专业蛋白设计和折叠工具，为 15 个靶点设计微型蛋白结合体，外部实验室在其中 14 个靶点上检测到成功结合；不同设置下单个设计的命中率约为 22%至 35%，高于文中给出的常见蛋白设计项目区间。第二组中，Claude Opus 5 接收合同实验室的原始 NMR 和 LC-MS 文件以及简短提示，在约 20 分钟内完成化学分析，氢原子计数和纯度判断与实验室结果接近。两项工作显示通用推理模型可减少复杂科研任务的人工编排时间，但湿实验成本、数据代表性、访问控制和独立复核仍决定其实际科研价值。



主要亮点

- 蛋白设计结果经过 Adaptyv Bio 和 Twist Bioscience 的外部湿实验测试。
- Claude 能够自主调用专业设计、折叠和筛选工具，缩短计算工作流的组织时间。
- 在分析化学任务中直接处理原始仪器数据，展示通用模型辅助日常科研分析的可能性。

相关链接

Research： https://www.anthropic.com/research/Claude-accelerates-protein-design

Technical Report： https://www-cdn.anthropic.com/30bf50e22a01388bb29bf077ee3f244531594b7a.pdf

● 论文十二

SWE-bench Science: Can Coding Agents Resolve Engineering Tasks in Science?

日期

2026-08-20

OpenMOSS

SWE-bench Science: Can Coding Agents Resolve Engineering Tasks in Science?

Zhipeng Xu[1,2], Jiahao Lu[1,2], Yining Zheng[1,2], Yuxin Wang[1,2,†], Xipeng Qiu[1,2,†]

[1]Shanghai Innovation Institute, [2]Fudan University

[†]Corresponding author: wangyuxin@sii.edu.cn, xpqiu@sii.edu.cn

内容摘要

SWE-bench Science 是面向科学软件工程的仓库级代码智能体基准，收集来自 20 个科学领域、98 个 GitHub 仓库的 119 个任务，并将任务划分为问题驱动、专家探索和工程集成三类范式。评测发现，即使是表现最好的 Claude Code with Opus-5（max），pass@1 仍低于 50%，说明科学代码修复同时要求工程能力与领域知识。论文归纳出科学知识或抽象能力不足、盲目探索或表层修复、修复覆盖与系统集成不完整、科学知识难以迁移四类常见失败机制，并通过消融实验分析显式科学指导的作用：可靠指导可提升平均性能和 token 效率，失配指导则可能造成锚定，未必提高精确修复成功率。

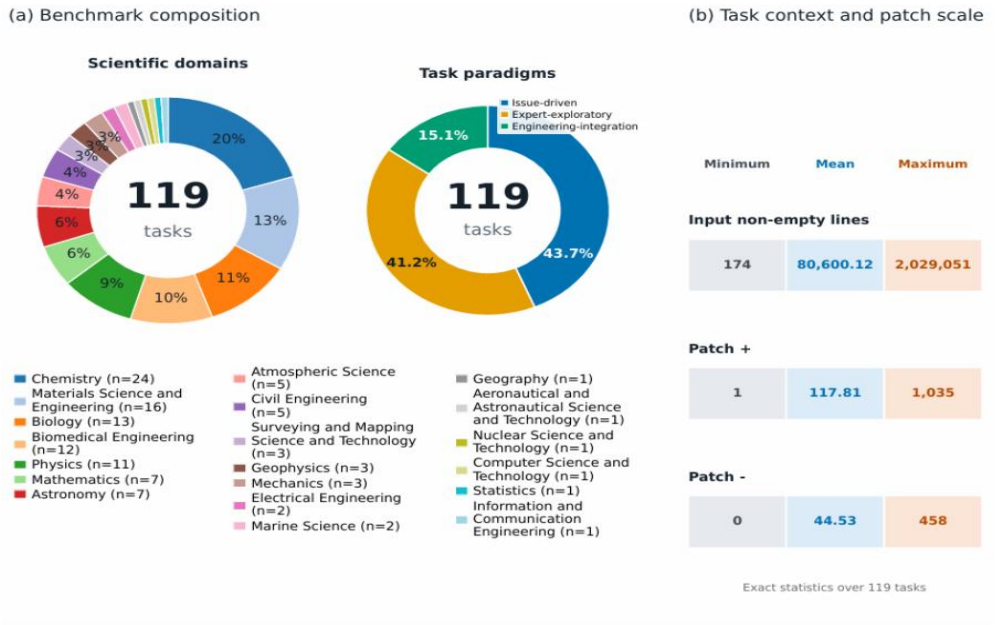


Figure 2 Benchmark coverage and scale over 119 tasks. (a) Scientific-domain distribution and task-paradigm composition. The domain legend reports the task count for each of the 20 domains; the task-paradigm chart contains 52 Issue-driven tasks (43.7%), 49 Expert-exploratory tasks (41.2%), and 18 Engineering-integration tasks (15.1%). Chemistry is the largest domain with 24 tasks, followed by Materials Science and Engineering with 16, Biology with 13, Biomedical Engineering with 12, and Physics with 11. (b) Minimum, mean, and maximum input and reference-patch sizes, shown directly in horizontal summary bands. Input size is measured as non-empty physical lines in the task code, while Patch + and Patch − count additions and deletions in the standard reference diff.

主要亮点

- 首个面向科学软件工程的 SWE-bench：覆盖 20 个科学领域、98 个仓库和 119 个真实任务。
- 三类任务范式：问题驱动、专家探索与工程集成，兼顾缺陷修复、科学推理和系统级改动。
- 揭示代码智能体的科学工程短板：最佳系统 pass@1 仍低于 50%，失败涉及知识、探索、集成和泛化。
- 分析科学指导的双刃剑效应：高质量知识可约束修复并提升效率，错误指导可能导致锚定。

相关链接

Paper： https://arxiv.org/abs/2608.19799
Code： https://github.com/OpenMOSS/SWE-bench-Science
Data： https://huggingface.co/datasets/OpenMOSS-Team/SWE-bench-Science
Leaderboard： https://swescience.github.io

TECHNICAL UPDATES
技术动态

技术动态一

OpenAI 官方 Prompt 指南：用目标、上下文、输出和边界组织高质量任务

日期

2026-07-11（中文转载发布日期）

Prompting

Write useful prompts for Chat, ChatGPT Work, and Codex

Prompting overview

Prompting is how you tell ChatGPT what you want to know, make, or change. A prompt can be a question, an instruction, or a goal. You don't need technical syntax or a rigid formula. Start in your own words, review the response, and use follow-up messages to shape the result.

A short prompt is often enough. For larger or more important tasks, include the parts that matter:

- **Goal:** What should ChatGPT do?
- **Context:** What information or sources will help?
- **Output:** What format, length, or level of detail do you need?
- **Boundaries:** What must stay unchanged? What should ChatGPT avoid or check with you before it acts?

Use only the parts that help. You don't need to fill in every item or follow a required format.

内容摘要

OpenAI 官方 Prompt 指南强调，提示词不需要固定公式，最重要的是先说明希望得到的结果，再补充真正会改变答案的上下文、输出要求和行动边界。对于较大任务，可使用“目标、上下文、输出、边界”四要素：明确要完成什么，提供必要文件或来源，说明受众、长度和格式，并指出哪些内容不能改、哪些动作需要先确认。指南还建议用后续消息逐步修正结果，重要工作在结束前增加可核验的终检要求；在 Work 或 Codex 任务中，应让系统自行规划、调用工具、创建文件和执行检查，而不是把每一步写死。该方法适用于简报、调研、代码修改和多工具工作流。

相关链接

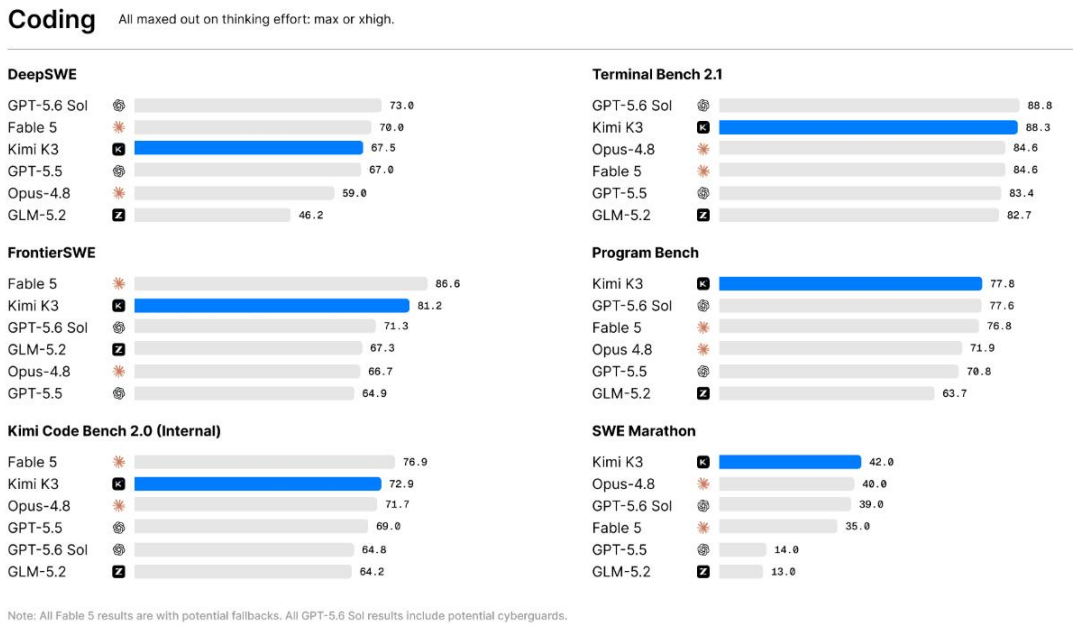
Official Guide： https://learn.chatgpt.com/docs/prompting

• 技术动态二

Kimi K3 发布：2.8 万亿参数开源模型瞄准前沿编程与长程 Agent

日期

2026-07-17



内容摘要

月之暗面推出 Kimi K3。公开信息显示，该模型采用 2.8 万亿总参数、约 1040 亿激活参数的混合专家架构，支持百万级上下文，并把前端开发、交互式 3D 和长程 Agent 任务作为重点能力。发布初期，国内外开发者通过网页应用、游戏原型和复杂编码任务进行体验，普遍关注其生成质量、视觉审美和多步执行能力，同时也指出推理速度较慢、API 价格较高以及官方评测条件与第三方场景可能存在差异。K3 的意义不只在参数规模，而在于中国开源模型开始从“低成本可用”向“高能力、可部署的前沿系统”转变；但真实生产价值仍需结合延迟、成本、工具链和独立评测判断。

相关链接

Official Guide： https://www.kimi.ai/ai-models/kimi-k3
Technical Report： https://github.com/MoonshotAI/Kimi-K3/blob/main/k3_tech_report.pdf

• 技术动态三

Claude Opus 5 发布，Anthropic 以“减少上下文负担”重构 Agent 协作方式

日期

2026-07-27



内容摘要

Anthropic 发布 Claude Opus 5，并同步分享面向新一代 Claude 模型的上下文工程经验。报道显示，Opus 5 在编码、知识工作、计算机操作和部分科研评测中较上一代提升，同时提供 effort 设置，让用户在能力、速度与 token 成本之间调节。更具方法论意义的是，Anthropic 为 Claude Code 删减了 80%以上系统提示内容，而编码评测未出现可测下降。团队据此提出：对更强模型，应从堆叠硬规则转向提供判断空间，从大量示例转向清晰接口，从一次性塞入所有材料转向渐进式披露，并将验证、代码审查和领域知识拆成按需加载的 Skills。该变化表明 Agent 工程的重点正由“约束模型每一步”转向“设计好环境、工具和信息结构”。

相关链接

Official Guide： https://www.anthropic.com/news/claude-opus-5
Blog： https://claude.com/blog/the-new-rules-of-context-engineering-for-claude-5-generation-models

技术动态四

Nature 2026 大模型研究脉络综述：从后训练与可信评测到科研 Agent

日期

2026-07-27



内容摘要

这篇综述汇集了 2026 年 1 月 1 日至 7 月 27 日发表于 Nature 正刊的 14 篇大模型论文（13 篇 Article、1 篇 Perspective），覆盖模型训练、能力评测、安全对齐与科研自动化。整体脉络显示，前沿研究的焦点正由“模型能否做得更强”转向“能力如何形成、风险如何测量、系统如何在真实任务中可靠闭环”。

第一条主线是模型与后训练。Emu3 以统一的下一词元预测连接文本、图像与视频生成；涌现失配、潜意识学习、温暖表达与迎合效应等研究则提示，局部微调可能通过隐含统计信号造成跨任务行为外溢。训练语料中的立场分布也会持续影响模型输出，因此后训练不仅要看目标任务收益，还应加入跨域回归测试、数据溯源和行为审计。

第二条主线是评测与可信度。Humanity’s Last Exam 把评测推向专家级知识边界，General Scales 进一步强调“模型能力—任务需求”的匹配；关于准确率激励与幻觉的研究说明，只奖励答对可能诱导模型在不确定时继续猜测。评测应从单一总分扩展到校准度、拒答能力、分层能力画像与分布外稳定性。

第三条主线是科研 Agent 与知识生产。OpenScholar、AI Scientist、ERA 与 Co-Scientist 分别推进证据检索、假设生成、代码实验、结果评估和迭代优化；对社会实验结果的预测则展示了大模型作为“计算研究对象”的潜力。科研 Agent 正在形成闭环，但高风险环节仍需可执行评测、可追溯证据与人工复核。

相关链接

链接：https://mp.weixin.qq.com/s/fk2EkyuG6dd06QilFxbwfg?scene=1&click_id=1840886142

paper list：

https://www.nature.com/articles/s41586-025-09937-5

https://www.nature.com/articles/s41586-025-09962-4

https://www.nature.com/articles/s41586-025-10041-x

https://www.nature.com/articles/s41586-025-10072-4

https://www.nature.com/articles/s41586-025-10021-1

https://www.nature.com/articles/s41586-026-10265-5

https://www.nature.com/articles/s41586-026-10303-2

https://www.nature.com/articles/s41586-026-10319-8

https://www.nature.com/articles/s41586-026-10549-w

https://www.nature.com/articles/s41586-026-10410-0

https://www.nature.com/articles/s41586-026-10506-7

https://www.nature.com/articles/s41586-026-10658-6

https://www.nature.com/articles/s41586-026-10644-y

https://www.nature.com/articles/s41586-026-10742-x

技术动态五

Kimi K3 完整权重与技术报告开放：重点解决长程 Agent 状态、训练与验证

日期

2026-07-28

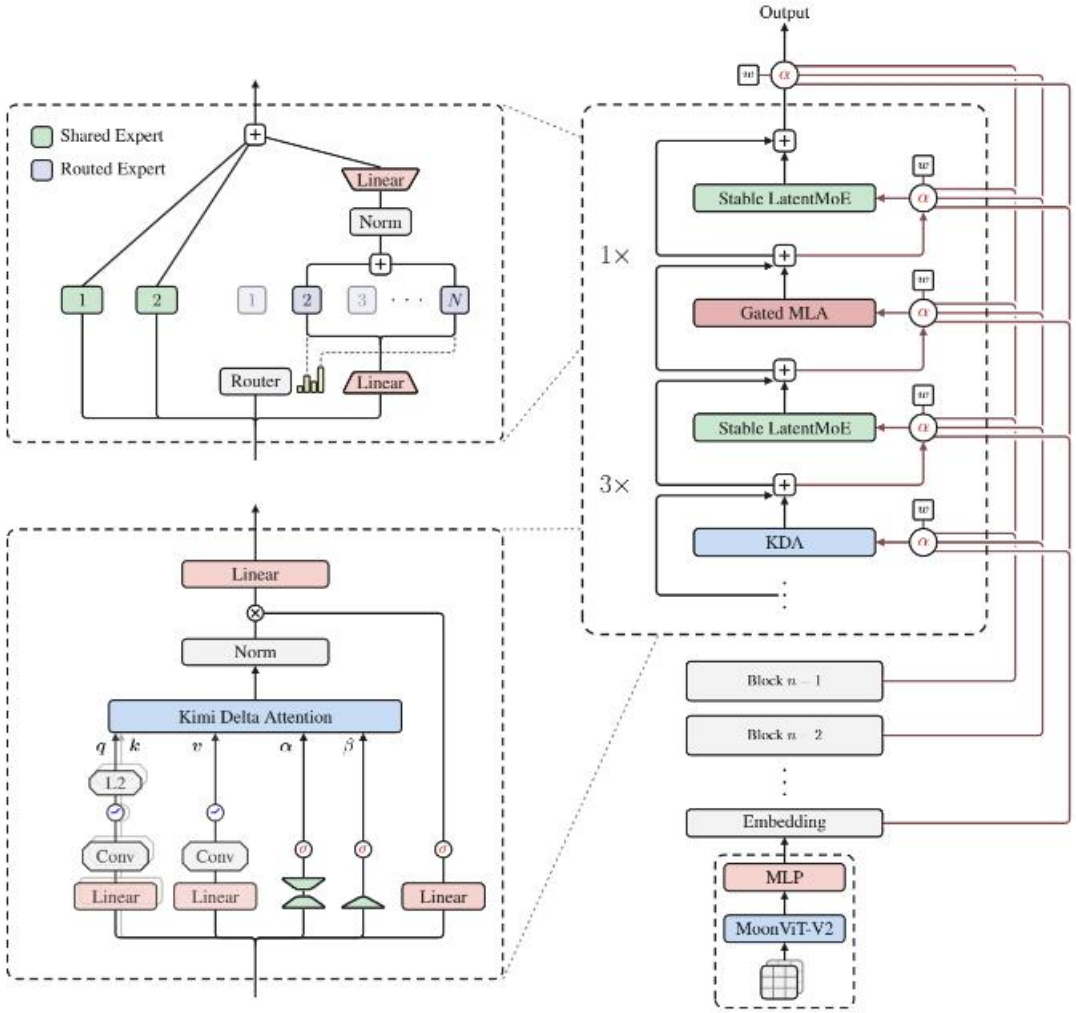


Figure 2: The Kimi K3 architecture, organized around token, channel, and layer mixing, with a native vision pathway at the input. Each block contains three Kimi Delta Attention (KDA) layers followed by one Gated MLA layer, with each attention layer paired with a Stable LatentMoE feed-forward network. Attention Residuals (AttnRes) use learned pseudo-queries (w) to derive attention weights (α) over the embedding and preceding block outputs, enabling selective information flow across depth. **Top left**: the Stable LatentMoE module with shared and routed experts. **Bottom left**: the KDA module. **Bottom right**: the native vision pathway.

内容摘要

Kimi K3 开放完整权重和技术报告后，其技术路线得到更清晰呈现。模型以 KDA 循环状态与 Gated MLA 全局注意力交替组合，在百万 token 窗口下兼顾固定大小的工作记忆和周期性全局交互；Block Attention Residuals 帮助 93 层深网重新访问早期层表示。MoE 部分包含 896 个路由专家，每个 token 激活 16 个路由专家及共享专家。后训练方面，K3 把通用、通用 Agent 和编码 Agent 与不同推理强度组合为多教师体系，并通过会变化的工具、提示词、Skills、记忆和 harness 环境减少对固定考场的过拟合。AET 任务、隐藏验证器与可恢复沙箱则用于缓解长任务中断和“骗分”问题。

相关链接

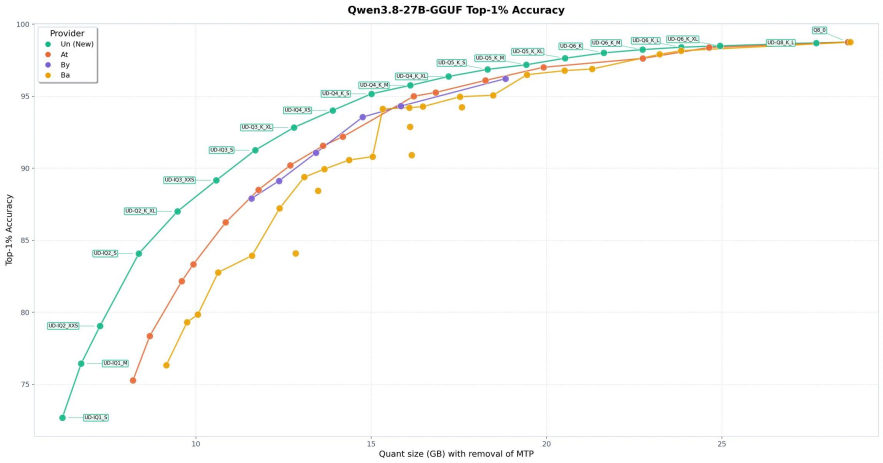
Model： https://huggingface.co/moonshotai/Kimi-K3
Technical Report： https://github.com/MoonshotAI/Kimi-K3/blob/main/k3_tech_report.pdf

● 技术动态六

Unsloth Dynamic 3.0 GGUFs：面向 Qwen3.8-27B 的高精度动态量化资源

日期

2026-08



内容摘要

Unsloth 发布 Dynamic 3.0 GGUF 量化方法及 Qwen3.8-27B 量化模型，目标是在相近文件体积下尽量保持高精度。模型仓库提供从 1-bit 到 8-bit 及 BF16 的多档版本，覆盖约 6 GB 至 55 GB 的不同内存预算，并可通过 llama.cpp、Ollama、Docker Model Runner 和 Unsloth Desktop 等工具运行。官方页面称 Dynamic 3.0 在同尺寸量化比较中具有更高准确率，并针对 Qwen3.8 改进工具调用、开发者角色和 Agent 工具兼容性。对本地用户而言，该资源的价值在于可按硬件选择精度与速度平衡；但“量化精度提升”仍应结合自身任务、上下文长度和设备进行实测。

相关链接

Docs： https://unsloth.ai/docs/basics/dynamic-3.0-ggufs

Model： https://huggingface.co/unsloth/Qwen3.8-27B-GGUF

• 技术动态七

小红书开源 dots.tts：2B 全连续端到端语音合成系统输出 48 kHz 音频

日期

2026-08-10

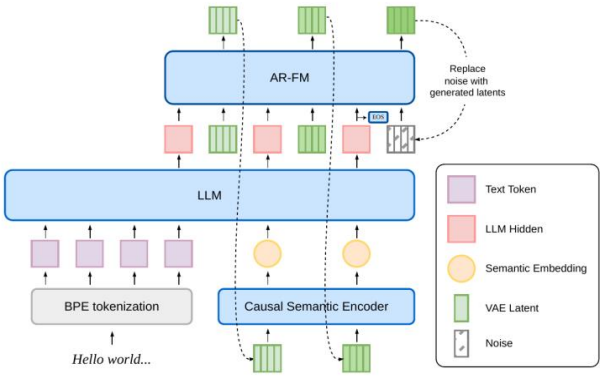


Figure 1: Overview of the dots.tts backbone. BPE text tokens and 6.25 Hz audio-semantic embeddings share a single LLM stream; each LLM hidden state conditions the AR-FM head to generate the next four-frame VAE-latent patch, which is fed back through the semantic encoder at the next step. The AudioVAE (Section 2.2) is trained separately and frozen here.

内容摘要

小红书 dots studio 开源 dots.tts 及基础模型 dots.tts-base。该系统采用 2B 参数的全连续端到端自回归架构，不依赖离散语音 codec token：冻结的 AudioVAE 将 48 kHz 波形压缩为连续潜变量，语义编码器提取紧凑语音表示，基于 Qwen2.5-1.5B 初始化的 LLM 直接读取 BPE 文本，自回归 flow-matching 声学头逐块生成潜变量。基础模型使用约 150 万小时语音预训练，支持零样本音色克隆，并作为微调与两个后训练版本的底座。官方模型卡同时给出中英文、多语言评测、命令行和 Python 接口。项目以 Apache 2.0 开放，但高保真音色克隆涉及冒充和欺诈风险，部署时应取得授权并标识合成音频。

相关链接

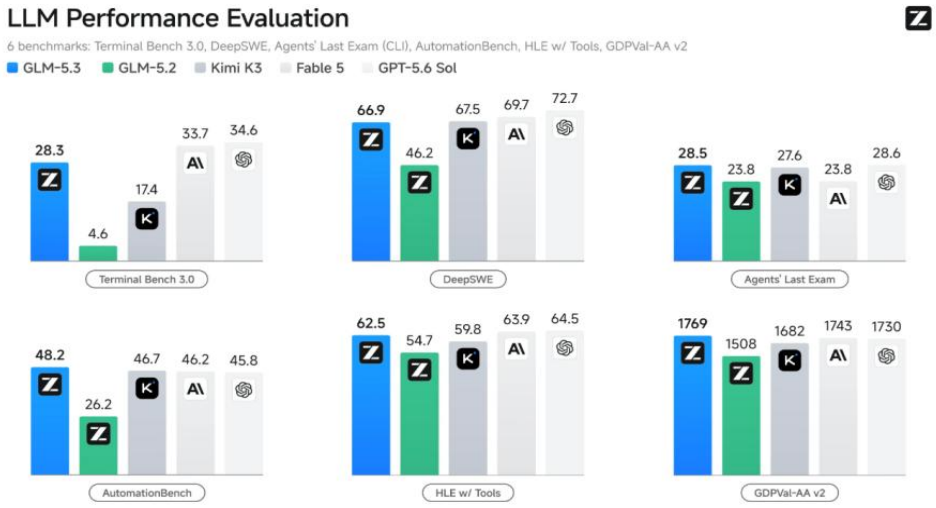
Model： https://huggingface.co/dots-studio/dots.tts-base
Code： https://github.com/studio-dots-ai/dots.tts
Collection： https://huggingface.co/collections/dots-studio/dots

技术动态八

GLM-5.3：Frontier Coding with Emergent Cyber Capabilities

日期

2026-08-14



内容摘要

智谱发布 GLM-5.3，在 GLM-5.2 基础上通过后训练缩放显著增强编程、长程 Agent 和网络安全能力。官方数据显示，模型在 Terminal-Bench 3.0、DeepSWE v1.1 和 Agents' Last Exam 等任务上较前代大幅提升，并在多项评测中达到或超过 Claude Fable 5、GPT-5.6 等前沿模型水平。随着后训练规模扩大，GLM-5.3 出现了超出预期的网络安全能力，在漏洞发现和利用相关测试中表现突出；智谱因此同步强化安全评估与披露机制，并对权重公开采取延迟安排。

相关链接

技术博客：https://z.ai/blog/glm-5.3

技术动态九

阿里巴巴开源 Qwen3.8-27B

日期

2026-08-14



内容摘要

阿里巴巴开源 Qwen3.8-27B，这是 Qwen 系列面向编程、专业工作、科研和长程 Agent 任务的新一代 27B 级稠密模型。模型原生支持图像和视频理解，提供可调节的思考深度与推理强度，原生上下文长度达到 262K，并可扩展至百万 token；模型卡显示其在 SWE-bench Pro、LiveCodeBench、OSWorld-Verified、AndroidWorld 等多项评测中超过上一代 Qwen，并在部分指标上超过 Opus 4.6。模型发布后在 Hugging Face 社区持续受到高度关注，成为开源模型生态的热门项目。

相关链接

Model： https://huggingface.co/Qwen/Qwen3.8-27B

• 技术动态十

Qwen3.8-27B 开源：27B 稠密原生多模态模型强化代码、Agent 与本地部署

日期

2026-08-18

	Qwen3.8-27B	Qwen3.6-27B	Qwen3.7-Plus	Muse Glimmer-30B	Opus4.6 Max
Coding					
Agentic terminal coding Terminal Bench 2.1 (Terminus)	73.0	63.4	64.0	51.7	**78.2**
Agentic coding SWE-bench Pro	**61.7**	53.5	57.6	51.2	53.4
Repo-level code generation NL2Repo-Bench	42.3	36.2	41.1	--	**47.6**
Agentic coding DeepSWE 1.1	**42.2**	13.3	14.2	--	--
Software engineering QwenSWEBench	**79.0**	49.3	59.2	--	63.8
Agent					
Long-horizon office work CoWorkBench	**70.7**	61.0	65.1	--	68.2
Professional job tasks JobBench	**33.4**	21.8	27.6	--	--
Frontier agentic tasks Agents' Last Exam	Pass@1 **20.4** Score **42.9**	Pass@1 10.6 Score 27.3	Pass@1 13.2 Score 33.6	--	--
General					
Instruction following IFBench	**79.5**	69.1	79.1	77.0	62.5
Scientific reasoning GPQA Diamond	89.2	87.8	90.3	83.5	**91.3**
Multidisciplinary reasoning HLE	30.8	24.0	34.7	22.0	**40.0**
Competitive coding LiveCodeBench v6	**90.3**	83.9	89.6	--	88.8

内容摘要

Qwen 团队开源 Qwen3.8-27B。这是一款 27B 参数的稠密视觉语言模型，原生支持图像与视频理解，具备 262K 上下文并可通过扩展技术覆盖更长输入。模型重点提升编程、专业知识工作、研究和长周期 Agent 任务，思考模式默认开启，开发者可按请求关闭，并用 reasoning_effort 调节推理深度。其参数规模使量化后本地部署更现实：社区提供从低比特到高精度的多种 GGUF 版本，可通过 llama.cpp、Ollama 等工具运行。公开评测与早期体验显示其在软件工程、计算机操作和视觉推理上具备较高能力密度，但跨模型比较仍需关注推理强度、工具环境、量化损失和硬件配置。

相关链接

Model： **https://huggingface.co/Qwen/Qwen3.8-27B**

技术动态十一

DeepSeek 首个多模态模型发布：V4-Flash-Vision-Exp 上线 API

日期

2026-08-21

Benchmark		DeepSeek V4-Flash-Vision-Exp	DeepSeek V4-Flash- 0731	Opus-4.8
文本 Agent 能力评测*	Terminal Bench 2.1	83.9	82.7	85.0
	NL2Repo	57.7	54.2	69.7
	Cybergym	75.3	76.7	78.3
	DeepSWE	59.3	54.4	58.0
	Toolathlon-Verified	75.9	70.3	76.2
	DSBench-Hard	63.6	59.6	71.7
	AutomationBench (Public)	25.7	25.1	27.2
多模态 Agent 能力评测	ApexBench (Pass@1)	36.5	26.2**	39.4
	Agents' Last Exam	27.3	25.2**	25.7
	Chartography	64.3	-	65.0
	ZeroBench (Pass@5)	35.0	-	34.0

内容摘要

DeepSeek 首个多模态模型 DeepSeek-V4-Flash-Vision-Exp 正式上线 API 平台。这是一款实验性质的视觉理解模型，可直接接收图片并接入 Agent 工作流；在纯文本的 Agent、推理和世界知识任务上与 V4-Flash 基本持平，而在 ApexBench、Agents' Last Exam 等需要视觉理解的评测中明显提升，官方称其多模态 Agent 能力已接近 Opus-4.8。开发者可通过 Chat Completions、Messages 或 Responses 接口调用，图片支持 Base64、外部 URL 和 Files API 三种输入方式，单张图片最多计 384 Tokens，价格与 V4-Flash 保持一致；同步上线的 Files API 可用 file_id 复用图片且暂不收费。此次更新标志着 DeepSeek 的视觉能力开始从模型展示走向 API 服务，并进一步融入多模态 Agent 工作流。

相关链接

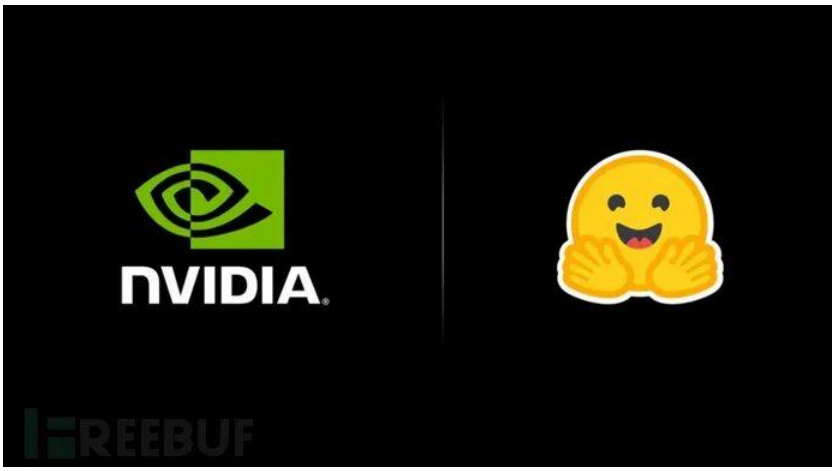
https://api-docs.deepseek.com/updates/

• 技术动态十二

NVIDIA 据悉洽谈收购 Hugging Face，估值或超 130 亿美元

日期

2026-08-27



内容摘要

据媒体报道，NVIDIA 正与开源 AI 模型平台 Hugging Face 就潜在收购进行洽谈，Hugging Face 的潜在估值或超过 130 亿美元。若交易达成，NVIDIA 的影响力将从 GPU 与 CUDA 等底层基础设施延伸到模型托管、开发工具和开源社区分发层，有助于整合软硬件生态。报道同时引发对平台中立性、开源社区治理和资源配置的讨论；截至目前，NVIDIA 与 Hugging Face 均未对收购传闻作出正式确认，因此相关估值与谈判进展仍应视为市场消息。

相关链接

https://securityonline.info/nvidia-hugging-face-acquisition/

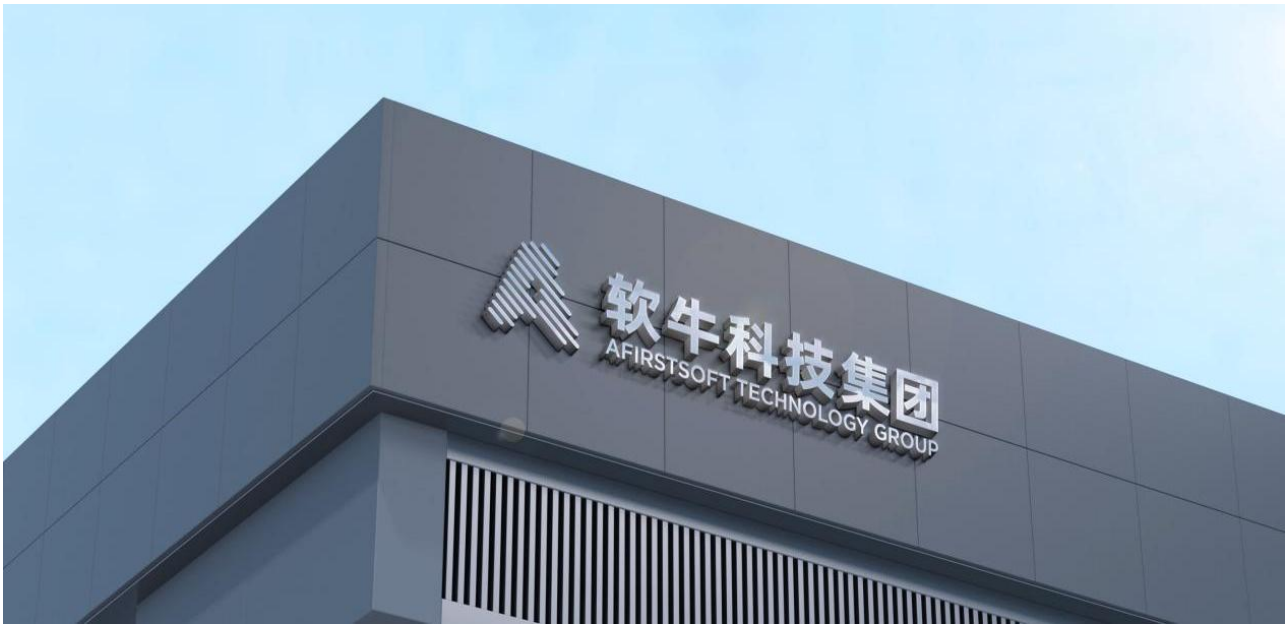


深圳软牛科技集团股份有限公司成立于 2014 年 6 月，作为国家级专精特新“小巨人”企业，始终以“让创意成为现实”为使命，专注于通过人工智能视觉大模型技术驱动全球数字创意生态。

公司深度聚焦图像修复、视频增强、多模态内容生成等视觉大模型核心技术，联合西安电子科技大学、香港中文大学（深圳）等顶尖高校，攻克了视频抠像、画质修复等难题，并与深圳大学共建“人工智能技术联合创新中心”，推动 AI 赋能的图像增强技术规模化落地。

目前，软牛科技能够为广电机构、影视制作、工业检测、农业测报等多个行业提供专业解决方案。从微米级工业精密测量，到食品异物智能检测；从农业害虫 AI 识别防治系统，到 AR 设备巡检实时画面 AI 增强与场景识别；从 VR 全息空间建模助力文博展陈数字化升级，到跨终端智能影像协作软件的全链路画质优化引擎，软牛科技正以技术革新重新定义新质生产力。

在消费级市场，旗下牛小影（https://www.niuxuezhang.cn/video-enhancer.html）、HitPaw 等海内外知名品牌，以“一键式 AI 视觉创意”为核心，为全球超 1 亿用户提供视频修复、老电影 AI 上色等场景化服务。例如，牛小影支持 4K 或 8K 超高清修复技术，帮助家庭用户重现祖辈黑白影像的生动细节；HitPaw Edimakor 通过 AI 语音合成、多语言实时翻译等功能，让自媒体创作者轻松实现跨语言内容生产。



这些创新成果的背后，是公司每年近亿元的研发投入和占比超 50%的顶尖技术团队，以及 CMMI、ISO56005 等国际权威认证体系支撑的硬核实力。立足深圳总部，我们通过北京、新加坡、香港等战略支点构建起辐射全球 200 多个国家和地区的智慧服务网络。作为高新技术企业、深圳市潜在科技独角兽，软牛科技始终以“技术无界”为理念，持续拓展 AIGC+产业应用的边界。

未来，软牛科技将加速推进物理世界与 AI 视觉的无缝衔接，让每个人都能通过指尖的艺术级创作，开启属于自己的数字时代。

人工智能前沿快报

Artificial Intelligence Newslettler

2026 年第 7 期

总第 32 期

广东省图象图形学会

主办 广东省图像图形学会

本期编委

金连文	华南理工大学
谭明奎	华南理工大学
钟亦武	北京大学
林上港	华南农业大学
李　斌	深圳大学
谢晓华	中山大学
王泽宇	香港科技大学（广州）
李冠彬	中山大学
段纪伟	金山办公
孙　成	金山办公
闫鹏宇	华南理工大学
刘俊乐	华南理工大学
许毅平	华南农业大学
蔡沐含	华南农业大学



人工智能前沿快报

2026 年第 7 期
总第 32 期
2026.09.01

声明：

（1）本快报内容提要、文章亮点等部分内容由 AI 生成，不一定准确及全面，章完整内容及思想应以原文为准。

（2）本文大部分插图来源于相关论文或文章，版权归原作者或原出版社所有。

（3）本快报摘录文章观点不代表编委会及主办方立场。

学会官方公众号

广东省图象图形学会
GDSIG
学术交流、技术咨询、科学普及