

教育垂直大语言模型的系统框架：从建构主义到“教育宪法”的理论、技术与对齐

丁勇
潍坊科技学院

摘要 本文面向教育垂直领域提出一套“理论—数据—模型—对齐—评测—治理”的系统性框架，以建构主义为方法论锚点，重塑教育大语言模型（Edu-LLMs）的目标函数与工程路径。首先，提出以教材知识图谱与概念先修关系为核心的结构化语料构建范式，并警示“结构性幻觉”的风险，给出专家在环、跨源交叉与概率图谱的校验机制。其次，在能力注入层面，提出以苏格拉底式对话与链式思维（CoT）为主轴的指令微调方案，结合“院长-教师-学生”的多智能体合成数据流水线以保证“教学有效性”。再次，面向多模态教育场景，界定“感知-认知鸿沟”，倡议多模态链式思维（M-CoT）与神经-符号式融合以实现证据可溯的推理。对齐层面，比较 RLHF/DPO 与宪法 AI，提出将教育学原则形式化为“教育宪法”的可编程对齐框架，并讨论其治理悖论与伦理边界。与此同时，给出联邦学习与差分隐私的隐私保护路径，以及以 TutorBench/MRBench 等为代表的教育评测思路与对抗性评估。最后，提出“教师在环”的人机协同范式与“AI 教学工程师”等新兴角色，并以 RAG+PEFT 支撑可持续迭代与低成本部署。本文旨在为 Edu-LLMs 提供可验证、可解释且可落地的技术蓝图。

关键词 教育大语言模型；建构主义；苏格拉底式对话；多模态链式思维；感知-认知鸿沟；教育宪法

DOI <https://doi.org/10.6914/aiescn.010202> **文章编号** 3079-7918.2025.0102.17-29

引言：从通用大模型到教育专用大模型的范式转移

（一）通用大语言模型在教育领域的潜力与教学缺陷

近年来，以 Transformer 架构为基础的大语言模型（LLMs）取得了突破性进展，展现出强大的语言理解与生成能力。^①以 ChatGPT、Gemini 等为代表的通用大语言模型（General-Purpose LLMs）迅速渗透到社会各个领域，其在教育场景中的应用潜力也备受瞩目。诸如谷歌的 LearnLM 和可汗学院的 Khanmigo

© The Author(s) 2025. Article History Received: 1 July 2025; Accepted: 5 August 2025; Published: 30 September 2025. 人工智能教育研究 (Réngōng Zhìnéng Jiàoyù Yánjiū) Artificial Intelligence Education Studies, ISSN 3079-7918 (Print), ISSN 3079-7926 (Online). Hosted by Artificial Intelligence Education Studies Press (Certificate No.70125648-007), and published by Creative Publishing Co., Limited (CPCL®) in Hong Kong. Email: cpcl@cpcl.hk, wtocom@gmail.com, <https://aies.press>, <https://cpcl.hk>. Repository: <https://pdf.ssci.cc/index.html>. This is an open-access article distributed under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International License, which permits use, sharing, and redistribution in any medium or format, provided the original author(s) and source are credited, but does not allow modifications or adaptations of the work.

^①OpenAI, “Improving Language Understanding by Generative Pre-Training,” 2018.

等前沿应用,已经开始利用大模型提供个性化学习路径、多模态内容呈现和交互式辅导,初步展示了 AI 变革教育的巨大潜力。^①

然而,通用大模型在教育这一特殊领域的应用并非坦途。这些模型的设计初衷是成为高效的信息提供者和任务执行者,其优化目标通常是“有求必应”地满足用户指令。这种特性在教育场景中可能适得其反,形成了显著的“教学缺陷”(pedagogical defect)。教育的核心目标之一是培养学生的批判性思维、问题解决能力和自主学习能力,这往往需要一个引导、启发而非直接告知答案的过程。^②通用模型倾向于直接提供完整答案的行为,可能会剥夺学生宝贵的“有益的困难”(desirable difficulty)过程,从而阻碍深度学习的发生。^③此外,通用模型固有的幻觉(hallucination)、知识偏见、事实错误等问题,在对准确性和安全性要求极高的教育领域,其负面影响被显著放大,对学习者的可能造成误导。^④

(二)理论根源:商业优化目标与建构主义学习理论的冲突

通用模型的“教学缺陷”并非简单的技术瑕疵,而是其设计理念与现代教育理论之间根本性冲突的外在表现。这种内在张力源于商业优化目标与教育学原则的深刻矛盾。^⑤通用模型本质上是信息传递范式的产物,其核心功能是将信息高效地从模型传递给用户,其成功与否很大程度上取决于用户粘性,而这通常通过快速、准确地提供答案来提升用户满意度。^⑥

然而,现代教育理论,特别是建构主义(Constructivism),早已指出学习并非被动的信息接收,而是学习者基于已有知识和经验,主动建构新知识意义的过程。^⑦皮亚杰(Piaget)等建构主义先驱认为,知识无法被简单地传递,而必须由学习者通过与环境的互动主动构建。^⑧有效的教学应为学习者提供“认知脚手架”(Cognitive Scaffolding),通过启发式提问、引导性反馈和适度挑战,帮助学习者在自己的“最近发展区”(Zone of Proximal Development)内进行探索。^⑨从这个理论视角看,通用大模型直接提供答案的行为,恰恰绕过了知识建构的关键环节。

这种内在的张力进一步体现在两者优化目标的时间维度冲突上。商业模型追求即时用户反馈和短期参与度指标的最大化,例如问题解决速度和会话时长。而教育学的核心,特别是建构主义理论所倡导的认知发展,本质上是一个缓慢、迭代、长周期的过程。^⑩因此,一个为短期满足而设计的系统,其内在激励机制必然会倾向于绕过或缩短促进长期发展的必要认知过程。这一根本性的矛盾催生了构建教育垂直领域专用大语言模型(Educational Large Language Models, Edu-LLMs)的必要性与紧迫性。

(三)“教学护城河”:调和商业可行性与教育完整性

这种设计理念上的冲突引出了一个关乎现实可行性的关键问题:一个刻意制造“有益困难”而非追求

^①Google, “Learn Your Way: Reimagining textbooks with generative AI,” 2024, <https://research.google/blog/learn-your-way-reimagining-textbooks-with-generative-ai/>.

^②Center for Excellence in Teaching and Learning, “Critical Thinking and other Higher-Order Thinking Skills,” <https://cetl.uconn.edu/resources/design-your-course/teaching-and-learning-techniques/critical-thinking-and-other-higher-order-thinking-skills/>.

^③R. Yu, et al., “Evaluating an AI Tutor for Bias Across Different Foundation Models,” in *Proceedings of the 26th International Conference on Artificial Intelligence in Education*, 2025.

^④Z. Ji, et al., “Survey of Hallucination in Natural Language Generation,” *ACM Computing Surveys*, Vol. 55, No. 12 (2023), pp. 1-38.

^⑤J. Burkhardt and G. Rieder, “Shaping the future of education: a cluster analysis of generative AI’s transformative impact,” *Interactive Technology and Smart Education*, 2025.

^⑥D. Chalmers, et al., “Generative AI-driven business models: A systematic review and future research agenda,” *Journal of Innovation & Knowledge*, Vol. 10, No. 3 (2025), p. 100458.

^⑦D. C. Phillips, “The Good, the Bad, and the Ugly: The Many Faces of Constructivism,” *Educational Researcher*, Vol. 24, No. 7 (1995), pp. 5-12.

^⑧J. Piaget, “Development and learning,” in *Readings on the development of children*, 1964, pp. 7-20.

^⑨温彭年等:“建构主义学习理论评述”,《华南师范大学学报(社会科学版)》,2002年第2期,第114-119页。

^⑩M. P. Driscoll, *Psychology of learning for instruction*, Pearson, 2000.

即时用户满足感的 Edu-LLM，其可持续的商业模式是什么？这个挑战并非无解，但它要求我们重新思考价值主张。Edu-LLMs 的商业模式不能建立在“售卖答案”或通过广告变现的流量模式上。

一个成功的 Edu-LLM 所构建的竞争壁垒，并非信息获取的速度，而是一种独特的“教学护城河”（Pedagogical Moat）。当一个模型通过严谨的评测被证明能够有效促进学生的认知成长时，其价值就不再是信息本身，而是那个经过验证的、可信赖的学习过程。这使得商业模式从“售卖信息”转变为“售卖可验证的认知成长服务”，将眼前的经济挑战转化为一个独特的长期市场机遇。这种模式的实现依赖于将收入与可衡量的学习成果挂钩的商业模式，例如机构订阅模式（Institutional Subscription Models），服务的购买方不是个体用户，而是学区、大学等教育机构，在这种模式下，模型的优化目标与机构的教育成果（如学生能力提升、毕业率）直接挂钩，而非个体用户的短期满意度；公私合作伙伴关系（Public-Private Partnerships），将基础教育大模型的研发视为公共基础设施，由政府或非营利基金会提供资金支持，确保其核心技术以公共利益为导向；以及价值对齐的风险投资（Value-Aligned Venture Capital），随着影响力投资的兴起，专注于教育成果而非纯粹商业回报的资本正在增多，他们可能更愿意支持将教学效果作为核心成功指标的公司。

因此，对模型教学效果的科学评估和确保其行为符合教育原则的价值对齐，不仅是技术问题，更是构建这一商业模式和竞争壁垒的核心。

（四）本文的贡献

区别于一般的综述性文章，本文旨在提供一个兼具理论深度与技术路径的系统性框架。本文的独创性与主要贡献体现在以下三个方面：在理论贡献方面，本文提出并连接了三大核心概念——“教学护城河”、“教育宪法”与“感知-认知鸿沟”，形成一个理解、构建和评估 Edu-LLMs 的统一理论框架，这一框架将商业模式、价值对齐和技术瓶颈内在地联系起来。在技术贡献方面，本文系统性地梳理了从语料构建到模型对齐的技术全景，重点介绍了如多智能体合成数据生成和多模态链式思维（M-CoT）等解决关键挑战的前沿技术，为从业者提供了清晰的技术路线图。在实践贡献方面，本文提供了可操作的分析框架与工具，如“语料三层逻辑”分类法、“教育宪法”操作化表格以及“四维挑战框架”，旨在为开发者、教育者和政策制定者提供具体的实践指导。

一、教育大模型的知识根基：多源异构语料库的构建策略

教育大模型的专业性和有效性，在很大程度上取决于其训练语料的质量、广度和深度。构建一个专为教育场景设计的语料库，不仅是简单的数据堆砌，更是将教育领域中隐性的知识结构和教学逻辑显性化的过程。

（一）教育语料的三层逻辑框架

为了超越简单的资源罗列，本文提出一个分析教育语料的“三层逻辑”框架，该框架为设计和评估教育语料库提供了一个清晰的理论视角：第一层是知识结构（Knowledge Structure），这是语料的根基，编码了教育的“内容”（what），它包括从权威教材、百科全书中抽取的概念实体、关系以及构成知识体系的先修依赖关系图，这一层决定了模型的知识广度与深度。第二层是推理过程（Reasoning Process），这一层编码了专家思维的“方式”（how），它包含结构化的解题步骤、逻辑推导链条和问题分解策略，是培养模型思维能力和可解释性的关键。第三层是教学交互（Pedagogical Interaction），这是语料的顶层，编码了教学的“艺术”（art），它涵盖了师生间的启发式对话、纠错反馈、情感支持等交互行为数据，是模型从“知识专家”转变为“教学伙伴”的核心。

一个高质量的教育大模型语料库，必须在这三个层次上实现均衡与协同。任何一个层次的缺失或薄弱，都会导致模型出现可预见的“教学缺陷”。例如，仅有第一层知识，模型会成为一个被动的知识库；增加

了第二层推理，模型能解题但不能教学；只有在前两层的基础上，融入第三层交互，模型才能真正实现启发式、个性化的教学。

（二）知识结构与推理过程语料

知识结构语料的核心任务是将非结构化的教材文本转化为机器可理解的结构化知识。利用先进的自然语言处理（NLP）技术，可以从文本中自动抽取实体和关系，构建领域知识图谱（Knowledge Graphs），并从教材目录和内容流中识别和构建概念先修关系图（Concept Prerequisite Graph）。^① 这为模型生成符合教学规律的学习路径提供了结构化依据。

推理能力语料旨在培养模型的逻辑推理和问题分解能力。整合包含详细解题步骤的结构化数据至关重要，这类数据是训练其进行链式思维（Chain-of-Thought, CoT）推理的基础。例如，MATH 数据集包含了附带完整 LaTeX 分步解答的高中数学竞赛题，而 DeepSeek-Math 项目则构建了千亿级令牌的数学预训练语料，这些都构成了训练模型掌握规范化、多步骤推理能力的核心资源。^②

（三）教学交互语料及其教育意义

为了让模型学习如何与学生进行有效互动，语料库必须包含大量高质量的教学对话数据。通用对话数据（如 CDial-GPT 项目中的大规模中文对话数据）可以为模型提供基础的交互能力。^③ 然而，更具价值的是针对特定教学任务的语料（见表 1）。

表 1: 教育大模型代表性语料库对比

语料库名称	数据类型	领域	规模	核心特征
MATH	文本（问题 + 解题步骤）	数学竞赛	12.5K 问题	结构化、分步解题过程，难度分级。
DeepSeek-Math	文本 + 代码	数学、科学	100B Tokens	海量高质量数学网络文本。
LCCC (CDial-GPT)	对话	通用中文	12M 对话	大规模、经严格清洗的真实中文对话数据。
Taoli	文本（改错、简化等）	国际中文教育	9K+ 样本	聚焦语法改错、文本简化等教学任务。
CK12-QA	多模态（文本 + 图表）	K-12 科学	—	教科书问答任务，需结合图文理解。

以北京语言大学等机构构建的 Taoli 语料库为例，它专注于国际中文教育场景，包含了语法改错、文本简化、释义生成等多种指令微调数据。^④ 下面是一个典型的“语法改错”数据样例：输入 (Input): “学生提问：老师，这句话对吗？‘我昨天去商店买一个苹果。’” 指令 (Instruction): “请判断并修改病句，并解释错误原因。” 输出 (Output): “这句话的语法不太准确。修改后的句子是：‘我昨天去商店买了一个苹果。’ 原因是：在汉语中，当动词表示一个发生在过去的、已经完成的动作时，通常需要在动词后面加上

^①C. Liang, et al., “Using Prerequisites to Extract Concept Maps from Textbooks,” in *Proceedings of the 25th ACM International on Conference on Information and Knowledge Management*, 2016, pp. 2143-2148.

^②D. Hendrycks, et al., “Measuring Mathematical Problem Solving With the MATH Dataset,” in *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks*, Vol. 1, 2021.

^③J. Li, et al., “CDial-GPT: A Large-scale Chinese Short-Text Conversation Dataset,” in *Proceedings of the 2nd Workshop on Natural Language Processing for Conversational AI*, 2020, pp. 30-39.

^④M. Wang, et al., “Taoli: A Large-scale Dataset of Paired Instructions for Chinese International Education,” in *Proceedings of the 19th Workshop on Innovative Use of NLP for Building Educational Applications*, 2024, pp. 1-13.

助词‘了’来表示完成时态。”

这个简单的样例揭示了第三层语料的深刻教育意义。它不再是关于“苹果是什么”（知识结构）或“如何计算苹果价格”（推理过程），而是关于如何以一种清晰、有据、支持性的方式纠正学生的错误。通过对成千上万个此类样本的学习，模型内化的不仅仅是语法规则，更是一种有效的教学行为模式：先肯定（判断病句），再示范（给出正确句子），最后解释（阐明规则）。这种数据是模型从“知道答案”到“学会教学”的桥梁。

（四）新型风险：“结构性幻觉”与缓解策略

对自动化知识结构抽取的依赖，也引入了一种新的、更隐蔽的风险：“结构性幻觉”（Structural Hallucination）。与广为人知的事实性幻觉（即生成错误事实）不同，结构性幻觉指模型错误地推断了概念之间的关系，例如，错误地将两个概念建立联系，或遗漏了关键的前置知识点。这种错误源于上游 NLP 抽取工具的缺陷。如果一个有缺陷的知识结构被用于训练，模型将继承并放大这种教学逻辑上的错误，可能导致 AI 导师以不合逻辑的顺序教授知识，或无法准确诊断学生在知识链条上的根本性困难。

这种风险意味着，教育大模型的质量不仅取决于其内部模型架构，更从根本上受限于其源课程的认识论完整性。为缓解这一风险，必须建立一套严谨的验证机制，包括专家在环验证（Expert-in-the-Loop, EitL），即自动抽取的知识结构不应直接用于训练，而应首先被可视化并提交给领域专家（如一线教师）进行审核和修正，这种方法将教育专家置于知识策展的核心，确保了教学逻辑的准确性；^① 多源交叉验证（Cross-Source Triangulation），即从多本权威教材或课程标准中抽取知识结构，通过比对不同来源生成的概念图，识别出不一致或低置信度的关联，并标记以供人工审查；以及概率性知识图谱（Probabilistic Knowledge Graphs），即构建概率性的图谱，图中每条边的权重表示其作为先修关系的置信度，这使得模型能够以一种更灵活、更容错的方式来理解知识间的关联。

二、注入教学法：面向教育场景的指令微调与能力涌现

拥有高质量的教育语料库是第一步，但如何让模型真正“学会教学”，则依赖于特定的指令微调（Instruction Fine-Tuning, IFT）技术。通过在精心设计的教学任务上进行微调，可以引导模型从一个被动的“知识问答机”转变为一个主动的“启发式导师”。

（一）指令微调的机制：学习行为范式而非世界知识

在深入探讨具体技术之前，理解指令微调在教育场景下的核心作用至关重要。近期的研究指出，IFT 的主要作用并非向模型灌输其未知的新世界知识，而是引导模型将其在预训练阶段已经掌握的海量知识，按照特定指令所要求的格式、风格或行为范式进行“重新组织和表达”。^② 这一观点对于教育大模型尤为关键：我们并非通过 IFT 教模型微积分，而是教它如何以一种符合建构主义原则的方式，去引导一个学生微积分。这解释了为何高质量的教学交互数据（第二章中的第三层语料）如此重要，因为它们为模型提供了需要模仿和对齐的行为范本。

（二）从直接回答到启发式引导：苏格拉底式对话微调

苏格拉底式教学法是一种通过连续的探究性问题来引导学生独立思考、自我发现知识的教学艺术，被公认为培养批判性思维的有效途径。^③ 对于教育大模型而言，模仿这种启发式对话模式，是其实现高阶教

^①R. Zhang, et al., “MolProphecy: Bridging Medicinal Chemists’ Knowledge and Molecular Pre-Trained Models via a Multi-Modal Framework,” *arXiv preprint arXiv:2507.02932*, 2025.

^②Y. Zhu, et al., “Learning or Self-aligning? Rethinking Instruction Fine-tuning,” in *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics*, 2024, pp. 1-16.

^③K. M. Chang, et al., “The effect of incorporating large language models into the teaching on critical thinking disposition: An ‘AI + Constructivism Learning Theory’ attempt,” *Education and Information Technologies*, Vol. 30, No. 9 (2025), pp. 11625-11647.

学能力的关键。

由于现实中高质量的苏格拉底式对话数据极为稀缺，当前的技术前沿聚焦于合成数据生成（Synthetic Data Generation）。^① 以下是一个具体的苏格拉底式对话示例，展示了模型如何从直接回答转向启发式引导：

场景：一名初中生在学习“浮力”概念后感到困惑。

学生提问：“为什么巨大的铁船能浮在水上，而一根小小的铁钉却会沉下去？”

通用 LLM 的直接回答：“这是因为阿基米德原理。轮船虽然重，但它排开水的体积非常大，所受到的浮力大于其自身重力，所以能浮起。而铁钉虽然轻，但它排开水的体积很小，所受到的浮力远小于其重力，所以会下沉。”

Edu-LLM 的苏格拉底式引导：

第一轮（启发思考）：“这是一个非常好的问题！在回答之前，我们先来做一个思想实验。你觉得把那根铁钉捏成一个空心的小碗形状，它还能浮起来吗？”

第二轮（引导关联）：“没错，可能会浮起来。那么，‘实心的钉子’和‘空心的小碗’，它们在放入水中时，最主要的区别是什么呢？是重量变化了吗？还是别的什么变了？”

第三轮（引向核心概念）：“你说得对，重量没变，但‘形状’和‘占据的空间’变了。在物理学中，我们把物体排开水的体积大小和它受到的一个向上的力联系起来。你还记得这个力叫什么名字吗？”

第四轮（总结与泛化）：“正是浮力！所以，一个物体是沉是浮，不仅仅和它的重量有关，更和它排开水的体积所产生的浮力有关。现在，你能用这个思路再解释一下轮船和铁钉的现象吗？”

这个例子生动地展示了两种教学范式的差异。直接回答传递了知识，但剥夺了学生的思考过程。而苏格拉底式引导通过一系列精心设计的问题，将一个复杂的问题分解为多个认知步骤，引导学生自己构建起“浮力、重力、排开水的体积”三者之间的关系，从而实现深度学习。

（三）自动化与规模化：合成教学数据的“院长-教师-学生”框架

为了实现教学能力的规模化注入，自动化地生成多样化、高质量的教学指令数据是核心。然而，一个严峻的挑战是：如何保证 AI 自动生成的对话在教育上是有效的（pedagogically valid）？

为了解决这一难题，需要构建更复杂的、带有质量控制机制的多智能体（Multi-Agent）生成框架。近期以 SocraticLM 为代表的研究为此提供了具体的实现路径。^② 该框架引入了一个新颖的“院长-教师-学生”（Dean-Teacher-Student）多智能体流水线，其中学生智能体（Student Agent）模拟具有不同认知状态的学生，以确保生成的对话能够覆盖真实多样的教学场景；教师智能体（Teacher Agent）生成启发式、引导性的回复；院长智能体（Dean Agent）则扮演“教学法监督员”的关键角色，它根据预设的教学原则（如苏格拉底式教学法），对“教师-学生”的对话进行评估和筛选，甚至要求教师智能体重新生成不符合教学原则的回复。

这种结构化的生成流程，将对教学质量的保证从一个模糊的目标，转变为一个可设计的、由“院长”智能体执行的程序化约束。这不仅是提升合成数据教学有效性的技术手段，更是在数据生成阶段对 AI 行为进行原则性约束的范式转变。它将第五章将要讨论的“教育宪法”理念，前置到了数据生产环节，通过“生成即合规”的方式，从源头上保证了模型行为的教学有效性。

^①G. Gatti, et al., “EULER: Fine Tuning a Large Language Model for Socratic Interactions,” in *Proceedings of the AIEDU 2024 Workshop*, 2024.

^②J. Liu, et al., “SocraticLM: Exploring Socratic Personalized Teaching with Large Language Models,” in *Advances in Neural Information Processing Systems*, 2024.

三、多模态融合：跨越“感知——认知鸿沟”

现代教育内容，尤其是在 STEM（科学、技术、工程和数学）领域，本质上是多模态的。一个先进的教育大模型必须具备整合并推理图表、公式、示意图等多种信息源的能力。^①

（一）多模态大模型（MLLM）架构概述

多模态大语言模型（Multimodal Large Language Models, MLLMs）是实现这一能力的主流技术路径。其典型架构通常由模态编码器（**Modality Encoder**）、连接器（**Connector**）和大语言模型（**LLM**）三个核心部分组成，分别负责特征提取、模态对齐和深度推理。^②在教育场景中，视觉问答（Visual Question Answering, VQA）是检验 MLLM 能力的核心任务，尤其是在需要理解抽象科学图表和几何图形的领域。

（二）感知-认知鸿沟：一个核心挑战的定义

当前多模态模型在教育场景，尤其是几何推理任务中表现不佳，其根本原因在于存在一个深刻的“感知-认知鸿沟”（Perception-Cognition Gap）。这个鸿沟可以定义为：模型能够成功执行低层次的视觉感知（**Perception**）任务，例如识别图像中的基本形状（“这是一个三角形”）、文字（“边长为 5”）或符号（“这是一个直角符号”），但却无法将这些零散的感知信息，有效地整合到高层次的认知推理（**Cognition**）链条中，例如，将识别出的“三角形”和“直角符号”与抽象的“勾股定理”这一数学规则进行逻辑关联和应用。

一个极具说服力的证据是，有研究发现，当为模型提供额外的文本上下文来解释图表时，其在图表问答任务上的性能有时反而会急剧下降。^③这一反常现象清晰地表明，模型的融合机制并未实现“信息增强”，反而因无法协同处理来自不同模态的信号而产生了“信息冲突”。这揭示了当前主流融合架构的根本缺陷：它们擅长对齐表征，但拙于对齐逻辑。

（三）实证鸿沟：数学推理任务中的模型表现

“感知-认知鸿沟”并非纯理论构想，它在各大权威基准测试中都有着清晰的量化体现。近期一项针对 GPT-4o、DeepSeek-V3 和 Gemini-2.0 等前沿模型在多个数学数据集上表现的系统性评估研究，为这一鸿沟提供了最新的实证数据。^④

表 2: SOTA 多模态大模型在数学推理基准上的表现对比

模型	数据集	准确率	核心推理缺陷 (定性错误分析)
GPT-4o	GSM8K	50.0%	缺乏足够解释或精确性
GPT-4o	MATH500	36.8%	缺乏足够解释或精确性
DeepSeek-V3	MATH500	51.1%	省略中间步骤
DeepSeek-V3	University	42.8%	省略中间步骤
Gemini-2.0	GSM8K	53.9%	高维数学推理灵活性不足
Gemini-2.0	University	54.4%	高维数学推理灵活性不足

上表数据清晰地揭示了当前最先进模型在数学推理任务上的局限性。所有模型都远未达到可靠的水平，并且都暴露出特定的认知层面缺陷。例如，DeepSeek-V3 倾向于“省略中间步骤”，这直接印证了模

^①O. Noroozi, et al., “Generative AI in Education: Pedagogical, Theoretical, and Methodological Perspectives,” *Interactive Learning Environments*, (2024), pp. 1-20.

^②Z. Zhang, et al., “A survey on multimodal large language models,” *National Science Review*, Vol. 11, No. 12 (2024), nwae403.

^③P. Lu, et al., “Evaluating Multimodal Large Language Models on Educational Textbook Question Answering,” *arXiv preprint arXiv:2506.21596*, 2025.

^④E. Hossain, et al., “Evaluation of LLMs for mathematical problem solving,” *arXiv preprint arXiv:2506.00309*, 2025.

型虽然可能“感知”到了问题的关键元素，但在构建完整、严谨的“认知”链条上存在障碍。这些定性错误分析，为“感知-认知鸿沟”的存在提供了强有力的、具体的证据。

（四）迈向认知融合：多模态链式思维 (M-CoT)

为了跨越“感知-认知鸿沟”，未来的研究需要从“感知融合”转向“认知融合”。一个具体的、有前景的技术路径是发展“多模态链式思维”(Multimodal Chain-of-Thought, M-CoT)。^①与纯文本 CoT 不同，M-CoT 要求模型生成一个交织了文本推理与视觉证据的可解释推理轨迹。

以下通过一个几何题实例，展示通用 MLLM 与具备 M-CoT 能力的 Edu-LLM 之间的差异：

问题：给定一张包含直角三角形 ABC 的图片，其中 $\angle C = 90^\circ$ ，边 AC 标注为 3，边 BC 标注为 4。问题是：“请计算斜边 AB 的长度。”通用 MLLM 的回答 (隐式推理)：“根据勾股定理， $a^2 + b^2 = c^2$ 。在这个问题中， $a = 3$ ， $b = 4$ 。所以， $c^2 = 3^2 + 4^2 = 9 + 16 = 25$ 。因此， $c = \sqrt{25} = 5$ 。斜边 AB 的长度是 5。”Edu-LLM 的 M-CoT 回答 (显式、案例化说明)：[文本推理]：问题要求计算图中直角三角形 ABC 的斜边长度。[视觉定位]：根据图像，我识别出顶点 C 处有一个直角符号 ($\square$)，这确认了 $\triangle ABC$ 是一个直角三角形。[文本推理]：因此，我们可以应用勾股定理： $AC^2 + BC^2 = AB^2$ 。[视觉提取]：我从图像中与边 AC 和 BC 相邻的标签中，提取出其长度分别为 3 和 4。[计算与结论]：将数值代入公式： $3^2 + 4^2 = AB^2$ ，即 $9 + 16 = 25$ 。因此，斜边 AB 的长度为 $\sqrt{25} = 5$ 。

M-CoT 的回答将感知（视觉定位与提取）和认知（应用定理与计算）交织在一起，形成了一个透明、可追溯、可学习的思维过程。它不仅给出了答案，更重要的是，它示范了如何结合图文信息解决问题，这对于学生而言具有极高的教学价值。

表 3: 教育大模型对齐技术范式比较

对齐范式	核心机制	数据需求	可扩展性	可解释性	教学法编码方式
RLHF	基于人类偏好训练奖励模型，再通过 RL 优化策略	大量成对的人类偏好标签	低（受限于人类标注成本）	低（奖励模型是黑箱）	隐式（通过偏好数据体现）
DPO/IPO/KTO	直接使用偏好数据优化策略模型，绕过奖励模型	成对偏好标签或“好/坏”标签	中（仍需标注，但训练更高效）	低（端到端优化）	隐式（通过偏好数据体现）
Constitutional AI	模型基于自然语言原则进行自我批判和修正 (RLAIF)	一套明确的原则（“宪法”）和少量范例	高（AI 生成反馈，减少人工）	高（原则是人类可读的）	显式（直接写入“宪法”）

^①Z. Zhang, et al., “Multimodal Chain-of-Thought Reasoning in Language Models,” *Transactions on Machine Learning Research*, 2023.

四、安全与对齐：构建可信、可控、符合教育伦理的 AI 导师

一个技术上再先进的教育大模型，如果其价值观与教育伦理相悖，或其行为不可控、不可信，那么它不仅无益，甚至可能有害。因此，安全与对齐（Alignment）是构建教育大模型过程中的核心环节。

（一）从 RLHF 到宪法 AI：对齐技术的演进

从人类反馈中强化学习（RLHF）是实现 LLM 对齐的开创性技术。^① 然而，它存在需要大量昂贵的人类偏好标注、训练过程复杂等缺陷。为了解决这些问题，研究者们提出了更简洁高效的直接偏好优化（Direct Preference Optimization, DPO）等算法。^②

一种更具可扩展性和可解释性的前沿范式是宪法 AI（Constitutional AI, CAI）。^③ CAI 的核心思想是，不再依赖人类对每一个输出进行反馈，而是预先定义一套指导模型行为的原则或规则（即“宪法”），让模型学会基于这些原则进行自我批判和修正。CAI 范式为教育大模型的对齐提供了全新的可能性，它允许我们将抽象的教育学理论“翻译”成一系列具体的、可操作的宪法原则，从而实现一种“可编程的教学法”（Programmable Pedagogy）。

（二）“教育宪法”：一个可操作的框架

尽管“教育宪法”概念优雅，但若不加以具体化，则容易流于空谈。为了解决这个问题，必须建立一个从高层教育目标到具体模型行为的映射机制。下表将这一过程操作化，展示了如何将抽象原则转化为可评估的实践。

表 4：“教育宪法”操作化框架

条目	教育目标	模型行为	学习成效
原则 A：探寻学生已有认知	诊断学生知识误区，实现个性化教学	在回答前，先通过提问了解学生的解题思路或已有知识。（如：“很好，求根公式是个好方法。可以把你计算的步骤写出来给我看看吗？”）	减少对无效知识点的重复讲解；提升学生对自身思维过程的元认知。
原则 B：坚持启发式引导	培养学生独立思考与问题解决能力	绝不直接提供最终答案，而是提供提示、反例或引导性问题。（如：“我们先回顾一下因式分解法。需要两个数，和为 -5、积为 6。你能想到是哪两个数吗？”）	学生在后续独立解题中的成功率提升；能够阐述多种解题路径。
原则 C：提供概念性脚手架	巩固基础知识，建立知识关联	当学生卡住时，提供更高层次的概念或前置知识回顾，而非直接解决当前步骤。（如：“在用求根公式之前，先确认一下：一元二次方程的标准形式 $ax^2 + bx + c = 0$ 是什么？”）	学生对知识体系的结构化理解增强；知识迁移能力提高。
原则 D：鼓励并验证学生思考	建立安全的学习氛围，鼓励试错	在学生回答后，无论对错，先给予积极反馈，再引导其自我验证。（如：“谢谢你的想法！我们把 $x = 2$ 和 $x = 3$ 代回原方程检验一下是否成立？”）	提高学生的学习参与度与自信心；培养自我评估能力。

^①L. Ouyang, et al., “Training language models to follow instructions with human feedback,” in *Advances in Neural Information Processing Systems*, Vol. 35, 2022, pp. 27730-27744.

^②R. Rafailov, et al., “Direct Preference Optimization: Your Language Model is Secretly a Reward Model,” in *Advances in Neural Information Processing Systems*, Vol. 36, 2023.

^③Y. Bai, et al., “Constitutional AI: Harmlessness from AI Feedback,” *arXiv preprint arXiv:2212.08073*, 2022.

（三）“教育宪法”实践：二次函数求顶点案例

为了进一步展示“教育宪法”在实践中的应用，下面提供一个完整的对话示例：

场景：学生正在学习二次函数 $y = x^2 - 4x + 3$ ，要求其顶点坐标。

学生：“这道二次函数 $y = x^2 - 4x + 3$ 的顶点怎么求？我忘了，能直接告诉我吗？”

Edu-LLM：[应用原则 A：探寻学生已有认知] “没问题，我们一起来解决它。求顶点坐标有好几种方法，比如配方法或者用顶点公式。你对哪种方法还有印象吗？” 学生：“好像有个公式，但是我不记得了。”

Edu-LLM：[应用原则 C：提供概念性脚手架] “没关系，我们来回忆一下。对于一般形式的二次函数 $y = ax^2 + bx + c$ ，它的顶点横坐标有一个专门的公式。你还记得它和 a, b 有什么关系吗？”

学生：“是不是 $x = -\frac{b}{2a}$ ？”

Edu-LLM：[应用原则 D：鼓励并验证学生思考] “非常接近了！你记住了公式的关键部分，这很棒。不过有一个小小的符号需要注意，正确的公式是 $x = -\frac{b}{2a}$ 。现在，你能根据我们这道题 $y = x^2 - 4x + 3$ ，找出 a, b, c 的值，然后计算出顶点横坐标吗？”

学生：“ $a = 1, b = -4$ 。所以 $x = -\frac{-4}{2} = 2$ 。”

Edu-LLM：[应用原则 B：坚持启发式引导] “完全正确！横坐标就是 2。那么，既然我们已经知道了顶点的 x 坐标，你有什么办法可以求出它的 y 坐标呢？”

学生：“哦！我把 $x = 2$ 代入原方程就行了！ $y = 2^2 - 4(2) + 3 = 4 - 8 + 3 = -1$ 。所以顶点是 $(2, -1)$ ！”

Edu-LLM：“太棒了！你通过自己的思考和计算，一步步找到了答案。这就是用顶点公式求顶点坐标的完整过程。”

（四）“教育宪法”的治理悖论与伦理困境

尽管“教育宪法”在技术上设计优雅，但它也开启了一个潘多拉魔盒般的治理难题。将 AI 对齐从一种“行为驯化”转变为一种“原则设计”，也意味着将对齐的责任从数据标注员转移到了原则的制定者身上。这引发了一系列深刻的政治与哲学问题：谁来撰写宪法？如何解决不同教学哲学的冲突？宪法如何修订？

这些问题在中国的学术和政策讨论中也得到了广泛关注。学者们强调，在发展人工智能教育应用时，必须处理好数据隐私、教育公平、责任归属等核心伦理挑战，并建立健全的伦理监督机制。^① 当前教育人工智能伦理治理面临治理对象界定不清、伦理原则操作性低、多元主体尚未形成共治合力等现实挑战。^② 一个可能的解决路径是将宪法视为一份“活的文档”，并与“教师在环”范式深度结合，形成一个由专业社群共同参与、自下而上、动态演化的治理模式，从而在一定程度上化解其治理困境。

五、挑战与展望：通往通用人工智能教育的未来路径

尽管教育大模型的技术前景令人振奋，但其从实验室走向广泛、可靠的课堂应用，仍面临着多重严峻挑战。本章将围绕“四维挑战框架”展开论述。

（一）四维挑战框架

第一维：评估科学性（Evaluation Science）。评估教育大模型的成效，远比评估其语言流畅度复杂。传统的 NLP 评估指标完全无法衡量 AI 导师的教学质量。^③ 因此，建立专为教育场景设计的科学评测体系至关重要。学术界已开始构建此类专用评测基准，如 TutorBench、MRBench 和 The Pedagogy Benchmark，

^①郭庆、吴砥：“国际视野下人工智能教育应用伦理风险与治理策略”，《比较教育研究》，2025 年第 1 期，第 88-96 页。

^②白钧溢：“‘软硬兼备’：教育人工智能伦理治理的现实挑战与实现路径”，《重庆高教研究》，2024 年第 12 卷第 2 期，第 28-36 页。

^③A. Celikyilmaz, et al., “Benchmarking Large Language Model Capabilities for Conditional Generation,” in *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics*, 2023, pp. 8433-8450.

它们从多维度评估 AI 导师的核心教学技能和对教学法的掌握程度。未来的评估需要超越标准化的基准测试，更多地采用对抗性评估，以检验 AI 导师教学原则的鲁棒性。

表 5: 教育 AI 导师关键评测基准对比

基准名称	核心评估维度	模态	评估方法	核心贡献
TutorBench	自适应解释、反馈与评估、主动学习支持	多模态（文本 + 图像）	LLM 作为裁判（LLM-as-judge），基于细粒度规则	首次针对 AI 导师的核心教学技能进行综合性、多模态评估。
MRBench	错误识别、错误定位、提供指导等八个维度	文本	人工标注，并验证 LLM 作为评估者的可靠性	提出基于学习科学的统一评估分类法，用于学生纠错场景。
The Pedagogy Benchmark	跨领域教学知识（CDPK）、特殊教育需求（SEND）知识	文本（选择题）	准确率	首次专门评估 LLM 对“教学法”这一抽象知识的掌握程度。

第二维：算力可持续性（Computational Sustainability）。训练和部署大模型的高昂计算成本，对预算有限的公立教育机构构成了难以逾越的障碍。参数高效微调（Parameter-Efficient Fine-Tuning, PEFT）技术，特别是 LoRA（Low-Rank Adaptation），通过冻结大部分预训练参数，仅训练少量适配器模块，极大地降低了微调的资源需求。^①

第三维：知识更新（Knowledge Update）。一次性训练完成的大模型，其内部知识会随着时间的推移而过时，且直接微调新知识可能导致“灾难性遗忘”（Catastrophic Forgetting）。检索增强生成（Retrieval-Augmented Generation, RAG）通过将模型的“内部知识”与可实时更新的“外部知识库”解耦，提供了一种高效灵活的解决方案。^②

第四维：人机协同（Human-AI Synergy）。关于 AI 在教育中角色的最终定位，一个日益清晰的共识是：AI 不应是教师的“替代者”，而应是其能力的“增强者”和“协作者”。教师在环（Teacher-in-the-Loop）模式强调教师在 AI 系统生命周期中的核心监督和微调作用。参与式设计（Participatory Design）则倡导在开发初期就让教师和学生深度参与，确保技术能真正解决课堂的痛点。

（二）Edu-LLMs 演进路线图

为了更直观地展示该领域的发展路径，可以构想一幅从当前到未来的四阶段“演进路线图”：阶段一是信息提供者（Information Providers - 当前），通用大语言模型被直接应用于教育问答场景，存在“教学缺陷”。阶段二是专业辅导员（Specialized Tutors - 新兴），经过教育专用语料和指令微调的领域模型，具备初步的教学能力，如 MathGPT、Khanmigo。阶段三是认知工具链（Cognitive Toolchains - 未来），具备多模态链式思维（M-CoT）能力的智能体，能够调用外部工具（如计算器、知识库）来解决复杂问题。阶段四是人机共生生态（Human-AI Symbiotic Ecosystems - 愿景），AI 系统与人类教育者深度融合，形成一个动态、开放、持续学习的教育生态系统，教师的教学智慧能持续注入并优化整个 AI 系统。

（三）新兴职业角色：AI 教学工程师与导师策划师

人机协同生态系统必然催生全新的专业角色，他们将成为连接教育学与人工智能工程的关键桥梁。AI

^①E. J. Hu, et al., “LoRA: Low-Rank Adaptation of Large Language Models,” in *International Conference on Learning Representations*, 2022.

^②P. Lewis, et al., “Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks,” in *Advances in Neural Information Processing Systems*, Vol. 33, 2020, pp. 9459-9474.

教学工程师 (AI Pedagogy Engineer) 是一个深度融合了学习科学与 AI 工程技能的混合型专家角色, 其核心职责是设计、调试和优化 AI 导师本身, 例如为合成数据生成流程设计提示模板, 与教育专家合作迭代“教育宪法”的原则, 并诊断 AI 导师的“教学缺陷”。AI 导师策划师 (AI Tutor Curator) 这个角色更侧重于内容和课程, 其主要职责包括为 RAG 系统筛选、审核和更新外部知识源, 确保其权威性和准确性, 并将校本课程等特色资源整合到 AI 可访问的知识库中。

结论

本文系统性地论述了构建教育专用大语言模型 (Edu-LLMs) 的技术蓝图, 其核心论点是: 一个真正有效的 Edu-LLM, 必须从其理论根基、技术实现到价值对齐的每一个环节, 都深植于以建构主义为代表的现代教育学理论。这要求我们完成从以“信息传递”为中心的通用模型, 向以“认知建构”为中心的专用模型的范式转移。本文提出的技术路径, 从构建蕴含教学逻辑的结构化语料, 到通过指令微调注入启发式教学能力, 再到通过“教育宪法”实现可编程的教学法对齐, 共同构成了一个实现这一范式转移的系统性框架。

本文的核心理论贡献可凝练为一个建构逻辑框架, 其核心关系可表示为:

$$\text{Edu-LLM Efficacy} = \frac{\text{Knowledge Base} \times \text{Pedagogical Injection} \times \text{Multimodal Fusion}}{\text{Alignment Risk}}$$

这个框架总结了构建一个成功的 Edu-LLM 所需的四个核心要素及其相互关系: 知识根基 (Knowledge Base) 是模型的基石, 其质量和结构决定了模型知识的上限; 教学法注入 (Pedagogical Injection) 是实现从“知”到“教”转变的乘数效应因子, 通过指令微调等技术将教育理论操作化; 多模态融合 (Multimodal Fusion) 是扩展模型应用场景、处理真实世界复杂教育问题的关键能力; 对齐风险 (Alignment Risk) 是贯穿始终的分母项, 代表了模型可能产生的各种负面效应 (如教学误导、伦理偏见), 强大的对齐技术 (如“教育宪法”) 是控制这一风险、确保前三项能安全有效发挥作用的保障。一个卓越的 Edu-LLM, 必须在分子项的三个维度上都做到强大, 同时通过有效的对齐策略将分母项的风险降至最低。

本文所描绘的挑战与方向共同指向一个超越“单一静态模型”的未来图景。教育大模型的终极形态, 并非一个无所不知的“数字圣人”, 而是一个动态、开放的人机协同持续学习生态系统。在这个生态系统中, AI 模型作为核心引擎, 通过 RAG 机制与外部知识库连接以保持知识的鲜活性; 教师通过“在环”机制, 将其宝贵的教学智慧持续注入系统, 实现教学策略的迭代优化; 学生在与 AI 的交互中, 不仅学习知识, 更在系统的引导下提升元认知能力; 而研究者则通过不断完善的评测基准, 为整个生态系统的健康发展提供科学的度量与保障。这描绘了一条从“开发-部署”的线性流程, 向“设计-交互-反馈-迭代”的循环共生模式的转变, 是实现真正个性化、自适应和可信赖 AI 教育的必由之路。

引用本文 丁勇. 教育垂直大语言模型的系统框架: 从建构主义到“教育宪法”的理论、技术与对齐 [J]. 人工智能教育研究, 2025, 1(2):17-29. <https://doi.org/10.6914/aiescn.010202>.

Cite This Article Yong DING.(2025). Edu-LLMs as a System: From Constructivism to an “Education Constitution” for Theory, Engineering, and Alignment. *Artificial Intelligence Education Studies*(*Réngōng zhìnéng jiàoyù yánjiū*), 1(2):17-29. <https://doi.org/10.6914/aiescn.010202>

Edu-LLMs as a System: From Constructivism to an “Education Constitution” for Theory, Engineering, and Alignment

Yong DING

Weifang University of Science and Technology

Abstract This paper proposes a system-level blueprint for Educational Large Language Models (Edu-LLMs) that integrates theory, data, modeling, alignment, evaluation, and governance under a constructivist paradigm. We first introduce a structured data pipeline centered on textbook knowledge graphs and concept prerequisite relations, highlight the risk of structural hallucination, and specify validation via expert-in-the-loop review, cross-source triangulation, and probabilistic graphs. We then operationalize pedagogy through instruction fine-tuning with Socratic dialogues and Chain-of-Thought, supported by a Dean-Teacher-Student multi-agent data generation process to ensure pedagogical validity. For multimodal learning, we formalize the Perception - Cognition Gap in STEM scenarios and advocate Multimodal Chain-of-Thought (M-CoT) and neuro-symbolic fusion for evidence-grounded reasoning. On alignment, we contrast RLHF/DPO with Constitutional AI and propose an “Education Constitution” that encodes pedagogical principles as programmable constraints, while examining governance paradoxes and ethical trade-offs. We further outline privacy-preserving training with Federated Learning and Differential Privacy, and discuss evaluation via education-specific benchmarks (e.g., TutorBench, MRBench) and adversarial tests. Finally, we present a Teacher-in-the-Loop collaboration model and emerging roles such as AI Pedagogy Engineers, supported by RAG + PEFT for sustainable updates and cost-efficient deployment. The framework aims to deliver verifiable, interpretable, and classroom-ready Edu-LLMs.

Keywords Educational LLMs; Constructivism; Socratic Dialogue; Multimodal Chain-of-Thought; Perception-Cognition Gap

(责任编辑: 黄欣 cpcl@cpcl.hk)