可定制机器学习系统

关键词：可定制机器学习　可微连续主动学习　多尺度时空超敏具身机理认知

林宙辰　方　聪　王奕森
北京大学智能学院

背景

机器学习作为人工智能（AI）的核心领域之一，在许多实际任务中取得了巨大的成功，由机器学习模型衍生的诸多应用已经融入现代生活的方方面面[1~3]。然而，在经典的机器学习研究范式下，解决一个全新的任务往往需要重新训练一个高质量的模型，这不仅依赖深度的专业领域知识，还依赖大规模高质量的数据和计算资源，较高的门槛导致大多数用户难以快速获得高性能的机器学习模型。与此同时，用户在重新利用现有模型时也存在很多问题，比如在特定任务上训练好的模型不能适用于其他任务，在特定环境中训练好的模型难以适配到不同环境，以及在逐步改进训练好的模型时可能出现灾难性遗忘等问题。基于预训练－微调范式的大语言模型的出现，在一定程度上纾解了为特定任务训练专用机器学习模型带来的高成本和高专业性的困难[4, 5]，但通过预训练模型适配领域特定任务同样具有局限性，例如在自然语言处理[6]和计算机视觉[7]的应用中难以同时处理跨模态问题。

对宇观、宏观、微观不同尺度下的具身影像进行学习和分析，被称作多尺度具身机理认知问题。在这类问题中，常常遇到“读不懂”的难题，即难以便捷地构建机器学习模型以对不同尺度下通过捕捉具身实例（如天体、生物、细胞）获得的一系列影像所蕴含的复杂机理规律进行准确、高效地解读与分析。从微观细胞到宏观宇宙，不同尺度现象的科学机理复杂多样；即使面对某一时空尺度下的动态对象，其展现的科学现象也可能包含多种机理且互相关联，其间的因果关系复杂，其动态过程是内部多种机理共同作用产生的复杂结果。现有机器学习方法面对复杂多样的时空超敏现象（时间和空间上都需要超高灵敏度测量的现象）时难以自动适配。同时，动态现象需要实时观测与解译，系统难以自动动态调整，因此当外部环境变化时，需要重新设计和训练这些方法，以满足时空超敏现象机理认知的实际需求。

总体来说，现有机器学习方法在时空超敏现象机理认知任务中面临的主要挑战有：

通用性差：在实际应用中，机器学习模型的通用性不高，模型通常是针对特定数据分布和任务设计的，导致其在面对新的、未曾见过的数据分布和任务时泛化能力较差。尽管预训练大模型具有一定的通用性能，但其仍不能很好地处理不同模态、不同领域、不同粒度的任务，如表1所示。

表1　常见大模型在不同领域和数据集上的准确率

数据集	MMLU	MATH	Floores-101	MedQA-MCMLE
领域 / 大模型	通用	数学	翻译	医学
GPT-4	83.93%	40.20%	20.83%	74.58%
GPT-3.5	68.54%	13.96%	17.59%	52.92%
LLaMA-7B	35.10%	3.02%	7.63%	21.72%
LLaMA2-7B	45.73%	3.24%	10.14%	24.78%

适配性弱：在设计过程中，机器学习模型的结构与任务需求之间存在较强的相关性，针对特定领域特定任务的模型难以直接适配到不同任务上，尤

其在训练样本较少时，不同模型在不同任务上的性能表现差异较大。比如随机森林模型可以处理一些分类问题，但难以直接用于目标检测。

动态调整慢：在现有的机器学习范式中，对模型进行大规模预训练，并对完成预训练的模型进行微调改进以适配特定的下游任务是一种常见的微调范式。然而，这种微调范式不仅依赖下游任务领域提供的相关优质数据，而且在逐步改进已训练好的模型的过程中也可能会出现灾难性遗忘等问题（如图 1 所示）。模型在应对动态数据和复杂环境时难以满足实时性和灵活性的需求。

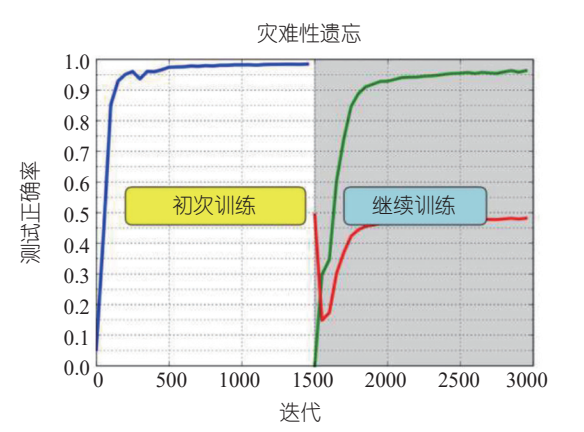


图 1　机器学习模型往往需要重新训练[8]，左图蓝色线表示初次训练的正确率。右图展示继续训练的正确率，分别训练新老两个任务，新任务在不同迭代次数时的测试正确率是绿线，老任务的是红线，可以看出训练出现了灾难性遗忘，即在新任务上训练后，老任务的正确率明显降低了

为应对这些挑战，一种可能的途径是开发满足用户需求的可定制机器学习系统。相比于现有大多数机器学习针对不同任务设计不同的模型结构这一范式，可定制机器学习系统强调根据用户需求自主配置机器学习组件，进而实现更加通用的问题求解模式。

相关研究

对于可定制机器学习系统，国内外已有初步研究，其中最具有代表性的是周志华团队开发的基于学件系统 [9, 10] 的北冥坞平台 [11]。北冥坞平台旨在使用户能够重复使用大量现有的训练好的模型，而无须从头开始构建机器学习模型。在这个范式中，开发者可以自发地将其训练好的模型提交到学件对接系统中，而不必透露其训练数据。对接系统一旦接受了模型，就会为模型分配一个规约（specification），这个规约允许系统根据未来用户的需求充分识别和组装模型以进行重复使用。学件系统与当前的大模型有很大不同，一个容纳数百万甚至更多模型的学件对接系统可以为大模型不适用的、不可预见的、专业化的情景和任务提供良好的解决方案。北冥坞平台在此基础上实现了学件对接系统针对新任务简单开发与之适配的模型的流程，该流程可以高效利用数据，无须专家参与。如果北冥坞中存在一些对任务有帮助的学件，那么仅通过几行代码即可获取和部署一个高性能模型，而无需大量数据和专业知识。北冥坞平台实现了集成和可扩展的系统引擎架构设计，包含了统一用户界面的开源学习软件对接系统，以及各种场景的全流程基准算法的实施和评估。

微软团队研究开发了一种新的人工智能系统 TaskMatrix.AI[12]，将基础模型与数百万个任务的 API 联系起来。与大多数旨在改进单个人工智能模型的工作不同，TaskMatrix.AI 更注重使用现有的基础模型（作为类似大脑的中央系统）与其他人工智能模型和系统的 API（作为子任务求解器）来完成多领域多样化任务。通过以基础大模型为核心，从 API 平台调用 API 完成指定任务，TaskMatrix.AI 在一定程度上实现了可定制化的学习流程。此外，微软还开发了与之类似的 Gorilla 系统 [13]，不在此赘述。

然而，现有的可定制化机器学习平台也存在一定局限性，主要在于平台依赖于已有的学件或 API，如果已有学件或 API 不能解决给定任务，也就无法产生改进的方案。另外，如何组装多个学件或 API 仍存在困难，而且现有平台基本没有考虑连续学习。由于平台开发者难以设计包含全部用户需求的学件或 API，因此如何进一步优化设计平台，使平台可以更自主地捕获任务求解的核心需求，进而自主构建有效的学习模型以完成任务，成为可定制机器学

习研究的核心问题。

可定制机器学习系统框架

针对上述问题，本文提出可定制机器学习系统的初步构想（如图2所示）。可定制机器学习系统实现集成与可扩展式的机器学习框架设计，通过主动学习范式自主选择与调整求解任务所需的组件，完成相应的模型搭建，甚至生成少量问题求解小组件，通过利用过往求解经验和将当前找到的求解方案应用于新的任务实现连续学习，从而不断提升系统的能力。

具体流程如下：当目标任务提交给可定制机器学习系统时，系统借助当前任务－模型库中的先验知识构建求解当前任务的初始模型，之后系统将初始模型可微分化，根据目标任务的具体需求改进学习模型，直至完成学习任务。任务－模型库会存储过往的求解经验，用于构建与改进求解之后新目标任务的模型。为支持高效的可定制机器学习系统，需要发展可微连续主动学习理论，以推动上述流程的高效运转。

在实际应用中，可定制机器学习系统根据任务的具体需求，自主组合现有组件并生成少量缺失的组件（如图3所示）。给定目标任务后，系统参考现有的任务－模型库，利用搜索算法检索出可能满足用户需求的组件组合，作为初始学习模型，之后通过微调改进模型，最后根据执行任务产生的反馈调整模型的组件和改善微调结果。在任务完成后，系统把能解决给定任务的模型存入任务－模型库，作为将来解决其他任务时可能用到的参考。下面简要介绍可定制机器学习系统的各个模块。

任务–模型库

任务－模型库的构建使可定制机器学习系统能够存储过往经验，包括求解的任务和对应的模型与功能组件，从而满足系统自主生成适配任务模型与组件的需求。任务－模型库的最原始状态包含各个能完成小功能的独立组件，这些组件由用户或开发者上传。在随后的使用过程中，任务－模型库通过存储已完成不同任务的不同模型，不断进行自主更新和增强。

任务－模型库相当于可定制机器学习系统中的模型缓存，对于高效求解结构化的任务具有事半功倍的效果，避免了对相同或类似任务的反复搜索优化。

当可定制机器学习系统完成待求解任务后，系

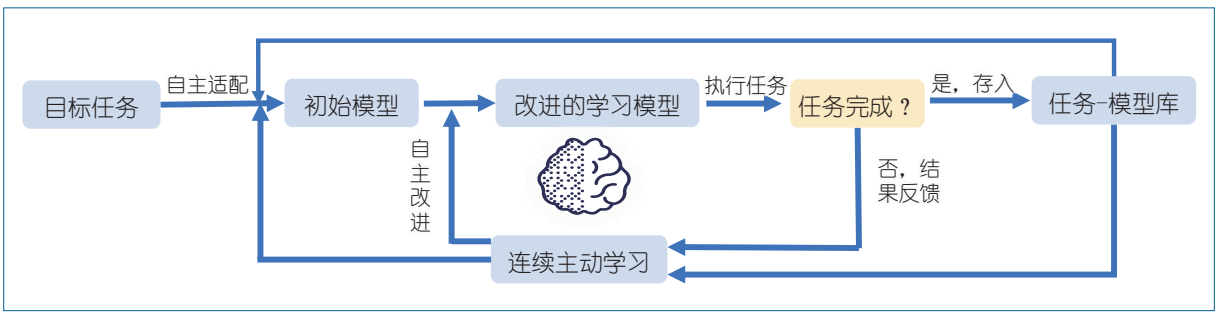


图2 可定制学习系统框架

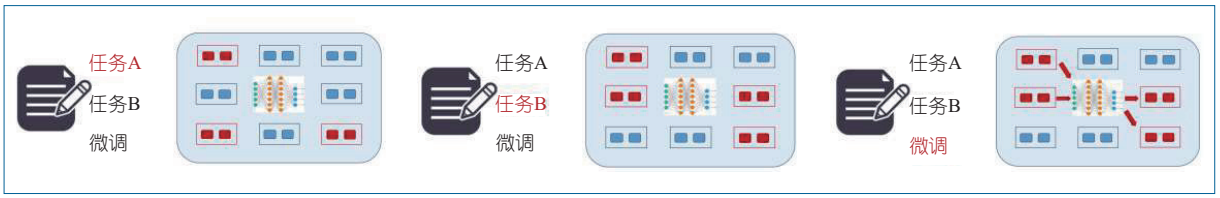


图3 可定制机器学习系统根据任务需求组合组件，不同任务系统组合不同的组件，然后通过微调增强性能。系统会在使用过程中不断提升组合组件的能力

统会将任务描述与完成该任务对应的模型存入任务－模型库中。将来需要求解类似任务时，系统会以该任务为索引，从任务－模型库中调出对应的模型，作为求解新任务的初始模型。任务－模型库还可作为系统学习组件的组合模式的数据来源，使系统在已有模型都不能很好地解决新任务时，能够自主产生新的组件组合，或对初始模型里的组件进行调整。

由此，当系统不断运行时，任务－模型库里能完成特定任务的模型会越来越多，系统的性能也会越来越强。

初始模型

可定制机器学习系统在获取目标任务之后，首先从任务－模型库中搜索相似的任务，若存在相似的任务及对应的可解决类似任务的模型与组件，系统则选取该模型作为初始模型；若不存在，系统将进一步根据任务需求或上一轮迭代构建的模型执行任务时产生的反馈，采用多种方法，如结合大语言模型建议的可能组合、参考已有的任务－模型库中的组合模式、借鉴神经网络架构搜索（Neural Architecture Search，NAS）技术搜索学习组件的可能组合（如图 4 所示）等，得到适用于目标任务求解的组件组合方式，初步完成初始模型的构建。

在初始模型的构建过程中，不同组件之间的不同组合可能需要不同的小组件完成数据类型对齐、维度对齐等基本功能，系统并不直接在任务－模型库中存储这些少量缺失的小型组件，而是可根据任务导向通过代码大模型生成，最终构建出整体初始模型。

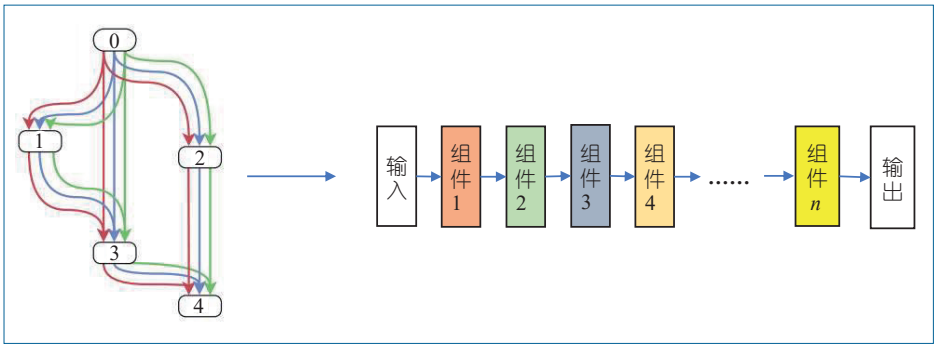


图4　借鉴神经网络架构搜索技术搜索学习组件的可能组合

学习模型的改进

在生成初始模型之后，可定制机器学习系统需要对模型进行改进与提升。首先把模型可微分化，之后让模型执行任务，根据执行获得的反馈对模型进行调整。如果模型始终都不能较为准确地完成任务，则可考虑调整模型采用的组件，如根据组件对应的梯度大小提示该组件被调换的概率，结合初始模型构建中采用的搜索方式产生新的初始模型。

本文所设想的可定制机器学习系统并不是要一步到位地生成完全可用的机器学习模型，而是让模型在应用中自我完善。如果实际情况不允许直接应用尚不成熟的模型，用户可在本地为模型提供训练数据，从而避免数据共享过程中可能产生的隐私泄露问题。

可微连续主动学习理论

可定制机器学习系统的正常运转需要多个底层机器学习技术支持，这些底层技术构成了可微连续主动学习理论的主要部分，即如何通过把系统可微化和引入连续学习机制，主动实现系统能力的提升。该理论主要包括给定任务下对任务－模型库中已有模型的快速评估与搜索、组件组合模式的高效学习、大模型加持的组件组合高效搜索与调整方法、系统性的模型可微分化方法、模型的快速优化算法、模型的高效安全改进方法等。

总而言之，可定制机器学习系统适用于绝大多数依赖机器学习进行开发的任务。以多尺度时空超敏现象具身机理认知为例，对于某个特定任务，首先设计针对该任务的主要组件，用于提高分析和处理数据的效率和精确度，包括误差反馈观测调整、时空超敏现象检测以及动态规则发现与表达等组件。在此基础上，可定制机器学习

系统进行整合与优化，对时空超敏现象进行机理认知，并提供一套精确、可持续和自适应的解决方案。这个系统不仅可用于科学研究，如多光子显微镜成像、生物力学分析和天文现象识别；还能用于实现动态规则的自动发现，如细胞生物力学规律提取和恒星光变曲线的建模与分类。

在多尺度具身机理认知中的应用

图5展示了可定制机器学习系统在多尺度时空超敏现象具身机理认知任务中的应用。搭建一个针对多尺度时空超敏现象机理认知的可定制机器学习系统主要分为两个步骤：组件设计和系统整合与优化。

组件设计：基本组件包括以下三类。（1）误差反馈观测调整组件用于系统对接收的信号进行分析，从而利用反馈机制实现自动观测调整，提升影像重建的精度和效率。该组件模块包括现象机理已知时基于现象机理的物理和数学模型设计的调整策略，以及现象机理未知时的调整策略，如利用神经网络实现的黑盒模型。（2）时空超敏现象检测组件用于系统对观测现象的实时检测与发现，该组件可分为基于物理机理的组件、低秩方法构成的组件和神经网络组件三类。基于物理机理的组件依据物理规律对已知机理事件进行高效检测，如使用匹配滤波器等；低秩方法构成的组件能更好地利用数据的低秩结构，通过低秩建模和张量分解技术提取关键成分以探索未知事件；神经网络组件利用数据优势实现对困难任务的自动检测。（3）动态规则发现与表达组件用于系统发现规律，通过数据对称性和守恒律转换，利用符号计算和深度学习方法自动发现自然现象的物理规则并进行数学化表达。三类基本组件构成初步的可定制机器学习系统的主要部分。

系统整合与优化：进一步对系统自身进行整合与优化，以实现对各领域时空超敏现象的机理认知。其中，须实现具身影像计算的整体可微分化，以使整个系统能以可微的方式进行连续学习。这将保证系统性能持续优化，为复杂科学现象的机理认知提供一套精确、可持续、自适应的解决方案。

搭建好可定制机器学习系统后，就可以利用其进行机理认知。例如，基于误差反馈组件，在微观方面，黑盒策略优化可用于多光子显微镜大视场成像，通过预测图像不确定性，指导扫描重点，提高成像效率；在宏观方面，通过生物力学分析和运动监测的黑盒反馈与调整，实现动态人物状态的高精度重建；在宇观方面，通过光变曲线不确定度和黑盒反馈与调整，实现瞬变源高精度成像。基于时空超敏现象检测组件，可实现生物样本分析、人物瞬间状态重建和罕见天文现象识别等。基于动态规则发现与表达组件，可实现细胞生物力学规律提取和恒星光变曲线的建模与分类等。

未来挑战和值得研究的课题

可定制机器学习系统的研究存在众多挑战。首先，初始时，学习组件和任务－模型库有限，可定制机器学习系统需要在复杂的实际环境中持续学习，逐渐完成很多特定的、不可预测的任务。目前可以通过用户持续提交学习组件，基于可微连续主动学习持续扩展学习组件和

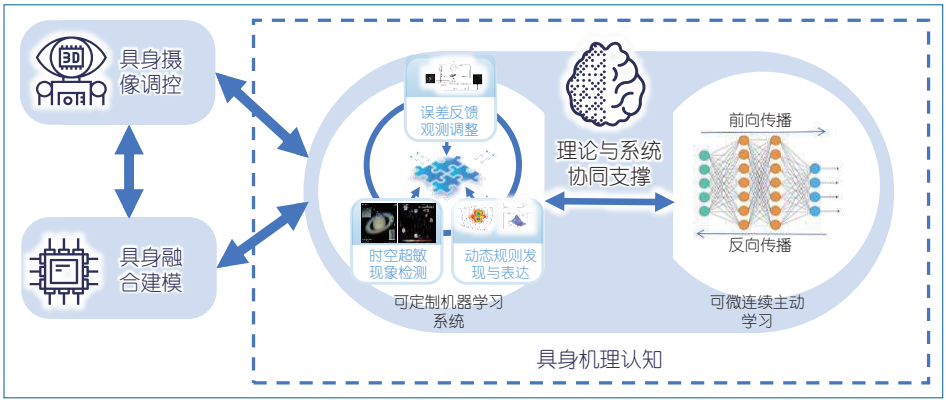


图5　可定制机器学习系统应用于多尺度时空超敏现象具身机理认知

任务 – 模型库，使系统具备终身学习的能力。其次，目前的学习组件通常假设是基于高性能的可以表示对应数据分布的模型，而实际上开发者提交的模型一般无法达到最优。对这些次优模型的使用以及它们对可定制机器学习的影响值得进一步研究。最后，由于开发者提交的模型常常从不同实际问题的特征空间训练得到，可定制机器学习系统需要在异质的环境中使用学习组件 [14, 15]，如何使用学习组件处理异质的特征空间问题也需要继续研究。

小结

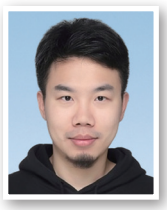
可定制机器学习是一种新的机器学习范式，能有效缓解现有机器学习方法通用性差、适配性弱和动态调整慢的问题。可以预见，随着用户数量的增加，学习组件和任务 – 模型库将不断丰富，可定制机器学习系统求解任务的能力将不断增强，为各类机器学习任务，特别是多尺度时空超敏现象具身机理认知任务，提供高效便捷的学习服务。本文在原理与方法层面简要描绘了设计可定制机器学习系统的蓝图，细节方面难免考虑不周，笔者将努力在具体实践中逐渐完善。 ■

林宙辰

CCF 杰出会员，CCF 计算机视觉专委会常务委员。北京大学智能学院副院长、博雅特聘教授，IEEE/IAPR/AAIA/CSIG 会士。主要研究方向为机器学习与计算机视觉。
zlin@pku.edu.cn

方　聪

北京大学智能学院助理教授。主要研究方向为机器学习。fangcong@pku.edu.cn



王奕森

CCF 专业会员。北京大学智能学院研究员。主要研究方向为机器学习。
yisen.wang@pku.edu.cn

参考文献

[1] Butler K T, Davies D W, Cartwright H, et al. Machine learning for molecular and materials science[J]. *Nature*, 2018, 559(7715): 547-555.

[2] Jumper J, Evans R, Pritzel A, et al. Highly accurate protein structure prediction with AlphaFold[J]. *Nature*, 2017, 596(7873): 583-589.

[3] LeCun Y, Bengio Y, Hinton G. Deep Learning[J]. *Nature*, 2015, 521(7553): 436-444.

[4] Devli J, Chang M W, Lee K, et al. BERT: Pre-training of deep bidirectional transformers for language understanding[C]// *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. 2019, 1 (Long and Short Papers): 4171-4186.

[5] Zhao W X, Zhou Kun, Li J Y, et al. A survey of large language models[OL]. arXiv preprint. arXiv:2303.18223, 2023.

[6] Brown T, Mann B, Ryder N, et al. Language models are few-shot learners[C]// *Proceedings of Advances in Neural Information Processing Systems*. 2020: 1877-1901.

[7] Radford A, Kim J W, Hallacy C, et al. Learning transferable visual models from natural language supervision[C]// *Proceedings of the 38th International Conference on Machine Learning*. 2021: 8748-8763.

[8] Gepperth A, Gondal S A. Incremental learning with deep neural networks using a test-time oracle[C]// *Proceedings of European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*. 2018: 37-42.

[9] Zhou Z H. Learnware: on the future of machine learning[J]. *Frontiers of Computer Science*, 2016, 10(4): 589-590.

[10]Zhou Z H, Tan Z H. Learnware: Small models do big[J]. *Science China Information Sciences*, 2021, 67(1): 112102.

[11]Tan Z H, Liu J D, Bi X D, et al. Beimingwu: A learnware dock system[OL]. arXiv preprint, arXiv:2401.14427, 2024.

[12]Liang Y, Wu C, Song T, Wu et al. TaskMatrix.ai: Completing tasks by connecting foundation models with millions of APIs[J]. *Intelligent Computing*, 2024, 3(2): 0063.

更多参考文献：http://dl.ccf.org.cn/cccf/list