

清华大学 交叉信息研究院

Institute for Interdisciplinary Information Sciences, Tsinghua University

学术科研简报

2022.07-12

人工智能

机器学习

自动驾驶

计算机系统结构

自然语言处理

区块链

计算生物学

计算机视觉

机器人学

AI基础理论

量子信息

量子信息基础理论

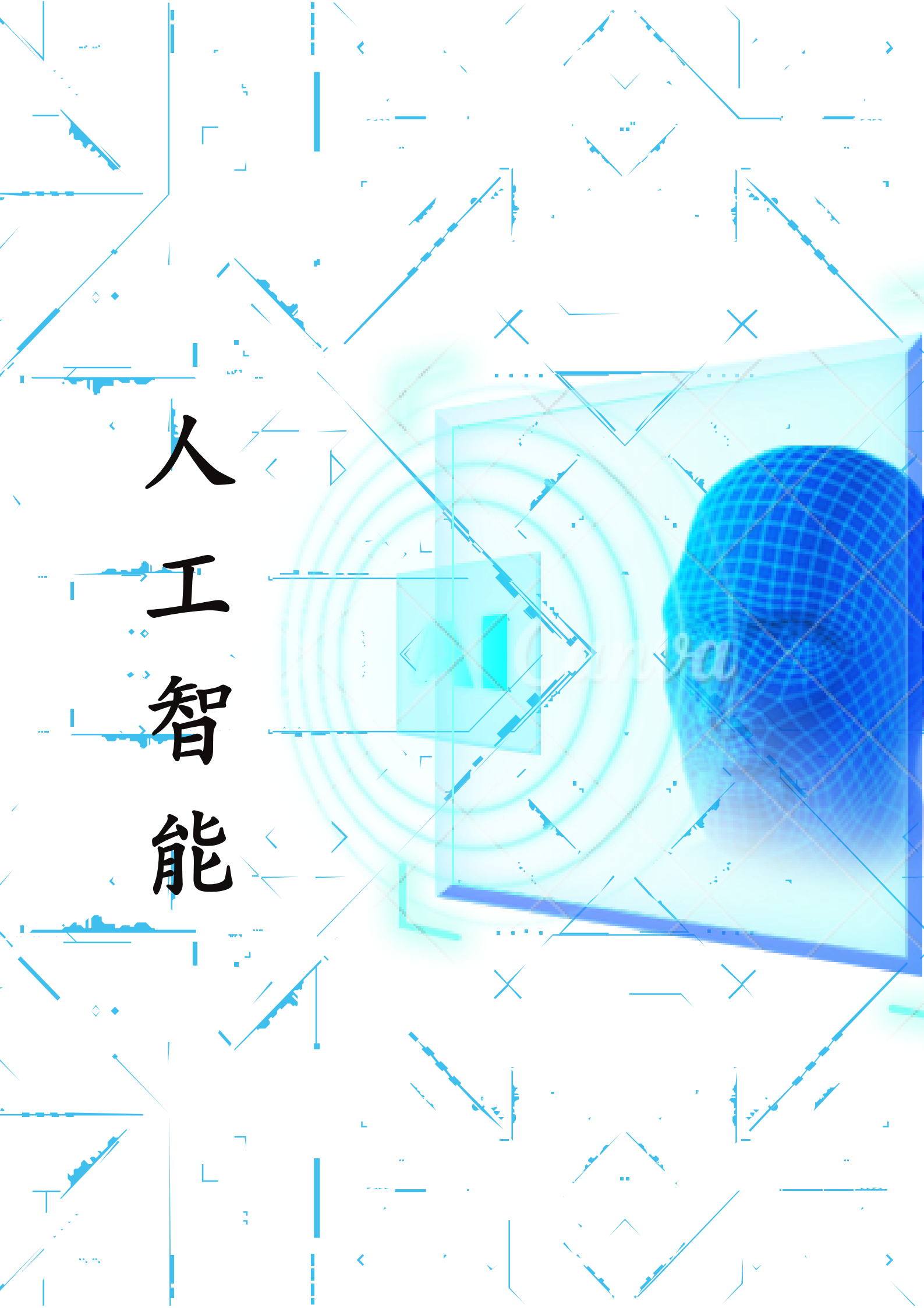
量子通信与密码

量子信息处理

量子人工智能

拓扑凝聚态物理

人工智能



一、机器学习

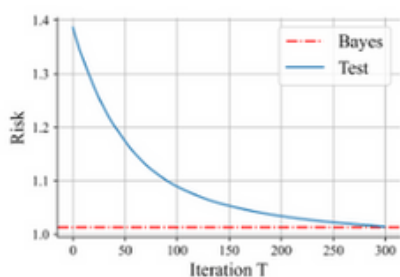
主要完成人：黄隆波研究组、李建研究组、陈建宇研究组、高阳研究组、赵行研究组、吴翼研究组、房智轩研究组、许华哲研究组

使用随机梯度下降训练的过参数化元学习的可证明泛化

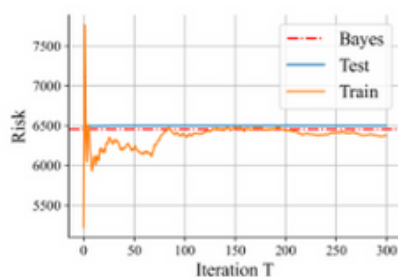
尽管度元学习在实践中取得了显著成功，但对过参数化元学习的理论理解仍然有限。该研究组考虑了一种广泛使用的元学习方法的泛化性能，即模型不可知元学习 (MAML)，旨在找到一个良好的初始化以快速适应新任务。在混合线性回归模型下，该研究组分析了在过参数化状态下使用随机梯度下降 (SGD) 训练的 MAML 的泛化特性。

此项工作主要包含三方面理论结果：1. 在一般的数据和任务设定下，给出过参数 MAML 的泛化超额损失函数的上下界。通过对泛化误差的刻画，可以导出在过参数化下，若要在 $T \rightarrow \infty$ 的情况下实现逐渐消失的元超额损失，需要满足的条件。2. 基于泛化超额损失函数的上下界，探究了任务多样性对过参数化下泛化误差的影响，对于多任务的 MAML，建立了 phase transition，对于任务多样性 r 较大的情形，元超额损失无法随着 T 的增长消失。3. 之前的研究发现负的适应学习率 β^{tr} 可以优化 MAML 的泛化表现，但它们仅考虑了高斯各向同性输入数据和任务。该项工作在实验中发现，对于更一般的数据和任务分布，这种趋势仍然存在。利用对泛化误差的理论刻画，对这种更一般的趋势给出理论保证，并揭示了 β^{tr} 新的权衡作用。

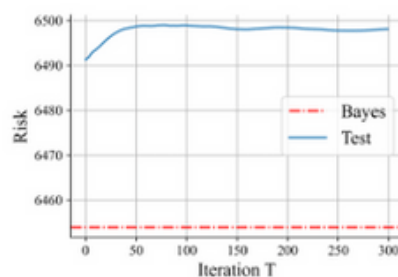
该成果研究论文：Yu Huang, Yingbin Liang, Longbo Huang. “Provable Generalization of Overparameterized Meta-learning Trained with SGD”, NeurIPS 2022.



(a) $\nu_i = 0.25 \log^{1.5}(i+1)$



(b) $\nu_i = 0.25 \log^8(i+1)$



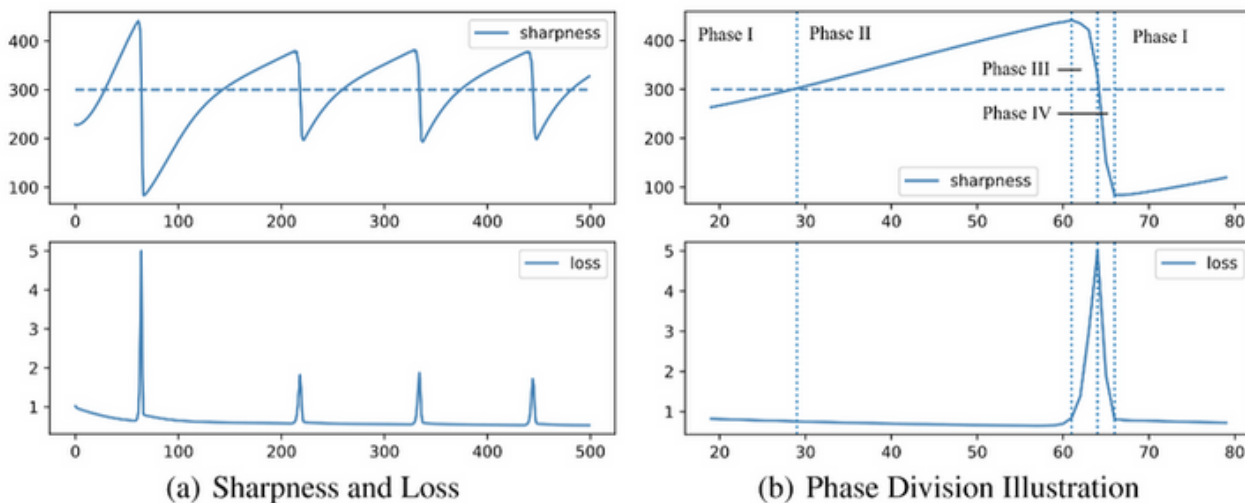
(c) $\nu_i = 0.25 \log^8(i+1)$

分析梯度下降路径上的锐度：逐步锐化与稳定性边缘

基于梯度的优化算法作为训练深度神经网络的普遍方式，在深度学习理论中处于非常重要的地位。在2021年Cohen等人在利用梯度下降算法训练神经网络时发现了一种叫做“稳定性边缘”（Edge of stability, EOS）的现象：神经网络在梯度下降的训练过程中会首先发生“逐步锐化”现象（Progressive Sharpening），即锐度（sharpness）逐渐增大；当锐度增大到超过稳定阈值 $2/(\text{学习率})$ 时，锐度则停止上升，在阈值附近震荡，即稳定性边缘。该现象和传统优化理论预测的行为非常不同，因此如何在理论上理解稳定性边缘现象是理解神经网络训练的全新挑战。

李建研究组将稳定性边缘阶段划分为四个阶段，首次在两层神经网络上证明了逐步锐化现象与稳定性边缘，同时基于最外层参数范数与锐度之间关系的假设，进一步对更广泛的神经网络中稳定性边缘发生时锐度与损失函数进行了理论上的分析与解释。

该成果研究论文：Li, Zhouzi, Zixuan Wang, and Jian Li. "Analyzing sharpness along gd trajectory: Progressive sharpening and edge of stability." Advances in Neural Information Processing Systems (NeurIPS), 2022.



带长期线性约束的组合多臂老虎机问题：背包约束与公平性约束

在以组合多臂老虎机模型(combinatorial multi-armed bandit)为代表的许多在线学习与决策场景中，决策必须满足一些长期的约束，包括采样的公平性、成本与预算等。例如，在库存或资源有限的动态定价场景中，决策者通常受到总资源或库存预算有限的背包约束，当总预算用完时，决策过程必须终止。在需要保证QoS的无线调度场景中，每个源或节点都应该按照特定的频率进行调度，以保证其QoS或吞吐量的要求。在联邦学习系统中，每个worker都应该按照预定义的频率被选择，以保证公平性。此外，在信息收集和能源调度等物联网应用中，决策者将受到背包和公平性的双重约束。已有的关于组合多臂老虎机问题的研究并不能应用到这些场景中。

基于这个问题，房智轩研究组首次提出并研究了具有长期线性约束条件的组合多臂老虎机问题。概括和统一了已有的几类研究，包括带公平约束的多臂老虎机问题，带背包约束的多臂老虎机问题(BwK)等。具体而言，该文章提出了一种置信区间LP型算法，称为UCB-LP算法，并证明了该算法能实现对数阶的遗憾(regret)和零约束违反(constraint violations)。在公平约束的特殊情况下，进一步证明UCB-LP可以保证常数级别的遗憾。该算法的遗憾阶优于所有目前关于BwK和具有公平约束的多臂老虎机问题的文献结果。此外，该文章还进一步提出了UCB-LP的另一个低复杂度版本，称作UCB-PLLP，并表明它能保证级别的遗憾和零约束违反。

该成果研究论文：Qingsong Liu, Weihang Xu, Siwei Wang, and Zhixuan Fang, “Combinatorial Bandits with Linear Constraints: Beyond Knapsacks and Fairness,” In Proceedings of the Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS), November 2022.

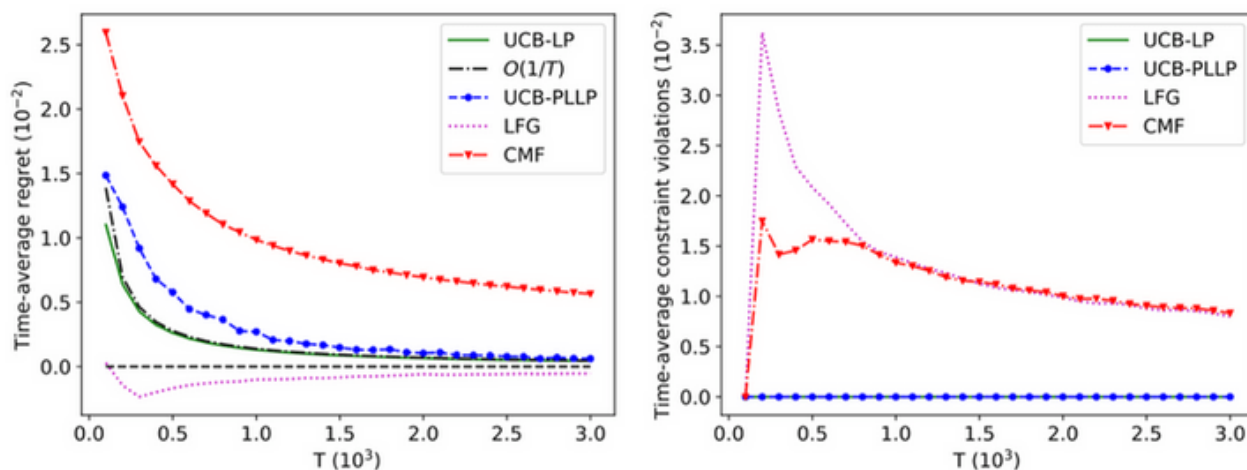


Figure 1: Results for fairness constraints

多智能体的在线学习与匹配问题

在许多双边市场中，（供需）双方的匹配是一个核心问题。而且匹配的双边常常具有未知的偏好，例如共享平台上的乘客和骑手（如Uber），或在线劳动力市场上的客户和自由职业者（如TaskRabbit）等。由于在实际场景中，在线市场的参与者主要通过自己的经验获取信息，因此一个关键问题就出现了，即如何通过从与另一方的迭代交互中学习，在这些竞争代理之间实现最佳的稳定匹配，以及以什么样的成本能够达成最佳的稳定匹配。更为一般地，是否能在去中心化的环境下实现双边的学习与匹配。

房智轩研究组考虑了多智能体的多臂老虎机(Multi-agent multi-armed bandit)问题，发现传统的利用碰撞进行通讯的算法在匹配市场中不可行，例如如果存在agent被所有的arm最偏爱，那么此agent永远不会遭受碰撞，更遑论利用碰撞来传递信息。为了解决这个问题，如果存在一个agent，不能向其余agents传递信息，那么也不会影响其余agents（包括其每一时间步的选择和最优匹配等）。基于此性质，房智轩研究组引入了communication graph和outer closed circle的概念，设计了一种基于分层迭代与通讯的去中心化算法ML-ETC，并首次在一般情形下实现了该问题上 $O(\log T)$ 的最佳遗憾。

该成果研究论文：Yirui Zhang, Siwei Wang, and Zhixuan Fang. “Matching in Multi-arm Bandit with Collision” . In Proceedings of the Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS), November 2022.

Algorithms	Model	Regret
UCB-D3	globally ranked agent	$O(M(M-1)K \log T/\Delta^2)$
UCB-D4	uniqueness consistency	$O(M(M-1)K \log T/\Delta^2)$
CA-UCB	partially decentralized	$O(\exp(M^4)M \log^2 T/\Delta^2)$ (pessimal regret)
Phased-ETC	general model	$O(MK \log^{1+\epsilon} T + \exp(1/\Delta^2))$
ML-ETC (our result)	general model	$O(MK \log T/\Delta^2)$

有期限和吞吐量限制情况下的在线任务调度

在在线任务(流量)调度问题中, 决策者(agent)每次从K个任务类型(K个不同传输节点)中激活一个任务(选择一个节点)进行调度。每次任务(传输)都有一个随机的完成时间, 只有在任务(传输)完成后才能获得奖励。所有任务类型的完成时间和产生的奖励的统计分布对决策者来说都是未知的, 决策者需要在线调度任务以在给定的时间范围内最大化累积奖励。这样的在线调度问题可以自然地建模为带有预算约束的多臂老虎机问题。然而, 这样一个带有预算约束的多臂老虎机模型未能捕捉到网络场景中的两个独特挑战: 数据新鲜度和吞吐量约束。数据新鲜度的要求出现在许多时间敏感的应用程序中, 这些应用程序对信息新鲜度或所接收数据包的信息年龄(AoI)有要求。而吞吐量约束则来自实践中常见的服务质量(QoS)要求。例如, 基站希望保证一定的总吞吐量。因此, 由于考虑中断机制和QoS约束, 已有的算法仍存在许多不足。

基于以上以及更多的实际网络场景, 房智轩研究组考虑了满足系统总吞吐量约束的在线调度算法设计。此外, 还引入了中断机制来终止持续时间超过特定期限的正在进行的任务。为了解决这个复杂的在线调度问题, 将其建模为一个有截止日期和吞吐量限制的在线学习问题。然后, 该研究组提出了一种最优离线策略, 并基于李亚普诺夫方法开发了高效的在线学习策略。证明了在线学习算法实现了一个阶的后悔(R)和零约束违反(Vio)。并且还进行了仿真实验来评估开发的在线学习算法的性能。

该研究成果论文: Qingsong Liu and Zhixuan Fang, “Learning to Schedule Tasks with Deadline and Throughput Constraints,” Proceedings of IEEE International Conference on Computer Communications (INFOCOM), May 2023.

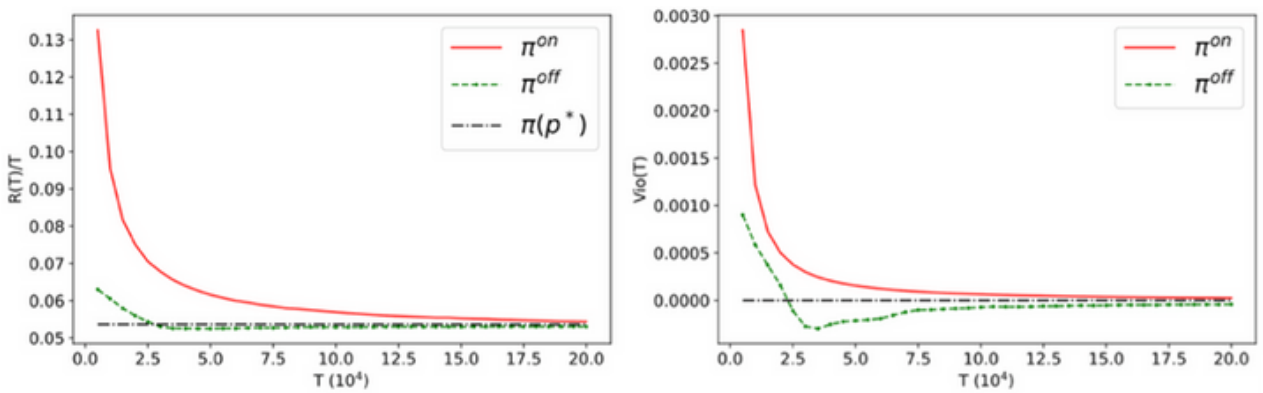


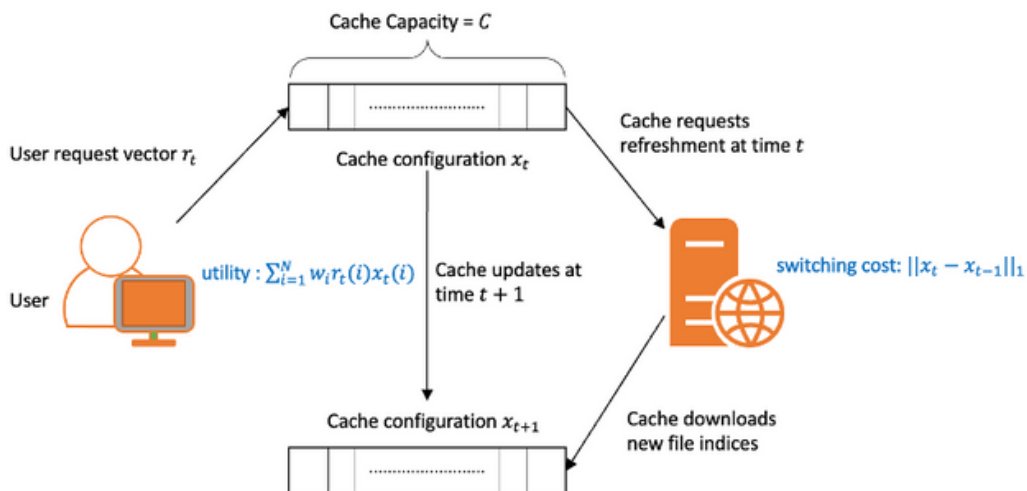
Fig. 1. Performance of π^{off} and π^{on}

带切换成本的在线凸优化：算法与性能

在许多控制和优化场景中，如电力分配或网络资源配置，决策者(agent)会同时产生决策成本和决策变化而导致的切换成本，即带切换成本的在线凸优化(SOCO)问题。当损失函数的序列是可预测的时候，目前最先进的R-OBDA算法已被证明对强凸损失函数具有最优的动态遗憾保证。一个自然的问题是：决策者是否可以在不能预测未来损失函数的情况下(即在线学习设置)获得最佳的动态遗憾保证？以往的研究提供了一些不错的理论结果，但它们要么假设损失函数是线性或光滑的，要么要求对动态遗憾比较器序列的路径长度有先验知识，因此没有具有一般性的理论结果。

基于以上问题，房智轩研究组考虑了带切换成本且无损失函数预测信息情况下的在线凸优化问题，并选择动态遗憾作为性能度量。最终证明，在不预测损失函数的情况下，该研究提出的算法IOMD-SOCO可以实现一般凸损失函数的最优阶动态遗憾保证。房智轩研究组还提出了它的无参数版本，即不需要有遗憾比较器基准序列的路径长度的先验知识，并实现了同阶的遗憾保证。也就是说，在损失函数不可预测的情况下，该研究首次给出了一般凸损失函数的无参数动态遗憾次线性保证。同时也给出了一些SOCO在实际网络场景中的应用，比如电力系统的经济性调度，带切换成本的cache缓存和云资源供应。

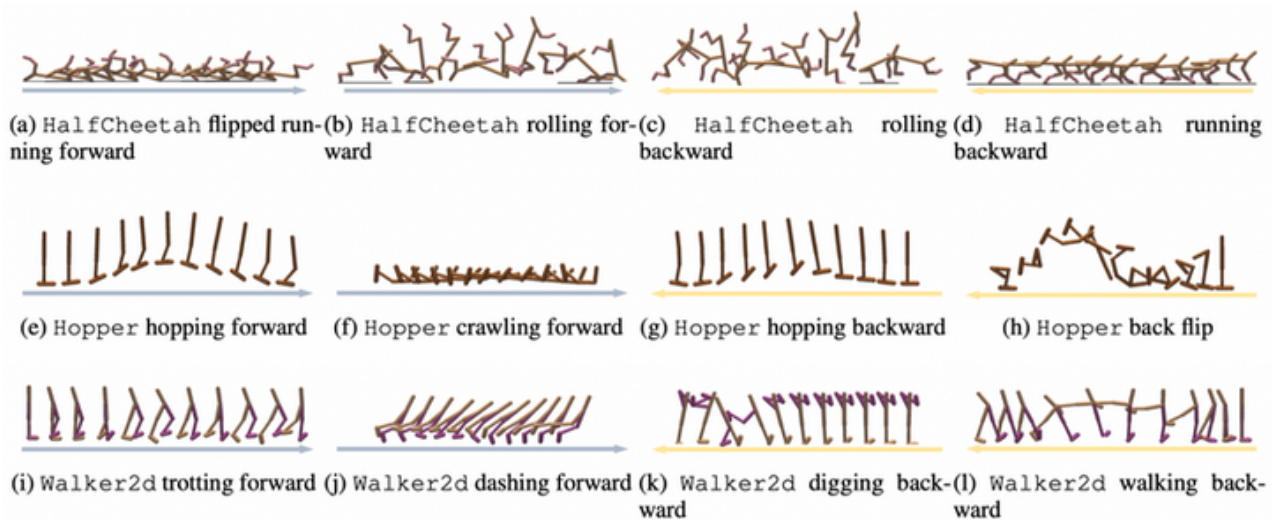
该成果研究论文：Qingsong Liu, Zhuoran Li, and Zhixuan Fang, “Online Convex Optimization with Switching Costs: Algorithms and Performance,” Proceedings of the 20th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), September 2022.



基于循环训练的无监督技能学习算法

在强化学习中，通常会遇到奖励函数稀疏或者难以设计的情况，此时将对学习的探索过程造成很大的挑战。无监督技能学习能够在没有奖励函数的情况下自主发现各种新的技能，是解决该挑战的有效方法。然而目前的无监督技能学习方法均采用策略并行学习的方式。陈建宇课题组研究发现这种并行学习架构将导致一种探索失效的现象，使得初期探索过的状态将在之后被抑制，从而影响了探索效率。该工作结合状态覆盖内生奖励设计出了一种新的循环技能学习架构，从而大幅提高了技能的状态覆盖率以及多样性。

该研究相关论文：Z. Jiang, J. Gao and J. Chen. “Unsupervised Skill Discovery via Recurrent Skill Training”, NeurIPS 2022.

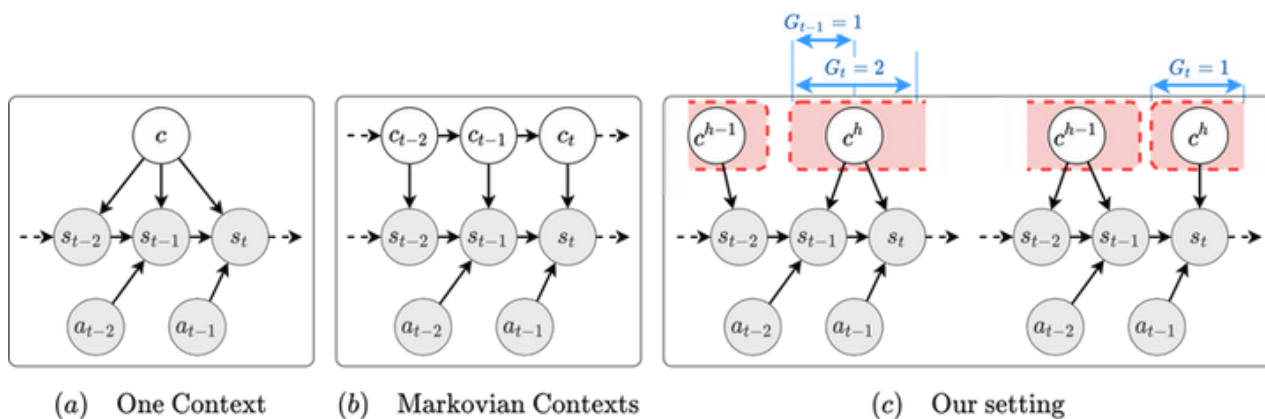


ReST算法自主发现的多样性智能体技能展示

基于分段语境的非静态环境自适应深度强化学习

将强化学习应用到机器人等真实世界任务中时，一个很重要的挑战就是如何自动适应非静态变化的环境，例如对足式机器人来说路面环境的变化。环境语境可以被用来描述环境的变化，已有工作多假设该语境是不变的或者具备马尔可夫性，然而很多条件下这些假设并不成立。陈建宇课题组提出了一种基于分段语境的非静态环境自适应深度强化学习方法，能够对环境变量的突然变化进行推断并获得自适应的控制策略。

该研究相关论文：X. Chen, X. Zhu, Y. Zheng, P. Zhang, L. Zhao, W. Cheng, P. Cheng, Y. Xiong, T. Qin, J. Chen, TY. Liu. “An Adaptive Deep RL Method for Non-Stationary Environments with Piecewise Stable Context”, NeurIPS 2022.

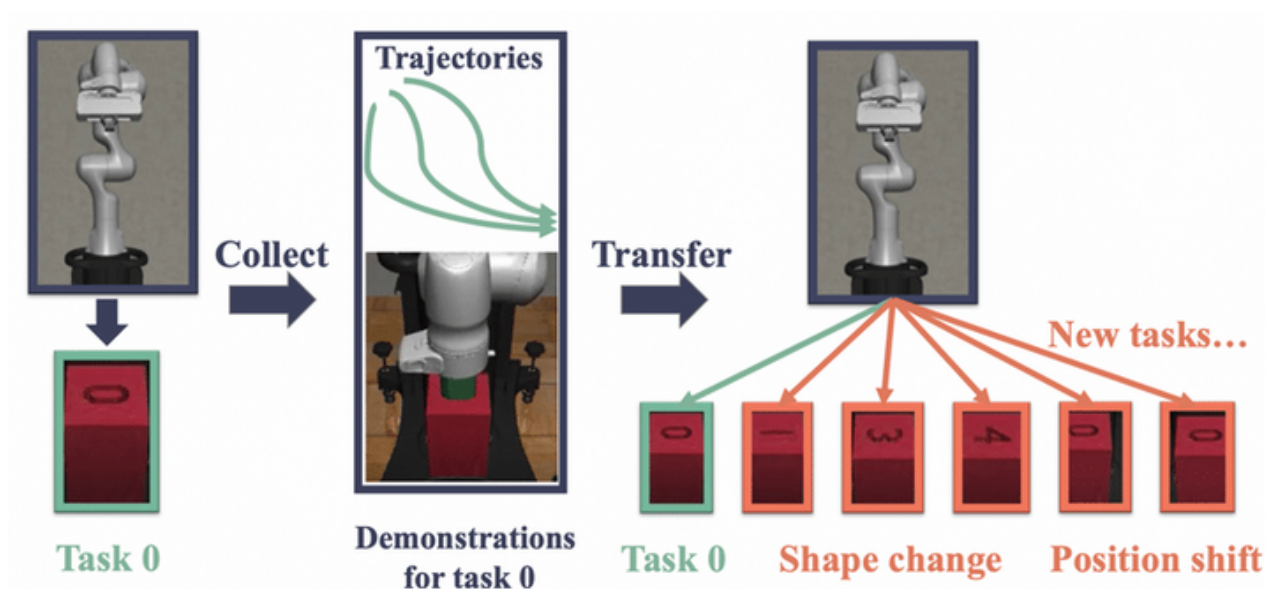


基于分段语境的非静态环境问题

稀疏奖励下的任务可迁移演示强化学习

在很多机器人学习任务，例如插孔装配等，其在任务完成时才会获得相应的奖励，这种稀疏的奖励对强化学习带来了很大的挑战。引入成功完成任务的演示是解决这一挑战的一种主要手段。然而，已有方案多要求对每一个任务都需要提供相应的演示，这是比较昂贵且耗时的。陈建宇课题组提出了一种稀疏奖励下的任务可迁移演示强化学习方法，通过对新的任务进行基于相似任务演示的奖励塑性，实现了仅提供一个任务下的演示就让其他相似的稀疏奖励任务都得到提升的效果。

该研究相关论文：Y. Guo, J. Gao, Z. Wu and J. Chen. “Reinforcement Learning with Demonstrations from Mismatched Task under Sparse Reward” , CoRL 2022.



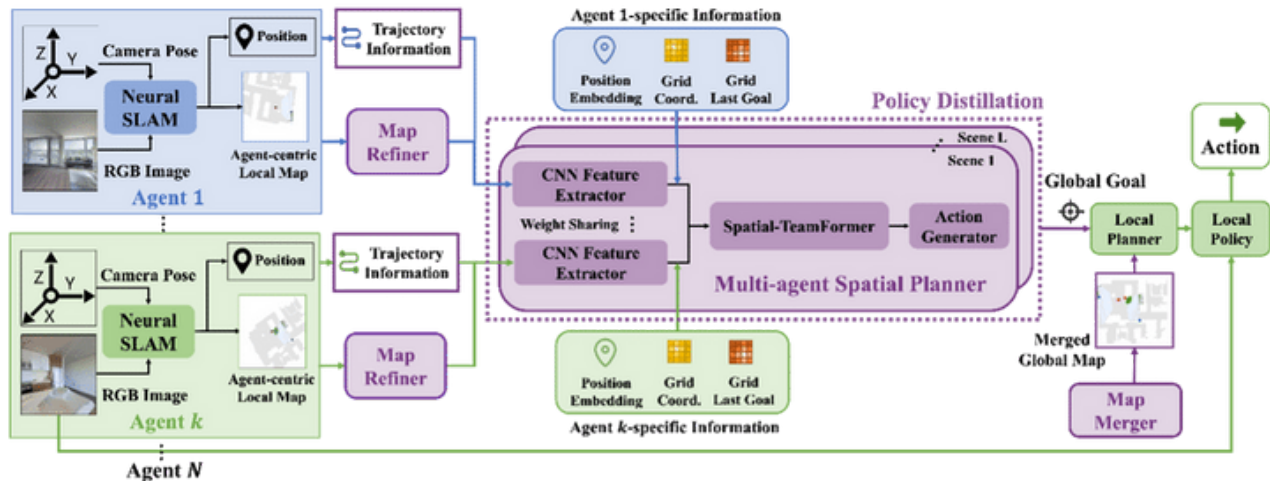
任务可迁移的演示强化学习

多机协同高效机器学习系统研究

探索是构建智能机器人系统的重要任务，已在救援、自动驾驶、无人机，移动机器人等众多应用领域得到广泛应用。在多机器人合作探索任务中，机器人间需要有效地分配探索工作量，从而获得比单机器人探索更高的探索效率。由于基于强化学习的方法可用于表达复杂策略，多智能体强化学习已成为解决该合作探索问题的一种趋势方法。

吴翼研究组在多机协同探索领域取得重要进展，首次提出了多智能体视觉探索方法，多智能体主动式神经SLAM (Multi-Agent Active Neural SLAM，简称MAANS)。MAANS首次在33个室内3D仿真场景中达到了远远超过传统规划方法的探索效率。MAANS中使用了一个基于Transformer的网络结构，通过层级化的自注意力机制，该网络结构可以有效提取空间以及机器人间的信息。目前该成果已有开源框架。该方法对于构建在真实世界中的智能机器人系统有重大意义。

该成果研究论文Yu Chao, Xinyi Yang, Jiaxuan Gao, Huazhong Yang, Yu Wang, and Yi Wu. "Learning efficient multi-agent cooperative visual exploration." In European Conference on Computer Vision, pp. 497-515. Springer, Cham, 2022.



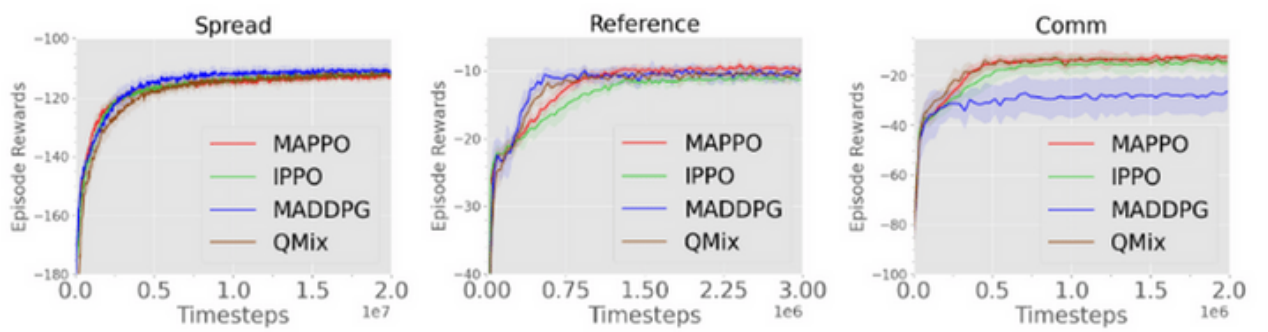
合作场景下的多智能体强化学习算法研究

在多智能体系统中，合作是最重要的行为模式之一。在合作场景下，多智能体强化学习的目标是通过与环境交互，优化策略，并最终得到最优的合作方案。如何达到高样本效率和高回报是该研究领域的一个研究热点。

吴翼研究组在多智能体强化学习领域取得突破性的进展，通过实验验证了基于近端策略优化方法的在线策略算法在多智能体合作场景下能够在最终回报上超过此前的离线策略方法，同时还有着与此前的离线策略方法相当的样本效率。多智能体近端策略优化方法对于参数具有较好的鲁棒性，并具有高度通用性，无需领域特定的算法改动和结构设计即可在所有测试任务中达到SOTA的水平。目前该成果开源框架已有超过600次引用。该方法对于多智能体强化学习领域的后续研究和应用有着重要价值。

该成果研究论文 Chao Yu, Akash Velu, Eugene Vinitzky, Jiaxuan Gao, Yu Wang, Alexandre Bayen, and Yi Wu. 2022. The Surprising Effectiveness of PPO in Cooperative Multi-Agent Games. In Thirty-sixth Conference on Neural Information Processing Systems Datasets and Benchmarks Track.

Scen.	MAPPO	QMix	CDS	TiKick	# Players	Metric	MAPPO	IPPO	SAD	VDN
3v.1	88.03 (1.06)	8.12(2.83)	76.60(3.27)	76.88(3.15)	2	Avg.	23.89(0.02)	24.00 (0.02)	23.87(0.03)	23.83(0.03)
CA(easy)	87.76 (1.34)	15.98(2.85)	63.28(4.89)	/		Best	24.23 (0.01)	24.19(0.02)	24.01(0.01)	23.96(0.01)
CA(hard)	77.38 (4.81)	3.22(1.60)	58.35(5.56)	73.09(2.08)	3	Avg.	23.77 (0.20)	23.25(0.33)	23.69(0.05)	23.71(0.06)
Corner	65.53 (2.19)	16.10(3.00)	3.80(0.54)	33.00(3.01)		Best	24.01 (0.01)	23.87(0.03)	23.93(0.01)	23.99(0.01)
PS	94.92 (0.68)	8.05(3.66)	94.15 (2.54)	/	4	Avg.	23.57 (0.13)	22.52(0.37)	23.27(0.26)	23.03(0.15)
RPS	76.83 (1.81)	8.08(4.71)	62.38(4.56)	79.12(2.06)		Best	23.71(0.01)	23.06(0.03)	23.81 (0.01)	23.79(0.00)
					5	Avg.	23.04 (0.10)	20.75(0.56)	22.06(0.23)	21.28(0.12)
						Best	23.16 (0.01)	22.54(0.02)	23.01(0.01)	21.80(0.01)

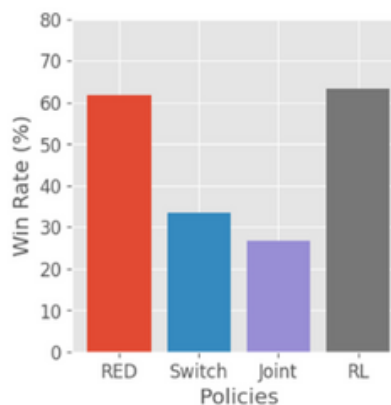
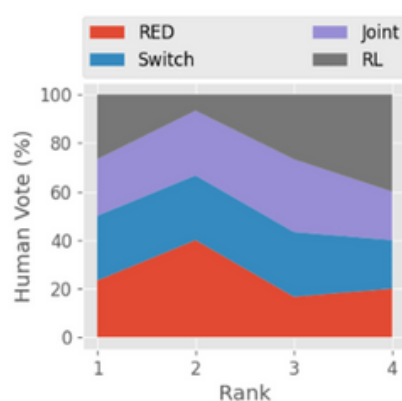
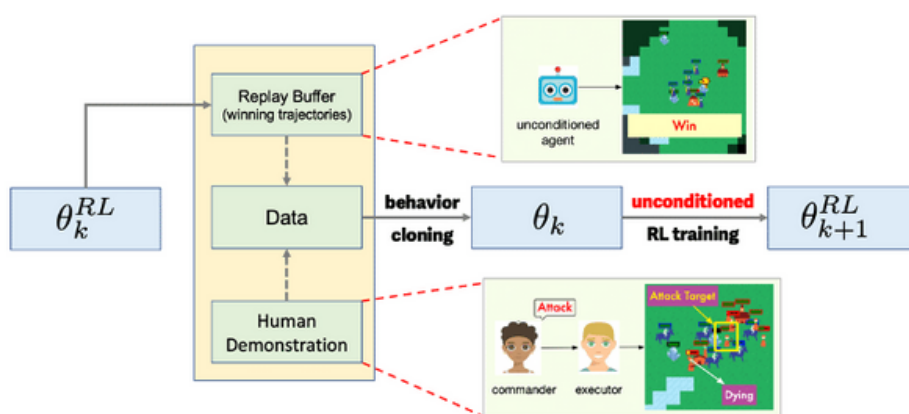


基于自然语言交互的强化学习智能体研究

自然语言是人类沟通的重要手段，为人类文明的发展和传播做出了巨大的贡献，也是人机交互的一个重要接口。通过自然语言交互，人类可以更方便地指挥智能体达成自己的目标，智能体也能更好地满足人类的各种偏好。但是自然语言的指令很多时候是精炼且模糊的，通常不会涉及具体的执行细节。一方面，希望智能体能够听从指挥，另一方面，又希望智能体更加聪明，其采取的措施能更好地完成既定的任务。

吴翼课题组在这个问题上取得了突破性进展，他们将这个问题建模成了一个带约束的强化学习问题，并且提出了强化演示蒸馏算法。首先，该课题组利用模仿学习，让智能体从人类演示数据中，学会如何跟从模糊的自然语言指令。然后，利用强化学习，进一步优化了智能体的执行细节。经过多次迭代，最终得到的智能体能够听从自然语言的指挥，并且更加高效地完成任务。例如，在复杂的实时战略游戏中，人类玩家只需要用简单的几句话描述自己的策略，智能体就能实现人类玩家的想法。这样的交互让智能体拥有了执行复杂策略的能力，恰当的策略能够大幅提高智能体的胜率。同时，这样的交互也让智能体变得更加安全可控。该研究对推进人机交互，人工智能的应用起到了重要作用。

该成果研究论文：Shusheng Xu, Huaijie Wang, Yi Wu. “Grounded Reinforcement Learning: Learning to Win the Game under Human Commands” Advances in Neural Information Processing Systems (2022).

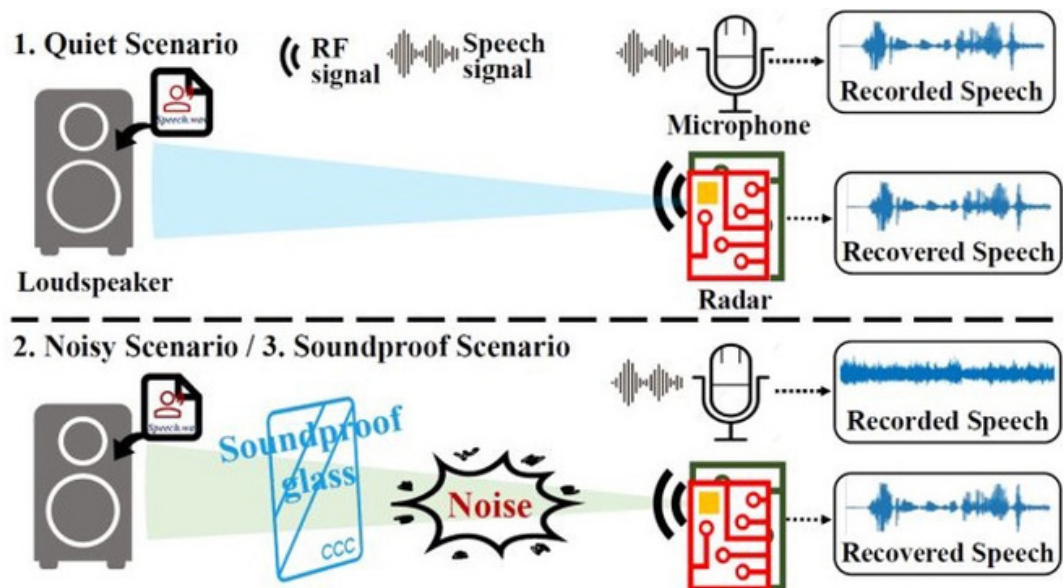


从射频信号中恢复高质量语音Radio2Speech

麦克风是人机交互和窃听领域中常见的设备，但在有干扰噪音和隔音材料的场景下，其性能会大幅下降。射频信号不受噪音和光照的影响并且可以穿过许多隔音以及不透明的障碍物。基于射频信号的这种性能，赵行研究组提出了Radio2Speech，一个使用毫米波雷达信号来恢复高质量语音的系统。Radio2Speech在安静环境下可以恢复与麦克风质量相当的语音，而在嘈杂环境和有隔音玻璃的环境下表现远优于传统的麦克风。

使用射频信号来恢复语音信号的原理是：声音产生于声源的震动，毫米波雷达向声源发射信号，通过对反射的雷达信号进行处理可以得到相应的震动信号，从而恢复原始的音频信号。过去射频“麦克风”系统的一些尝试只能恢复出单音音乐和不容易让听众辨识的语音，而Radio2Speech则可以恢复出高质量且自然的人说话的语音。

该成果研究论文：Running Zhao, Jiangtao Yu, Tingle Li, Hang Zhao*, Edith C.H. Ngai*, Radio2Speech: High Quality Speech Recovery from Radio Frequency Signals, Interspeech 2022.

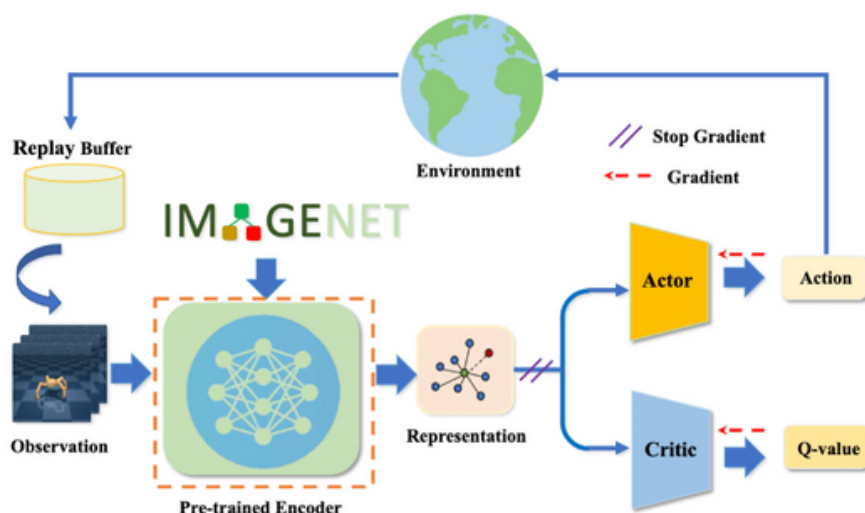


一种基于预训练图像编码器的可泛化视觉强化学习方法

许华哲研究组提出了可泛化强化学习智能体的训练方案PIE-G。如何训练出能够在不同视觉场景中都具有泛化能力的智能体受到研究者的关注。通过利用外部数据来引导编码器得到鲁棒表征是一种常用的做法。但外部数据与训练数据之间存在分布偏移，如何利用外部数据，在不影响训练的同时提升模型泛化能力是该问题的重要难点之一。

该研究提出了一种新的范式，通过加载ImageNet预训练模型作为智能体编码器，利用该编码器提取的表征进行下游任务训练。与现有方案不同，PIE-G无需针对每个任务都去单独训练编码器生成表征，而是直接利用ImageNet的预训练模型生成的表征，即可在多个控制任务中取得在样本利用率和泛化性能上的优异表现。该研究通过使用浅层特征，重新计算BatchNorm统计参数等方法，在最具挑战的setting下，PIE-G获得了超过此前最优方案55%的性能提升。该项目的研究论文已收录于NeurIPS2022，并获得优选高光论文spotlight奖励(top 5%)。

该成果研究论文：Zhecheng Yuan, Zhengrong Xue, Bo Yuan , Xueqian Wang , Yi Wu, Yang Gao, Huazhe Xu, Pre-Trained Image Encoder for Generalizable Visual Reinforcement Learning, NeurIPS 2022.

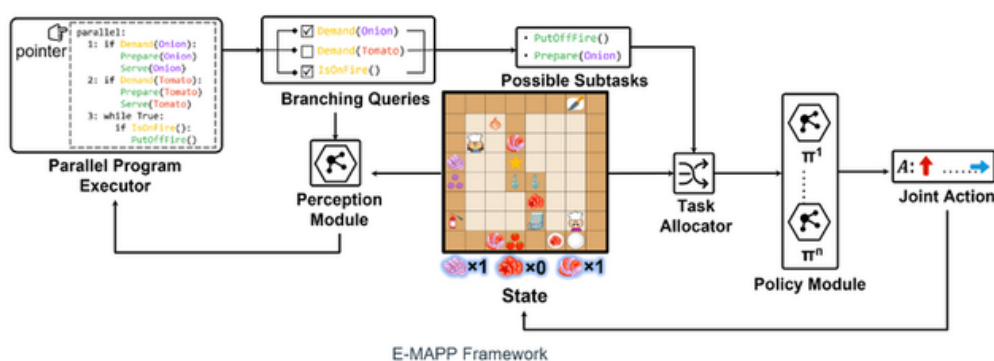


提出了多智能体在并程序指导下的强化学习框架E-MAPP

多智能体系统完成复杂的长阶段任务一直是多智能体强化学习领域的一个重大挑战。基于指导程序的强化学习利用程序的任务结构表达能力和组合泛化能力，已经证实了能够帮助单智能体较好地完成长阶段任务，但应用于多智能体系统仍会面临许多挑战，包括 1) 智能体需要推理子任务间依赖关系； 2) 智能体需要进行合理的分工合作。

为了解决这些问题，许华哲课题组提出定义了一种新的任务形式：基于并程序指导的多智能体强化学习，并提出了框架E-MAPP来高效地完成智能体对程序语义的理解和利用程序规划行动路线。同时，在Overcooked-v2 环境上进行了实验。实验结果表明，在拥有超过5个阶段子任务的复杂长阶段任务上，使用端到端强化学习和基于自然语言指导的强化学习只有约1%的成功率，而使用已提出的E-MAPP框架可以获得56%的成功率，同时拥有不错的零样本组合泛化能力。该项目的研究论文已收录于NeurIPS2022，并获得优选高光论文spotlight奖励(top 5%)。

该成果研究论文：Can Chang, Ni Mu, Jiajun Wu, Ling Pan, Huazhe Xu, E-MAPP: Efficient Multi-Agent Reinforcement Learning with Parallel Program Guidance, NeurIPS 2022.

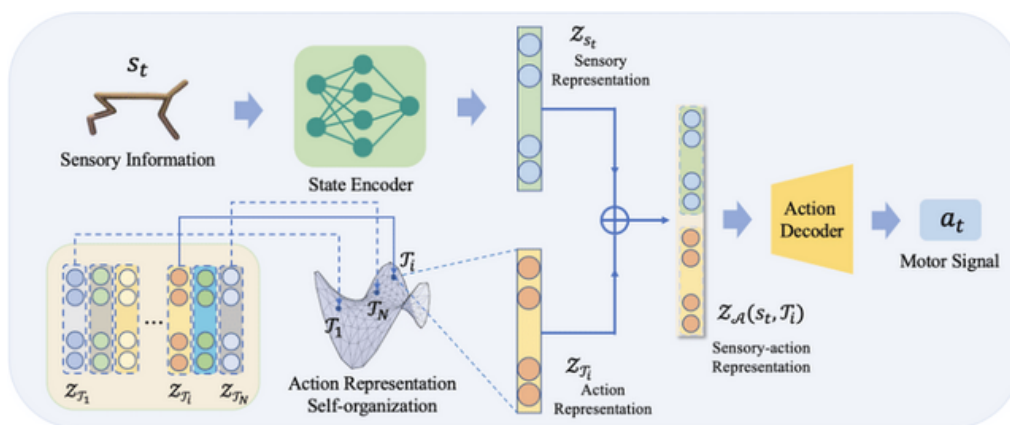


使用多任务强化学习得到自组织的动作表征空间

人类执行多项任务时，会自然地将底层的肌肉运动概括为顶层的、更抽象的“动作表征”，例如“拿起物体”或“向左转”，这些表征只需稍作修改即可在新的任务中重复使用。通过类比人类的这种能力，人们希望强化学习中的智能体也能拥有将底层的运动控制抽象为顶层的动作表征，然后它们可以通过重复使用、修改或组合这些动作表征来执行新的任务。

为了解决以上的问题，课题组提出，在多任务学习的框架下使智能体学习到可泛化的动作表征，从而实现任务层面对新的未接触任务的泛化。在训练过程中，时变的感知信息与时不变的动作信息被解耦，而后两者拼接成为感知-动作表征并被策略网络转化为底层的动作控制信号。经过训练，智能体学习到了一个自组织的动作表征空间，在表征空间内对预训练的任务表征向量进行简单的插值、组合以及搜索都能够十分高效地获得新任务的动作表征。

该项目的研究论文已被NeurIPS 2022 Deep RL Workshop接收，同时投稿至ICLR 2023。论文预印本：Hua Pu, Yubei Chen, and Huazhe Xu. "Simple Emergent Action Representations from Multi-Task Policy Training." arXiv preprint arXiv:2210.09566 (2022).



二、自动驾驶

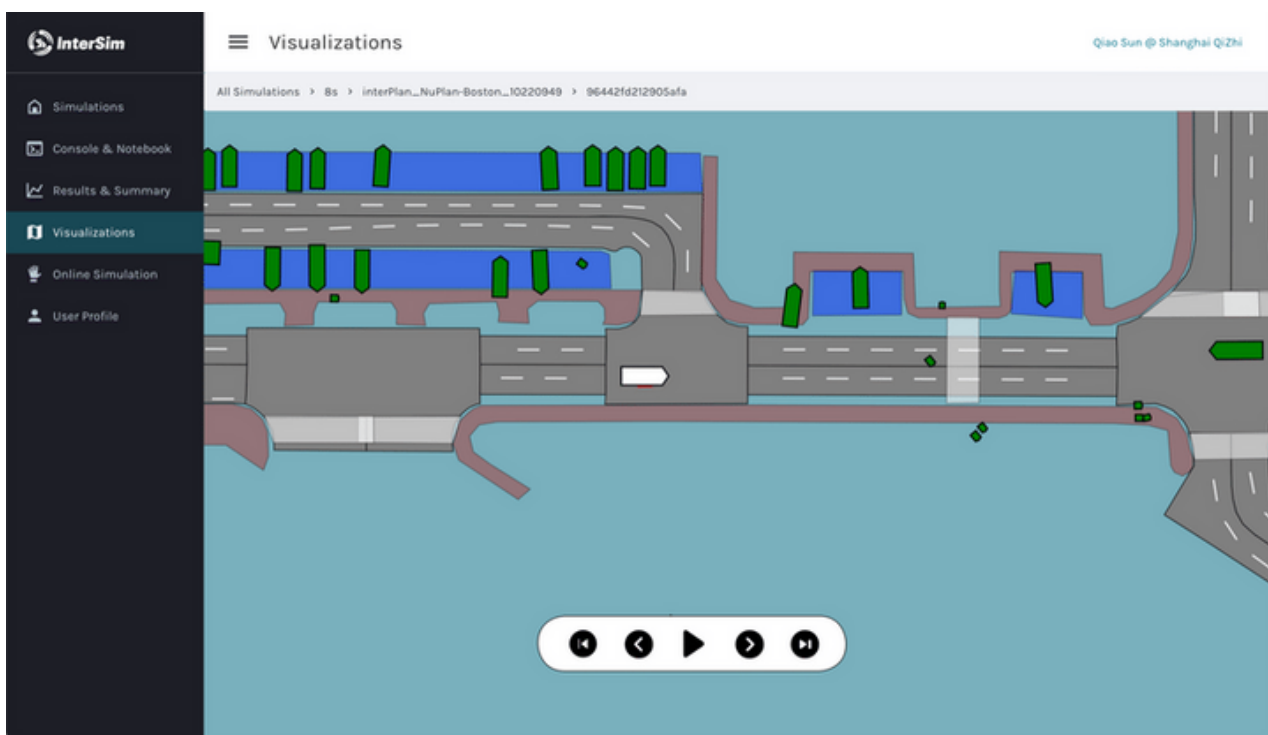
主要完成人：赵行研究组、陈建宇研究组

发布自动驾驶中的闭环行为交互仿真器InterSim

仿真一直是机器学习应用在机器人上的重要一环，被广泛用于生成更多的训练数据，性能测试和调试。自动驾驶系统中的行为仿真主要进行对人的意图和轨迹的建模，同时需要考虑自车对环境和人的响应。自动驾驶仿真器对于自动驾驶的大规模有着重要的意义。

赵行研究组开发并且发布了首个基于大规模真实数据集（Waymo Open Dataset）的自动驾驶仿真器InterSim。InterSim基于真实数据集的车辆行为进行模型训练；在应用时，当轨迹规划器使用不同的策略时，仿真器能给出不同的、且逼真的行为反应。InterSim可以为自动驾驶规划算法提供评测平台和训练数据。目前InterSim已经公开发布，吸引了全世界几十个团队使用。

该成果研究论文：Qiao Sun, Xin Huang, Brian C Williams, Hang Zhao, InterSim: Interactive Traffic Simulation via Explicit Relation Modeling, IROS 2022.

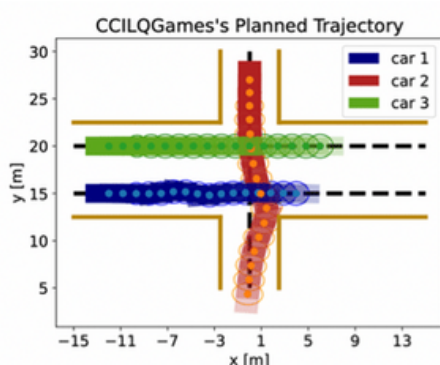


概率安全约束下的迭代线性二次型随机博弈

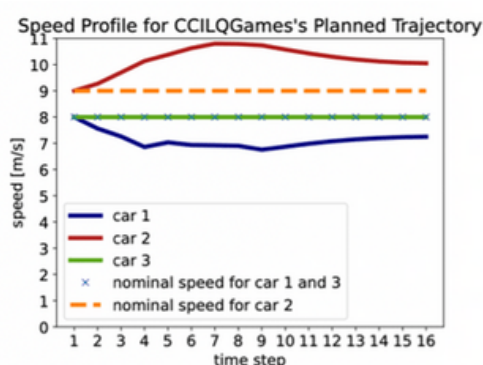
对于自动驾驶等多智能体/人机交互问题，现有的决策规划方法多采用先预测再规划的方法。然而此种方法忽略了多机器人的博弈交互特性：其他智能体的未来行为轨迹将随被控智能体行为的变化而改变。动态博弈是解决多机器人/人机交互决策规划的重要课题，其中安全约束的满足和对不确定性的处理对其在真实世界中的应用尤其重要，然而已有方法缺乏对不确定条件下安全约束的处理。

陈建宇课题组通过融合增广拉格朗日、概率约束、以及线性二次型博弈算法，提出了能满足安全约束条件的随机博弈策略规划算法（CCILQG），从而使得智能体能在满足安全的条件下规划出具有强交互性的轨迹，并在无人驾驶任务上做了仿真验证。该方法对不确定条件下无人驾驶等多机器人/人机交互场景的安全强交互性决策规划提供了理论与算法基础。

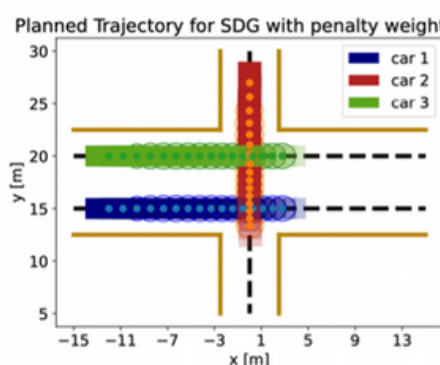
该研究相关论文：H. Zhong, Y. Shimizu and J. Chen. “Chance-Constrained Iterative Linear-Quadratic Stochastic Games”, IEEE Robotics and Automation Letter, 2023.



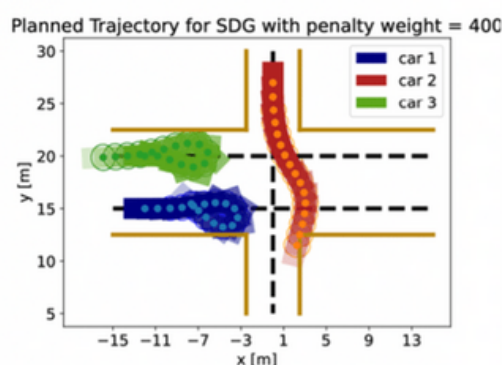
(a)



(b)



(c)



(d)

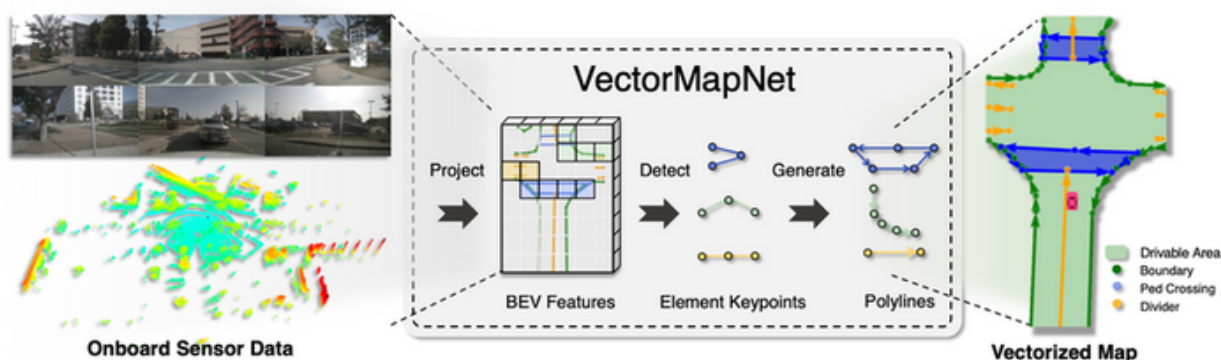
CCILQG方法应用于无人车交互博弈决策场景

在线构建自动驾驶的高精度矢量地图VectorMapNet

在线地图构建是近年来最为热门的自动驾驶问题之一，赵行研究组去年的工作HDMaPNet首次通过实例分割和后处理的方式来生成矢量化地图，但这种方法仍然依赖于栅格化的地图分割，并不能方便的扩展到三维空间中，而且其启发式的后处理会让整个框架变得特别复杂。

今年，赵行研究组提出了端到端的矢量地图构建方法VectorMapNet。该方法首先采用了一种统一的polyline（多段线）来表示地图元素，而后利用集合预测（set prediction）和序列生成（sequence generation）的方法来检测和恢复地图中的所有地图元素。该方法不仅更高效简洁地生成了矢量地图，并且证明了生成的地图可以用于提升下游轨迹预测的任务的效果。

该成果研究论文：Yicheng Liu, Yuantian Yuan, Yue Wang, Yilun Wang, Hang Zhao, VectorMapNet: End-to-end Vectorized HD Map Learning, arXiv:2206.08920, 2022.

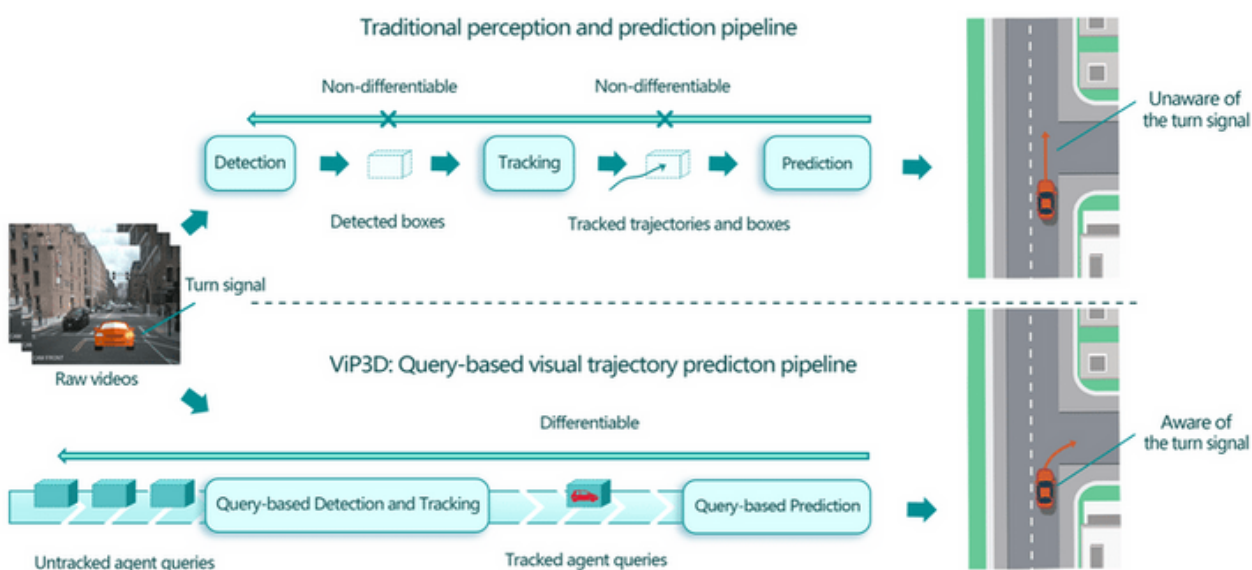


端到端的视觉轨迹预测ViP3D

在自动驾驶中，视觉图像相比LiDAR数据有着更丰富的语义信息，充分挖掘视觉中的语义信息可以极大地帮助对场景中车和人的行为预测。然而，传统的自动驾驶方案将检测、跟踪、预测三个模块分别进行开发和建模，使其无法获取视觉中的精细特征。

赵行研究组提出了第一个基于视觉的轨迹预测方案ViP3D。ViP3D是第一个基于视觉的自动驾驶轨迹预测框架，并且从检测、跟踪到预测整个流程都是可微的。ViP3D使用agent query作为模块之间的接口，显式地对周围的车辆和行人进行建模。此外，ViP3D支持流式处理模式，只需维护和更新agent query，不需要存储历史帧的图像特征，在保持高效的同时拥有更好的性能。

该成果研究论文：Junru Gu, Chenxu Hu, Tianyuan Zhang, Xuanyao Chen, Yilun Wang, Yue Wang, Hang Zhao, ViP3D: End-to-end Visual Trajectory Prediction via 3D Agent Queries, arXiv:2208.01582, 2022.



三、计算机系统结构

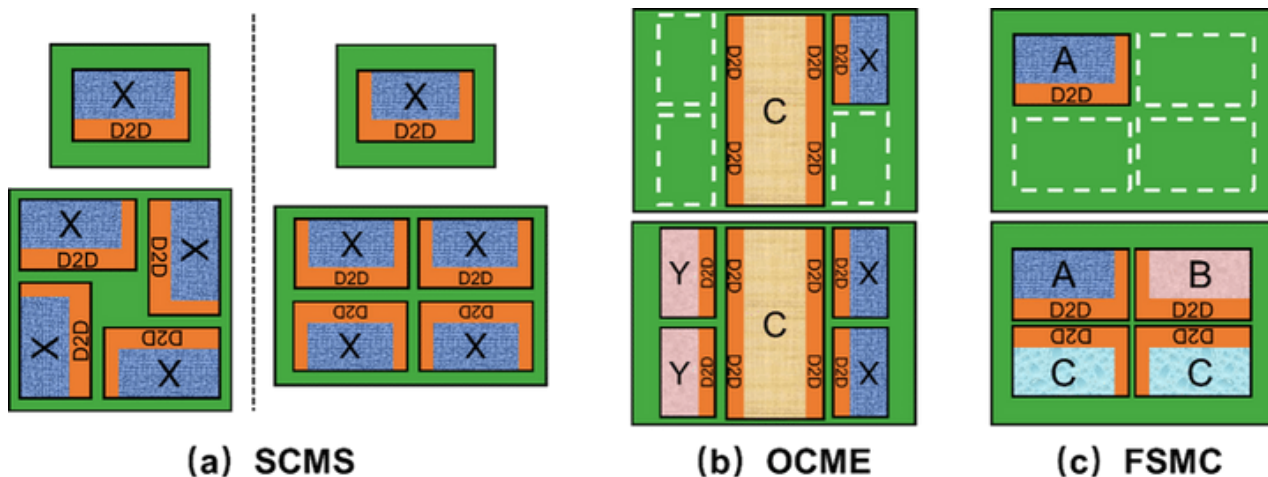
主要完成人：高鸣宇研究组、马恺声研究组

Chiplet精算师：定量成本模型与芯片复用探索

多芯片集成技术被业界广泛认为是摩尔定律的延续，节省成本是其广为人知的优势之一，但是很少有工作能够定量地展示多芯片集成系统对比单芯片的成本优势。清华大学交叉信息研究院马恺声研究组基于三种典型的多芯片2.5D集成技术，建立了一个定量的多芯片系统成本模型，并提出了一套分析方法，从良品率提高、芯片和封装复用以及异构集成等多方面分析了多芯片系统的成本效益。

研究发现，不是所有的芯片都适合用多芯片技术，对于单个系统，除非是已经接近甚至超过了“摩尔极限”，否则单芯片系统是更合适的；多芯片系统的真正优势在于芯片的复用，当芯片的可复用性被充分利用时，芯片的NRE投入被均摊至几乎可以忽略不计。

该研究成果论文：Yinxiao Feng, Kaisheng Ma. “Chiplet Chiplet Actuary: A Quantitative Cost Model and Multi-Chiplet Architecture Exploration.” Design Automation Conference, 2022.

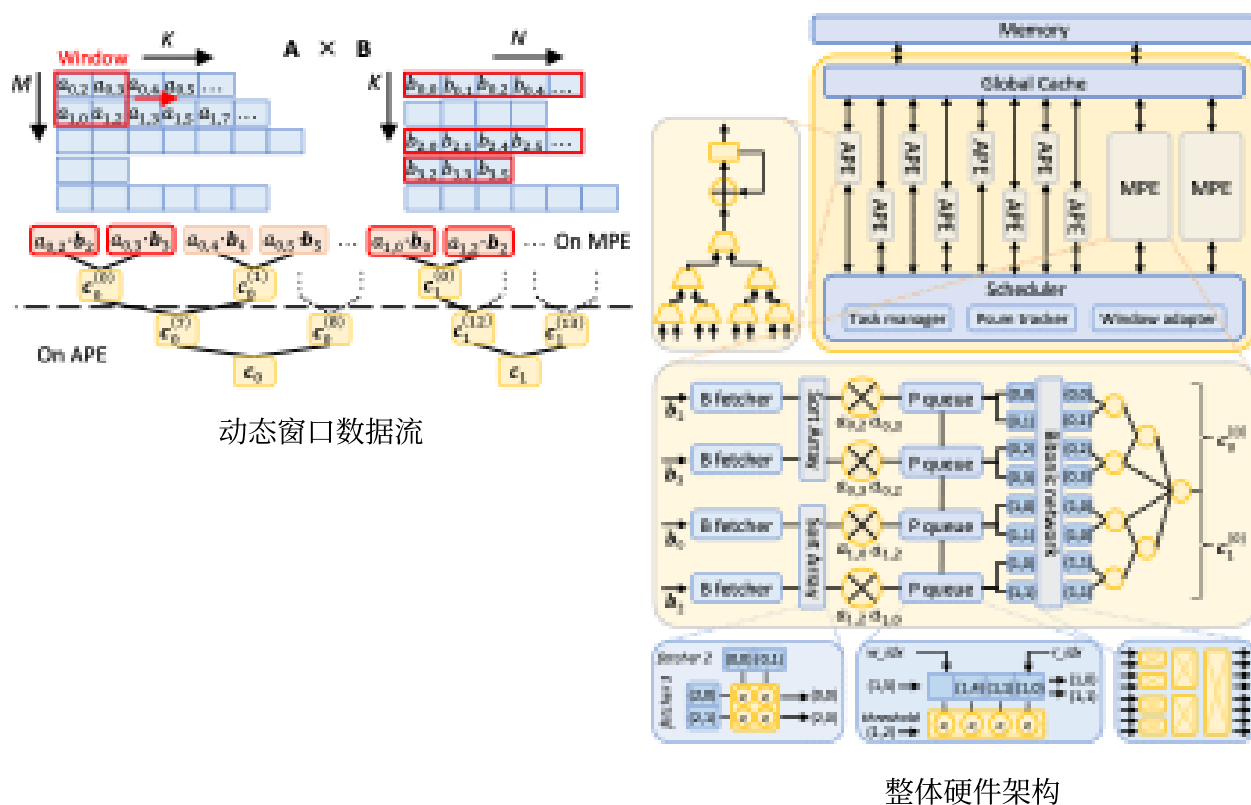


稀疏矩阵乘的自适应加速硬件架构

稀疏矩阵乘法在许多科学计算和深度学习应用中被广泛使用。其高度不规则的稀疏结构限制了它在传统计算平台上的性能和效率，由此催生了大量的硬件加速器设计。现有的稀疏矩阵乘法加速硬件只支持特定的数据流，如内积、外积、基于行的数据流等。每种数据流只在特定的稀疏结构上有优势，无法在所有的数据分布上保持高效。

由此，高鸣宇研究组提出了一个新的稀疏矩阵乘法加速硬件SPADA，可以有效适应各种稀疏结构。首先，该研究组设计了一个基于动态窗口的自适应数据流作为现有方案的统一，可以灵活地在不同的数据流间切换，从而最好地匹配数据分布。其次，为有效地支持这种自适应数据流，同时设计了相应的硬件架构，具有灵活、快速、低成本的可重构性和有效的负载均衡功能。最后，基于邻近矩阵区域的稀疏结构具有相似性的这一观察，该研究利用历史性能来预测稀疏结构并确定要使用的最优数据流。实验结果表明，SPADA能够达到或超过现有的两个最佳稀疏矩阵乘法加速硬件，避免稀疏结构和数据流不匹配导致的性能下降。在由来自图计算及压缩神经网络模型的测试集上，SPADA平均性能提高了40%。

该研究成果论文：Zhiyao Li, Jiaxiang Li, Taijie Chen, Dimin Niu, Hongzhong Zheng, Yuan Xie, Mingyu Gao, “Spada: Accelerating Sparse Matrix Multiplication with Adaptive Dataflow”, ASPLOS 2023.

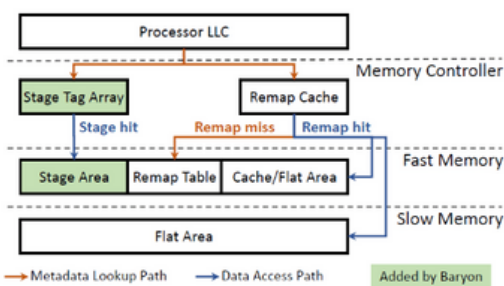


基于压缩和分块的高效率异构内存管理系统

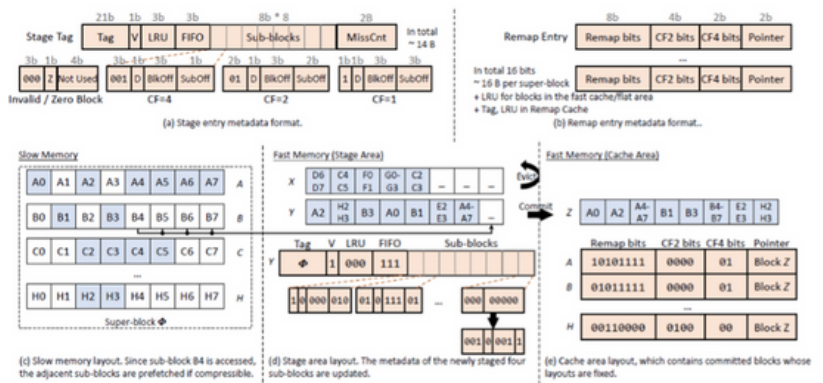
通过结合多种带宽性能和存储密度特点的内存类型，异构内存系统（hybrid memory system）可满足大数据和人工智能时代应用负载的内存需要。目前典型的异构内存实例将传统动态随机存取存储器（DRAM）作为快内存，将高密度低带宽的非易失存储器（NVM）作为慢内存。近年来，使用纯硬件管理机制的异构内存系统成为研究热点，具有无需修改上层应用、消除操作系统虚拟内存管理的粗粒度和缺页中断的高开销等优点。

高鸣宇研究组发现现有异构内存系统中基于替换算法设计的工作在慢存带宽利用率和快存容量利用率上只能互相权衡，整体系统利用率提升有限。为了进一步提高异构内存管理系统的性能和效率，该研究组提出使用分块（sub-blocking）和压缩（compression）技术同时提高两方面利用率，达到比之前工作更优的性能。分块技术将数据块细分为更小粒度的子块，只传输和缓存所需的子块。压缩技术将低熵数据块以压缩子块的粒度储存和传输。然而，支持压缩和分块带来了更高的元数据存储开销和更复杂可变的数据布局管理挑战。该研究组提出“暂存区”的概念以适应数据布局在初始状态的多变性。同时利用数据布局在稳定状态的不变性、压缩局部性等实验观察，简化元数据格式和大小。该系统相比当前最佳工作可达到平均1.27倍、最高1.74倍性能提升。

该研究成果论文：Yiwei Li, Mingyu Gao, “Baryon: Efficient Hybrid Memory Management with Compression and Sub-Blocking,” HPCA 2023.



系统整体架构



暂存区和缓存区的数据布局和元数据格式

四、自然语言处理

主要完成人：李建研究组、杨植麟研究组

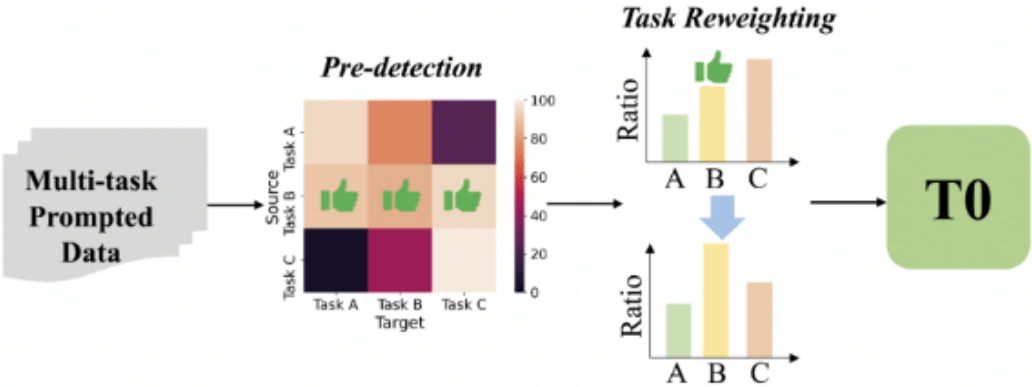
首次提出基于提示符的多任务预训练的零样本学习效果极大依赖于关键数据集的实验现象，提出重采样方法提高零样本泛化性能

预训练语言模型因其强大的性能被广泛关注。基于提示符的多任务预训练的零样本学习方法以其极强的性能引起了学术界的广泛关注，但人们对于其泛化能力的来源知之甚少。对于零样本泛化性能的了解不足限制了零样本领域的继续发展。

杨植麟研究组首次表明在少数关键任务上的训练胜过使用所有训练任务，而去除这些关键任务则会严重影响性能（如表格所示）。另一个发现是，这些关键任务大多是问答（QA）任务。这些发现表明对某些任务（如QA）的训练编码蕴含了可用于广泛任务的一般知识。基于以上发现，研究组设计了一种方法，在不观察测试任务的情况下，识别并重采样关键训练任务（如图所示），并提高了零样本泛化性能。ImprovingT0的提出具有重要意义，它引发更多对现有零样本学习泛化能力来源对思考，并进一步推动了零样本领域的发展。

该成果研究论文：Jing Zhou, Zongyu Lin, Yanan Zheng, Jian Li, Zhilin Yang: Not All Tasks Are Born Equal: Understanding Zero-Shot Generalization.

Train Tasks	Met.	Natural Language Inference					Sentence Completion			Co-Reference		WSD.	Avg.
		RTE	CB	ANLI1	ANLI2	ANLI3	COPA	Hella.	Story.	WSC	Wino.	WiC	
All T0 Tasks	Mean	72.53	50.60	30.93	31.96	32.23	82.20	27.16	92.05	62.21	52.00	50.14	53.09
	Med.	74.01	57.14	30.40	31.60	31.75	83.00	27.60	91.77	62.98	52.33	50.00	54.87
Top-8 Only	Mean	73.10	66.55	33.55	32.46	36.34	84.62	30.93	94.51	64.04	53.02	50.52	56.33
	Med.	74.91	71.42	33.10	32.10	36.42	84.50	30.96	94.76	65.38	52.96	50.16	56.97
T0 Tasks w/o Top-8	Mean	60.47	44.17	30.68	32.81	32.87	67.07	26.46	68.81	51.83	51.29	50.92	47.03
	Med.	60.29	44.64	30.80	33.00	33.33	66.83	26.65	72.53	47.12	51.54	50.71	47.04

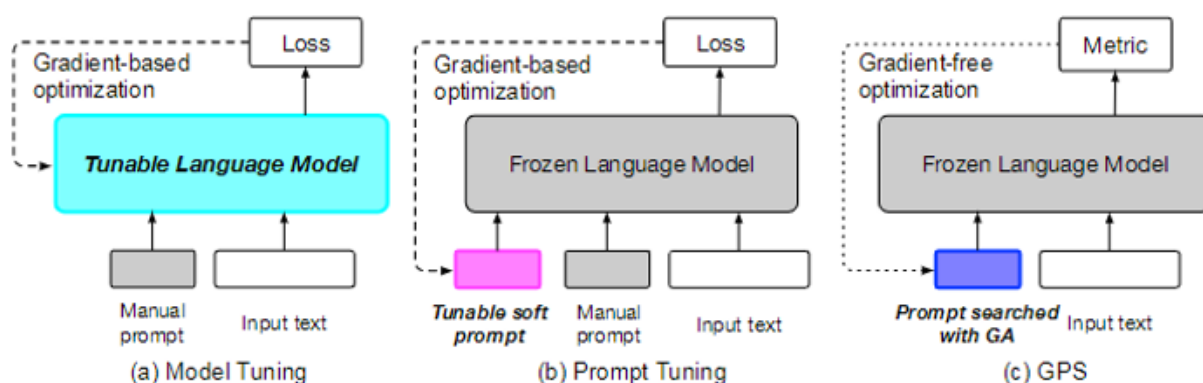


提出基于遗传算法的提示搜索，少样本学习的效果超过人工手写提示以及其他微调的方法，且在效率上有明显的优势

提示(Prompt)是提取预训练语言模型知识的一种高效方式，近年来受到NLP学界的广泛关注。通过人工手写提示(manual prompt)的方法，GPT-3等大规模预训练模型在零样本、少样本上取得了非常好的效果，但是人工手写提示的方法存在着效果差、不同提示之间差距大、人力成本高的问题，给实际下游任务的应用造成了困难。

杨植麟研究组首次提出一种基于遗传算法的提示搜索算法(GPS, Genetic Prompt Search)。对于少样本学习，和人工手写提示、全模型微调(Model tuning)和部分参数微调(Prompt Tuning, Black-Box Tuning)等其他方法相比(如下图所示)，GPS通过自动化地生成和评估不同提示，不仅取得了较好的效果，而且这一方法不需要模型的梯度信息即可进行调优，能够节省10倍的计算资源。GPS提出了一种新的范式，即自动化地构建、评估提示而固定预训练模型的参数，这种方式对大规模预训练模型的应用有积极推广作用。

该成果研究论文已被EMNLP' 22接收：Hanwei Xu, Yujun Chen, Yulun Du, Nan Shao, Yanggang Wang, Haiyu Li, Zhilin Yang: GPS: Genetic Prompt Search for Efficient Few-shot Learning.



Methods	Serving Efficiency	Tunable Parameters	Performance	Computation Cost [†]
Model Tuning	✗	100%	61.73	11.1x
Prompt Tuning	✓	~ 0.01%	58.56	11.1x
Black-Box Tuning	✓	~ 0.001%	57.82	9.3x
In-Context Learning	✗ [‡]	0%	51.28	0x
our GPS	✓	0%	60.12	1.0x

首次提出将NLP任务分解为离散特征的组合：通过特征组合泛化实现零样本学习

零样本学习是NLP研究的一个热点。之前的研究假设通过自然语言提示将NLP任务转化为seq2seq形式并且对语言模型进行多任务训练可以帮助语言模型将学到的知识泛化到其他任务上，这一研究视角推动了很多改进提示学习的工作，包括设计更好的自然语言提示、增加自然语言提示的数量以及提升提示学习的训练效率等等。杨植麟研究组提出了一种研究泛化能力的新视角：组合泛化，即可以用一组离散特征的组合来代表多个不同的任务，再通过多任务学习来训练这些离散特征，通过特征的组合泛化来实现强大的零样本学习能力。

杨植麟研究组首次提出一种通过多任务训练来学习离散的任务特征表示的方法（CTR, Compositional Task Representation）。这一方法通过多任务学习来得到一个离散的任务特征集合。在推理阶段通过模型对新任务的输入数据打出的伪标签来找到针对该任务的特征组合，最后利用该特征组合实现在新任务上的泛化（如图1所示）。相比较于之前的零样本学习方法（例如T0），CTR在众多零样本学习任务上表现出卓越的性能（如图2所示），并且拥有一定程度上的可解释性和可控性。作为这一领域的一项突破性进展，CTR的提出具有重要意义，它引发更多对零样本学习本质的思考，并进一步推动零样本学习的发展。

该成果研究论文：Nan Shao, Zefan Cai, Hanwei Xu, Chonghua Liao, Yanan Zheng, Zhilin Yang: Compositional Task Representation for Large Language Models.

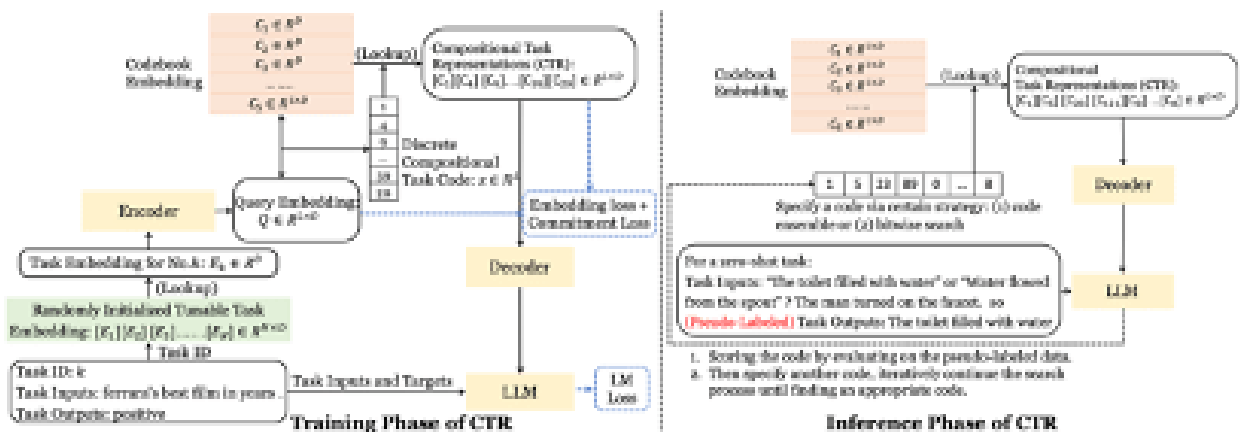


Figure 2: An overview of the architecture of our proposed CTR . The left part illustrates the training phase, while the right part shows how CTR works during the inference phase.

Method	Natural Language Inference					Sentence Completion			Co-reference		WSD	Avg.
	RTE	CB	ANLI1	ANLI2	ANLI3	COPA	Hella.	Story.	WSC	Wino.	WiC	
Zero-Label Setting (unlabeled data of each test task)												
T0-Large	72.67	56.55	32.77	32.15	34.38	85.36	27.18	93.04	63.94	54.35	50.33	54.79
Self-Training	73.57	76.14	34.42	32.90	37.44	87.45	30.33	94.54	57.08	56.56	50.75	57.38
Manual-Code	75.19	56.89	33.12	32.49	33.48	75.76	30.84	93.10	61.16	54.10	51.45	54.33
ZPS	79.06	67.86	31.20	31.10	34.25	88.00	29.16	93.43	65.38	53.43	49.84	56.61
Our CTR	80.51	87.50	33.40	34.40	33.80	92.00	27.50	90.10	56.58	49.40	62.50	58.88
Few-Shot Setting (32 labeled data of each test task)												
Model Tuning, 16/16	75.31	80.95	35.73	31.31	35.93	82.05	41.86	92.04	55.96	56.74	52.15	58.18
i Model Tuning, 32/0	79.20	77.50	36.78	30.73	35.98	82.30	42.24	93.16	54.35	59.56	54.18	58.73
Prompt Tuning, 16/16	77.08	76.90	31.89	31.86	35.53	81.70	31.18	94.10	62.88	55.42	51.22	57.25
Prompt Tuning, 32/0	77.51	73.21	34.17	33.43	34.34	81.82	26.63	92.46	62.12	54.34	50.30	56.39
GPS	77.68	79.64	32.71	31.49	37.56	81.08	28.11	93.40	64.23	52.72	52.52	57.38
GRIPS	71.56	70.89	32.14	32.26	34.77	77.56	26.44	93.40	62.12	52.96	52.12	55.11
BBT	71.19	57.26	33.79	32.00	35.30	76.49	28.95	93.11	62.12	53.40	52.93	54.23
Our CTR	80.51	83.93	34.40	34.20	36.60	89.00	35.07	91.70	68.18	55.00	58.62	60.66

Table 1: Main results of CTR and baselines on 11 test tasks under the zero-label setting and the few-shot setting. “16/16” denotes we use 16 examples for finetuning and 16 examples for model selection. “32/0” denotes we use all labeled data for finetuning and directly evaluate the checkpoint at the last training step. The zero-label setting allows using unlabeled data of the test task while the few-shot setting uses 32 labeled data of the test task. All methods share a similar model size (i.e., 770M).

第一个通过系统性的实验分析大规模语言模型生产重复文本的原因

尽管大规模神经语言模型，如 GPT2 和 BART，在各种文本生成任务上取得了令人瞩目的结果。但是，在基于贪心的解码算法下，它们往往会陷入重复的句子循环。这种现象是违反直觉的，因为在训练语料库中很少有连续的句子级重复（例如，在 Wikitext-103 中句子级别的重复只有为 0.02%）。已经有众多研究学者注意到了这一个现象，但是关于为什么这些模型会产生这些反常的现象的原因还没有工作进行过深入的研究。该文章旨在探究语言模型生产重复文本的本质原因，弥补该领域的空白。

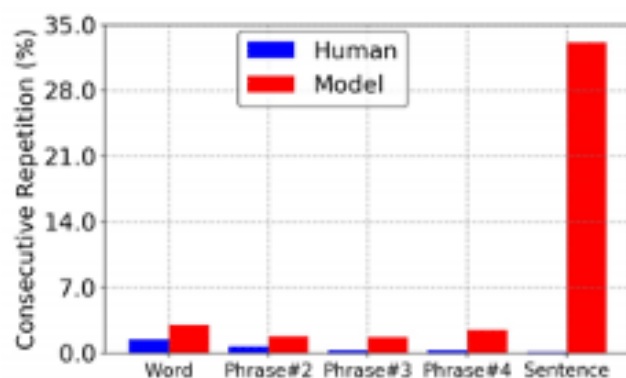
通过李建研究组的定量实验，发现 1) 语言模型有很强的倾向去重复前面的句子；2) 句子级重复具有自我强化效应：一个句子在上下文中重复的次数越多，继续生成那个句子的概率就越高；3) 初始概率较高的句子通常具有较强的自我强化效果。该研究组进一步提出了一种简单有效的训练方法DITTO，让模型学习惩罚伪重复数据中句子级重复的概率。实验表明，DITTO 不仅在不牺牲困惑度的情况下减轻了重复问题，而且还实现了更好的生成质量。关于开放式文本生成和文本摘要的大量实验证明了该方法的通用性和有效性。

该成果研究论文Jin Xu, Xiaojiang Liu, Jianhao Yan, Deng Cai, Huayang Li, Jian Li. “Learning to Break the Loop: Analyzing and Mitigating Repetitions for Neural Text Generation.” Advances in Neural Information Processing Systems (NeurIPS), 2022.

Prefix: The rim is slightly raised about the surrounding surface and it has an outer rampart that has been only lightly impacted . No significant craters intersect the rim , and it is sloped about 1 @. @ 5 ° toward the direction 50 – 90 ° from the Earth .

Greedy Decoding:

The age of the crater is about 3 @. @ 6 billion years and it has been in the proximity of the south lunar pole for at least 10 @. @ 000 years . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands . The South Crater is located on the southern edge of the northern highlands ...



五、区块链

主要完成人：房智轩研究组

支付通道网络中的实时递归寻路算法：基于竞价机制的设计

支付通道网络（Payment Channel Network, PCN）是一种区块链链下扩容的技术，该技术使得区块链的用户可以在链下完成交易，而不需要将每一笔交易都上链，这极大地提高了区块链处理交易的能力。当交易双方并没有支付通道直接相连接时，支付通道网络将路由寻路并通过中间节点来完成该笔交易。设计一个高效的路由寻路算法是提高支付通道网络性能的关键。

房智轩研究组提出了基于竞价机制的支付通道网络实时递归寻路算法（RTRR）。与传统的源节点寻路方案不同，RTRR算法通过节点竞价的方式，把支付通道网络中的路由任务层层外包，并实时递归寻路。该算法能够在较短时间内完成支付通道网络中的交易路由，同时可以较好地保护用户隐私，在动态的场景下相比现有算法有较明显的性能优势。此外，该研究还详尽地分析了RTRR算法中的竞价机制，推导了纳什均衡下的竞价策略，分析了RTRR的性能。理论分析和实验结果表明RTRR算法在交易等待时间，隐私保护，交易成功率等方面有明显优势。

该成果研究论文：Jiayuan Liu, Canhui Chen, Lulu Zhou and Zhixuan Fang. “Real-Time Recursive Routing in Payment Channel Network: A Bidding-based Design.” Proceedings of the 20th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks. (WiOpt). 2022.

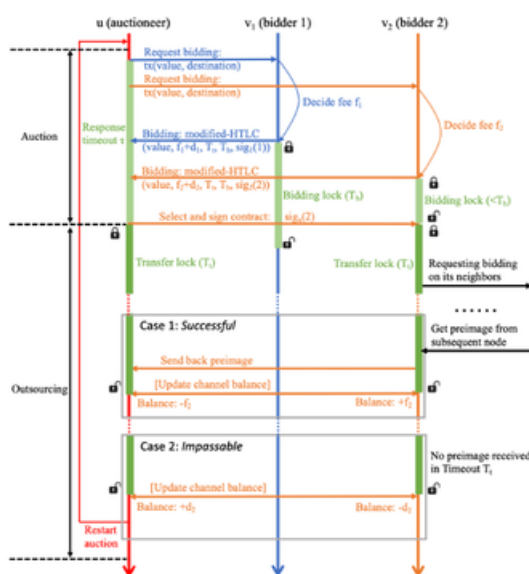


Fig. 1. Flow chart of RTRR.

六、计算生物学

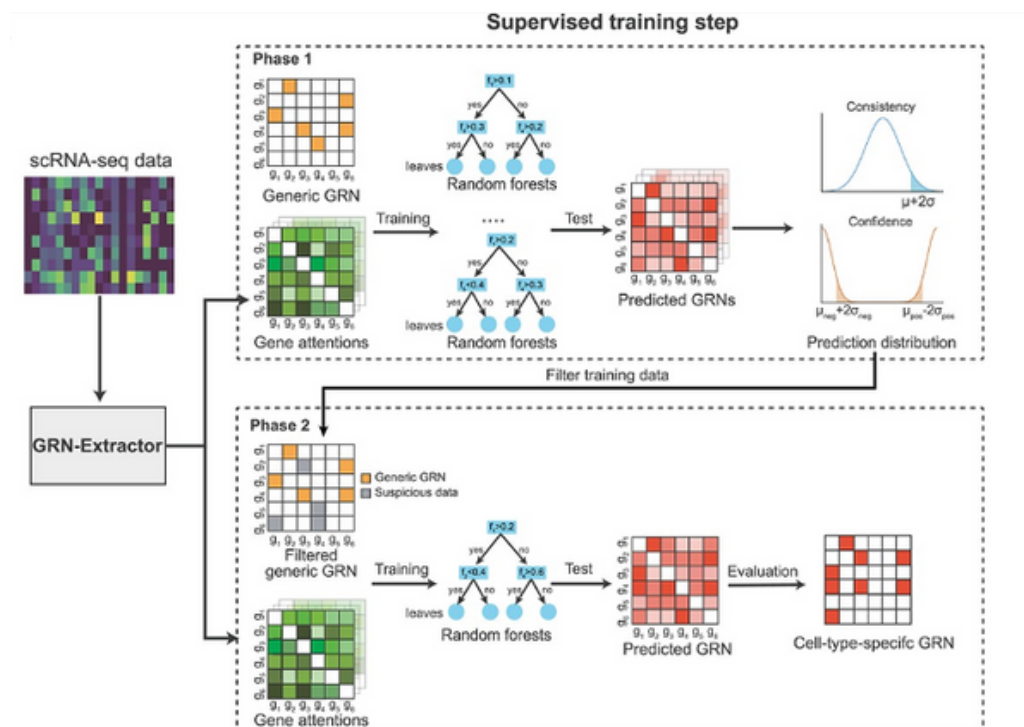
主要完成人：曾坚阳研究组

单细胞基因调控网络预测框架GRN-Transformer

ScRNA-seq作为单细胞组学中至关重要的技术，在靶点发现中起到重要作用，而单细胞精度下的基因调控网络建模对于靶点发现尤其重要。在这项工作中，曾坚阳研究组发现使用通用基因调控网络(从bulk测序实验或文献中获得)能提高特定细胞类型的基因调控网络预测性能，并提出了一种两步法的弱监督基因调控网络预测框架GRN-Transformer，通过大量实验证实了通用基因调控网络可以改进特定细胞类型的基因调控网络预测性能。此外，研究组还发现，在各种实验环境下，GRN-Transformer皆优于其他有监督和无监督的基因调控网络预测方法。

基于上述模型，曾坚阳研究团队对阿尔茨海默病患者内嗅皮质细胞进行了深入研究，发现了阿兹海默病致病基因APOE的上调控因子，这为疾病新靶点的发现提供了研究基础。

该成果研究论文: Hantao Shu, Fan Ding, Jingtian Zhou, Yexiang Xue, Dan Zhao, Jianyang Zeng, Jianzhu Ma, Boosting single-cell gene regulatory network reconstruction via bulk-cell transcriptomic data, Briefings in Bioinformatics, Volume 23, Issue 5, September 2022, bbac389.

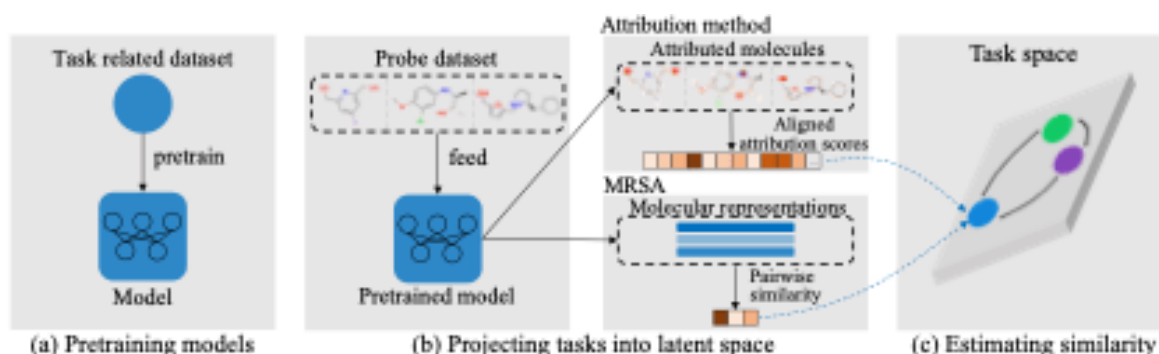


任务相似性增强的迁移学习策略用于提高小分子性质预测

准确预测和理解小分子的性质, 例如理化性质以及生物活性, 在药物发现过程中至关重要。由于大多数的小分子数据集存在数据量匮乏的问题, 妨碍了以数据为驱动模型, 特别是深度学习模型在小分子性质预测任务中的应用。为了提高深度学习模型在小数据集上的预测效果, 如何最大化地利用已有的数据是一个重要的问题。

为了解决这个问题, 曾坚阳研究组开发了一个估计小分子性质预测任务间相似度的方法, 并利用估计的相似度提高了深度学习模型在小数据集上的预测性能。该方法从预训练的深度学习模型中提取并向量化小分子性质预测任务相关的知识, 从而将任务映射到一个隐层空间, 最后在这个隐层空间中衡量任务间的相似度。利用该方法估计的任务间的相似度可以指导迁移学习中源任务的选择, 从而实现更高效地利用已有的数据集。实验结果证明, 给定一个目标任务, 通过选择相似度较高的任务作为源任务可以有效地提升通过迁移学习训练的深度学习模型对目标任务的预测效果。另外, 该方法中的归因方法可以用来可视化小分子中重要的官能团, 为估计的任务间的相似度提供了一定的可解释性。这个特性能够帮助更加深入地理解小分子间的关系以及性质内在的原理, 从而为药物研发做出贡献。

该成果研究论文: Han Li, Xinyi Zhao, Shuya Li, Fangping Wan, Shao Li, Dan Zhao and Jianyang Zeng. “Improving molecular property prediction through a task similarity enhanced transfer learning strategy”, iScience, 2022 Sep 30;25(10):105231.

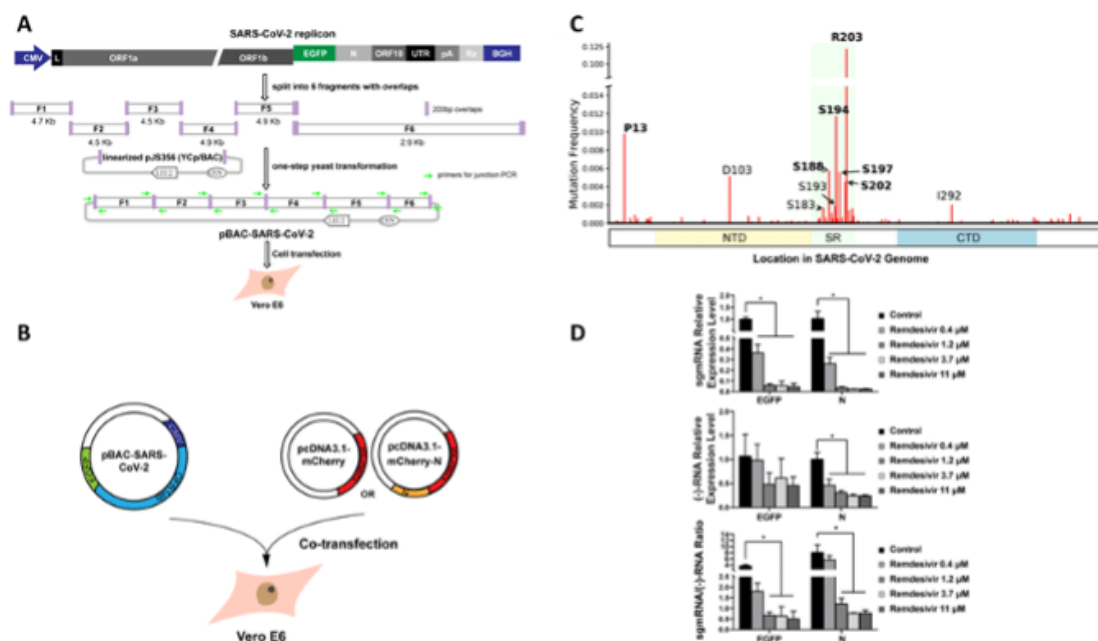


非感染性的SARS-CoV-2复制子研究系统

新冠疫情的爆发和蔓延，对全世界人民的健康带来了巨大威胁。由于新冠病毒传播力强且变异较快，加之缺乏有效的治疗措施，活病毒相关的研究必需在生物安全防护三级实验室（BSL-3）才能开展，而国内BSL-3实验室资源相对紧缺，这为研究新冠病毒的致病机制和寻找相关抗病毒药物提出了严峻的挑战。面对上述问题，国内外科学家纷纷开始研究不受限于BSL-3条件的病毒模拟系统，以期在BSL-2实验条件下也可以广泛开展新冠病毒相关研究，深入理解其致病机制，加速特效药物的研发，从而阻止疾病的全球蔓延。

曾坚阳研究团队与合作者通过将SARS-CoV-2的基因组进行合理拆分并重新克隆至细菌人工染色体的载体中，从而构建了一个非感染性的病毒复制子系统。利用该复制子系统，研究团队证明了新冠病毒的N蛋白能促进从负链sgRNAs到正链sgRNAs的转化效率，N蛋白R203K突变对病毒转录过程的影响最大。此外，该系统对瑞德西韦和氯喹这两种已知抗病毒药物处理下的病毒增殖能力具有明显的效应活性。因此，研究组开发的该复制子系统无活病毒颗粒包装能力，使用安全、方便，且组分表达稳定，为探索SARS-CoV-2中RNA合成等生理机制和高通量筛选抗病毒药物提供了一个有力工具。

该成果研究论文：Xiaolong Feng, Xiaofan Zhang, Shuangying Jiang, Yuanwei Tang, Chao Cheng, Parthasarathy Abinand Krishna, Xiaoting Wang, Junbiao Dai, Jianyang Zeng, Tian Xia, and Dan Zhao “A DNA-based non-infectious replicon system to study SARS-CoV-2 RNA synthesis.” *Computational and Structural Biotechnology Journal*, 2022, 20: 5193-5202.



七、计算机视觉

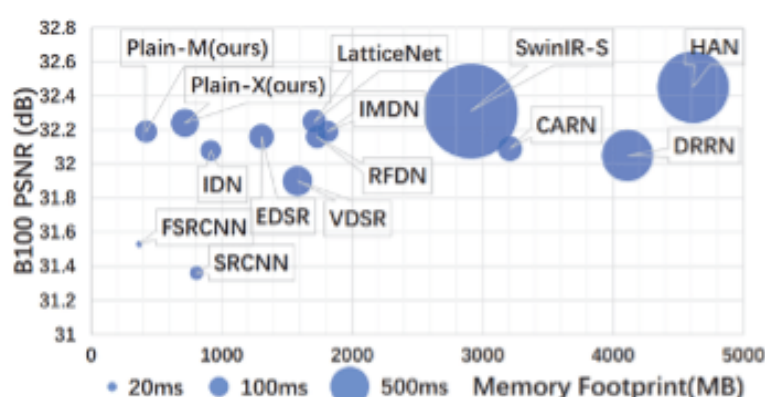
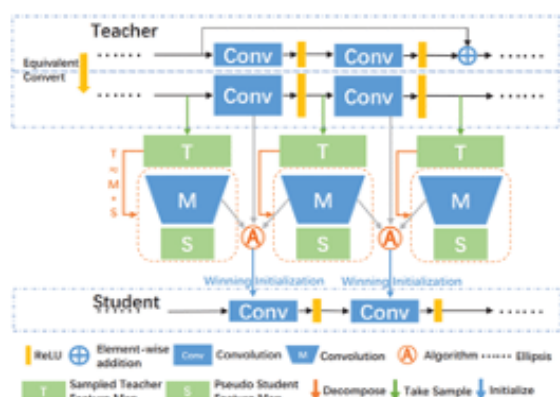
主要完成人：马恺声研究组、弋力研究组

首次将多分支超分辨率模型在转化为无分支朴素模型并获得相同性能和更低显存需求

传统的超分网络结构通常会使用大量的跨层连接以提升有限算力下的性能，这给模型推理时带来了大量的显存开销，限制了很多超分方法在手机等边缘设备上的使用。该研究旨在从多分枝的老师模型中为无分枝的朴素学生模型（只包含卷积与ReLU）计算出一个强力的初始化权重（称之为winning initialization），使得直接训练朴素学生网络便可以获得与多分枝模型相当的超分性能。

方法上，该研究组先将老师模型转换为一个等效的大尺寸朴素模型，并使用类似于低秩分解的算法计算出学生模型的初始化权重。其中，学生网络的各层宽度可以人为指定为等宽（Plain-M）以严格控制显存需求，也可以由算法计算自适应宽度（Plain-X）以兼顾推理速度与准确率。实验表明，该研究组所提出的方法能够训练出的学术网络在准确度和速度与其他轻量化超分模型相当的情况下，其显存需求远低于其他方法（2x~10x）。

该成果研究论文：Kailu Wu, Chung-Kuei Lee, and Kaisheng Ma. “MemSR: Training Memory-efficient Lightweight Model for Image Super-Resolution.” ICML, 2022.



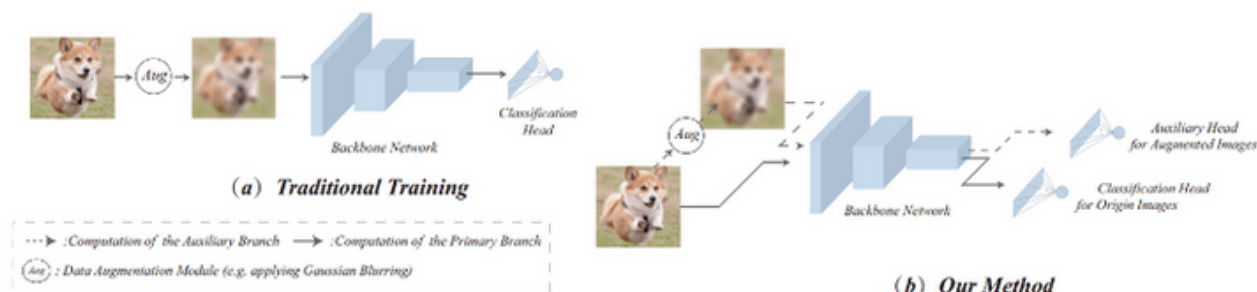
基于多任务学习的数据增强方式

在深度学习中，数据增强算法通过对输入的数据进行各类不同的变换，以此扩充数据集的大小，提高神经网络模型的泛化性。一般来说，当数据增强的力度较小时，数据集的多样性增长较小。当数据增强的力度较大时，数据增强带来的正则化效果可能过大，进而损伤模型的拟合能力。因此，如何找到最合适的数据增强力度是深度学习中亟待解决的问题。

近年来，自动化数据增强方法引起了学术界的广泛关注。该类方法首先规定大量待选择的基础数据增强操作，然后使用强化学习、演化学习、对抗学习等方式，搜索对于给定任务和数据集中对适宜的数据增强策略。最终，将该策略用于训练中的数据增强。尽管这类方法取得了较好的性能，然而，使用强化学习等算法搜索最优策略的过程极其复杂且耗时。例如，AutoAug算法在ImageNet数据集上需要使用15000个GPU小时进行搜索，这严重限制了该算法在实际应用中的使用。

为解决该问题，马恺声研究组提出了一种基于多任务学习的数据增强方式。该研究组发现，传统数据增强训练中影响模型性能的主要原因是在神经网络最后一层中有截然不同的梯度，这导致了优化的困难。为解决这个问题，马恺声研究组提出用多任务学习的方式去建模数据增强任务，将采用数据增强和未采用数据增强作为多任务学习中的两个分支，最终在不需要任何数据增强策略搜索的情况下达到了超越传统需要搜索的数据增强算法的效果。

该成果研究论文：Linfeng Zhang, Kaisheng Ma. “A Good Data Augmentation Policy Is Not All You Need: A Multi-Task Learning Perspective.” IEEE TCSVT, 2022.



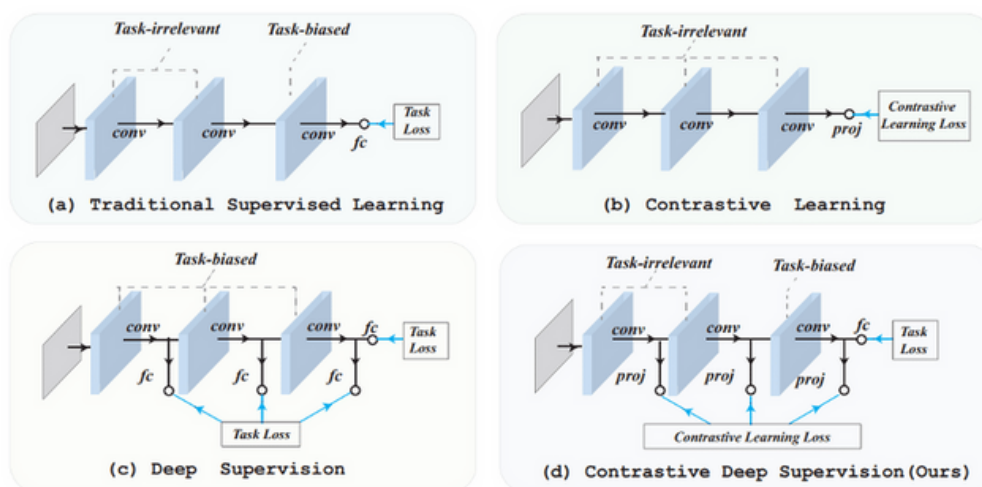
基于对比学习的深度监督算法

近年来，随着大型数据集和高性能计算设备的出现，深度神经网络在多个领域取得重大突破。然而，随着神经网络深度的增长，神经网络的训练优化过程变得困难，出现了例如梯度消失等诸多问题。为解决该问题，深度监督算法通过在神经网络的不同层增加额外的分类器，直接训练神经网络的中间层，提升了神经网络的训练效果。

一般来说，神经网络的不同层学习的知识是截然不同的，中间层一般应该学习低层次的集合信息。然而，传统的深度监督算法往往让中间层与最终层神经网络共用相同的分类任务，这导致神经网络的中间层会偏向于学习与任务相关的特征。这个矛盾导致传统的深度监督训练得到的特征缺乏迁移性，即虽然在训练所用的数据集上表现良好，但是在各种不同的下游任务上性能不佳。这一问题限制了深度监督算法的使用。

近年来，通过构造基于数据增强的对比学习方法在计算机视觉任务中广泛发展。通过将同一图像的数据增强作为正样本对，将不同图像的数据增强作为负样本对，通过降低正样本对的距离并最大化负样本对的距离，使得神经网络模型学到与任务无关的更具有泛化性的特征。观测到这一现象，马恺声研究组提出一种基于对比学习的深度监督算法，通过使用基于数据增强的对比学习方法训练神经网络的中间层，以此使得中间层在获得训练梯度的情况下学习到任务不相关的特征，显著提升深度监督算法特征的泛化能力，在大规模图像分类，细粒度图像分类、视频分类，目标检测等多个任务上获得显著提升。

该成果研究论文: Linfeng Zhang, Xin Chen, Junbo Zhang, Runpei Dong, and Kaisheng Ma. “Contrastive Deep Supervision.” ECCV, 2022. (Oral)

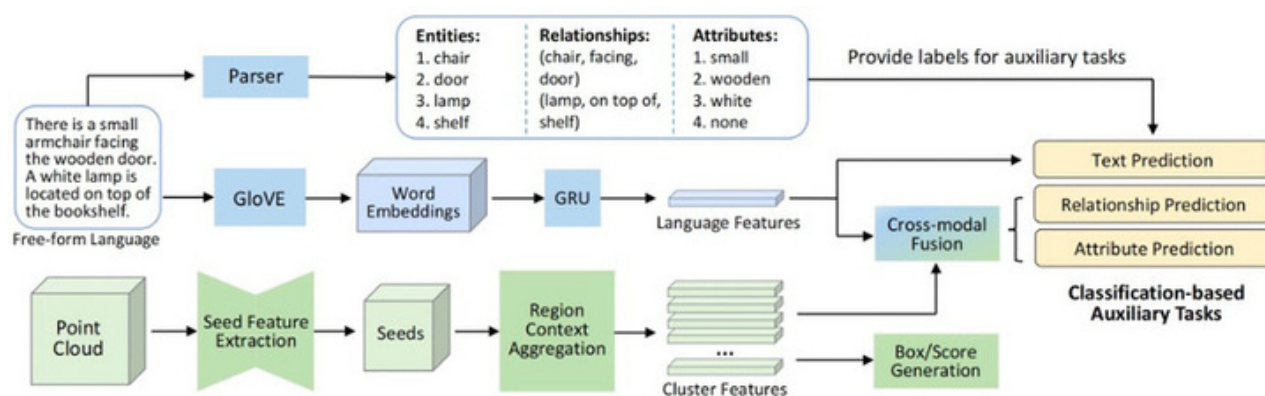


自然语言辅助的室内场景三维表征学习

场景中三维物体的表征学习是室内场景理解的关键步骤。对物体的属性（如颜色、形状）以及物体之间的空间位置关系信息的提取，对于室内场景中物体的定位和分类至关重要。然而，当前以目标检测、实例分割为优化目标的端到端训练方式难以确保这些关键信息在三维物体表征中的充分编码。

针对这一问题，弋力研究组首次提出利用自然语言文本来辅助三维室内场景理解，通过分析和筛选描述场景的大量自然语言文本中的关键信息，构建文本预测、物体属性预测、空间位置关系预测三种辅助任务，来强化三维表征编码物体属性以及环境信息的能力。此方法能够广泛地应用于现有的三维目标检测、实例分割算法，通过弥补物体表征中信息的缺失来提升其性能，且能够显著提升标注缺乏条件下的训练效果。此外，三维物体表征中编码的多模态信息有助于完成视觉-语言多模态任务，如视觉语言定位（visual grounding）、标注（visual captioning），对于室内场景理解有广泛的应用价值。

该成果研究论文：Junbo Zhang, Guofan Fan, Guanghan Wang, Zhengyuan Su, Kaisheng Ma, Li Yi. “Language-Assisted 3D Feature Learning for Semantic Scene Understanding” 将发表于AAAI 2023。

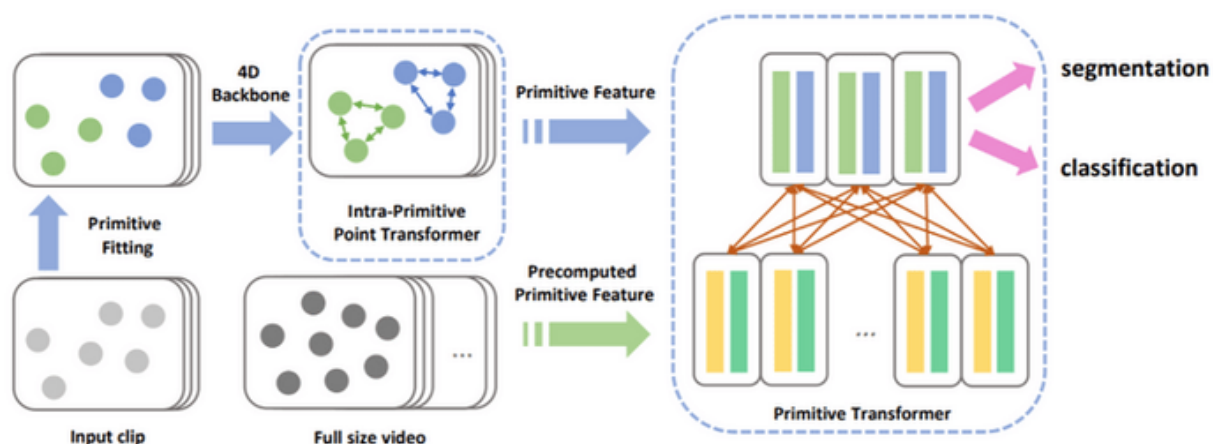


可用于长期4D点云视频理解的Transformer

点云视频在机器人和VR/AR系统中无处不在，这是一种体现动态真实3D世界的形式。不同于2D图片和3D静态点云，点云视频记录3D物理空间中的运动，在理解环境变化和与世界的交互方面发挥着关键作用。因此，智能机器人需要精确处理这种形式的数据，以更好地理解现实世界，适应环境变化并与之交互。但由于相机运动，场景变化，遮挡变化，和采样模式不同，不同帧之间的点是非结构化和不一致的，这使得不同帧之间很难有效地整合有效信息。同时，4D数据的复杂性易导致内存和计算爆炸。随着视频长度的增加，这两个挑战都急剧增加。

弋力研究组利用几何基元设计了一个高效且有效的4D骨干网络，名为 Point Primitive Transformer (PPTr)。由于引入几何基元可以在空间自然形成场景-几何基元-点的层次结构，PPTr 是一个可以在两个层次上计算的多层Transformer。在点的层次上，PPTr 通过一个Point Transformer提取短期时空特征。Primitive用于限制Point Transformer中注意力机制的空间范围。这种局部几何感不仅有利于Transformer的优化，而且对于提取时间稳定的几何特征也非常有效。在Primitive的层级上，PPTr 通过Primitive Transformer提取长期时空特征。通过Primitive Transformer，网络可以更好地将来自不同帧的Primitive关联起来，更有效地整合长期上下文到感兴趣的点云帧中。

该成果研究论文：Wen, Hao, Yunze Liu, Jingwei Huang, Bo Duan, and Li Yi. "Point Primitive Transformer for Long-Term 4D Point Cloud Video Understanding." In European Conference on Computer Vision, pp. 19-35. Springer, Cham, 2022.



八、机器人学

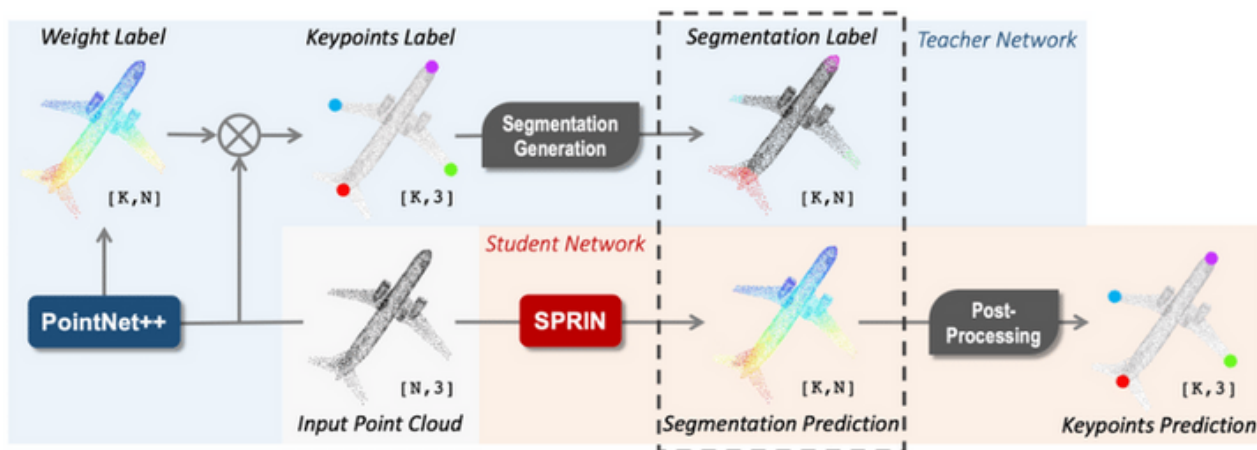
主要完成人：许华哲研究组

用于可泛化机器人操作的三维点云关键点提取

真正智能的机器人应该拥有将掌握的操作技能泛化至开放世界的能力。面向这一宏大的目标，在机器人、具身智能等领域，一个现阶段的研究热点是：如何实现具有类内泛化能力的机器人操作。该问题的核心挑战在于，需要提出一种可类内泛化的物体表征方法。

针对这一目标，许华哲研究组提出了USEEK，一种无监督的三维点云关键点提取方法。该方法提取出的关键点具有类内对齐的特点、并且享有SE(3)等变换的保证，因此特别适用于需要类内泛化的机器人操作任务。相较于其他形式的用于机器人操作的物体表征，USEEK在泛化性、鲁棒性、高效性等多个维度均取得了较为显著的优势。

该成果研究论文预印本：Zhengrong Xue, Zhecheng Yuan, Jiashun Wang, Xueqian Wang, Yang Gao, Huazhe Xu. (2022). USEEK: Unsupervised SE (3)-Equivariant 3D Keypoints for Generalizable Manipulation. arXiv preprint arXiv:2209.13864.

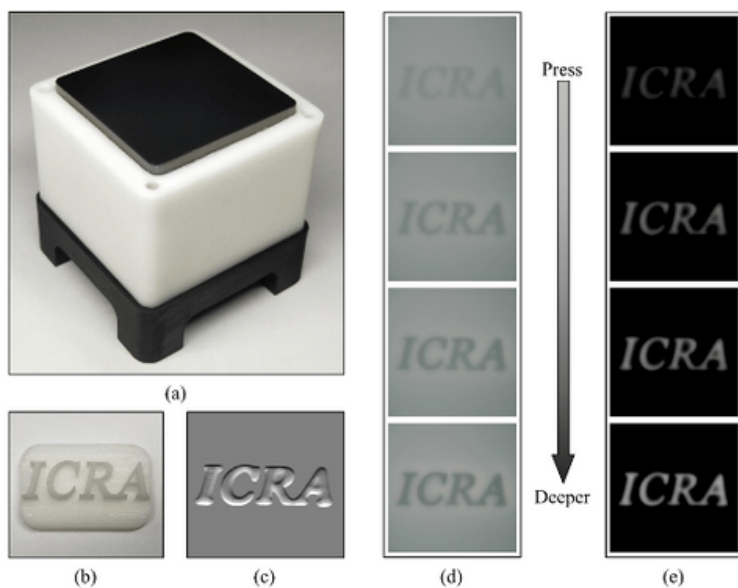


用于测量高分辨率接触几何的视触觉传感器

触觉传感器为机器人提供了接触物体丰富的物理信息。基于视觉的触觉传感器因为具有测量高分辨率接触几何的能力，为机器人研究提供了新的感知模态。然而，目前主流的视触觉传感器高度依赖于内部光源的光照传播路径，使得其制造与装配流程复杂，并大大降低了扩展其接触表面至曲面的能力。

许华哲研究组将半透明硅胶作为触觉传感器的接触表面，利用其光反射的物理性质测量硅胶的按压深度，从而通过摄像头重建接触物体的三维几何。该新型视触觉传感器从根本上突破了现有视触觉传感器高度依赖光照条件的限制，同时它还具备低成本，易装配，以及只需要一张图片即可标定的优良性质。

该成果研究论文：Changyi Lin, Ziqi Lin, Shaoxiong Wang, and Huazhe Xu. “DTact: A Vision-Based Tactile Sensor that Measures High-Resolution 3D Geometry Directly from Darkness.” arXiv preprint arXiv:2209.13916 2022.

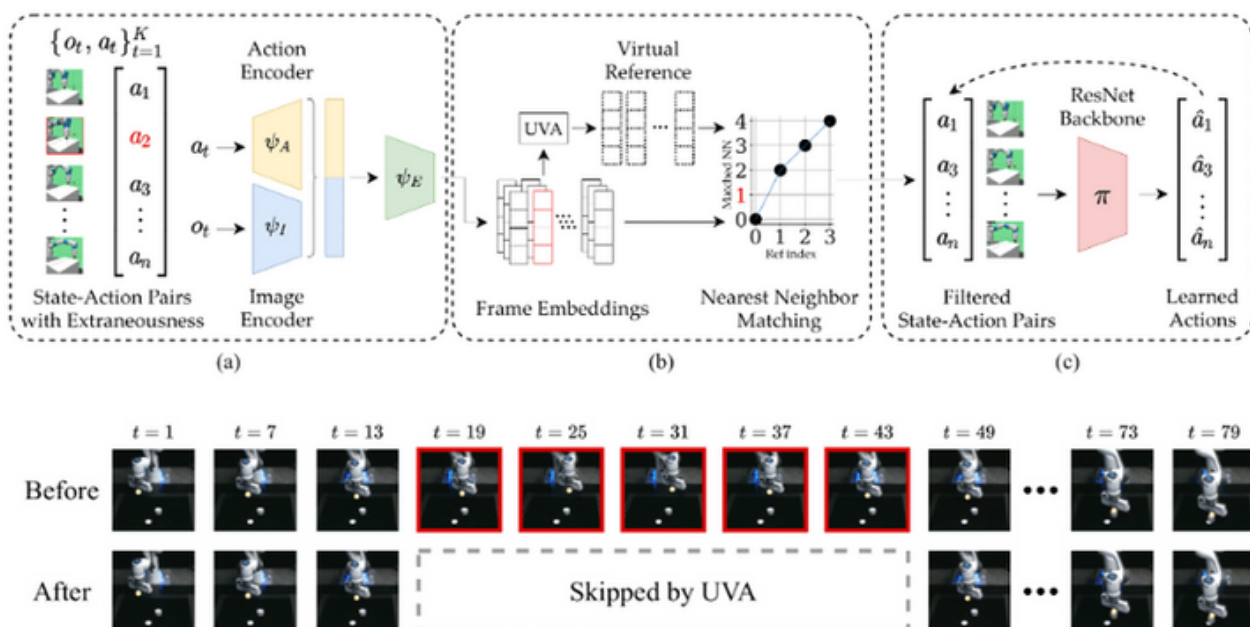


冗余动作扰动下的模仿学习

在视觉模仿学习过程中，智能体通过模仿由专家人类或者专家智能体录制的演示进行学习，而该演示的质量则会对模仿学习的效果有较大影响。在专家演示当中，专家经常会做出一些冗余的动作，这些冗余动作与演示任务无关但并非随机噪声，无法被已有方法有效检测到，智能体在模仿时会受到负面影响。

为解决此问题，许华哲研究组提出了EIL，一种冗余动作扰动下的模仿学习方法。该方法首先使用时间循环一致性的方法对视频编码器进行训练，得到含观测、动作、时间等语义信息视频帧表示后，使用一种无监督方法找出视频中的冗余部分。由于冗余动作在视频中占用时间不会超过50%且出现时间不规则，因此在将数据集所有视频沿时间维度对齐后，可查看固定时刻下所有视频的帧表示，筛选出少部分视频的冗余动作，并将该帧从视频中切除。使用经过投票筛选的演示数据集重新进行模仿学习的训练，大幅提升学习效果。

该项目的研究论文已被 NeurIPS 2021 Workshop on Deployable Decision Making 接受。预印本：Zheng, R. C., Hu, K., Yuan, Z., Chen, B., & Xu, H. (2022). Extraneousness-Aware Imitation Learning (arXiv:2210.01379). arXiv.



基于人类动作的场景生成

基于人体动作姿态，估计场景中家具摆放位置，从而使得人体模型在其中的动作合理、可行。许华哲研究组开发的该模型主要解决了领域中，数据集昂贵且稀少的问题，通过较为廉价的人体位姿数据生成人体与物体和场景交互的数据。这样的数据对于机器人领域中对于场景的理解和猜测亦有价值 and 意义。

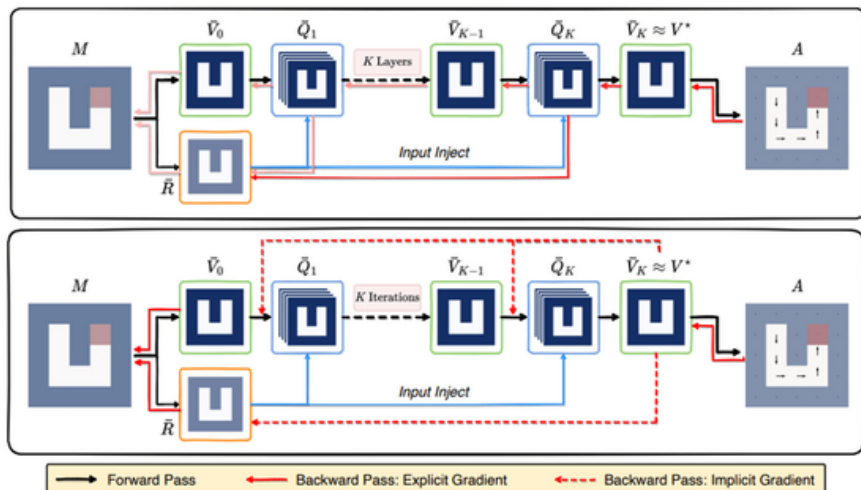
该成果研究论文：Yixing Wang*, Sifan Ye*, Jiaman Li, Dennis Lee, Karen Liu, Huazhe Xu+, Jiajun Wu+. Scene Synthesis from Human Motion, Siggraph Asia, 2022.



可微分隐式规划控制算法

基于值迭代网络的方法往往面临无法稳定规模化训练的问题，许华哲研究组提出一种结合深度平衡网络的方法，并对该系列方法的稳定性进行提升。

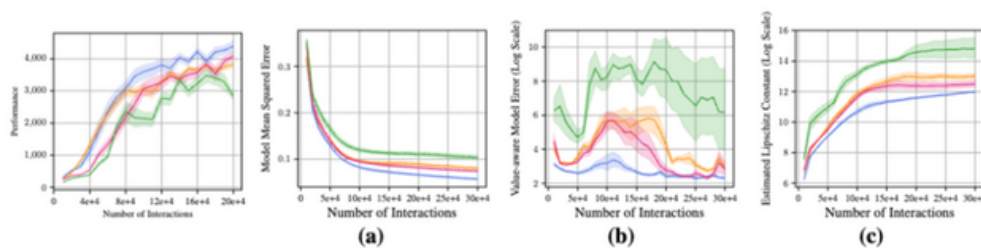
该成果研究论文：Linfeng Zhao, Huazhe Xu, Lawson L.S. Wong. Scaling up and Stabilizing Differentiable Planning with Implicit Differentiation, NeurIPS Deep RL Workshop.



强化学习中的动力学模型合奏问题

在基于模型的强化学习算法中，动力学模型合奏(model ensemble)是一个常用且有效的算法。许华哲研究组深入研究了模型合奏的本质，并发现模型合奏中的主要性能提升来自于随机性带来的连续性而不是泛化性能等普遍认同的观点。

该成果研究论文：Ruijie Zheng*, Xiyao Wang*, Huazhe Xu, Furong Huang. Is Model Ensemble Necessary? Model-based RL via a Single Model with Lipschitz Regularized Value Function, NeurIPS Deep RL Workshop (spotlight).



九、AI基础理论

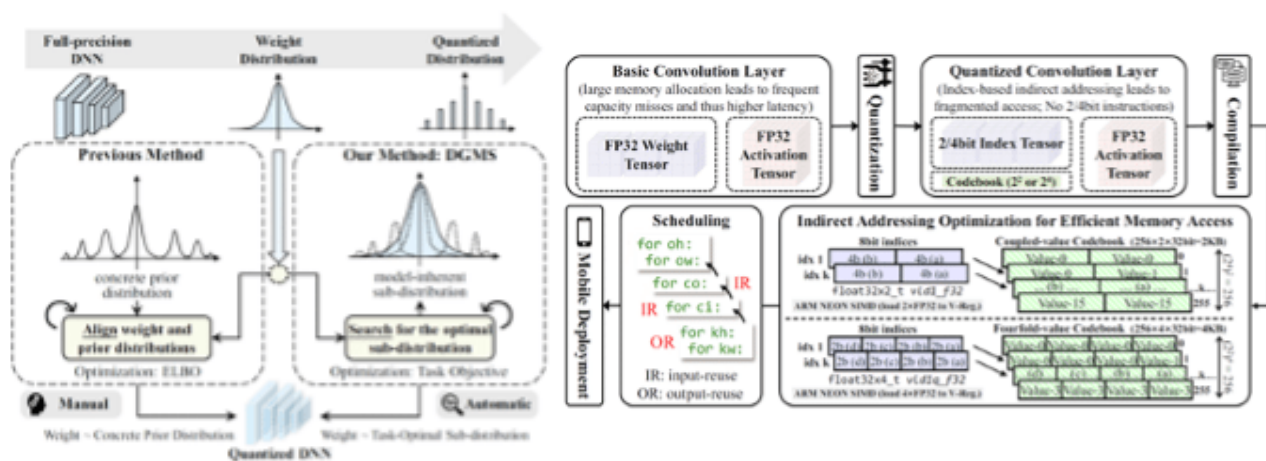
主要完成人：马恺声研究组、张景昭研究组、徐葳研究组

寻找量化神经网络的最优低比特子分布

量化神经网络通常需要更小的内存占用和更低的计算复杂度，这对于高效的边缘设备部署至关重要。然而，神经网络量化不可避免地会导致网络分布与原始网络的分布的巨大差异，这通常会降低性能。为了解决这个问题，研究学者已经做出了巨大的努力，但大多数现有方法都缺乏统计考虑，并且依赖于多种复杂且次优的人工参数配置。

马恺声研究组首次提出并探索了一种自适应映射量化方法来学习模型中固有的最优潜在子分布，并用具体的高斯混合 (Concrete GM) 进行平滑逼近。具体的，网络权重的预测符合混合高斯模型近似的子分布，该子分布随着直接任务目标优化指导的协同调整模式中的权重更新而发展。他们在各种现代架构上进行的图像分类和对象检测的充分实验和分析证明了该方法的有效性、泛化性和可迁移性。此外，他们还设计了一个移动CPU的高效部署流程，在八核ARM CPU上实现高达7.46倍的推理加速。

该成果研究论文：Runpei Dong, Zhanhong Tan, Mengdi Wu, Linfeng Zhang, and Kaisheng Ma. “Finding the Task-Optimal Low-Bit Sub-Distribution in Deep Neural Networks.” ICML, 2022.



支持网内计算的远程过程调用

近年来可编程网络设备的发展推动了网内计算在高性能计算领域的应用。通过片上编程，网络设备可以按照用户定义的程序来处理数据包，因而能够将一部分应用卸载到网络设备上，实现应用加速。网内计算在数据挖掘、分布式机器学习、网络监控、分布式共识等领域的应用已经成为高性能网络方向的研究热点。

然而，现有的网内计算编程对普通应用程序开发人员并不友好。开发者需要处理繁琐的网络工程细节，如流量控制、数据包组织、了解芯片特定的编程语言和 ASIC 架构，因而限制了这一技术的进一步推广。

为了解决这一难题，徐葳研究组设计了一个支持网内计算的通用RPC 系统：NetRPC。NetRPC为软件开发人员提供了一组基于RPC的轻量级接口，通过传统的RPC 编程模型来描述网内计算应用程序。同时，在数据平面上NetRPC提供了一套通用的网内计算实现以及优化技术，包括协议设计、流水线设计、内存管理和计算回退等，以保证在同时支持不同的网内计算应用时，共享数据平面能够带来足够的性能优化。NetRPC简化了网内计算的应用开发，在可编程性和通用性上取得了平衡，使得应用开发者在不甚了解网内编程的前提下也能够享受到网内计算带来的性能提升。

该成果研究论文：Bohan Zhao, Wei Xu. NetRPC: Enabling In-Network Computation in Remote Procedure Calls[C]//20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23). 2023.

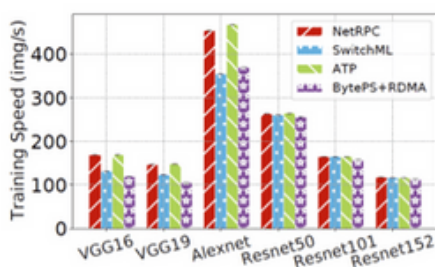


Figure 6: Deep Learning Training Speed

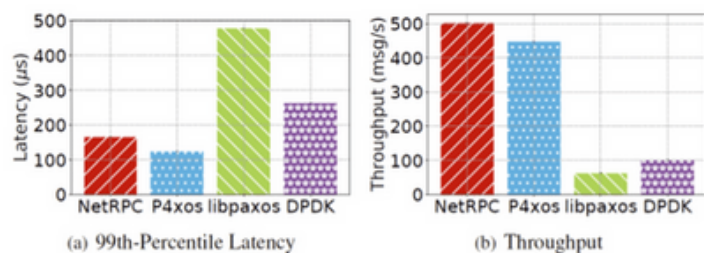


Figure 7: End-to-end Performance of Paxos Systems.

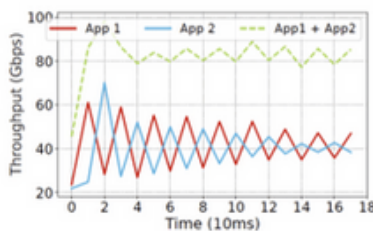


Figure 8: Congestion Control: Fairness

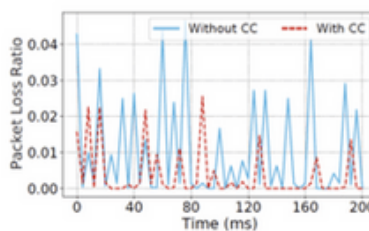


Figure 9: Congestion Control: Packet Loss

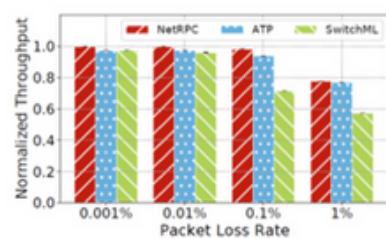


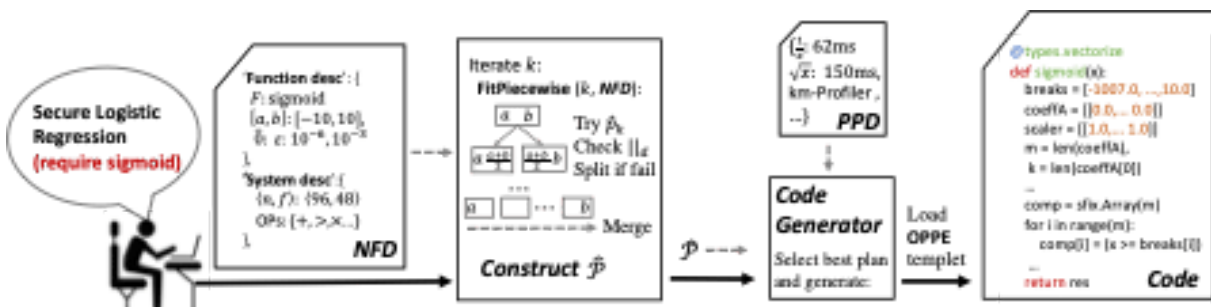
Figure 10: Packet Loss Rates vs. Throughput

基于多方安全计算的非线性函数代码生成器

在通用多方安全计算（MPC）平台上高效地计算非线性函数一直是一个难点问题，目前采取的主要方案是各个平台自行实现几个基本算子，如倒数、开方、e指数和对数，再用基本算子组合的方式来逐步串行计算复杂的非线性函数。但受限于MPC计算中数的表示多为定点数且在计算过程中无法确定计算结果的特性，这种计算方式存在一系列问题，包括：1）低精度或计算错误：定点数表示精度有限且易发生溢出；2）效率低下：非线性函数基本算子自身效率有限，其组合进一步降低效率；3）通用型差：部分复杂函数如密文上的积分很难实现以及4）迁移性差：一个MPC平台上可用的计算协议很难迁移到其他平台。

徐葳研究组提出NFGGen，对任一光滑连续的非线性函数自动化构造一个定点数分段多项式，在秒级生成针对某一特定MPC平台的定点数分段多项式计算协议。相比起基本算子组合的计算方式，NFGGen，1）保证了计算结果的准确率限制在给定精度要求内，避免了定点数计算的误差累积和溢出；2）极大提升了计算效率，在进行测试的15个非线性函数及6个MPC协议上，NFGGen平均提升了6.5倍计算效率，节省 39.3%通信量，最好情况下提升86倍计算效率；3）提升了通用性和迁移性。

该成果研究论文：Xiaoyu Fan, Kun Chen, Guosai Wang, Mingchun Zhuang, Yi Li, and Wei Xu. 2022. NFGGen: Automatic Non-linear Function Evaluation Code Generator for General-purpose MPC Platforms. In Proceedings of Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). ACM, New York, NY, USA, 14 pages.



随机梯度优化的复杂度分析

随机优化理论的证明通常考虑的是所有优化问题中的最差情况，如下图所示。这种情况下优化问题的理论分析比较简明，也比较容易得到理论最优的结果。

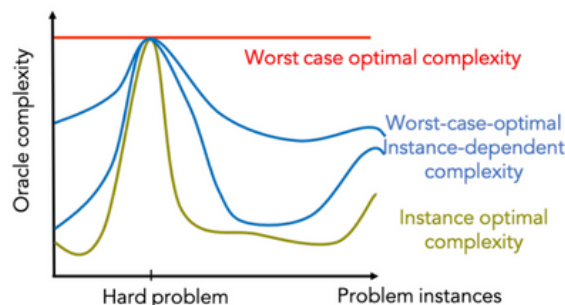


Figure 1. Different notions of complexity and optimality.

然而这些最差情况所涉及的问题在实际生活中常常不会出现，这就导致了一些实践中应用的比较好的方法（例如ADAM算法中的矩估计 moment estimation）并没有得到理论解释。张景昭研究组分析了更精细的复杂度，发现当随机优化中的噪音在每个循环中有较大变化时，矩估计可以提升收敛速度。

该成果研究论文：Jingzhao Zhang, Hongzhou Lin, Subhro Das, Suvrit Sra, Ali Jadbabaie Beyond Worst-Case Analysis in Stochastic Approximation: Moment Estimation Improves Instance Complexity, ICML 2022 July.

神经网络训练并不是在寻找驻点

非凸优化理论常常分析梯度算法寻找驻点的速率。虽然在这种分析框架下，最优的梯度算法已经被理论证明，但这些算法（如 variance reduction 或者 Nesterov momentum）的实验性质并不明显。在这个工作中，张景昭研究组发现这种理论偏差是由于其研究目标与实际不符造成的。该研究组通过大量ImageNet与Wiki102实验发现，绝大多数模型虽然损失函数收敛，而其参数并不在驻点上：

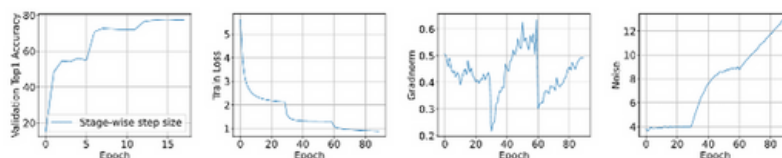


Figure 1. The validation accuracy and the quantities of interest (1) for the default training schedule of ImageNet + ResNet101 experiment.

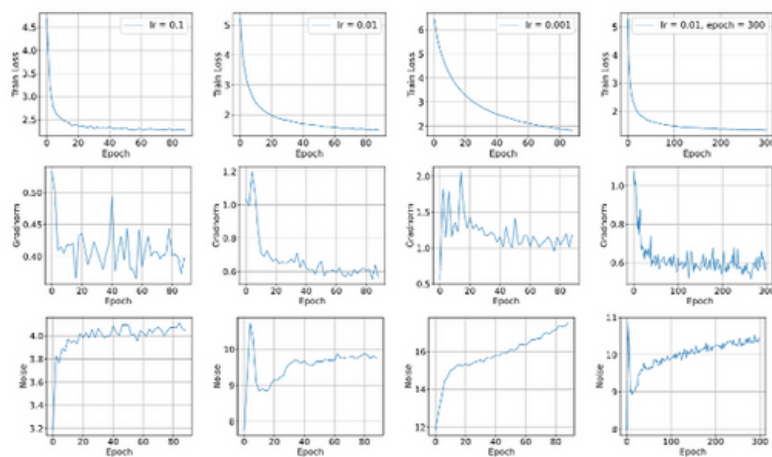
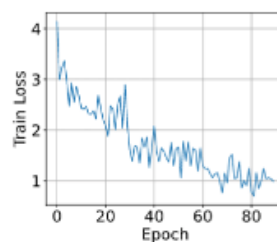
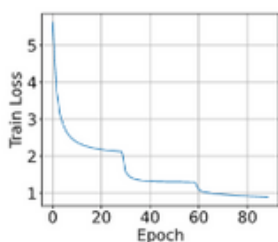


Figure 2. The quantities of interest (1) vs epoch for the constant learning rate training schedule in ImageNet experiments. The learning rate is set to be 0.1, 0.01, 0.001, 0.01 respectively starting from the left column. All models are trained for 90 epochs, except that the last experiment in the column ran for 300 epochs

基于上述实验，该研究组借助动力系统的invariant measure理念提出了一种新的收敛定义，即参数的时间平均收敛。该研究组为这种收敛提供了神经网络优化的理论分析。并且还发现，实际中损失函数的平滑收敛，是由于估计器在时间维度做了平滑。

该成果研究论文：Jingzhao Zhang, Haochuan Li, Suvrit Sra, Ali Jadbabaie. Neural Network Weights Do Not Converge to Stationary Points: An Invariant Measure Perspective, ICML 2022 July.



$$\text{Loss} = \frac{1}{N} \sum_{i=1}^N l(\theta_i, x_i),$$

$$\text{Loss} = \frac{1}{N} \sum_{i=1}^N l(\theta_N, x_i).$$



量子信息

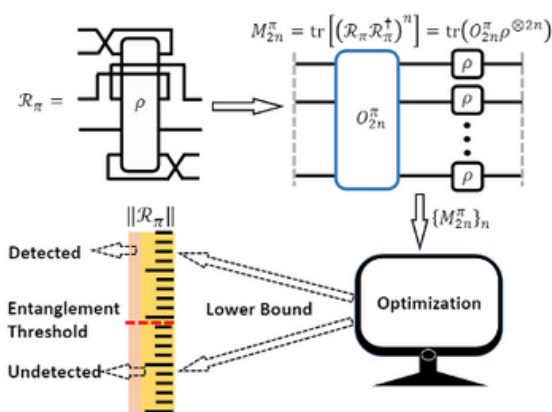


一、量子信息基础理论

主要完成人：马雄峰研究组

实用化的多体纠缠探测协议

量子纠缠是理论物理研究以及量子信息科学中的基础概念，发展高效的纠缠探测协议对于标定大型量子设备的可靠性有着重要意义。传统的纠缠探测手段往往有着各种限制。例如纠缠见证（Entanglement Witness）虽然是最常用的实验方案，但是它的有效性很大程度依赖于对被测量量子态的先验知识。正映射判据（Positive Map Criterion）是另一种理论上具有强大探测能力的纠缠判据，然而这一判据的实现往往需要极高实验复杂度的量子态层析。近期，研究者们提出了一种基于矩测量的实验方案可以避免量子态层析而实现一种弱化版本的正映射判据。这一实验方案只要求对单份量量子态进行操作以及测量，并且具有较低的实验复杂度和较强的探测能力。然而，受限於正映射判据自身的性质，这一方案只能探测两体量子系统的纠缠。



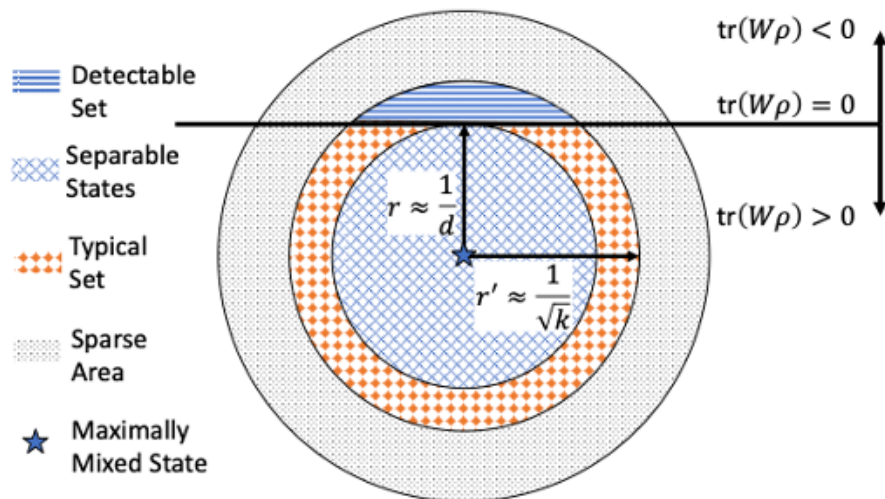
多体纠缠探测协议示意图

为了解决这一问题，在这一工作中，刘振寰、唐一凡、代昊、刘鹏宇、陈澍、马雄峰等引入了一种新的多体纠缠判据——指标轮换纠缠判据，并且成功将其转化为了基于矩测量的实验框架。这一实验方案具有更低的实验复杂度，并且可以探测多体系统中更加复杂的纠缠结构。在两体系统中，这一框架给出了新的两体纠缠判据，极大增强了两体纠缠的探测能力。此外，一些数值实验表明，这一框架中的一些关键物理量还可以作为纠缠的度量，在量子多体物理的研究中起到重要的作用。

该成果研究论文：Zhenhuan Liu, Yifan Tang, Hao Dai, Pengyu Liu, Shu Chen, and Xiongfeng Ma, Detecting Entanglement in Quantum Many-Body Systems via Permutation Moments, Phys. Rev. Lett. 129, 260501 (2022) .

纠缠探测协议效果的基本限制

量子信息技术有望在各种信息处理任务中展示优势。目前正处于“嘈杂的中等规模量子设备”的阶段：研究人员可以操控至多50到200个量子比特以展示量子优势。对于这些设备，纠缠的产生与探测是衡量设备质量的重要基准。然而反直觉的是，即使纠缠态几乎占据整个量子态空间，纠缠探测的难度仍超出预估。在各种纠缠判据中，纠缠见证是最直接的也是实验中最常使用的一种。然而，许多证据表明，纠缠见证只有在事先对目标量子态有精确了解的情况下才有效。态制备中不可预测的噪音会大大降低纠缠见证的成功概率。为了解决这个问题，研究人员开发了非线性纠缠判据，如著名的部分转置判据等。尽管比纠缠见证更有效，这些非线性判据在很大程度上依赖于量子态层析。然而态层析需要消耗指数多的资源，在实验上往往无法负担。



态空间和纠缠见证示意图

上述事实表明了一个有趣的现象：高效的纠缠判据往往不够强大，而强大的纠缠判据则无法被高效的实验实现。在此项工作中，刘鹏宇、刘振寰、陈澍、马雄峰对上述观察进行了理论的研究。通过一种系统的方法来评估纠缠判据的探测能力，该研究组发现了纠缠判据的效率和有效性之间的限制。对于一个与环境耦合的随机系统，他们证明了，任何基于单拷贝测量的纠缠判据，都需要指数多的测量来有效地探测纠缠。否则，该判据的探测能力将双指数衰减。此外，如果允许多拷贝联合测量，纠缠判据的有效性可以得到指数级的提高，这意味着在纠缠探测问题上的量子优势。

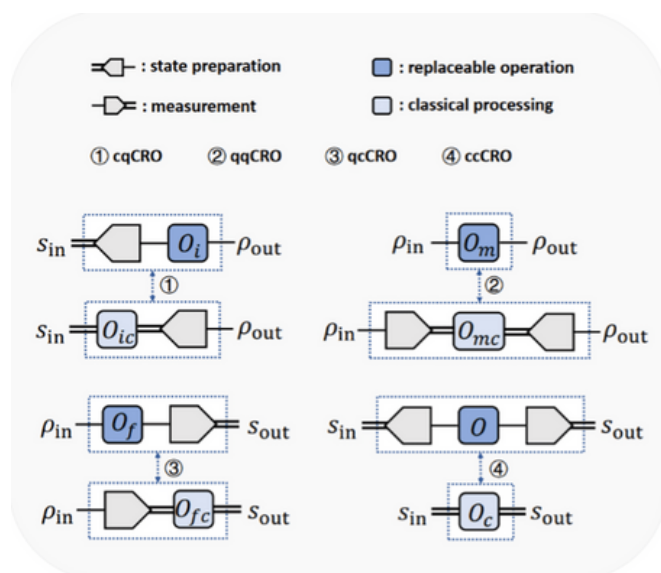
该成果研究论文：Pengyu Liu, Zhenhuan Liu, Shu Chen, and Xiongfeng Ma, Fundamental Limitation on the Detectability of Entanglement, Phys. Rev. Lett. 129, 230503 (2022) .

经典可替代操作

在当今的实验条件下，实现高保真度的多量子比特门仍然是具有挑战性的。一般情况下，经典处理要比量子处理具有更高的准确性且更容易实现。经典处理的这些优点启发研究者在实现一个量子线路时，在确保量子线路输出结果不变的情况下，同时可以把部分量子操作替换成经典操作。这一想法已经在量子密钥分发中被使用，并帮助量子密钥分发成为量子信息科学中最早可实用化的应用。除此之外，经典替代这一思想也可以被用在量子计算中，比如最近发展起来的量子-经典混合算法。

然而，纵使经典替代的想法已经被广泛应用，什么样的量子操作可以被经典替代却仍没有一个系统的研究。为了解决这一问题，刘国定、张行健、马雄峰合作的工作严格定义了四种情况下的经典可替代操作。该研究组推导了“经典可替代操作”集合的等价数学刻画，并进一步从量子信道资源理论角度出发量化了一个量子信道的“经典不可替代性”。此外，该研究组将“经典不可替代性”和量子信道在一个非局域游戏中的量子优势联系起来。这一工作有助于以更少的资源实现一个量子线路，并进一步理解量子优势的来源。

该成果研究论文：G. Liu, X. Zhang, and X. Ma, “Classically Replaceable Operations,” Quantum, vol. 6, p. 845, Oct. 2022.



经典可替代操作示意图

二、量子通信与密码

主要完成人：段路明研究组、马雄峰研究组

模式配对量子密钥分发协议

量子密钥分发是目前量子信息领域最为成功的应用之一，也是构建量子通信网络的第一步。基于现有的商用光学设备，量子密钥分发已经可以在一些商用环境下进行实际应用，比如我国的京沪干线工程、合肥的城市密钥分发网络等等。为推动量子密钥分发的实用化，需进一步提高其实际设备的安全距离和成码速率。一方面，量子密钥分发的安全距离和成码速率受光学信道传输损耗的严重限制。另一方面，在用实际设备实现量子密钥分发的过程中，设备往往存在不符合理论假设的漏洞。这些漏洞可以被窃听者使用，从而降低了量子密钥分发协议的实际安全性。

清华大学交叉信息研究院马雄峰及研究组成员曾培、周泓伊和吴蔚捷设计了一种新型测量设备无关的协议，同时兼顾高性能和实用性，突破点对点量子密钥分发成码率。该协议不需要复杂的激光相位锁定、信道相位监控，大幅提升了测量设备无关密钥分发协议的性能，为高性能、高安全性量子密钥分发实用化提供了理论基础。

该成果研究论文：P. Zeng, H. Zhou, W. Wu, and X. Ma, “Mode-pairing quantum key distribution,” Nature Communications, vol. 13, no. 1, p. 3903, Jul 2022.

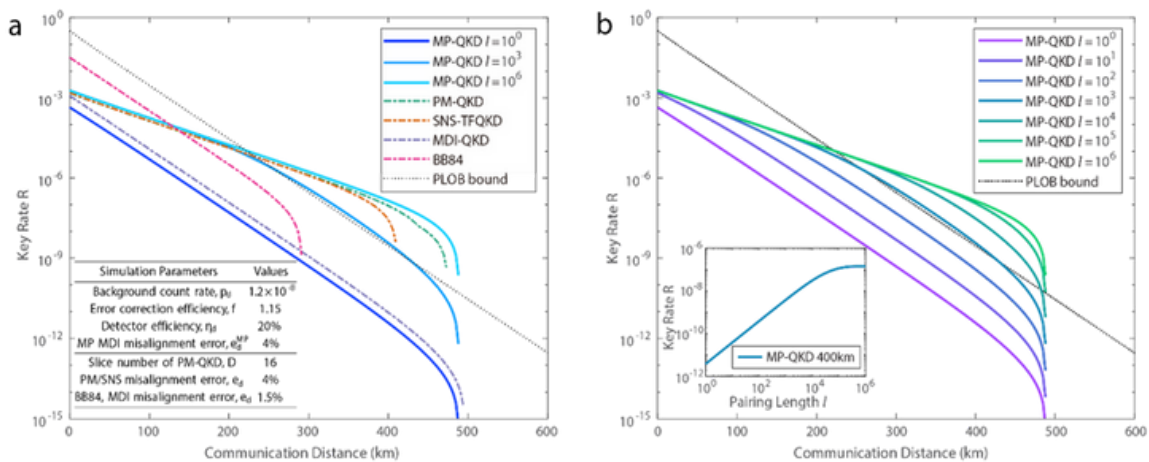


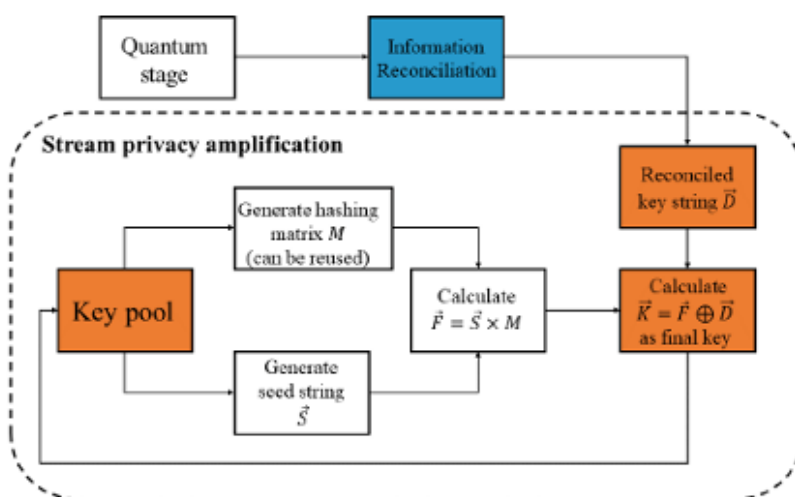
图 5 模式配对协议的成码率数值比较。

量子密码的流式隐私放大方案

隐私放大（privacy amplification）是保证量子通信安全的关键步骤。现有的隐私放大方案基于矩阵乘法，需要积累足够的原始密钥才能进行计算并得到最终密钥。这类似于经典密码学中的分组密码。出于效率的考虑，一次隐私放大所处理的数据块通常非常巨大，导致数据累积的时间会比较长，进而会延迟最终密钥的生成。这个问题在通信链路流量较小或是链路不稳定时，例如卫星-地面链路中，尤为明显。此外，信息协商中遗留的任何错误都会导致整个分组的最终密钥无法使用。

通过重构基于量子纠错的安全性证明过程，马雄峰和博士生黄溢智、张行健提出了一种类似于经典流密码的流式隐私放大方案，以解决最终密钥生成延迟和错误扩散的问题。此外，流式隐私放大方案与传统方案不同，可以在信息协商步骤进行，从而有助于提高量子通信后处理的灵活性。应用方面，流式隐私放大方案还可以与量子网络中的延迟隐私放大方案相结合，有助于降低对量子网络中中继节点的安全性要求。

该成果研究论文：Y. Huang, X. Zhang, and X. Ma, “Stream privacy amplification for quantum cryptography,” PRX Quantum, vol. 3, p. 020353, Jun 2022.

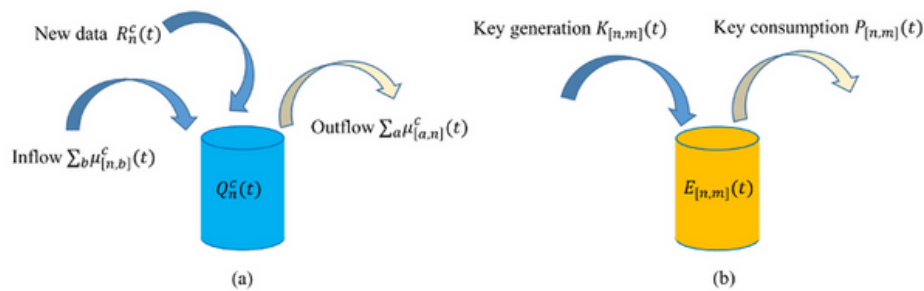


流式隐私放大的安全性来源

量子网络中的安全评估与密钥管理

作为量子密钥分发的扩展，多用户之间的安全通信是量子网络中的一项基本任务。当量子网络结构因大量用户而变得复杂时，调查网络问题很重要，包括安全性、密钥管理、延迟、可靠性、可扩展性和成本。对此，马雄峰和黄隆波合作课题组利用经典网络理论和图论来解决量子网络中的两个关键问题，即安全性和密钥管理。首先，该课题组设计了一种具有最高安全级别的通信方案，它信任最少数量的中间节点。其次，当量子密钥是一种有限的资源时，还设计了密钥管理和数据调度方案来优化数据传输的效用。这些结果可以直接应用于当前的城域和自由空间量子网络实现，并有可能成为未来量子网络设计的标准方法。

该成果研究论文：H. Zhou, K. Lv, L. Huang, and X. Ma, “Quantum network: Security assessment and key management,” IEEE/ACM Transactions on Networking, vol. 30, no. 3, pp. 1328–1339, 2022.



量子网络中的动力学

实现高增益的微波单光子三极管

段路明研究组在单光子三极管的研究工作中取得重要进展，首次在实验中利用超导量子电路实现了微波单光子三极管，并实现了高达53.4dB的增益和超过20dB的开关比，相比之前的器件提高几个量级。

电子三极管是一种重要的半导体器件，它既可以工作在数字电路中实现经典逻辑门，又能够用于模拟电路实现电流放大。与之类似，单光子三极管是一种能够通过单个栅极光子控制输入光信号开关和放大的光量子器件，在光量子网络 and 全光计算领域具有重要的应用。但是由于光子之间的相互作用非常微弱，实现高性能的单光子三极管非常具有挑战性。在之前的工作中，有研究组借助单个原子、原子系综、或者半导体量子点实现了光子之间的有效相互作用，研制出了光波频段的单光子三极管，但受限于这些体系中不完美的量子操控或者相对较弱的光和物质相互作用，单光子三极管的有效增益最高不超过100，开关比也相对较差，极大的限制了可能的应用。

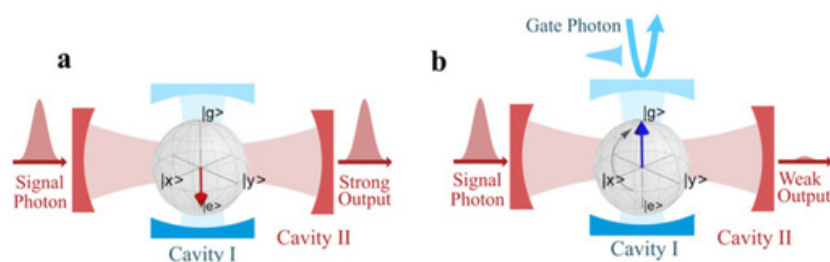


图1:单光子三极管的工作原理

在此项工作中，研究人员利用超导量子电路实现了极高增益和开关比的微波单光子三极管。如图 1a 和 b 所示，他们采用一个超导量子比特和微波谐振腔的耦合系统作为三极管的栅极，在栅极入射的单光子可以改变超导量子比特的状态，进而改变与之耦合的另一个微波谐振腔（提供源极和漏极）的共振频率，从而能够对在源极入射的微波光子完成开关操作。在实验中，研究人员用微弱的相干态微波信号模拟单光子态用作栅极的控制信号，他们发现单个光子确实能够有效的控制三极管的开启和关断，实现对源极微波信号的开关操作。由于源极微波光子数可以很高，这也相当于实现了对栅极单光子信号的有效放大。研究人员发现，该三极管可以在一个很大的源极信号强度范围内正常工作，这相当于实现了一个增益极高的单光子放大过程。如图 2a 和 b 所示，即使当源极的入射光子数接近 10⁶ 个的时候，该三极管依然可以有超过 20dB 的开关比，同时实现约 53.4dB（相当于 2.19×10^5 ）的增益，比之前的工作提高了三个数量级。这项工作为基于微波光子的量子网络和量子信息处理技术奠定了重要的基础。

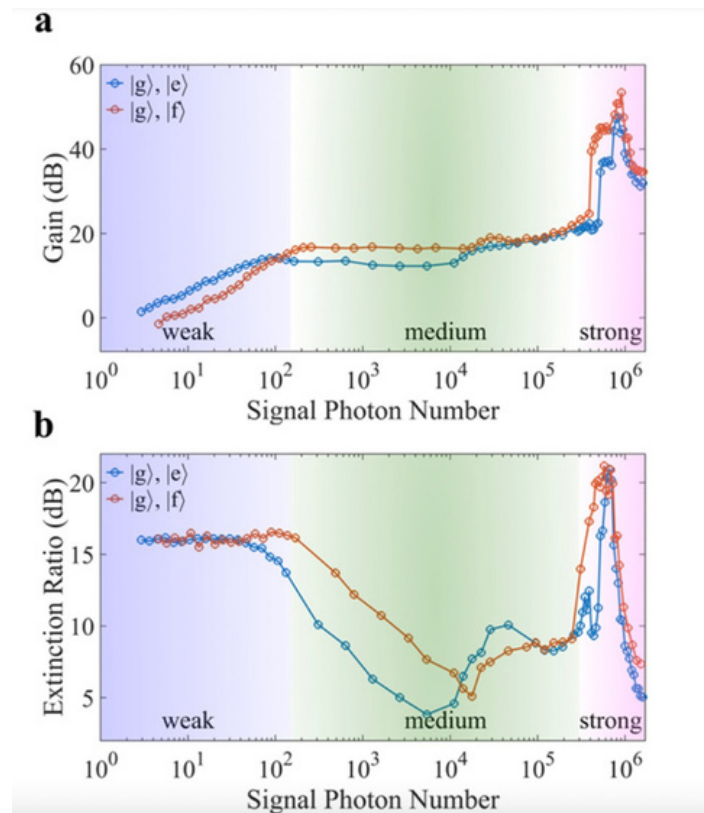


图2:极高增益和开关比的微波单光子三极管

该成果研究论文: "An ultra-high gain single-photon transistor in the microwave regime", Z. Wang, Z. Bao, Y. Li, Y. Wu, W. Cai, W. Wang, X. Han, J. Wang, Y. Song, L. Sun, H. Zhang* & L. Duan*, Nat. Commun. 13,6104 (2022).

三、量子人工智能

主要完成人：邓东灵研究组

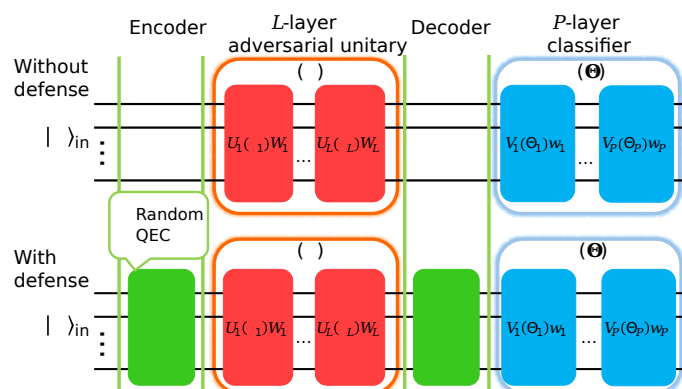
提升量子机器学习对抗鲁棒性的随机编码方法

量子机器学习是一个近年来广受关注的交叉前沿领域。近期的研究揭示了量子机器学习系统对于对抗攻击的脆弱性，即加入很小的扰动就可以导致量子分类器给出错误预测。这一性质说明了量子学习系统在恶意环境可能存在安全隐患。如何在未来为量子机器学习，尤其是在含噪声物理系统中的应用提供有效的安全保障成为一个重要的问题。

在这一背景下，该研究提出了提升量子学习系统对抗鲁棒性的随机编码量子数据的方法，在量子机器学习中首次从理论上严格证明了随机编码可以降低机器学习系统的收到对抗性攻击的风险。该文系统地研究了针对不同的对抗性攻击模型的随机编码方法。首先，对基于变分量子神经网络的机器学习系统，该研究证明了不论是全局还是局域的随机量子编码器都可以隐藏梯度信息，从而使得基于梯度下降和变分量子电路的对抗性攻击难以奏效。之后，该研究组考虑了局域对抗性攻击的情形，并且证明了只需要反比于系统大小的强度的攻击就可以以很高的概率造成误分类。为对抗这一类攻击，该研究组证明使用黑盒式量子纠错码编码的量子数据样本可以给量子分类算法提供差分隐私性质，从而提高量子分类算法的对抗鲁棒性。当使用多级量子纠错码后，对于鲁棒性的提升效果会进一步增加。相比于过去提升量子机器学习鲁棒性的方法，此方案具有在近期量子设备上相对容易实现和使用的量子纠错码编码同时也是未来容错量子计算的基本模块等优势，在未来量子机器学习中，具有广泛的应用价值。

该研究为提升量子机器学习系统的可靠性和安全性提供了应用广泛的方案，构建了机器学习与量子计算之间新的联系，对未来相关方面的理论和实验研究提供了指导。

该成果研究论文：Weiyuan Gong, Dong Yuan, Weikang Li, Dong-Ling Deng, Enhancing Quantum Adversarial Robustness by Randomized Encoding, arXiv:2212.02531v1.



四、量子信息处理

主要完成人：孙麓岩研究组

量子信息处理的超导光子声子混合芯片

量子计算由于其独特的并行计算优势受到了广泛的关注。近年来，多种量子信息处理平台（如中性原子，离子阱，光子和超导集成电路等）由于各自的优点都得到了广泛的发展，其中以光量子芯片和低温超导量子芯片为代表的固态量子芯片由于小体积、高稳定性和高可拓展性成为非常有竞争力的发展平台。

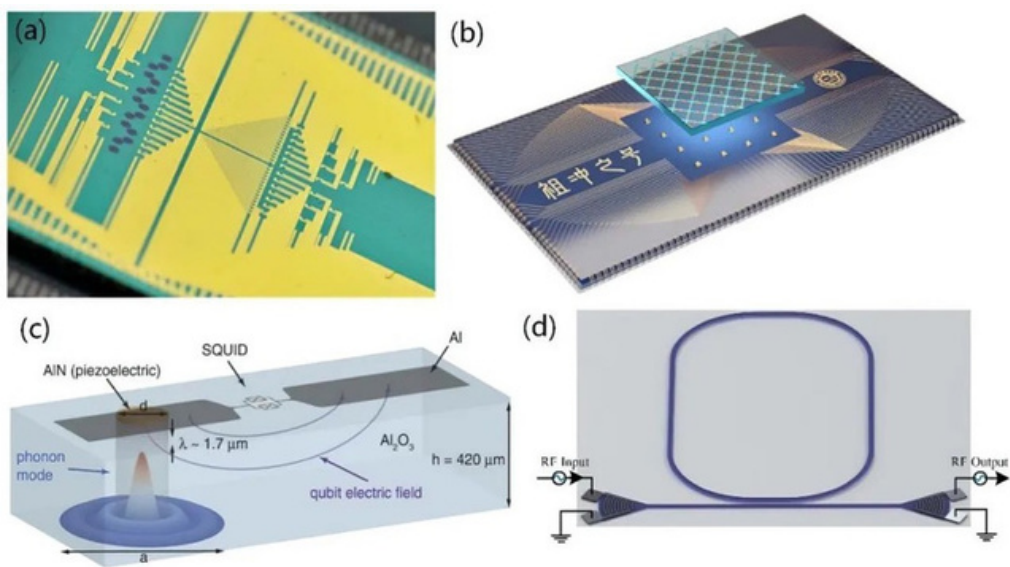


图1 (a) 可编程集成量子光子回路，(b) 固态可编程超导量子处理器，(c) 体声波谐振腔，(d) 高频集成声子回路

光子由于其百太赫兹量级的工作频率具有非常小的热光子激发，可以很好地维持其量子相干性。因此，利用集成光量子芯片有望在将来发展出一种室温量子信息处理平台，有助于拓展其使用场景，如图1 (a)。虽然集成光量子芯片具有以上优势，但它依然面临一些挑战，如缺乏高效的片上光存储器、延时器和强非线性。相比之下，虽然超导系统是利用复杂且精密的稀释制冷机在mK的温度下工作以降低环境的热激发，但基于可编程固态超导量子芯片的量子信息处理平台发展则更加超前。

该研究结合集成光量子芯片和超导量子芯片各自的优点和面临的核心挑战，将二者有机地结合可以发挥各自的优点解决彼此面临的一些问题。但是，通信波段光子与超导系统天然不兼容：一方面，由于光波与微波的频率相差巨大，二者很难直接相互作用；另一方面，超导金属对光波的吸收容易破坏低温环境且给光波带来损耗。因此，引入GHz的高频声子作为媒介是一种可行的方法（图1 (c-d)）。

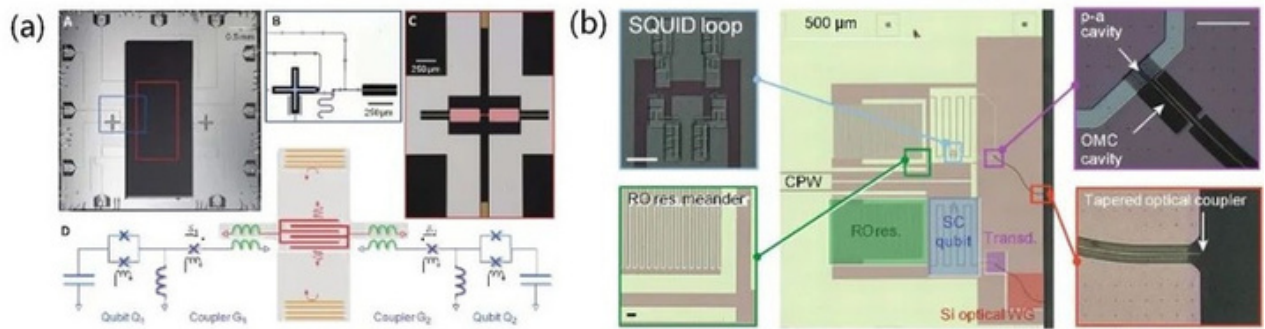


图2 (a) 基于表面声波的量子态传输和远程纠缠，(b) 基于超导-光子-声子混合集成芯片的超导比特量子信息的光学读出

通过引入声子实现声子、光子、超导系统的混合集成具有以下优势：利用高效的光-声相互作用和微波-声波相互作用可以实现高效的光波-微波频率转换，解决微波量子信息无法远距离传输的问题（图2（b））；此外，由于声子的传播速度比光子慢五个数量级，非常适合做延时（图2（a）），且相同频率下集成声子器件的尺寸也比微波器件的尺寸小五个数量级。因此，利用集成声子器件代替微波器件将可以极大地提高超导量子芯片的集成度；由于声波在真空中无法传播且高频声波的波长很短，利用声子可以减小芯片上各个器件的串扰。

基于量子芯片在近年来的激动人心的进展，混合集成量子芯片毫无疑问地将会在分布式量子计算、量子网络、量子通信和基础物理等研究方面扮演越来越重要的角色。

该成果研究论文发表在全球唯一聚焦芯片类综合性国际学术期刊Chip上，Xu, X.-B., Wang, W.-T., Sun, L.-Y. & Zou, C.-L. Hybrid superconducting photonic-phononic chip for quantum information processing. Chip 1, 100016 (2022).

五、拓扑凝聚态物理

主要完成人：徐勇研究组

非厄米吸收谱

尽管非厄米系统已经在冷原子系统中被实现，然而如何测量其动量空间的复数能谱仍然是一个未解决的问题。非厄米趋肤效应的存在会使情况更加复杂，此时系统的开放边界能谱与动量空间能谱有显著不同，由此引发出另一个问题：是否非厄米趋肤效应会使动量空间能谱无法在有边界的系统中测得？这个问题的重要性来源于绝大多数实验系统都存在边界。

在冷原子系统中射频光谱学是一种广泛使用的谱学测量手段，此方法的原理是用微波将系统与辅助能级耦合，并通过测量系统与辅助能级间转移的粒子数与微波频率间的关系得到系统的能谱信息，同时粒子的动量信息可以通过飞行时间测量法得到，从而获得动量分辨的能谱。

研究人员将射频光谱学方法应用于非厄米系统中，提出一种可以同时测量系统复能谱的实部和虚部的方法，测量方案的示意图见图1。由于系统部分存在耗散，初态粒子需制备在无耗散的辅助能级上（图1a），否则粒子会很快全部丢失。测量得到的辅助能级占据数随微波失谐变化的一个典型示例如图1b所示，其吸收峰的中心值和半高宽与能谱的实部和虚部相关。

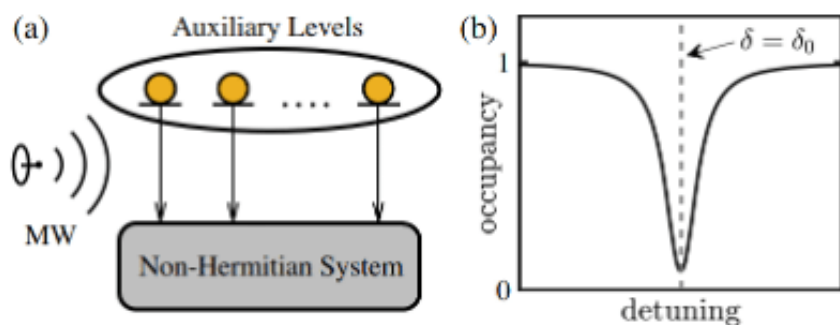


图1: (a)实验系统示意图，其中非厄米系统与辅助能级通过弱微波耦合。原子首先制备在辅助能级上，经过一段时间后测量辅助能级剩余的粒子数。(b)辅助能级占据数随微波失谐变化的典型示例。

研究人员采用主方程与线性响应理论，推导出周期边界条件下动量为 k 的辅助能级占据数与微波失谐和动量空间本征能量的关系，基于该公式，可以对辅助能级占据数随微波失谐的变化曲线进行拟合得到系统动量空间能谱；同时，研究人员证明当系统存在边界时，测量结果随着系统尺寸增大逐渐趋于周期边界下的结果，这意味着对于一个无穷大的系统，测量结果与边界和非厄米趋肤效应无关。研究人员进一步基于Hatano-Nelson模型数值验证了这一现象（图2）。

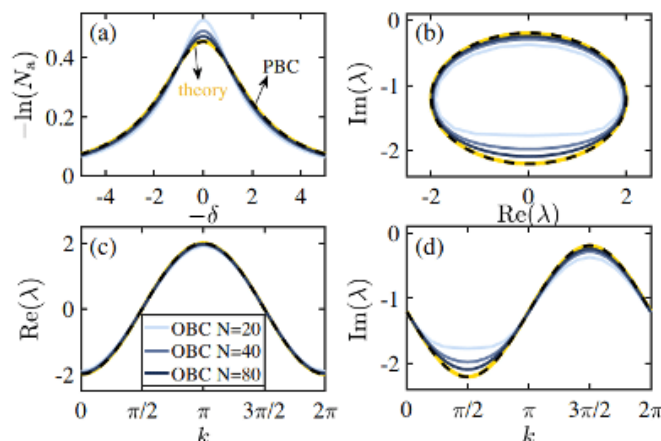


图2: (a)辅助能级占据数随微波失谐的变化曲线。(b-d)复数能谱以及能谱实部和虚部与动量 k 的关系，其中黄色实线、黑色虚线和蓝色实线分别为理论结果、周期边界和开放边界条件下的拟合结果。

研究人员还发现若将动量分辨测量改为格点分辨测量，通过测量辅助能级边界处的局域粒子占据数，可以得到系统开边界拓扑零能模式的信息，该信息体现在边界处微波失谐为0时存在一个吸收峰。通过对非厄米Su-Schrieffer-Heeger模型的数值模拟，研究人员发现当系统存在零能边界态时，边界处局域占据数在失谐为0时有响应，并且该响应只存在于边界附近（图3），而系统处在拓扑平庸态时则不存在上述响应。

该成果研究论文：“Non-Hermitian Absorption Spectroscopy”，Kai Li and Yong Xu, Phys. Rev. Lett. 129, 093001 (2022).

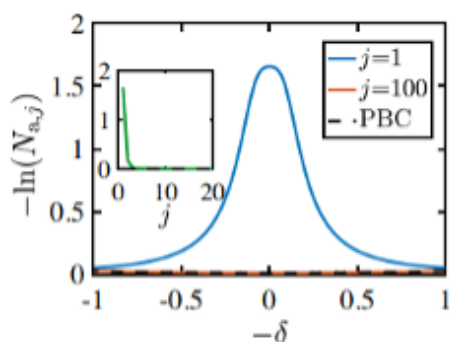


图3: 吸收指数随失谐的变化，小图为失谐为0时吸收指数随格点 j 的变化。

金属Shiba晶格中的拓扑量子相变

拓扑超导体由于其在拓扑量子计算中的潜在应用，在过去十年中引起了广泛关注。在拓扑超导体的研究中，Shiba晶格发挥着重要作用，因为它们可以用来实现高度可控的拓扑超导相。当磁性杂质被放置在超导体表面时，超导体能隙中会出现局域在磁性杂质附近的束缚态，该束缚态被称为Yu-Shiba-Rusinov (YSR) 子能隙态，而Shiba晶格正是由一系列YSR子能隙态形成的。由于YSR态之间存在长程跃迁，该晶格可用于实现具有高陈数的拓扑超导相 [Phys. Rev. Lett. 114, 236803 (2015)]。值得一提的是，最近的一项实验 [Nat. Phys. 17, 943 (2021)] 在磁体和超导体的混合系统中观察到了拓扑Shiba能带。

拓扑相不仅可以存在于有能隙系统中，也可以存在于金属体系中。对于Shiba晶格，之前的研究主要集中在Shiba晶格中的有能隙超导体或Shiba玻璃中的无能隙（但出现安德森局域化）超导体。受拓扑Shiba能带实验进展的推动，研究人员关注二维s波超导表面上由铁磁杂质形成的二维规则Shiba晶格，并从理论上预测弱面内磁场可以在保持杂质铁磁性的同时使其磁矩方向偏离表面法向量（见图1），使得二维规则Shiba晶格中可以出现拓扑金属相，而当磁性杂质的磁矩与表面法向量平行时，系统中的对称性排除了金属相存在的可能。

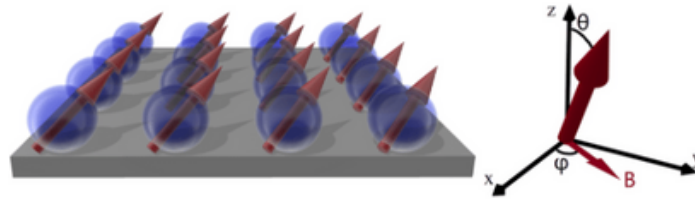


图1：铁磁杂质二维s波超导体表面上排列成方晶格。由于平面内磁场B的存在，磁化方向（由极角 θ 和方位角 ϕ 确定）偏离超导体表面法线方向（z方向）。

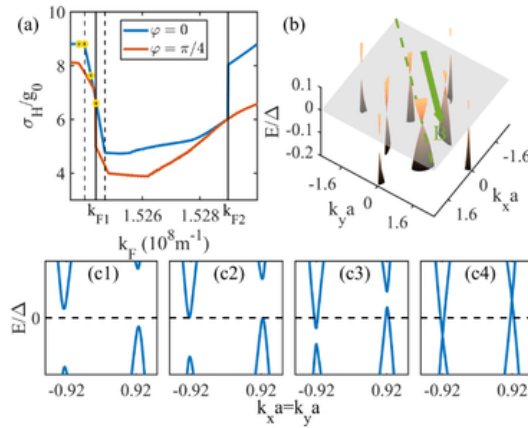


图2：(a)本征热霍尔电导随费米波矢的变化，其中纵向实线和虚线分别表示一阶和二阶相变点。(b)零能附近的能谱，对应(a)中 $\phi=\pi/4, k_F=k_{F1}$ 。(c1-c4)能谱随波矢的演化，从左到右分别对应(a)中4个黄圈。

研究人员进一步发现，从有能隙的拓扑超导相出发，通过改变费米波矢等系统参数，系统可以经历Lifshitz相变到达金属相 [图2(c1-c4)]，这种相变也体现在本征热霍尔电导的二阶量子相变上 [图2(a)]。此外，若系统能隙在高对称点上闭合，粒子-空穴对称性保证能隙闭合一定发生在零能处，导致本征热霍尔电导总是会表现出一阶量子相变。但在金属体系中系统能隙很难刚好在高对称点上闭合，因此能隙闭合一般不会发生在零能处，此时本征热霍尔电导的一阶量子相变不受保护。值得注意的是，研究人员发现Shiba金属中存在许多由非高对称点上的能隙闭合引起的一阶量子相变 [图2(a,b)]。为解释该现象，研究人员提出Shiba金属中的一种机制（称为倒易晶格反射对称性）将能隙闭合固定在零能处，从而保护一阶相变。此外，研究人员还展示了由于YSR态存在长程跃迁，Shiba金属中可以存在较大的非量子化本征热霍尔电导，使得二阶量子相变能够多次出现 (图3)。

该成果研究论文：“Topological quantum phase transitions in metallic Shiba lattices” , Ning Dai, Kai Li, Yan-Bin Yang, and Yong Xu, Phys. Rev. B 106, 115409 (2022).

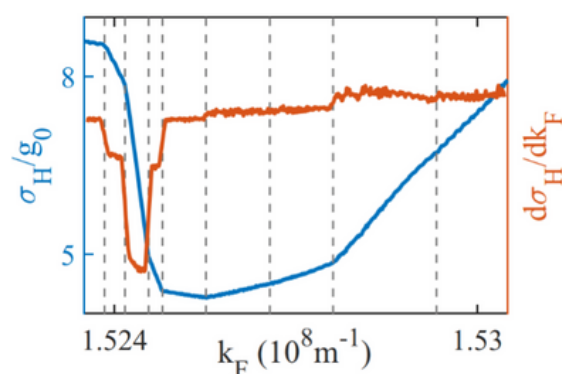


图3：本征热霍尔电导及其导数随费米波矢的变化，其中纵向虚线表示二阶相变点。

Edited by Xuechao Zhang
Reviewed by Luming Duan, Jian Li, Xiamin Lv