清華大學 交叉信息研究院

Institute for Interdisciplinary Information Sciences, Tsinghua University

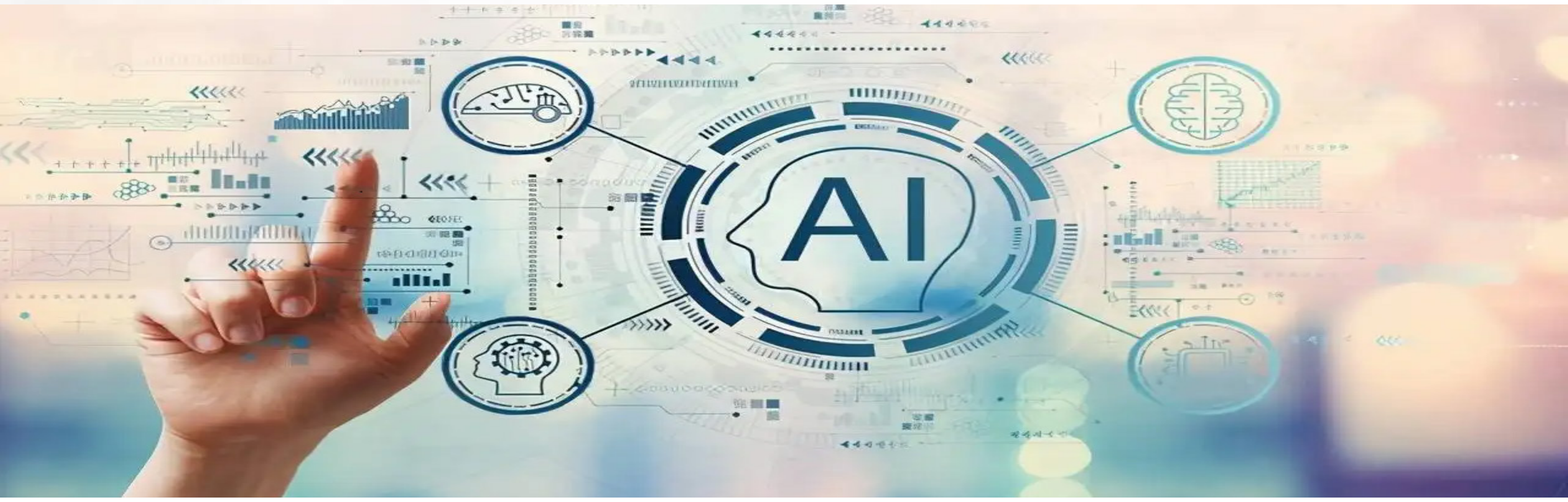
学术科研简报

2022.01-06

人工智能

量子信息

人工智能



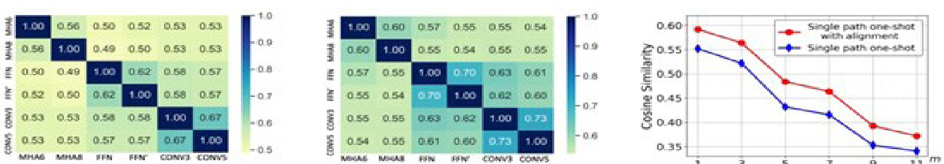
一、深度学习与强化学习

主要完成人：李建研究组、陈建宇研究组、高阳研究组、吴翼研究组、马恺声研究组、赵行研究组

分析与缓解自动架构搜索中的干扰问题

在当代的自动架构搜索技术中，权重共享作为一种最为流行的核心技术被广泛应用。权值共享通过复用之前训练的子结构的部分权重来减少从零开始训练不同子模型的代价。然而，由于不同的子模型的共享权重的梯度更新时存在干扰，真实的子模型的准确率和最后估计的子模型的准确率的相关度往往比较低，这严重影响了自动架构搜索技术的性能和适用性。在这篇工作里，李建研究组深入调查了权值共享中的干扰问题。通过采样不同的子模型并计算这些子模型在共享的部分权值上的梯度，他们观察到了两个现象 1）共享权值上的梯度的干扰程度和两个子模型之间的不同的网络层结构的数量是正相关的；2）两个子架构在共享网络结构上的输入和输出值越相似，他们之间的干扰就越小。从这两个观察出发，他们提供了 MAGIC-AT 技术来有效的缓解干扰问题，他包括两项关键技术：1) MAGIC-A: 与之前的随机采样子模型进行梯度更新的工作不同，研究组提出了一个渐进子架构修改的采样范式。在每一次临接的梯度更新步数之间，他们让其采样的子架构仅仅存在一个网络层结构的差别以最小化不同邻接梯度更新的干扰；2) MAGIC-A: 研究组强制让不同子模型在共享网络结构上的输入输出尽可能相似来进一步减少他们之间的干扰。研究组首先在一个复杂的 BERT 搜索空间中验证了，他们提出的两项关键技术都能够提出超网络的排序性能，并且两种技术结合能够得到进一步的提升。接着，该研究组使用 MAGIC-AT 在 BERT 语言模型，SQuAD 自然语言理解任务以及大规模图像分类问题 ImageNet 上做了自动架构搜索，实验证明 MAGIC-AT 搜索得到的架构一致切显著的超过之前的工作，证明了他们提出的方法的有效性。该工作是和微软亚洲研究院合作完成，并发表于机器学习顶级会议 ICML 2022，并被选为 spotlight 论文。

该成果研究论文：Jin Xu, Xu Tan, Kaitao Song, Renqian Luo, Yichong Leng, Tao Qin, Tie-Yan Liu, Jian Li, "Analyzing and Mitigating Interference in Neural Architecture Search", ICML 2022.



(a) Cosine similarity matrix of the super-net trained by single path one-shot
(b) Cosine similarity matrix of the super-net trained by single path one-shot with alignment
(c) Gradient similarity with respect to m

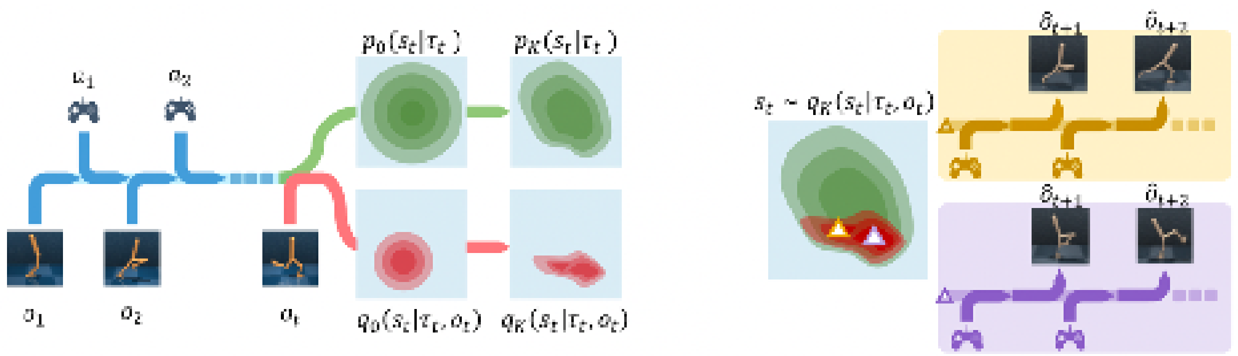
Model	Params	FLOPs	MNLI	QQP	QNLI	CoLA	SST-2	STS-B	RTE	MRPC	AVG
dev set											
$BERT_{base}$ (Devlin et al., 2019)	110M	2.9e10	84.4	89.9	88.4	54.3	92.7	88.9	71.1	86.7	82.1
$RoBERTa_{base}$ (Liu et al., 2019)	125M	3.3e10	85.3	91.1	91.1	61.0	92.7	90.0	77.5	87.9	84.6
$ELECTRA_{base}$ (Clark et al., 2020)	110M	2.9e10	-	-	-	-	-	-	-	-	85.1
$MPNet_{base}$ (Song et al., 2020)	110M	2.9e10	85.2	-	-	-	93.4	-	-	-	-
SPOS (Guo et al., 2020)	114M	3.3e10	84.7	91.4	91.4	59.6	92.1	89.7	80.9	86.3	84.4
MAGIC-AT	113M	3.3e10	85.6	91.3	91.8	61.1	**93.5**	90.3	80.9	**90.9**	85.7
E-MAGIC-AT	110M	2.9e10	**86.3**	**91.7**	**92.5**	**65.8**	92.5	**91.0**	**84.0**	89.7	**86.7**
test set											
$BERT_{base}$ (Devlin et al., 2019)	110M	2.9e10	84.6	89.2	90.5	52.1	93.5	85.8	66.4	84.8	80.9
$RoBERTa_{base}$ (Liu et al., 2019)	125M	3.3e10	84.8	89.0	91.7	57.1	93.3	88.0	74.1	84.1	82.8
$ELECTRA_{base}$ (Clark et al., 2020)	110M	2.9e10	85.8	89.1	**92.7**	59.7	93.4	87.7	73.1	86.7	83.5
SPOS (Guo et al., 2020)	114M	3.3e10	84.3	88.6	91.0	56.1	92.8	88.1	74.9	83.4	82.4
MAGIC-AT	113M	3.3e10	84.9	89.1	92.0	57.0	**94.1**	**87.8**	77.4	85.2	83.4
E-MAGIC-AT	110M	2.9e10	**85.9**	**89.6**	92.4	**60.3**	93.4	87.3	**80.4**	**87.4**	**84.6**

基于标准化流的部分可观测马尔可夫决策过程学习

部分可观测马尔可夫决策过程是对真实世界序贯决策过程的通用模型，然而其目前在高维连续空间、模型未知的条件下并未得到良好解决。其中最主要的挑战之一在于如何准确获取其信仰状态。已有的结合世界模型、隐状态表征学习以及强化学习的方法虽然能够对复杂的部分可观测马尔可夫决策模型进行学习，但其信仰状态空间以高斯和离散化分布为主，欠缺对复杂分布的建模能力。

陈建宇研究组通过将标准化流模型整合到变分推断框架中，提出了一种通用的循环信仰状态学习方法（FORBES），使其能够建模任意复杂的概率分布。该方法提高了对通用部分可观测马尔可夫决策过程的重建和预测精度，从而显著提升了下游强化学习任务的性能和泛化性。该方法对研发基于高维传感器输入的高级别自动驾驶与机器人等决策系统具有重要的意义。

该成果研究论文：X. Chen, Y. Mu, P. Luo, SE. Li and J. Chen, “Flow-based Recurrent Belief State Learning for POMDPs”, ICML 2022.



(a) Belief state inference　　(b) Predictions beginning from different samples

保障接触安全的机器人强化学习框架

强化学习对解决带复杂接触的机器人操作任务具有巨大的前景，包括工业装配、平面打磨等。然而将强化学习应用于实体机器人上时却有很大的安全隐患。无论是训练过程中还是训练收敛后，基于神经网络的机器人控制策略都可能出现问题并造成与环境之间的危险碰撞。

陈建宇研究组通过整合冗余自由度机械臂的零空间控制、变阻抗控制、以及基于视觉的强化学习等理论与算法，提出了一套保障接触安全的强化学习框架。该框架能不仅能保障真实机器人应用强化学习时，其末端执行器的接触力比较柔顺，同时在机械臂身遇到意外的接触与碰撞时能及时推断出来并进行柔顺处理。该工作为强化学习在真实机器人上的安全应用奠定了理论、算法和实验基础。

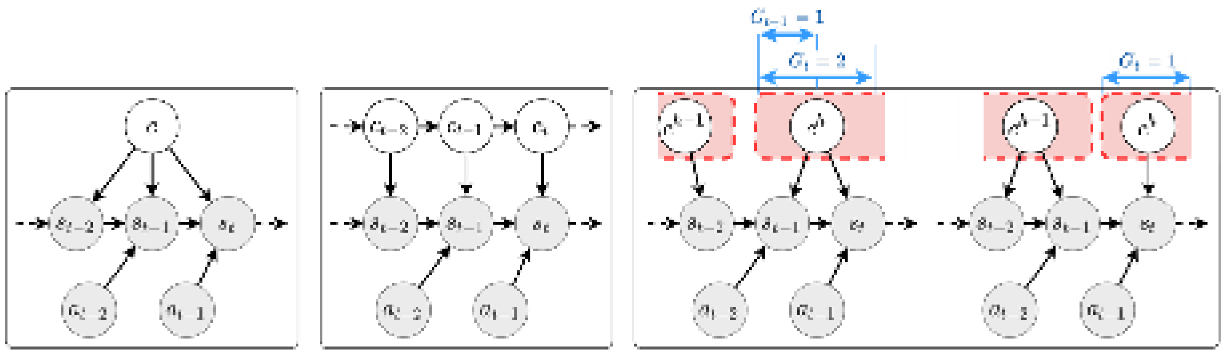
该成果研究论文：X. Zhu, S. Kang and J. Chen, "A Contact-Safe Reinforcement Learning Framework for Contact-Rich Robot Manipulation", IROS 2022.

保障接触安全的机器人强化学习演示

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。陈建宇研究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。

该成果研究论文：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.



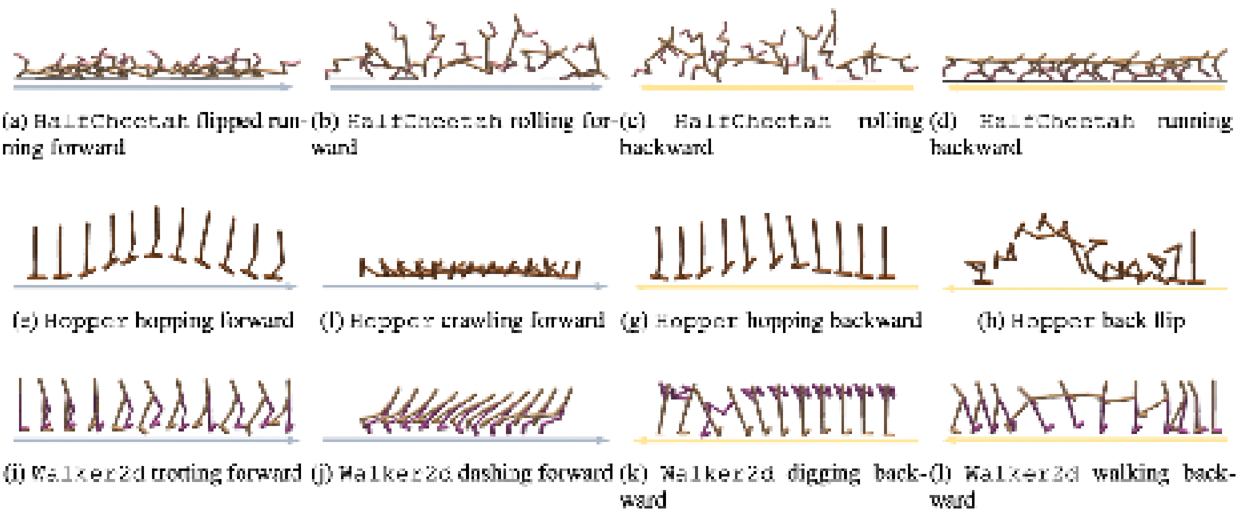
(a) One Context　(b) Markovian Contexts　(c) Our setting

基于分段语境的非静态环境问题

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。陈建宇研究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。

该成果研究论文：Z. Jiang, J. Gao and J. Chen, "Unsupervised Skill Discovery via Recurrent Skill Training", NeurIPS 2022.

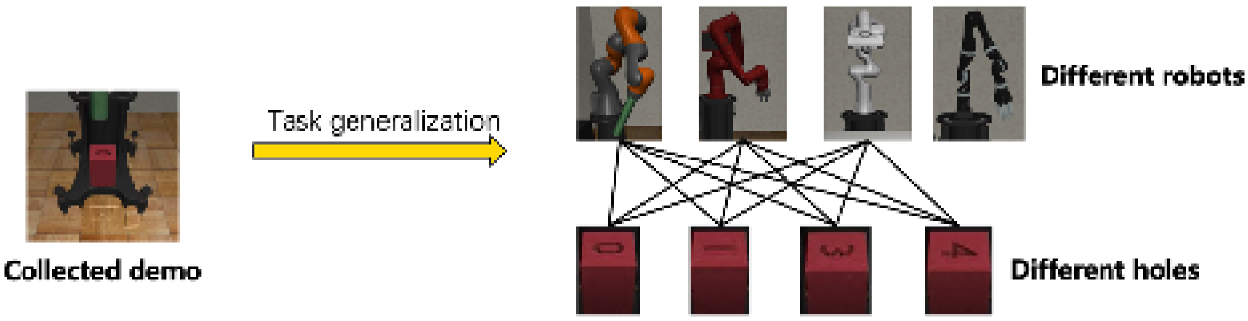


ReST 算法自主发现的多样性智能体技能展示

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。陈建宇研究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。

该成果研究论文：Y. Guo, J. Gao, Z. Wu and J. Chen, "Reinforcement Learning with Demonstrations from Mismatched Task under Sparse Reward", CoRL 2022.

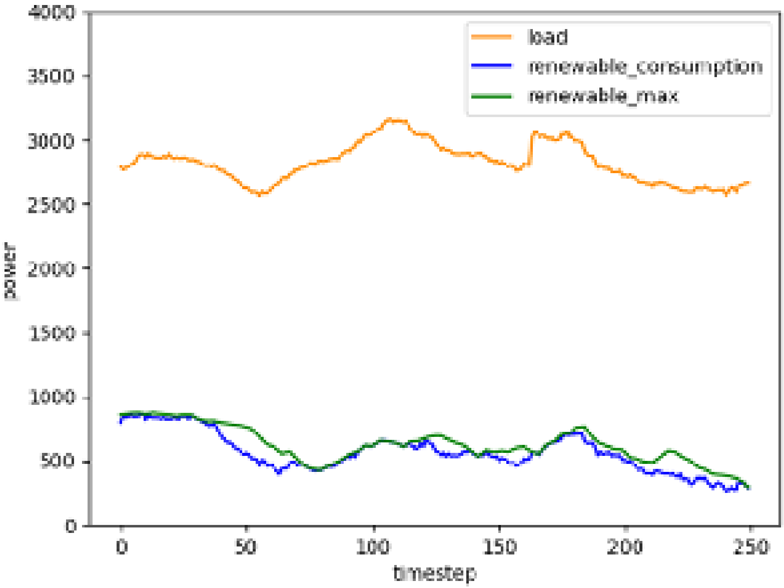


任务可迁移的演示强化学习

GridZero: 面向高比例可再生能源电网的实时调度算法

新型电力系统的调度优化一直是困扰电力行业的难题之一。随着风电光伏规模的不断扩大，以及超短期功率预测精度的提升，电力系统迫切需要一种实时滚动的优化方法，以适应新能源和负荷的快速波动。得益于电网中广泛部署的量测装置产生的海量数据，以及电力行业发展完备的仿真计算，基于数据驱动的深度强化学习算法为这一难题提供了解决方案。

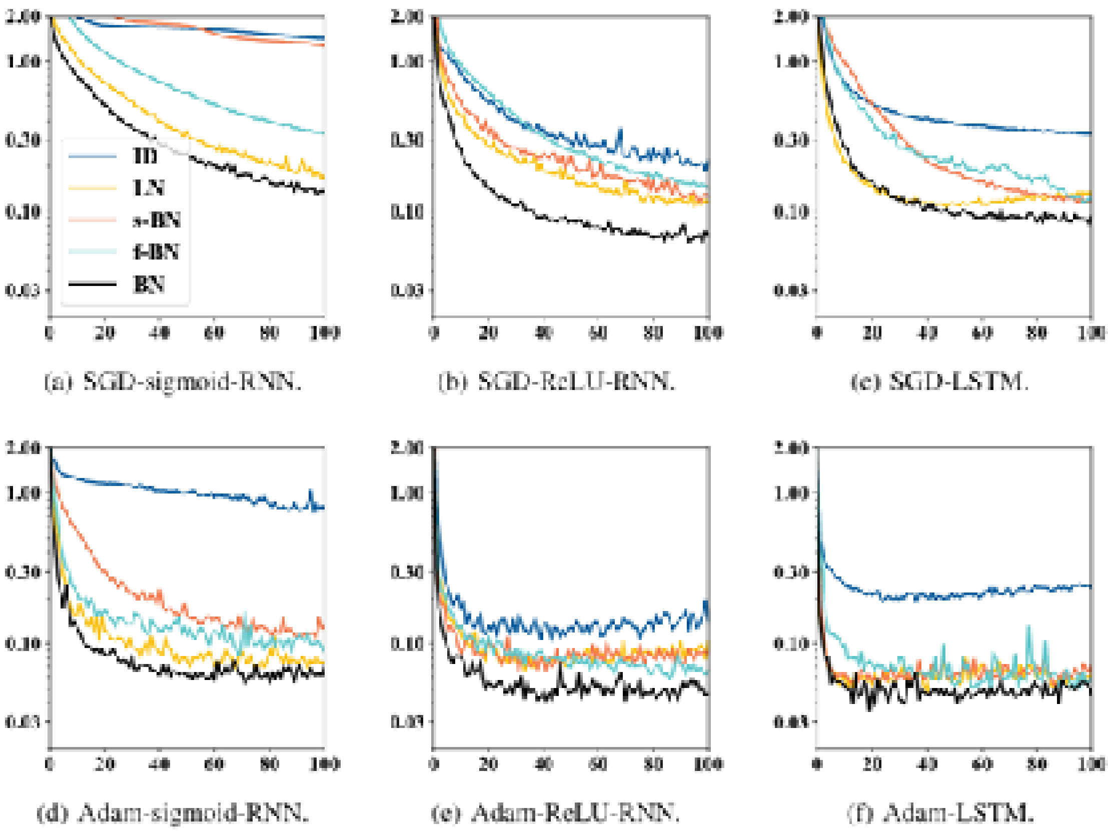
为了适应电力系统调度的复杂的动作空间和约束，高阳研究组在 EfficientZero 算法的基础上改进形成了 GridZero 算法。GridZero 通过融合连续和离散动作，同时解决新型电力系统的经济调度和机组组合问题。在完全不需要模仿人类调度员和传统求解器的基础上，GridZero 可以达到传统最优解 90% 的性能，并且做到求解速度与电网规模解耦。在全天的调度测试中，新能源消纳率达到 89.7%，这对今后可能的实际应用来说意义重大。



将批标准化应用于循环神经网络：通过 Delocalization 技术计算全时间步统计信息

批标准化 (batch normalization) 对小批次中每个单元的均值和方差进行归一化，显著减少了训练深度神经网络的难度，因此，批标准化被广泛应用于很多神经网络模型。然而，批标准化仍难以应用于循环神经网络 (recurrent neural network) ，因为循环神经网络在每个时间步的统计信息可能完全不同。高阳研究组提出了一种将批量归一化应用于循环神经网络的新方法，可以计算全部时间步的统计信息用于归一化。实验结果表明，新方法可以显著提高循环神经网络的收敛速度和精度。

该成果研究论文：Yunsheng Zhang, Yang Gao, “Applying Batch Normalization to Recurrent Neural Networkby Delocalization and Whole Time-step Statistics Calculation", submitted to NeurIPS 2022.



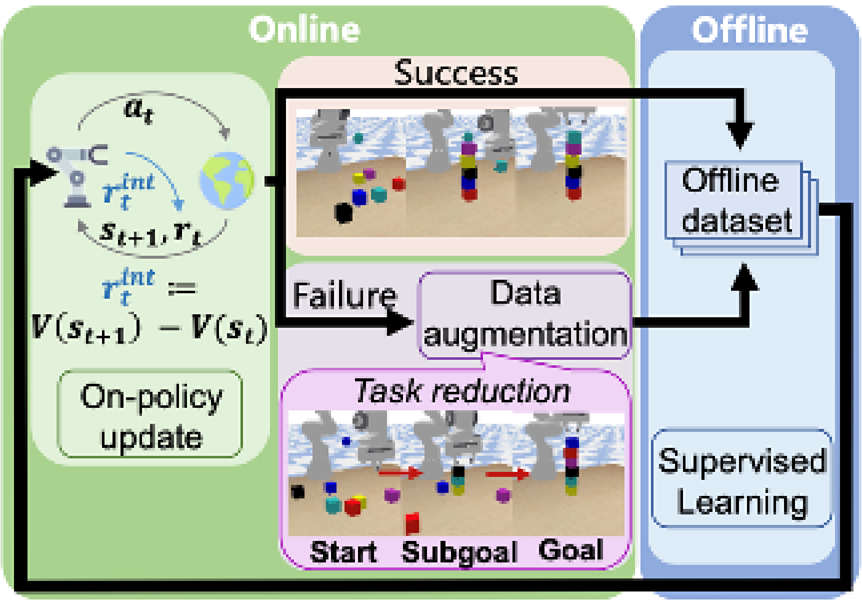
在 MNIST 数据集上与基线算法的对比，BN（黑线）为该文方法

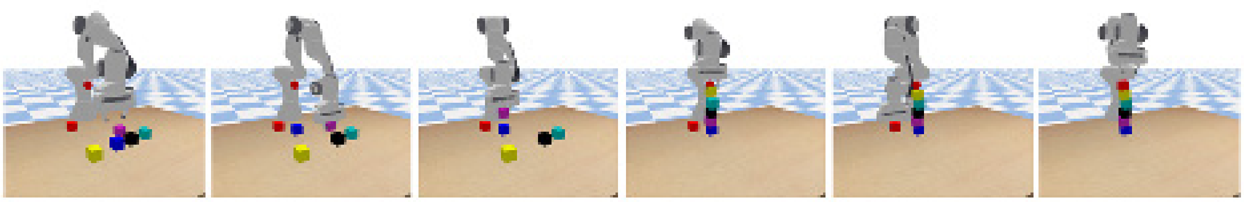
阶段化的自我归纳学习：一种高效的稀疏奖赏强化学习方法

近年来，深度强化学习在许多任务中都取得了惊人的突破，但由于其对超参数极为敏感，距离实际落地还有很大差距。相比之下，监督学习是一种更加稳定的学习范式，许多基础“大模型”正是监督学习的产物。吴翼研究组提出了一种结合两种范式的框架“PAIR”，通过自我归纳产生模仿学习数据，从而将监督学习引入强化学习，高效稳定地解决极具挑战性的稀疏奖赏强化学习问题。

该框架核心设计是交替进行在线和离线学习阶段：在线阶段智能体一边进行强化学习，一边收集用于离线学习的数据；离线阶段智能体在自己采集的数据中成功的轨迹上进行自我模仿学习。在线阶段还加入了自我归纳技术，让智能体把原本不会的困难任务分解成可以解决的简单的任务，大大扩充可用于离线学习的数据集。吴翼研究组还引入了基于值函数的内在奖赏来提升稀疏奖赏下的学习效率。PAIR 是目前已知的第一种在仅给代表成功与否的二值化奖励情况下，学会控制机械臂堆出六层高的积木塔的方法。

该成果研究论文： Yunfei Li, Tian Gao, Jiaqi Yang, Huazhe Xu and Yi Wu, "Phasic Self-Imitative Reduction for Sparse-Reward Goal-Conditioned Reinforcement Learning", ICML 2022.





重新验证合作性多智能体强化学习领域的设计原则

合作性多智能体强化学习领域的研究具有重大的实践意义，例如应用于交通控制、无人机编队、军棋推演等等。目前，此领域大部分表现优异的算法都基于两种典型的设计原则：参数共享（parameter sharing）和值分解（value decomposition）。

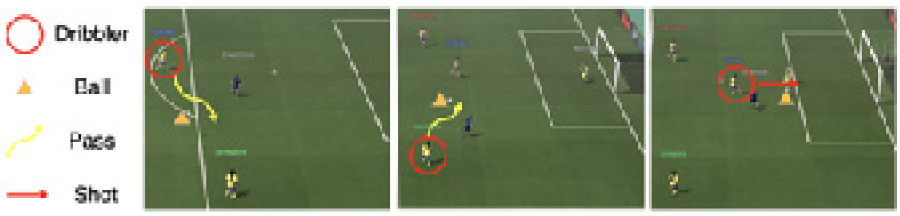
尽管这两个设计原则被广泛应用，然而吴翼研究组发现，这两个算法原则在策略表达能力上存在根本的局限性。吴翼研究组证明，如果对应任务的奖励函数多峰（multi-modal）并存在关联（correlated）的多个最优纳什均衡，则基于上述原则的算法无法表达任意最优解。与此对应的，独立的策略梯度（policy gradient）算法，尽管被广泛认为实际效果不佳，却能够被证明可以在这种多峰情形下稳定收敛到最优策略。

基于理论分析，吴翼研究组改进了多智能体策略梯度算法 MAPPO 并进一步提出了自回归（auto-regressive）策略表示，并在多个复杂多智能体环境，即星际争霸多和谷歌足球，中进行了测试。实验结果表明，基于策略梯度的算法表现能够在大部分环境中超越基于值分解的算法，并通过自回归的策略表示发现了需要复杂合作的智能行为。该研究能够为新一代多智能体强化学习算法的研究提供更深入的理解以及全新的思路。

该成果研究论文： Wei Fu, Chao Yu, Zelai Xu, Jiaqi Yang, and Yi Wu, "Revisiting Some Common Practices in Cooperative Multi-Agent Reinforcement Learning", ICML 2022.

Scenario	PG-ID	PG-Ind.	CDS(QMIX)	CDS(QPLEX)
3v1	**90.7(1.5)**	**90.2(1.7)**	73.7(3.4)	83.6(4.0)
CA(Easy)	79.5(6.7)	**92.4(2.6)**	43.0(5.6)	40.4(4.8)
CA(Hard)	**68.2(2.0)**	**67.8(3.4)**	35.4(2.9)	34.8(3.4)
Corner	**27.3(1.3)**	21.6(2.4)	1.8(0.3)	20.8(1.7)
PS	43.4(8.8)	53.3(3.5)	83.5(4.0)	**86.8(1.9)**
RPS	66.6(3.1)	**78.8(1.5)**	65.5(7.0)	75.1(2.4)

Map	PG-ID	PG-sh.	PG-Ind.	RODE
1c3s5z	**100.0(0.0)**	97.4(1.0)	99.1(0.7)	**100.0(0.0)**
2s3z	**100.0(0.7)**	99.0(0.5)	99.1(0.9)	**100.0(0.0)**
3s_vs_5z	**100.0(0.6)**	96.7(1.8)	93.8(1.8)	78.9(4.2)
3s5z	**96.9(0.7)**	95.2(1.5)	80.4(3.3)	93.8(2.0)
3s5z_vs_3s6z	84.4(34.0)	42.3(4.0)	37.8(5.6)	**96.8(25.1)**
5m_vs_6m	**89.1(2.5)**	35.3(2.1)	44.4(2.9)	71.1(9.2)
6h_vs_8z	**88.3(3.7)**	79.9(4.8)	11.4(2.5)	78.1(37.0)
10m_vs_11m	**96.9(4.8)**	86.5(2.3)	78.4(2.7)	95.3(2.2)
corridor	**100.0(1.2)**	92.6(2.4)	82.2(1.8)	65.6(32.1)
MMM2	90.6(2.8)	**92.3(1.9)**	13.0(3.7)	89.8(6.7)

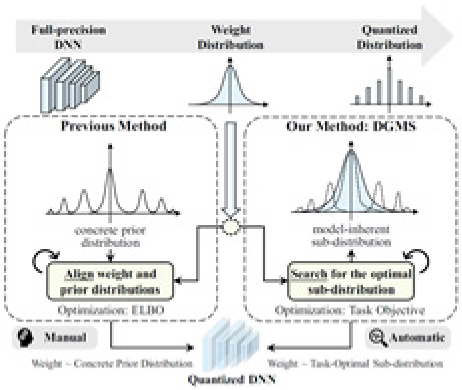


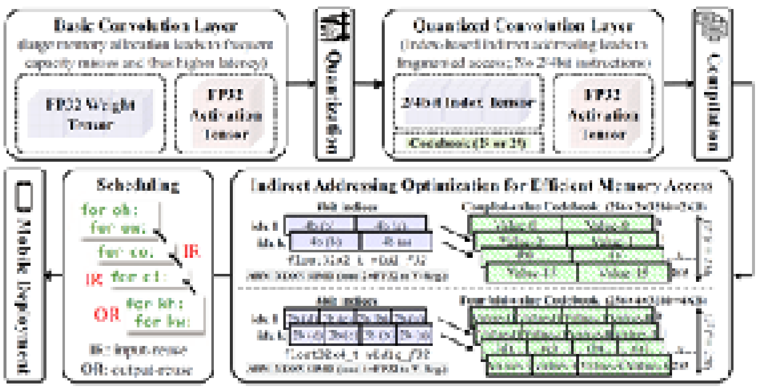
寻找量化神经网络的最优低比特子分布

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。

在该研究中，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, Kaisheng Ma, “Finding the Task-Optimal Low-Bit Sub-Distribution in Deep Neural Networks”, ICML 2022.



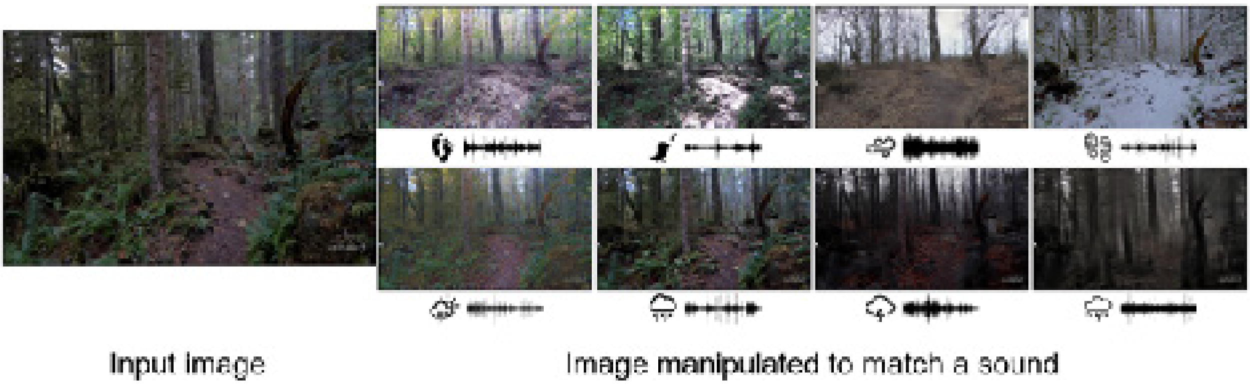


首次利用声音来控制图像风格变换

声音和图像是通过时间变化自然产生的两种模态。人们平时听到的声音往往能够传达一定的视觉信息，比如听见雨落下的滴答声，可以联想到阴天下雨的场景。

基于此，赵行研究组提出了一种自监督式的多模态风格变换模型，即可在无标注数据的情况下做到利用声音转换视觉场景的风格，并将该过程称为“声音驱动的图像风格变换”。给定一个视频（图像加声音）数据，该模型可以使用给出的声音来转变输入图像的风格，使之看起来与该声音相对应。比如输入是晴天的森林图像以及雨声，输出则是阴雨天的森林图像。除此之外，该研究组还发现了声音的属性可以影响生成图像的风格，例如调整声音的音量或将两个声音混合在一起会使图像的风格发生合理的变化——雨声越大会使生成的图像越阴暗、雨声与雪地脚步声混合会使生成的图像同时具备雨和雪的特征。主观和客观的实验结果表明，与一些经典的基于文字和图像标注的风格变换模型相比，该模型能够取得更好的生成效果。

该成果研究论文：Tingle Li, Yichen Liu, Andrew Owens, Hang Zhao, “Learning Visual Styles from Audio-Visual Associations", In submission to ECCV, 2022.

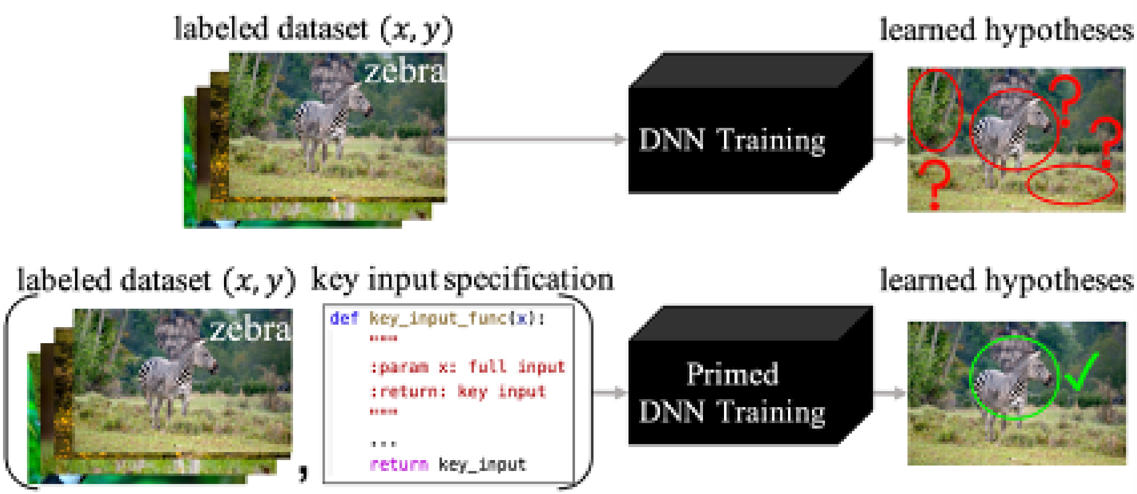


以毒攻毒：引导深度神经网络避免优化捷径

在监督学习的分类问题与序列决策问题中，基于深度学习的算法凭借优异的性能得到了广泛的关注与应用。然而，研究人员发现深度学习网络常常倾向于寻找“捷径”的解决方案。比如，在自动驾驶场景下，数据集中的专家动作往往具有高度的时序连贯性（即当前时刻是停车等待，则下一时刻也极大概率在停车等待），所以自动驾驶模型常常学到一种错误的捷径策略：简单地保持前一时刻的动作；在图像分类问题中，分类模型常常会错误地将背景的草地作为图片分类为牛的依据。当测试数据分布与训练集有稍许偏差时，这样的捷径解常常会出现灾难性的错误，比如当绿灯亮起时车辆仍然保持静止，当一个骆驼出现在草地上时会被误认为牛。

高阳研究组提出，为了使深度神经网络成功避免捷径方案，当人们可以根据输入信号中的关键成分提供一个额外的“引导”特征时，这个“引导”特征可以是一个对于输出目标的粗略估计。这样的“引导”是根据输入信号中与任务相关成分的领域知识而获得的，在实际应用中这样的领域知识非常容易定义与获取。比如，人们能够很清楚地意识到：在视觉模仿学习中，一段视频输入的当前帧是比其他的历史帧更为重要的；在图像分类中，图片的前景物体要比背景的像素对分类任务更加关键。

高阳研究组根据这样的原理提出了“引导网络”(PrimeNet)，在图像分类、机器人控制和自动驾驶任务中显著超过了现有的最优方法，成功缓解了深度神经网络对捷径解的倾向。并且，研究组在深度神经网络的优化角度为引导网络提供了理论保证，证明了引导特征通过为神经网络提供了一个正确的并且更简单的捷径来避免了错误的捷径方案。



以 PrimeNet 示意图

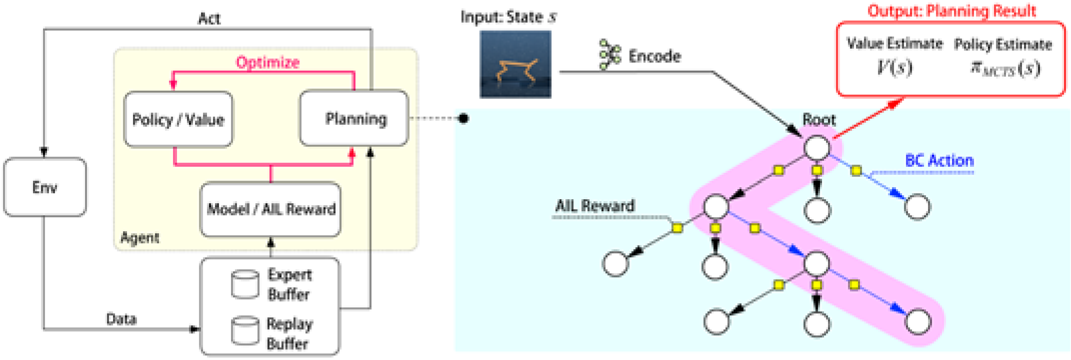
基于 MCTS 规划的高交互样本效率模仿学习

模仿学习是解决机器人控制问题的有效途径之一。然而，当下的模仿学习算法难以同时达到很高的表现性能和交互样本效率。这里，交互样本效率描述的是算法在学习时在环境中需要交互的次数。算法所需要的交互次数越少，则它的交互样本效率越高。一类模仿学习算法是行为克隆 (Behavioral Cloning)。行为克隆算法不需要在学习时和环境交互，因而有着最高的交互样本效率。但是，它却因为协变量漂移 (covariate shift) 的问题而难以取得令人满意的表现。另一类最近兴起的模仿学习算法是对抗模仿学习 (Adversarial Imitation Learning)。对抗模仿学习算法通过显式地鼓励算法将自身的长期行动轨迹和专家轨迹匹配，可以一定程度上避免了协变量漂移的问题，因此它能够取得比行为克隆算法更好的表现。不过，由于对抗模仿学习算法在学习时需要和环境大量交互采集样本，它的交互样本效率非常地低下，限制了它在现实中的应用。

因此，一个自然的研究问题便是如何设计一个兼具高表现性能和高样本效率的模仿学习算法。受到近期在高交互样本效率强化学习领域里 EfficientZero 算法的启发，高阳研究组提出了 EfficientImitate 算法来解决此问题。他们将对抗学习算法通过蒙特卡洛搜索树 (Monte Carlo Tree Search, MCTS) 规划来求解以显著提高其样本效率。与此同时，他们发现 MCTS 规划可以用一种新方式把行为克隆算法融合进来，从而能够促进学习时的探索，并进一步提高样本效率。该研究组还发现把融合行为克隆算法融入对抗模仿学习过程中对于例如类人 (Humanoid) 控制这类高难度控制问题十分关键。

高阳研究组使用 DMControl 基准，在基于状态输入和图像输入的模仿学习问题上评估了 EfficientImitate 算法的效果。在给定的交互样本数量上，EfficientImitate 算法取得的效果平均比之前最好的算法高 4 倍。尤其是在一些基于状态输入的任务上，它仅需要现实世界里约半小时不到的样本量便可完成学习。在未来，他们将继续研究把 EfficientImitate 直接运用在现实中的机器人控制上，以推动机器学习在机器人领域的发展。

该成果研究论文：Zhao-Heng Yin, Weirui Ye, Qifeng Chen, Yang Gao, “Planning for Sample Efficient Imitation Learning", submitted to NeurIPS 2022.



EfficientImitate 算法的示意图

二、计算机视觉

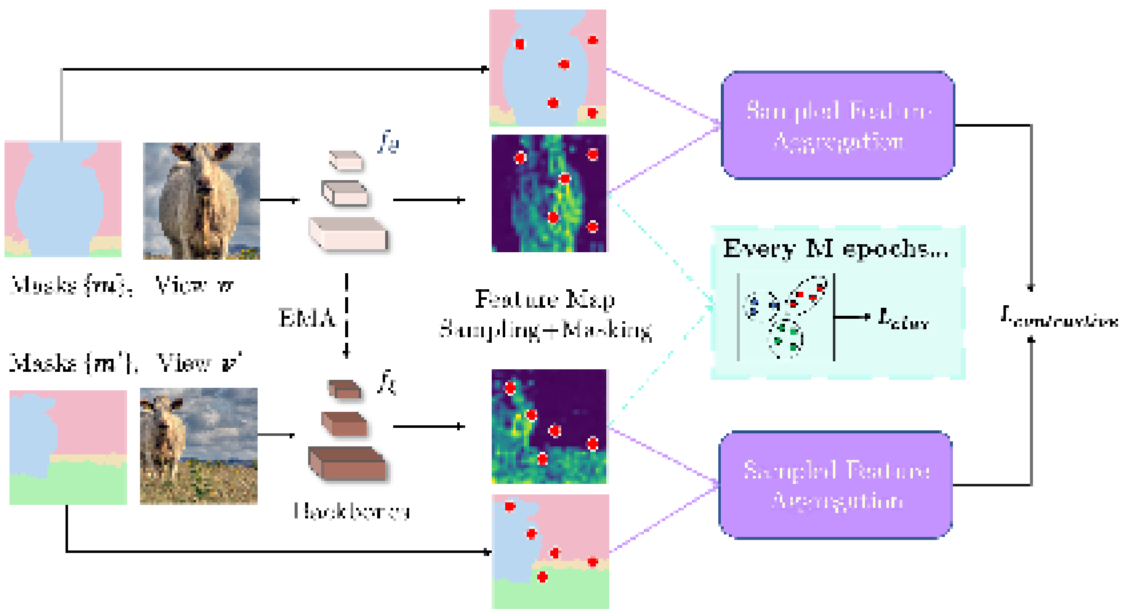
主要完成人：赵行研究组、高阳研究组、马恺声研究组

对比表征和物体分割的自监督联合学习

最近几年，对比学习已成为一种自监督学习视觉表征的重要方法。之前的很多工作比如 SimCLR 和 MoCo 都只在 ImageNet 上做预训练。ImageNet 中的图像大多都是“以物体为中心”，即一张图像中包含一个占据主体的前景物体。但是现实世界中的图像很多是包含多个物体的复杂场景图像，在这种图像上用对比学习会有一个严重问题：随机裁剪（对比学习中常用的数据增强方法）会有很大概率将两个语义不同的物体作为正样本。所以常见的对比学习算法都还无法在复杂场景数据中学习到非常有效的视觉表征。

高阳和赵行研究组提出了改进算法 CYBORGS。新算法利用物体分割图将场景图像中语义相同的物体作为正样本，解决了上述的正样本语义不一致的问题。在更好的视觉表征的基础上，CYBORGS 又能通过对表征进行聚类来获得更准确的物体分割图。两个阶段不断交替进行，并且相辅相成，最终实现在复杂场景数据中学习到物体分割图和有效的视觉表征。该视觉表征可以迁移到众多的下游任务中，比如在物体识别，目标检测，物体分割中，CYBORGS 都获得了很大的性能提升。

该成果研究论文：Renhao Wang, Hang Zhao, Yang Gao, "CYBORGS: Contrastively Bootstrapping Object Representations via Grounding in Segmentation", submitted to ECCV 2022.



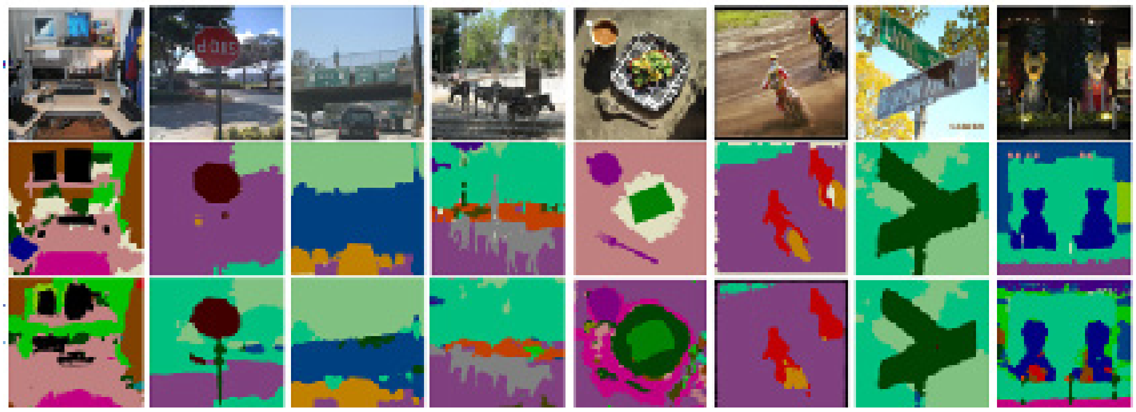
无监督预训练多尺度编码解码结构的视觉 Transformer 结构在语义分割的应用

在视觉模型预训练中，无监督预训练成为目前更为主流的预训练方式。相比于受限于有标注数据集的有监督预训练，无监督预训练能使模型在大规模数据集上具有更好的泛化性，并且无需依赖文本标注的监督信号。前期研究工作也证明无监督的预训练模型在下游的目标检测、物体识别、物体分割等任务中均有出色的表现。使得无监督预训练模型正逐渐替代有监督预训练模型成为下游任务特征提取的骨干网络。

然而对于像素密集预测的无监督预训练中，当前主流的无监督模型忽略了像素级语义的问题，即在结构上由于卷积网络下采样阶段 /Vision Transformer 的线性变换阶段造成图像空间信息丢失，导致在下游任务中无法保证高级语义信息在细粒度上与原图匹配。针对该问题，高阳研究组发现多层级的特征学习和高分辨语义信息重建能有效解决细粒度问题。并在自蒸馏方法的基础上提出了多尺度编码解码结构的视觉 Transformer(Multi-scale Encoder-decoder Vision Transformer)，简称 MEVT。

在多层级 Transformer 结构的基础上，MEVT 提出了多层级的局部注意力和全局注意力的模型。与常见多层级网络不同，MEVT 增加了全局注意力在学习高级信息阶段的应用层数以增强对应像素令牌对于全局信息的融合。与此同时，MEVT 通过从低分辨率的高级语义特征拓展上采样 / 还原合并和局部 / 全局注意力模块重建高分辨率的高级语义特征，并且通过直接连接重建原始图像空间信息。通过自蒸馏训练在编码解码器结构的像素密集一致性，使得该多层级结构能更好学到细粒度表征，进一步提升在下游分割任务中的表现性能。如下图中仅通过无监督预训练便能分割出较为完整的物理轮廓。该方法也为之后的其他拓展的下游任务提供关键的细粒度语义表征。

该成果研究论文：Xianfan Gu, Yingdong Hu, Yang Gao, "Unsupervised Pre-Training of Multi-scale Encoder-decoder Vision Transformer for Semantic Segmentation", submitted to ECCV 2022.



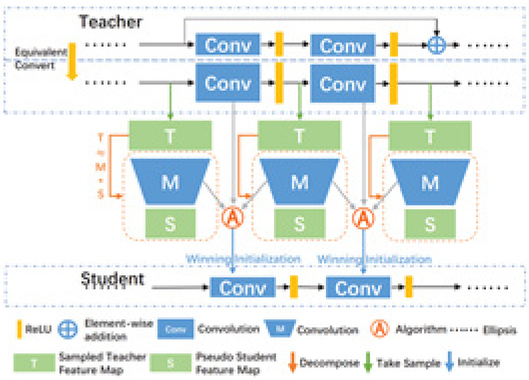
在 COCO 数据集生成的分割结果 (原图 (上), 标签结果 (中)，MEVT 生成结果 (下))

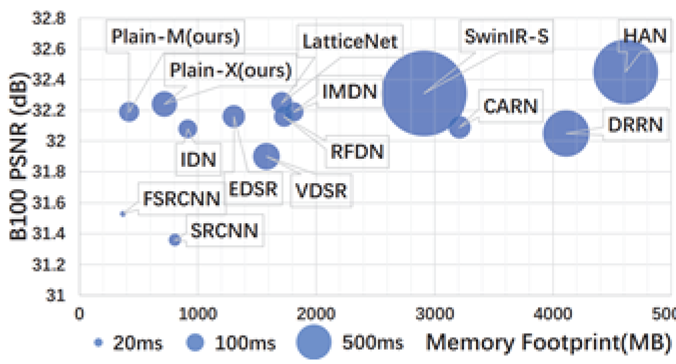
首次将多分支超分辨率模型在转化为无分支朴素模型并获得相同性能和更低显存需求

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。该文章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，他们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，马恺声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：Wu, Kailu, Chung-Kuei Lee, and Kaisheng Ma, "MemSR: Training Memory-efficient Lightweight Model for Image Super-Resolution", ICML 2022.



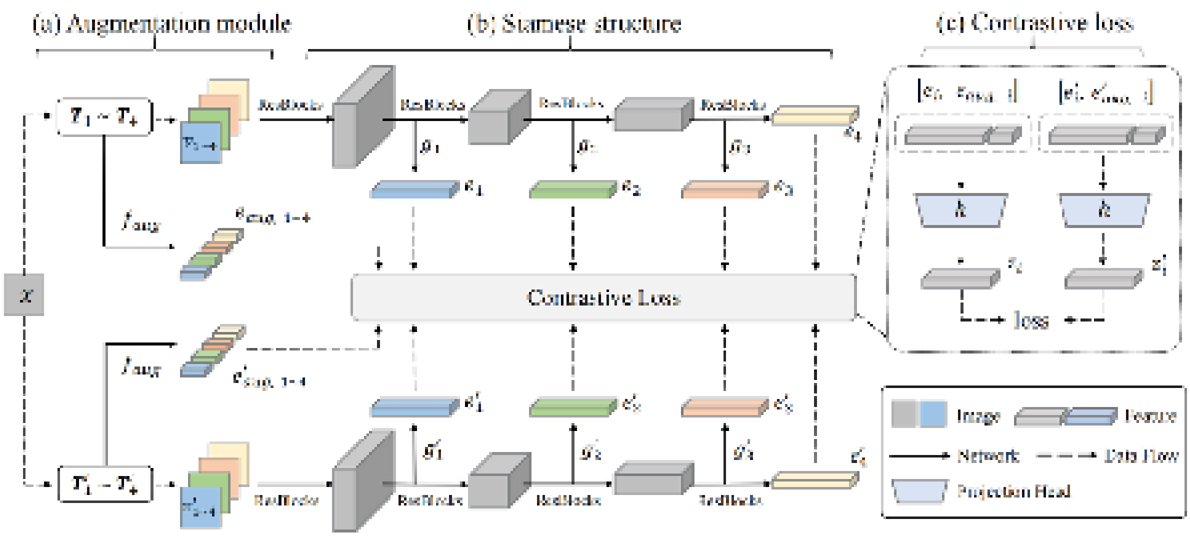


改善对比学习算法中预先设定数据增强种类和强度带来的缺陷

近年来，对比学习算法被证明在自监督视觉表征学习中具有极大的潜力。而数据增强模块是对比学习算法中不可或缺的环节，是模型能够学到有意义视觉表征的基本保证。现有的对比学习算法往往采用预先设定的数据增强种类和强度，马恺声研究组认为这样的范式会对模型的训练产生两方面缺陷。首先，不同种类的数据增强对对比学习效果的影响有很大差别，并且针对不同下游任务的影响也不同，因此在训练时同等地对待每种数据增强无法保证学到最优的数据表征。其次，对比学习中惯常使用的强数据增强方式会给模型带来不必要的表征不变性，并导致细粒度类别相关信息的损失。

针对这两方面缺陷，马恺声研究组首先提出在模型的不同阶段构建多个数据增强样本和对比学习损失，让模型学习层次化的表征不变性；其次，马恺声研究组提出对每个样本特征附加上其使用的数据增强参数的特征编码，在对比学习过程中促进数据增强相关的信息在视觉表征中的保留。该算法可以和当前主流的对比学习算法相结合，在图像分类、检测、分割任务的多个数据集上显著提升了模型表征学习的效果，为对比学习算法中数据增强种类和强度的选择提供了更大的灵活性。

该成果研究论文：Junbo Zhang, Kaisheng Ma, "Rethinking the Augmentation Module in Contrastive Learning: Learning Hierarchical Augmentation Invariance with Expanded Views", CVPR 2022.

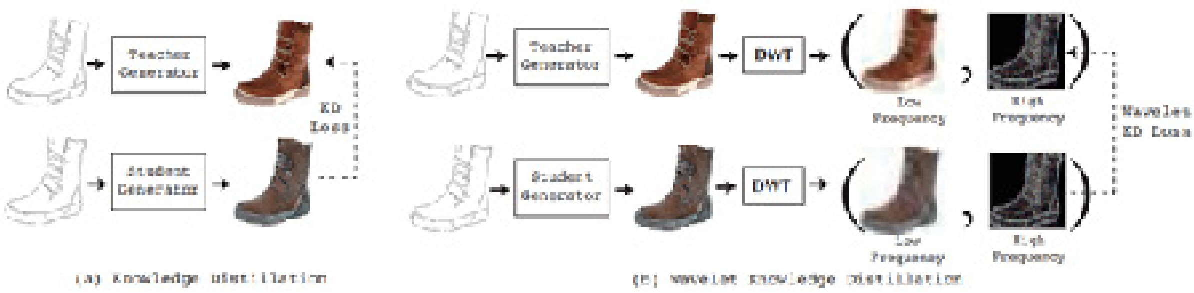


通过小波知识蒸馏实现高效的图像翻译

近年来，随着对抗生成神经网络的发展，图像到图像翻译任务的性能取得了不断的突破，并在许多现实世界应用中得到部署，例如各类直播软件中的美颜功能、图像动漫化功能等。然而，由于对抗生成神经网络往往具有海量的计算量和参数量，这些模型的计算速度较慢，无法实时的在手机等边缘设备上运行，限制了这一技术的广泛应用。

为解决这一问题，马恺声研究组提出了一种基于离散小波变换的知识蒸馏算法，对图像到图像翻译模型进行压缩。他们研究发现，较大的图像翻译模型和较小的图像翻译模型对于图像的低频信息部分都有比较好的生成效果。与大模型相比，小的图像翻译模型在高频信息的生成上表现不佳。因此，他们高频信息为切入点，通过离散小波变换提取不同模型在高频信息的生成结果，通过知识蒸馏的方式提高小模型在高频信息上的表现。相关论文发表在 CVPR2022 会议上。

该成果研究论文：Linfeng Zhang, Xin Chen, Xiaobing Tu, Pengfei Wan, Ning Xu, Kaisheng Ma, "Wavelet Knowledge Distillation: Towards Efficient Image-to-Image Translation", CVPR 2022.



三、自然语言处理

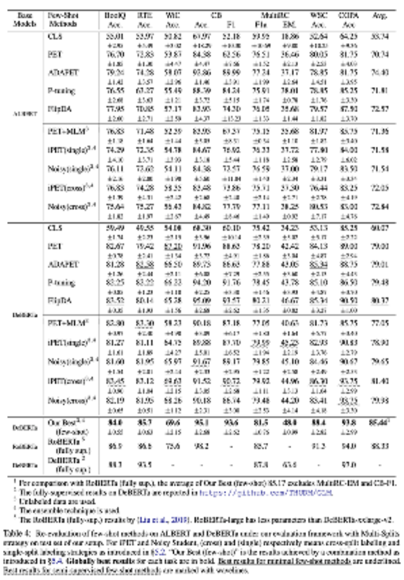
主要完成人：杨植麟研究组、李建研究组

清华大学联合 CMU、Google 等机构学者首次提出小样本自然语言理解评价基准，揭示小样本自然语言理解研究发展现状

以 GPT-3 为代表的预训练语言模型展示出强大的小样本学习能力，仅使用少量标签数据即可快速学习新的自然语言理解 (Natural Language Understanding, NLU) 任务并取得良好性能。然而该领域的现状是，尚缺乏一个标准的评价准则；小样本学习高方差不稳定的特点为其客观评价基准的提出进一步带来严峻挑战。已有的各种相关研究工作采取各不相同的评价方式， 导致它们或者面临高估真实性能的风险（超参数选择是在既往经验中观测了测试集性能的结果）；或者对于多种因素敏感导致严重性能评价偏差。

针对小样本自然语言理解领域这一严峻挑战，杨植麟研究组首次提出一个新的小样本自然语言理解评价框架 FewNLU，并且从三个关键方面（即测试集小样本学习性能、测试集和验证集相关性、以及稳定性）量化评估该评价准则的优势。基于该基准对大量已有前沿工作的再评估结果（如图所示）表明：现有多数小样本学习方法的真实性能提升有限，小样本自然语言理解领域发展依然面临着严峻的挑战！此外 FewNLU 还揭示：已有工作未准确估计现有小样本学习方法的绝对性能和相对差距；目前尚不存在单一的能够在多数 NLU 任务均取得优势性能的方法；不同方法的增益是优势互补的，最佳组合模型的性能接近于全监督 NLU 系统等关键结论。FewNLU 研究成果的提出是对小样本自然语言理解评价的修正、改进和统一，对于促进该领域未来研究的快速发展具有重要意义。该工作已发表于 ACL’22 主会。

该成果研究论文：Yanan Zheng, Jing Zhou, Yujie Qian, Ming Ding, Chonghua Liao, Li Jian, Ruslan Salakhutdinov, Jie Tang, Sebastian Ruder, Zhilin Yang, "FewNLU: Benchmarking State-of-the-Art Methods for Few-Shot Natural Language Understanding", ACL (1) 2022: 501-516.



通过标签翻转实现高效且鲁棒的小样本数据增广

数据增广是通过自动生成新的训练数据来提升模型性能的方法，被广泛应用于自然语言理解任务。目前已有的多种数据增广方法大多基于难度较低的简单问题设置。该研究工作指出，将数据增广应用于难度更高的任务以及更强的基线模型时，现有数据增广方法在该极限问题场景下均全部失效，并陷入 " 故障模式 (Failure Modes)"。

针对数据增广方法在高难度任务 (例如：小样本自然语言理解任务) 以及更强的基线模型 (例如：超过 1 亿参数量的大规模预训练模型) 条件下的 " 故障模式 (Failure Modes)" 问题，杨植麟研究组提出一项研究工作 FlipDA 进行有效的数据增广。通过自动化的标签反转数据增广，FlipDA 进一步提升小样本泛化性能，进而实现了更大幅度更稳健的性能提升，有效避免“故障模式”的发生；FlipDA 对于推动大规模模型在实际应用场景中有效实践，同时保证稳健的性能提升具有重要意义。该工作已发表于 ACL’22 主会。

该成果研究论文：Jing Zhou, Yanan Zheng, Jie Tang, Li Jian, Zhilin Yang, "FlipDA: Effective and Robust Data Augmentation for Few-Shot Learning", ACL (1) 2022: 8646-8665.

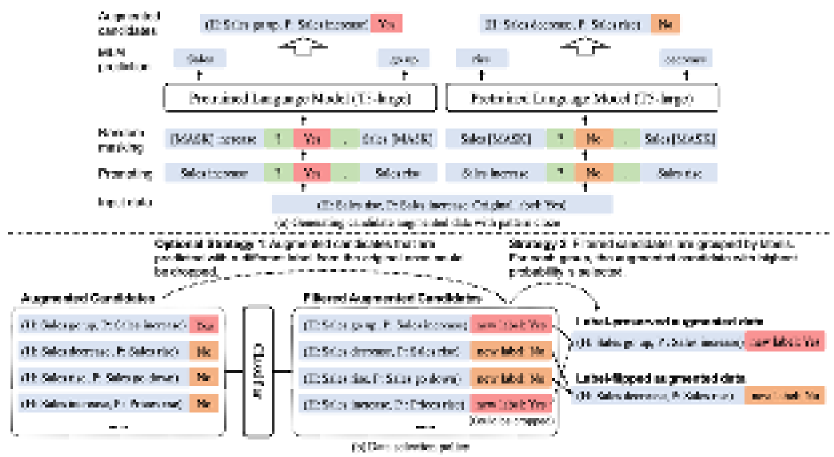


Figure 1: An illustration of (a) our prompt-based augmentation algorithm for both preserved/flipped labeled data, and (b) our data selection policy. Whether to use Strategy 1 depends on the relative power of the augmentation model and the classification model. If the augmentation model is accurate enough, drop the candidates with inconsistent labels, and otherwise, keep it.

首次提出一种通用预训练框架 —— 一切自然语言处理任务皆生成任务

目前预训练架构有多种不同类型，包括自编码模型 (例如 BERT)、自回归模型 (例如 GPT)、以及编码器 - 解码器模型 (例如 T5)。然而，到目前为止尚没有一个预训练框架能够实现同时在自然语言理解、无条件生成、以及有条件生成三类重要类别任务上表现最佳。这意味着目前预训练技术距离“通用”的目标尚存在一定距离。

该工作首次提出一种基于自回归空白填充的通用语言模型 (General Language Model, GLM)。GLM 增加了 2D 位置编码，并允许以任意顺序预测 span，这使其在自然语言理解任务上的性能优于 BERT 和 T5。此外 GLM 还可以通过改变空白的数量和长度，针对不同类型的任务对 GLM 进行预训练。实验表明，在自然语言理解、条件和无条件生成的三种类型任务上，在相同模型大小和数据情况下，GLM 优于 BERT、T5 和 GPT；并且在单一预训练模型 (参数规模仅 BERT-Large 的 1.25 倍) 上实现了最佳性能。该工作对进一步推进预训练技术实现更强的通用和泛化能力具有重要意义。该工作已发表于 ACL’22 主会。

该成果研究论文：Zhengxiao Du, Yujie Qian, Xiao Liu, Ming Ding, Jiezhong Qiu, Zhilin Yang, Jie Tang, "GLM: General Language Model Pretraining with Autoregressive Blank Infilling", ACL (1) 2022: 320-335.

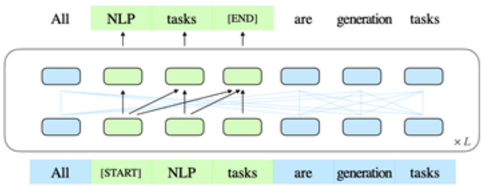


Figure 1: Illustration of GLM. We blank out text spans (green part) and generate them autoregressively. (Some attention edges are omitted; cf. Figure 2.)

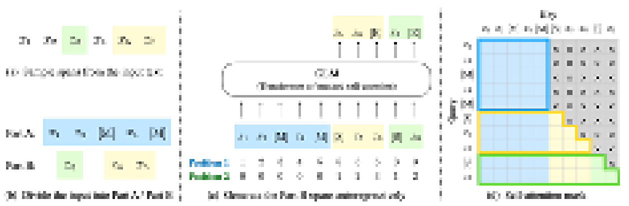


Figure 2: GLM pretraining. (a) The original text is $[x_1, x_2, x_3, x_4, x_5, x_6]$. Two spans $[x_3]$ and $[x_5, x_6]$ are sampled. (b) Replace the sampled spans with [M] in Part A, and shuffle the spans in Part B. (c) GLM autoregressively generates Part B. Each span is prepended with [S] as input and appended with [E] as output. 2D positional encoding represents inter- and intra-span positions. (d) Self-attention mask. Grey areas are masked out. Part A tokens can attend to themselves (blue frame) but not B. Part B tokens can attend to A and their antecedents in B (yellow and green frames correspond to the two spans). [M] := [MASK], [S] := [START], and [E] := [END].

首次实现了在多种模型规模以及多种任务上，参数高效的提示调优技术达至和标准微调相当的结果

提示调优技术是基于参数冻结的预训练语言模型对一组连续向量的提示表示进行优化调整，从而实现预训练语言模型在下游任务良好性能；它可以极大减少训练时每个任务的存储和内存的使用量，从而实现更高效率。然而，已有工作表明，在目前的自然语言理解的任务上，提示调优技术表现效果不佳，远不及标准微调技术；此外现有快速微调方法无法处理序列标记任务，即缺乏对下游任务普遍兼容性。这导致提示微调技术无法在实际的应用场景中发挥其优势。

为了应对这一挑战，该研究工作基于经验发现提出，适当优化的提示调优技术 P-Tuning v2 可以在多种不同模型规模以及多种不同任务上普遍有效（如下图所示）；它通过优化 0.1%-3% 的参数即实现和标准微调相匹配的性能。P-Tuning v2 的在多种模型规模以及任务类型上的普遍适配特性，以及简单易用和节省显存等优势，使其有潜力作为标准微调的替代方案和未来研究的强大基线。该工作已发表于 ACL’22 主会。

该成果研究论文：TXiao Liu, Kaixuan Ji, Yicheng Fu, Zhengxiao Du, Zhilin Yang, Jie Tang, "P-Tuning v2: Prompt Tuning Can Be Comparable to Fine-tuning Universally Across Scales and Tasks", CoRR abs/2110.07602 (2021).

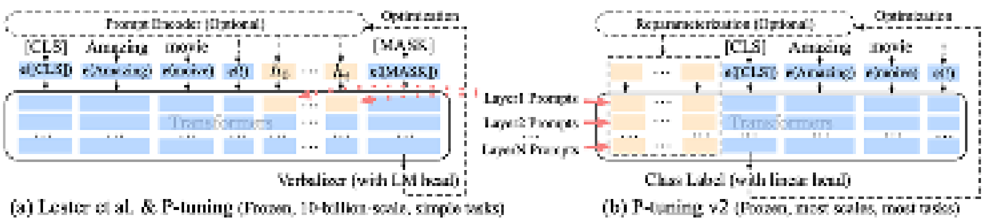


Figure 2: From Lester et al. (2021) & P-tuning to P-tuning v2. Orange blocks (i.e., $h_0, ..., h_i$) refer to trainable prompt embeddings; blue blocks are embeddings stored or computed by frozen pre-trained language models.

Figure 1: Average scores on RTE, BoolQ and CB of SuperGLUE dev. With 0.1% task-specific parameters, P-tuning v2 can match fine-tuning across wide scales of pre-trained models, while Lester et al. (2021) & P-tuning can make it conditionally at 10B scale.

Method	Task	Re-param.	Deep PT	Multi-task	No verb.
P-tuning (Liu et al., 2021)	KP NLU	LSTM	-	-	-
PromptTuning (Lester et al., 2021)	NLU	-	-	✓	-
Prefix Tuning (Li and Liang, 2021)	NLG	MLP	✓	-	-
Soft Prompts (Qin and Eisner, 2021)	KP	-	✓	-	-
P-tuning v2 (Ours)	NLU SeqTag	*(depends)*	✓	✓	✓

Table 1: Conceptual comparison between P-tuning v2 and existing Prompt Tuning approaches (KP: Knowledge Probe; SeqTag: Sequence Tagging; Re-param.: Reparameterization; No verb.: No verbalizer).

首次提出无需预训练的高效 NLP 学习框架：1% 算力 +1% 语料即可比肩预训练语言模型

预训练语言模型因其强大的性能被广泛关注。基于预训练 - 微调 (Pretraining-Finetuning) 的范式也已经成为许多 NLP 任务的标准方法。然而，当前通用语言模型的预训练成本极其高昂，这使得只有少数资源充足的研究机构或者组织能够对其展开探索。这种“昂贵而集权”的研究模式限制了平民研究者们为 NLP 社区做出贡献的边界，甚至为该领域的长期发展带来了障碍。

杨植麟研究组首次提出一种完全不需要预训练语言模型的高效学习框架：任务驱动的语言建模 (TLM, Task-driven Language Modeling)。这一框架从通用语料中筛选出与下游任务相关的子集，并将语言建模任务与下游任务进行联合训练（如左图所示）。相较于传统的预训练模型（例如 RoBERTa），TLM 仅需要约 1% 的训练时间与 1% 的语料，即可在众多 NLP 任务上比肩甚至超出预训练模型的性能（如右图所示）。作为这一领域的一项突破性进展， TLM 的提出具有重要意义，它引发更多对现有预训练微调范式的思考，并进一步推动 NLP 民主化的进程。

该成果研究论文：Xingcheng Yao, Yanan Zheng, Xiaocong Yang, Zhilin Yang, "From Scratch Without Large-Scale Pretraining: A Simple and Efficient Framework", CoRRabs/2111.04130 (2021).

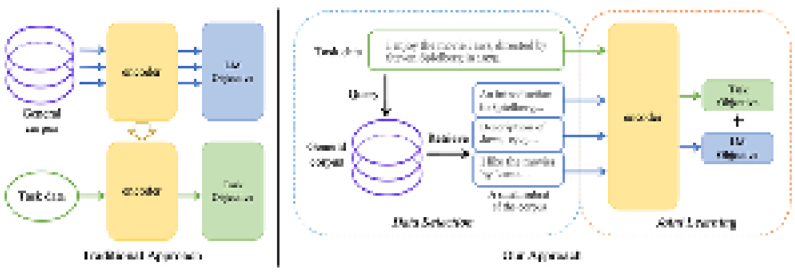


Figure 2: Comparison between the traditional pretraining-finetuning approach and our proposed framework TLM: instead of training a language model over the entire general corpus and then finetuning it on task data, we first use task data as queries to retrieve a tiny subset of the general corpus, and then perform joint learning on both the task objective and self-supervised language modeling objective.

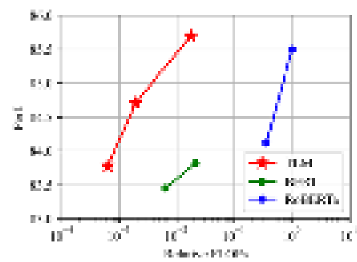


Figure 1: Average performance on eight tasks v.s. relative FLOPs w.r.t. RoBERTa-Large (Liu et al., 2019). TLM slightly outperforms RoBERTa-Large while reducing FLOPs by two orders of magnitude.

四、自动驾驶

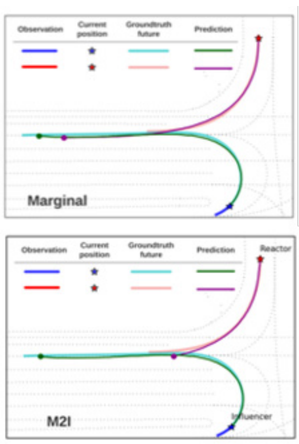
主要完成人：赵行研究组、陈建宇研究组

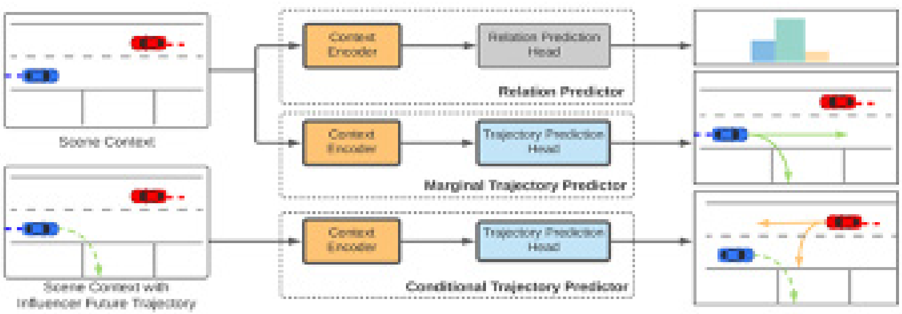
首次提出通过预测车辆间关系进行多车交互式轨迹预测

轨迹预测是自动驾驶系统中的重要模块，负责预测车辆行驶时周围其他车辆或行人未来可能作出的行为。轨迹预测的结果一般被用于下游的规划系统来避免自动驾驶车辆与其他车辆或行人发生碰撞。近年来，相关研究大多从大型的真实道路上提前采集的数据集上使用深度学习去建模其他车辆或行人的行为模式来进行轨迹预测。之前的方法在预测多车轨迹时，轨迹通常是每辆车单独预测，预测结果中的轨迹会出现互相交叉等情况损害场景级别上的预测精度。

作为轨迹预测和自动驾驶领域的一项重要突破，赵行研究组首次提出运用车辆之间的关系进行联合轨迹预测 (Joint Prediction) 的方法 M2I。M2I 可以通过自动标注为数据集中的场景精准地标注车辆间的关系以便作为样本进行训练。训练之后的模型可以准确预测车辆间的交互关系，判断冲突中哪一方先行，哪一方让行，并利用此关系分别预测先行车辆的轨迹，再运用先行车辆的预测结果进一步预测让行车辆的轨迹，以做到预测轨迹之间的一致性从而提升预测精度。实验结果表明，M2I 预测效果超过其他直接预测的方法，并成功刷新了在面向全球该领域学者的 Waymo 交互式轨迹预测 (Interactive Motion Prediction) 挑战上的最佳结果。

该成果研究论文：Qiao Sun, Xin Huang, Junru Gu, Brian C. Williams, Hang Zhao, "M2I: From Factored Marginal Trajectory Prediction to Interactive Prediction", CVPR 2022.



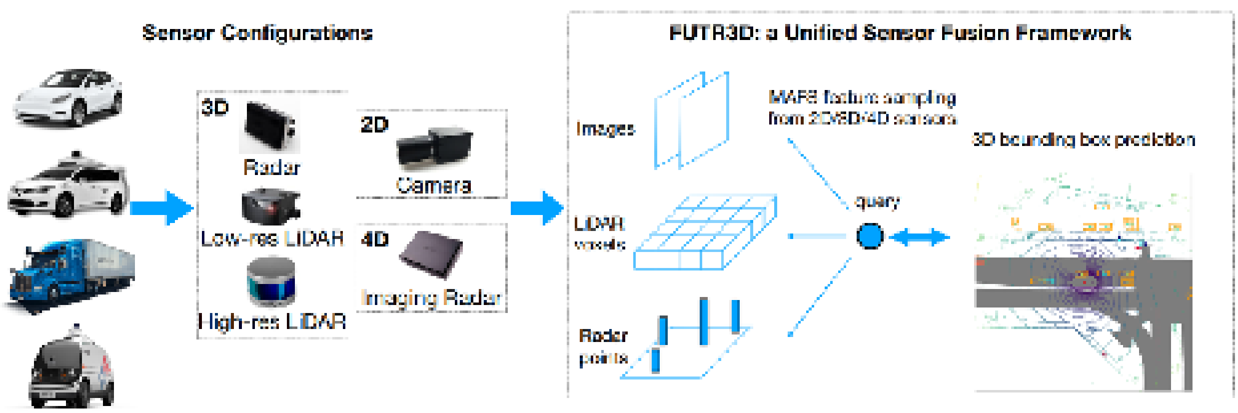


BEV 下统一通用的多传感器融合目标检测框架

在自动驾驶中如何去有效地融合各个不同传感器，如相机、激光雷达、毫米波雷达等，去准确地感知周围的场景是一个关键的问题。在多模态目标检测中，之前的工作主要聚焦于如何针对特定的输入传感器组合去设计专门的算法来融合信息，在实际应用中有其局限性。

赵行研究组首次提出了端到端且统一通用的多传感器融合目标检测 FUTR3D。FUTR3D 中以 3D Object Query 为中心，基于不同传感器的物理特性对不同模态不同网络骨干提取出的模态特征进行采样，投影到统一的隐空间中，并直接在三维空间中得到预测结果。FUTR3D 不仅能应用于各种不同的传感器组合，并且在各个模态组合的情况下都能实现领先结果，能持平或超过针对特定组合设计的算法，有着很强的灵活性和实用性。另外在相机和 4 线激光雷达组合的情况下能够超过 32 线激光雷达的方法，能极大地促使未来低成本的移动感知系统的发展。

该成果研究论文：Xuanyao Chen, Tianyuan Zhang, Yue Wang, Yilun Wang, Hang Zhao, "FUTR3D: A Unified Sensor Fusion Framework for 3D Detection", arXiv:2203.10642.

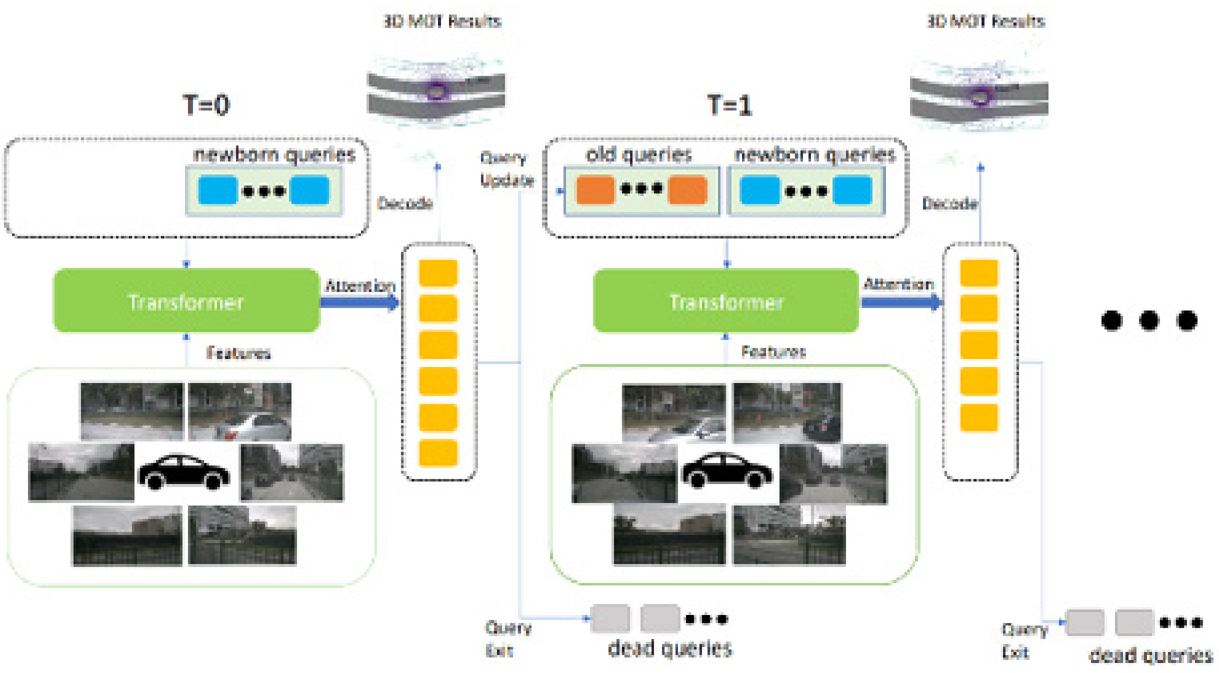


BEV 下的多相机多目标跟踪框架

在自动驾驶中，通常会配备多个摄像机，如何能够在繁杂的场景中融合各个相机的信息去做多目标的跟踪是一个很关键且困难的事情。在多相机多目标跟踪中，传统的做法通常分为两阶段，先对每帧图像做目标检测，再根据检测结果之间的相关性做关联。

赵行研究组首次提出了端到端的多相机多目标跟踪框架 MUTR3D，对该领域做出了突破性的成果。为了解决多相机之间信息交融以及第二阶段目标关联的问题，MUTR3D 中以 3D Track Query 为核心，隐式地表达物体的空间形状信息，直接在三维空间中去预测整一串的目标跟踪结果。对于每一帧，每个 Track Query 会解码为一个 3D 目标检测框，对多相机进行特征采集去更新跟踪结果，并且由于同个 Query 在不同帧预测出的检测框是天然联系在一起的，这样就能实现端到端多相机多目标的跟踪，避免了两阶段的实现。MUTR3D 在自动驾驶的数据集 nuScenes 上实现了 SOTA 的结果，体现了该方法的优越性。

该成果研究论文：Tianyuan Zhang, Xuanyao Chen, Yue Wang, Yilun Wang, Hang Zhao, "MUTR3D: A Multi-camera Tracking Framework via 3D-to-2D Queries", arXiv:2205.00613.

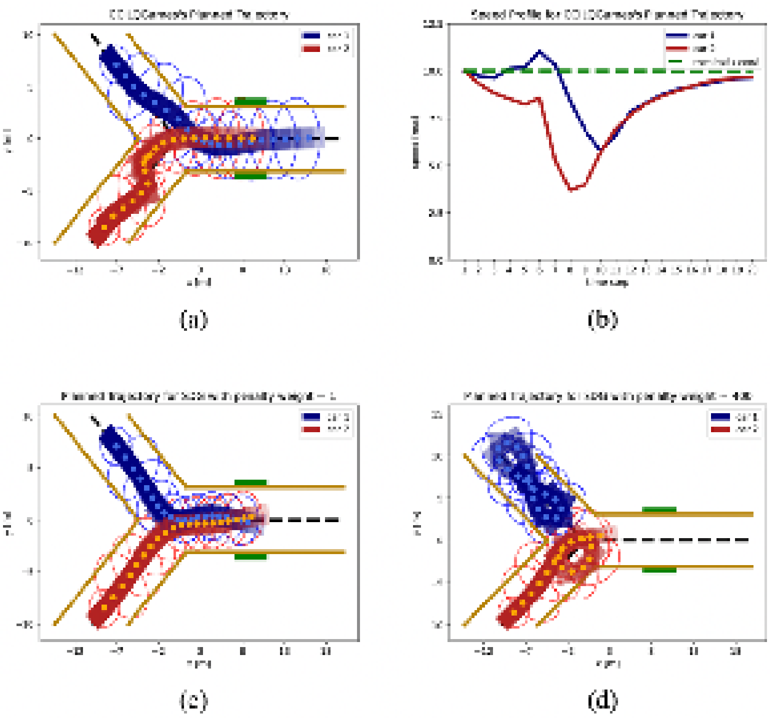


概率安全约束下的迭代线性二次型随机博弈

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。

陈建宇研究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。

该成果研究论文：H. Zhong, Y. Shimizu and J. Chen, "Chance-Constrained Iterative Linear-Quadratic Stochastic Games", IROS 2022.



CCILQG 方法应用于无人车交互博弈决策场景

五、计算生物学

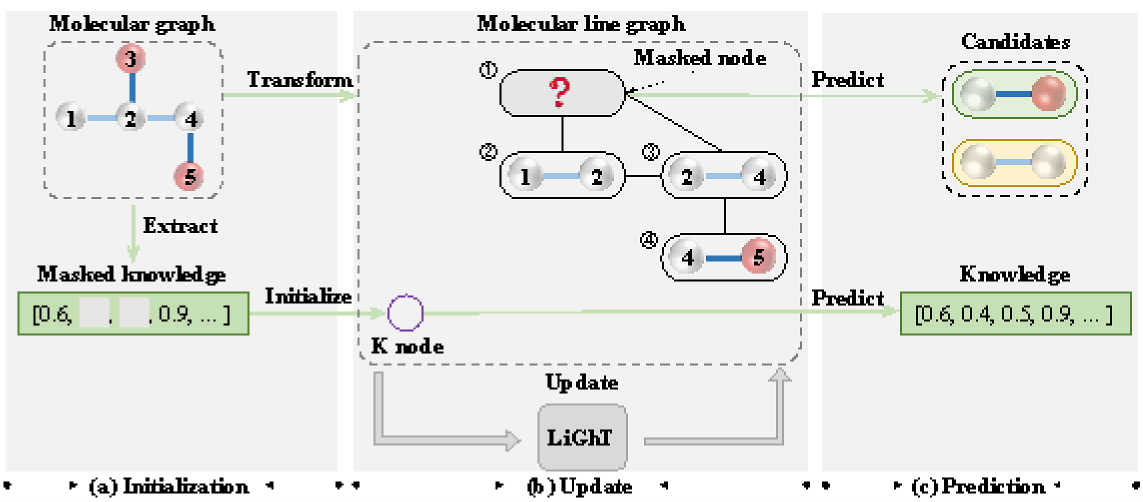
主要完成人：曾坚阳研究组

知识引导的图 Transformer 预训练框架用于小分子性质预测

传统的小分子药物开发流程通常非常的耗时且价格昂贵，开发能准确预测小分子物化性质以及生物活性的机器学习算法，对加速药物发现的过程、减小药物设计的成本至关重要。目前，受限于小分子数据集的规模，有监督学习算法往往无法取得令人满意的预测性能。所以，研究者们开始关注能够从大规模无标签数据中提取通用小分子特征的自监督学习算法，来提高小分子性质预测的性能。但当前用于小分子图的自监督学习算法有两个亟待解决的问题：预训练任务设计不恰当和主干网络容量有限。

为了解决这些问题，曾坚阳研究组开发了一个知识引导的图 Transformer 预训练框架，该框架主要由两个部分组成。首先，为了提高主干网络的容量，该研究组提出了一个新的图 Transformer 模型，能够更好的关注化学键的性质并建模小分子的结构信息。然后，该研究组提出了一个新的预训练框架，利用小分子的描述符和分子指纹来矫正当前被错误设计的预训练任务，从而更好的从大规模无标签数据中提取小分子的语义和结构信息。通过在多个数据集上和多个基线方法的比较，证明该预训练框架能够显著提升小分子性质预测任务的性能。此外，该研究组还通过消融实验证明了该预训练框架中各个模块设计的有效性。

该成果研究论文：Han Li, Dan Zhao and Jianyang Zeng, "KPGT: Knowledge-Guided Pre-training of Graph Transformer for Molecular Property Prediction", KDD 2022.



六、计算机系统结构

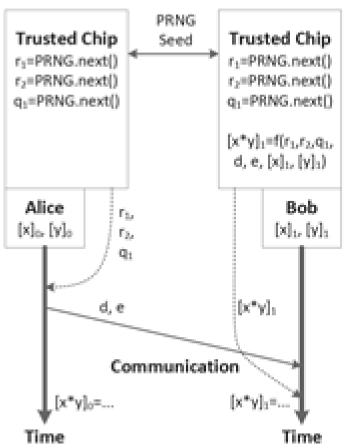
主要完成人：高鸣宇研究组、马恺声研究组

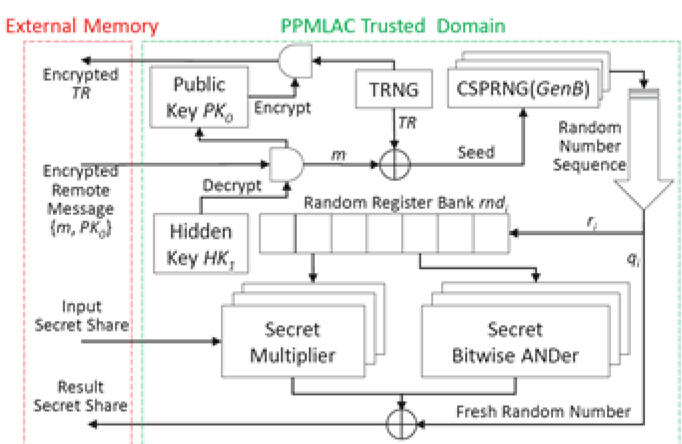
安全多方计算的硬件加速优化

安全多方计算（Secure Multi-Party Computation）自 20 世纪 80 年代由姚智期先生首先提出，是一种可在多个互不信任的参与方之间进行通用计算而又不会泄漏各方私有的隐私数据的密码学算法。经过数十年发展，安全多方计算的理论复杂度已经大大降低，但其实际性能仍难以满足复杂现实应用如人工智能算法的需求。其主要瓶颈在于每次乘法运算所引入的多方数据通信开销，和依赖可信第三方的初始化代价。

高鸣宇研究组提出了名为 PPMLAC 的系统架构，在专用芯片中引入最少所需的可信硬件单元，从而大大减小安全多方计算的初始化代价和通信开销。他们的可信硬件仅包含一个真随机数发生器、一组伪随机数发生器、一组乘法器和少量存储，与现有硬件可信执行环境相比大大减小了信任基，从而增加了侧信道防御。通过一个安全的同步协议，可信硬件在运行时可在本地按需生成辅助数据，并将原有算法中的双向通信转化为单向通信，将通信开销从关键路径上移除，显著降低延时。配合一定的数据缓存，数据通信带宽需求也可明显减小。在 ResNet50 等人工智能算法上，他们的 FPGA 原型设计与 V100 GPU 相比可达到百倍以上的性能提升。

该研究成果论文：Xing Zhou, Zhilei Xu, Cong Wang, Mingyu Gao, "PPMLAC: High Performance Chipset Architecture for Secure Multi-Party Computation", ISCA 2022.



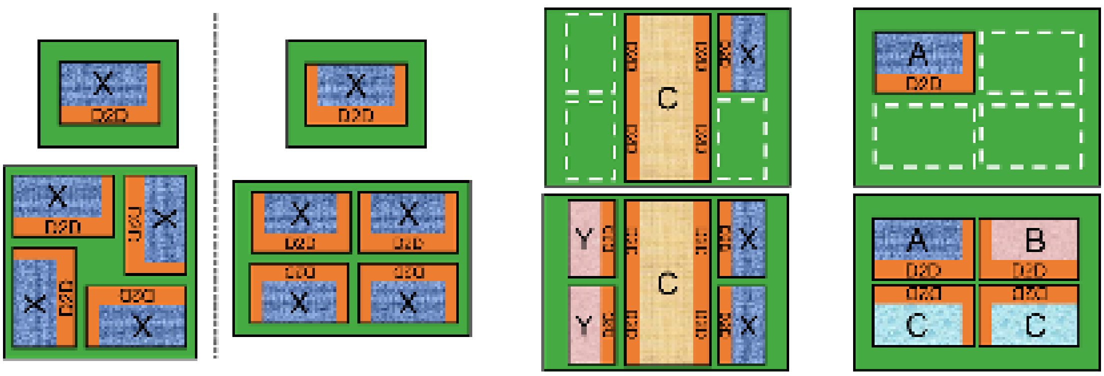


Chiplet 精算师：定量成本模型与芯片复用探索

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。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急。

该成果研究论文：Yinxiao Feng, Kaisheng Ma, "Chiplet Chiplet Actuary: A Quantitative Cost Model and Multi-Chiplet Architecture Exploration", DAC 2022.



(a) SCMS (b) OCME (c) FSMC

七、数据库系统

主要完成人：张焕晨及其合作者

自适应型混合索引

索引数据结构是高性能数据库管理系统中不可或缺的组成部分，但是它们却占据很大一部分可用内存空间。近期工作中提出的压缩索引技术能有效减小索引大小，使数据库能够利用更多的内存来缓存数据从而加速查询。然而，这些压缩索引在性能上比传统的索引要差，原因在于它们使用了“以性能换取空间”的数据结构编码形式。一个自然的想法是在同一个索引中使用不同的编码以求同时优化性能和空间两个维度。这个想法的难点在于如何智能地决定在何时将何种编码用于索引的哪个部分。

为了在一个索引结构中利用多种编码，张焕晨及其合作者提出了一个新的框架。该框架能够在数据库运行过程中，根据负载的变化自动调整索引中不同部分节点的编码类型。他们的框架会对进入数据库的查询进行实时采样，并保存细粒度的索引访问统计信息。以此为依据，他们周期性地改变部分节点的编码形式来优化索引的空间和性能：“冷”数据为主的节点使用高压缩的编码形式，热数据为主的节点则使用性能优化的编码形式。他们把这个框架应用在了两种常见的数据库索引上：B+trees 和 tries. 实验证明他们的新框架在有一定的负载倾斜情况下（现实中很常见），能够使索引所占内存空间减少多达 82%，同时保留 90% 以上的原索引性能。

该研究成果论文：Christoph Anneser, Andreas Kipf, Huanchen Zhang, Thomas Neumann, and Alfons Kemper. 2022. Adaptive Hybrid Indexes. In Proceedings of the 2022 International Conference on Management of Data (SIGMOD ’22), June 12 – 17, 2022, Philadelphia, PA, USA.

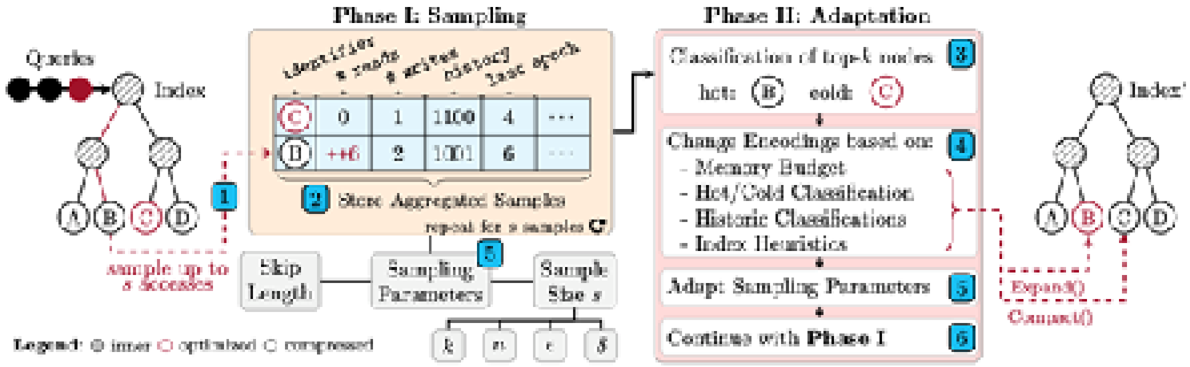


Figure 4: Basic overview of our workload-sampling approach applied to the example of a tree-like index structure.

Proteus：自动设计的范围过滤器

范围查询是大数据应用中的一个基础操作。给定一个集合 S，范围查询 [a, b] 会返回落在查询区间内的所有成员，即 S ∩ [a, b]。 大规模范围查询的应用非常广泛，包括社交平台对用户在时间和空间上的聚合，时间序列数据流中的异常检测，图数据库，以及区块链分析等。对此类数据集的范围查询通常需要在存储的磁盘或网络上消耗大量的成本。因此，用一个可以放进内存的范围过滤器来提前甄别结果为空的范围查询可以节省很多不必要的 I/O 开销。

张焕晨及其合作者在这项工作中提出了一种新的可以自我设计的范围过滤器 Proteus。Proteus 可以根据采样数据进行自我配置，以便针对给定的空间要求优化其假阳性概率 (FPR)。Proteus 统一了 state-of-the-art 中的确定性结构设计以及概率性结构设计，在大量的用例中实现了高效并且稳定的性能。Proteus 的核心是他们的 Contextual Prefix FPR (CPFPR) 模型。该模型可对基于前缀的过滤器的 FPR 进行建模分析。他们通过实际用例证明了该模型的准确性以及 Proteus 在真是数据集上卓越的效果。他们把 Proteus 应用在了常用数据库 / 存储引擎 RocksDB 中。实验发现 Proteus 能够提升多达 5.3 倍的端到端性能。相比于 state-of-the-art 方法 SuRF 和 Rosetta，Proteus 对性能的提升更为稳定。该研究组的实验还表明 Proteus 建模的成本与端到端的性能提升相比几乎可以忽略。因此，Proteus 对于负载变化具有鲁棒性。

该成果研究论文： Eric R. Knorr, Baptiste Lemaire, Andrew Lim, Siqiang Luo, Huanchen Zhang, Stratos Idreos, Michael Mitzenmacher. 2022. Proteus: A Self-Designing Range Filter. In Proceedings of the 2022 International Conference on Management of Data (SIGMOD ’22), June 12 – 17, 2022, Philadelphia, PA, USA.

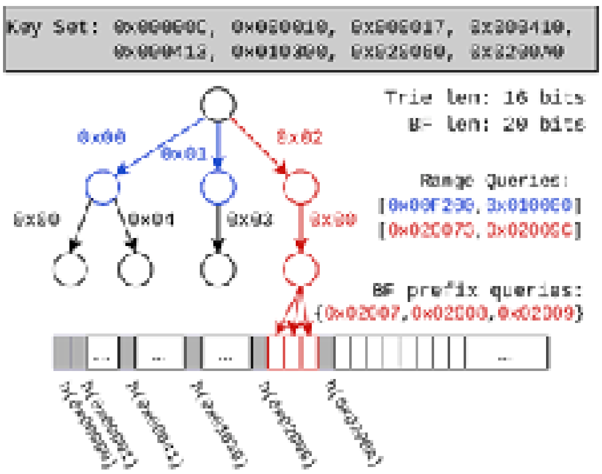


Figure 3: An example of Proteus using 24 bit keys with a trie depth of 16 bits and a Bloom filter prefix length of 20 bits. The blue and red show the logical paths of two empty range queries, the first of which is resolved in the trie while the second is resolved in the Bloom filter and could result in a false positive.

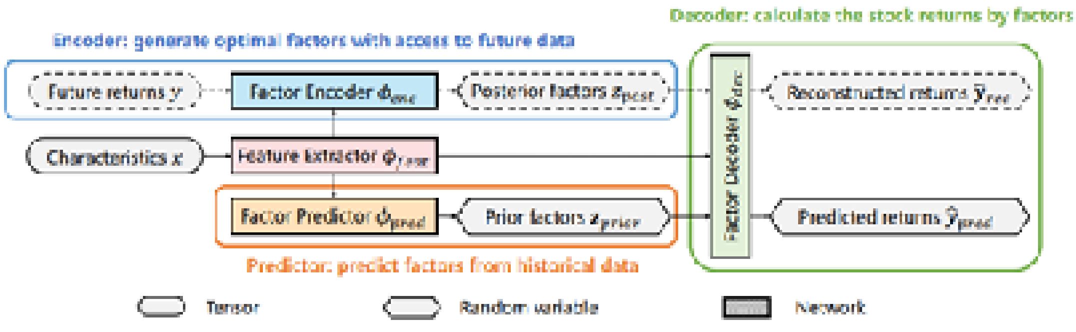
八、金融科技

主要完成人：李建研究组

概率多因子金融定价模型

多因子模型作为金融领域中的一种资产定价模型，在量化投资领域中有着广泛的应用。由于金融数据具有低信噪比的特点，如何克服金融数据中的噪声并构建出有效的多因子模型仍然存在着挑战。李建研究组以机器学习领域的变分自编码器为基础，提出了一个概率多因子模型——FactorVAE，模型包含的关键技术有：1) 采用先验 - 后验的学习范式，可以更好地从金融数据中提取因子；2) 设计了专门的概率因子机制，使模型不仅可以增强对噪声数据的建模能力，还可以估计资产未来收益的潜在风险。他们在中国 A 股市场的真实股票数据上进行了实验，其中截面股票预测实验结果表明，FactorVAE 在股票的截面预测的准确性（Rank IC 为 0.055）与稳定性（Rank ICIR 为 0.568）方面均表现得很好；另外投资组合回测实验结果表明，FactorVAE 在年化收益率（AR）、夏普比率（SR）以及最大回撤率（MDD）这些投资指标上也达到了很高的质量，证明了模型在量化投资中的有效性。

该成果研究论文：Yitong Duan, Lei Wang, Qizhong Zhang, Jian Li, "FactorVAE: A Probabilistic Dynamic Factor Model Based on Variational Autoencoder for Predicting Cross-sectional Stock Returns", AAAI 2022.



九、算法经济学

主要完成人：于洋研究组

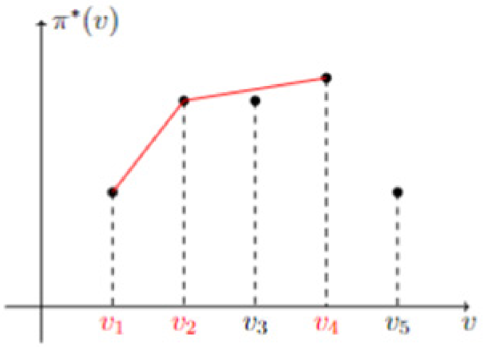
用户自编辑标签：对抗平台价格歧视的罗宾汉信息战

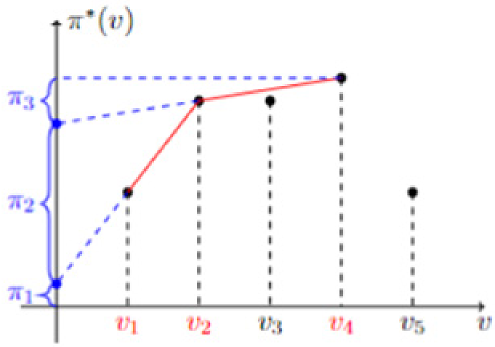
平台通过给用户进行数据画像、打标签，能够将市场进行细分、并分别定价。而如果不允许平台对用户进行画像和标签，推荐等基本平台服务又难以推进。这一直是平台价格歧视管制的难题。然而，于洋研究组指出，最近的数据隐私保护政策，能够被用户利用起来，成为对抗平台价格歧视的武器。每当用户可以删除、编辑自己的标签，他就从一个细分市场转移到另一个细分市场。因此，用户完全可以策略性的边际自己的标签，从而选择对自己性价比最高的细分市场。

然而，现有细分市场理论模型，不能够支撑对用户策略性编辑标签、对抗价格歧视的分析。该研究组重构了细分市场模型，并提出了稳定市场细分、群体稳定的市场细分两个关键概念。在每个稳定的市场细分中，生产者剩余保持在统一垄断水平，消费者剩余取买方最优水平和统一垄断水平之间的值。没有一个消费者比统一垄断更糟糕：匿名消费者被收取统一垄断价格，而其他消费者则以隐私换取折扣。研究组进一步给出了稳定，群体稳定市场细分的一种多项式时间验证算法。

该研究组分析发现：允许用户自行编辑标签且要求平台进行价格歧视，能够达到买方最优的剩余的市场细分。他们分析了买方最优的稳定市场细分的内部结构，证明了稳定和群体稳定在社会最优条件下的等价性，证明了所有稳定且社会最优的市场细分都有同样的价格组合，他们给予了求出这样子最优的价格组合的一种可视化构造，阐述了社会最优的稳定市场细分的唯一性。因此，该研究组的结果证明了价格歧视的帕累托最优，并揭示了现行法规的福利影响。

需要强调的是，这是一种全新的、对价格歧视的管制思路——让用户根据平台价格歧视来策略性的进行信息设计，从而“劝说”平台选择对消费者有利的市场细分。该研究组的研究还揭示了对于平台的价格管制，不能不允许它价格歧视，相反要要求平台进行价格歧视。





保护外卖员安全劳动权的调度

外卖员的安全引起了很多关注。舆论和政策都指责平台算法逼迫骑手过快行驶，导致骑手劳动安全无法得到保障。然而于洋研究组发现，目前关于外卖平台配送的研究中，往往通过排队论，在建模时聚焦于消费者尽快获得服务，或者平台能尽快和尽量少的雇佣骑手来完成服务。建模忽视了平台对骑手安全能够进行控制和改善的环节。

为了探索骑手的劳动安全和消费者的及时配送之间是否是零和关系，也为了探索提供骑手尽可能充裕时间、保护骑手劳动安全的调度算法，本研究构建了以骑手为中心的调度服务模型。该模型体现了平台、商家和消费者的决策和特征对骑手配送时间的影响。通过分析他们证明了骑手的生产安全和消费者的快速获得订单是零和矛盾的。但是商家如果分享自己线下订单的信息，能够大幅的缓解这种矛盾。

本研究证明了在平台经济中，消费者权益和劳动者权益的对立。指出了商家的商业机密信息公开，对于改善劳动者权益和消费者权益有着巨大的作用。同时为未来数据驱动的算法设计提供了理论建模框架，和传统的调度理论框架相比，能够支撑保护劳动安全的机器学习算法开发。

该成果研究论文：Weng, Wentao, and Yang Yu, “Labor-right protecting dispatch of meal delivery platforms”, In 2021 60th IEEE Conference on Decision and Control (CDC), pp. 1349-1355. IEEE, 2021.

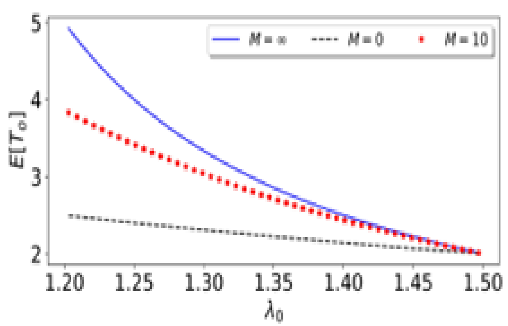


Fig. 4: Averaged Order Waiting Time After Using Restaurant Data

用多主体智能强化学习解释政府干预合法性——以疫情防控为例

诺贝尔经济学奖得主詹姆斯·布坎南构建了“同意的公共计算”框架来讨论个人自由的边界和政府存在的必要。许多需要人们合作来完成的公共服务供给，个人的自由意志会被约束。特别的：在一些复杂公共服务任务中，人们需要复杂的分工合作。但由于分工合作的复杂性，使得很难解释每个人分工的合法性。比如在疫情防控中，一些没有疫情的地区也需要风控，相反一些有疫情的地区则需要放开。这种集体合作的策略，亟需有方法去提供合法性解释。

本研究用多主体智能强化学习（MARL）构建了对政府在组织合作中合法性的分析框架，并利用这一框架，讨论了在疫情防控中多区域复杂合作策略的合法性解释问题。同时，将不同的意识形态建模为差异化的多主体目标方程，从而解释了在不同意识形态下政府合法性策略的差异性和效果。

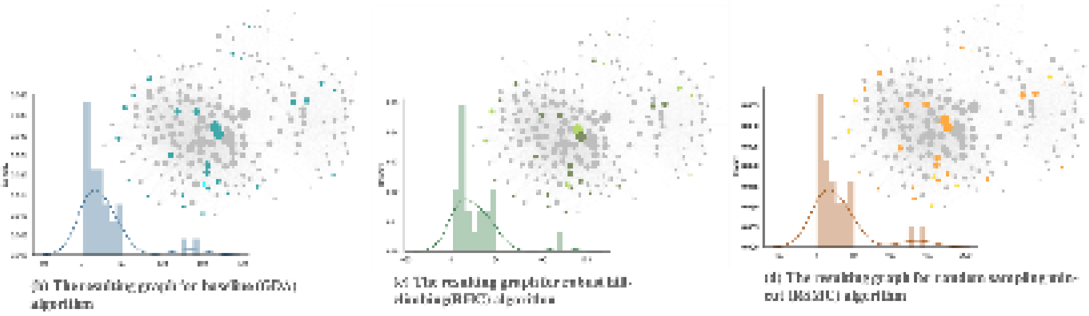
该成果研究论文：Hu, Yang, Zhui Zhu, Sirui Song, Xue Liu, and Yang Yu， "Calculus of Consent via MARL: Legitimating the Collaborative Governance Supplying Public Goods", NIPS 2021.

兼顾知情权的有害信息传播控制机制

社交网络平台上不实信息的病毒传播引起了学术和业界的广泛关注。然而，目前不实信息传播面临两个管制困境:一方面，有害信息被发现时已经广泛传播；另一方面，如果在完成验证前，不允许信息传播，则伤害了网络用户尽快获得信息的知情权。因此，于洋研究组研究了如何在保障知情权的前提下，避免有害信息再核验前已经广泛传播。

为此，他们提出了一种新的优化模型来解决事实检查期间的信息传播管理问题。具体而言，他们的模型基于阻塞节点，控制不当信息传播范围的期望值。从模型的固有性质出发，消除紧急信息被控制而无法传递的隐患，从而实现智能精准控制。将阻塞节点的总权重最小化作为模型的目标函数，解决了降低宏观调控成本的问题，并且提出了两种启发式方案，从算法层面解决这个优化问题。

该成果研究论文：Jiayi Mao, and Yang Yu, " Wait for Fact Checking: Information Dissemination Management on Social Network", Submitted to 2022 61th IEEE Conference on Decision and Control (CDC).



十、计算能源经济学

主要完成人：于洋研究组

物联网里的 AI 攻击：用物理资产对抗魔法

论文研究了智能电网中的人工智能算法攻击带来的经济风险和对策。研究指出，算法攻击已经能够威胁实体经济的新型风险，这类风险隐蔽性强，因此难以被察觉和究责，但却会给经济带来重大损失。然而，和计算机领域“用算法对抗迎击算法攻击”的“魔法对抗魔法”思路不同的是，实体经济中存在着能够对抗算法攻击的物理设备——也就是用物理方法对抗魔法。因此，人工智能时代，实体经济有必要投建“对抗算法攻击的新基建”。智能电网是一个依赖数据和学习模式的信息物理系统，人工智能算法（AI）构成了智能电网的“思考和感知系统”。然而，智能电网面临一种新型威胁：通过设计噪声误导数据驱动的 AI 模型，诱使 AI 基于错误感知学会错误知识、最后做出错误决策。

论文指出 AI 的错误决策会给物理电网带来巨大经济损失——。在德克萨斯州，5% 的对抗性攻击可以使一个季度的总发电成本增加 17%，约有二千万美元。研究组还发现，在低碳化后，这种隐蔽的供给会带来更大顿时：当风能渗透率增加到 40% 以上时，5% 的对抗性攻击会使发电成本增加 23%。需要指出的是，算法攻击和传统对电网的攻击完全不同。传统电网攻击，是通过造成设备损坏和大面积停电来实现。而算法攻击，目的不是一次性瘫痪电网，而是以“润物细无声”的方式，让电力系统在不知不觉中遭受“聚沙成塔”的巨大经济损失。

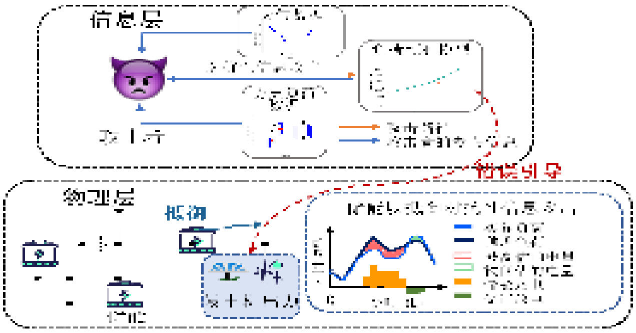


图 1 对智能电网中 AI 算法的攻击方法以及对电力系统运行的威胁

该研究还提出了利用物理资产防御对抗性算法攻击的新方法：投资于储能系统。目前所有的文献都集中在开发防御对抗性攻击的算法上。于洋研究组发现，当智能电网中有足够多的储能资产时，即便他们察觉不到算法攻击、算法攻击也成功的误导了 AI，储能也能阻隔 AI 的错误衍生为经济损失。实际上，AI 被误导会改变价格信号，从而触发储能的响应，这种储能的逐利行为却避免了整个系统的经济损失。该研究获得获得能源领域顶会 IEEE PESGM 2022 年最佳论文奖。每年在会议上获得该荣誉的论文比例不到投稿总数的 2%。

该成果研究论文：Li, Jiawei, Jianxiao Wang, Lin Chen, and Yang Yu, "Defending Against Adversarial Attacks by Energy Storage Facility," arXiv preprint arXiv:2205.09522 (2022).

经济体制改革中的鲁棒政策设计：用计算科学视角理解中国经济改革

经济体制改革，是中国发展中的一个最重要的因素。许多研究虽然对经济体制改革对生产效率、收入分配等问题进行了研究。但是忽略了经济体制改革过程中，公共政策的绩效是否会发生变化？为研究这一问题，他们将鲁棒优化的思路引入政策分析，讨论在体制改革中什么样的政策才是鲁棒的。我国很多公共政策是在计划体制下设计和实施了，体制改革后这些政策是否仍将有效？如何能够设计出在体制改革进程不确定、体制改革模式不确定下，鲁棒的公共政策。这一问题并未被讨论过。在本研究中，于洋研究组为政策稳健性分析开发了一个框架和相关指标。

该研究组特别关注了中国的低碳政策在市场自由化改革进程中的鲁棒性。考察了改革前设计的已实施和规划的低碳政策在改革后是否会失效。应用政策鲁棒性的分析框架，他们分析和比较了两个低碳政策在市场改革中的鲁棒性。这两个政策是机组燃煤效率改进政策 (FEIP) 和碳税政策 (PCP)。分析表明，FEIP 和 PCP 都将在市场改革中失去部分效力。但是， PCP 比 FEIP 更为稳健。这是因为 PCP 能够激励具有成本竞争力的燃煤发电机组改造它的机组。在市场改革后，这些机组的市场份额将扩大，因此 PCP 的效果能够得到较大保持。相反，FEIP 就无法激励低成本机组改造，因此将变得非常抵消。

他们发现，政策的鲁棒性和各地的能源效率现状非常相关。由于福建电厂的能源效率差距显著，这就导致了 FEIP 在福建的鲁棒性特别差。研究组进一步得出结论，对发电能力的过度投资导致改革期间 FEIP 和 PCP 的鲁棒性降低。中国的发电能力已经过度投资，但当前的燃油效率改进政策 (FEIP) 可能严重不健全，并在电力改革过程中造成重大的效率损失。

该成果研究论文：Zhang, Yaoyu, Chenye Wu, Nan Gu, and Yang Yu, "The robustness of low-carbon policies during China’s electricity reform", Energy Economics 111 (2022): 106037.

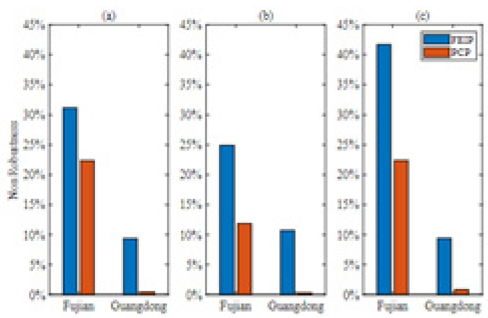


Figure 2: The non robustness of FEIP and PCP in Fujian and Shandong.
(a)low demand and low retrofit-cost scenario (b)high demand scenario (c)high retrofit-cost scenario

新能源越多、碳排放越多？核电被挤出后的碳反弹

研究发现：到 2030 年前，风电光伏的增长，在美国的两个主要电力市场中会因为挤出核电，而累积造成接近 1.4 亿吨的额外温室气体排放。风电和光伏，普遍被认为是零碳排放的发电技术。因此，推动风电光伏替代化石能源发电，成为了各国和各地区能源低碳转型最主要的策略。这一反直觉的发现，揭示了现有碳减排战略对气候变化带来了潜在的风险，有必要及时进行调整。

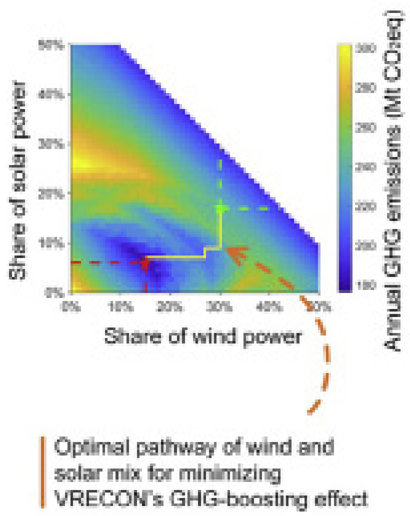
过对风电光伏不确定性对市场竞争和投资的分析，研究发现了风电光伏进入电力市场后的复杂链式反应：在有核电的市场中，风电光伏的增长会导致核电过早退出市场。与此同时，风电和光伏又不能完全填补因为核电退出而遗留的市场份额——这导致了化石能源填补了核电留下的部分市场份额。也就是说，风电光伏的增长，推动了高碳排放的煤炭和天然气发电替代了零碳排放的核电，因而造成碳排放的上升。

该研究进一步分析发现，由于挤出效应的存在，风电和光伏的组成比对未来几十年碳排放累积量的大小有关键性的影响。合理的风光比能最大限度的推迟挤出效应的发生，同时带来最和缓的碳排放增加速度，从而最小化碳排放的累积量。例如，有图中就给出了美国得克萨斯州市场的风电和光伏比例最优演化路径。

令人忧虑的是，一些被基于厚望的技术——例如储能技术，并不能有效缓解风电光伏挤出核电造成的碳排放。

上述发现不仅指出了现有全球碳排放削减战略的风险，也提出了一些列政策改进建议：包括了在现有新能源发电指标政策中，明确风电光伏在不同阶段的比例；补贴核电避免其过早退出市场等。

该成果研究论文：Zhao, Xiaoli, Zewei Zhong, Xi Lu, and Yang Yu, "Potential greenhouse gas risk led by renewable energy crowding out nuclear power", Iscience 25, no. 2 (2022): 103741.



十一、区块链

主要完成人：房智轩研究组

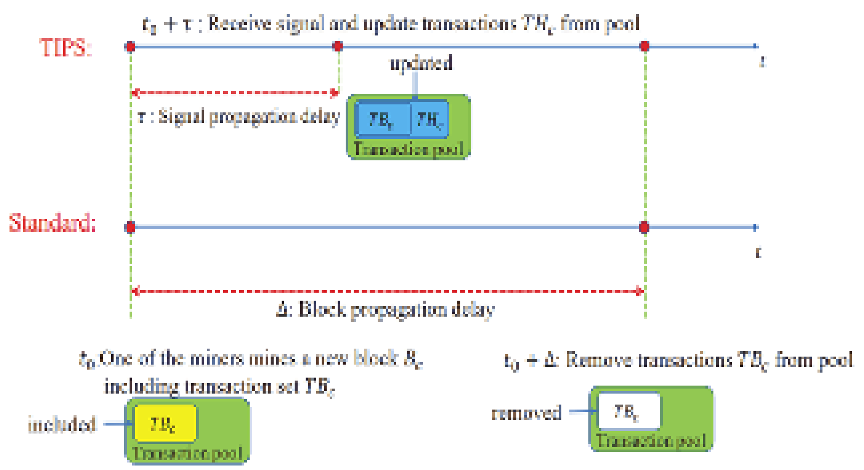
设计有向无环图的区块链系统中基于信号的交易包含协议 (TIPS)

基于有向无环图的区块链系统允许同一时刻多个区块并发地添加到区块链系统中，这极大地提高了区块链系统性能。但并发的区块中可能会包含相同的交易，而这些冗余的交易碰撞会降低系统的利用率，甚至可能还会严重影响系统性能。

在这个工作中，房智轩研究组指出基于有向无环图的区块链系统中存在的两个困境，分别是矿工收益困境和系统吞吐量困境。矿工收益困境指的是矿工很难提高自己的交易费收益。具体而言，矿工倾向于选择交易费更高的交易进行打包，但是由于并发区块的交易碰撞问题，选择高额交易费的交易会导致交易碰撞，从而降低矿工的收益；系统吞吐量困境指的是系统难以通过增加区块大小来进一步提高系统吞吐量。具体来说，提高系统吞吐量的一种直观方式是增加区块大小，使得一个区块中能包含更多交易。但区块大小增加会导致传输区块的网络延时增大，从而导致更多的交易碰撞，降低了系统利用率，从而约束了系统吞吐量的提升。

为了解决有向无环图区块链系统中的这两个困境，该研究组提出了一种基于信号的交易包含协议 Transaction Inclusion Protocol with Signaling (TIPS)。在所设计的协议中，他们将布隆过滤器加入到区块头中，并将其作为挖矿过程中的信号。该信号足够小，所以可以在短时间内广播到全网中。网络中的矿工也可以通过该信号来避免交易选择碰撞。结合理论分析和实验验证，该研究组说明了通过广播该信号，TIPS 可以有效减少交易碰撞，大幅提升系统吞吐性能，从而解决了有向无环图区块链系统中的两个困境。

该成果研究论文：Canhui Chen, Xu Chen, and Zhixuan Fang, "TIPS: Transaction Inclusion Protocol with Signaling in DAG-Based Blockchain", IEEE Journal on Selected Areas in Communications (JSAC), to appear.



十二、密码学

主要完成人：陈一镭研究组

解决特殊格问题的量子算法

寻找格上的最短向量一直被认为是计算机领域最困难的问题之一，至今没有经典或量子算法能在多项式时间内解决这个问题。因此构造基于格问题的密码一直被认为是构造防止量子计算机攻击的密码的有效途径之一。其中被用来构造公钥密码的 SIS 和 LWE 问题被证明和格上的最短向量问题是等价的。

陈一镭和他的合作者，普林斯顿大学的刘启鹏和 Mark Zhandry 提出了一个能解决“特殊”格问题的多项式时间量子算法。这些特殊格问题是 SIS 和 LWE 的变种。他们虽然并不等价于标准的格问题，但是已经非常接近于密码学常用的问题。他们的量子算法中使用了一种被称为“过滤”的方法，是在量子算法的设计中第一次使用，可能为未来量子算法的设计带来新的思路。

该论文于 2022 年二月被欧洲密码大会（Eurocrypt）接收，并被邀请投稿到 Journal of Cryptology。

该成果研究论文：Yilei Chen, Qipeng Liu, Mark Zhandry, "Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering", EUROCRYPT 2022.

对于 ADP 代码混淆方案的攻击

代码混淆（program obfuscation）力求将一段明文程序变为不能够被理解的，但是还是能运行的“混淆程序”。自 2000 年以来，代码混淆一直是理论密码学研究的重点，至今已有多达六十多个不同的方案被提出。Bartusek 等人在 2019 年提出了一个基于 Affine Determinant Program 的代码混淆方案。这个方案非常新颖，不同于其他代码混淆的方案的设计思路。如果其安全性能经受考验，它将有可能是现存最高效的代码混淆方案。

陈一镭与上海交大的郁昱老师和研究生姚立提出了第一个对于 Bartusek 等人的 ADP 代码混淆方案的攻击，并提出了修补的方法。这使基于 ADP 的代码混淆成为除了基于 LWE 的众多方案之外唯一的可能抗量子的代码混淆方案。这将推动 ADP 系列代码混淆方案的后续研究。该论文于 2022 年二月被欧洲密码大会（Eurocrypt）接收。

该成果研究论文：Li Yao, Yilei Chen, Yu Yu, "Cryptanalysis of Candidate Obfuscators for Affine Determinant Programs", EUROCRYPT 2022.

伪随机函数的精准上下界与其对复杂度理论的影响

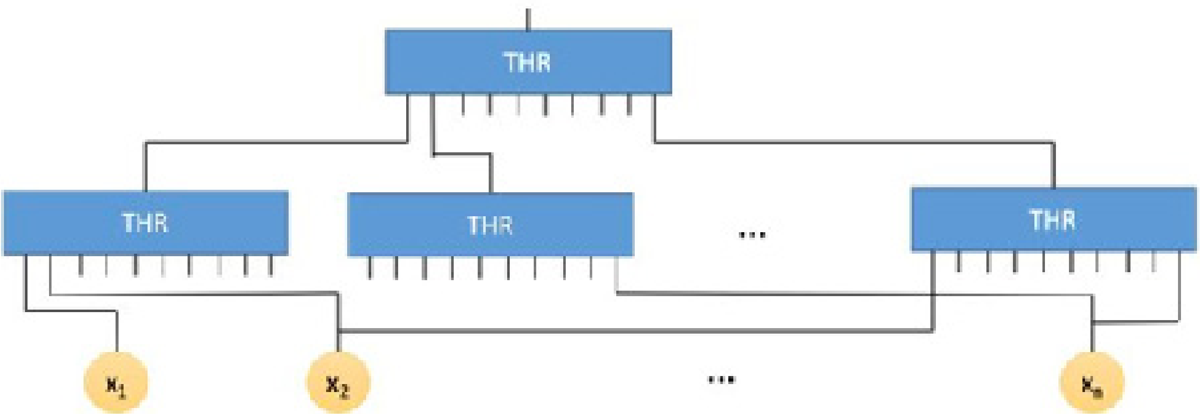
伪随机函数 (pseudorandom functions) 是无法与随机函数区分开的函数族。它作为密码学许多构造的起点，是密码学的基础。因此构造高效的伪随机函数在理论及应用中有多种意义。

姚班的本科生范致远、李嘉图、和杨天祺在陈一镭老师的密码学基础课研究课题中研究了伪随机函数的电路复杂性，在多个重要的电路复杂性类中对伪随机函数给出了紧的上界与下界。例如证明了在一般电路中，若多项式大小的电路可计算的伪随机函数存在，则存在一个仅需大约 2n 个门的电路族即可计算的伪随机函数。同时，该研究无条件地证明了计算任何伪随机函数至少需要 2n-2 个门。

这些上下界结果为电路复杂性理论提供了新的理解，也解释了为何一些广为相信的猜想难以被证明。特别地，针对目前电路复杂性理论中存在许多被称为 "bootstrapping phenomena" 的现象，该研究指出，要想从这些现象推出 P vs NP 等重要开放问题的答案，还需要一些全新的证明思路。

该论文于 2022 年二月被 STOC 接收，并获得最佳学生论文奖。

该成果研究论文：Zhiyuan Fan, Jiatu Li, Tianqi Yang, "The Exact Complexity of Pseudorandom Functions and the Black-Box Natural Proof Barrier for Bootstrapping Results in Computational Complexity", STOC 2022.



两层线性阈门电路

十三、理论计算机科学

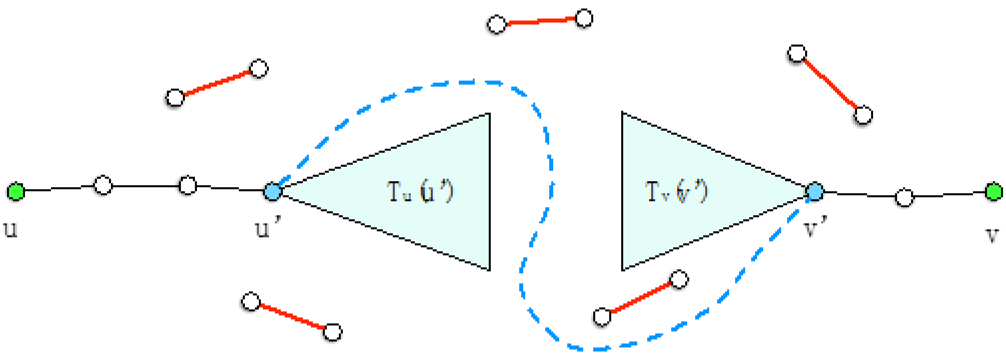
主要完成人：段然研究组

多边失效时的精确最短路数据结构

多边或多点失效时最短路问题是数据结构领域的一个经典难题。因为动态最短路问题目前没有 o(n2)- 维护时间的数据结构，边或点失效模型（d-failure model）就更加重要。在多边失效模型上，对于一个图他们希望建造一个数据结构，使得当最多 d 条边失效时仍能快速查询任意两点间的距离。此前的结果包括两条边或两个点失效时精确最短路结构 [Duan & Pettie 2009]、无向图中 d 条边失效时 [Chechik et al. 2017] 和 d 个点失效时 [Duan, Gu, Ren 2021] 近似最短路结构。

段然副教授与 2021 届姚班毕业生（现牛津大学研究生）任瀚林同学合作的论文给出了无向图上第一个高效的 d 条边失效时精确最短路结构。对任意常数 d，其空间复杂度为 O(dn^4)，查询时间为 d^{O(d)}。该论文提出了与之前成果不同的方法，也为之后的研究提供了思路。

该成果研究论文：Ran Duan and Hanlin Ren, "Maintaining Exact Distances under Multiple Edge Failures", STOC 2022.



图：多边失效时最短路数据结构设计示意图

更快的单调矩阵（数组）的距离乘法算法

段然副教授与研究生迟舒乘、谢添乐以及研究生校友（现特拉维夫大学博士后）张天翼合作的论文给出了更快的单调矩阵的 (min,+)- 乘法算法。(min,+)- 矩阵乘法，也叫距离乘法，是算法领域的经典难题，因其与每两点间最短路问题等价。对于 $n \times n$ 矩阵，目前仍然没有真正的快于立方时间的算法。当 A 为任意矩阵，B 的每行（或每列）都是单调非递减，并且 B 中的元素大小是 O(n) 时，他们给出了时间复杂度为 O(n^{2.686}) 的新算法，改进了之前 O(n^{2.875}) 的算法 [Gu et al. 2021]，同时也将一些能归约到这个问题的其他问题的时间复杂度改进到了 O(n^{2.686})，包括有限差矩阵（即相邻元素的差为常数）的 (min,+)- 矩阵乘法。[Bringmann et al. 2016] 证明了很多问题，像上下文无关文法的带权分析和编辑距离、RNA- 折叠、栈生成等，都可以归约到有限差矩阵的 (min,+)- 矩阵乘法，所以这些问题的复杂度都被改进到了 O(n^{2.686})。本论文还提出了时间复杂度为 Õ(n^{1.5}) 的单调有界（大小是 O(n)）数组的 (min,+)- 卷积算法，改进了此前 O(n^{1.859}) 时间的算法 [Chan & Lewenstein 2015]。

该成果研究论文：Shucheng Chi, Ran Duan, Tianle Xie and Tianyi Zhang, "Faster Min-Plus Product for Monotone Instances", STOC 2022.

图：任意矩阵与单调矩阵的距离乘法

量子信息

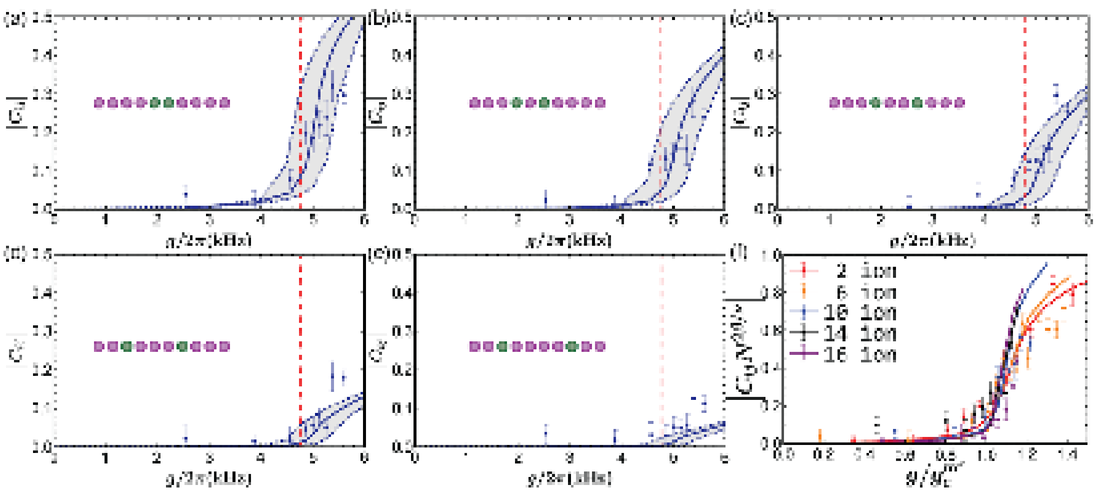
一、离子阱量子模拟

主要完成人：段路明研究组、吴宇恺研究组

多体拉比 - 哈伯德（Rabi-Hubbard）模型的离子阱量子模拟，超越经典超算的模拟能力

段路明研究组在离子阱量子模拟领域取得重要进展，首次在实验中借助离子量子比特实现了拉比 - 哈伯德（Rabi-Hubbard）模型，并验证了该模型的量子相变以及量子动力学过程。通过对 16 个离子和 16 个简谐振动模式的操控，该量子模拟问题的有效空间维度达到了 257，超越了现有经典超级计算机的模拟能力。

拉比 - 哈伯德模型由量子光学和凝聚态物理中的两个基本模型结合而成，拉比模型历史悠久，可以追溯到 1936 年，它描述了光场与物质的相互作用；而哈伯德模型起源于 1963 年，是描述晶格中粒子相互作用的最基本的模型，现已发展成为凝聚态物理学中许多领域的出发点。拉比 - 哈伯德模型包含了局域的拉比模型自旋 - 声子相互作用以及格点之间的声子 - 声子相互作用，两者的结合使得该模型表现出丰富的物理特性。该模型的实验方案最初在腔量子电动力学系统中提出，但是由于技术困难一直没有在实验上实现。

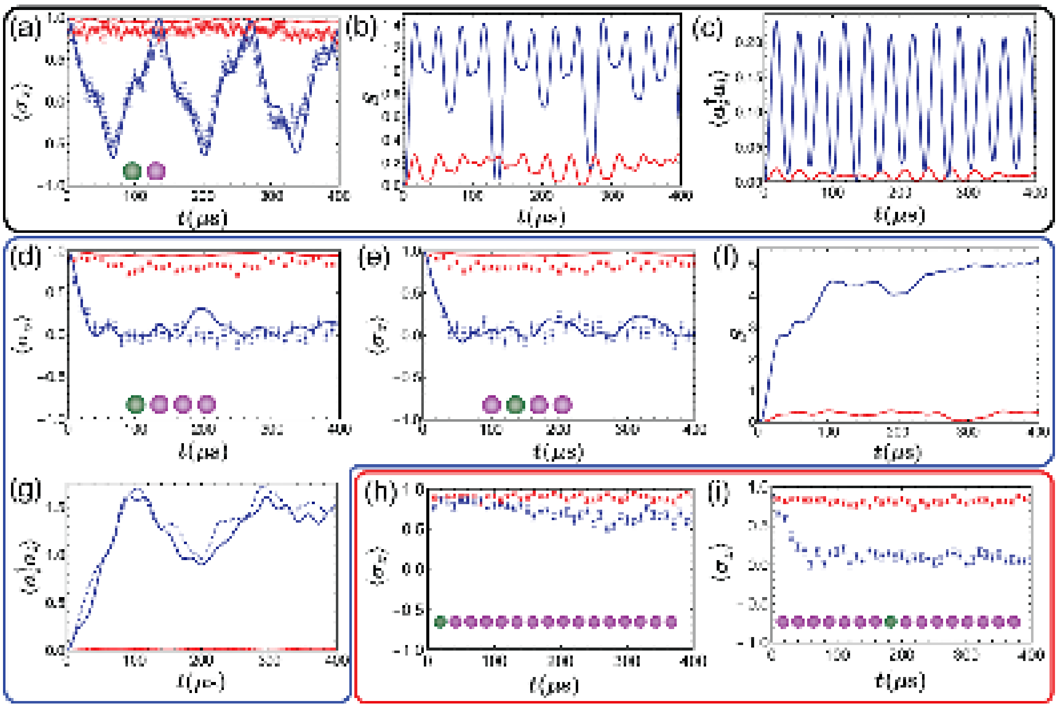


拉比 - 哈伯德模型的序参量演化和量子相变

得益于离子阱量子模拟平台的高度可控性，研究人员实现了对拉比 - 哈伯德模型的可控量子模拟研究。研究人员通过对激光的精密操控实现了离子量子比特与 局域声子的相互作用，而离子阱系统中的库伦相互作用形成了不同离子间的局域声子交换项。在这项工作中，研究人员通过量子相变和量子动力学两个方面验证了拉比 - 哈伯德模型的成功实现。在量子相变方面，研究人员通过绝热演化实现了相干相和非相干相之间的转化，在此过程中通过测量空间自旋关联这一序参量，成功在不同规模的离子阵列中观测到量子相变现象，且与 DMRG 方法近似计算的结果相符。而在量子动力学方面，拉比 - 哈伯德模型包含了离子的自旋模式和空间振动模式的相互耦合，这显著增加了该系统有效的希

尔伯特空间维度，使得经典模拟难度增加。研究人员在小规模体系（2 离子、4 离子）下观测到了符合经典模拟预期的量子动力学演化，与量子相变一同证明了本实验中拉比 - 哈伯德模型的成功实现。而在大规模体系（16 离子）和强耦合参数区间，常用的经典近似方法将不再适用，实验系统的有效态空间维度高达 257，相关的动力学过程已经难以通过经典计算机模拟计算。该实验展示了基于离子阱平台的量子多体模拟，将空间振动自由度引入量子模拟中，实现了经典计算机难以计算的问题规模，是通向未来大规模离子阱量子计算、量子模拟的重要一步。

该成果研究论文：Q.-X. Mei, B.-W. Li, Y.-K. Wu, M.-L. Cai, Y. Wang, L. Yao, Z.-C. Zhou, and L.-M. Duan, "Experimental Realization of the Rabi-Hubbard Model with Trapped Ions", Phys. Rev. Lett. 128, 160504 .

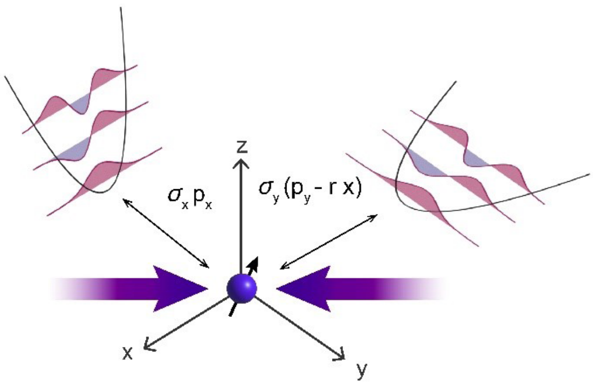


拉比 - 哈伯德模型的自旋动力学演化

在离子阱中实现二维外尔方程的量子模拟

段路明研究组在离子阱量子模拟领域取得重要进展，利用单个囚禁离子成功实现了磁场中的二维外尔粒子的量子模拟。

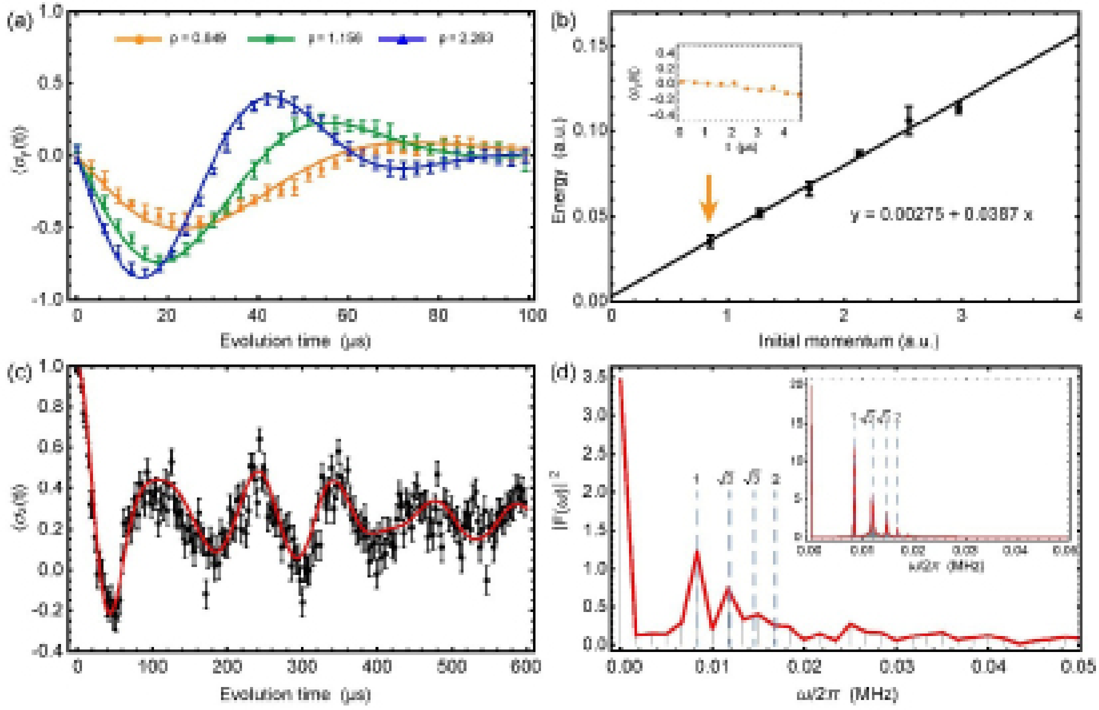
相对论量子力学结合了现代物理学中两个最重要的理论：狭义相对论和量子力学。外尔方程则是最简单的相对论量子力学方程之一，描述了自旋为 1/2 的零质量粒子——外尔费米子。作为相对论量子力学理论所允许的几种基本粒子之一，外尔费米子尚未在实验中被发现：它曾被认为可用于描述中微子，但现在已知中微子具有微小的质量，并非零质量粒子。因此，目前要从实验上研究外尔费米子的性质，只能通过量子模拟的手段。此前的实验在光子晶体和凝聚态系统中对外尔费米子的能谱和输运性质等进行了测量，但无法对其动力学进行直接研究。另一方面，在离子阱系统中对有质量的狄拉克粒子的动力学进行过量子模拟，但只限于一维空间，而无法研究自旋动力学和对磁场的响应等性质。



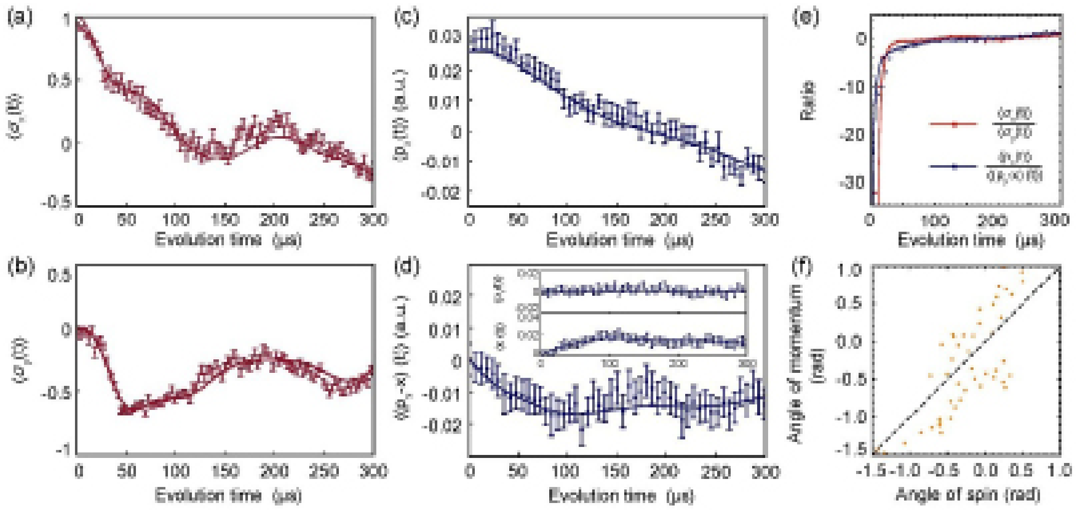
实验原理图

在此项工作中，研究人员通过激光操控囚禁离子的内态和两个不同空间方向的声子模式，成功实现了磁场中二维外尔方程的量子模拟。通过制备不同的初态以及对不同自旋观测量的测量，研究人员成功验证了二维外尔粒子的线性色散关系、磁场中分立的朗道能级、螺旋性守恒等性质。通过引入额外的空间和自旋自由度，此项工作拓展了量子模拟在粒子物理领域的应用。

该成果研究论文：Y. Jiang, M.-L. Cai, Y.-K. Wu, Q.-X. Mei, W.-D. Zhao, X.-Y. Chang, L. Yao, L. He, Z.-C. Zhou, and L.-M. Duan, "Quantum Simulation of the Two-Dimensional Weyl Equation in a Magnetic Field", Phys. Rev. Lett. 128, 200502 .



线性色散关系与磁场中的分立能级



动力学演化测量

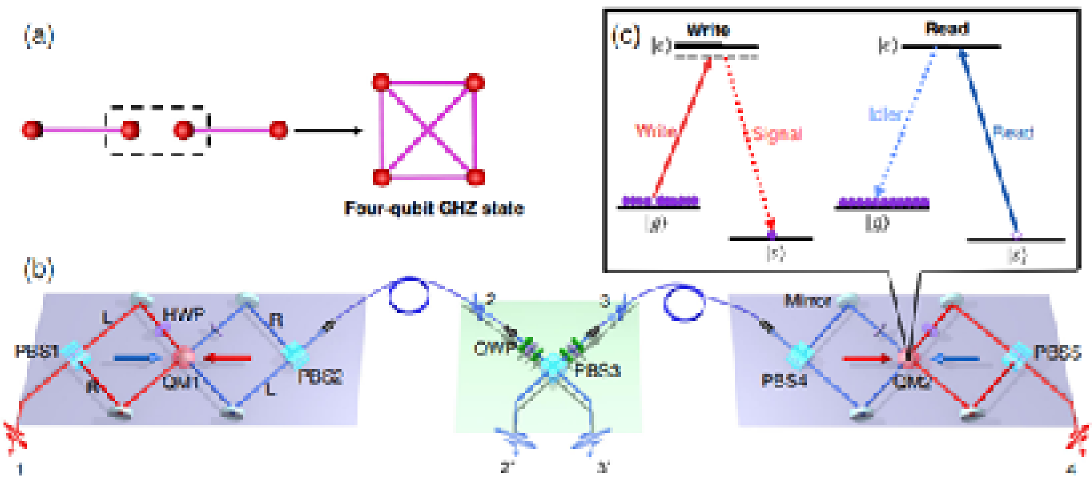
二、量子信息

主要完成人：段路明研究组、马雄峰研究组、吴宇恺研究组、濮云飞研究组

实现量子存储器增强的非局域图态制备

段路明研究组在量子信息领域取得重要进展，首次在实验上利用量子存储器实现高效制备非局域图态，展示了量子存储器在大规模分布式系统中进行量子信息处理和量子测量的应用前景。

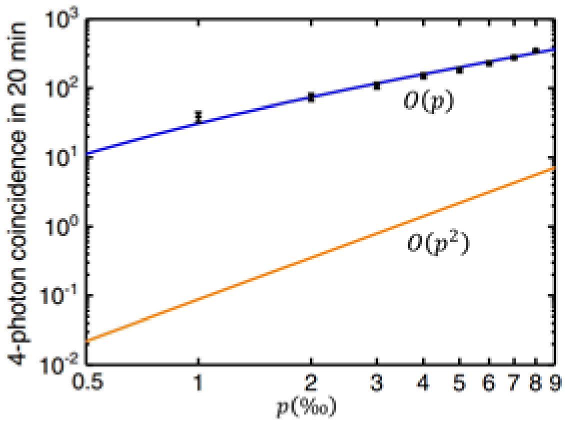
图态是一类重要的多体纠缠态，因其广泛的应用前景而不断受到研究人员的关注，包括测试量子力学基本概念，量子计算，量子密码学和量子计量学等。之前的实验制备图态，特别是线性光学系统中的 Greenberger-Horne-Zeilinger (GHZ) 态，其制备效率随系统规模呈现指数衰减定律，这限制了其在大规模量子网络中的应用。为了克服非局域图态制备的可扩展性问题，段路明教授等人提出了一套高效制备图态的理论方案 (Phys. Rev. Lett. 97,143601(2006))，制备效率随系统规模呈现多项式衰减。该方案的核心思想是，不参与后期操作的光子可以被提前测量和后选择；然后利用长寿命量子存储器以分治的方法生成大规模图态。然而由于实验技术方面存在的困难，该方案此前未能实现。模块从而扩大量子纠缠在空间中的分布，因为实验技术方面存在的困难，一直尚未实现。



实验方案示意图

在此项工作中，研究人员通过将超低温的铷原子气体囚禁在光晶格中，并利用原子基态能级当中一对钟态能级跃迁，成功将冷原子量子存储器的相干时间提升至数十毫秒量级。研究人员先利用第一个量子存储器（QM1）产生一对光子和原子之间的纠缠态并将量子态存储下来，然后再利用第二个量子存储器（QM2）产生第二对光子和原子之间的纠缠态，最后同时读取两个量子存储器内部的量子态并将他们投影到目标的四光子 GHZ 态上。研究结果表明，通过这种方式产生的四光子 GHZ 态，其制备效率线性正比于单个 EPR 纠缠对制备效率，与没有使用量子存储方案所导致的制备效率正比于单个 EPR 纠缠对制备效率二次方关系相比，改变了制备效率在规模化上的复杂度。当未来需要连接 N 对纠缠对时，其制备效率将从指数衰减量级上升到多项式级别，展示了量子存储方案在制备大规模图态的优越性。此外，研究人员还进一步利用制备的四光子 GHZ 态验证了 MABK 不等式，并演示了量子密码学当中的量子秘钥分发协议。此项工作实现了一个高效制备大规模图态的原型，从而为其在量子信息科学和量子计量中的各种应用迈出了重要的一步。

该成果研究论文：Sheng Zhang, Yu-Kai Wu, Chang Li, Nan Jiang, Yun-Fei Pu, and Lu-Ming Duan, "Quantum-Memory-Enhanced Preparation of Nonlocal Graph States", Phys. Rev. Lett. 128, 080501.



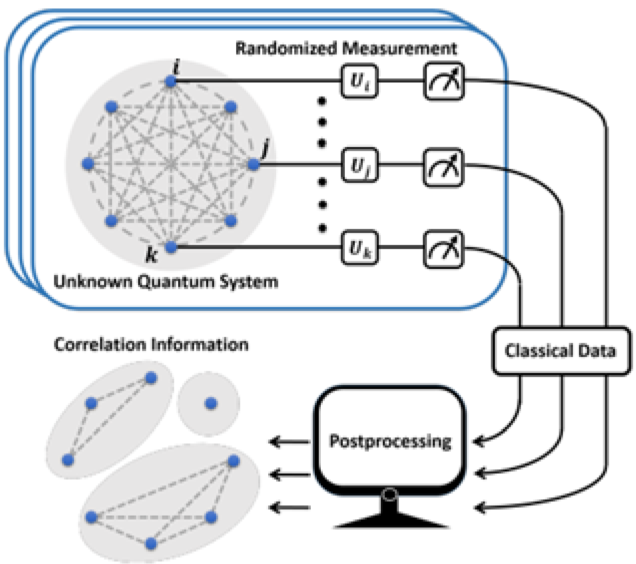
四光子 GHZ 态制备效率提升

多体量子关联的有效标定

量子系统具有经典系统不具有的关联性质，具有高度多体关联的量子态是量子信息处理任务中的重要资源，也是量子优越性的来源，一个量子设备产生强多体关联量子态的能力是标定量子设备信息处理能力的关键指标。传统的度量多体量子关联的方案需要量子层析技术，这一方案的复杂度往往是实际物理实验中无法接受的，也会带来很多的信息冗余。

针对这一问题，马雄峰研究组的博士生刘振寰，与该组博士毕业生曾培，复旦大学周游，以及新加坡南洋理工大学 Mile Gu 教授提出了一种基于多体量子态与其子系统量子态内积的多体量子关联度量。这一度量具有可加性，局域操作不变性等作为多体关联度量应有的良好性质。另外，这一新的度量解决了之前常用的基于二阶瑞丽熵的多体关联度量对于某些量子态会出现负值的问题。除了在理论方面具有诸多良好性质之外，这一多体关联度量还可以被有效测定。文章作者基于随机测量方案，设计了测量这一度量的实验框架，并且通过理论分析以及数值模拟得到了这一框架的复杂度，证明了它比传统的量子层析方案具有指数优越性。

该研究成果论文：Zhenhuan Liu, Pei Zeng, You Zhou, and Mile Gu, "ECharacterizing correlation within multipartite quantum systems via local randomized measurements", Physical Review A, 105(2): 022407 (2022).



图一：利用随机测量标定量子系统多体关联的框架

三、超导量子计算

主要完成人：孙麓岩研究组

超导量子系统中利用玻色量子纠错码提升量子精密测量的灵敏度

上个世纪以来，测量精度的不断提高促进了生物、医学、天文、化学等各个领域的技术和研究的发展。测量精度每提高一个分贝，都可能推动研究的前沿，甚至可能开辟一个新的研究领域。大多数精密测量利用自旋系统或玻色谐振子来探测微弱信号。例如，LIGO 利用激光干涉仪来探测宇宙中的引力波引起的空间振动。在人们的努力下，这些传感器正在接近其最终的经典极限。

近些年发展的量子信息技术利用独特的量子效应，有望实现超越精密测量精度的经典极限。因此在过去十年中，量子精密测量在理论上得到了广泛的研究。人们提出奇异量子态可以提高传感器的信息获取率，许多初步的实验也显示了它们在精密测量方面的潜力。然而，由于环境噪声引起的退相干影响，这些奇异的量子态是脆弱的。与其它量子技术所面临的问题相同，量子优势因而也受到退相干的影响，在实践中难以实现。尽管有人提出可以通过量子纠错来保护量子态的相干性，但在实践中将量子纠错与量子精密测量结合起来极具挑战性。

在过去的几年里，孙麓岩研究组一直致力于量子纠错的研究。最近，他们开发了近似量子纠错和量子跃迁跟踪的方法，首次展示了通过近似玻色量子纠错编码来增强量子精密测量的精度。

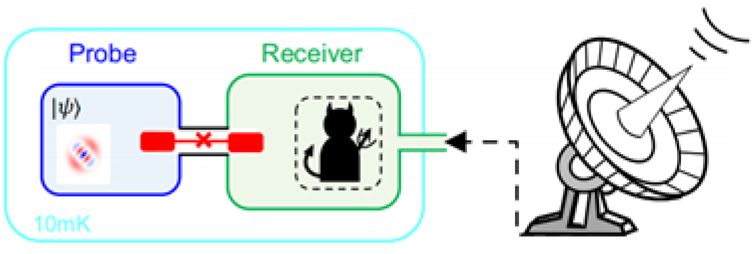


图 1： 实验系统示意图

实验样品由一个超导量子比特分别和两个微波谐振腔耦合组成（如图 1 所示），两个微波谐振腔中寿命高的作为探测腔，寿命低的作为接收腔。实验中先将探测腔内的光场态制备到不同光子态的叠加态上，该状态是一个典型的奇异量子态；再用接收腔接收外界信号源发射的微波信号，通过两个腔之间的相互作用，探测腔内光场叠加态的相对相位会随着时间积累；最后，通过读取探测腔内光场态的相位信息，可以测得接收腔内微波信号强度。同时，在探测过

程中，为了抵抗环境噪声引起的接收腔内光场叠加态的退相干影响，他们在单次实验中多次使用了近似量子纠错操作并能跟踪错误发生的次数，从而增强了该量子精密测量方案可达到的测量灵敏度（如图 2 所示）。

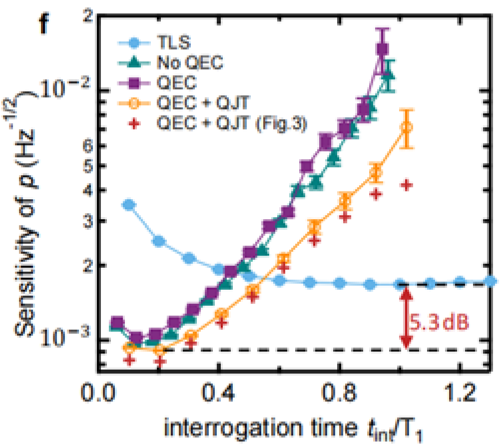


图 2：通过量子态 |1> 和 |7> 的叠加态实现了相比二能级系统 5.3 dB 的灵敏度提升，最好的测量灵敏度达到了 9.1×10^(-4)/ √ Hz

该实验是近年来首次将玻色量子纠错码用于增强量子精密测量的工作，证明了量子纠错可以用于提升量子精密测量的性能。该方案可以扩展到离子阱系统和新兴的量子声学平台。不同于量子纠错在量子信息存储方面的传统应用，该实验所展示的利用近似量子纠错来增强量子精密测量的精度是近期量子应用的新概念，并为未来量子精密测量和量子纠错结合的研究提供了新思路。

该研究成果论文：W. Wang, Z.-J. Chen, X. Liu, W. Cai, Y. Ma, X. Mu, X. Pan, Z. Hua, L. Hu, Y. Xu,H. Wang, Y. P. Song, X.-B. Zou, C.-L. Zou, L. Sun, "Quantum-enhanced radiometry via approximate quantum error correction", Nature Communications 13, 3214 (2022).

四、量子人工智能

主要完成人：邓东灵研究组

量子通道编译

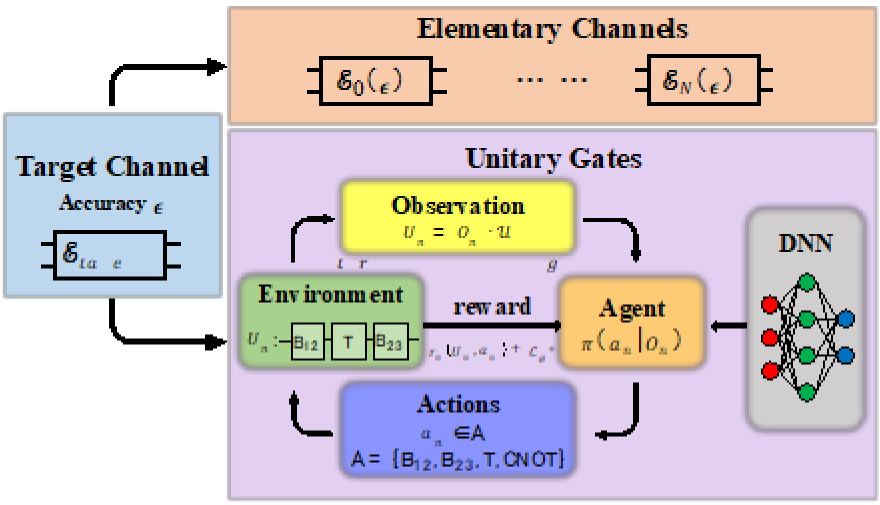
在含噪声中等规模量子计算时代，如何将复杂的量子操作分解成量子器件上可以兼容的基本操作序列是一个非常重要的问题。尽管目前已经有很多关于编译复杂量子门和孤立量子系统演化过程的工作，但是仍然缺少在不使用辅助量子比特的情况下，如何编译量子通道的科学研究。

在该文章中，邓东灵研究组严格证明了两个关于编译量子通道的定理。首先他们证明了定理一，即有限个基本量子通道和一个任意的量子门无法以任意精度编译所有量子通道；但是在有限的精 ε 下，他们可以用有限个和精度相 ε 的基本量子通道，和一个任意的量子门编译所有量子通道，编译序列的长度上限 $O(\frac{1}{\epsilon}\log\frac{1}{\epsilon})$))；之后他们在定理二中证明，以有限的精 ε 编译任意的量子门，至少需 $\Omega(\log(1/\epsilon))$)) 基本的量子门。

在该工作中，邓东灵研究组采用强化学习技术和近端学习优化算法将量子门编译成量子器件可兼容的基础量子门序列，并且在代价函数中对不同的量子门设置不同的权重，从而降低一些实验上实现成本较高的量子门的使用，与之前提出的宽度优先搜索算法相比较，他们提出的算法在训练过程和搜索过程中，需要的时间和内存都显著降低了，有利于未来在更大规模的量子系统上完成编译任务。

本研究引入强化学习算法解决量子通道编译问题，构建了机器学习与量子计算之间新的联系，将对今后相关方向的理论和实验研究提供指导。

该成果研究论文：Weiyuan Gong, Si Jiang, Dong-Ling Deng, "Weighted Quantum Channel Compiling through Proximal Policy Optimization", arXiv:2111.02426v1.



五、拓扑凝聚态物理

主要完成人：徐勇研究组

首次发现里德堡玻璃中的对称性保护拓扑相

对称性保护拓扑相是一种新奇的物相，在不破坏对称性的前提下，其基态拓扑性质在连续变化下保持不变，其独特的体边对应关系和拓扑量子相变使其在凝聚态物理研究中备受关注。尽管人们主要在晶体材料中研究拓扑物相，但最近研究表明，拓扑相也可以存在于无相互作用的二维或三维非晶系统中，甚至，这种结构无序可以诱导出拓扑相。但在实验上观测比较困难。随着实验技术的发展，研究人员已经可以将里德堡原子随意摆放，并在一维规则晶格中观测到了拓扑相，这说明里德堡原子为实现结构无序诱导的拓扑相变提供了理想的平台。

基于光镊操纵的里德堡原子阵列这一实验体系，徐勇研究组在单体和多体层面研究了一维无定形里德堡原子链的拓扑性质，通过使用精确对角化以及矩阵乘积态计算系统基态性质，发现了由手征对称性（单体）和时间反演对称性（多体）保护的无能隙拓扑相（图 1 左）。与此同时，该论文发现通过增加结构无序的强度使系统由晶态向无定形态转变，系统可经过一个拓扑相变由拓扑平庸态变为拓扑非平庸态，对应的拓扑不变量在相变点处由 0 跃变至 0.5，此现象在单体和多体情况均有发生（图 1 右）。

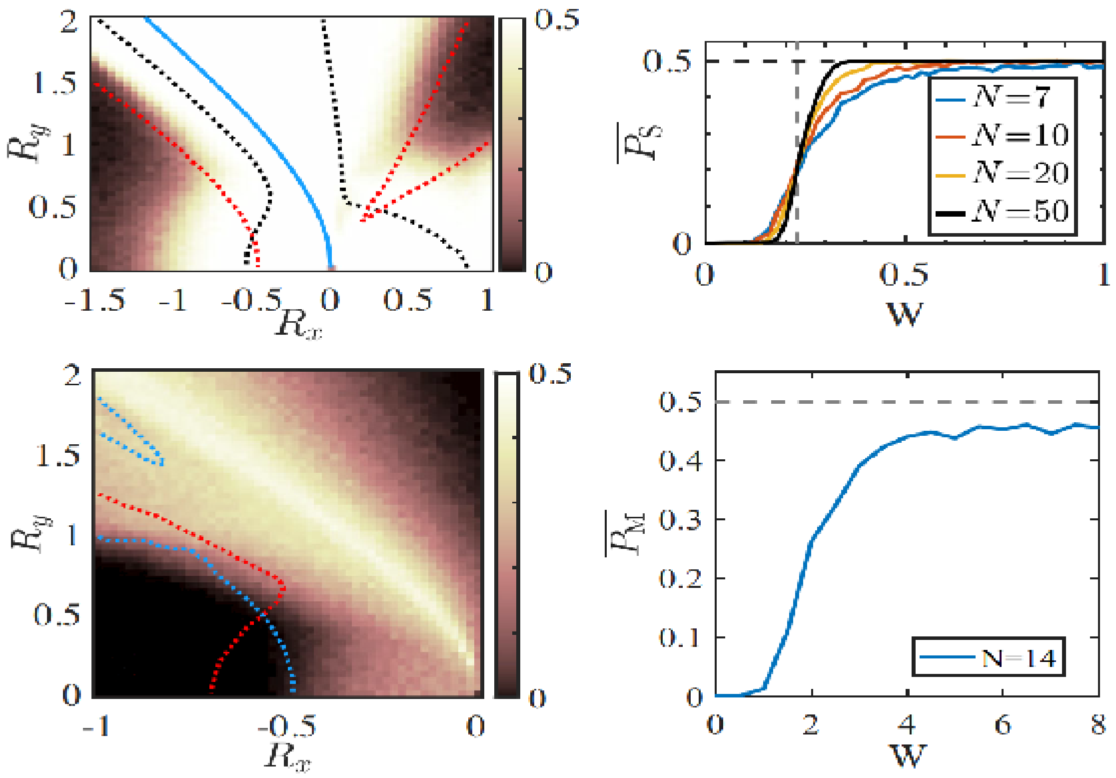


图 1：单体（上）与多体（下）情况下，无定形里德堡原子链的相图与结构无序诱导的拓扑相变

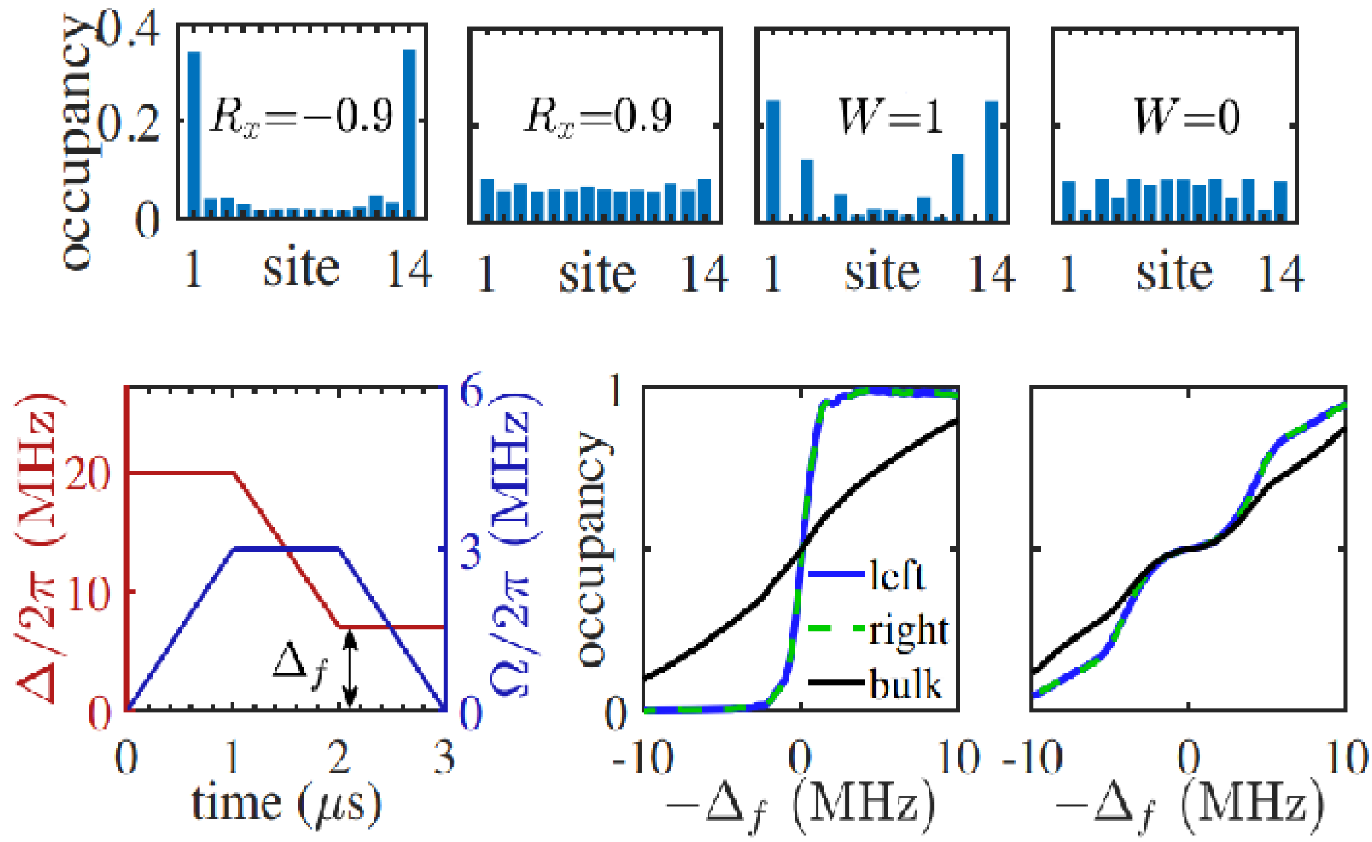


图 2：单体（上）与多体（下）情况下对真实实验体系的模拟结果

此外，为说明上述理论结果均可被实验探测，研究人员模拟了真实实验体系下的动力学演化并计算实验可测量的观测量。模拟结果显示：单体情况下可通过制备零能态并测量其空间分布来刻画系统拓扑，对于拓扑非平庸态，零能态主要集中于边界，而对于拓扑平庸态，其均匀分布于系统中（图 2 上）；多体情况下的拓扑可以由末态边界占据数随失谐的变化来刻画，系统的非平庸性质体现在失谐为 0 处边界占据数的突然变化（图 2 下）。

该成果研究论文：Kai Li, Jiong-Hao Wang, Yan-Bin Yang, and Yong Xu, “Symmetry-Protected Topological Phases in a Rydberg Glass”, Phys. Rev. Lett. 127, 263004 (2021).

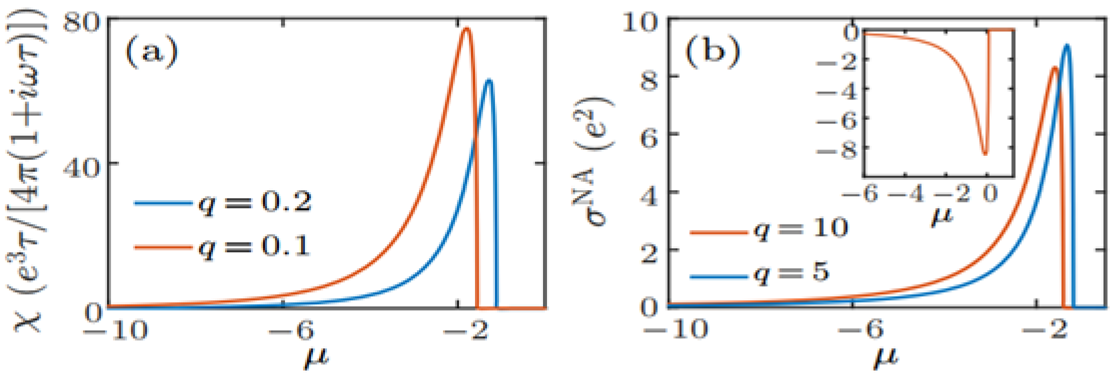
非厄米反常贝里联络诱导的奇异输运现象

非厄米物理用于描述与环境有耦合的体系，可在多种经典和量子的开放系统中存在，受到人们的广泛关注。近期有研究发现无序和强关联凝聚态体系中有限寿命的准粒子可由非厄米物理描述，因此非厄米性质对输运现象的影响成为一个重要问题。事实上，2017 年，研究发现非厄米体系中非厄米反常贝里联络会对布洛赫电子群速度贡献一个反常项 [Phys. Rev. Lett. 118, 045701 (2017)]，但是这一反常速度会对输运性质产生何种影响至今仍不清楚。

最近，徐勇研究组理论上预言非厄米反常贝里联络会在非厄米系统中诱导出厄米系统中不存在的奇异输运现象。研究人员发现，电子在恒定或交变电场作用下会出现反常振荡，据此，研究人员提出基于光波导耦合谐振腔的实验方案观测这种异常现象。另外，传统的固体物理表明波函数的几何结构只会产生霍尔电导，而不会影响纵向电导。研究人员发现，对于非厄米系统，波函数的几何结构不仅会产生霍尔电导，还会对纵向线性电导有贡献。该纵向电导起源于非厄米反常贝里联络贡献的异常速度。类似固有的霍尔电导，该线性电导与散射时间无关。另一方面，在厄米体系中，当能带对称时，二阶非线性纵向电导通常为零。研究人员发现，在非厄米系统中，非厄米反常贝里联络可以产生非零的二阶非线性纵向电导。

非厄米反常贝里联络会使非厄米体系中出现厄米体系中不存在的奇异输运现象，尤其是非厄米反常贝里联络作为一种新的几何结构，会对纵向电导有贡献，这刷新了人们对波函数几何结构的认知。该研究为非厄米体系中输运现象的研究打开了新的方向，将在非厄米物理和强关联材料等领域引起巨大的研究兴趣。

该 成 果 研 究 论 文：Jiong-Hao Wang, Yu-Liang Tao, Yong Xu，“Anomalous Transport Induced by Non-Hermitian Anomalous Berry Connection in Non-Hermitian Systems”，J Chin. Phys. Lett., 2022 39 (1): 010301 Express letter.



非厄米反常贝里联络诱导的 (a) 二阶非线性纵向电导和 (b) 线性纵向电导随化学势变化

清華大學 交叉信息研究院

Institute for Interdisciplinary Information Sciences, Tsinghua University

Edited by Kailin Li

Reviewed by Luming Duan, Jian Li, Xiamin Lv