清華大學 交叉信息研究院
Institute for Interdisciplinary Information Sciences, Tsinghua University

Newsletter

交叉信息研究院

学术科研简报

2020 年 1 月 - 6 月

Institute for Interdisciplinary Information Sciences,
Tsinghua University
IIIS Academic Newsletter
Jan-Jun, 2020

目录

人工智能

量子信息

人工智能

一、计算生物学

主要完成人：曾坚阳研究组（曾坚阳、葛以跃、李舒雅、万方平、洪礼翔等）

发现新冠肺炎潜在有效药物

新型冠状病毒肺炎（COVID-19）疫情在全球的传播已经波及到 200 多个国家和地区。由于特效药和疫苗的缺乏，寻找有效的抗病毒药物从而遏制疫情的进一步传播成为当前的迫切需求。曾坚阳研究组与合作团队通过老药新用、药物重定位方法，从已经获得批准的老药中挖掘其新的用途，成功发现可能有效治疗 COVID-19 的潜在药物。

曾坚阳研究组与合作团队开发了一套药物重定位框架，通过整合机器学习和统计分析等方法，系统地集成并挖掘大规模知识图谱、文献和转录组数据，从老药中寻找新冠病毒的候选药物。使用以 SARS 和 MERS 冠状病毒数据进行的回顾性研究表明，基于机器学习的药物重定位方法可以成功预测针对特定冠状病毒的有效候选药物。结合一系列生物湿实验验证，该计算框架发现聚 ADP-核糖聚合酶 1（PARP1）抑制剂 CVL218 可能是一个治疗 COVID-19 的有效药物。体外细胞实验表明，CVL218 能够有效抑制 SARS-CoV-2 病毒的复制，没有明显的细胞毒性。同时，和另一个抗病毒药物法匹拉韦（favipiravir）的联合用药能够进一步提高 CVL218 对病毒的抑制功效。此外，表面等离子体共振（SPR）实验表明，和同时测定的其它 PARP1 抑制剂或抗病毒药物相比，CVL218 能够以更高的亲和力与 SARS-CoV-2 病毒的核衣壳蛋白（N 蛋白）相互作用。进一步的分子对接（molecular docking）计算模拟结果显示，CVL218 有可能结合在 SARS-CoV-2 病毒 N 蛋白的 N 端结构域（N-terminal domain）上，为 CVL218 的抗病毒机制提供了一种可能的解释。另外，实验发现 CVL218 能够在人外周血单核细胞（PBMC）样本中抑制由脂多糖（LPS）诱导的炎症细胞因子含量升高，表明该药物还可能在减轻 SARS-CoV-2 诱导的过度炎症反应和组织损伤中发挥抗炎作用。在老鼠和猴子体内的药代动力学和毒理学实验表明，CVL218 在肺组织中浓度很高，并且没有明显的毒性迹象，表明该药物具有治疗新冠肺炎的潜力。基于本研究中的数据和先前文献中报道的证据，研究团队还提出了几种可能的机制来解释 CVL218 用于治疗 COVID-19 的潜在作用机理。综合而言，团队开发的药物重定位框架发现的 PARP1 抑制剂 CVL218 可能成为治疗 COVID-19 的潜在有效治疗药物。

PARP1 在 DNA 损伤修复过程中起着重要的作用，是近年来癌症治疗中的重要靶标之一。此前的研究表明，PARP1 抑制剂在病毒复制过程中会妨碍病毒核衣壳蛋白和 RNA 的组装，同时在调控促炎症因子的表达上也起着关键作用。CVL218（又名盐酸美呋哌瑞）是一种 PARP1 抑制剂，目前已进入临床 I / II 期试验阶段。

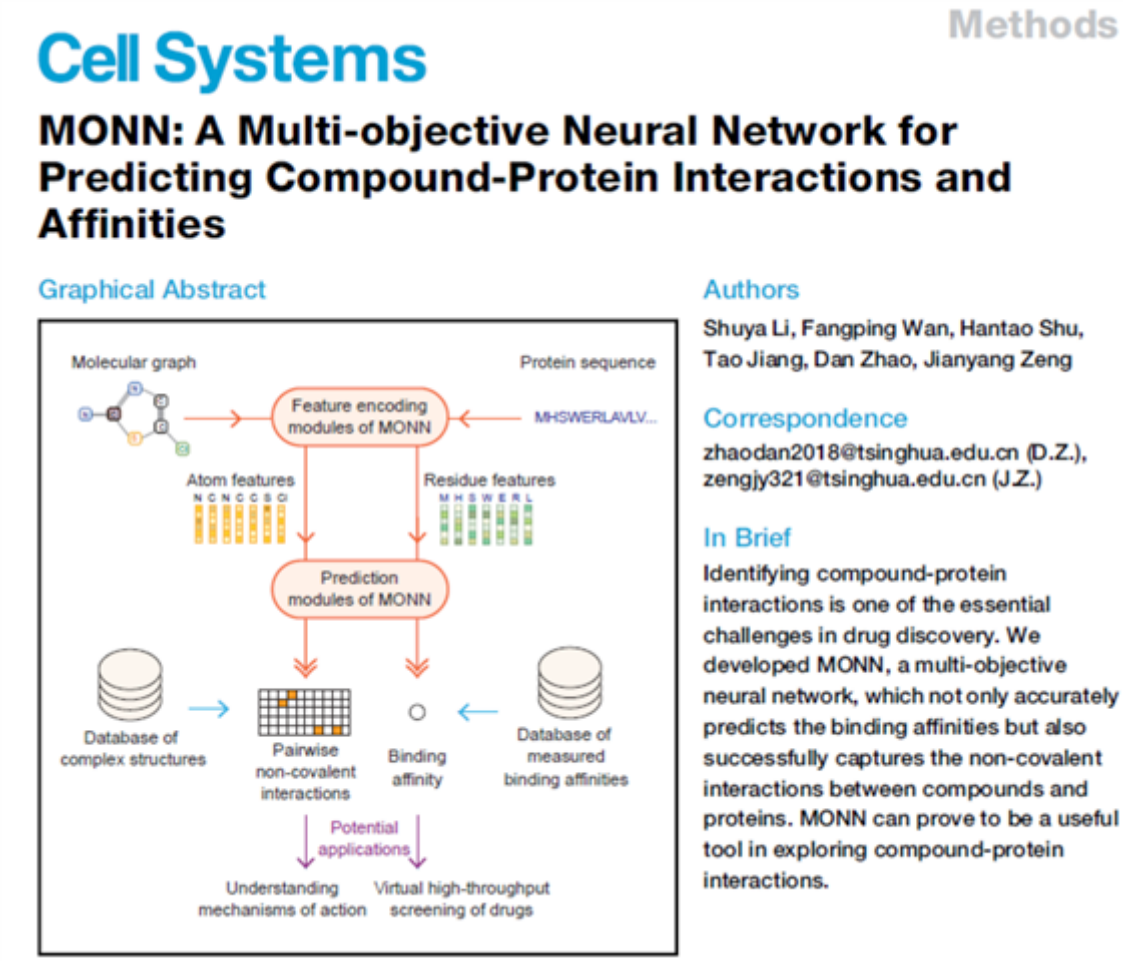
该成果研究论文：Yiyue Ge, Tingzhong Tian, Suling Huang, Fangping Wan, Jingxin Li, Shuya Li, Hui Yang, Lixiang Hong, Nian Wu, Enming Yuan, Lili Cheng, Yipin Lei, Hantao Shu, Xiaolong Feng, Ziyuan Jiang, Ying Chi, Xiling Guo, Lunbiao Cui, Liang Xiao, Zeng Li, Chunhao Yang, Zehong Miao, Haidong Tang, Ligong Chen, Hainian Zeng, Dan Zhao, Fengcai Zhu, Xiaokun Shen, Jianyang Zeng. “A data-driven drug repositioning framework discovered a potential therapeutic agent targeting COVID-19”, bioRxiv 2020.

发现蛋白质 - 小分子间局部共价相互作用和结合强度的深度学习模型

蛋白质 - 小分子相互作用（CPI）是药物研发过程中的关键问题，准确预测这一相互作用有助于提高药物研发的效率。虽然近年来有一些深度学习算法应用在这一领域的工作，但是这些神经网络模型的可解释性仍然比较局限，仅能在少数案例上通过注意力机制分析分子间的结合位点。曾坚阳研究组首次整理了一个大规模数据集来验证现有 CPI 预测模型的可解释性，并发现现有的基于神经网络的注意力机制模型很难自动捕获蛋白质和小分子之间形成的非共价键。

基于上述发现，曾坚阳研究组重新定义了 CPI 预测的机器学习问题，将预测分子间非共价键和预测亲和力这两个任务结合起来，开发了一个多目标神经网络模型，同时预测蛋白质 - 小分子间形成的局部非共价键和亲和力。前者是揭示 CPI 作用机制的重要线索，而后者是虚拟高通量药物分子筛选的重要指标。分子间形成的非共价键会影响其相互作用强度，因此本研究猜测引入这一信息能够更好地帮助亲和力预测，而计算实验也证明了这一假设。测试表明，这一模型在两个任务上均能实现准确的预测，效果优于现有的机器学习模型。在没有可利用的结构信息来支持非共价键预测的大规模虚拟筛选数据集上，模型也能够成功获得优于其他算法的预测效果。除此之外，模型还能够自动捕获分子间相互作用的化学规则。

该成果研究论文：ShuyaLi, FangpingWan, HantaoShu, TaoJiang, DanZhao, JianyangZeng. "MONN: a multi-objective neural network for predicting compound-protein interactions and affinities", Cell Systems 2020.



提出从大规模科学文献中提取生物医学实体关系的新型深度学习模型

理解药物、靶点、病毒、副作用等等生物医学实体之间的相互作用规律，是生物医学研究者们长期以来致力于探索和研究的问题，关于这些作用规律的研究成果广泛分布在超过 3 千万篇的科研文献当中，且文献的数量还在不断增加。目前，大多数知名的生物医学数据库，例如 DrugBank、CTD、SIDER 和 BioGRID，都是由人类科学家花费大量的时间和精力从科学文献中整理而来的。虽然深度学习技术可以被用来加速这一过程，但在生物医学这种专业性领域，大规模的训练数据却并非能够轻易得到。为了解决这一问题，来自清华大学的曾坚阳研究团队采用了一种基于远监督的深度学习策略，使得模型能够在不依赖于人工标注数据的情况下应用到各种生物医学关系抽取场景当中。此外，作者所提出的集成了隐式句法树学习和注意力机制的模型，在多项生物医学关系抽取任务当中，都取得了领先的实验结果。这项研究成果表明，这种新型的机器学习框架能够为生物医学关系发现提供有力的帮助。目前，该工作已被应用到一项旨在从已有的老药中发现治疗 COVID-19 的潜在药物的工作当中，相关的研究成果已发布在生物预印本网站 bioRxiv 上。

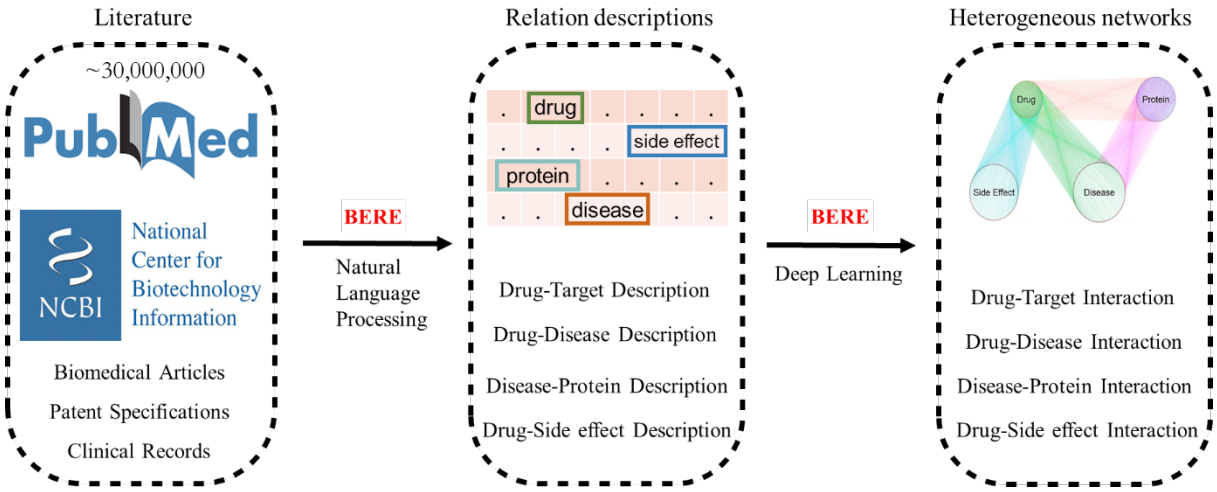
目前，曾坚阳研究组所提出的生物医学关系自动抽取框架已成功应用到多个生物医学场景当中，包括：

1. 通过抽取出的提示性信息指导了若干湿实验验证，从而确认了新的药物 - 靶点作用关系。

2. 在一项针对新冠肺炎的老药新用研发任务中，该关系抽取模型被应用到一个回顾性研究当中，即通过查找文献支持来验证针对 SARS 或 MERS 的老药新用策略的可行性，从而间接证明该老药新用策略针对 COVID-19 的有效性。

3. 针对更多的生物实体间的作用关系抽取，如病毒 - 宿主、药物 - 副作用间的关系抽取，该框架已在初步实验中验证了其有效性。

该成果研究论文：Lixiang Hong, Jinjian Lin, Shuya Li, Fangping Wan, Hui Yang, Tao Jiang, Dan Zhao, Jianyang Zeng. “A novel machine learning framework for automated biomedical relation extraction from large-scale literature repositories”, Nature Machine Intelligence 2020.



二、机器学习

主要完成人：李建研究组（李建、李志泽）、黄隆波研究组（黄隆波、潘玲、杜伊涵、汪思为等）、张崇洁研究组（张崇洁、王同翰等）

优化理论进展：Anderson 加速算法的最优性理论证明

Anderson 加速是定点迭代的有效加速方法。例如，梯度下降可以看作是一种典型的迭代算法。Anderson 加速很早由 Anderson 在 1965 年提出，在实践中非常有效。这种方法可以看作是非线性问题的 Krylov 子空间方法的扩展，因此大家猜测 Anderson 加速至少在强凸优化种可以达到最优的收敛速率。在本文中，李建研究组证明结合了 Chebyshev 多项式系数的 Anderson 加速可以达到最佳收敛速度 O（k $\sqrt{}$ ln1/ε），从而改进了（Toth and Kelley，2015）为二次函数先前结果 O（kln1ε）。最后，该研究组的实验结果表明，提出的 Anderson-Chebyshev 加速方法的收敛速度明显快于其他算法，例如普通梯度下降法（GD），著名的 Nestorov 的 Accelerated GD 法。

该成果研究论文：Zhize Li, Jian Li. "A Fast Anderson-Chebyshev Acceleration for Nonlinear Optimization"，AISTATS 2020.

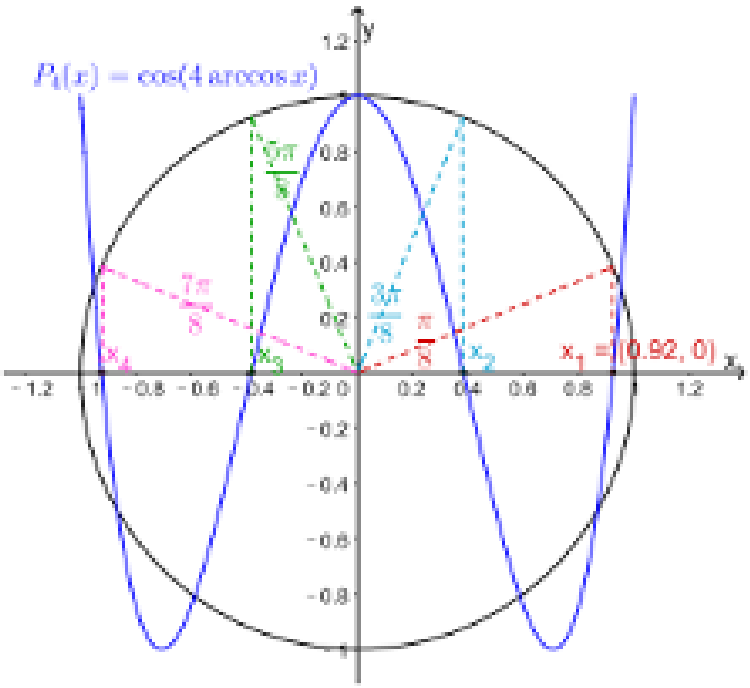


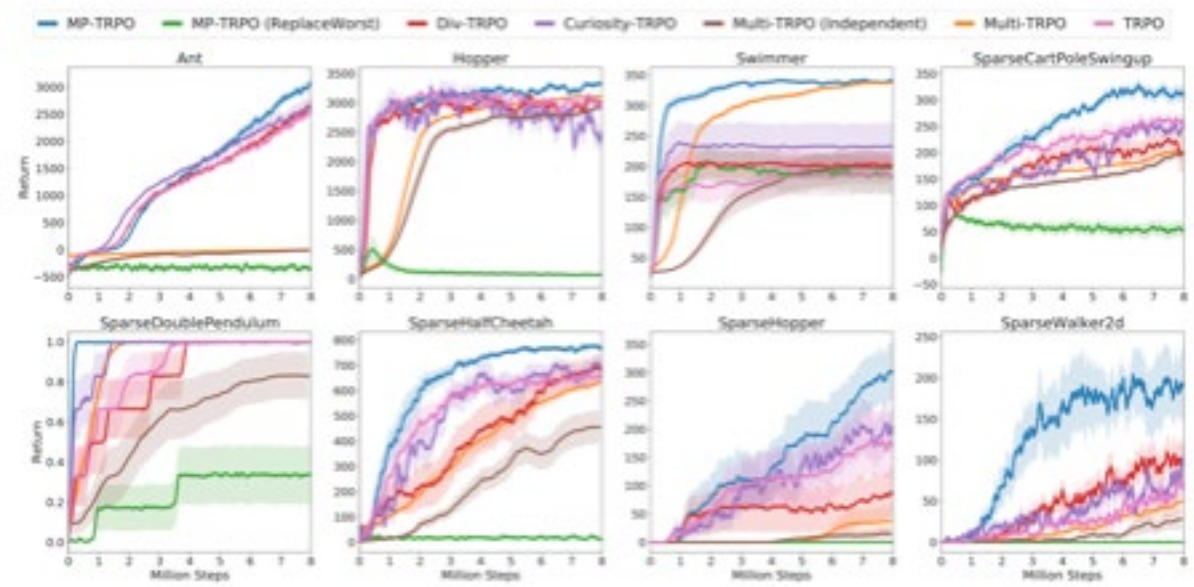
Figure 1: The Chebyshev polynomial $P_4(x)$

多路策略优化

在强化学习中，智能体通过与未知的环境交互来学习最大化长期奖励的最优策略。对于强化学习算法而言，尤其是对于 on-policy 算法，一个困难的问题在于智能体可能缺乏高效的探索能力。之前的探索方法一般需要依赖于复杂的结构来估计状态的新颖性，或者对超参数敏感，会导致性能不稳定。

黄隆波研究组提出一种高效的探索方法，多路策略优化 (Multi-Path Policy Optimization, MPPO) 算法，不会带来较高的计算开销，同时能够保证稳定性。MPPO 算法维护了一个高效的探索机制——利用一个多样化的策略种群来提升探索能力，在奖励信号稀疏的环境中尤为有效。同时，该方法在理论上有稳定的性能保证。该研究组将 MPPO 算法应用于两类广泛使用的 on-policy 方法——TRPO 算法和 PPO 算法，并在若干个传统的以及稀疏化奖励信号的 MuJoCo 平台上进行了充分的实验验证。实验结果表明 MPPO 能够在采样效率以及最终性能上表现优于目前的方法。

该成果研究论文：Ling Pan, Qingpeng Cai, Longbo Huang. “Multi-Path Policy Optimization”, AAMAS 2020.

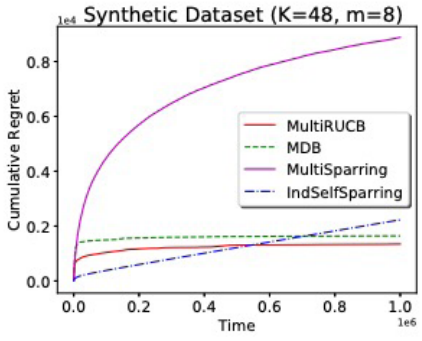


多臂老虎机问题：从双对决到多对决的算法分析

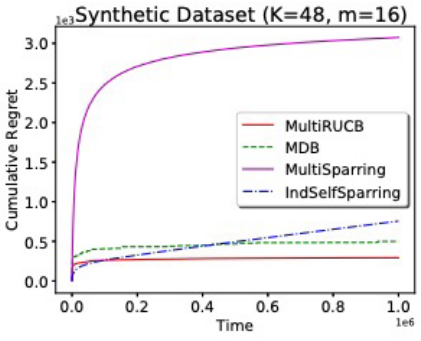
多臂老虎机(Multi-Armed Bandit)是一个经典的在线学习问题，并且在临床试验、在线广告等领域被广泛应用。对决老虎机（Dueling Bandit）问题是多臂老虎机的一个重要变体，特别适用于推荐系统、信息检索等涉及到用户主观反馈的领域。现有的对决老虎机算法主要侧重于双对决（Two-dueling Bandit），即每次只对两个待学习项目（即“臂”）采样。但是在一些应用场景中需要同时对多个待学习项目采样。例如，在运动损伤的临床试验中，由于运动损伤恢复情况难以定量评估，医生常常通过比较不同受试者的恢复情况来判断不同治疗方法的优劣。而临床试验是十分耗时且昂贵的，医生常常在一次试验中比较多种不同的治疗方法。针对这种场景，多对决老虎机（Multi-dueling Bandit）是一个非常适用的在线学习模型。

现有的多对决老虎机研究只有实验结果分析和渐进时间的理论结果分析，黄隆波研究组首次给出了多对决老虎机问题有限时间的理论结果分析。在这项工作中，他们首先分析双对决老虎机问题，基于现有算法提出了两个新的双对决老虎机算法，并给出了实验和理论结果分析。两个新算法的实验和理论结果均明显优于其原有算法。进一步地，他们分析多对决老虎机问题，提出了新的多对决老虎机算法，并给出了优于现有算法的实验结果和新颖的有限时间理论结果分析，为经典的多臂老虎机问题中从双对决到多对决的算法分析做出了贡献。

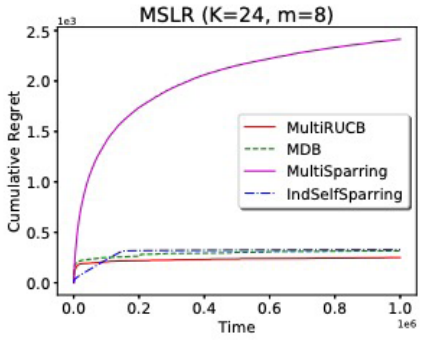
该成果研究论文：Yihan Du, Siwei Wang and Longbo Huang, “Dueling Bandits: From Two-dueling to Multi-dueling”, Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2020.



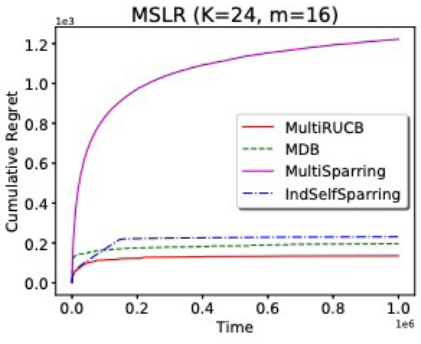
(a) Synthetic, $K = 48$, $m = 8$



(b) Synthetic, $K = 48$, $m = 16$



(c) MSLR, $K = 24$, $m = 8$



(d) MSLR, $K = 24$, $m = 16$

基于角色涌现的多智能体强化学习

近期协同多智能体强化学习取得了显著进展，相关工作提出了许多基于深度学习的方法。为了可拓展性，这些方法往往会让所有智能体共享同一个值网络或者策略网络。但在有复杂子任务的测试环境下，该共享网络需要表征所有的子任务策略，这导致共享同一个网络并不有效。另一方面，每个智能体使用一个单独的网络也是没必要的，因为某些智能体会经常处理相似子任务。因此，如何利用智能体的分工来动态地共享网络参数以提升学习性能成为了问题的关键。

张崇洁研究组对于这一领域进行了开创性研究，首次建立了基于角色理论的多智能体强化学习框架 ROMA，研究了通过引入角色来更高效地解决有复杂子任务的多智能体问题。该框架中，角色是涌现的而不是预定义的，拥有相似角色的智能体会共享训练以及专注于某个子任务。为了达到这个目标，作者通过引入两个新颖的正则项来构建一个随机角色嵌入空间，然后将每个智能体的策略取决于自己的采样角色。在星际争霸 2 测试环境上该算法获得了超过其他相关算法性能，同时可视化实验表明该框架在同质和异质的环境中都能学到专业化的、动态的、可识别的角色，以及拥有相似子任务的智能体拥有相似的角色，除此之外对角色的演化和涌现过程的展示也深刻表现了角色驱动的子任务专业化和集体性能提高的关联。总之，这篇工作提供了一个理解和促进智能体协作涌现的新视角。

该成果研究论文：Tonghan Wang, Heng Dong, Victor Lesser, Chongjie Zhang. “ROMA: Multi-Agent Reinforcement Learning with Emergent Roles”, ICML 2020.

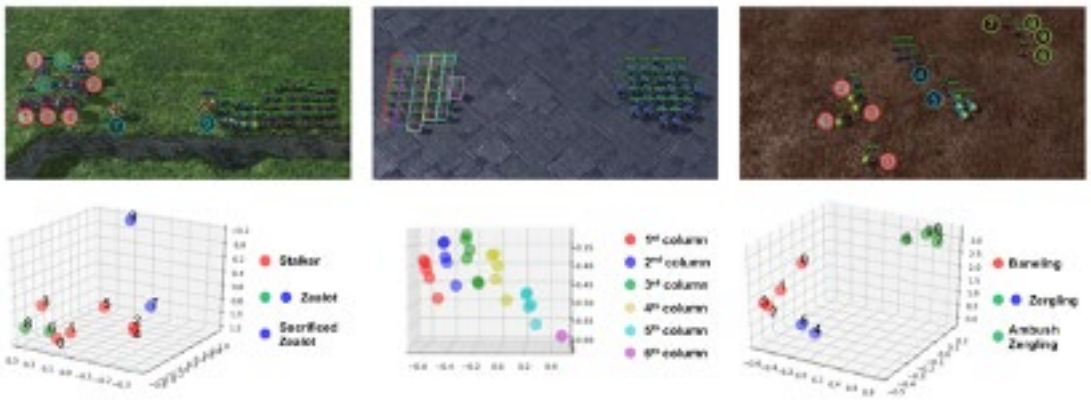


图 1：三个地图上角色的表征以及对应的自动发现的子任务

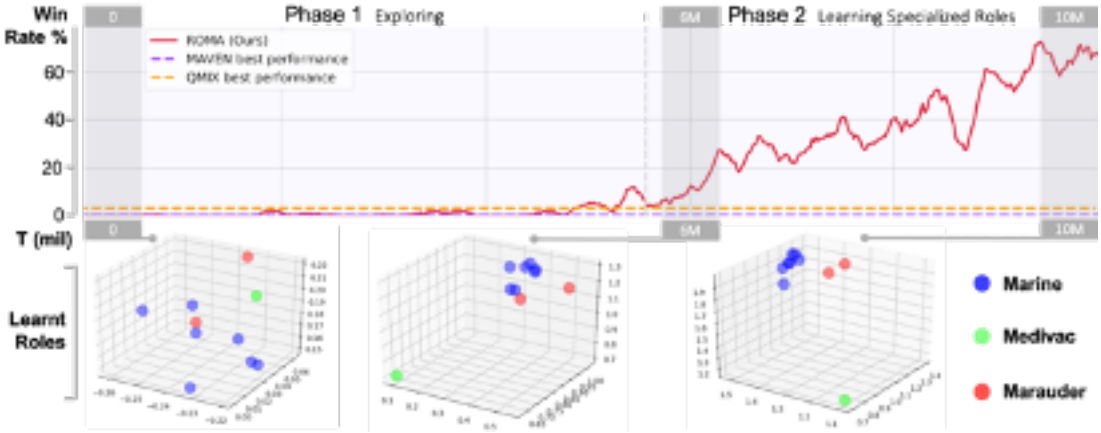


图 2：在地图 MMM2 上角色的演化和涌现过程

三、前沿架构与智能芯片

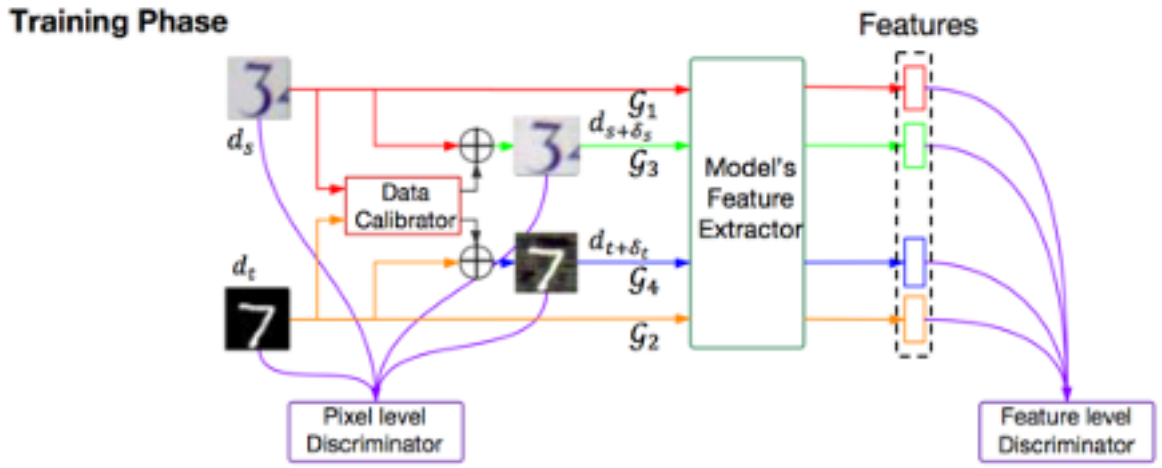
主要完成人：马恺声研究组（马恺声、叶绍凯、张林峰等）

一种用于领域适应的可分离的轻量级组件

由于现实世界能够收集的数据在数量和多样性上有限，领域适应的研究近些年在自动驾驶和机器人等应用上拥有广泛的应用价值。人们通常使用虚拟环境来制造标签数据集，被称为原始数据集，然后在其上训练模型，最后在现实世界的目标数据集上微调并使用。然而，在另一类使用场景中，原始数据集也可能直接由现实数据组成。过去的领域适应方法只希望提高神经网络在目标数据集上的效果而忽略了其在原始数据集上的性能。实验结果显示，过去的领域适应方法往往对于原始数据集上的性能有较大损伤。领域适应算法的另一个突出的问题在于其灵活性。过去的领域适应方法通常需要更新网络的权重。然而，大部分网络因为参数量过大的缘故会使用模型压缩方法来减少存储。这意味着如果模型遭遇了新的环境，将会无法对环境进行反应。

马恺声研究组提出通过训练一种轻量级的可分离的领域适应组件以解决上述问题。在模型训练过程中，针对输入图片制造出类似于对抗扰动的噪音来欺骗放置于图片端和特征端的领域分类器。当领域分类器无力分辨图片来自哪个领域后，领域适应组件通过修改数据来帮助被部署在终端的网络进行领域适应。该方法在 Digits 的多个数据集和 GTA5 到 CityScapes 的领域适应中超过了前人的结果。同时，该研究组创新性地提出，类似对抗攻击的方法实际可以制造有益的扰动，将对抗攻防的研究和领域适应的研究第一次进行了连接。

该成果研究论文：Shaokai Ye, Kailu Wu, Mu Zhou, Yunfei Yang, Sia Huat Tan, Kaidi Xu, Jiebo Song, Chenglong Bao, Kaisheng Ma. “Light-weight Calibrator: A Separable Component for Unsupervised Domain Adaptation”, CVPR2020.

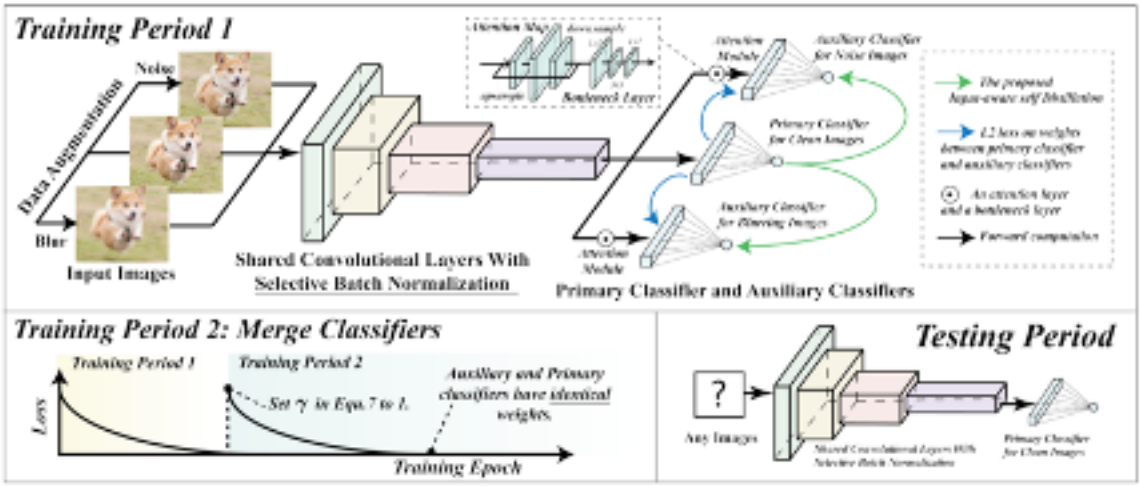


通过辅助训练算法同时提高神经网络的准确率与鲁棒性

以神经网络为基础的计算机视觉模型对于现实世界中图片的旋转、模糊、雨雾等情况极其敏感，这严重限制了此类算法在真实应用场景下的部署。解决该问题的传统方法是数据增强，即在神经网络的训练过程中加入人工合成的旋转、模糊等类型图片。然而，实验结果显示这种数据增强的算法虽然可以提高神经网络的鲁棒性，但是常常会对神经网络的准确率带来负面影响，这也是现实应用中无法接受的。

为了解决该问题，马恺声研究组提出了一种新型的神经网络训练方法——辅助训练算法。辅助训练算法将数据增强下的网络训练视为一个多任务学习问题，不同类型的数据增强被视为不同的任务。在神经网络的训练初期，多个任务共享同一个卷积网络以提取特征，而在不同的全连接层中分类，并通过一种新型的选择性批标准化算法和输入相关的知识蒸馏算法训练。在训练末期，辅助训练算法将多个任务的全连接层分类器进行融合，最终实现在不增加网络计算量、参数量，不修改网络结构的前提下，极大程度地提高了网络对于自然图片损坏的鲁棒性与预测准确率。同时，实验显示辅助训练算法对于各类对抗样本的防御同样有积极效果。该算法的提出，首次实现了同时提高神经网络的鲁棒性与准确率，对于人工智能技术在现实场景中的落地应用有很大的积极影响。

该成果研究论文：Linfeng Zhang, Muzhou Yu, Tong Chen, Zuoqiang Shi, Chenglong Bao, Kaisheng Ma. “Auxiliary Training: Towards Accurate and Robust Models”, CVPR2020.



四、网络科学

主要完成人：徐葳研究组（徐葳、张晗、高凯文、陈天佳等）、黄隆波研究组（黄隆波、李玉星等）、吴文斐研究组（吴文斐、邓帮文等）

基于对抗分布的高维空间异构统计特征识别无监督学习框架

机器学习任务中，高质量的样本标签采集十分昂贵且耗时。例如在反欺诈应用中，获取到的样本标签往往意味着巨大的经济损失，而且获取到的样本标签往往会失效，因为欺诈者会弃用这些已经暴露的资源（例如网络 IP 地址、电话或身份证号码等）。因此，无监督学习成为了这些应用中更可靠的手段。传统的无监督学习旨在利用数据之间相似的统计特征将数据划分为不同的类簇再分析，但是随着大数据时代的来临，数据维度逐渐增高，数据中不同类簇的统计特征也越发呈现出异构的现象。例如，欺诈数据中的恶意账户往往只会在某些特征上显示出明显的统计特性，且不同的欺诈群组的统计特性不同。

为了解决高维空间中异构统计特征识别的问题，徐葳研究组提出基于对抗分布的无监督学习框架。对抗分布定义为偏好不同统计特征的一组分布，通过让对抗分布在拟合数据上进行竞争，更能建模某一类簇统计特征的分布会从对抗分布中胜出。通过最大化似然框架，对于不同的类簇模型会适应性地学到最合适的对抗分布以描述其统计特征。并且由于该框架属于概率图模型，框架具有很强的概率推理能力以及很高的可解释性，因此具有很高的扩展性和可靠性。徐葳研究组将该模型应用在了欺诈检测和异常检测两个重要的应用场景中，该方法被证实在两个应用中均有大大超过已有算法的表现。

该成果研究论文：Han Zhang, Wenhao Zheng, Charley Chen, Kevin Gao, Yao Hu, Ling Huang, Wei Xu. “Modeling Heterogeneous Statistical Patterns in High-dimensional Data by Adversarial Distributions: An Unsupervised Generative Framework”, Proceedings of The Web Conference 2020.

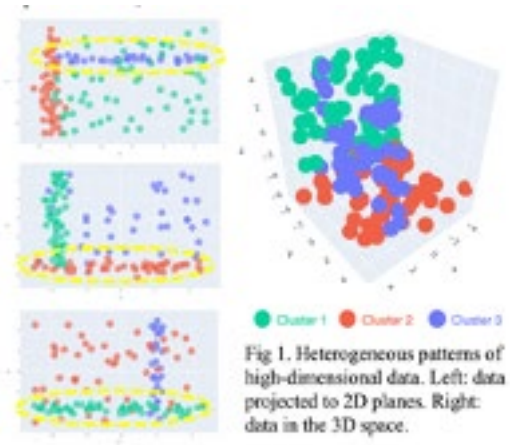
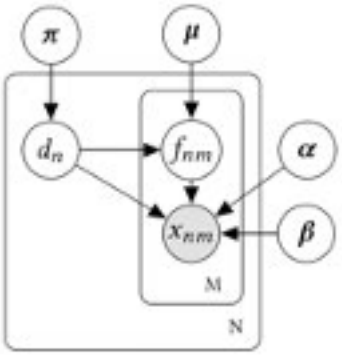


Fig 1. Heterogeneous patterns of high-dimensional data. Left: data projected to 2D planes. Right: data in the 3D space.



基于优化理论的计算机网络传输层拥塞控制优化

计算机网络传输层拥塞控制旨在通过更合理的数据包发送策略设计以达到数据传输高吞吐量、低延迟、低延迟抖动的控制目标。发送端通过收集数据包传输过程中所能获取到的传输状态信息，如往返时间、数据包头特殊数据位标记等，对数据包发送的频率、一次性发送数据量大小等信息进行决策，使得整个数据包能够完整、快速的到达接收端。近年来，许多工作从网络中间设备着手，通过数据包标记和筛选对数据传输进行了优化。但是越来越多的工作也证明，由于计算机网络硬件设备的不断发展，我们仅使用发送端收集到的状态信息足以对数据传输过程进行有效的优化。

黄隆波研究组利用基于优化理论的思想，仅使用发送端收集到的状态信息进行网络控制，设计了一种端到端的控制协议 RTCP，达到了非常好的传输控制效果。该工作使用优化理论的李雅普诺夫方法，巧妙地引入了辅助变量对传统效用方程进行填充，将网络连接中对单速率变量的控制转化为对网络连接设备数据包积压的调整，形成了 RTCP 最终的控制策略。通过在试验台和模拟环境中的不同传输场景中进行部署和评估，该研究组验证了相比于当前的主流传输层拥塞控制算法如 DCTCP, BBR, PCC, LEDBAT, TIMELY, Vegas, Cubic 和 NewReno，RTCP 不仅部署方便，而且其在保持稳定吞吐量的同时有效降低了数据流的延迟和延迟抖动。

该成果研究论文：Longbo Huang, Yuxing Li, Jean Walrand. “RTCP Reduce Delay Variability with an Endtoend Approach”, IFIP Networking 2020.

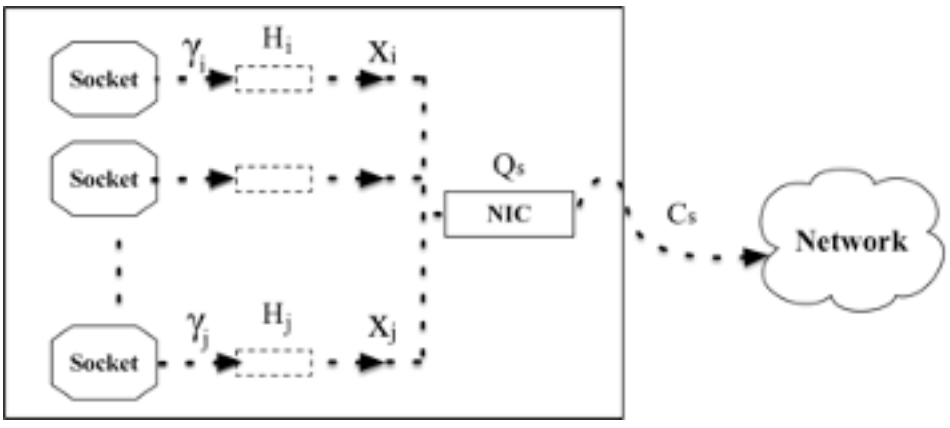


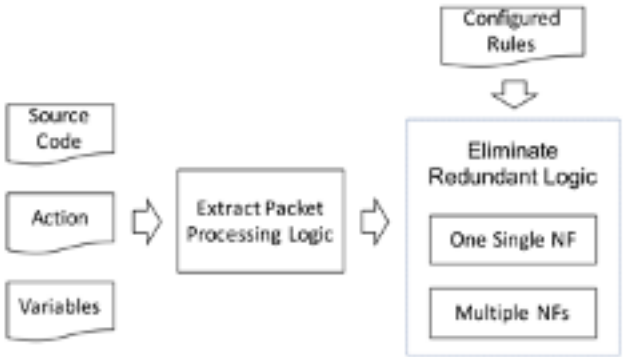
Figure 1 RTCP introduces a virtual counter H for the deficit between the “desired rate” and the “actual rate” at each socket, which smooths the packet sending.

首次提出利用软件分析技术消除网络功能冗余逻辑

作为现今网络数据平面里重要的组成成分，虚拟网络功能软件（如防火墙）处理着所有通过的网络数据流量，因此，它们对网络数据包的处理效率以延迟累积等方式严重地影响着整个网络的端对端性能。近年来学者们主要从以下两个方面提升网络功能软件的性能，一方面是通过专用硬件如 FPGA、GPU 等提升网络功能软件对网络数据包的处理效率，另一方面是通过探索网络功能软件间的并行可能性，使网络功能间的处理过程并行化，从而提升网络的端对端性能。

与目前主流方法不同，吴文斐研究组从网络功能软件本身出发，首次提出以软件分析的方式，结合实际网络的特性，消除网络功能软件内在的冗余逻辑，从而提升其网络性能。研究组不仅总结和分类了三种存在于网络功能软件中的冗余逻辑，还针对这些冗余，以 LLVM 平台为基础实现了名叫 NFReducer 的优化原型，在示例开源网络功能软件上取得了明显的优化效果。该工作证明了网络功能软件中存在着冗余逻辑，并提出了新的性能优化方法，为进一步提升网络功能性能提供了新的思路。

该成果研究论文：Bangwen Deng , Wenfei Wu, Linhai Song. "Redundant Logic Elimination in Network Functions", SOSR 2020.

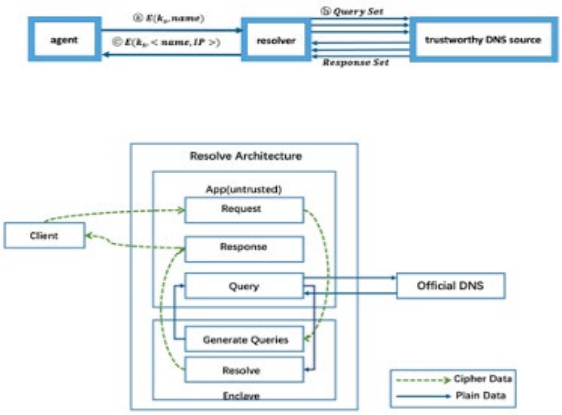


T2DNS: 具有隐私保护功能的可信第三方 DNS 服务

近年来，互联网域名系统 (DNS) 的安全问题引起了广泛的关注，然而目前已有的解决方案大多都集中于解决通信通道上的攻击，并假定用户的终端主机或官方 DNS 服务器是可信的，但这是不对的。因为用户的终端主机甚至官方 DNS 服务器都有可能受到恶意程序的攻击。

针对以上问题，吴文斐研究组利用 Intel 的可信计算技术 SGX(Intel SoftwareGuard Extensions) 以及密码学理论设计了一个能保护用户隐私的可信第三方 DNS 服务，名为 T2DNS。T2DNS 结合了加密协议、混淆机制、可信执行环境和远程认证机制，它除了利用相关密码学加密技术来避免监听，还可以提供运行时的内存保护和初始化时程序的远程认证来防止恶意程序篡改和攻击，下图为 T2DNS 的 overview 和 workflow。评估结果表明，T2DNS 不仅可以部署在现有的互联网基础设施上（不用修改互联网基础设施），还能抵御信道上、用户终端和官方 DNS 服务器的监听和攻击，同时具有优秀的性能。

该成果研究论文：Qingxiu Liu, Wenfei Wu, Qingsong Liu, and Qun Huang. “T2DNS: A Third-Party DNS Service with Privacy Preservation and Trustworthiness”, ICCCN 2020.



五、计算经济学

主要完成人：唐平中研究组（唐平中、赵晟宇等）

首次刻画“群体策略防护”的非确定性机制

“策略防护”（strategyproof）的机制设计问题在经济学和理论计算机科学都有着极为重要的学术地位。早在40年前，Moulin等理论经济学者们就开始刻画在单峰偏好下策略防护的投票机制，并进一步将其拓展到高维空间中。然而，非确定性的机制刻画至今仍然是该领域的尚未解决的主要难题。从10年前开始，Procaccia等学者开始研究在社会成本（social cost）与最大成本（maximum cost）意义下一维空间中的近似机制设计，并发现在策略防护与群体策略防护的条件下，一些非确定性的机制具有比确定性机制显著更好的界。大量后续工作进一步研究在非线性代价、离散网络上的近似机制设计。然而，没有任何工作适用于高维空间中的非确定性机制设计。

唐平中副教授，2017级本科生赵晟宇与2014级校友俞鼎力，首次成功刻画了任意维度严格凸空间中群体策略防护的确定性与非确定性机制。该研究证明任意确定性的、一致的、群体策略防护的机制必须是独裁的（dictatorial）；任意非确定性的、一致的、平移不变的、群体策略防护的机制必须是2-独裁的（2-dictatorial）。这一结论直接推出在社会成本与最大成本意义下群体策略防护的确定性与非确定性近似机制的紧界，突破性地解决了任意严格凸空间中群体策略防护的机制设计问题。

该成果研究论文：Tang Pingzhong, Yu Dingli, Zhao Shengyu. “Characterization of Group-Strategyproof Mechanisms for Facility Location in Strictly Convex Space”, EC 2020.

首次提出“非透视”动态机制设计框架

最优机制设计问题（又名最优拍卖问题）在经济学和理论计算机科学都有着极为重要的学术地位。在理论方面，从40年前诺贝尔经济学奖得主Roger Myerson的单个商品最优拍卖开山之作，到5年前，图灵奖得主姚期智院士震惊世界地解决多商品最优拍卖的常数近似，最优拍卖理论在微观经济学与理论计算机科学中一直是公认的、最具挑战的科研高峰。在工业应用方面，全球每年3000亿美元在线广告市场均由自动拍卖完成定价与交易。每天数以千亿计的用户访问都通过广告拍卖精准的分配给渴求市场推广的大中小型企业，帮助中小型企业完成赖以生存地产品宣发和品牌推广。如何设计最优拍卖，并应用于互联网广告，是一个国家互联网的核心竞争力和最基础的经济学问题之一。

尽管最优拍卖理论在过去的四十年有了长足的发展，然而广泛应用于互联网广告拍卖的理论却存在致命的缺陷：这类拍卖源于单轮静态拍卖环境，面对动态重复地互联网环境，难以保证理论最优和实际收益。交叉信息院长聘副教授唐平中与左淞博士，以及谷歌研究院的合作者们从根本上指出了传统理论与实际需求的出入，首次提出了“非透视”（non-clairvoyance）的动态机制设计框架，并用这个框架充分地描述了实践中最为关键的买方鲁棒性需求。在该框架下，完全刻画了最优动态拍卖机制的形式，并进一步给出了该形式下具有简单结构的（渐进）最优机制。该结果在理论与实践中具有重要的双重意义：一方面首次在理论研究中原创性地引入了实践中具有关键意义的框架，而另一方面，其理论结果对实践中动态拍卖的设计具有积极的指导意义。

该成果研究论文：Vahab Mirrokni, Renato Paes Leme, Pingzhong Tang, Song Zuo. “Non-clairvoyant Dynamic Mechanism Design”, Econometrica 2020.

六、能源经济学

主要完成人：吴辰晔研究组（吴辰晔、孙健、吴佳蔓、张家声、崔竞时等）

针对不平衡数据集的导线舞动预测算法设计

输电线路舞动指的是架空高压传输线的低频高振幅运动。由于架空输电线路杆塔的大跨度高耸结构等因素，极端天气可造成输电线路的舞动现象，容易引起相间闪络，造成线路跳闸停电，甚至杆塔倒塌，给电网的安全运行带来较大的危害。因此高精度预测导线舞动对于提升电网稳定性具有重要意义。

基于物理理论模型的预测方法目前无法提供高精度的预测结果。随着测量仪器的发展，数据驱动的预测模型得到了广泛的关注。然而数据驱动的模型遭遇两点挑战：一是导线舞动数据主要在极端天气下获得，数据占比小，数据集严重不平衡。二是铺设高精度测量仪器成本过高，难以大范围推广。

作为这一领域的突破性进展，吴辰晔研究组首先探究了数据体量、数据集平衡程度、训练集与测试集分布差异程度对于机器学习预测器性能的影响，得出了“平衡数据集前提下，大体量数据有助于提高预测准确率”、“训练集与测试集分布差异越大，预测准确率越低”等诸多对于数据预处理工作具有指导性意见的重要结论。同时，吴辰晔研究组立足于工程实际，探究高精度仪器之间的可替代性，旨在降低工程成本，通过研究特征的重要性，尝试不同特征的排列组合，得到了 F1 score 高达 98% 的特征预测器，该探测器仅需要三种特征，大大降低了舞动预测的建设成本。

该项成果共发表了两篇论文。其中一篇被 IEEE PES General Meeting 2020 录用，并获得了最佳论文奖，另一篇已投稿至 IEEE SmartGridComm 2020。

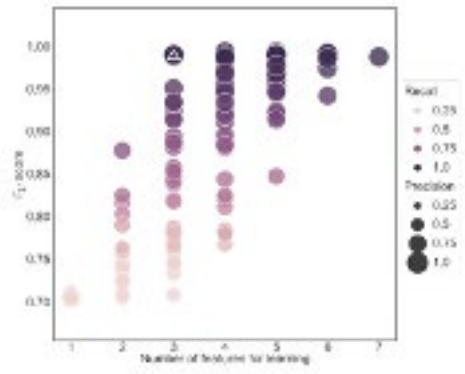


图 1：不同特征组合模型的性能：我们检测了全部特征组合模型（共 127 种），其中白色三角形指出，存在某三特征预测器（风速，温度，降水量）可达到最佳表现——F1 score 高达 98%。

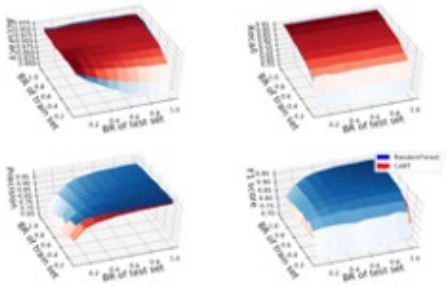


图 2：训练集与测试集的平衡程度（BR）对于不同分类器性能的影响：图中颜色越深表示性能越佳。

电力市场双边拍卖机制设计

电力市场由于其复杂的潜在物理约束而遭受市场操纵。大多数现有市场都采用双边拍卖来组织市场：独立的系统运营商从供应双方收集竞标信息，并采用瓦尔拉斯均衡以进行调度。在实际的运营过程中，市场参与者经常会汇报虚假信息以操纵市场价格。因此，为了遏制这种操纵，一种可行的解决方案是设计双边拍卖机制以确保真实的竞标信息。我们比较将四种双边拍卖机制（瓦尔拉斯均衡机制，VCG 机制，MUDA（Lottery）机制和 MUDA（VCG）机制）应用在电力市场中的可能性，并提出了评估各种机制性能的关键指标。在此基础上，我们根据真实的市场数据进行了广泛的仿真研究，以对四种机制进行全面比较，并确定每种机制的独特特征（图 1-2）。这可以作为电力市场双边拍卖机制设计的理论指导。本篇论文已投稿至 IEEE Smart Grid Comm 2020.

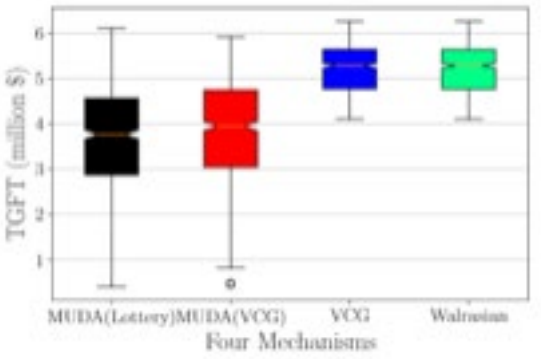


图 1 四种机制的社会总福利

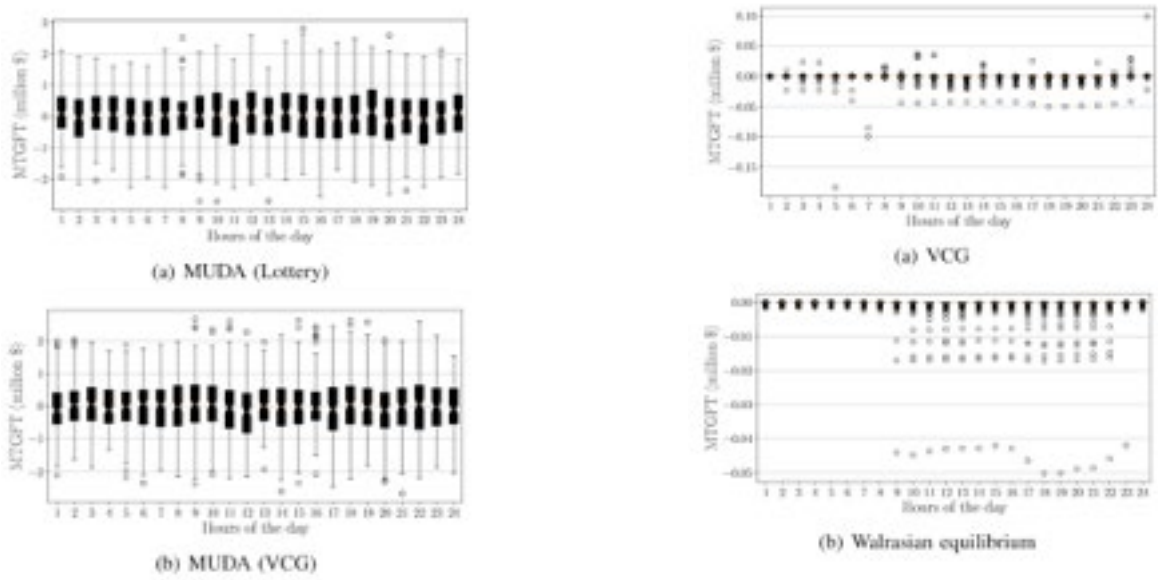


图 2 四种机制的边际社会总福利

深度学习在储能设备控制上的应用

深度学习方案的主要优势之一是能够进行准确的各类预测。我们利用这一优势试图解决存在双重不确定性（动态价格和可再生能源带来的不确定性）的储能设备控制问题。与电力行业的大多数深度学习研究不同，我们使用负载分解技术将问题的结构信息编码到深度学习框架中，从而构建了用于存储控制的深度学习框架。 我们进一步分析了由可再生能源发电中的预测误差引起的近似性能损失上界。 最后，数值研究说明了我们提出的框架在实际应用中有稳定的表现，这也揭示了数据对于存储控制的价值。下面重点介绍我们的主要贡献：

§ 净负载分解：我们提出了基于可预测可再生发电量的净负载分解。 我们分析了可再生能源发电中预测误差导致的一次负荷分解中的近似性能损失。

§ 深度学习控制框架：通过一次性负载分解来利用结构，我们设计了一个简单的阈值控制策略，该策略仅需要对未来价格和可再生能源发电进行短期预测。 为了解决可再生能源发电和价格的高度不确定性，我们充分利用了大数据并诉诸于深度学习方法，得到了深度学习存储控制框架 （图 1）。这篇论文正投稿至 IEEE Transaction on Industrial Informatics。

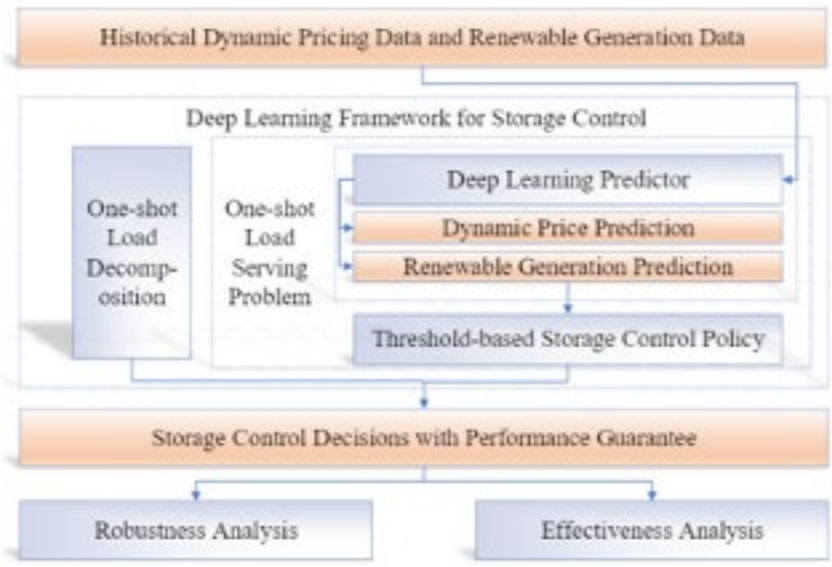


图 1 深度学习存储控制框架

电力存储作为公共资产对电力市场的影响机理研究

储能技术可以满足电力系统临界峰值需求，从而降低总发电成本，因此在稳定电价方面显示出巨大的潜力。电力存储的成本不断下降，使得在电力系统中大规模部署电力存储系统变得可行。通常，电力存储系统是私有的，于是如何统筹和管理私有的电力存储系统会给独立系统运行商（ISO）带来巨大的挑战。

基于以上原因，吴辰晔研究组探讨将电力存储系统作为公共资产的可能性，并阐述了储能系统作为公共资产给电力市场带来的机遇与挑战。电力存储系统作为公共资产，即该系统由 ISO 统一投资和管理，从而提升市场效率以及社会福利。在给定不同的存储投资量的情况下，他们采用参数最优化分析方法研究了电力系统的经济调度问题。研究表明，这种投资对用户的预期是有益的，然而不一定对每个人都有利。他们采用边际系统成本指数（MCI）的概念来衡量每个用户的福利，并显示其与传统的节点边际价格的关系。通过研究可以发现 MCI 具有有趣的收敛特性。

该研究成果最近被 ACM e-Energy 2020 接收，成为该会议近几年来唯一一篇作者全部来自大陆高校的全文。

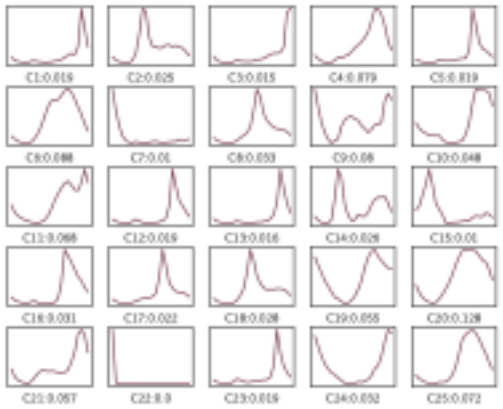


图 1 用户聚类

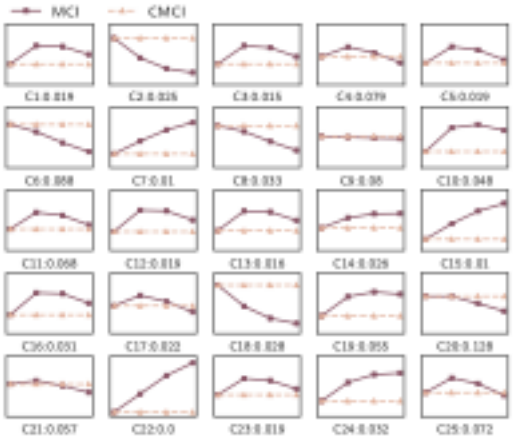


图 2 不同类别用户各阶段 MCI

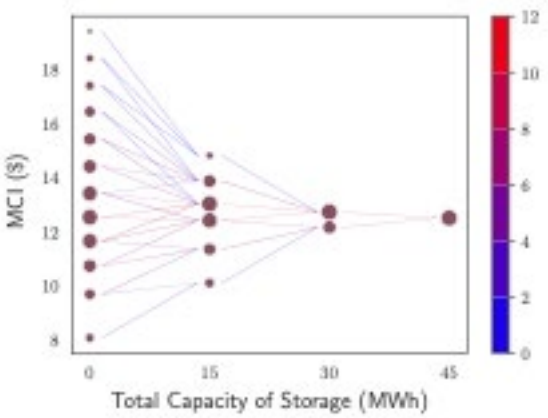


图 3 随存储容量上升的 MCI 聚类变化

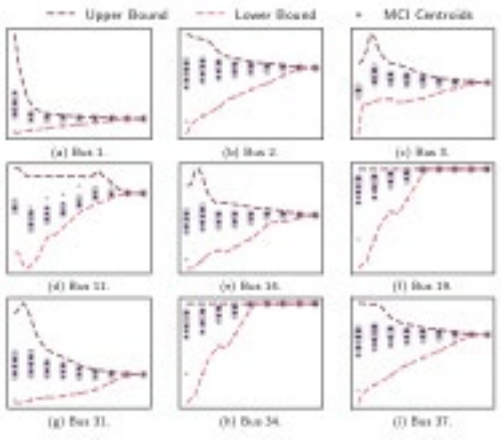
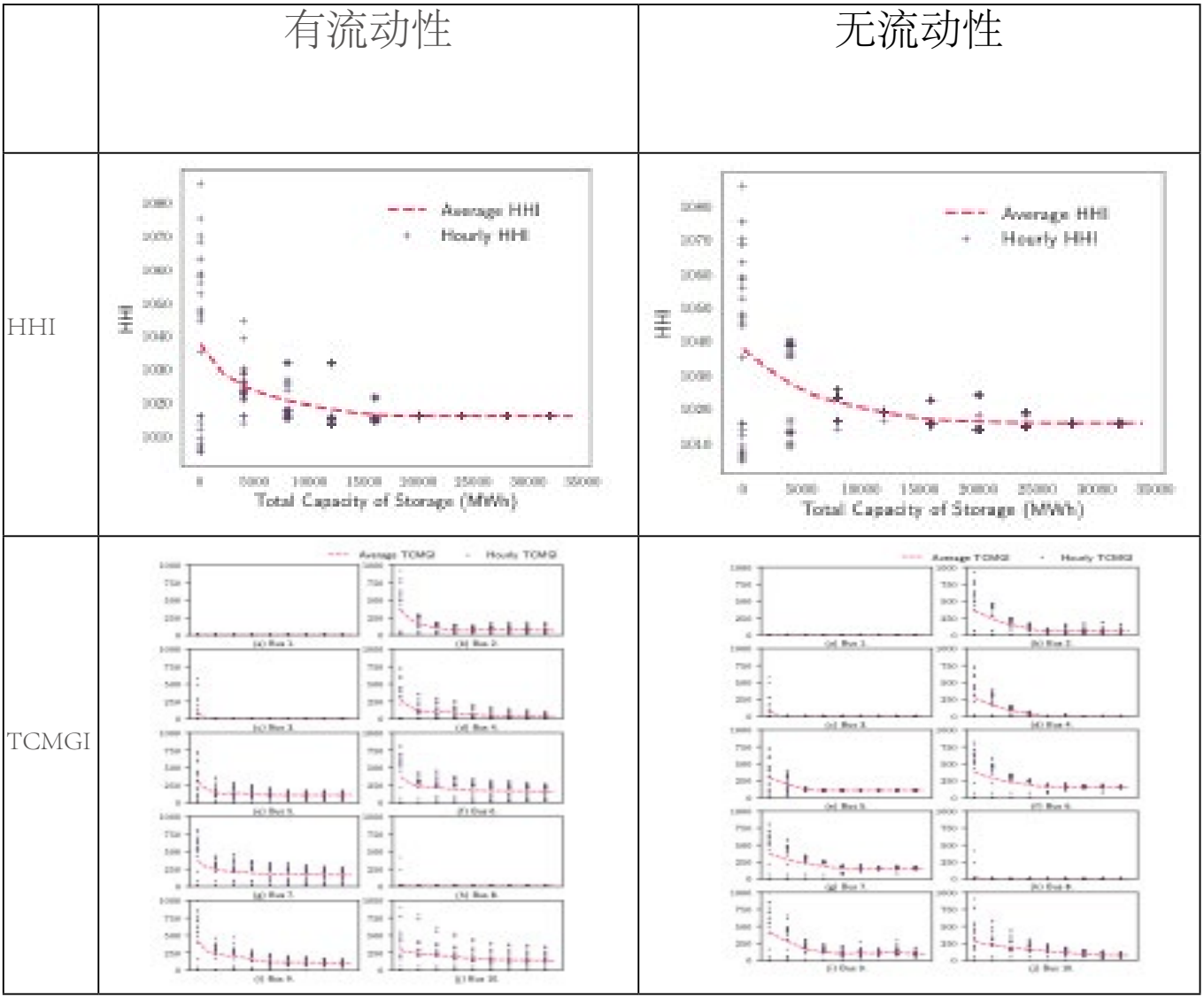


图 4 IEEE 39 节点系统各节点 MCI 及其上下界

电力市场中市场灵活性与市场力量：挑战与机遇

储能系统的部署可以为电网运行带来更多灵活性。随着近年来电力存储的成本不断下降，电力系统中储能的并网比重迅速提高。大规模存储设备的接入对电网中的实时负载有很大的影响，将不可避免地改变市场中原有电厂的市场份额。这种转变为电力系统创造了新的机遇，也带来了新的挑战。在新的市场条件下，需要重新评估各个电厂的潜在市场力量。

基于这个背景，吴辰晔研究组探讨将储能作为公共资产（由独立系统运营商（ISO）投资和管理）时系统弹性与市场力量之间的关系。为了量化这种关系，研究中使用两个指标进行了数值研究：赫斯曼 - 赫芬达尔指数（HHI）以及机组受传输容量限制的最小发电量指数（TCMGI）。此外，吴辰晔研究组分析了储能设备流动性对两个指标的影响。这项研究的结果可以帮助 ISO 评估将储能系统大规模接入后电力系统的潜在的风险和收益。该研究成果已经向 IEEE SmartGridComm 2020 投稿。



图一： 不同设备流动性情况下存储容量对 HHI、TCMGI 指标的影响

凸包定价模式下的电力市场潜在风险分析

良好的定价机制能正确反映商品的供求关系，对于市场的健康成长具有重要的意义。然而电力市场包括机组组合、实时市场、以及各类辅助服务市场等多个市场，这些市场的目的和起源均不同，这进一步加剧了电力市场的脆弱性和潜在被操纵的风险。为了解决上述困境，Gribik 等人在节点电价的基础上，提出了凸包定价模式。这种定价模式的优势在于综合考虑了机组组合和实时电力市场两个阶段，针对传统机组组合中的整数规划问题求解效率低等难点，提出了更有效率的计算出清价格的方法。值得注意的是，由于采用了凸包这一数学工具，其出清价格也具有较为清晰的经济学含义，而凸包定价模式中采用的上调费用也可以部分地解决对市场参与者激励不足的问题。

但这一模式依然存在尚未解决的理论和实际应用难点，主要集中在市场出清过程需要采集的数据更多，以及市场参与者获利模式更加多元等。这些都使得电力市场的潜在被操纵风险愈演愈烈。然而，国内外文献较少研究凸包定价模式下潜在市场风险以及市场参与者的潜在操纵策略。

吴辰晔研究组率先突破该领域的思维瓶颈，首先提出了一种新的市场出清价格刻画方式以揭示其经济含义，基于这一刻画方式，进一步分解市场参与者的获利结构，并刻画潜在的市场操纵行为。进而提出衡量市场力的指标，并证明在简化模型中，这一指标满足超模性，指出了对市场参与者合谋行为的预警。除此之外，还进行了大量数值模拟，强有力地指出了市场力风险在现实中的存在性、显著性。

该项成果共发表了两篇论文。其中一篇被 ACM e-Energy 2020 以海报张贴形式录用，另一篇被 IEEE Control System Letters 录用。

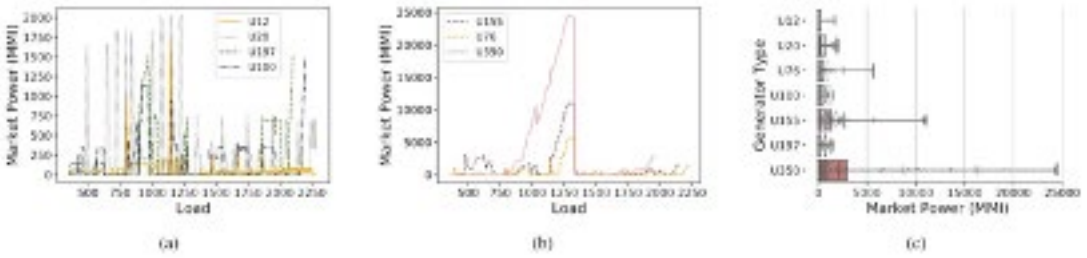


图 1：不考虑网络结构下，不同机组的市场力随着系统需求的变化

MARKET POWER ANALYSIS OF THE IIT 6-BUS SYSTEM

Scenario	Demand at Bus [3,4,5]	Congestion	Price under Truthful Bidding	Dishonest Generator	Price after Strategical Bidding	Uniform Price[1]
1	[54,108,108]	[line 3]	[13.95,42.00,46.16]	Gen 1	[4999,4999,4999]	17.70
				Gen 2	[13.95,4999,4999]	17.70
				Gen 6	[13.95,42.00,46.17]	42.00
2	[135,27,108]	[line 2]	[13.95,13.21,17.70]	Gen 1	[4999,42.00,4999]	17.70
				Gen 2	[13.95,13.21,17.70]	17.70
				Gen 6	[13.95,13.20,17.76]	42.00
3	[135,0,135]	[line 2]	[13.95,42.00,71.96]	Gen 1	[4999,42.00,4999]	17.70
				Gen 2	[13.95,4999,4999]	17.70
				Gen 6	[13.95,42.00,4999]	42.00

[1] Uniform price under enough transmission capabilities

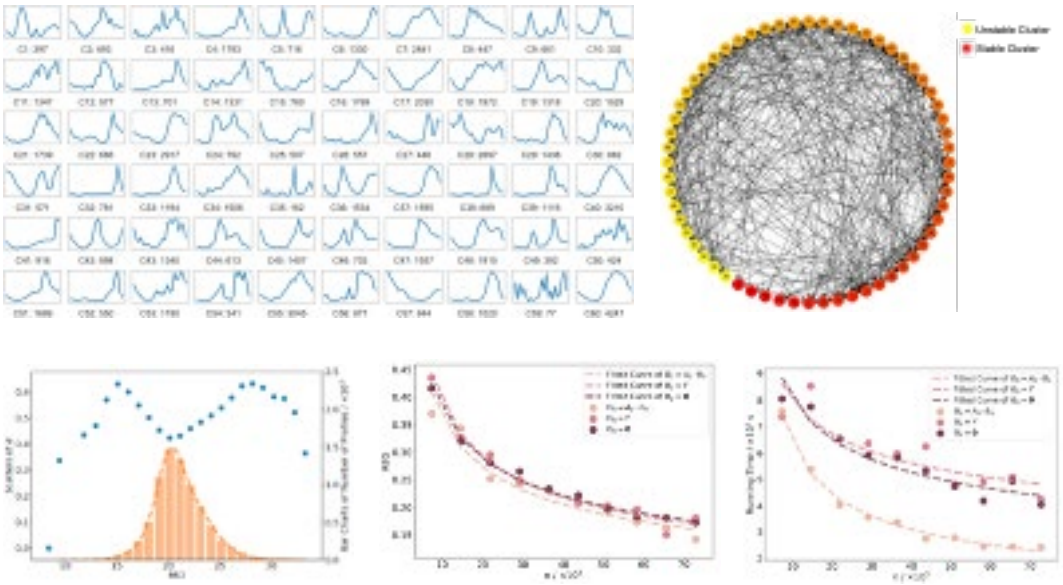
图 2：考虑网络结构下，不同节点处机组对于凸包价格的操纵能力

基于用户画像的电力定价

基于用户画像的定价模式，如果采用聚类的形式推广，则每一类用户将被收取相同的电价。然而，由于在同一类中的用户的实际日用电曲线并非完全一致，因此部分用户可能可以用很小的代价改变自己的日用电曲线形状，从而伪装成另一类用户，享受更低的价格。为了分析定价机制的脆弱性，能源与信息研究组提出了用户想要伪装成其他类型以获取更低价格的最小改变成本的优化问题，并且定义了衡量用户改变用电行为的潜在动机。结合数据分析，揭示了很多潜在的用户行为。该研究成果论文：Jingshi Cui, Haoxiang Wang, Chenye Wu, Yang Yu. "Vulnerability Analysis for Data Driven Pricing Schemes[C]"，IEEE PES General Meeting 2020.

尽管基于用户画像聚类的方式进行定价可能存在市场漏洞，但是如果选择的聚类方法得当，可以保证单一用户的获利空间非常有限，那么相关的定价机制依然不失为一种鲁棒定价机制。能源与信息研究组用聚类方法的 δ- 平滑刻画了鲁棒性，并建立了聚类方法和鲁棒性的关系。同时，为了解决 k-means 聚类方法 NP-hard 的问题，提出一种高效的一维聚类算法：贪心算法 GkC。该研究成果论文：Jingshi Cui, Haoxiang Wang, Chenye Wu, Yang Yu, “Robust Data-driven Profile-based Pricing Schemes”, IEEE SmartGridComm 2020.

大数据可实现需求侧管理以及实时价格预测，能源与信息研究组结合了这两个研究方向，并为电力市场用户设计了一个鲁棒的个性化长期定价方案。沿用 MCI 的概念将每个用户的需求侧信息和实时价格编码为单个每日指标，从而为长期电价设计生成用户 - 天矩阵。为了解决潜在的用户改变用电行为的问题，使用矩阵补全框架为鲁棒定价设计问题提出了一种新颖的解决方案。同时，结合问题的结构，提出了一种矩阵补全的初始化方法，从效率和鲁棒性两方面提高了经典矩阵补全算法的性能。理论分析和数值研究都证实了该定价方案的有效性。该研究成果论文：Jingshi Cui, Chenye Wu, Jian Li, “Robust Long-term Rate Design via Matrix Completion”, IEEE Control System Letters 2020.



七、理论计算机科学

主要完成人：段然研究组（段然、岑若虚、辜勇等）

接近最优的有向图往返距离支撑子图

在给定图 G=(V, E) 中，支撑子图（Spanner）是 G 的一个稀疏子图并且能够保持所有点之间的近似距离，也就是说，在支撑子图 S 中，只保留 G 的一部分边，使得对所有点对 u 和 v，u 和 v 之间的距离 $d_S(u,v)$ 是原图中距离 $d_G(u,v)$ 的近似。无向图中的 $O(n^{1+1/k})$ 大小的 (2k-1)- 近似支撑子图由 Althöfer et al. 在 1993 年给出（n 是点数，大小指支撑子图的边数）。这个大小和近似比的关系在 Erdős 猜想下已达到最优。而在有向图中，如果考虑每两点间的最短路，那么对于一个简单二分图就没有 $o(n^2)$ 大小的支撑子图（见图 1，删掉任意一条边都会影响连通性）。所以在有向图中我们考虑往返距离上的支撑子图，这里 u 和 v 之间的往返距离指 u 到 v 的距离加上 v 到 u 的距离，也就是经过 u 和 v 的最短有向环。之前有向图中往返距离支撑子图最好的结果包括 (2k+ε)- 近似的大小为 $O((k/\varepsilon) \cdot n^{1+1/k} \log(nW))$ 的支撑子图 [Zhu and Lam 2018]，和 (2k+ε)- 近似的大小为 $O((k/\varepsilon)^2 n^{1+1/k} (\log n)^{2-1/k})$ 的支撑子图 [Roditty, Thorup and Zwick 2008]。（这里边权为 [1,W] 之间的实数，所以第二个结果为强多项式大小的支撑子图。）

段然助理教授与计科 50 班学生岑若虚合作，给出了 (2k-1)- 近似的大小为 $O(kn^{1+1/k} \cdot \log (nW))$ 的有向图往返距离支撑子图的结果，并且将其改进为强多项式 $O(kn^{1+1/k} \cdot \log n)$ 大小的近似比为 (2k-1+o(1)) 的往返距离支撑子图。今年，与研究生辜勇合作，进一步改进为强多项式 $O(kn^{1+1/k} \cdot \log n)$ 大小的近似比为 (2k-1) 的往返距离支撑子图，接近 Erdős 猜想下的最优解。这个结果已发表在欧洲理论计算机会议 ICALP 20。

该成果研究论文：Ruoxu Cen, Ran Duan and Yong Gu, "Roundtrip Spanners with (2k − 1) Stretch", ICALP 2020.

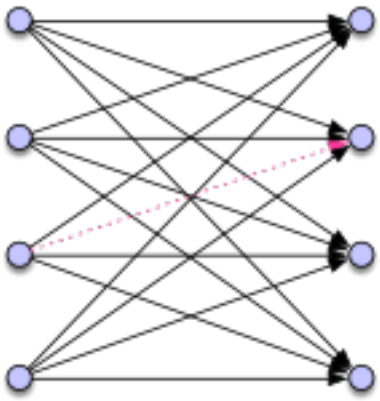


图 1

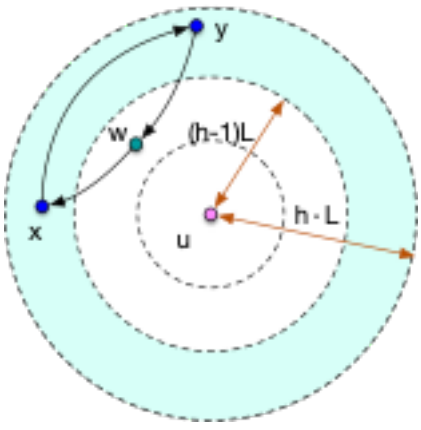


图 2

量子信息

一、量子相变

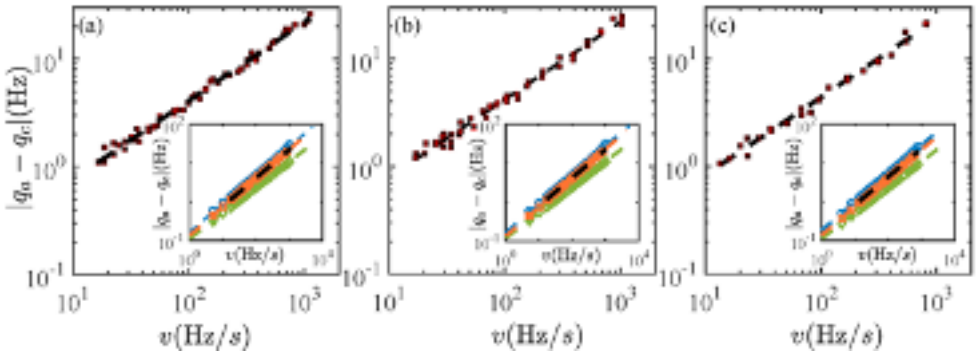
主要完成人：段路明、徐勇研究组（段路明、仇丽媛、田天等）

首次观测到在一阶量子相变上的推广 Kibble-Zurek 机制

量子相变中的非平衡动力学是一个比较复杂的问题。然而，对于二阶量子相变，Kibble-Zurek 机制提供了一个统一的理论来描述该过程动力学中的通用标度定律，在物理学与宇宙学中有广泛应用。具体来说，Kibble-Zurek 机制预测，通过调控系统参数将系统驱动跨过相变点的过程中，系统会经历三个阶段：绝热阶段，冷冻阶段，然后再次进入绝热阶段。根据 Kibble-Zurek 机制预测，在线性扫描过程中，系统解冻的动力学相变点与线性扫描速度具有幂律标度关系。

与二阶相变不同，一阶相变在相变点处多相共存。当系统偏离相变点时，也会有亚稳态的存在，这导致一阶相变的标度关系通常不能用传统的 Kibble-Zurek 机制描述。段路明教授研究组与徐勇助理教授合作理论上发现对于一阶相变，相关能隙由压稳态和其相应的第一激发态决定，而非二阶相变中的基态和相应的第一激发态决定。这个相关能隙的倒数决定了系统的弛豫时间，从而决定了系统解冻时的参数值。这一机制称为广义 Kibble-Zurek 机制。段路明教授研究组进一步实验观测钠原子凝聚体在极性相和反铁磁相的一阶相变中的幂律标度关系，发现该实验结果与广义 Kibble-Zurek 机制预测高度吻合（如图所示）。该结果为进一步研究一阶相变中广义 Kibble-Zurek 机制奠定了基础。

该成果研究论文：Liyuan Qiu, Haiyu Liang, Yanbing Yang, Haoxiang Yang, Tian Tian, Yong Xu, Luming Duan. “Observation of generalized Kibble-Zurek mechanism across a first-order quantum phase transition in a spinor condensate”. Science Advances 2020.

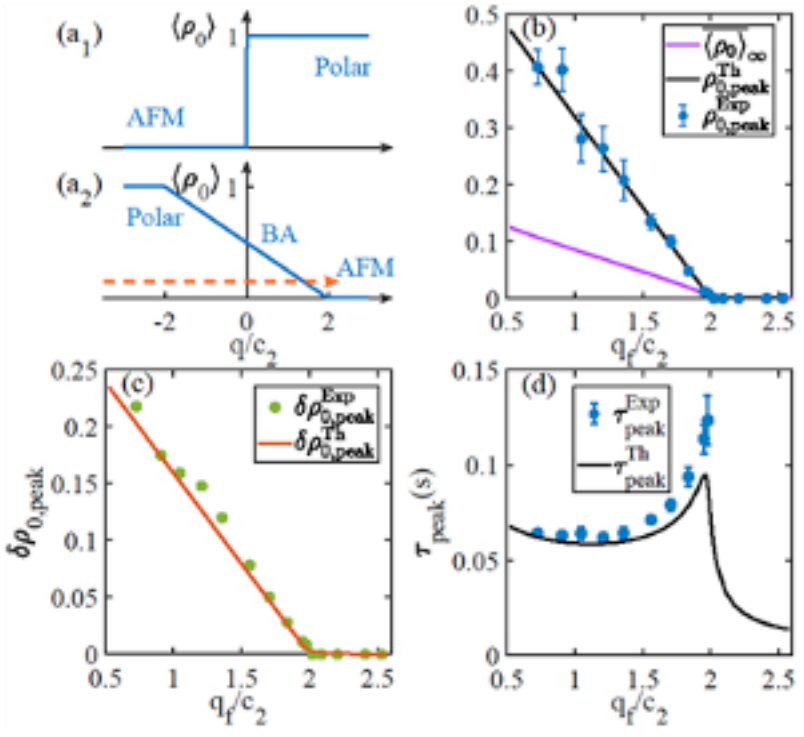


首次观测到与多体激发态相对应的动力学量子相变

多相变是广泛存在于宏观系统中的现象，例如，水在固液气三态之间随温度变化的转变。在接近绝对零度时，量子效应占据主导作用，此时的相变称为量子相变，例如，在自旋等于 1 的反铁磁旋量玻色爱因斯坦凝聚体中，随着二阶塞曼能量的改变，系统基态在极化态（polar phase）与反铁磁态（antiferromagnetic phase）之间转变。上述相变着眼于平衡态物理，为了探究非平衡态物理，人们将“相变”的概念推广至非平衡过程。研究发现，当系统受到扰动后，其动力学响应在相变点两边表现出截然不同的性质，这种现象被称为动力学量子相变。此前，理论与实验研究均表明动力学量子相变与基态量子相变并不总是存在一一对应的关系；也有理论研究表明动力学量子相变与激发态量子相变有一定的关系，但缺乏实验证据。

为这一领域提供新的重要实验证据，段路明教授研究组与徐勇助理教授合作，基于钠原子玻色爱因斯坦凝聚体系统，利用微波对系统施加瞬时扰动，首次在量子多体系统中观测到与激发态相变对应的动力学量子相变。该实验同时表明量子淬火的动力学方法可以用来测量激发态相图。

该成果研究论文：T. Tian, H.-X. Yang, L.-Y. Qiu, H.-Y. Liang, Y.-B. Yang, Y. Xu and L.-M. Duan. ”Observation of Dynamical Quantum Phase Transitions with Correspondence in an Excited State Phase Diagram.” Phys. Rev. Lett. 2020.



二、量子通信

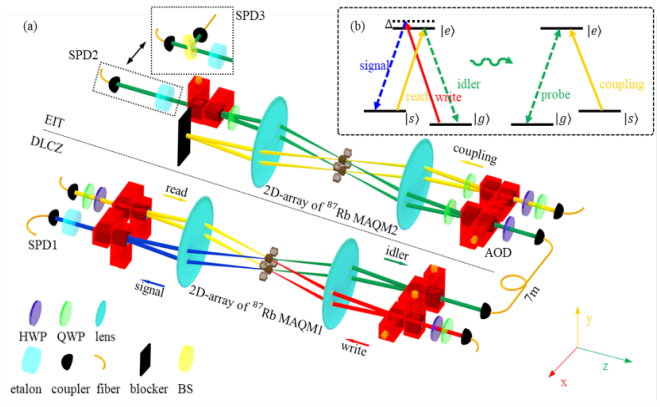
主要完成人：段路明研究组（段路明、李畅等）

实现多路复用原子存储器间的量子通信

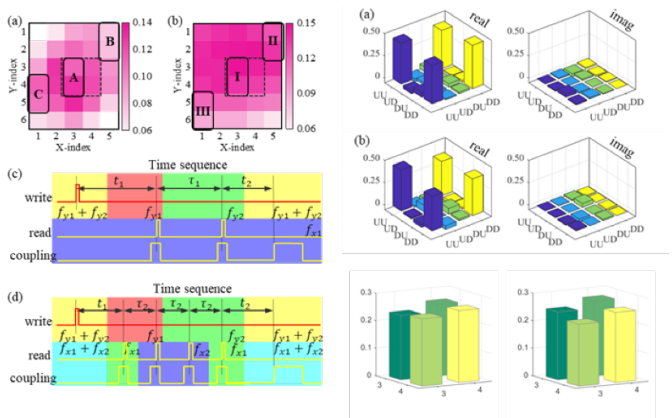
为了克服单光子信号在量子信道传输时面临的指数衰减问题，长程量子通信需要利用量子中继器方案。DLCZ（Duan-Lukin-Cirac-Zoller）协议作为量子中继器方案影响最大的物理实现方式，通过在长程信道中插入量子存储器节点，利用量子存储器产生和传输纠缠态，实现相邻量子存储器间的纠缠，进而通过多步纠缠交换操作最终完成长程纠缠信道的建立，克服单光子信号在光纤中的指数衰减问题。多路量子存储器的使用可以进一步提升量子中继器方案的性能。在一个物理装置中，多路复用量子存储器具有许多独立的量子存储单元，每个单元均可以产生和存储量子态，并维持之间的相干性，进而减少纠缠分发和纠缠交换所需要的时间。此前该研究组分别利用 DLCZ 协议和电磁诱导透明（EIT）效应，在冷原子系综中实现了多路复用的原子量子存储器。然而如何相干地将多比特或多维量子态从多路复用的原子存储器耦合到单光子光纤，是一个急需解决的问题。

这项工作设计了独特的操作，使得在不同实验平台的多路复用原子存储器之间可以完成量子态传输。实验利用声光偏转器实现动态寻址，使得在一个多路复用原子存储器中通过 DLCZ 协议产生的、利用不同存储单元编码的自旋波（spin-wave）量子比特，转换为时间段（time-bin）量子比特，进而通过 EIT 效应存储到另一个多路复用原子存储器中。实验测量了不同原子存储单元中产生、传输和储存的纠缠态，其在操作前后均能保持较高的保真度，证明了多路复用原子存储器可以完成量子中继器方案所要求的量子连接。此外高维量子态作为提升量子信道容量的载体，也被验证可以完成高保真传输。这项工作验证了利用多路复用原子存储器实现量子中继器方案的可行性，审稿人认为这对量子网络的研究有重要的推动。

该成果研究论文：C. Li, N. Jiang, Y.-K. Wu, W. Chang, Y.-F. Pu, S. Zhang, L.-M. Duan. "Quantum Communication between Multiplexed Atomic Quantum Memories", Phys. Rev. Lett. 2020.



多路复用原子存储器间的量子通信实验装置示意图



多路复用原子存储器的单独寻址操作演示和量子态传输的实验验证

三、超导量子计算

主要完成人：孙麓岩研究组（孙麓岩、马雨玮、徐源等）

实现逻辑比特上错误透明的相位门操作

众所周知，量子计算在某些问题的处理能力上比经典计算有指数级别的提升，在近二十年来成为一个热门的研究方向。然而，在实际的量子系统中，与环境耦合而产生的噪声与退相干使得量子门的保真度远未达到可以处理实际问题的程度。为了克服这个困难，可容错量子计算不仅要求对存储量子信息的逻辑比特进行量子纠错保护，而且还需要对逻辑比特操控的动力学过程进行保护，从而得到可靠的量子逻辑门。近些年来，量子纠错已经在实验上得到了演示，然而在受量子纠错保护的逻辑比特上进行可容错的量子门操作依然是个难题。

在通常由多个物理比特编码一个逻辑比特的框架下，容错的逻辑门操作主要由横向门与魔术态蒸馏组成，它的实现需要大量资源，非常具有挑战性。另一种实现容错量子门的方法被称作错误透明的量子门。该理论也首先在多物理比特编码的框架下被提出，其实现方式需要多比特的同时耦合，因此实验上也非常难以实现。2019 年，孙麓岩研究组首先在实验中采用玻色量子编码，实现了基于微波光子的二项式量子纠错码，从而可以缓解光子损耗对光子携带的量子信息的影响，并首次实现逻辑量子比特的量子纠错和通用量子门操控（Nature Physics 15, 503 – 508 (2019)）。现在，他们进一步考虑对纠错码的量子门操作中的错误，将错误透明的概念拓展到玻色编码的逻辑比特上，演示了基于玻色编码的逻辑量子比特上的错误透明相位门操作。

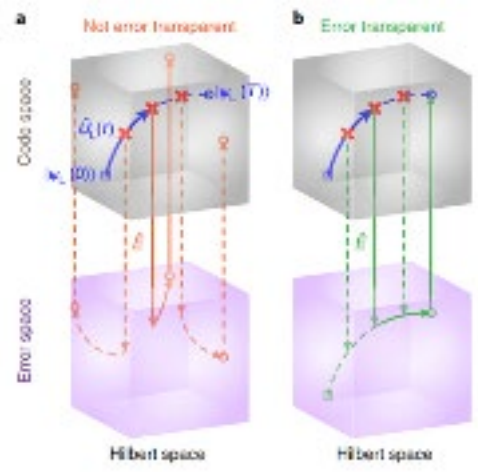


图 1 错误透明的量子操作的示意图

实验样品由一个超导量子比特，一个快速读取腔和一个高寿命存储腔构成，而逻辑比特是对存储腔中的光子态进行二项式编码构成。错误透明的门操作要求逻辑比特在编码空间和错误空间的演化完全一致。为此，研究组在实验中发展了一种新的量子比特驱动技术，称之为“PASS”（Photon-number-resolved AC-Stark Shift）。由于超导量子比特与存储腔有着极强的色散耦合，超导比特的本征频率会随着存储腔内的光子数的变化而变化。因此，在接近超导比特本征频率的频域范围内施加非共振驱动，就能诱导出存储腔内各个光子数态可控的频率偏移。通过设计这种频率偏移，逻辑比特在编码空间和错误空间可以进行完全相同的相位门演化，从而可以实现错误透明的相位门。实验显示，在发生错误的情况下，错误透明的相位门的表现确实比普通的相位门有显著的提升；而且在连续纠错的情况下，逻辑比特在错误透明的相位门操作下比普通相位门有更加优异的相干寿命，展示了该相位门的容错性。

该实验实现的错误透明的相位门是近几年来在量子纠错方面的一个重要进展。其实现错误透明相位门的技术可以很容易扩展到 Hadamard 门以及两逻辑比特门，从而能实现错误透明的通用量子门，为将来基于玻色子编码的容错量子计算提供了一种新思路。

该成果研究论文：Y. Ma, Y. Xu, X. Mu, W. Cai, L. Hu, W. Wang, X. Pan, H. Wang, Y. P. Song, C.-L. Zou & L. Sun .“Error-transparent operations on a logical qubit protected by quantum error correction”, Nature Physics 2020.

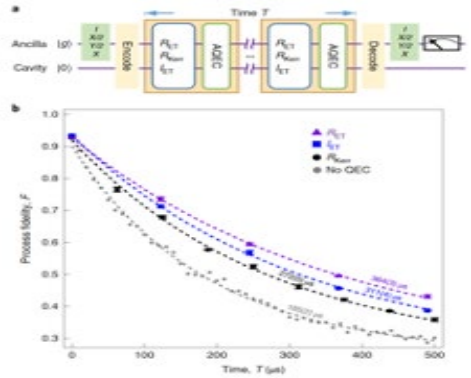


图 2：错误透明的相位门操作过程中随机发生的错误可以在其完成之后通过量子纠错来纠正，其相干性能的表现比普通相位门有明显的提升，展示了很好的容错性。

量子逻辑门组合并验证其抗噪特性

量子计算是基于量子力学规律调控量子信息单元进行计算的一种新型计算模型，在某些问题的处理能力上比经典计算有指数级别的提升，是当前世界科技前沿的热点之一。实现高保真度、强鲁棒性的量子逻辑门是实现大规模量子计算的关键。几何量子计算利用几何相位的整体性质避免某些局域噪声对量子操作的影响，从而实现高保真度的量子逻辑门。因此，基于几何相位的量子操控是量子信息处理领域中非常重要的研究课题。近年来，几何相位已经在实验上得到了演示，然而普适几何量子计算依然是个难题。

2018 年，薛正远研究组提出在二维电容耦合超导比特链上实现完备非绝热几何量子计算的理论方案 [Phys. Rev. Appl. 10, 054051 (2018)]。数值模拟结果显示，方案在现有的实验参数下，可以达到非常高的保真度。同时，解析证明和数值验证了几何量子操控对比特频率漂移误差比动力学操控的鲁棒性更好。

根据他们进一步简化的方案，孙麓岩研究组在一维超导量子芯片上首次实验实现了完备非绝热几何量子计算，取得了高保真度的几何量子门，如图 1 所示。同时，该实验也首次实验验证了几何量子门对控制误差以及频率漂移噪声这两种主要量子门误差来源的鲁棒性都优于动力学门。如图 2 所示，实验结果表明在某种量子噪声条件下，对于任意的量子操作，总可以找到合适的演化路径使构造的几何量子门对该噪声的鲁棒性能够好于动力学量子门。

该实验实现是几何量子计算领域的一个重要进展，证明了几何量子门性能的优势，为大规模量子计算的实现提供了更好的备选方案。

该成果研究论文：Y. Xu, Z. Hua, Tao Chen, X. Pan, X. Li, J. Han, W. Cai, Y. Ma, H. Wang, Y. P. Song, Zheng-Yuan Xue, and L. Sun.“Experimental Implementation of Universal Nonadiabatic Geometric Quantum Gates in a Superconducting Circuit”, Phys. Rev. Lett. 2020.

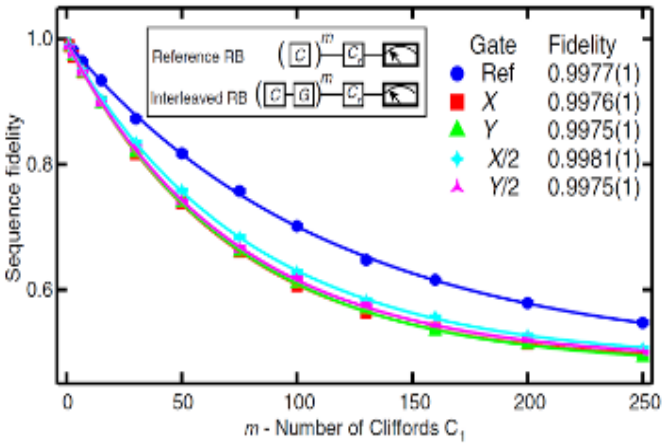


图 1：各种量子门操作的插入式随机基准测试结果。

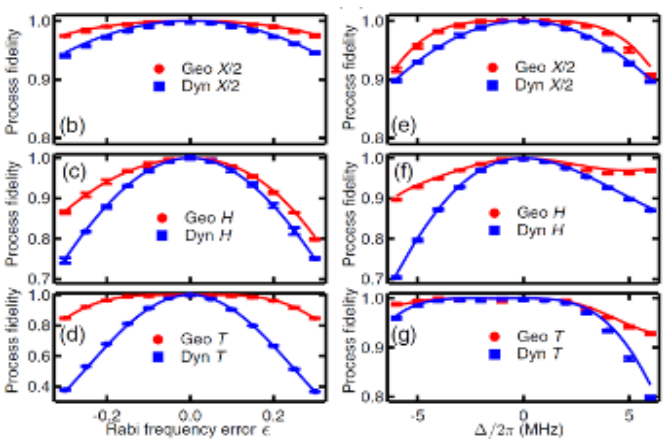


图 2：几何量子门鲁棒性的实验验证。

实现在两个可纠错的光子比特上的控制相位门

量子计算在原理层面上利用由量子态的叠加和纠缠带来的并行计算能力，在某些问题的处理能力上比经典计算有极大的提升。另一方面，相较于经典比特，量子比特对于环境噪声十分敏感，容易退相干和出错。为了克服这个困难，需要对量子比特进行纠错码的编码，形成逻辑比特，并实现可容错的量子计算。因此，在实验上对可纠错的逻辑比特进行量子门操作是实现量子计算的重要一步。

与传统的由多个物理比特编码一个逻辑比特的方式相比，近年来利用光场的谐振模式进行纠错编码的方式因为其更节省硬件资源而发展迅速，基于不同编码的光子逻辑比特的量子纠错以及单逻辑比特的普适量子门都相继实现。为了实现普适量子计算，还需要在两个光子逻辑比特之间实现控制相位门的操作，而这部分的研究目前还很少。本实验就是利用了几何相位门的方法，分别实现了基于猫态编码的光子逻辑比特上的单、双比特相位门，以及在可纠错的、二项式编码的光子逻辑比特上的两比特控制相位门。

实验样品 [图 2（a）] 由三个超导量子比特及其分别对应的三个快速读取腔，和两个高寿命存储腔构成，而光子比特是对存储腔中的光子态进行纠错编码构成。其中一个超导比特同时耦合两个存储腔，用以进行光子比特之间的两比特门操作，而另外两个超导比特分别只和一个存储腔耦合，用以初始化和测量对应的光子比特。本实验利用几何相位的方式进行单、双比特的相位门操作，相较于其它方式有更强的抗噪能力，这也已经被该实验组先前的实验所证明 [Phys. Rev. Lett. 124, 230503 (2020)]。几何相位门主要通过操纵与之耦合的超导比特围绕出一个闭合路径，从而诱导出光场比特的相位，如图 1 所示。由于超导比特和存储腔间的强色散耦合，不同的光子数态对应了不同的超导比特频率，因此在对应频率下绕出的闭合路径可以在对应的光子数态上产生一个相位。闭合路径所围的面积决定了诱导出的相位大小，从而实现光子比特的任意相位门操作。

这种方法很容易推广到两比特相位门。对于中间耦合两个存储腔的超导比特而言，它和两个腔都有上述的强色散耦合，且耦合强度不同，因此除了少数简并情况外，可以通过该超导比特频率来区分两个存储腔中各自的光子数。利用这个性质，就可以实现两光子比特的几何相位门。图 2 展示了基于猫态编码的两比特控制相位门，实验给出的保真度为 90.5%。另外，对二项式编码的光子比特也进行的两比特控制相位门，实验给出的保真度为 89.4%。

该成果研究论文：Y. Xu, Y. Ma, W. Cai, X. Mu, W. Dai, W. Wang, L. Hu, X. Li, J. Han, H. Wang, Y.P. Song, Zhen-Biao Yang, Shi-Biao Zheng, and L. Sun.“Demonstration of Controlled-Phase Gates between Two Error-Correctable Photonic Qubits”, Phys. Rev. Lett. 2020.

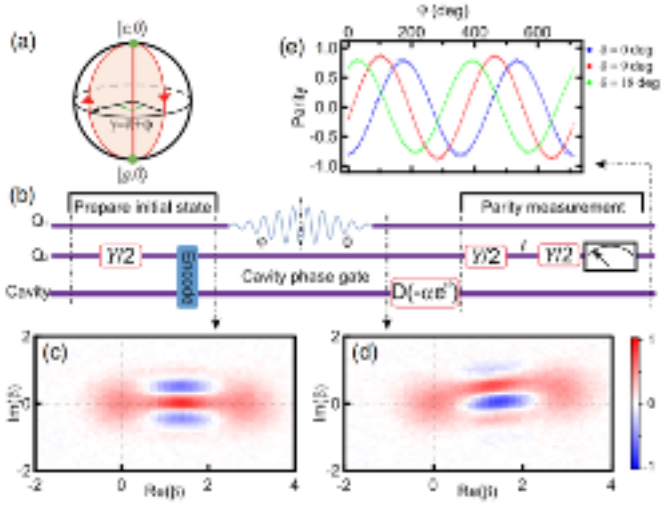


图 1：用几何相位的方式在基于猫态编码的光子逻辑比特上进行单比特相位门操作。

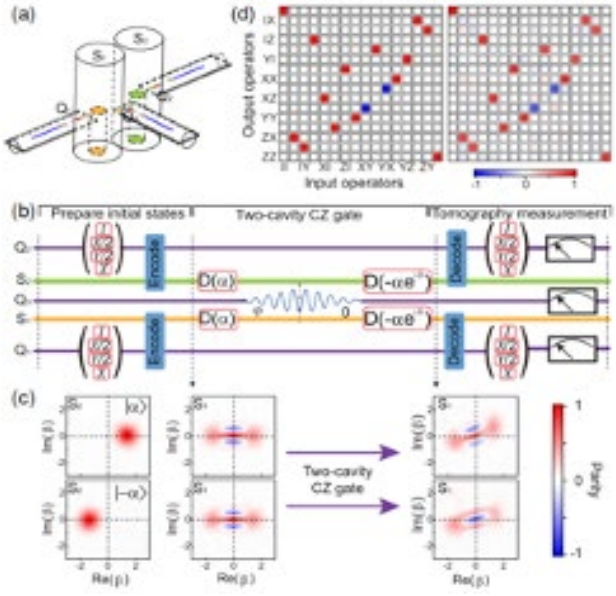


图 2：实验样品示意图以及在猫态编码上实现两比特控制相位门的示意图。

四、离子阱量子计算

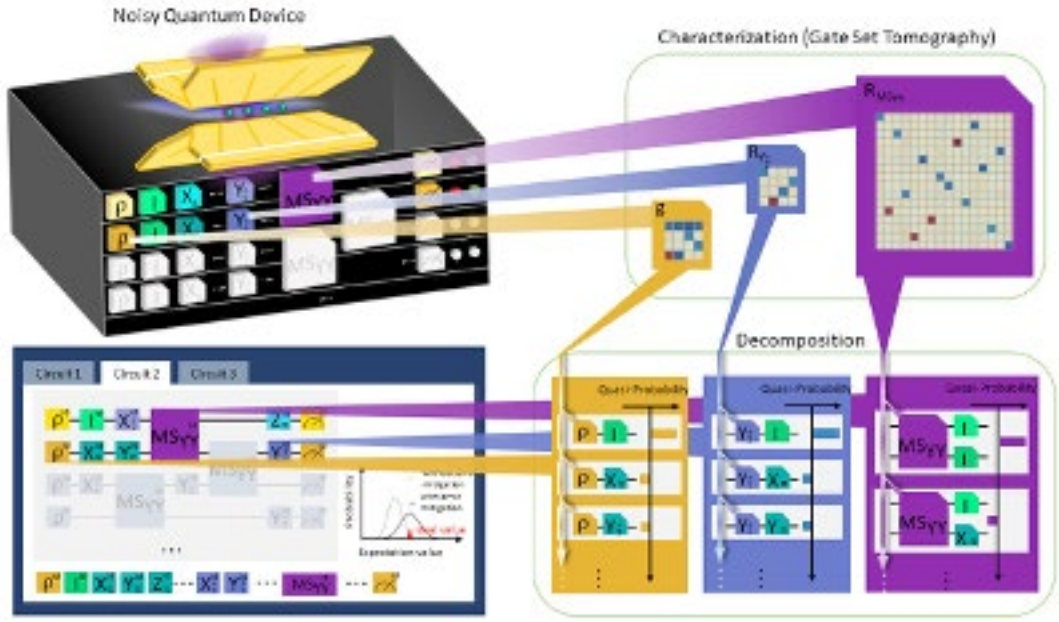
主要完成人：金奇奂、马雄峰研究组（金奇奂、张帅宁、路尧、严马可、赵琦等）

利用量子误差缓解方案实现优于物理门保真度的量子计算

量子逻辑门的保真度是实现容错量子计算的关键因素。多种量子应用都可以通过单比特和两比特量子门组成的量子电路实现，并简化为测量结果的期望值，其不可避免由于环境和操作误差而偏离理想值。近年来，量子计算理论工作者发现，不同于在物理层面提高量子门的保真度，可以通过编程量子电路来获得更准确的期望值估计，进而等效地提高量子门的保真度。

作为这一领域的一项突破性进展，金奇奂研究组首次在囚禁离子系统中实现了编程量子电路的量子误差缓解方案，并成功地将单比特和两比特门的有效门保真度比物理门的保真度分别提高了两个和一个数量级。这种方案不同于量子纠错，不需要复杂的编码方案，极低的量子门误差率和额外的量子比特资源，在估计期望值的量子任务中就能够越过物理门保真度的 break-even point。该方案可用于近期中等规模的量子计算技术，并打开了将来在不完美的量子设备上实现高保真度量子计算的可能性。

该成果研究论文：Shuaining Zhang, Yao Lu, Kuan Zhang, Wentao Chen, Ying Li, Jing-Ning Zhang, Kihwan Kim. "Error-mitigated quantum gates exceeding physical fidelities in a trapped-ion system", Nature Commun. 2020.

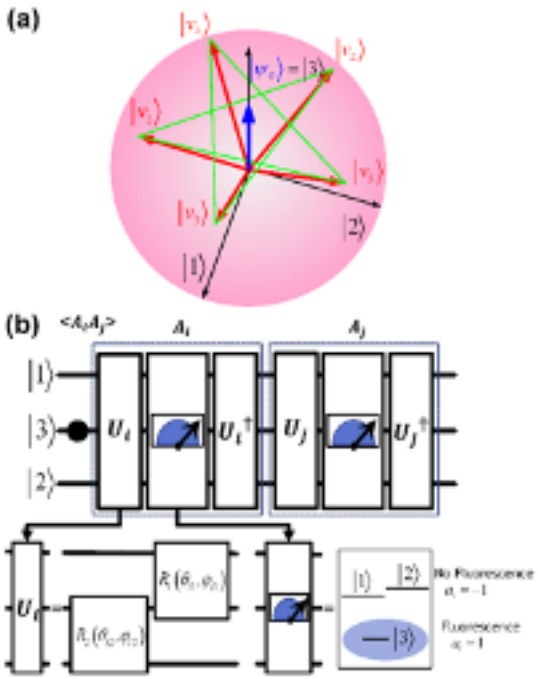


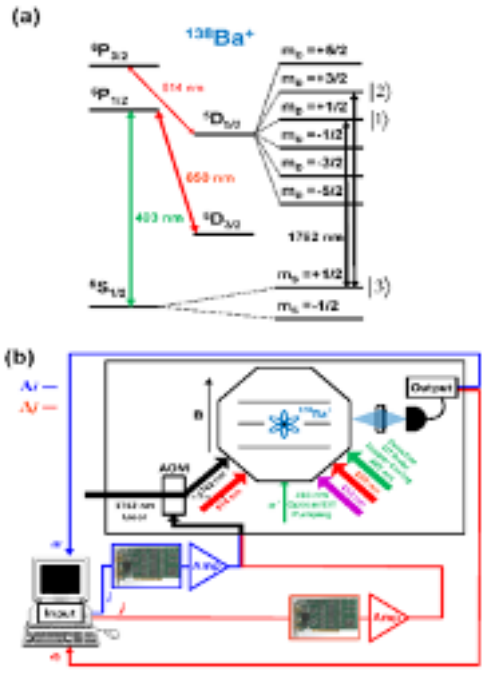
量子互文性保证的量子随机数扩展器

随机数生成器输出的随机性可以通过观察到破坏以Kochen-Specker定理为基础的量子互文不等式得到验证。在一个单量子系统中就能够验证量子互文性，相比基于非局域性测试的随机数生成器，实验要求大大简化。然而，如何保证量子互文性测试中所要求的同步测量的相容性问题仍未被攻克。

金奇奂和马雄峰研究组对著名的Klyachko-Can-Binicioglu-Shumovsky不等式进行了经过严格证明的修补，由此可以进一步简化测量中的相容性要求。他们在一个囚禁的138Ba+离子系统中进行实验，研制出了借由破坏量子互文性不等式保证的量子随机数扩展器，并且关闭了探测漏洞。他们进行了1.29×108次实验，从中提取出真正随机数5.28×105比特，生成速率达到了270比特/秒。这项研究为未来实用的高速抽查量子随机数生成器等更多安全快速的信息处理应用设备打下了坚实的基础。

该成果研究论文：Mark Um, Qi Zhao, Junhua Zhang, Pengfei Wang, Ye Wang, Mu Qiao, Hongyi Zhou, Xiongfeng Ma, and Kihwan Kim, "Randomness Expansion Secured by Quantum Contextuality", Phys. Rev. Applied 2020.



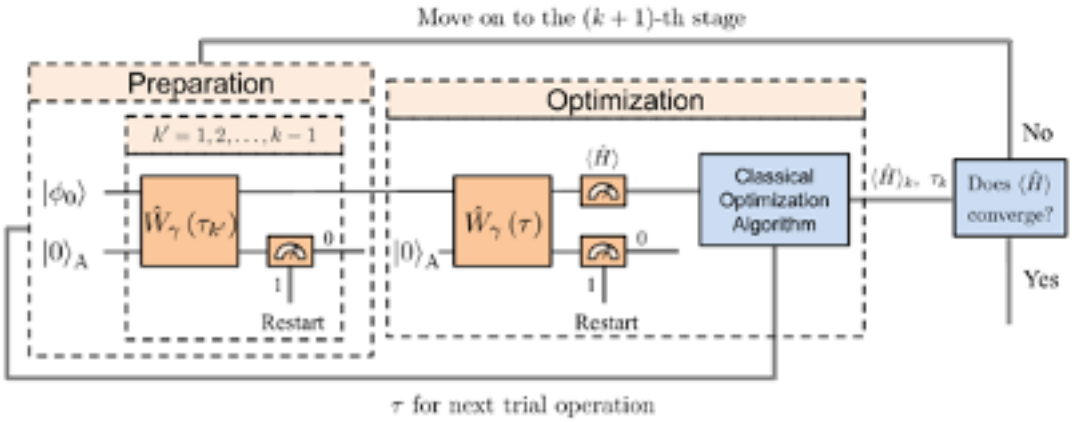


基于囚禁离子的概率本征求解器

由于希尔伯特空间的维度随体系中的粒子数目指数增长，人们公认复杂量子多体系统的演化是经典计算机难以胜任的一项计算任务。为解决这一问题，著名物理学家费恩曼提出利用可控的量子系统来模拟目标量子系统的演化，即量子模拟。于量子模拟相比，基于量子线路的量子计算是更加普适的一种量子技术，不仅可以模拟量子动力学，还可以用来求解线性方程组和复杂哈密顿量的本征值问题。其中，物理系统的能谱信息在许多研究领域，如量子化学和凝聚态物理等，都具有重要意义。

在这项工作中，助理研究员张静宁博士和金奇奂副教授领导的离子阱量子信息小组，与西班牙巴斯克地区大学物理化学系的 Enrique Solano 教授领导的 Qutis 理论研究小组合作，共同提出了基于囚禁离子系统的概率本征求解器的实现方案。提出一种经典——量子混合的算法，通过投影测量和后选择将系统的熵泵浦到环境中，等效地降低系统的平均能量，最终实现基态制备并通过测量得到基态能量。该算法要求初态和目标哈密顿量的基态具有非零的重叠积分，其数值与基态制备过程的整体成功率正相关。熵泵浦是通过单个辅助量子比特实现的。

该成果研究论文：Jing-Ning Zhang, Iñigo Arrazola, Jorge Casanova, Lucas Lamata, Kihwan Kim, and Enrique Solano,” Probabilistic eigensolver with a trapped-ion quantum processor”， Phys. Rev. 2020.



五、量子密码学

主要完成人：马雄峰研究组（马雄峰、曾培等）

基于编码对称性的测量设备无关量子密钥分发安全性分析

量子密钥分发实用化的关键问题在于提高性能和实现安全性。量子密钥分发的实际性能由密钥成码率来刻画，一般被量子信道传输损耗和噪声两方面的因素影响。量子信道的传输损耗通常用光子传输率 η 来刻画，即一个光子能够经发送端（Alice）顺利通过量子信道达到接收端（Bob）并且被探测到的概率。在离散变量的量子密钥分发协议中，一般采用单光子进行密钥信息编码，因而单光子在信道中的损耗意味着密钥信息的丢失。因此，通过率 η 是密钥产生速率的自然上界。可以严格证明，在所有的 Alice 向 Bob 发送信号的协议中，其密钥产生速率 R 存在一个上界，为量子信道通过率 η 的线性函数，即 $R \leqslant O(\eta)$。在光纤量子密钥分发中，由于量子信道通过率随着传输距离的增加而指数衰减，该上界严重限制了量子密钥分发协议在远距离条件下的密钥生成速率。

有趣的是，最近的一系列研究表明，通过改进以前的测量设备无关协议，新的相位匹配量子密钥分发协议可以突破上述的线性成码上界。在数值模拟实验中，相位匹配量子密钥分发协议的成码率在传输距离大于 250 公里的时候可以显著超越线性密钥率上界。在传输距离大于 300 公里的时候，该协议的密钥率能够比原始的测量设备无关量子密钥分发协议高出 4~6 个数量级。这种新型的量子密钥分发协议显著提升了密钥分发的效率，对于推进协议实用化有重大意义。然而，由于实验过程中激光相位涨落和漂移产生的噪声，这种新型密钥分发协议在实际实验中有很高的误码率。在原来的分析中，噪声将会严重影响协议的性能。

为了解决该问题，曾培，吴蔚捷和马雄峰从编码对称性的角度出发来考虑一般的测量设备无关协议的安全性，从而改进并推广了之前相位匹配量子密钥分发的安全性分析方法。在新型的安全性分析中，相位匹配协议的性能对于噪声有很高的容忍度。在光强较低，暗计数很低的极限情况下，即使噪声引起的误码率接近 50%，相位匹配协议依然可以成码。在数值实验里，使用典型的实验参数和 13% 的高误码率的情况下，相位匹配协议依然可以突破线性成码上界。同时，工作中还对相位匹配协议进行了有限数据下的安全性分析，可以用 $10^{\wedge 12}$ 的合理数据大小实现突破线性成码上界的协议性能。

该研究成果论文：Pei Zeng, Weijie Wu, and Xiongfeng Ma. “Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound Over a Noisy Channel”, Phys. Rev. Applied 2020.

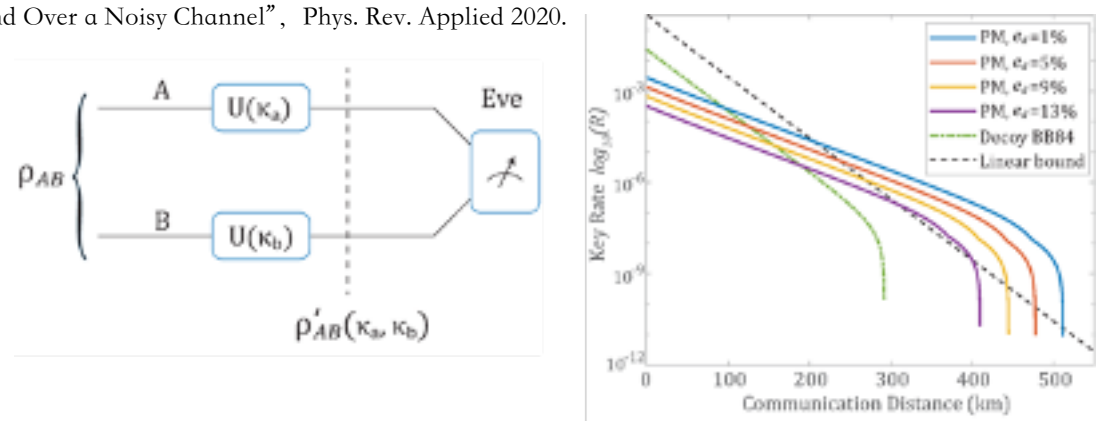


图 1 左图为测量设备无关协议的示意图，右图为对称分析下相位匹配协议在不同误码率下的表现。

首次实现超过 500 公里无中继的光纤量子密钥分发实验

马雄峰研究组基于该小组的相位匹配量子密钥分发的上述理论工作，和中国科学技术大学的实验团队进行合作，引入了激光注入锁定和相位后补偿方法，在超过 500 公里的光纤通信情况下上述研究成果成功创造了地基量子密钥分发最远距离新的世界纪录，在 300-400 公里的光纤成码率打破了传统无中继量子密钥分发所限定的成码率极限，即超过了理想的探测装置（探测器效率为 100%）下的无中继量子密钥分发成码极限（图 2）。如果将系统重复频率升级至京沪干线等远距离量子通信网络中采用的 1GHz，在 300 公里处，成码率可达 5kbps，这将大量减少骨干光纤量子通信网络中的可信中继数量，大幅提升光纤量子保密通信网络的安全性。

另外，马雄峰参与合作完成了量子密钥分发方向的综述文章。

该成果研究论文：Xiao-Tian Fang, Pei Zeng, Hui Liu, Mi Zou, Weijie Wu, Yan-Lin Tang, Ying-Jie Sheng, Yao Xiang, Weijun Zhang, Hao Li, Zhen Wang, Lixing You, Ming-Jun Li, Hao Chen, Yu-Ao Chen, Qiang Zhang, Cheng-Zhi Peng, Xiongfeng Ma, Teng-Yun Chen & Jian-Wei Pan. “Implementation of quantum key distribution surpassing the linear rate-transmittance bound”, Nature Photonics 2020；Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. "Secure quantum key distribution with realistic devices", Rev. Mod. Phys. 2020.

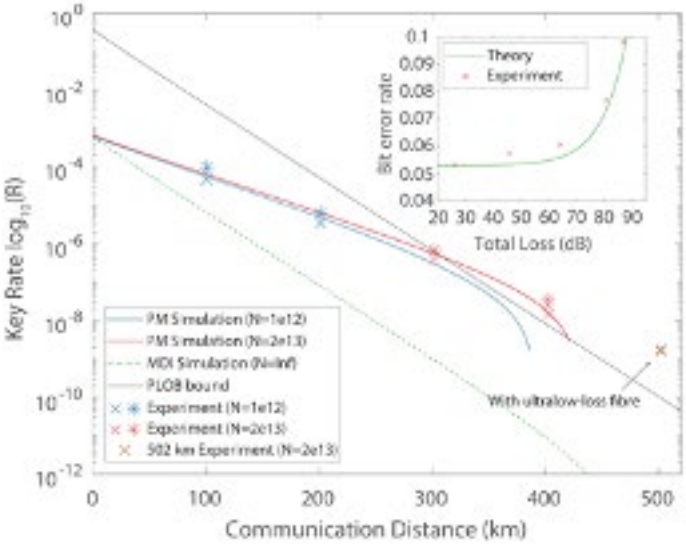


图 2 相位匹配量子密钥分发协议 (PM-QKD) 密钥率与传输距离关系的实验结果。星号的数据点为实验结果，红色和蓝色的实线为相应的数值模拟结果。通过 502 公里的超损光纤，实验实现了超远距离密钥分发。黑色实线为以前的线性成码上界。

六、量子人工智能

主要完成人：邓东灵研究组（邓东灵、张远航等）

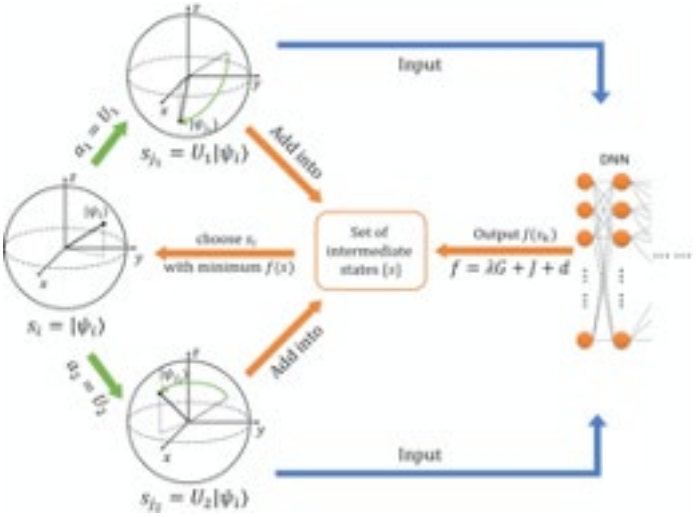
应用强化学习算法实现拓扑量子编译

量子编译是指把量子算法分解为一系列可以在硬件上实现的基本门操作的过程，它是实现量子计算的基石。传统方法在解决这一问题时面临一些困难：如 Solovay-Kitaev 算法不能输出长度最优的序列以实现某个特定的量子门操作，而暴力穷举算法虽可实现长度最优，但其耗时随序列长度指数增加。

最近，在机器学习领域有一个重要进展是通过强化学习算法可以有效解决魔方还原问题。本文通过研究发现，魔方还原问题与量子编译问题有很强的相似性，因此邓东灵研究组也可以用强化学习的方法来解决编译问题。在本文中，该研究组提出了一个解决量子编译问题的普适强化学习算法。为展示此算法相对传统算法的优势，该研究组研究了拓扑量子计算中对 Fibonacci 任意子的编译问题。

本研究在强化机器学习与量子计算之间架设了新的桥梁，将对今后此方向的理论和实验研究都产生影响。

该成果研究论文：Yuan Hang Zhang, Pei Lin Zheng, Yi Zhang, and Dong-Ling Deng. "Topological Quantum Compiling with Reinforcement Learning", arXiv: 2004.04743v1.



七、拓扑凝聚态物理

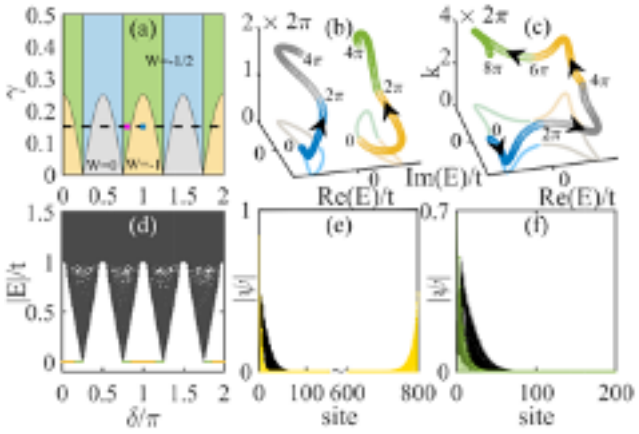
主要完成人：徐勇研究组（徐勇、曾琦波、杨炎彬等）

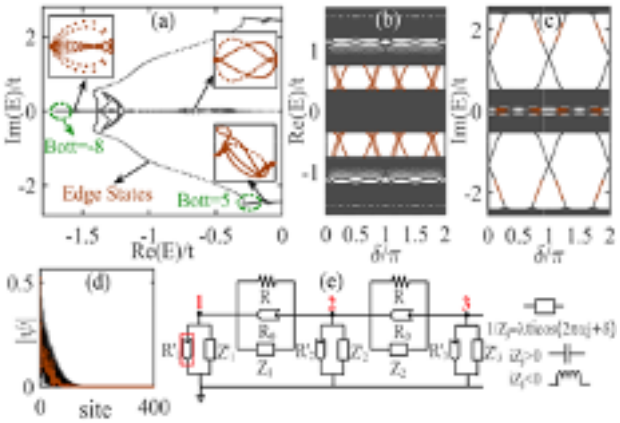
非厄米 Aubry-André-Harper 模型中中的拓扑态

非厄米拓扑系统近年来受到了研究人员的广泛关注。不同于厄米系统，非厄米系统通常用来描述与环境之间有能量或者物质交换的开放系统。通过在厄米系统中引入物理增益和损耗，我们可以研究系统性质在受到环境影响时会发生哪些变化。对拓扑系统的研究表明，非厄米因素的引入能够导致很多在厄米系统中不存在的新奇现象和拓扑态，比如 Weyl 奇异值环（Weyl exceptional ring）、能谱中的点能隙（point gap）以及非厄米趋肤效应（non-Hermitian skin effect）等。

近年来关于非厄米拓扑系统的研究主要局限在两能带模型，人们对于非厄米的多能带拓扑系统的性质了解的不够清楚。徐勇研究组首次针对这一问题进行了探索。基于一维 Aubry-André-Harper 模型，他们在系统的哈密顿量中引入非厄米项，发现在合适的参数条件下，系统中可以同时存在零能和非零能的拓扑边界态。这些拓扑态可以利用卷绕数及 Bott 指数来进行表征。由于相邻格点之间的跃迁振幅是不对称的，具有开边界条件的系统中将存在非厄米趋肤效应，即系统所有的体态都被局域在一维链的某一个端点处。与此同时，当非对称跃迁振幅增强到一定的临界值时，原本存在于一维系统两端的拓扑边界态也会被移动到同一端。尤为有趣的是，对于零能边界态，此时其边界态的数量会从两个变成一个。此外，该研究还发现在无公度系统中，拓扑能带和边界态依旧存在，从而得到拓扑准晶体。最后，他们还提出了利用电子电路对非厄米系统进行模拟的实验方案。

该成果研究论文：Qi-Bo Zeng, Yan-Bin Yang, and Yong Xu. “Topological phases in non-Hermitian Aubry-André-Harper models”, Phys. Rev. B (Rapid Communication) 2020.



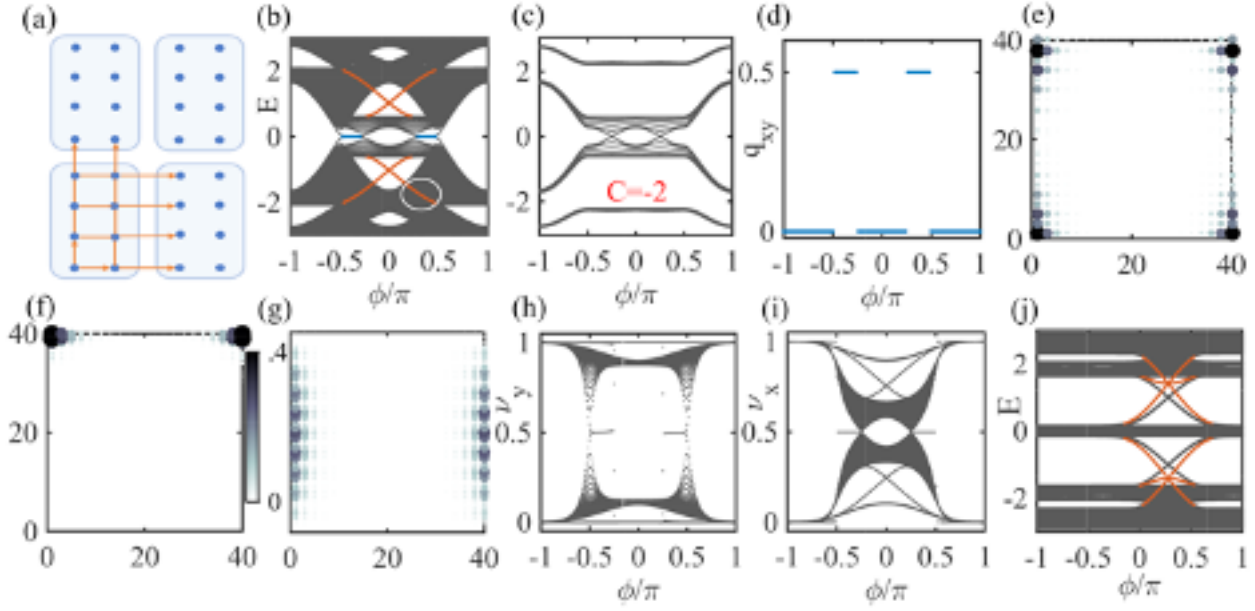


二维 Aubry-André-Harper 模型中的高阶拓扑绝缘体和半金属

根据拓扑系统的块体 - 边界对应原理，如果系统的块体波函数具有非平庸的拓扑性质，那么在该系统的边界上将会存在无能隙的拓扑边界态。对于传统的拓扑系统，拓扑边界态通常都存在于比系统维度低一维的边界上。近年来，有研究表明，通过引入晶格对称性等方式，系统的拓扑边界态可以存在于更低维度的边界上，这一类新发现的拓扑态被称为高阶拓扑态。比如，对于三维拓扑绝缘体，如果其存在二阶拓扑态，则其边界态存在于该系统的一维边界上；而如果其存在三阶拓扑态，则其边界态存在于该系统的顶点处。

高阶拓扑系统具有的奇异性质近年来得到了广泛的关注，但现有的研究主要关注较多的是具有零能角态的二维四极距拓扑绝缘体以及具有非零能量手性边界态（hinge states）的三维二阶拓扑绝缘体。然而，这两种边界态能否存在于同一系统中依然是一个疑问。针对这一问题，徐勇研究组利用一维 Aubry-André-Harper 模型构建了一个二维的高阶拓扑系统。他们发现在这一模型中，零能角态和非零能手性角态可以共同存在。其中，零能角态由系统的四极距进行表征；而非零能角态则是由系统的 Wannier 能带的陈数来刻画。有趣的是，这一系统可以化成三维系统，且非零能角态可以看成是该三维系统的二维表面上存在的陈绝缘体导致的。此外，他们还发现系统中的非零能角态不仅可以存在于能谱的能隙中，也能在连续的块体能谱中存在，从而观察到连续谱中的束缚态现象。基于电子电路模型，他们进一步提出了观测这些现象的实验方案。

该成果研究论文：Qi-Bo Zeng, Yan-Bin Yang, and Yong Xu. “Higher-order topological insulators and semimetals in generalized Aubry-André-Harper models”, Phys. Rev. B (Rapid Communication) 2020.



Edited by Kailin Li

Reviewed by Luming Duan, Jian Li, Xiamin Lv

清華大學 交叉信息研究院
Institute for Interdisciplinary Information Sciences, Tsinghua University