交叉信息研究院

学术科研简报

2019 年 9 月 -12 月

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

目录

人工智能

量子信息

人工智能

一、计算生物学

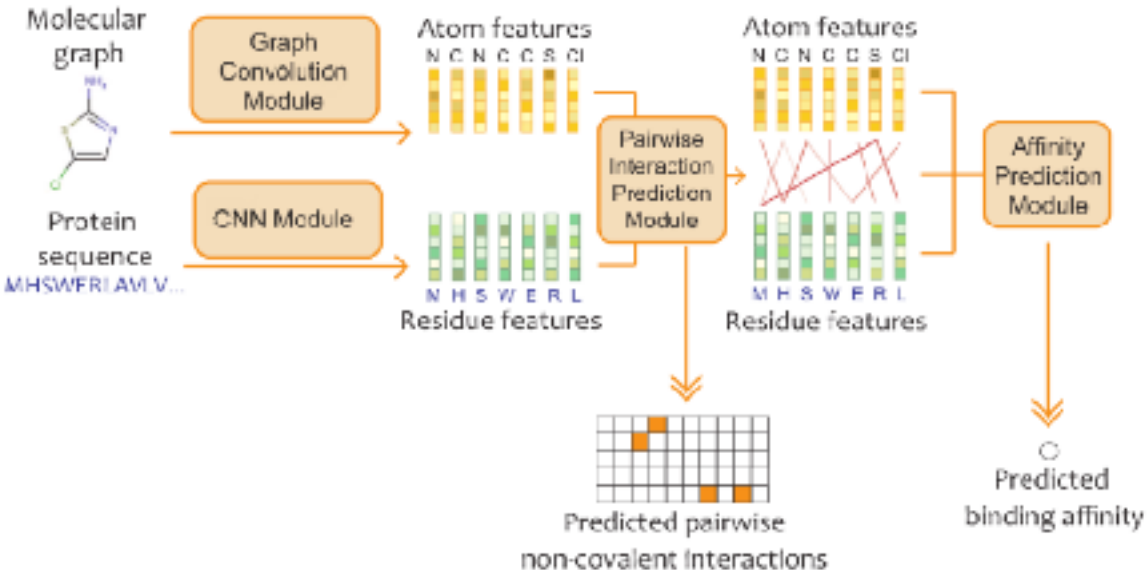
主要完成人：曾坚阳研究组（曾坚阳、李舒雅、万方平等）

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。在曾坚阳研究组的工作中，他们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，并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。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。

该成果研究论文：Shuya Li, Fangping Wan, Hantao Shu, Tao Jiang, Dan Zhao, and Jianyang Zeng. “MONN: a Multi-Objective Neural Network for Predicting Pairwise Non-Covalent Interactions and Binding Affinities between Compounds and Proteins”，RECOMB 2020.



二、机器学习

主要完成人：李建研究组（李建、吕凯风、骆轩源、张楚珩等）

深度学习理论新进展：梯度下在齐次神经网络中的隐式偏好

研究了梯度下降算法在齐次神经网络训练中对不同最优解的隐式偏好。常见的齐次神经网络包括了 ReLU 激活的全连接或卷积神经网络，分析梯度下降在这类网络上是否会收敛到分类间隔较大的最优解，可以帮助研究组更好地理解神经网络的优化及泛化问题。本文的理论分析表明，离散的梯度下降和连续的梯度流在最小化齐次神经网络的逻辑损失或交叉熵损失的过程中，也会逐渐增大标准化分类间隔的一个光滑版变种。经过足够长的训练，标准化分类间隔及其光滑版变种还将收敛到同一极限，并且该极限和一个分类间隔最大化问题的 KKT 点处值相等。本文的结果极大地推广了前人在线性网络上得到的类似结果；相比于前人在齐次网络上的研究，也在使用的假设更弱的情况下给出了更量化的结果。

该成果研究论文：Kaifeng Lyu, Jian Li. "Gradient Descent Maximizes the Margin of Homogeneous Neural Networks"，ICLR 2020.

非凸学习理论新进展：非凸学习随机梯度的泛化误差理论

本文理论上分析了若干梯度学习算法在非凸目标上的泛化能力。泛化误差也即一个学习算法在训练集和真实未知数据集上表现的差距，是机器学习理论最重要的问题之一。基于该文新提出 Bayes-Stability 理论框架，研究组得到了比前人更优的 SGLD 的期望泛化误差上界 O(G/n)，其中 G 和 n 分别是训练路径上梯度的范数之和以及训练集大小。同时该上界对于非高斯噪音、动量加速、和滑动平均等扩展情况一样成立。除此之外，该文还证明了连续时间朗之万运动 (CLD) 任意时刻的 Log-Sobolev 不等式，基于该结论，研究组证明了在加入了 l2 正则化之后，CLD 的期望泛化误差以 O(1/n) 的速度减小，并且该上界可以与训练时间无关。

该成果研究论文：Jian Li, Xuanyuan Luo, Mingda Qiao. "On Generalization Error Bounds of Noisy Gradient Methods for Non-ConvexLearning"，ICLR 2020.

基于学习目标分布的强化学习策略搜索算法

强化学习算法的稳定性是强化学习方法在实际应用中面临的一个重要问题。对于连续控制优化问题，一类常见的做法如下：对于任意一个状态，策略输出一个行动分布，然后再从该分布中采样得到需要采取的行动；算法通过迭代地收集样本和优化策略来学习得到一个好的策略。在该工作中，李建研究组发现现有的一些常见算法在逐渐收敛到确定性策略的过程中会产生较大的梯度，从而影响了训练过程中的稳定性。为了解决该稳定性问题，研究组提出了目标分布学习（TDL）方法用于强化学习中的连续控制优化问题。该方法通过迭代优化的方式来进行策略学习。在每一轮迭代中，该方法先根据按当前策略采样得到的样本来计算得到一个目标行动分布，再通过优化策略神经网络来逼近该分布。该方法在稳定性方面具有以下两方面的优势：其一是该方法能够有效地限定每一轮迭代中策略的变化，从而使得训练的过程变得更加稳定；其二是在每一轮迭代的优化步中，神经网络针对一个固定的目标来做优化，因此该步骤的优化效果受优化参数的影响更小，从而使得整个算法更加稳定。在 Mujoco 中的连续控制任务上，该算法的性能都接近或者超过了现有最优的算法。同时，相比于现有的一些方法，该算法在训练过程中的表现更为稳定，对于超参数也更为鲁棒。

该成果研究论文：Chuheng Zhang, Yuanqi Li, Jian Li. "Policy Search by Target Distribution Learning for Continuous Control"，AAAI 2020.

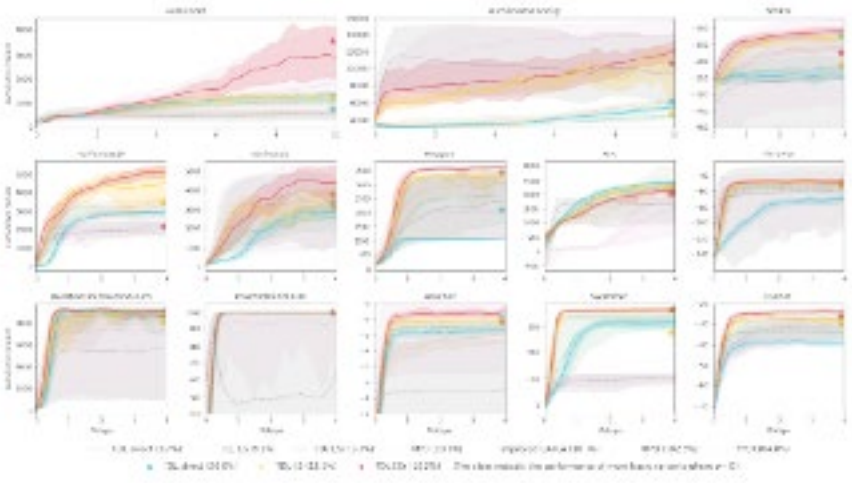


Figure 2: Comparison of several algorithms on MuJoCo tasks. The lines indicate the moving average across five independent runs and the shaded areas indicate the 10% and 90% quantiles. The percentage numbers in the legend indicate the normalized fluctuation of the scores in the last 100 iterations averaged over all the tasks.

三、深度强化学习

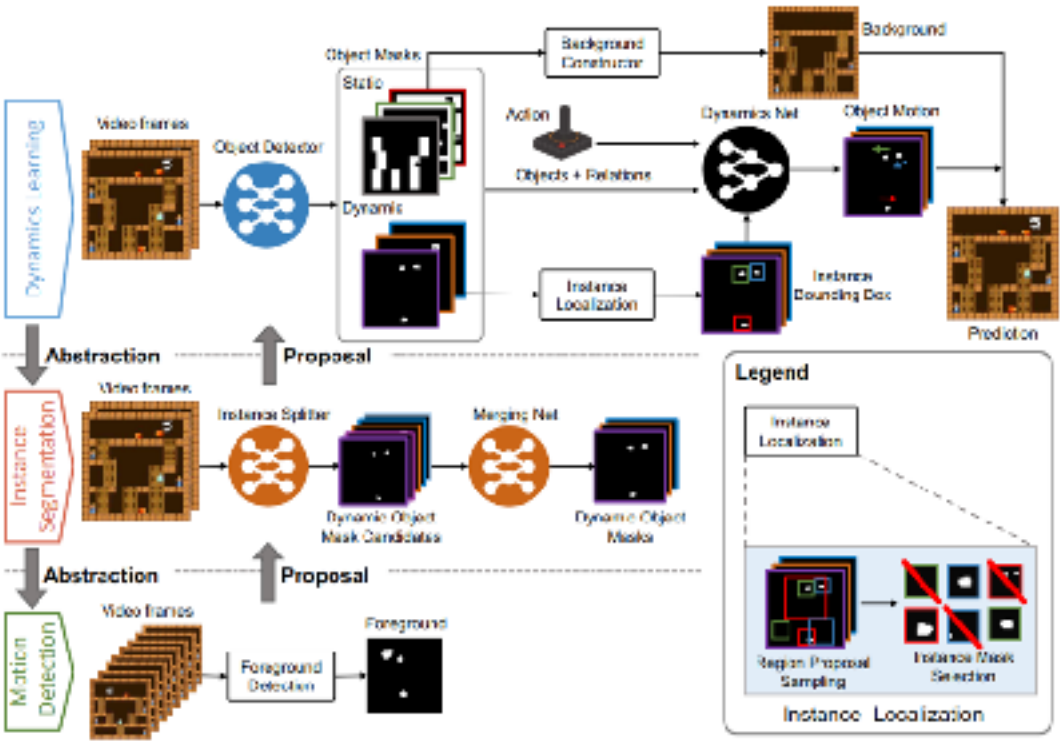
主要完成人：张崇洁研究组（张崇洁、朱广翔、王同翰、王鉴浩等）

基于多级抽象的物体动力学模型学习框架

深度强化学习在博弈对抗、策略规划、任务调度、自动控制、机器人等领域取得了非常惊人的进展，在某些复杂任务上已经超越人类智能。然而，现阶段的深度强化学习主要还只局限于模拟环境中的单一场景下。因为它需要大量的数据进行学习，并且学到的知识难以泛化到新的场景，对于很多人类能在几分钟内熟练掌握的任务，强化学习可能需要采样几天的时间来进行学习。

作为这一领域的一项突破性进展，张崇洁研究组着眼于提高深度强化学习的样本利用效率和泛化能力，提出了面向物体的动力学模型通用学习和规划框架，将物体动力学模型的自监督学习过程分为三级：前后景分离，运动物体分割，和物体动力学预测，并进行基于模型的策略规划。核心思想是，将较难求解的动力学模型学习问题，逐渐分解成更简单的动态物体分割、前后景分离问题。先学习这些简单问题的解，再从学到的简单知识出发作为初始解，最终逐渐学习最终的动力学模型，并根据该模型在未知环境中进行策略规划。通过在 Atari、Pygame 等游戏平台上的实验验证，该三层学习框架具有很强的通用性和泛化能力，提高了样本利用效率。该框架可以使智能体从少量样本中学习，然后在全新的未知环境中准确地预测所有物体的运动，并进行基于模型的策略规划。

该成果研究论文：Guangxiang Zhu, Jianhao Wang, Zhizhou Ren, Zichuan Lin, Chongjie Zhang.“Object-Oriented Dynamics Learning through Multi-Level Abstraction”, AAAI 2020.

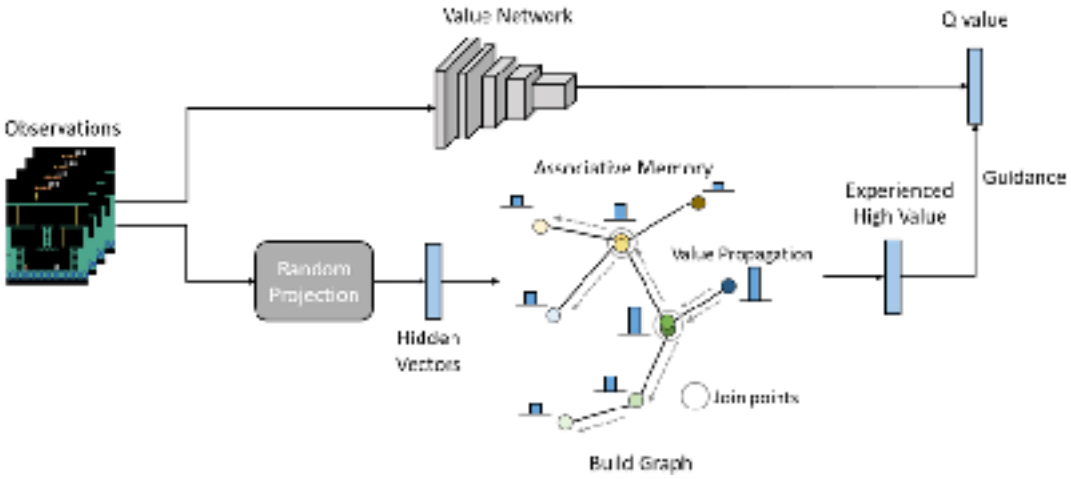


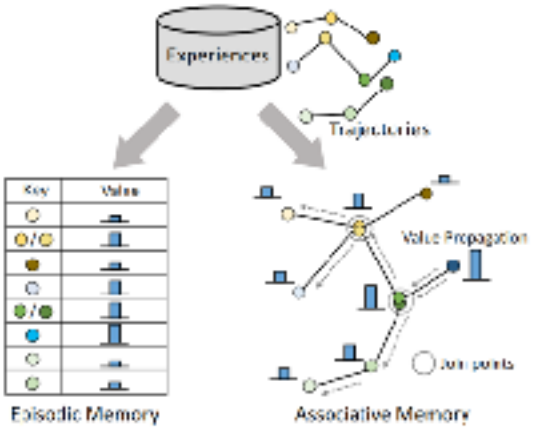
基于联想记忆的情景控制强化学习

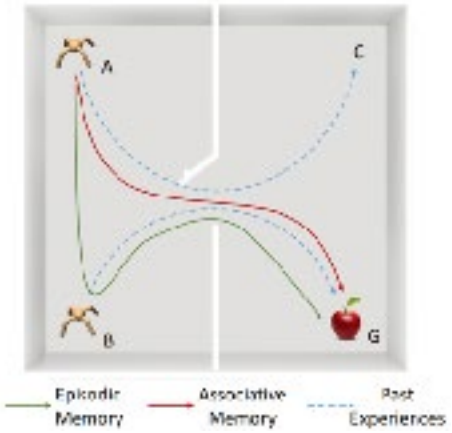
目前深度强化学习已展现很强的学习能力，在一些复杂决策控制的人工问题上，达到或超越人类水平。但是当前强化学习的样本效率非常低，无法应用于大多数现实问题。认知学研究发现，人类的高效学习部分源于类似情景控制的学习模式。在日常学习中我们会记住一些成功的经历，每当遇到一个新情景时，我们会从记忆中搜索过去遇到过的相似经历，根据当时成功的策略来做出快速决策。

作为这一领域的一项突破性进展，张崇洁研究组着眼于提高深度强化学习的样本利用效率，提出了一个新颖的策略学习框架（ERLAM），结合情景控制和强化学习，将情景记忆中有关系的经历关联起来，将独立的记忆碎片连结形成了联想记忆网，更高效地利用已有的成功经历来提高强化学习效率。具体来说，ERLAM 基于状态转换函数进行建图，将所有记忆中的状态关联起来，并开发了一个高效的传播算法，使得值函数可以在图上进行快速更新迭代，最后利用它们更好地指导强化学习。在经典 Atari 游戏上的实验结果表明，该方法相比其他的情景控制强化学习方法平均提高 4 倍以上学习效率。

该成果研究论文：Guangxiang Zhu, Zichuan Lin, Guangwen Yang, Chongjie Zhang. “Episodic Reinforcement Learning with Associative Memory”，ICLR 2020.







通过最简化交流学习近似可分解值函数

多智能体强化学习为研究智能体之间的交流以及深入理解自然语言的起源和进化提供了一种可计算的途径。相关工作在这一领域取得了很大的进展，但其目标大都是学习完全沟通的交流策略，即在一个决策过程中，智能体在每一时刻都要与其他所有智能体进行交流。这与人类所采取的交流方法完全不同——我们只有在有需要的时候才会与特定的人发起一场对话。

针对多智能体协作中的交流问题，张崇洁研究组创新性地提出了最简交流策略的学习方法，即学习智能体在什么时刻与谁交换什么信息，并基于此提出了一个新颖的多智能体值函数分解学习框架（NDQ）。在该框架中，每个智能体学习一个局部价值函数用以评估自己的动作的好坏。智能体传递的信息被要求必须能够减少其他智能体值函数的不确定性；同时通过优化信息的熵值来剔除不能减少他人决策过程不确定性的冗余信息。智能体的价值函数通过一个混合网络被映射到一个全局价值函数。在此结构中，优化后的交流信道实现了近似可分解结构的动态调整。在极具挑战性的星际争霸 2(StarCraft II) 微管理测试集上的实验结果表明，该方法成为了目前最有效的多智能体强化学习算法，并能在不损失性能的前提下完成 80% 的结构分解。

该成果研究论文：Tonghan Wang, Jianhao Wang, Chongyi Zheng, Chongjie Zhang. “Learning Nearly Decomposable Value Functions via Communication Minimization”，ICLR 2020.

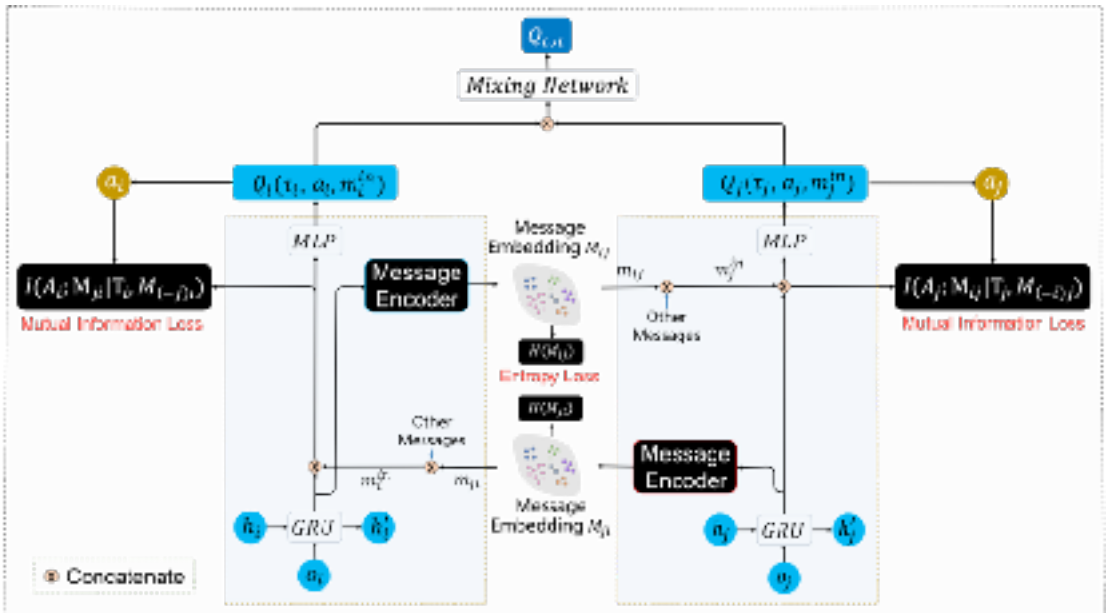


图 1 近似可分解值函数结构

基于相互影响的多智能体协作探索

近期深度强化学习在一些人工的决策控制问题上取得了惊人的进展，取得了接近或超越人类的水准。但是许多复杂的现实问题往往需要多个智能体学习协作来完成。这种多智能体强化学习的一个核心问题就是探索 - 利用困境。因为智能体之间相互作用，以及多智能体系统的决策空间随着智能体的个数呈指数级增长，因而传统单智能体的探索方法在多智能体环境中并不高效。

张崇洁研究组对于这一领域进行了开创性研究，首次建立了协作探索的框架，提出了两种基于智能体之间相互影响的多智能体协作探索策略（EITI 和 EDTI），阐述了通过激励智能体间的相互影响，引导智能体对环境的探索 - 利用，在提高多智能体深度强学习的协作探索效率方面取得了显著突破。具体地说，EITI 和 EDTI 分别利用互信息和交互价值来形式化刻画智能体间的相互影响，进一步推导了互信息和交互价值相对于智能体策略的导数，将两者的优化融入到了经典的策略梯度强化学习框架中，得到了简洁的优化公式。该方法揭示了多智能体协作探索与个体内在奖赏分配之间的联系，将智能体间的相互影响定义成智能体对内在激励，在多智能体强化学习典型探索任务中取得了超过其他算法至少 2 倍的高效探索效率。

该研究成果论文：Tonghan Wang, Jianhao Wang, Yi Wu, Chongjie Zhang. “Influence-Based Multi-Agent Exploration”，ICLR 2020.

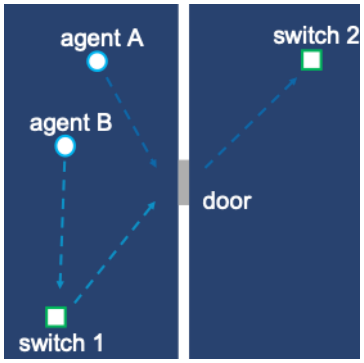


图 1：过门任务

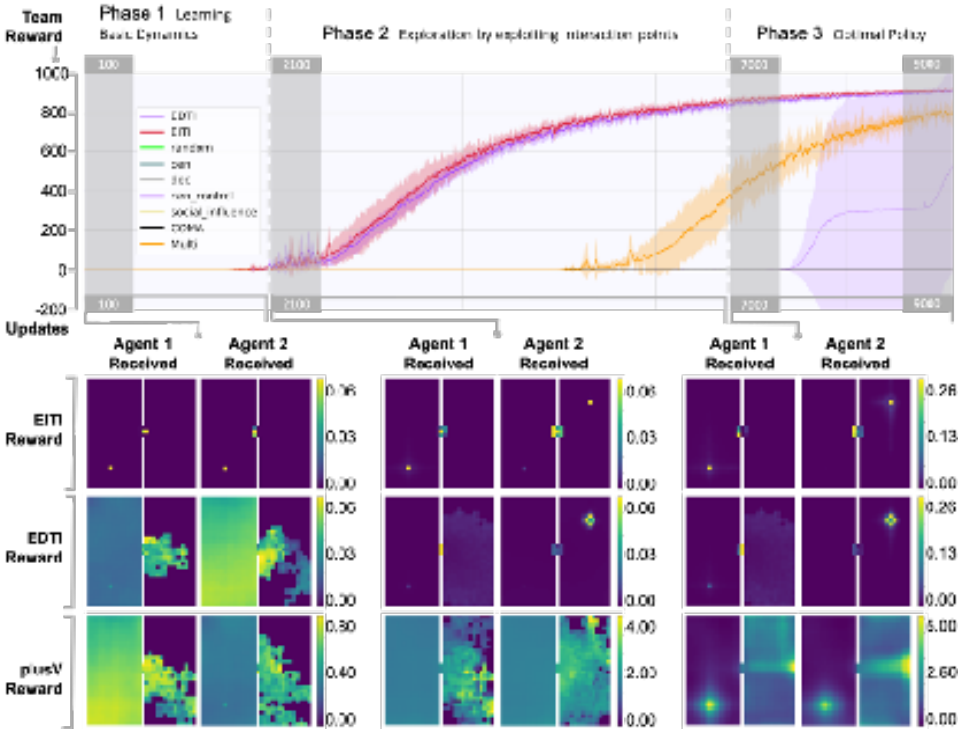


图 2：在 9000 次多智能体强化学习算法迭代更新的过程中，EITI、EDTI 和其他基线的性能对比示意图和不同时刻策略的热点示意图

四、多路策略优化算法

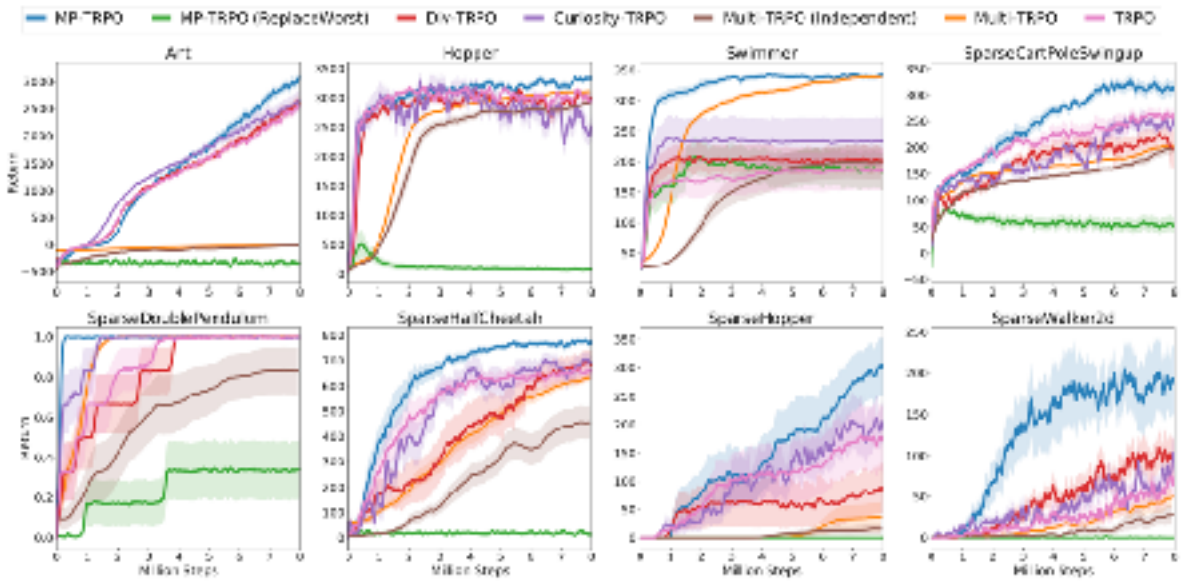
主要完成人：黄隆波研究组（黄隆波、潘玲等）

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。

该研究成果论文在投稿中：Ling Pan, Qingpeng Cai, Longbo Huang. “Multi-Path Policy Optimization”, AAMAS 2020.



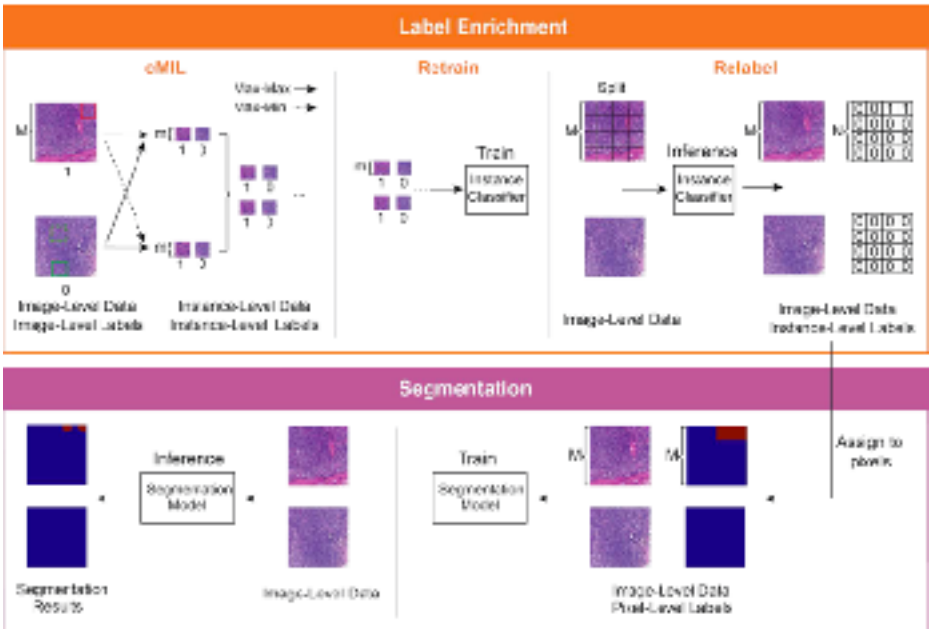
五、网络科学

主要完成人：徐葳研究组（徐葳、孙娇等）

基于弱监督学习的病理影像分析框架

病理报告是肿瘤临床诊断和治疗的“金标准”，是癌症确诊和治疗的基本依据。为了缓解世界范围内病理医生短缺的现状，人工智能病理诊断成为当今学术研究和工程落地的热点。数字病理切片的体积通常都在 500MB 至 2GB，像素数超过百亿，有监督的病理诊断模型需要进行繁琐的像素级切片标注，对这一领域的快速发展带来了挑战。相比之下，弱监督学习仅需要图像级别的粗粒度标签，能够大幅降低标注的工作量。在此研究中，徐葳研究组与透彻影像、解放军总医院合作，提出弱监督学习框架 CAMEL，通过多实例学习（multiple instance learning, MIL），CAMEL 能够通过建模自动生成细粒度（像素级）的标注信息，从而可以使用有监督的深度学习算法完成图像分割模型的建立。通过在 CAMELYON16 和解放军总医院肠腺瘤数据集上的验证，CAMEL 能够取得接近完全有监督模型的准确率。

该成果研究论文：Xu, G., Song, Z., Sun, Z., Ku, C., Yang, Z., Liu, C., Wang, S., Xu, W.. "CAMEL: A Weakly Supervised Learning Framework for Histopathology Image Segmentation"，ICCV 2019.

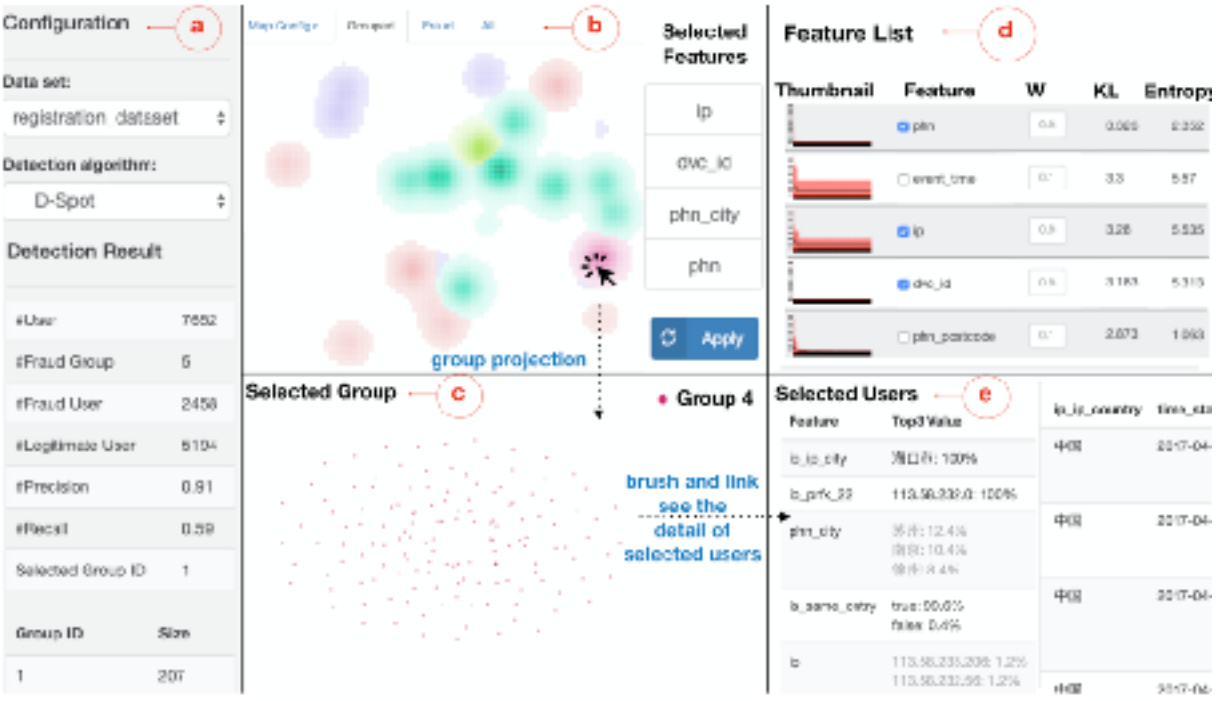


使用可视化交互系统辅助无监督欺诈检测专家进行特征选择和评估

网上欺诈是当今互联网广为人知的阴暗面，学者们提出了很多无监督的欺诈检测算法来检测这些欺诈用户。然而，在特征选择、调整超参数、评估算法效果以及消除那些检测错个体的过程中都需要人类专家的参与，而不能通过算法实现自动化。在欺诈检测领域中，通过可视化系统实现人类专家与检测算法的互动、将人类专家的经验用于帮助进一步提升检测效果一直缺失前沿研究。

作为这一领域的一项突破性进展，徐葳研究组通过对可视化检测算法专家不断采访于密切合作，首次提出并实现了一个端对端的可视化交互系统。算法专家们能够在这个系统中选择他们认为重要的特征并调整这些特征对应的权重，他们也可以在系统中调整算法的超参数，点击系统中“应用”按钮就能在后端重新运行算法并实时地得到新的算法输出。为了近一步简化算法评估，他们还设计了一个基于熵的评价指标，这一指标能够同时体现欺诈群体的行动一致性、罕见性、与正常群体的不同以及消除了异常值对欺诈结果的影响。他们利用这一指标将之前的算法输出结果进行投影，通过一些视觉特性使得欺诈检测专家能够迅速评估本次检测结果的质量。此外，他们还通过两个案例研究以及对欺诈检测算法专家的采访进一步确定了这一交互式可视化系统的有效性。

该成果研究论文：Jiao Sun, Yin Li, Charley Chen, Jihae Lee, Xin Liu, Zhongping Zhang, Ling Huang, Lei Shi and Wei Xu.“ FDHelper: Assist Unsupervised Fraud Detection Experts with Interactive Feature Selection and Evaluation”, CHI 2020.



六、计算经济学

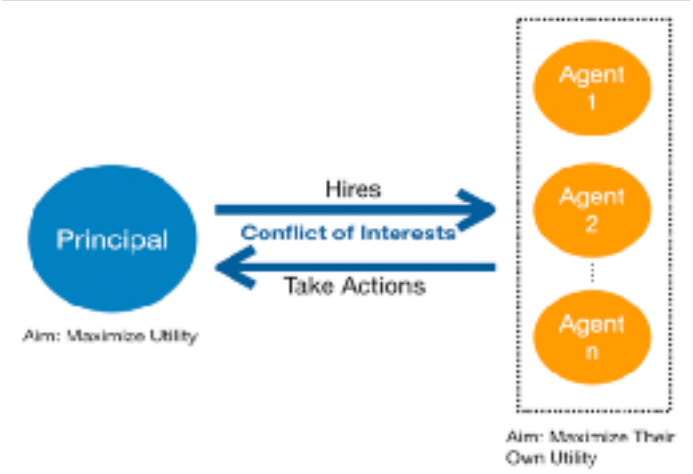
主要完成人：唐平中研究组（唐平中、陈梦静、沈蔚然等）

首次解决多个代理下的委托代理问题

委托代理理论（Principal-Agent Theory）是机制设计（Mechanism Design）的一个重要子领域。在委托代理理论的设定下，一个委托人（Principal）雇佣一个或多个代理（Agent）来完成一项任务。代理可以选择不同的方法来完成这项任务，相应地，委托人会收到不同的报酬。同时，委托人会根据事先商定的合同（Contract）和收到的报酬给予代理相应的奖励。在这类设定下，如何设计合同来最大化委托人的收益是委托代理理论里一个重要的研究课题。以前，对该领域的研究主要集中在一个委托人和一个代理的情景，一个委托人和多个代理的情景由于其复杂性则鲜有经济学家研究。

最近，唐平中研究组在这一领域取得了突破性进展。他们首次证明了在一个委托人和多个代理的情景下，为委托人设计最优合同是一个强 NP 难的问题。同时，他们提出了一个多项式时间的算法来计算一个 O(log n) 的近似最优合同。更进一步，如果代理们满足一些合理的性质，他们还给出了一个多项式时间的动态规划算法来为委托人计算最优合同。

该成果研究论文：Mengjing Chen, Pingzhong Tang, Zihe Wang, Shenke Xiao, Xiwang Yang. “Optimal Common Contract with Heterogeneous Agents”，AAAI 2020.



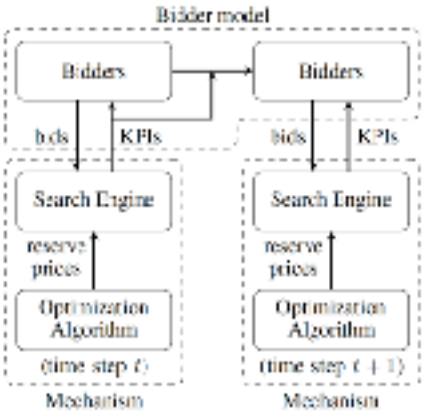
首次提出强化机制设计框架并成功应用于互联网广告拍卖

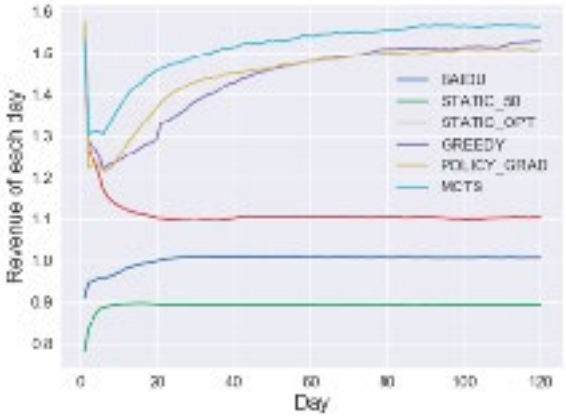
机制设计已成为计算机科学与经济学交叉学科的中心研究课题之一。作为机制设计最重要的应用之一，互联网广告拍卖是 Google，Facebook，百度等互联网企业的主要变现手段。目前，机制设计研究中，理论模型与实际应用之间存在巨大差距。如何结合理论指导，更好地为应用实践服务是一个重要的研究方向。

为了解决以上问题，唐平中研究组结合多年研究成果，首次提出了强化机制设计框架，利用神经网络对平台环境进行建模，利用机制设计理论对机制空间进行合理参数化，并采用强化学习算法对机制进行动态优化。

该框架基于机制设计理论指导和人工智能最新成果，给应用机制设计提供了全新而系统的建模和优化方法。除此之外，唐平中研究组还与百度公司进行深度合作，成功将该框架应用上线，给百度带来了较大幅度的收入提升，百度公司也在其 2018 年第一季度财报中予以重点强调。

该成果研究论文：Shen, Weiran, Binghui Peng, Hanpeng Liu, Michael Zhang, Ruohan Qian, Yan Hong, Zhi Guo, Zongyao Ding, Pengjun Lu, and Pingzhong Tang. "Reinforcement mechanism design, with applications to dynamic pricing in sponsored search auctions"，AAAI 2020.





七、能源经济学

主要完成人：吴辰晔、于洋研究组（吴辰晔、于洋、吴佳蔓、崔竞时等）

用电池就像炒股票?

动态定价，类似于电力市场中的实时电价，可以有效地反映出来电力市场地实时供需变化。本来，如果在经济学理性人的假设下，每个接受动态定价的用户都能实时准确理性地对定价做出反馈，那么系统效率是很有希望大幅度提升的。但是，但由于需求测灵活性的本身不足以及智能控制设备的缺失（无法实时自动做出理性最优决策），这种定价方式在实际中并不能保证有效减少用户端的电费。

不过随着存储系统成本的下降和智能电表的广泛部署，研究组或许可以找到新的机会。认准这个机会，研究组开始探求动态定价机制下，针对终端用户的最优存储控制框架。

储能控制框架设计的关键挑战在于价格的不确定性，如果研究组事先知道动态价格，那么大可以将存储控制问题表述为简单的线性规划问题。但是，动态定价机制下，研究组只能设计在线算法。而由于储能设备自身的特性约束，研究组所有的决策变量，都是在时间上高度耦合的。

受 Chau 等人 [1] 启发，研究组使用负荷分解技术 (one-shot load decomposition) 将原始优化问题分解为一系列单段负荷服务问题（如图 1 所示）。通过假设价格服从的分布，研究组发现一个简单的阈值策略已经可以最小化单段负载服务问题的期望成本 [2]，图 2 通过检验在线与离线算法的差异，展示了阈值策略的有效性。

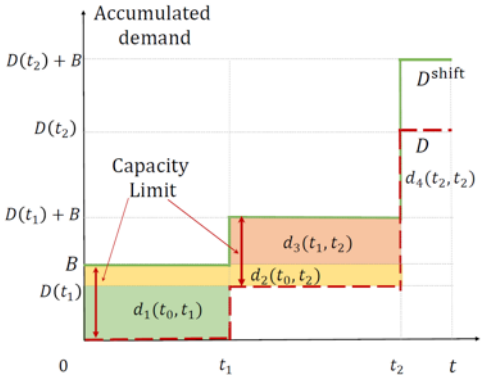


图 1 时段负荷分解技术

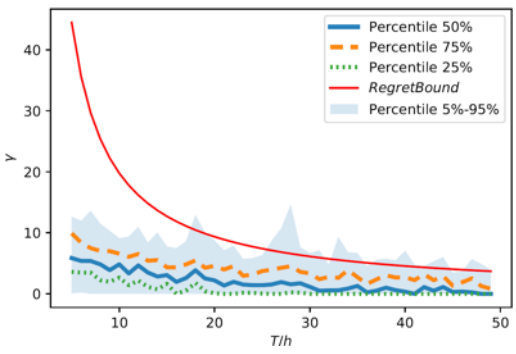


图 2 算法在单段负荷服务问题表现

而单段负荷服务问题，就像买股票一样。假设你今天无论如何也要买某一个股票，现在想要知道，什么时间购买最为合适。最简单的离线方法，就是全天的价格求个最小值，那当然就是最便宜的。但是如果不知道价格的未来信息，研

究组能做的就很有限。如果所有信息均不知道，研究组需要观察一段时间，然后计算出来一个阈值，这种算法可以达到 1/e 的近似最优。不过如果假设价格的分布已知，那么就可以设计一系列的时变阈值，来辅助决策，这个算法就可以达到期望最优。

事实上，研究组还可以通过计算在线策略和离线策略的期望差值将阈值策略的性能与离线最优值进行比较。通过证明时段负载分解技术可以维持解空间不变，研究组说明这种最优控制策略可以有效地构造针对原始问题的最优控制策略 [3]。

另一方面，通过设计数据驱动的价格分布估算器，研究组可以放宽对价格分布知识的假设。这项任务可以采用高斯混合模型（GMM）来实现，使用 EM 算法进行 GMM 参数估计。

该成果研究论文：[1] Chi-Kin Chau, Guanglin Zhang, Minghua Chen.“Cost minimizing online algorithms for energy storage management with worst-case guarantee,” IEEE Trans. on Smart Grid, vol. 7, no. 6, pp. 2691 – 2702, 2016.; [2] Jiaman Wu, Zhiqi Wang, Yang Yu, Chenye Wu.“Optimal Storage Control for Dynamic Pricing”, in submission to IEEE PES General Meeting 2020. https://arxiv.org/abs/1911.06963; [3] Jiaman Wu, Zhiqi Wang, Chenye Wu, Kui Wang, Yang Yu.“A Data-driven Storage Control Framework for Dynamic Pricing”, in submission to IEEE Transactions on Smart Grid, Initial Submission: Nov. 2019. http://arxiv.org/abs/1912.01440.

电力市场中的个性化定价

对于商家而言，好的定价策略至关重要，一般来讲，如果要获得最大的收益，可以进行价格歧视，也就是针对用户进行个性化的定价。对于电力系统而言，个性化的定价指的就是基于用户行为的定价方案，这种方案很可能可以更好地探索需求侧的灵活性。但是，由于电力系统中有海量的客户，对于电力系统运营商来说，在大数据技术兴起之前，这样的任务实在太繁重了。

电力系统中最早“个性化定价”当属对于大用户（日均耗电量大户）的惩罚了。这一惩罚其实蕴涵着一个基本的假设，就是大多数用户用电行为模式几乎相同。在这种假设下，系统的负荷高峰，自然是有大用户贡献的，所以自然该受惩罚！但是，简单的 k- 均值聚类表明这种假设是不成立的。如图 1 所示，我们既能观察到和传统系统负荷类似的类型（C8，C25 这些类的用户），也有各种青椒和研究生的夜猫子类型（C12 这类用户）！

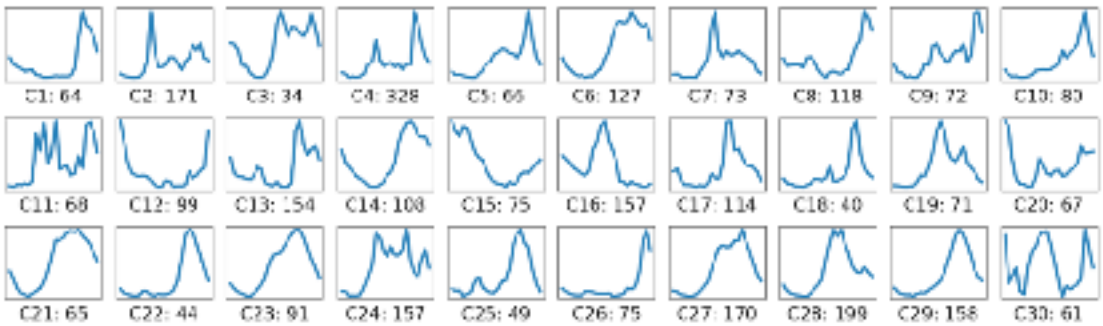


图 1 每个类中心的用电量曲线，每个子图中的标记 (C_n:N) 表示是类 n 的中心用电量，并且该类有 N 个用户（x- 轴：时间，y- 轴：归一化的用电量）

为了识别用户用电行为的不同形态，于洋等研究者提出可以使用 l_1- 范数衡量每个用户对系统的影响，并提出了一个指标，叫做 MCI [1]。该论文的作者论证 MCI 可以作为一个很好的个性化定价策略，并且由每个用户负载曲线的形状（而不是总能耗）唯一确定。 这一观察启发了最朴素的基于用户负载曲线形状，使用 k 均值聚类实现的个性化定价方案。

然而朴素的聚类算法可能会导致市场出现漏洞！这是因为同一类中用户的用电行为并不完全相同，但是却以相同的电价收费。这样的漏洞使得有些“别有用心”的用户仅需对自己的用电行为进行很小的修改就可以跳进电价更低的类。我们在 [2] 中对这种朴素的定价方案进行了脆弱性分析，并引入了一个含参数的脆弱性定义来描述用户的这种行为。在实际数据中，研究组发现使用朴素的定价方案，这样的用户确实存在。图 2 显示了仅仅改变 1% 的需求，部分用户就可以伪装成价格更低的类别，图中的箭头表示这些用户的伪装轨迹。图中类别的颜色越深，表示该类别越稳定，也意味着该类别中的用户更难改变自己的行为。

但是，这个漏洞是否可以被弥补呢？最近，研究组又研究了为什么上述朴素的定价方案容易受到影响。最简单的回答，自然是这类定价方案不具有鲁棒性。但是，其更深层的原因是由于选择了间接的聚类标准。研究组不妨考虑端到端的机器学习，研究组之所以要进行 k- 均值聚类是因为要进行定价！所以聚类应该直接基于 MCI，而不是用户用电形状！图 3 显示，如果要保证鲁棒性，基于 MCI 的聚类仅产生 24 个类，但基于用户用电形状的聚类至少需要产生与红色矩形数量相同数量的类别。

研究组进一步证明，对于基于 MCI 的 k- 均值聚类算法，只要保持每个类的局部特性，就可以保证全局鲁棒性 [3]。此外，由于这种 k- 均值聚类基于单个指标（MCI），因此仅仅使用一个贪婪算法就足以提供到达最优的 k- 均值聚类！

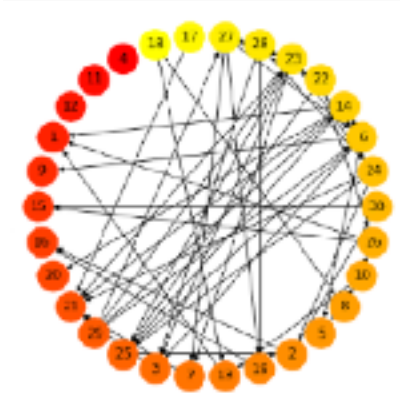


图 2 用户改变类别的轨迹

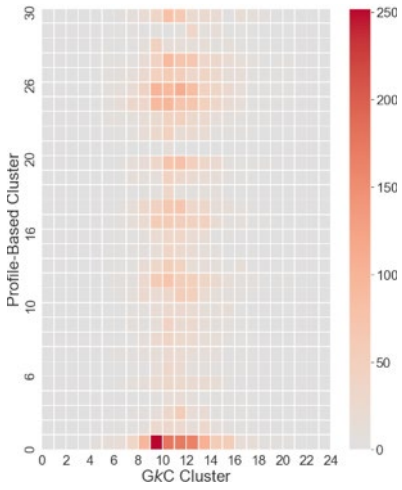


图 3 两种聚类方法之间的关系

该成果研究论文：[1] Yang Yu, Guangyi Liu, Wendong Zhu, Fei Wang, et al. Good consumer or bad consumer: Economic information revealed from demand profiles, IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 2347-2358, May 2018; [2] Jingshi Cui, Haoxiang Wang, Chenye Wu, Yang Yu.“Vulnerable Analysis for Data Driven Pricing Schemes”, in submission to IEEE PES General Meeting 2020, https://arxiv.org/abs/1911.07453, 2019; [3] Jingshi Cui, Haoxiang Wang, Chenye Wu, Yang Yu.“Robust Data-driven Profile-based Pricing Schemes”, in submission to IEEE Transactions on Smart Grid, Initial Submission: Nov. 2019.

八、理论计算机科学

主要完成人：段然研究组（段然、何昊青、张天翼）

多重匹配的新算法

在一般匹配中，每个点只能匹配一个点，即只有一条相邻的匹配边。在广义的匹配中，一个点可以相邻多条匹配边。在图 G=(V,E) 中，广义匹配具体地分为两个问题：

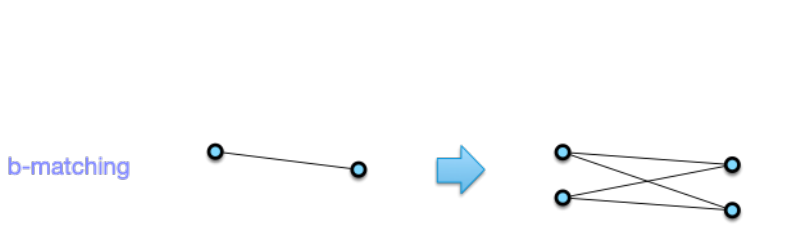
• b-matching: 对于每个点 u 有 1 个正整数 b(u)，b-matching 为边上的函数 x: E → N 使得对于每一个点 u，$\sum_{e=(u,v)} x(e) \leqslant b(u)$。

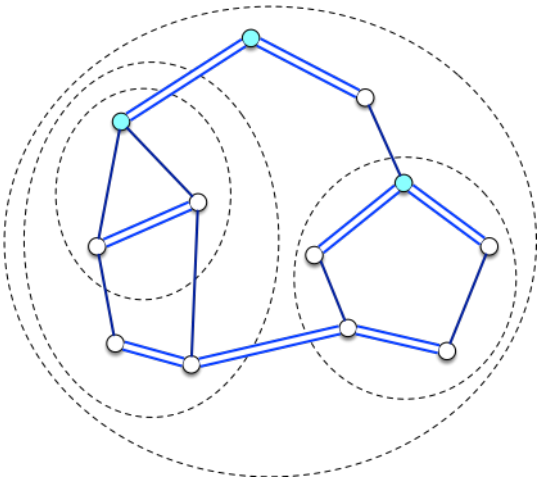
• f-factor: 对于每个点 u 有 1 个正整数 f(u)，f-factor 为边集 E 的 1 个子集 F，使得在 F 中每个点 u 的度 ⩽ f(u)。

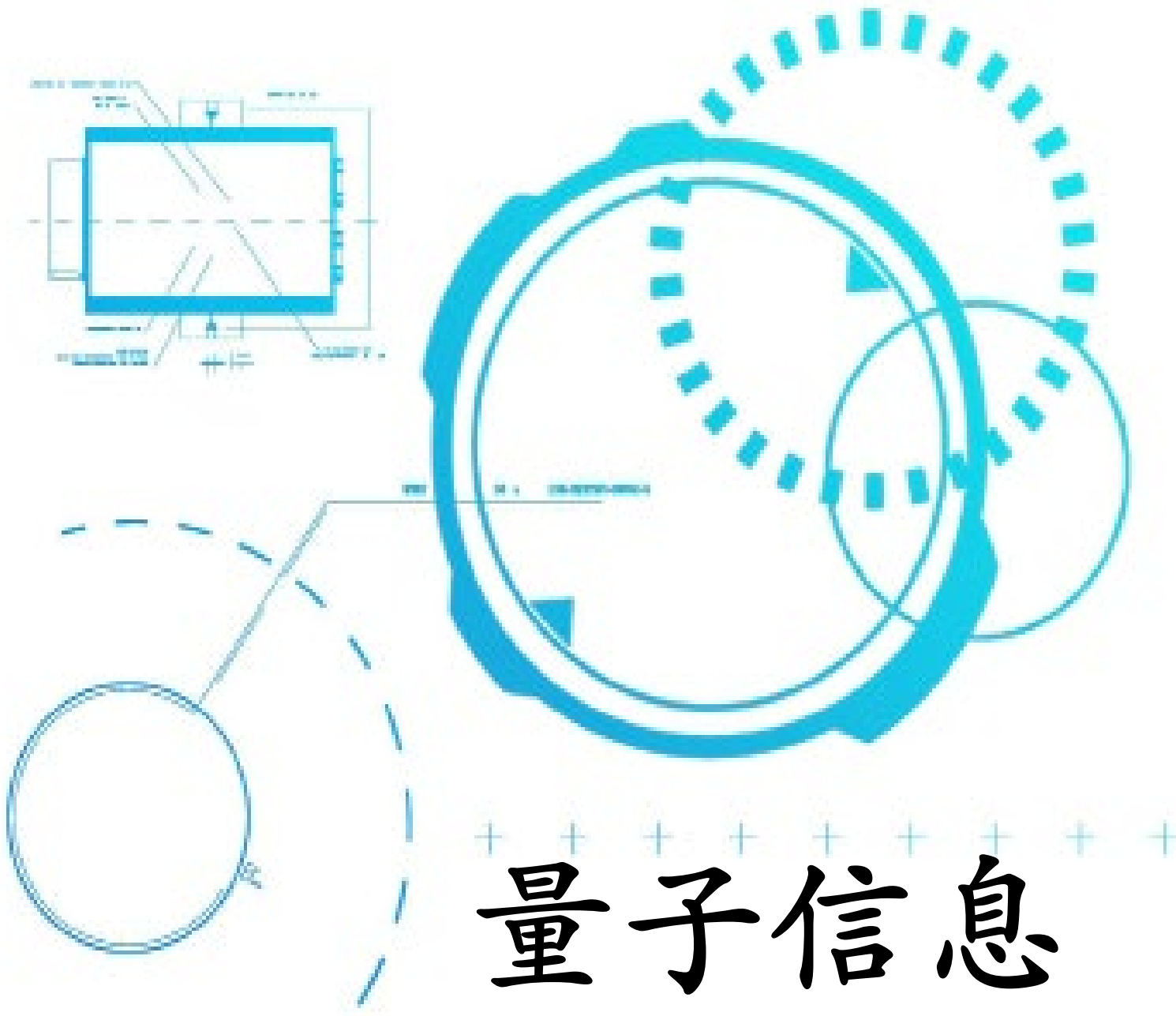
即在 b-matching 中每条边可被重复计算，而在 f-factor 中每条边只会被算一次。在有权图中段然研究组希望找到总权值最大的 b-matching 或 f-factor。研究组可以将 b-matching 或 f-factor 简单地规约到一般匹配，如图一所示。但对于 b 或 f 很大时边数会增大到$\Omega(mn)$；而且对于 f-factor，点数也会增大为$\Omega(m)$，所以即使使用 $\tilde{O}(mn^{1/2} \log W)$ 的算法 [Gabow & Tarjan 1991, Duan, Pettie & Su 2017] 复杂度也会变为 $\tilde{O}(m^{3/2}n \log W)$。（W 为最大整数权值。）对于二分图，b-matching 和 f-factor 可以看作最小费用流，所以有 $\tilde{O}(mn^{1/2} \log^2 W)$ 的代数算法 [Lee & Sidford 2013]。

段然助理教授与学生张天翼、何昊青合作的论文给出了第一个一般图上最大 f-factor 的 o(mn) 的算法，其时间复杂度为 $\tilde{O}(mn^{2/3} \log W)$。因为复杂度与 f 值无关，所以也证明了 f-edge cover 问题（每个点在 F 上的度⩾ f(u)）的复杂度为 $\tilde{O}(mn^{2/3} \log W)$。该研究组的方法将 [Duan, Pettie & Su 2017] 的 scaling 方法用在了 [Gabow 2014] 定义的广义带花树（blossom）上（见图二）。如何将这样的思路推广到 b-matching 上是接下来需要研究的问题。

该成果研究论文：Ran Duan, Haoqing He, Tianyi Zhang. "A Scaling Algorithm for Weighted f-Factors in General Graphs", in submission.







量子信息

一、量子纠缠

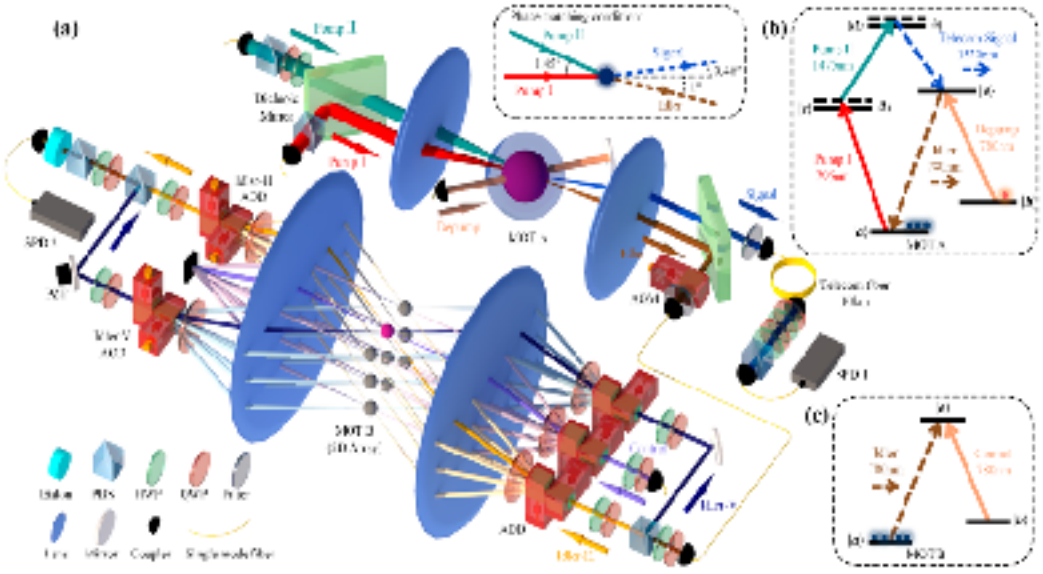
主要完成人：段路明研究组（段路明、常炜等）、马雄峰研究组（马雄峰、周游等）、魏朝晖研究组（魏朝晖、林漓尽致）

远距离量子纠缠态的分发与存储

现阶段构建大规模量子通信网络主要受限于量子信号在自由空间或光纤中传播时会遭受到指数级增长的传输损耗。为了克服这一困难，类似于经典通信中中继器的概念，长程量子通信需要利用量子中继器。量子中继的实现，通常基于 DLCZ（Duan-Lukin-Cirac-Zoller）协议，将长距离信道分割成多个小段并使量子信号在每个小段中高保真地传输，利用量子存储器和纠缠交换来链接分段的信道。DLCZ 量子中继协议的实现，需要具备能够有效存储量子纠缠态的量子存储器以及适合长距离传输的通信波段光子接口。近年来，科学家在此领域开发了量子复用存储技术，大大提高了量子存储器的存储效率和读取速度，同时通信波段光子接口技术也得到了长足发展，但是将这两项技术稳定而又高效地结合起来仍然是该领域的一个难题。

段路明研究组利用巧妙的实验设计，将一个独立的铷原子系综作为光源产生出窄带偏振纠缠光子对，通过选取铷原子特定的原子能级使产生的光子对中一个光子处于衰减系数最小的通信波段（C 波段），另一个光子可以存储于基于铷原子系综的量子复用存储器中。此量子复用存储器利用二维可编程光路，具有多个原子存储单元，并通过电磁感应透明存储技术，可以实现光子态与其中任意一个原子存储单元间量子纠缠态的存储与读取。实验测量出的多个存储单元中读取的光子与经过 10 公里光纤传输后的通信波段光子之间均保持较高的纠缠保真度，证明了此装置可以实现高质量的量子纠缠态的存储和分发，为量子中继器的发展迈出了坚实的一步。

该成果研究论文：W Chang, C Li, YK Wu, N Jiang, S Zhang, YF Pu, XY Chang, LM Duan. "Long-distance entanglement between a multiplexed quantum memory and a telecom photon" , Phys. Rev. X.



基于图态的多体纠缠结构的有效探测

多体纠缠的量子态的制备与检验在很多量子信息处理任务中至关重要。随着近来多体量子系统控制能力的增加，人们迫切需要通过探测多体量子态的性质进而对硬件系统进行有效标定的方法。然而，由于量子态本身的维数随着量子比特数量指数增加，在实际系统中估计多体纠缠的性质一般来说将会极具挑战性。

基于以前关于多体纠缠探测的有关工作，马雄峰研究组提出了一个系统性的基于图态来实现纠缠结构探测的方法。图态是多体纠缠态中最重要的种类之一，其对于基于测量的量子计算，量子网络和量子纠错中均有重要意义。在此工作中，基于一般的图态中 Schmidt 数和 von Neumann 熵的联系，研究组对图态和给定的分离态（separable state）之间的保真度 (fidelity) 给出了解析的表达式，并且提供了估计保真度的有效方法，从而可以灵活地实现纠缠结构的探测。对于一些常见的图态，比如 GHZ 态和一维、二维簇态，该研究组可以仅通过 2 个局域的测量设置来实现纠缠结构探测，极大地提高了探测效率。该方法为多体量子系统的标定提供了系统和有效的方法。

该成果研究论文：You Zhou, Qi Zhao, Xiao Yuan, and Xiongfeng Ma. “Detecting multipartite entanglement structure with minimal resources”, npj Quantum Information.

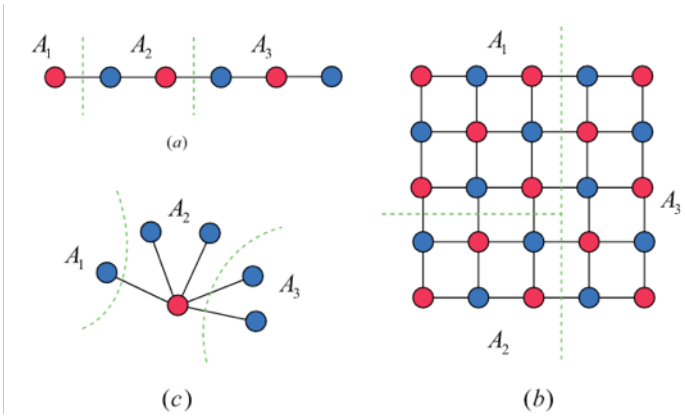


图 1 常见图态的示意图以及测量设置。(a) 一维簇态，（b）二维簇态，（c）GHZ 态

非简并贝尔不等式的判定和纠缠度的实验估计

量子纠缠是量子计算和量子信息的关键资源，在实验室里如何可靠地探测未知量子系统是否存在纠缠是不容易的事情，对纠缠度进行可靠的实验定量估计更是困难得多的任务。魏朝晖研究组的前期工作已证明，通过提出非简并贝尔不等式的全新概念，可以在贝尔实验中得到的关联数据的基础之上，对未知量子态的纠缠度给出解析的定量估计。但是，如何判定一个贝尔不等式是否满足非简并的定义要求，以及此方案的整体性能如何，是未解决的关键遗留问题。

最近，通过分析非简并贝尔不等式的数学结构，研究组发现一个贝尔不等式满足非简并定义要求的充分条件。基于该条件，研究组证明了一大批最常见的贝尔不等式满足此条件，因而表明了提出非简并贝尔不等式概念的合理性。并且，魏朝晖研究组也提出了新的机制来实现基于非简并贝尔不等式的纠缠度解析定量估计。对比表明，新机制的性能远远超出早期的版本。该研究组将新方法应用到 qutrit-qutrit 量子系统中，在不太强的非局域性质下成功给出了提纯纠缠度的下界，显示了该方案的良好效果。经过实验物理学家同行的评估，此理论的要求很合理，现有的光学实验平台完全可以对其进行验证。因此，本结果为纠缠度的可靠实验探测提供了完全可行的理论方案。实验验证的工作已经开始。

该成果的研究论文为：Zhaohui Wei, Lijinzhi Lin. "Analytic Semi-deviceindependent Entanglement Quantification for Bipartite Quantum States", arXiv:1903.05303v3.

基于哈代佯谬的多体量子纠缠结构研究

相对于两体量子纠缠，多体量子纠缠的数学结构要复杂得多，迄今为止人们对这方面的了解依然十分有限。困难的来源之一在于，多体纠缠可以以完全不同的方式呈现。例如，三量子比特系统的纠缠可以有 W 态和 GHZ 态两种不同的形式，它们之间不能通过局域操作来互相转换。刻画和理解多体纠缠的不同结构，以及比较它们的特征，是量子信息研究的基本问题之一。

魏朝晖研究组提出了一个对比多体纠缠不同结构的全新角度，即基于哈代佯谬来刻画它们所呈现的非局域性的不同。具体来说，研究组首先发展出一个新的几何模型来估计三量子比特 W 态在哈代佯谬中的最大违背概率，并将其与 GHZ 态的对应概率做比对，发现前者明显小于后者。因而实现了 W 态和 GHZ 态的一个新对比，对比结果也与我们关于 GHZ 态更纠缠的直觉一致。研究组也将上述几何模型推广到任意 N 量子比特的 W 态，得出了随着 N 的增长，W 态的最大违背概率衰减的速度比 GHZ 态慢得多的对比结果（指数差距），再一次以哈代佯谬的视角观察到两种不同纠缠结构的区别。魏朝晖研究组也完成了一系列数值模拟，验证了上述理论结果。

该成果的研究论文为：Lijinzhi Lin, Zhaohui Wei. "Testing the Structure of Multipartite Entanglement with Hardy's Nonlocality", arXiv:2001.02143.

二、超导量子计算

主要完成人：孙麓岩研究组（孙麓岩、王韦婷等）

超导量子系统中演示量子资源的动态转化

量子计算机遵从量子力学，具有超越经典计算机的强大能力。但究竟是哪一个量子特性使得量子计算机具有超越经典的量子优势，这一问题一直以来困扰着人们。最初科学家们认为量子纠缠为量子计算机提供了超越经典计算机的必要条件，然而，“deterministic quantum computation with one qubit”（DQC1）算法的提出挑战了人们原有的认知。当计算某一特定问题时，即使量子系统的纠缠度很小甚至没有纠缠，DQC1 算法仍可以实现指数级的量子加速。这也就是说除了量子纠缠，还有更广义的量子资源为量子计算机提供了量子优势。其中，discord 和 coherence 被认为是最主要的两种量子资源。2016 年，科研人员在理论上证明这两种资源可以相互转化，类似在热机中两种能量的相互转化。DQC1 算法为研究这两种量子资源的转化提供了可能。

2008 年，DQC1 算法在光学系统中首次被演示，随后 2011 年在核磁共振系统中也得到实验验证。清华大学量子中心实验团队首次在超导平台中实现了 DQC1 算法。孙麓岩研究组利用量子反馈控制技术在超导电路中确定性地制备了高维最大混合态，不仅成功演示了该算法，还更进一步跟踪了在 DQC1 算法中两种量子资源 discord 和 coherence 的相互转化，首次在实验上表征了量子资源的动力学转化过程。这一实验结果为广受关注的量子资源的理论研究提供了又一个重要的实验平台，也是在复杂量子计算过程中研究量子资源动力学的关键一步。

该成果研究论文：W. Wang, J. Han, B. Yadin, Y. Ma, J. Ma, W. Cai, Y. Xu, L. Hu, H. Wang, Y.P. Song, Mile Gu, and L. Sun.“Witnessing Quantum Resource Conversion within Deterministic Quantum Computation Using One Pure Superconducting Qubit”, Phys. Rev. Lett..

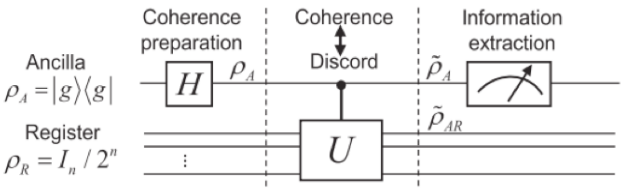


图 1 DQC1 模型

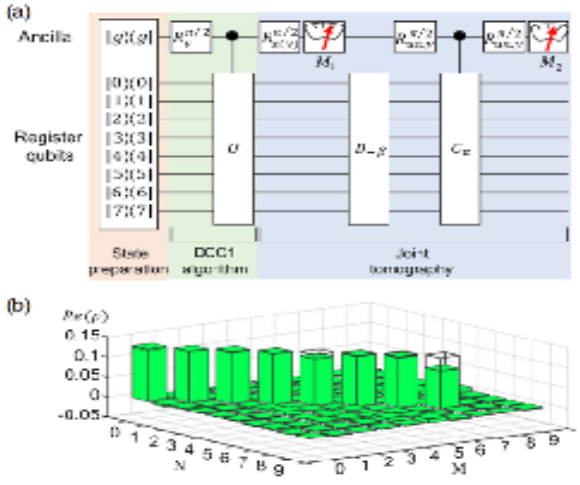


图 2 QDC1 算法的实验流程图和实验上确定性制备的最大混合态

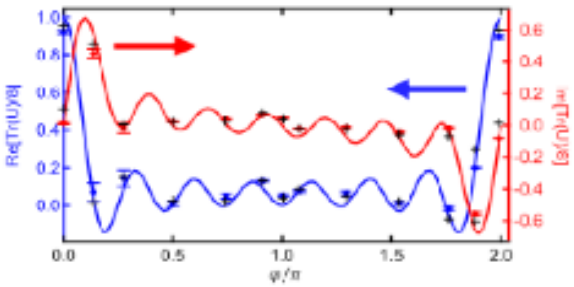


图 3 DQC1 算法实验结果

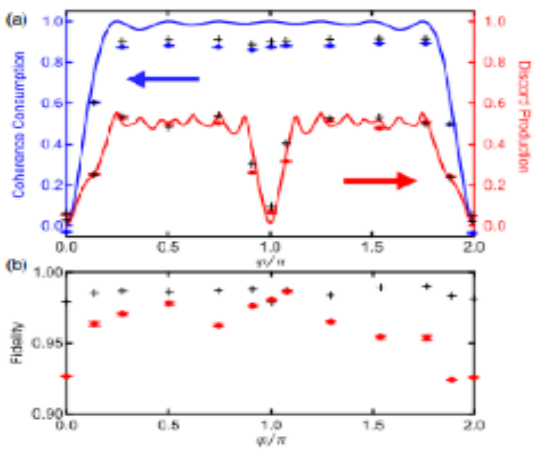


图 4 实验中跟踪在 DQC1 算法中 discord 和 coherence 的相互转化

超导量子系统中实现单模量子传感器

精确测量一个物理量的值是物理学家们孜孜以求的目标，同时也是科学技术发展的一个重要推动力。在量子测度学中，科学家们一直都在探索利用量子特性来提高测量精度。利用高度纠缠的 NOON 态或 GHZ 态的双模干涉仪和利用压缩态的迈克尔逊干涉仪在量子测度学中有着广泛的应用，例如著名的引力波探测仪 LIGO。但无论是高纠缠度的 NOON 态和 GHZ 态，还是压缩态都很难制备，而且这些双模干涉仪都需要非局域操作和非局域测量，这使得这些方案的应用面临非常大的挑战。

为了解决这些困难，近年来科学家们提出了单模量子传感器的概念。孙麓岩研究组与理论物理学家合作，首次在超导量子电路系统中演示了单模量子传感器。在这个实验中，他们利用高相干的超导微波谐振腔与超导量子比特的耦合，以微波谐振腔中的福克态叠加态作为传感器，实现了高精度的相位估计。这个工作避开了传统量子测度学中多模纠缠需要的非局域操作，而测量精度能够接近量子海森堡极限。这一工作还演示了一种可扩展到光学与微波复合系统的测量方案，展示了超越经典极限的测量精度，促进了量子测度学在不同物理系统之间的应用。

该成果研究论文：W. Wang, Y. Wu, Y. Ma, W. Cai, L. Hu, X. Mu, Y. Xu, Zi-Jie Chen, H. Wang, Y. P. Song, H. Yuan, C.-L. Zou, L.-M. Duan & L. Sun.“Heisenberg-limited single-mode quantum metrology in a superconducting circuit”, Nature Communications.

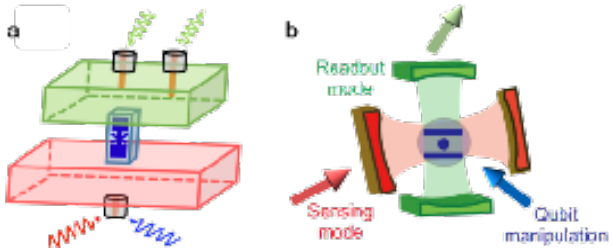


图 1：实验装置图和单模量子传感器示意图

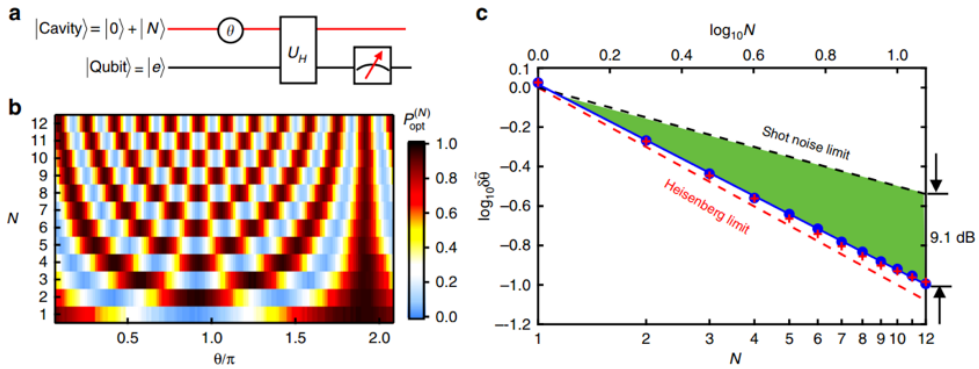


图 2：最优化单模传感器方案的实验流程图和实验结果。测量精度接近量子海森堡极限

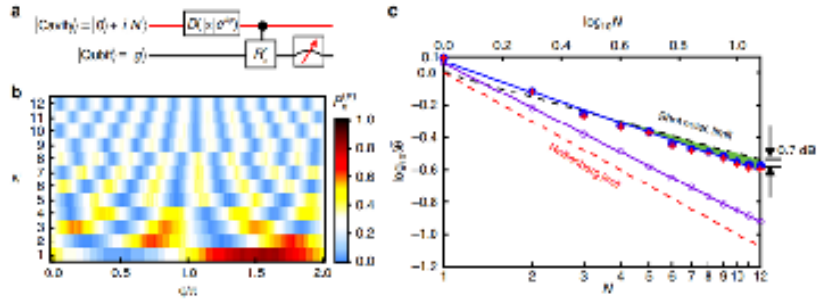


图 3：微波与光波复合单模传感器方案的实验流程图和实验结果。在超导平台中演示该方案，实现测量精度超越经典极限

三、量子计算

主要完成人：金奇奂研究组（金奇奂、张宽等）

协作计算的从经典到量子

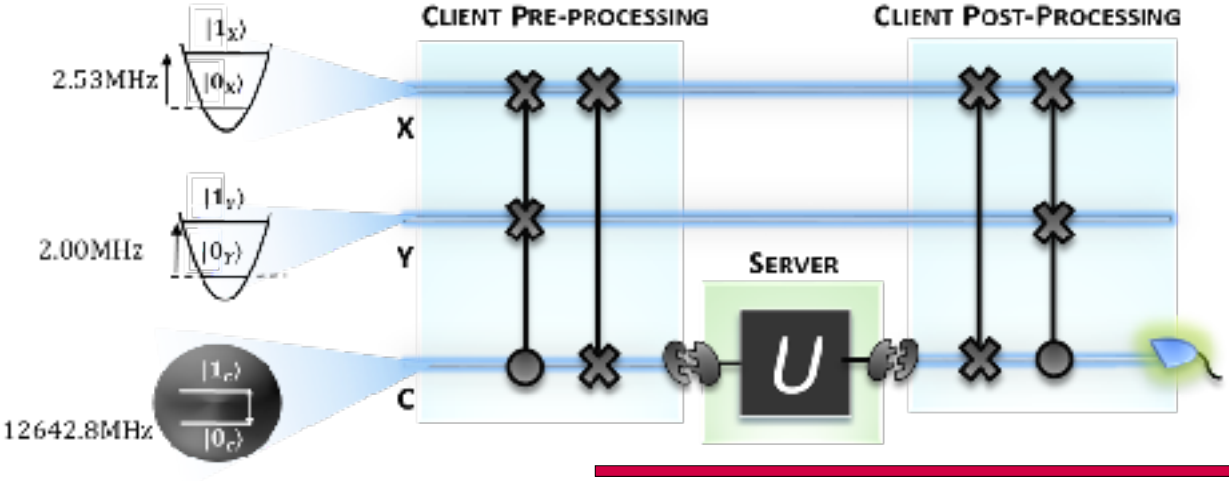
在乐高电影中，大师建造者具有绝地般的能力，能够通过将边角料和部分现有结构组装在一起，来制造不同的逃跑用的交通工具，例如飞行沙发。这些构造仅受制于建造者的想像力（以及一些关于结构完整性的工程原理）。然而，这种强大的能力是通过一种称为模块性的非常微妙的技术实现的——这种技术使人们可以即插即用，将无数模块以无限组合的方式结合在一起。模块性是一种经典的设计原理，它允许不同的零件（如乐高积木）被独立构建，然后通过标准化接口连接到一起——这里所有的乐高积木都具有相同的凹凸图案，即使形状和功能各不相同，也可以实现互连。

乐高世界之外，模块性对人类社会和科技也是至关重要的。它的用途从模块化家具之类的简单事物一直扩展到复杂的计算机代码，以至于人们可以在线连接服务器，通过应用程序编程接口 (API)——使人们可以将部分计算或服务与远程服务器相连接或断开。在现实世界中，这给了人们与大师建造者相似的能力——人们可以独立升级设备的不同部分，或自由地更换服务器。

然而，当人们开始计算量子力学时，模块化架构会变得有些棘手。量子计算机的特别之处在于，它从量子叠加和量子纠缠中汲取了很多能力。一个量子位可以同时为 0 或 1，更有甚者，两个量子位可以纠缠在一起，以使它们同时为全 0 或全 1。为了在协作环境中获得量子计算的全部能力，人们需要在服务器和客户端之间维护这些量子属性。例如，客户端是否可以请求服务器以量子叠加的方式同时执行函数 1 和函数 2，甚至将此操作与她计算机中的量子位纠缠在一起？事实上，目前实现这些设想的现有方法与模块化设计存在根本冲突。为了升级协作量子计算的任一方，其它各方都将受到影响。因此，各个组件不再可以在即插即用架构中互换。

在这里，研究组报告该原型是在离子阱量子计算机实现如何使用量子 API 来实现称为 DQC1 的分布式量子算法——它能高效地计算一些经典计算机难以处理的函数。

该成果研究论文：Kuan Zhang, Jayne Thompson, Xiang Zhang, Yangchao Shen, Yao Lu, Shuaining Zhang, Jiajun Ma, Vlatko Vedral, Mile Gu & Kihwan Kim. "Modular quantum computation in a trapped ion system", Nature Communications.



四、量子相干性

主要完成人：马雄峰研究组（马雄峰、周游、赵琦等）

相干噪声下纠缠探测

量子信息实验系统在制备量子态的过程中不可避免地会遭受各类噪声，大致可以分为白噪声和与系统误差相关的相干噪声。以往的纠缠目击算符在相干噪声的影响下很难反应系统真实的纠缠。马雄峰研究组博士生周游针对于广泛使用的 GHZ 态，通过离散傅里叶变换的方法改进了目击算符，只需要在以前的基础上增加一个测量就能通过数据后处理很好地消除相干噪声的影响。该工作不仅可以提升纠缠探测成功率还能反馈系统噪声参数，

该研究成果论文：You Zhou. “Entanglement detection under coherent noise: Greenberger-Horne-Zeilinger-like states”，Phys. Rev. A.

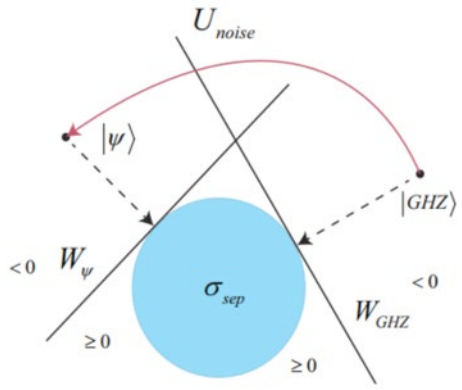


图 2 抵抗相干噪声的纠缠探测示意图

量子相干性与内禀随机性

量子力学中测量的不确定性是量子信息领域目前研究的热点。量子相干性资源理论研究相干性度量的解释以及与其他量子特性（例如量子纠缠、量子失谐和内禀随机性）的相互作用。量子相干性可以被视为通过在一个给定的计算基矢上测量量子态来生成内禀随机性的资源。以前的工作表明，在渐近意义下，量子相干性的稀释率确实量化了相关（经典）系统关于系统测量结果的不确定性。

在这项工作中，马雄峰研究组分析了更加一般的情况，将内禀随机性与相干性的相对熵联系起来。相对熵是量化渐近可蒸馏相干性的另一个重要的相干性度量。研究组比较了两种相干性度量：基于 formation 的相干性和相对熵的相干性度量，并论证了两种度量在一般情况下的不同。有趣的是，在对系统进行局部测量之后，两种度量的差别由另一种量子资源：量子失协来反映。

该成果研究论文：Xiao Yuan, Qi Zhao, Davide Girolami, and Xiongfeng Ma. “Quantum Coherence and Intrinsic Randomness”, Advanced Quantum Technology.

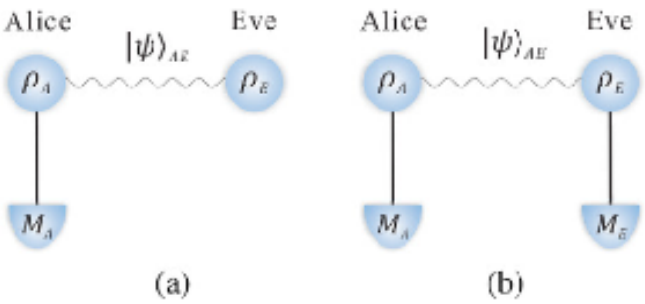


图 2 在量子环境和经典环境下的量子随机性的环境比较。（a）量子环境下，窃听者 Eve 存取量子态，从其中获得 Alice 的测量结果有关信息。（b）在经典环境中，Eve 选取最优测量，通过测量结果来推测 Alice 的测量信息。

五、量子人工智能

主要完成人：邓东灵研究组（邓东灵、蒋飚，陆思锐等）

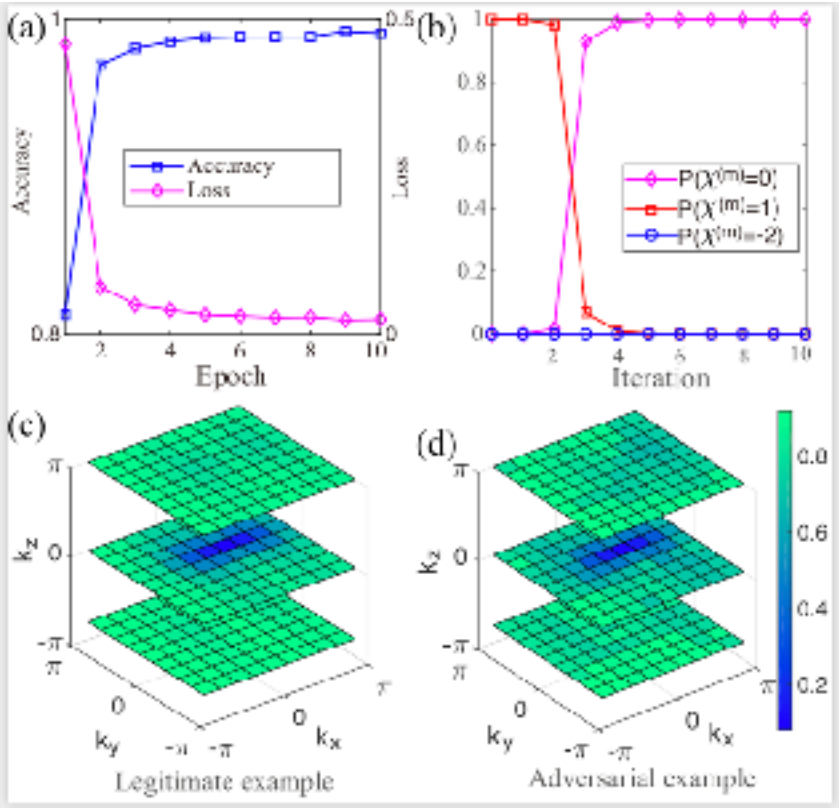
机器学习物质相的脆弱性

机器学习物质相是最近新兴的前沿交叉领域，受到了凝聚态物理学界极大关注。其主要思想是把机器学习领域的一些方法和技术运用于凝聚态物理的研究中，比如用监督学习的方法来识别不同的物质相。

通过研究深度神经网络对于对抗样本的脆弱性，即加入很小的扰动就可以导致神经网络给出错误预测的性质，邓东灵研究组发现运用机器学习研究物质相的方法同样具有相似的脆弱性。为更直观清晰地揭示这一点，本文研究了两个具体的实例。一个是二维的 Ising 模型，研究发现如果在原始自旋构型图片中加入精心构造的微小扰动，甚至只改变一个像素，则训练好的深度前馈神经网络会给出错误的预测（比如把来自铁磁相的图片错误地判断成了反铁磁相）。另一个例子是三维的手性拓扑绝缘体，研究发现一个简单的三维卷积神经网络可以很有效地区分不同的拓扑态，但是如果往输入数据（比如冷原子实验中直接测量的 time-of-flight 图片）中加入非常小的精心设计的扰动，则此网络同样会给出错误的预测，把来自于拓扑相的图片识别成非拓扑相。

本文揭示了用机器学习方法研究物质相的脆弱性，对今后此方向的理论和实验研究都将产生影响。

该成果研究论文：Si Jiang, Sirui Lu, and Dong-Ling Deng. "Vulnerability of Machine Learning Phases of Matter", arXiv: 1910.13453.



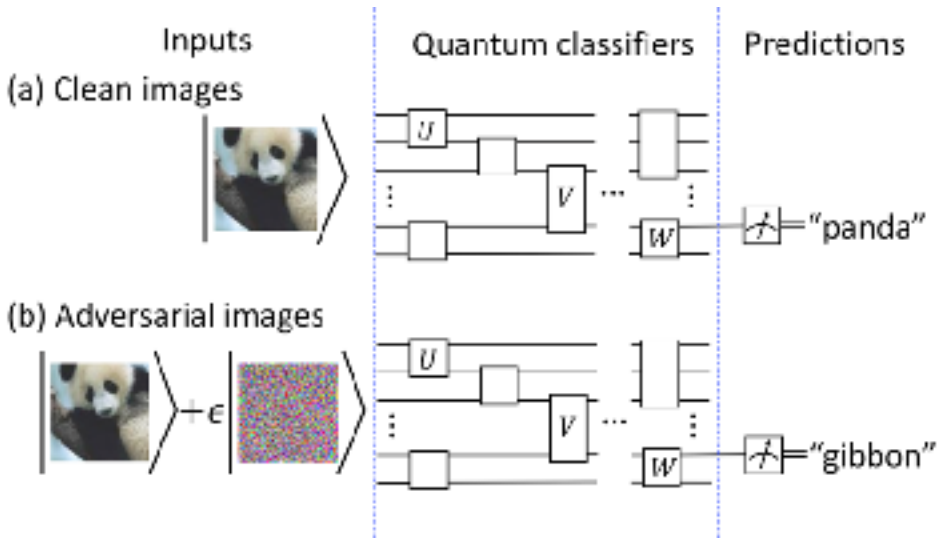
量子对抗机器学习

在经典机器学习中，一个重要的分支是对抗机器学习。这是一个机器学习与计算机安全的交叉领域，旨在给恶意环境下的机器学习技术提供安全保障。在机器学习中，对抗样本普遍存在。一个非常著名的例子是 Szegedy 等人在 2013 年发现的：在对一张标签为熊猫的图片添加部分扰动后，在人眼中仍然分为熊猫，但深度神经网络模型却将其错误地分成了长臂猿，且给出了高达 99.3% 的置信度。

本研究引入了量子对抗机器学习的概念，指出对量子机器学习系统也有对抗样本的存在，且其存在性是普遍的，不依赖于输入数据是经典的或量子的，也不依赖于具体的量子学习模型。本论文研究了量子分类器在三个具体场景中的应用，通过大量全面的数值模拟充分地展示了量子学习系统对于对抗扰动的脆弱性以及如何获取对抗样本，如何增强其鲁棒性等。

本研究在量子机器学习与计算机安全之间架设了一个桥梁，揭示了量子学习系统可能的安全隐患，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：Sirui Lu, Lu-Ming Duan, and Dong-Ling Deng. "Quantum Adversaril Machine Learning", arXiv: 2001.00030.



Edited by Kailin Li

Reviewed by Xiamin Lv

Institute for Interdisciplinary Information Sciences, Tsinghua University