

黄仁泓

浙江大学，中国杭州

+86-13620950268 | renh2@zju.edu.cn | renh2.github.io

教育背景

浙江大学

中国杭州

博士研究生，计算机科学

2022.9 - 至今

- 导师：杨洋

浙江大学

中国杭州

工学学士，计算机科学

2018.9 - 2022.6

- GPA: 3.97/4.00

新加坡国立大学

新加坡肯特岗下路

访问学生，计算机科学

2021.8 - 2021.9

- 课程：机器学习、物联网

复旦大学

中国上海

访问学生，计算机科学

2022.9 - 2023.9

- 导师：许嘉蓉

发表论文

- Renhong Huang**, Ning Tang, Jiarong Xu, Yuxuan Cao, Qingqian Tu, Sheng Guo, Bo Zheng, Yang Yang. *PolicySim: An LLM-Based Agent Social Simulation Sandbox for Proactive Policy Optimization*. WWW 2026 口头报告.
- Siwei Zhang, Yun Xiong, Xi Chen, Zi'an Jia, **Renhong Huang**, Jiarong Xu, Jiawei Zhang. *RAPO: Expanding Exploration for LLM Agents via Retrieval-Augmented Policy Optimization*. KDD 2026 口头报告.
- Renhong Huang**, Dongdong Hua, Yifei Sun, Sitao Ding, Hanyang Yuan, Daixin Wang, Yang Yang. *RAT: RunAnything via Fully Automated Environment Configuration*. EMNLP 在审.
- Chaojian Shi*, **Renhong Huang***, Xulan Qiu, Jiawei Zhou, Yunsong Zhou. *Modular Representation Steering for Multi-Attribute LLM Alignment*. EMNLP main.
- Dongdong Hua, Yifei Sun, **Renhong Huang**, Feng Gao, Chunping Wang, Yang Yang. *PTCG-Bench: Can LLM Agents Master Pokemon Trading Card Game?*. EMNLP 在审.
- Ning Tang, Chenghan Xie, Hanyang Yuan, Yi Li, **Renhong Huang**, Qian Kou, Xiaofeng Shi, Hua Zhou, Jiarong Xu. *ChartWalker: Benchmarking the Cross-Chart RAG Task*. arXiv 2026.
- Yuxuan Wang, Yateng Tang, **Renhong Huang**, Jingwen Zhou, Siwei Zhang, Yun Xiong, Xuehao Zheng, Jiarong Xu. *A Transaction Foundation Model for Financial Risk Assessment on Online Payment Platforms*. CIKM 2026.
- Renhong Huang**, Yuxuan Cao, Yi Li, Junwei Hu, Zihua Xiong, Shuai Fang, Sheng Guo, Bo Zheng, Yang Yang. *Trimming the Fat: Redundancy-Aware Acceleration Framework for DGNNs*. AAAI 2026.
- Hanyang Yuan, Ning Tang, Tongya Zheng, Jiarong Xu, Xintong Hu, **Renhong Huang**, Shunyu Liu, Jiacong Hu, Jiawei Chen, Mingli Song. *Tree of Preferences for Diversified Recommendation*. NeurIPS 2025.
- Renhong Huang**, Jiarong Xu, Zhiming Yang, Xiang Si, Xin Jiang, Hanyang Yuan, Chunping Wang, Yang Yang. *Extracting Training Data from Molecular Pre-trained Models*. NeurIPS 2024.
- Hanyang Yuan, Jiarong Xu, **Renhong Huang**, Mingli Song, Chunping Wang, Yang Yang. *Towards More Efficient Property Inference Attacks on Graph Neural Networks*. NeurIPS 2024.
- Renhong Huang**, Jiarong Xu, Xin Jiang, Ruichuan An, Yang Yang. *Can Modifying Data Address Graph Domain Adaptation?* KDD 2024 口头报告.

Renhong Huang, Jiarong Xu, Xin Jiang, Chenglu Pan, Zhiming Yang, Chunping Wang, Yang Yang. *Measuring Task Similarity and Its Implication in Fine-Tuning Graph Neural Networks*. AAAI 2024.

Jiarong Xu, **Renhong Huang**, Xin Jiang, Yuxuan Cao, Carl Yang, Chunping Wang, Yang Yang. *Better with Less: A Data-Centric Perspective on Pre-Training Graph Neural Networks*. NeurIPS 2023.

Yifei Sun, Haoran Deng, Yang Yang, Chunping Wang, Jiarong Xu, **Renhong Huang**, Linfeng Cao, Yang Wang, Lei Chen. *Beyond Homophily: Structure-aware Path Aggregation Graph Neural Network*. IJCAI 2022.

Jiarong Xu, Zhiming Yang, Xiang Ao, **Renhong Huang**, Chenglu Pan. *Release Graph Pre-Trained Model via Privacy-Preserving Data Augmentation*.

Zhengzhe Fu, Renhong Huang, Rongjie Jiang, Guandong Sun, Feng Zhao, Yang Yang. *From Bag-of-Documents to Structure-Aware Synthesis: Resolving Conflicts in RAG*. KDD 在审.

研究经历

具身 VLA Harness 架构人形机器人系统	2026.07 - 至今
在研项目	浙江大学
- 提出首个面向人形机器人的具身 VLA Harness 架构，将规划、推理、监控、记忆与工具调用解耦为独立模块，提升长程任务执行的稳定性与安全可控性。 - 从零构建仿真和真实接口，开发遥操和数据采集系统，部署 VLA，并设计 VLA 任务提升真机表现。	
自动化 CoT 数据合成流水线自进化	2026.06 - 至今
在研项目	浙江大学
- 面向 RL 前冷启动，构建可自动迭代的 CoT 数据合成流水线，通过 teacher 选择、prompt / reasoning 改写、难度分布与多样性控制生成高质量训练数据。 - 以 SFT / RL 信号、数据熵、多样性、覆盖率、自一致性增益和 recovery / turning-point 指标驱动闭环优化，使数据生成策略随训练结果自进化。	
RAPO：检索增强策略优化	2025.12 - 2026.03
导师：许嘉蓉教授	浙江大学
- 研究智能体强化学习中的探索瓶颈：纯在线策略采样容易重复相似推理路径，遗漏有价值的步骤级探索行为。 - 提出 RAPO，一个检索增强的策略优化框架，将离线步骤轨迹注入智能体采样过程，在 14 个数据集上取得平均 5.0% 的性能提升，并实现 1.2× 的训练效率提升。	
RAT：全自动环境配置	2025.12 - 2026.04
导师：杨洋教授	浙江大学
- 发现可执行环境配置是仓库级代码智能体的关键瓶颈：许多智能体可以生成看似合理的代码，却难以安装依赖、配置运行时并获得可靠的执行反馈。 - 提出 RunAnything (RAT)，一个语言无关的自动化配置流水线，相比强基线平均提升 29.6% 的环境配置成功率 (ESSR)，推动智能体更接近真实部署。	
PTCG-Bench：长程策略智能体评测	2026.02 - 2026.05
导师：杨洋教授	浙江大学
- 围绕 Pokemon Trading Card Game 构建 PTCG-Bench，在单一且生动的环境中压力测试大语言模型智能体，覆盖隐藏信息推理、长程规划、随机抽牌、规则遵循和文本数值混合决策。 - 实验表明，大语言模型智能体能够达到非平凡的游戏表现，但基于经验积累的稳定自我演化仍然困难，且测评结果对评测框架设计高度敏感，揭示了语言能力与可靠策略智能体之间的具体差距。	
TrimDG：DGNN 冗余感知加速	2024.12 - 2025.3
导师：许嘉蓉教授、杨洋教授	浙江大学 & 蚂蚁集团
- 时序图对于建模复杂真实系统非常重要，但高计算成本为动态图神经网络 (DGNN) 的实际部署带来挑战。 - 提出 TrimDG，一个通过消除静态冗余和运行时冗余来加速 DGNN 的通用框架，在多种 DGNN 上平均减少 83.80% 的运行时间。	

- PolicySim: 大语言模型社会仿真沙盘** 2024.12 - 2025.3
导师: 许嘉蓉教授、杨洋教授 浙江大学 & 复旦大学
- 研究社交媒体平台如何影响信息传播, 尤其是推荐系统等干预措施在未经预先评估时可能放大风险的问题。
 - 提出 PolicySim, 一个基于大语言模型的社会仿真沙盘, 用于在真实部署前主动评估和优化平台干预策略。
- ToP: 多样化推荐的偏好树** 2025.06 - 2026.01
导师: 许嘉蓉教授 浙江大学 & 复旦大学
- 研究多样化推荐中的数据偏差问题: 观测到的用户反馈难以反映未充分探索的偏好, 进而导致推荐同质化。
 - 提出 Tree of Preferences (ToP), 利用大语言模型的零样本推理能力和世界知识, 发现并组织未充分探索的用户偏好, 形成层次化树结构。
- 分子预训练模型训练数据提取** 2023.10 - 2024.6
导师: 许嘉蓉教授、杨洋教授 浙江大学 & 复旦大学
- 预训练模型包含大量信息; 本工作首次系统研究分子图预训练模型是否存在训练数据提取风险。
 - 实验表明, 即使攻击者只有对分子预训练模型的查询访问权限, 仍然存在显著的训练数据提取风险。
- 图神经网络高效属性推断攻击** 2023.10 - 2024.4
导师: 许嘉蓉教授 浙江大学 & 复旦大学
- 研究攻击者试图从预训练模型中提取知识或训练数据时产生的隐私泄露问题。
 - 提出一种基于模型近似技术的高效图属性推断攻击, 在真实场景中平均提升 2.7% 的攻击准确率。
- 图域适应的数据修改方法** 2023.4 - 2023.9
导师: 许嘉蓉教授、杨洋教授 浙江大学 & 复旦大学
- 识别仅依赖模型的图域适应方法的局限, 并基于泛化理论提出两个以数据为中心的原则: 对齐与重缩放。
 - 提出 GraphAlign, 一个以数据为中心的方法, 可生成规模小但迁移性强的图; 仅使用原图 1% 的数据便相比基线提升 3.38%。
- 图神经网络微调中的任务相似性度量** 2022.9 - 2023.1
导师: 许嘉蓉教授、杨洋教授 浙江大学 & 复旦大学
- 研究图预训练模型的具体适用范围, 即下游任务可以从特定预训练任务中获益到什么程度。
 - 引入任务一致性来量化预训练任务与下游任务之间的对齐程度, 并提出 Bridge-Tune 微调策略以缓解二者之间的差距。
- 隐私保护数据增强发布图预训练模型** 2022.8 - 2022.10
导师: 许嘉蓉教授 复旦大学
- 面向隐私保护的图预训练模型发布场景, 支持数据所有者公开预训练模型, 同时避免暴露隐私信息。
 - 引入两个受因果思想启发的图预训练原则: 隐私保护与泛化。
- Better with Less: 数据中心视角下的图预训练** 2021.1 - 2022.9
导师: 许嘉蓉教授、杨洋教授 浙江大学
- 通过大量实验研究预训练数据如何影响图预训练效果, 揭示“大数据诅咒”: 更多数据并不总是带来更好结果。
 - 提出 better-with-less 框架, 通过更少但精心选择的样本提升 GNN 预训练效果; 相比现有图预训练基线, 冻结设置提升 9.94%, 微调设置提升 17.83%。
- 结构感知路径聚合图神经网络** 2021.10 - 2022.1
导师: 杨洋教授 浙江大学
- 从路径级模式出发, 提升图神经网络在同质图和异质图上的泛化能力。
 - 引入由顺序保持组件和距离感知组件构成的结构感知循环单元, 用于学习邻域语义信息。

代表性奖项与荣誉

- 国家奖学金，2024。
- 优秀毕业论文，2022。
- 浙江大学竺可桢学院荣誉毕业生，2022。
- 浙江大学学年奖学金三等奖，2018 - 2021。
- 美国数学竞赛 Meritorious Winner（前 7%），2021。
- 浙江大学优秀学生标兵，2018 - 2021。
- 浙江省大学生数学竞赛二等奖，2020。

研究兴趣

大语言模型智能体、大语言模型推理与对齐、人形 VLA、LLM 基准测试、以数据为中心的 AI。

Renhong Huang

Zhejiang University, Hangzhou, China
+86-13620950268 | renh2@zju.edu.cn | renh2.github.io

EDUCATION

Zhejiang University <i>PhD, Computer Science</i> Advised by Yang Yang	Hangzhou, China 2022.9 - Current
Zhejiang University <i>B.E., Computer Science</i> GPA: 3.97/4.00	Hangzhou, China 2018.9 - 2022.6
National University of Singapore <i>Visiting Student, Computer Science</i> Courses: Machine Learning, IoT	Lower Kent Ridge Road, Singapore 2021.8 - 2021.9
Fudan University <i>Visiting Student, Computer Science</i> Advised by Jiarong Xu	Shanghai, China 2022.9 - 2023.9

PUBLICATIONS

- Renhong Huang**, Ning Tang, Jiarong Xu, Yuxuan Cao, Qingqian Tu, Sheng Guo, Bo Zheng, Yang Yang. *PolicySim: An LLM-Based Agent Social Simulation Sandbox for Proactive Policy Optimization*. WWW 2026 Oral.
- Siwei Zhang, Yun Xiong, Xi Chen, Zi'an Jia, **Renhong Huang**, Jiarong Xu, Jiawei Zhang. *RAPO: Expanding Exploration for LLM Agents via Retrieval-Augmented Policy Optimization*. KDD 2026 Oral.
- Renhong Huang**, Dongdong Hua, Yifei Sun, Sitao Ding, Hanyang Yuan, Daixin Wang, Yang Yang. *RAT: RunAnything via Fully Automated Environment Configuration*. EMNLP under review.
- Chaojian Shi*, **Renhong Huang***, Xulan Qiu, Jiawei Zhou, Yunsong Zhou. *Modular Representation Steering for Multi-Attribute LLM Alignment*. EMNLP under review.
- Dongdong Hua, Yifei Sun, **Renhong Huang**, Feng Gao, Chunping Wang, Yang Yang. *PTCG-Bench: Can LLM Agents Master Pokemon Trading Card Game?*. arXiv 2026.
- Yuxuan Wang, Yateng Tang, **Renhong Huang**, Jingwen Zhou, Siwei Zhang, Yun Xiong, Xuehao Zheng, Jiarong Xu. *A Transaction Foundation Model for Financial Risk Assessment on Online Payment Platforms*. CIKM 2026.
- Renhong Huang**, Yuxuan Cao, Yi Li, Junwei Hu, Zihua Xiong, Shuai Fang, Sheng Guo, Bo Zheng, Yang Yang. *Trimming the Fat: Redundancy-Aware Acceleration Framework for DGNNs*. AAAI 2026.
- Hanyang Yuan, Ning Tang, Tongya Zheng, Jiarong Xu, Xintong Hu, **Renhong Huang**, Shunyu Liu, Jiacong Hu, Jiawei Chen, Mingli Song. *Tree of Preferences for Diversified Recommendation*. NeurIPS 2025.
- Renhong Huang**, Jiarong Xu, Zhiming Yang, Xiang Si, Xin Jiang, Hanyang Yuan, Chunping Wang, Yang Yang. *Extracting Training Data from Molecular Pre-trained Models*. NeurIPS 2024.
- Hanyang Yuan, Jiarong Xu, **Renhong Huang**, Mingli Song, Chunping Wang, Yang Yang. *Towards More Efficient Property Inference Attacks on Graph Neural Networks*. NeurIPS 2024.
- Renhong Huang**, Jiarong Xu, Xin Jiang, Ruichuan An, Yang Yang. *Can Modifying Data Address Graph Domain Adaptation?* KDD 2024 Oral.
- Renhong Huang**, Jiarong Xu, Xin Jiang, Chenglu Pan, Zhiming Yang, Chunping Wang, Yang Yang. *Measuring Task Similarity and Its Implication in Fine-Tuning Graph Neural Networks*. AAAI 2024.
- Jiarong Xu, **Renhong Huang**, Xin Jiang, Yuxuan Cao, Carl Yang, Chunping Wang, Yang Yang. *Better with Less: A Data-Centric Perspective on Pre-Training Graph Neural Networks*. NeurIPS 2023.
- Yifei Sun, Haoran Deng, Yang Yang, Chunping Wang, Jiarong Xu, **Renhong Huang**, Linfeng Cao, Yang Wang, Lei Chen. *Beyond Homophily: Structure-aware Path Aggregation Graph Neural Network*. IJCAI 2022.
- Jiarong Xu, Zhiming Yang, Xiang Ao, **Renhong Huang**, Chenglu Pan. *Release Graph Pre-Trained Model via Privacy-Preserving Data Augmentation*.
- Zhengzhe Fu, Renhong Huang, Rongjie Jiang, Guandong Sun, Feng Zhao, Yang Yang. *From Bag-of-Documents to Structure-Aware Synthesis: Resolving Conflicts in RAG*. KDD under review.

RAPO: Retrieval-Augmented Policy Optimization for LLM Agents.

2025.12 - 2026.03

*Supervisor: Prof. Jiarong Xu**Zhejiang University*

- Studied the exploration bottleneck in agentic reinforcement learning, where pure on-policy rollouts often repeat similar reasoning paths and miss useful step-level exploratory behaviors.
- Developed RAPO, a retrieval-augmented policy optimization framework that injects off-policy step traces into agent rollouts, achieving a 5.0% average performance gain across 14 datasets and 1.2× faster training efficiency.

RAT: Fully Automated Environment Configuration for LLM Agents.

2025.12 - 2026.04

*Supervisor: Prof. Yang Yang**Zhejiang University*

- Identified executable environment setup as bottleneck for repository-level code agents, since many agents can write plausible code but fail to install dependencies, configure runtimes, and obtain reliable execution feedback.
- Proposed RunAnything (RAT), a language-agnostic automated configuration pipeline that improves Environment Setup Success Rate (ESSR) by 29.6% on average over strong baselines, moving agents closer to real deployment.

PTCG-Bench: Long-Horizon Strategic Benchmarking for LLM Agents.

2026.02 - 2026.05

*Supervisor: Prof. Yang Yang**Zhejiang University*

- Built PTCG-Bench around Pokemon Trading Card Game to stress-test LLM agents in a single vivid environment requiring hidden-information reasoning, long-horizon planning, stochastic card draws, rule following, and text-numeric decision making.
- Showed that LLM agents can reach non-trivial gameplay performance, but stable self-evolution from accumulated experience remains difficult and measured performance is highly sensitive to harness design, highlighting a concrete gap between language competence and reliable strategic agency.

Trimming the Fat: Redundancy-Aware Acceleration Framework for DGNNs.

2024.12 - 2025.3

*Supervisor: Prof. Jiarong Xu and Prof. Yang Yang**Zhejiang University & Ant Group*

- Temporal graphs are essential for modeling complex real-world systems, but the high computational cost poses practical challenges for deploying dynamic graph neural networks (DGNNs).
- Proposed TrimDG, a general framework that accelerates DGNNs by eliminating both static and runtime redundancy, reducing runtime by an average of 83.80% across diverse DGNNs.

LLM-Agent Social Simulation Sandbox for Empowering Intervention.

2024.12 - 2025.3

*Supervisor: Prof. Jiarong Xu and Prof. Yang Yang**Zhejiang University & Fudan University*

- Studied how social media platforms influence information propagation, where interventions such as recommendation systems may amplify risks if deployed without prior assessment.
- Proposed PolicySim, an LLM-based social simulation sandbox for proactively evaluating and optimizing platform intervention policies before real-world deployment.

Tree of Preferences for Diversified Recommendation.

2025.06 - 2026.01

*Supervisor: Prof. Jiarong Xu**Zhejiang University & Fudan University*

- Diversified recommendation often suffers from data bias, where observed user feedback fails to reflect underexplored preferences, leading to recommendation homogeneity.
- Proposed Tree of Preferences (ToP), a framework that leverages LLMs' zero-shot inference and world knowledge to uncover and organize underexplored user preferences into a hierarchical tree structure.

Extracting Training Data from Molecular Pre-trained Models.

2023.10 - 2024.6

*Supervisor: Prof. Jiarong Xu and Prof. Yang Yang**Zhejiang University & Fudan University*

- Pre-trained models contain a large amount of information. This work provides the first investigation into whether molecular graph pre-trained models carry data extraction risks.
- Experiments demonstrate that even with only query access to molecular pre-trained models, there is a considerable risk of extracting training data.

Towards More Efficient Property Inference Attacks on GNN.

2023.10 - 2024.4

*Supervisor: Prof. Jiarong Xu**Zhejiang University & Fudan University*

- Pre-trained models contain a large amount of information. Privacy leakage issues need to be considered when attackers attempt to extract knowledge (training datasets) from pre-trained models.
- Proposed an efficient graph property inference attack using model approximation techniques, achieving an average 2.7% improvement in attack accuracy across real-world settings.

Can Modifying Data Address Graph Domain Adaptation?

2023.4 - 2023.9

*Supervisor: Prof. Jiarong Xu and Prof. Yang Yang**Zhejiang University & Fudan University*

- Identify limitations of model-only graph domain adaptation and propose two data-centric principles (alignment & rescaling) based on generalization theory.
- Proposed GraphAlign, a data-centric method that generates a small but transferable graph, outperforming baselines by 3.38% using just 1% of the original graph.

- Measuring Task Similarity in Fine-Tuning Graph Neural Networks** 2022.9 - 2023.1
Supervisor: Prof. Jiarong Xu and Prof. Yang Yang Zhejiang University & Fudan University
- Studies the specific application scope of graph pre-trained models, i.e., the extent to which downstream tasks can benefit from specific pre-training tasks.
 - Introduced task consistency to quantify the alignment between pre-training and downstream tasks, and proposed Bridge-Tune, a fine-tuning strategy that mitigates their gaps.
- Release Graph Pre-trained Model via Privacy-Preserving Data Augmentation.** 2022.8 - 2022.10
Supervisor: Prof. Jiarong Xu Fudan University
- Target a privacy-preserving graph pre-training model to facilitate the knowledge sharing environment, which allows data owners to disclose their pre-trained models without exposing privacy.
 - Introduced two causality-inspired principles for graph pre-training: privacy preservation and generalization.
- Better with Less: A Data-Centric Perspective on Pre-Training Graph Neural Networks** 2021.1 - 2022.9
Supervisor: Prof. Jiarong Xu and Prof. Yang Yang Zhejiang University
- Conduct extensive experiments to study how pre-training data affects graph pre-training performance, revealing curse of big data where more data does not always yield better results.
 - Proposed a better-with-less framework that uses fewer but carefully selected samples to boost GNN pre-training. Our method surpasses existing graph pre-training baselines by 9.94% (freezing) and 17.83% (fine-tuning).
- Beyond Homophily: Structure-aware Path Aggregation Graph Neural Network** 2021.10 - 2022.1
Supervisor: Prof. Yang Yang Zhejiang University
- Shed light on the path level patterns in graphs to generalize GNNs for both homophily and heterophily graphs.
 - Introduced a structure-aware recurrent cell consisting of order-preserving and distance-aware components to learn the semantic information of neighborhoods.

SELECTED AWARDS AND HONORS

National Scholarship, 2024.
 Outstanding Graduate Thesis, 2022.
 Award of Honor for Graduate at Chu Kochen Honors College of Zhejiang University, 2022.
 Third Prize, Zhejiang University's Academic Year Scholarship, 2018 - 2021.
 Meritorious Winner for American Mathematical Competition (top 7%), 2021.
 Outstanding Academic Model, Zhejiang University, 2018-2021.
 Second Prize, Province Mathematics Competition, 2020.

RESEARCH INTERESTS

LLM Agents, LLM Reasoning and Alignment, Humanoid VLA, Environment-Grounded Agents, Data-centric AI.