Yanchao Sun

Email : ycsun1531@gmail.com

Research Focus

Large-scale foundation model training across diverse modalities.
Expertise in LLM reasoning, reinforcement learning, and data-centric model improvement.
Trustworthiness and adversarial robustness of deep neural networks.

Work and Research Experience

- **Apple, Inc.** New York, U.S.
  Machine Learning Research Engineer *Feb 2024 – Present*
  - **Building Apple foundation model**
    - *Reasoning*: core contributor to reasoning model development with knowledge distillation and RLVR.
    - *Post-training*: responsible for RLHF training of various-sized models for on-devide and server models.
    - *Pre-training*: leading recipe design for reasoning capabilities in pretraining and continued pretraining.
    - *Data*: proposed a large-scale data retrieval and rewrite pipeline, leading to 30% math performance boost; designed RLHF data selection pipeline, leading to 6% improvement on key benchmarks.
    - *Agentic*: main contributor to coding and reasoning evaluation on agentic LLM in MMAU benchmark.

- **JPMorgan Chase & Co.** New York, U.S.
  AI Research Scientist *Jun 2023 – Feb 2024*
  - **Applied research on LLM agents and foundation models.**
    - Advanced LLM agents with multi-task offline reinforcement learning, leading to COLM Publication.
    - Pioneered foundation models for financial data.

- **University of Maryland, College Park** College Park, U.S.
  Graduate Assistant *Sep 2018 – May 2023*
  - **Robust and adaptable reinforcement learning**
    - Conducted foundational research on robustness, transferability, and adaptability of RL agents.
    - Published 20+ papers in leading machine learning venues (e.g., ICLR, NeurIPS, ICML).

- **Microsoft** Redmond, U.S.
  Research Intern *Jun 2022 – Aug 2022*
  - **Large-scale pretraining for multi-task visual reinforcement learning.**
    Proposed a control-transformer architecture, and a self-supervised pretraining framework that works for various downstream continuous control tasks with visual observations. ICLR Spotlight.

- **JPMorgan Chase & Co.** New York, U.S.
  AI Research Intern *Jun 2021 – Aug 2021*
  - **Robustifying agents in a communicative multi-agent system.**
    Proposed an adversarially robust multi-agent training algorithm against the emergence of adversarial communication. ICLR Paper.

- **Unity Technologies** San Francisco, U.S.
  Machine Learning Research Intern *May 2020 – Aug 2020*
  - **Cross-domain knowledge transfer for reinforcement learning.**
    Designed the first algorithm that transfers a learned policy to a new task with different observation space without prior knowledge, contributed to the ML-Agents toolkit. ICLR Paper.

Education

- **University of Maryland, College Park** Maryland, U.S.A.
  Ph.D. in Computer Science. GPA: 3.97/4. Advisor: Furong Huang. *Sep 2018 – May 2023*

- **Sichuan University** Chengdu, China
  B.E. in Computer Science and Technology. GPA: 95/100. Rank: 1/380. *Sep 2014 – Jun 2018*

Selected Publications

Foundation Models

1. **Yanchao Sun**, Shuang Ma, Ratnesh Madaan, Rogerio Bonatti, Furong Huang, and Ashish Kapoor. "SMART: Self-supervised Multi-task pretrAining with contRol Transformers". ICLR 2023 (***Spotlight***).

2. Yao Wei, **Yanchao Sun**, Ruijie Zheng, Sai Vemprala, Rogerio Bonatti, Shuhang Chen, Ratnesh Madaan, Zhongjie Ba, Ashish Kapoor and Shuang Ma. "Is Imitation All You Need? Generalized Decision-Making with Dual-Phase Training". ICCV 2023.

3. Aiwei Liu, Haoping Bai, Zhiyun Lu, **Yanchao Sun**, et al. "TIS-DPO: Token-level Importance Sampling for Direct Preference Optimization With Estimated Weights." ICLR 2025.

4. Guoli Yin*, Haoping Bai*, Shuang Ma*, Feng Nan, **Yanchao Sun**, et al. "MMAU: A Holistic Benchmark of Agent Capabilities Across Diverse Domains." NAACL 2025.

5. Yuchen Xiao*, **Yanchao Sun***, Mengda Xu, Udari Madhushani, Jared Vann, Deepeka Garg and Sumitra Ganesh. "O3D: Offline Data-driven Discovery and Distillation for Sequential Decision-Making with Large Language Models". COLM 2024. (*Equal Contribution.)

6. Yuancheng Xu, Jiarui Yao, Manli Shu, **Yanchao Sun**, Ning Yu, Zichu Wu, Tom Goldstein and Furong Huang. "Shadowcast: Stealthy Data Poisoning Attacks Against Vision-Language Models". NeurIPS 2024.

Robust Reinforcement Learning

1. **Yanchao Sun**, Ruijie Zheng, Yongyuan Liang, and Furong Huang. "Who Is the Strongest Enemy? Towards Optimal and Efficient Evasion Attacks in Deep RL". ICLR 2022. (***Best Paper Award*** at the NeurIPS 2021 SafeRL Workshop.)

2. **Yanchao Sun**, Ruijie Zheng, Parisa Hassanzadeh, Yongyuan Liang, Soheil Feizi, Sumitra Ganesh and Furong Huang. "Certifiably Robust Multi-Agent Reinforcement Learning against Adversarial Communication". ICLR 2023.

3. Yongyuan Liang*, **Yanchao Sun***, Ruijie Zheng, and Furong Huang. "Efficient Adversarial Training without Attacking: Worst-Case-Aware Robust Reinforcement Learning". NeurIPS 2022. (*Equal Contribution.)

4. **Yanchao Sun**, Da Huo, and Furong Huang. "Vulnerability-Aware Poisoning Mechanism for Online RL with Unknown Dynamics". ICLR 2021.

5. Xiangyu Liu, Chenghao Deng, **Yanchao Sun**, Yongyuan Liang and Furong Huang. "Beyond Worst-case Attacks: Robust RL with Adaptive Defense via Non-dominated Policies". ICLR 2024 (***Spotlight)***.

Transfer Reinforcement Learning

1. **Yanchao Sun**, Ruijie Zheng, Xiyao Wang, Andrew Cohen, and Furong Huang. "Transfer RL across Observation Feature Spaces via Model-Based Regularization" ICLR 2022.

2. **Yanchao Sun**, Xiangyu Yin, and Furong Huang. "TempLe: Learning Template of Transitions for Sample Efficient Multi-task RL". AAAI 2021.

3. **Yanchao Sun** and Furong Huang. "Can Agents Learn by Analogy? An Inferable Model for PAC Reinforcement Learning". AAMAS 2020.

Full publication list: Google Scholar Page.

Honors and Awards

- **Outstanding Research Assistant Award** (top 2%), University of Maryland, College Park, 2022
- **Best Paper Award** at the NeurIPS SafeRL Workshop, 2021
- Dean's Fellowship, University of Maryland, College Park, 2018
- Special Award of Wang Wen Guo Scholarship, Wuyuzhang Honors College, 2016
- National Endeavor Scholarship, China, 2016
- The **1st Prize** of Blue Bridge Cup National C/C++ Programming Contest, Sichuan Province, 2016
- National Scholarship, China, 2015
- The **1st Prize** of The Seventh Chinese Mathematics Competitions, Sichuan Province, 2015

Professional Services

- Reviewer of International Conference on Machine Learning (ICML), 2020 to 2025
- Reviewer of International Conference on Learning Representations (ICLR), 2021 to 2025
- Reviewer of Advances in Neural Information Processing Systems (NeurIPS), 2021 to 2025
- Program Committee of the GenPlan Workshop at AAAI 2025
- Co-organizer of the PerDream Workshop at ICCV 2023
- Co-organizer of the 1st Reincarnating RL Workshop at ICLR 2023
- Program Committee of NeurIPS 2022 Deep RL Workshop

Invited Talks

- Invited talk at Naver Labs Europe. 2025.
- Invited talk at Scaled Foundation. 2025.
- Invited talk at the Robotics Session at the 18th Coordinated Science Laboratory Student Conference (CSLSC), University of Illinois at Urbana-Champaign. 2023.
- Invited talk at the Microsoft Research NYC Seminar. 2023.
- Talk at the Machine Learning Seminar Series, University of Maryland. 2019.