Yanchao Sun

Email : ycs@umd.edu
Phone: +1 (240) 413-8873

Education

- **University of Maryland, College Park** Maryland, U.S.A.
  Ph.D. in Computer Science; GPA: 3.966/4 *Sep 2018 – Present*
- **Sichuan University** Chengdu, China
  B.S. in Computer Science and Technology; GPA: 3.9/4 (95/100); Rank: 1/380 *Sep. 2014 – Jun 2018*

Research Interests

- **Knowledge transfer in reinforcement learning** (in-domain and cross-domain transfer)
- **Robustness of reinforcement learning** agents against adversarial attacks (training-time and test-time robustness)
- **Representation learning and contrastive learning** driven by theoretical understandings

Publications

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, Xiyao Wang, Andrew Cohen, and Furong Huang. "Transfer RL across Observation Feature Spaces via Model-Based Regularization". ICLR 2022.
3. **Yanchao Sun**, Da Huo, and Furong Huang. "Vulnerability-Aware Poisoning Mechanism for Online RL with Unknown Dynamics". ICLR 2021.
4. **Yanchao Sun**, Xiangyu Yin, and Furong Huang. "TempLe: Learning Template of Transitions for Sample Efficient Multi-task RL". AAAI 2021.
5. **Yanchao Sun** and Furong Huang. "Can Agents Learn by Analogy? An Inferable Model for PAC Reinforcement Learning". AAMAS 2020.
6. Jingling Li, **Yanchao Sun**, Ziyin Liu, Taiji Suzuki and Furong Huang. "Understanding Generalization in Deep Learning via Tensor Methods". AISTATS 2020.
7. **Yanchao Sun**, Cong Qian, Ning Yang and Philip S. Yu. "Collaborative Inference of Coexisting Information Diffusions". ICDM 2017.

Preprints

1. **Yanchao Sun**, Ruijie Zheng, Parisa Hassanzadeh, Yongyuan Liang, Soheil Feizi, Sumitra Ganesh and Furong Huang. "Provably Robust Multi-agent Reinforcement Learning against Adversarial Communication". Under review.
2. Yongyuan Liang*, **Yanchao Sun***, Ruijie Zheng, and Furong Huang. "Efficiently Improving the Robustness of RL Agents against Strongest Adversaries". (*Equal contribution.) Under review. (Oral presentation at the NeurIPS 2021 SafeRL Workshop.)

Research Experience

- **Research Assistant** University of Maryland, College Park, U.S.A.
  Advisor: Prof. Furong Huang *Jun 2019 – Present*
  - **Adversarial Reinforcement Learning**
    - proposed an efficient and theoretically optimal evasion attack (test-time attack) algorithm that achieves state-of-the-art attacking performance against deep RL agents with small attack budgets.
    - formulated a principled lower bound of an RL agent's cumulative reward under any adversarial attacks, based on which we present an efficient adversarial training method that outperforms existing robust training approaches.
    - proposed the first poisoning (training-time attack) algorithm against deep policy-based RL methods without prior knowledge of the environment, introduced a novel metric to measure the training-time vulnerability of RL agents.

  - **Sample Efficient Multi-task Reinforcement Learning**
    proposed the first PAC-MDP method for multi-task reinforcement learning that could be applied to tasks with varying state/action space and achieves state-of-the-art sample complexity under mild assumptions.
  - **Provable Sample Efficient RL Algorithms**
    introduced a new reinforcement learning algorithm with a novel exploration strategy and the ability to infer unknown dynamics via spectral methods, reducing both sample and computational complexity of existing model-based methods.
  - **Understanding Contrastive Learning via Information Theory**
    established a theoretical explanation for “why and how contrastive learning generates good representations”, and proposed a new data augmentation method that improves the representation quality.
  - **Generalization Theory for Deep Learning**
    proposed a highly compressible neural network architecture and derived state-of-the-art generalization bounds for fully connected networks, convolutional neural networks, and networks with skip connections.

- **AI Research Summer Associate** — JPMorgan Chase & Co., New York (remote), U.S.A.
  Supervisor: Dr. Sumitra Ganesh — *Jun 2021 – Aug 2021*
  - **Robustifying Agents in a Communicative Multi-agent System.**
    studied the emergence of adversarial communication in a multi-agent system and how to make agents robust against adversarial communication with a focus on defensive information sharing and selective information usage.
- **Machine Learning Research Intern** — Unity Technologies, San Francisco (remote), U.S.A.
  Mentor: Dr. Andrew Cohen — *May 2020 – Aug 2020*
  - **Cross-domain Transfer RL with Model Regularizers.**
    designed an algorithm that utilizes model-based regularizers to transfer a learned policy to a new task with different observation space, contributed to the ML-Agents toolkit.
- **Research Assistant Intern** — Sichuan University, China
  Advisor: Prof. Ning Yang — *Apr 2016 – Jun 2018*
  - **Collaborative Inference of Coexisting Information Diffusions.**
    built a model that accurately recovers and predicts information diffusion trails in coexisting information diffusion networks (e.g. on social networks), by using context-aware tensor decomposition with heterogeneous constraints.
- **Independent Research** — Sichuan University, China
  Advisor: Prof. Yu Chen — *Mar 2016 – Nov 2016*
  - **Modified Linear Time Selection Algorithm.**
    improved the selection step of the classic linear time selection algorithm to make it faster.

Honors and Awards

- Dean’s Fellowship, University of Maryland, College Park — *Sep 2018*
- Outstanding Graduates of Sichuan University — *Nov 2017*
- Special Award of Wang Wen Guo Scholarship, Wuyuzhang Honors College — *Nov 2016*
- Excellent Student Cadre of Sichuan University — *Nov 2016*
- National Endeavor Scholarship, China — *Nov 2016*
- The **1st Prize** of Blue Bridge Cup National C/C++ Programming Contest, Sichuan Province — *Mar 2016*
- National Scholarship, China — *Nov 2015*
- Excellent Student of Sichuan University — *Nov 2015*
- The **1st Prize** of The Seventh Chinese Mathematics Competitions, Sichuan Province — *Nov 2015*

Skills

- **Programming Languages**: Python, C/C++, Java, Javascript, PHP, HTML/CSS, Matlab, Scala, SQL