

YIHUA ZHANG

Ph.D. Student in Computer Science

📞 (+1) 517-980-3880 ✉️ zhan1908@msu.edu 🌐 www.yihua-zhang.com 🔄 NormalUhr 📄 Yihua Zhang

PERSONAL INFORMATION

I am a third-year Ph.D. student in computer science at Michigan State University, where I am advised by **Dr. Sijia Liu**. I am interested in the optimization foundation of **trustworthy, reliable, and scalable machine learning**, including the optimization theories to improve the robustness, alignment, fairness, and scalability of current machine learning algorithms.

EDUCATION

Doctor of Computer Science <i>Michigan State University, East Lansing, USA</i> Advisor: Dr. Sijia Liu OPTML Lab	01 2022 — Present
Bachelor of Engineering <i>Huazhong University of Science and Technology, Wuhan, China</i>	09 2015 — 06 2019

AWARDS

Scholarly Awards

• CVPR Outstanding Reviewer	2023
• Best Paper Runner-up Award of UAI 2022	2022
• NeurIPS Top Reviewer	2022
• NeurIPS Top Reviewer	2023
• UAI Student Scholarship	2022

Conference Scholar Award

• NeurIPS Scholar Award	2022, 2023
• AAAI 2023 Travel Award	2023
• Travel Grant Award of ICML 2022	2022

PUBLICATIONS

Survey Paper

- [1] **Y. Zhang**, P. Khanduri, I. Tsaknakis, Y. Zhang, M. Hong, S. Liu "An Introduction to Bi-level Optimization: Foundations and Applications in Signal Processing and Machine Learning", Signal Processing Magazine, [PDF].

Conference Papers

(* represents equal contributions)

- [2] **Y. Zhang**, Y. Zhang, A. Chen, J. Jia, J. Liu, G. Liu, S. Chang, M. Hong, S. Liu "Selectivity Drives Productivity: Efficient Dataset Pruning for Enhanced Transfer Learning", 37th Conference on Neural Information Processing Systems (NeurIPS'23), [PDF], [Code].
- [3] **Y. Zhang**, R. Cai, T. Chen, G. Zhang, P. Chen, H. Zhang, S. Chang, W. Zhang, S. Liu "Robust Mixture-of-Expert Training for Convolutional Neural Networks", International Conference on Computer Vision 2023 (ICCV'23 - Oral), [PDF], [Code], [Poster].
- [4] **Y. Zhang**, P. Sharma, P. Ram, M. Hong, K. R. Varshney, S. Liu "What Is Missing in IRM Training and Evaluation? Challenges and Solutions", 11th International Conference on Learning Representations (ICLR'23), [PDF], [Poster].
- [5] C. Fan, J. Liu, **Y. Zhang**, E. Wong, D. Wei, S. Liu "Salun : Empowering Machine Unlearning via Gradient-based Weight Saliency in Both Image Classification and Generation", 12th International Conference on Learning Representations (ICLR'24), [PDF], [Code].
- [6] A. Chen, Y. Zhang, J. Jia, J. Diffenderfer, J. Liu, K. Parasyris, **Y. Zhang**, Z. Zhang, B. Kailkhura, S. Liu "DeepZero: Scaling up Zeroth-Order Optimization for Deep Model Training", 12th International Conference on Learning Representations (ICLR'24), [PDF], [Code].
- [7] B. Hou, **Y. Zhang**, J. Jia, G. Zhang, Y. Zhang, S. Liu, S. Chang "TextGrad: Advancing Robustness Evaluation in NLP by Gradient-Driven Optimization", 11th International Conference on Learning Representations (ICLR'23), [PDF], [Code].
- [8] P. Khanduri, I. Tsaknakis, **Y. Zhang**, J. Liu, S. Liu, J. Zhang, M. Hong "Linearly Constrained Bilevel Optimization: A Smoothed Implicit Gradient Approach", 40th International Conference on Machine Learning (ICML'23), [PDF].
- [9] **Y. Zhang***, Y. Yao*, P. Ram, P. Zhao, T. Chen, M. Hong, Y. Wang, S. Liu, "Advancing Model Pruning via Bi-level Optimization", 36th Conference on Neural Information Processing Systems (NeurIPS'22), [PDF], [Code], [Poster], [Project Website].

- [10] **Y. Zhang***, G. Zhang*, Y. Zhang, W. Fan, Q. Li, S. Liu, S. Chang, "[Fairness Reprogramming](#)", 36th Conference on Neural Information Processing Systems (NeurIPS'22), [PDF], [Code], [Poster], [Project Website].
- [11] G. Zhang*, S. Lu*, **Y. Zhang**, X. Chen, P. Chen, Q. Fan, L. Martie, M. Hong, S. Liu, "[Distributed Adversarial Training to Robustify Deep Neural Networks at Scale](#)", 38th Conference on Uncertainty in Artificial Intelligence (UAI'22 - *Oral, Best Paper Runner-up Award*), [PDF], [Code], [Poster], [Slides], [Award].
- [12] **Y. Zhang***, G. Zhang*, P. Khanduri, M. Hong, S. Chang, S. Liu, "[Fast-BAT: Revisiting and Advancing Fast Adversarial Training through the Lens of Bi-level Optimization](#)", 39th International Conference on Machine Learning (ICML'22), [PDF], [Code], [Poster], [Slides], [Talk].
- [13] T. Chen*, Z. Zhang*, **Y. Zhang***, S. Chang, S. Liu, Z. Wang "[Quarantine: Sparsity Can Uncover the Trojan Attack Trigger for Free](#)", Computer Vision and Pattern Recognition Conference 2022 (CVPR'22), [PDF], [Code], [Poster], [Project Website].

Preprint Paper

- [1] Y. Zhang, J. Jia, X. Chen, A. Chen, **Y. Zhang**, J. Liu, K. Ding, S. Liu "[To Generate or Not? Safety-Driven Unlearned Diffusion Models Are Still Easy To Generate Unsafe Images ... For Now](#)", [PDF].

TUTORIALS/INVITED TALKS

- **02/2023**: "Bi-level Optimization in Machine Learning: Foundations and Applications", **AAAI 2023 (Tutorial)**
- **11/2022**: "Invariant Risk Minimization through Bi-level Optimization and Beyond", **Invited Talk in UMN**
- **10/2022**: "Revisiting and Advancing Fast Adversarial Training through the Lens of Bi-level Optimization", **INFORMS Annual Meeting (2022)**
- **04/2022**: "Adversarial Training via Bi-level Optimization", **Invited Talk in UCSB**.

PROFESSIONAL ACTIVITIES

- **Volunteer**: AAAI'23, ICLR'23
- **Reviewer**: NeurIPS'22/23, AISTATS'23, ICLR'23, ICASSP'23, ICCV'23, CVPR'23, TMRL
- **Student Chair** for the ICML Workshop AdvML: New Frontiers in Adversarial Machine Learning in 2022 and 2023.