

# Yuzheng Hu

✉ YH46@ILLINOIS.EDU

## EDUCATION

### University of Illinois at Urbana-Champaign

*Ph.D. in Computer Science*

Urbana, IL, USA

Aug. 2021 –

- GPA: 4.0/4.0    Advisor: Prof. Han Zhao

### Peking University

*B.S. in Mathematics (Math and Applied Math)*

Beijing, China

Sep. 2017 – Jul. 2021





- Major GPA: 3.8/4.0 (89.5/100)    TOEFL: 114    GRE: 160+170



## RESEARCH INTERESTS

**Data-centric machine learning**, with a focus on *data attribution* and *data privacy*. I'm also broadly interested in core machine learning problems.

## PUBLICATIONS

★ stands for equal contribution or alphabetical order

- [P1] Most Influential Subset Selection: Challenges, Promises, and Beyond   
**Yuzheng Hu**, Pingbang Hu, Han Zhao, Jiaqi Ma  
*The 38th Annual Conference on Neural Information Processing Systems (NeurIPS 2024)*
- [P2] Localize-and-Stitch: Efficient Model Merging via Sparse Task Arithmetic   
Yifei He, **Yuzheng Hu**, Yong Lin, Tong Zhang, Han Zhao  
*Transactions on Machine Learning Research (TMLR 2024)*
- [P3] SoK: Privacy-Preserving Data Synthesis    
**Yuzheng Hu**<sup>\*</sup>, Fan Wu<sup>\*</sup>, Qinbin Li, Yunhui Long, Gonzalo Munilla Garrido, Chang Ge, Bolin Ding, David Forsyth, Bo Li, Dawn Song  
*The 45th IEEE Symposium on Security and Privacy (S&P 2024)*
- [P4] HPL-ViT: A Unified Perception Framework for Heterogeneous Parallel LiDARs in V2V   
Yuhang Liu, Boyi Sun, Yuke Li, **Yuzheng Hu**, Fei-Yue Wang  
*The 41th IEEE International Conference on Robotics and Automation (ICRA 2024)*
- [P5] Revisiting Scalarization in Multi-Task Learning: A Theoretical Perspective   
**Yuzheng Hu**, Ruicheng Xian, Qilong Wu, Qiuling Fan, Lang Yin, Han Zhao  
*The 37th Annual Conference on Neural Information Processing Systems (NeurIPS 2023)*
- [P6] Understanding the Impact of Adversarial Robustness on Accuracy Disparity    
**Yuzheng Hu**, Fan Wu, Hongyang Zhang, Han Zhao  
*The 40th International Conference on Machine Learning (ICML 2023)*
- [P7] Actor-critic is implicitly biased towards high entropy optimal policies   
**Yuzheng Hu**<sup>\*</sup>, Ziwei Ji<sup>\*</sup>, Matus Telgarsky<sup>\*</sup>  
*The 10th International Conference on Learning Representations (ICLR 2022)*
- [P8] Towards Understanding the Data Dependency of Mixup-style Training   
Muthu Chidambaram, Xiang Wang, **Yuzheng Hu**, Chenwei Wu, Rong Ge  
*The 10th International Conference on Learning Representations (ICLR 2022, Spotlight)*
- [P9] Don't Waste Your Bits! Squeeze Activations and Gradients for Deep Neural Networks via TinyScript   
Fangcheng Fu, **Yuzheng Hu**, Yihan He, Jiawei Jiang, Yingxia Shao, Ce Zhang, Bin Cui  
*The 37th International Conference on Machine Learning (ICML 2020)*

MANUSCRIPTS	[M1] Empirical Privacy Variance <b>Yuzheng Hu*</b> , Fan Wu*, Ruicheng Xian, Yuhang Liu, Lydia Zakynthinou, Pritish Kamath, Chiyuan Zhang, David Forsyth	
	[M2] An Improved Autoregressive Evaluation Paradigm for Large Language Models Jipeng Zhang, Rui Pan, <b>Yuzheng Hu</b> , Kashun Shum, Guanyu Yao, Xiang Liu, Renjie Pi, Hanze Dong, Shizhe Diao, Yong Lin, Han Zhao, Tong Zhang	
	[M3] Is Vertical Logistic Regression Privacy-Preserving? A Comprehensive Privacy Analysis and Beyond  <b>Yuzheng Hu</b> , Tianle Cai, Jinyong Shan, Shange Tang, Chaochao Cai, Ethan Song, Bo Li, Dawn Song	
INTERNSHIP EXPERIENCE	<b>Jane Street Group, LLC</b> <i>Quantitative Trading Intern</i> <ul style="list-style-type: none"> <li>Ranked 2nd (1st among all interns) in the Tenth Annual Figgie World Championships</li> <li>Conducted data projects on options and equities</li> </ul>	New York, NY, US May. 2024 – July. 2024
	<b>Damo Academy, Alibaba Group (U.S.) Inc.</b> <i>Research Intern, Mentor: Dr. Bolin Ding</i> <ul style="list-style-type: none"> <li>Worked on the intersection of privacy and law</li> <li>Wrote a systematization of knowledge paper on privacy-preserving data synthesis (P3)</li> </ul>	Bellevue, WA, US May. 2022 – Aug. 2022
	<b>Beijing Sudo Technology Co., Ltd.</b> <i>Student Researcher, Advisor: Prof. Dawn Song</i> <ul style="list-style-type: none"> <li>Analyzed the privacy risks and countermeasures in vertical logistic regression (M2)</li> </ul>	Beijing, China Jun. 2021 – Aug. 2021
	<b>Baidu Research (Big Data Lab)</b> <i>Research Intern, Mentor: Dr. Dejing Dou</i>	Beijing, China Dec. 2019 – Feb. 2020
	<b>Simons Institute for the Theory of Computing</b> <i>Visiting Graduate Student</i> <ul style="list-style-type: none"> <li>Visiting program: <i>Modern Paradigms in Generalization</i> </li> <li>Ongoing projects on data attribution and differential privacy</li> </ul>	Berkeley, CA, US Aug. 2024 – Dec. 2024
RESEARCH EXPERIENCE	<b>University of Illinois at Urbana-Champaign</b> <i>Graduate Research Assistant, Advisor: Prof. Han Zhao</i> <ul style="list-style-type: none"> <li>Analyzed the strengths and limitations of a large class of greedy heuristics in MISS (P1)</li> <li>Uncovered the representational weakness of linear scalarization in multi-task learning (P5)</li> <li>Analyzed the trade-off between adversarial robustness and accuracy parity (P6)</li> </ul>	Urbana, IL, US Feb. 2022 – now
	<b>University of Illinois at Urbana-Champaign</b> <i>Graduate Research Assistant, Advisor: Prof. Matus Telgarsky</i> <ul style="list-style-type: none"> <li>Proved that actor-critic converges to high entropy optimal policy without explicit regularization (P7)</li> </ul>	Urbana, IL, US Aug. 2021 – Dec. 2021
	<b>Duke University</b> <i>Undergraduate Research Assistant, Advisor: Prof. Rong Ge</i> <ul style="list-style-type: none"> <li>Demonstrated that the effectiveness of mixup is highly dependent on the training data (P8)</li> </ul>	Remote Jun. 2020 – Feb. 2021
	<b>School of Intelligence Science and Technology, Peking University</b> <i>Undergraduate Research Assistant, Advisor: Prof. Liwei Wang</i>	Beijing, China Aug. 2019 – Jun. 2020

- Identified two non-local properties of the loss landscape of neural networks

**School of Computer Science, Peking University**  
*Undergraduate Research Assistant, Advisor: Prof. Bin Cui*

Beijing, China  
Aug. 2018 – Aug. 2019

- Introduced a distribution-aware, non-uniform quantization algorithm for multilayer perceptrons (P9)

TEACHING EXPERIENCE	UIUC CS 591 – Machine Learning Reading Group	Spring 2024, Fall 2024
	UIUC CS 598 – Transfer Learning	Spring 2023
	UIUC CS 498 – Trustworthy Machine Learning	Fall 2022
SERVICES	Student Co-Organizer of the Machine Learning Seminar at UIUC 🌐	2024
	Reviewer for NeurIPS (2020, 2022-2024), ICML (2023,2024), ICLR (2024,2025), AISTATS (2024)	
HONORS AND AWARDS	IEEE S&P Student Travel Grants Award	2024
	NeurIPS 2023 Scholar Award & Top Reviewer 🌐	2023
	Saburo Muroga Endowed Fellowship, UIUC	2021-2022
	Exceptional Award for Academic Innovation (Top 1% in Peking University)	2020
	Elite Undergraduate Training Program of Applied Math (Top 15% in SMS) 🌐	2019-2021
	Candidates Team Member, 58th International Mathematical Olympiad (IMO)	2017
	Gold Medal, 32th China Mathematical Olympiad (CMO) (Top 60 in China)	2016
SKILLS	<div> <div>Programming</div> <div>Language</div> </div> <div> Python, MATLAB, <math>\text{\LaTeX}</math>, Markdown  English, Chinese </div>	