Xinyun Chen

Curriculum Vitae

Education

2017/08-Present **Ph.D., Computer Science**, *University of California, Berkeley, USA*.
Advisor: Prof. Dawn Song

2013/09-2017/06 **B.Eng., Computer Science and Technology**, *Shanghai Jiao Tong University, China*.
ACM Honored Class (an elite training program of computer science in China)
GPA Ranking: **1/30**

Honors and Awards

2021 **Rising Stars in Machine Learning**.
2021 **Rising Stars in EECS**.
2021 **Outstanding Reviewer Award**, *Top 8% reviewers in NeurIPS 2021*.
2020 **Facebook Fellowship**, *Machine Learning*.
2020 **Rising Stars in EECS**.
2020 **Outstanding Reviewer Award**, *Top 10% reviewers in NeurIPS 2020*.
2017 **Departmental Fellowship of EECS**, *UC Berkeley*.
2017 **The Prize of Excellent Bachelor Thesis**, *top* 1% *in Shanghai Jiao Tong University*.
2017 **Outstanding Graduate of Shanghai Jiao Tong University**.
2012 **Gold Medal**, *Asia-Pacific Informatics Olympiad in China District*.
2012 **Silver Medal**, *Chinese Team Selection Contest*.

Research Experience

2021/05-08 **Research Intern (remote)**, *DeepMind, London, UK*.

Mentor: Yujia Li

Deep learning for program synthesis

2020/05-08 **Research Intern (remote)**, *Google Brain, Mountain View, CA, USA*.

Mentors: Denny Zhou, Rishabh Singh, Petros Maniatis, Charles Sutton

Deep learning for program synthesis

- SpreadsheetCoder: Formula Prediction from Semi-structured Context, paper accepted by ICML 2021.
- Our work was released to support **formula suggestions in Google Sheets** for all users.

2019/05-08 **Research Intern**, *Google Brain, Kirkland, WA, USA*.

Mentor: Denny Zhou

Neural-Symbolic Techniques for Natural Language Understanding

- Neural Symbolic Reader, paper accepted by ICLR 2020 with a spotlight presentation.
- Neural-Symbolic Stack Machines, paper accepted by NeurIPS 2020.

2018/05-08 **Research Intern**, *Facebook AI Research (FAIR), Menlo Park, CA, USA*.

Mentor: Yuandong Tian

Deep Reinforcement Learning for Optimization

- Learning to Perform Local Rewriting for Combinatorial Optimization, paper accepted by NeurIPS 2019.

2015/10 **Visiting Student**, *National Institute of Informatics, Tokyo, Japan*.

Advisor: Prof. Helmut Prendinger
- Project: Deep learning for drone's object detection.
- My results encouraged the lab to continue this research direction, which finally led to the DRONET (Drone as Life Infrastructure) commercial project.

Conference Publications

2021 [1] **Xinyun Chen**, Dawn Song, Yuandong Tian, "Latent Execution for Neural Program Synthesis Beyond Domain-Specific Languages", *Advances in Neural Information Processing Systems*, 2021 (**NeurIPS '21**).

2021 [2] **Xinyun Chen**, Petros Maniatis, Rishabh Singh, Charles Sutton, Hanjun Dai, Max Lin, Denny Zhou, "SpreadsheetCoder: Formula Prediction from Semi-structured Context", International Conference on Machine Learning, 2021 (**ICML'21**).
Our work was released to support **formula suggestions in Google Sheets** for all users.
Other related links: [Google AI Blog] | [The Verge]

2021 [3] Hongyu Ren, Hanjun Dai, Bo Dai, **Xinyun Chen**, Michihiro Yasunaga, Haitian Sun, Dale Schuurmans, Jure Leskovec, Denny Zhou, "LEGO: Latent Execution-Guided Reasoning for Multi-Hop Question Answering on Knowledge Graphs", International Conference on Machine Learning, 2021 (**ICML'21**).

2021 [4] Cheng Fu, Hanxian Huang, **Xinyun Chen**, Yuandong Tian, Jishen Zhao, "Learn-to-Share: A Hardware-friendly Transfer Learning Framework Exploiting Computation and Parameter Sharing", International Conference on Machine Learning, 2021 (**ICML'21, Long Talk**).

2021 [5] **Xinyun Chen**, Linyuan Gong, Alvin Cheung, Dawn Song, "PlotCoder: Hierarchical Decoding for Synthesizing Visualization Code in Programmatic Context", Annual Meeting of the Association for Computational Linguistics, 2021 (**ACL'21**).

2021 [6] Yujian Gan, **Xinyun Chen**, Qiuping Huang, Matthew Purver, John R. Woodward, Jinxia Xie, Pengsheng Huang, "Towards Robustness of Text-to-SQL Models against Synonym Substitution", Annual Meeting of the Association for Computational Linguistics, 2021 (**ACL'21**).

2021 [7] **Xinyun Chen***, Wenxiao Wang*, Chris Bender, Yiming Ding, Ruoxi Jia, Bo Li, Dawn Song, "REFIT: a Unified Watermark Removal Framework for Deep Learning Systems with Limited Data", ACM Asia Conference on Computer and Communications Security, 2021 (**AsiaCCS'21**). (* Equal contribution)

2021 [8] Yujian Gan, **Xinyun Chen**, Matthew Purver, "Exploring Underexplored Limitations of Cross-Domain Text-to-SQL Generalization", Conference on Empirical Methods in Natural Language Processing, 2021 (**EMNLP'21**).

2021 [9] Yujian Gan, **Xinyun Chen**, Jinxia Xie, Matthew Purver, John R. Woodward, John Drake, Qiaofu Zhang, "Natural SQL: Making SQL Easier to Infer from Natural Language Specifications", Findings of Conference on Empirical Methods in Natural Language Processing, 2021 (**EMNLP Findings'21**).

2021 [10] Zhuolin Yang*, Zhaoxi Chen, Tiffany (Tianhui) Cai, **Xinyun Chen**, Bo Li, Yuandong Tian*, "Understanding Robustness in Teacher-Student Setting: A New Perspective", *Artificial Intelligence and Statistics*, 2021 (**AISTATS '21**). (* Equal contribution)

2020 [11] **Xinyun Chen**, Chen Liang, Adams Wei Yu, Dawn Song, Denny Zhou, "Compositional Generalization via Neural-Symbolic Stack Machines", *Advances in Neural Information Processing Systems*, 2020 (**NeurIPS '20**).

2020 [12] Kavi Gupta, Peter Ebert Christensen*, **Xinyun Chen***, Dawn Song, "Synthesize, Execute and Debug: Learning to Repair for Neural Program Synthesis", *Advances in Neural Information Processing Systems*, 2020 (**NeurIPS '20**). (* Equal contribution)

2020 [13] Aishan Liu, Tairan Huang, Xianglong Liu, Yitao Xu, Yuqing Ma, **Xinyun Chen**, Stephen Maybank, Dacheng Tao, "Spatiotemporal Attacks for Embodied Agents", *European Conference on Computer Vision*, 2020 (**ECCV '20**).

2020 [14] **Xinyun Chen**, Chen Liang, Adams Wei Yu, Denny Zhou, Dawn Song, Quoc Le, "Neural Symbolic Reader: Scalable Integration of Distributed and Symbolic Representations for Reading Comprehension", *International Conference on Learning Representations*, 2020 (**ICLR '20, Spotlight**).

2020 [15] Hui Shi, Yang Zhang, **Xinyun Chen**, Yuandong Tian, Jishen Zhao, "Deep Symbolic Superoptimization Without Human Knowledge", *International Conference on Learning Representations*, 2020 (**ICLR '20**).

2019 [16] **Xinyun Chen**, Yuandong Tian, "Learning to Perform Local Rewriting for Combinatorial Optimization", *Advances in Neural Information Processing Systems*, 2019 (**NeurIPS '19**).

2019 [17] Cheng Fu, Huili Chen, Haolan Liu, **Xinyun Chen**, Yuandong Tian, Farinaz Koushanfar, Jishen Zhao, "Coda: An End-to-End Neural Program Decompiler", *Advances in Neural Information Processing Systems*, 2019 (**NeurIPS '19**).

2019 [18] **Xinyun Chen**, Chang Liu, Dawn Song, "Execution-Guided Neural Program Synthesis", *International Conference on Learning Representations*, 2019 (**ICLR '19**).

2018 [19] **Xinyun Chen**, Chang Liu, Dawn Song, "Tree-to-tree Neural Networks for Program Translation", *Advances in Neural Information Processing Systems*, 2018 (**NeurIPS '18**).

2018 [20] Xiaojun Xu, **Xinyun Chen**, Chang Liu, Anna Rohrbach, Trevor Darell, Dawn Song, "Fooling Vision and Language Models Despite Localization and Attention Mechanism", *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018 (**CVPR '18**).

2018 [21] **Xinyun Chen**, Chang Liu, Dawn Song, "Towards Synthesizing Complex Programs from Input-Output Examples", *International Conference on Learning Representations*, 2018 (**ICLR '18**).

2017 [22] Yanpei Liu, **Xinyun Chen**, Chang Liu, Dawn Song, "Delving into Transferable Adversarial Examples and Black-box Attacks", *International Conference on Learning Representations*, 2017 (**ICLR '17**).

2016 [23] **Xinyun Chen**, Chang Liu, Richard Shin, Dawn Song, Mingcheng Chen, "Latent Attention For If-Then Program Synthesis", *Advances in Neural Information Processing Systems*, 2016 (**NeurIPS '16**).

Workshop Publications

2020 [1] Hongyu Ren, Hanjun Dai, Bo Dai, **Xinyun Chen**, Denny Zhou, Jure Leskovec, Dale Schuurmans, "Scaling up Logical Query Embeddings on Knowledge Graphs", early version in ICML 2021 Workshop on Self-Supervised Learning for Reasoning and Perception (**Oral**).

2020 [2] Pratyush Maini, **Xinyun Chen**, Bo Li, Dawn Song, "Perturbation Type Categorization for Multiple l_p Bounded Adversarial Robustness", early version in ICML 2020 Workshop on Uncertainty and Robustness in Deep Learning.

2017 [3] Warren He, James Wei, **Xinyun Chen**, Nicolas Carlini, Dawn Song, "Adversarial Example Defenses: Ensembles of Weak Defenses are not Strong", in 11th USENIX Workshop on Offensive Technologies, 2017 (**WOOT '17**).

2016 [4] Bo Li, Yevgeniy Vorobeychik, **Xinyun Chen**, "A General Retraining Framework for Scalable Adversarial Classification", in NeurIPS 2016 Workshop on Adversarial Training, 2016.

Preprints

2021 [1] Shiyu Tang, Ruihao Gong, Wang Yan, Aishan Liu, Jiakai Wang, **Xinyun Chen**, Fengwei Yu, Xianglong Liu, Dawn Song, Alan Yuille, Philip Torr, Dacheng Tao, "RobustART : Benchmarking Robustness on Architecture Design and Training Techniques", arXiv preprint arXiv:2109.05211.

2020 [2] Micah Goldblum, Dimitris Tsipras, Chulin Xie, **Xinyun Chen**, Avi Schwarzschild, Dawn Song, Aleksander Madry, Bo Li, Tom Goldstein, "Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses", arXiv preprint arXiv:2012.10544.

2017 [3] **Xinyun Chen**, Chang Liu, Bo Li, Kimberly Lu, Dawn Song, "Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning", arXiv preprint arXiv:1712.05526.
Media coverage: Motherboard, The Register

Talks

2021/11 **Deep Learning for Program Synthesis: Towards Human-like Reasoning**, Rising Stars in Machine Learning Speaker Series, University of Maryland.

2021/10 **Neural Program Synthesis for Language Understanding in the Wild**, Neurosym Webinar Series.

2021/10 **Deep Learning for Program Synthesis: Towards Human-like Reasoning**, Stanford Software Research Lunch.

2021/09 **Deep Learning for Program Synthesis: Towards Human-like Reasoning**, Facebook Fellowship Summit.

2021/08 **Deep Learning for Program Synthesis: Towards Human-like Reasoning**, University of Southern California.

2021/06 **Adversarial Attacks in Computer Vision: An Overview**, CVPR Tutorial on Adversarial Machine Learning in Computer Vision.

2021/04 **Deep Learning for Program Synthesis**, SJSU SCE Spark Tech Conference.

2021/03 **Neural-Symbolic Reasoning for Language Understanding**, Keynote speech at WSDM Workshop on Machine Reasoning.

2020/12 **Deep Learning for Program Synthesis from Input-Output Examples**, NeurIPS Workshop on Computer-Assisted Programming.

2020/06 **Neural Program Synthesis for Navigation and Language Understanding**, CVPR Tutorial on Neuro-Symbolic Visual Reasoning and Program Synthesis.

2020/04 **Learning to Perform Local Rewriting for Combinatorial Optimization**, Google, Mountain View.

2020/02 **Neural-Symbolic Reader for Reading Comprehension**, Google, Mountain View.

2020/01 **Learning to Perform Local Rewriting in Discrete Search Spaces**, Alibaba Group, Sunnyvale.

2019/10 **Neural Program Synthesis from Natural Language Specification**, Open Virtual Assistant Lab, Stanford University.

2019/02 **Neural Program Synthesis from Input-Output Examples**, UC San Diego.

2018/11 **Towards Synthesizing Complex Programs from Input-Output Examples**, Guest lecture in CS294-157: Deep Learning and Program Synthesis, UC Berkeley.

2018/10 **Neural Program Synthesis from Input-Output Examples**, Facebook Big Code Summit.

2018/05 **Deep Learning for Program Synthesis**, Guest lecture in CS379C: Computational Models of the Neocortex, Stanford University.

Services

Co-Organizer, Workshop on Security and Safety in Machine Learning Systems (ICLR 2021).

Co-Organizer, Tutorial on Adversarial Machine Learning in Computer Vision (CVPR 2021).

Co-Organizer, Workshop on Adversarial Machine Learning in Real-world Computer Vision Systems and Online Challenges (CVPR 2021).

Co-Organizer, Workshop on Socially Responsible Machine Learning (ICML 2021).

Co-Organizer, Workshop on Adversarial Robustness in the Real World (ICCV 2021).

Co-Organizer, Workshop on Practical Deep Learning in the Wild (AAAI 2022).

Co-Organizer, Workshop on Adversarial Learning for Multimedia (ACM MM 2021).

Co-Organizer, Workshop on Adversarial Machine Learning in Computer Vision (CVPR 2020).

Senior Program Committee, IJCAI 2021.

Expert Reviewer, ICML 2021.

Program Committee / Reviewer, NeurIPS, ICLR, AAAI, ACL, EMNLP, NAACL, CVPR, ICCV, ECCV, TPAMI, IJCV, Artificial Intelligence, TIP, TIFS, TDSC.

2020-Present **Mentor**, Undergraduate AI Research Mentoring Program, UC Berkeley.

Mentor undergraduates from underrepresented groups who are considering a career in research.

2020/09 **Facilitator**, *London Machine Learning Meetup*.

2020 **Student Reviewer**, *UC Berkeley EECS Ph.D. Admissions*.

Review Ph.D. applications in Security and AI-Security.

Teaching Experience

Fall 2021 **Advisor**, Teaming and Project Management (ENGIN 270C), UC Berkeley.

Propose the project topics for M.Eng students, design the project milestones and deliverables, mentor the students to fulfill the course requirements.

Fall 2021 **Graduate Student Instructor**, Deep Reinforcement Learning (CS 285), UC Berkeley.

Spring 2021 **Graduate Student Instructor**, Introduction to Artificial Intelligence (CS 188), UC Berkeley.

Fall 2014 **Teaching Assistant**, Computer Programming (CS 122), Shanghai Jiao Tong University.

Mentoring

Kavi Gupta, Master student at UC Berkeley, now a Ph.D. student at MIT.

Pratyush Maini, Visiting undergraduate from IIT Delhi, now a Ph.D. student at Carnegie Mellon University.

Wenxiao Wang, Visiting undergraduate from Tsinghua University, now a Ph.D. student at University of Maryland.

Peter Ebert Christensen, Visiting master student from Technical University of Denmark.

Da Shen, Visiting master student from University of Maryland.

Anish Doshi, M.Eng student at UC Berkeley.

Wesley Cheng, M.Eng student at UC Berkeley.

Harry Singh, M.Eng student at UC Berkeley.

Chia-En Chiang, M.Eng student at UC Berkeley.

Chris Bender, Undergraduate at UC Berkeley.

Yiming Ding, Undergraduate at UC Berkeley.

Kimberly Lu, Undergraduate at UC Berkeley.

Arnav Gudibande, Undergraduate at UC Berkeley.

Jason Xiong, Undergraduate at UC Berkeley.

Misc

Music: Grade 9 Certificate of Piano, Grade 10 Certificate of Music Theory