Jiameng Fan

Contact Information

302 PHO
8 Saint Mary's St.
Boston, MA 02215

e-mail: jmfan@bu.edu
homepage: https://jiamengf.com

Research Interests

My research lies at the intersection of Machine Learning, Formal Methods and Robotics. I am particularly interested in

- Developing formal analysis tools for learning-enabled systems to prove safety and robustness.
- Developing data-efficient techniques that combine machine learning and formal methods to improve system performance and ensure safety in unknown environments.
- Developing computationally efficient representation learning algorithms to train robust models and bridge the gap between simulation and real-world applications.

Education

Boston University Sep. 2017 - Aug. 2022
Ph.D. in Electrical Engineering *Advisor: Prof. Wenchao Li*

Beijing Institute of Technology Sep. 2013 - Jul. 2017
B.E. in Mechtronic Engineering (with honor) *Advisors: Prof. Qiang Huang and Weimin Zhang*

University of California, Irvine Jul. 2016 - Nov. 2016
Visiting Student *Advisor: Prof. Mohammad Al Faruque*

University of California, Berkeley Jul. 2015 - Aug. 2015
Summer School Student

Work Experience

Google Sep. 2022 - Present
Software Engineering
Working at the intersection of machine learning, computer vision and multimodal learning. Deploying state-of-the-art machine learning techniques on real world problems.

Google, Remote Sep. 2021 - Dec.2021
Software Engineering Intern *Mentors: Bryan Klingner and Rongqi Qiu*
Developing a novel constrained-optimization based data alignment technique for world-scale Geo imagery data (e.g. ground-level, aerial and satellite). The technique provides a new imagery alignment quality metric and improves the alignment quality with black-box optimization methods.

Selected Publications

Google Scholar

1. **Safety-Assured Design and Adaptation of Connected and Autonomous Vehicles**
   Xin Chen, Jiameng Fan, Chao Huang, Ruochen Jiao, Wenchao Li, Xiangguo Liu, Yixuan Wang, Zhilu Wang, Weichao Zhou, and Qi Zhu
   Chapter in Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems, Springer, 2023 (to appear).
2. **DRIBO: Robust Deep Reinforcement Learning via Multi-View Information Bottleneck** [pdf]
   Jiameng Fan and Wenchao Li
   International Conference on Machine Learning (ICML), July 2022
3. **POLAR: A Polynomial Arithmetic Framework for Verifying Neural-Network Controlled Systems** [preprint]
   Chao Huang, Jiameng Fan, Xin Chen, Wenchao Li and Qi Zhu
   The 20th International Symposium on Automated Technology for Verification and Analysis (ATVA), October 2022
4. **Adversarial Training and Provable Robustness: A Tale of Two Objectives** [pdf]
   Jiameng Fan and Wenchao Li
   AAAI Conference on Artificial Intelligence (AAAI), February 2021.

5. **Divide and Slide: Layer-Wise Refinement for Output Range Analysis of Deep Neural Networks** [pdf]
   Chao Huang, Jiameng Fan, Xin Chen, Wenchao Li and Qi Zhu
   In Proceedings of the ACM SIGBED International Conference on Embedded Software (EMSOFT), September 2020.
6. **ReachNN*: A Tool for Reachability Analysis of Neural-Network Controlled Systems** [pdf]
   Jiameng Fan, Chao Huang, Xin Chen, Wenchao Li and Qi Zhu
   The 18th International Symposium on Automated Technology for Verification and Analysis (ATVA), October 2020.
7. **Towards Verification-Aware Knowledge Distillation for Neural-Network Controlled Systems** [pdf]
   Jiameng Fan, Chao Huang, Wenchao Li, Xin Chen and Qi Zhu
   In Proceedings of the 38th ACM/IEEE International Conference on Computer Aided Design (ICCAD), November 2019.
8. **ReachNN: Reachability Analysis of Neural-Network Controlled Systems** [pdf]
   Chao Huang, Jiameng Fan, Wenchao Li, Xin Chen and Qi Zhu
   In Proceedings of the ACM SIGBED International Conference on Embedded Software (EMSOFT), October 2019.
9. **Safety-Guided Deep Reinforcement Learning via Online Gaussian Process Estimation** [pdf]
   Jiameng Fan and Wenchao Li
   International Conference on Learning Representation (ICLR), Workshop on Safe Machine Learning: Specification, Robustness, and Assurance, May 2019.

Peer Reviewing

Reviewer for Journals and Conference Articles

1. AAAI Conference on Artificial Intelligence (AAAI), 2023
2. Neural Information Processing Systems (NeurIPS), 2022
3. International Conference on Machine Learning (ICML), 2022, 2023
4. IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2020, 2021
5. Transactions on Design Automation of Electronic Systems (TODAES), 2020
6. Design, Automation and Test in Europe Conference (DATE), 2020, 2021
7. Design Automation Conference (DAC), 2018, 2019, 2020
8. International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2020, 2022
9. ACM International Conference on Hybrid Systems: Computation and Control (HSCC), 2020
10. IEEE Robotics & Automation Magazine (RAM), 2019
11. International Conference On Computer Aided Design (ICCAD), 2018, 2022
12. Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021, 2022

Selected Awards

- **Silver Medal (2nd Place) in the 2021 ACM SIGBED Student Research Competition**: Association for Computing Machinery, 2021
- **ESWEEK Student Travel Grant**: the US National Science Foundation (NSF), 2019.
- **Distinguished Electrical Engineering Fellowship**: Boston University, 2017
- **College Graduate Excellence Award of Beijing**: Beijing City Ministry of Education, 2017
- **Diwen Scholarship**: Beijing Institute of Technology, 2016
- **National Scholarship**: Ministry of Education of the People's Republic of China, 2014
- **First-class Scholarships**: Beijing Institute of Technology, 2013, 2014, 2015, 2016

Skills

Python, C++, MATLAB, Robot Operating System (ROS), Pytorch, Tensorflow, Gurobi, LaTeX

Open-Source Tools

AdvIBP: Certified Adversarial Training by Combining Adversarial Training and Provable Robustness Verification in a Principled Way.

- AdvIBP achieved state-of-the-art verified (certified) errors on MNIST and CIFAR-10.
- Github Repository: https://github.com/JmfanBU/AdvIBP

ReachNN*: A formal reachability analysis tool to verify the neural-network controlled system (NNCS) with GPU support.

- ReachNN* uses Bernstein polynomials to approximate neural networks with general types of activation functions. It also offers a feature to automatically retrain a verification-friendly network.
- Github Repository: https://github.com/JmfanBU/ReachNNStar

Core Graduate Coursework

EC 719 Statistical Machine Learning	Spring 2019
ME 570 Robot Motion Planning	Fall 2018
EC 724 Advanced Optimization Methods	Spring 2017
EC 505 Stochastic Process	Fall 2017