

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

Ph.D. in Electrical Engineering

Sep. 2017 - present
Advisor: Prof. [Wenchao Li](#)

Beijing Institute of Technology

B.E. in Mechtronic Engineering (with honor)

Sep. 2013 - Jul. 2017
Advisors: Prof. [Qiang Huang](#) and [Weimin Zhang](#)

University of California, Irvine

Visiting Student

Jul. 2016 - Nov. 2016
Advisor: Prof. [Mohammad Al Faruque](#)

University of California, Berkeley

Summer School Student

Jul. 2015 - Aug. 2015

WORK EXPERIENCE

Google, Remote

Software Engineering Intern

Sep. 2021 - Dec. 2021

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. **POLAR: A Polynomial Arithmetic Framework for Verifying Neural-Network Controlled Systems** [[preprint](#)]
Chao Huang, [Jiameng Fan](#), Xin Chen, Wenchao Li and Qi Zhu
Preprint, 2021 (Under review)
2. **DRIBO: Robust Deep Reinforcement Learning via Multi-View Information Bottleneck** [[preprint](#)]
[Jiameng Fan](#) and Wenchao Li
Preprint, 2021 (Under review)
3. **Adversarial Training and Provable Robustness: A Tale of Two Objectives** [[pdf](#)]
[Jiameng Fan](#) and Wenchao Li
AAAI Conference on Artificial Intelligence (AAAI), February 2021.
4. **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.
5. **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.

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

- 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, L^AT_EX

- 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
ME 570 Robot Motion Planning
EC 724 Advanced Optimization Methods
EC 505 Stochastic Process

Spring 2019
Fall 2018
Spring 2017
Fall 2017