

Computer Science and Engineering Department  
Michigan State University  
East Lansing, MI 48823, USA

Mobile: (+1)-352-870-5374  
Email: [jiajingh@msu.edu](mailto:jiajingh@msu.edu)  
Website: [Homepage](#)

## RESEARCH FOCUSES

**Deep learning:** Adversarial Learning (adversarial attack & defense), Programming language problem (code generation, code understanding), Computer Vision (image classification, image reconstruction), Natural language processing (representation learning, sentiment analysis, text classification)

**Optimization:** Bi-level optimization, Zeroth-order black-box optimization

## EDUCATION

**Ph.D. Candidate in Computer Science, Michigan State University** Aug. 2021– Present.  
**M.S. in Electrical and Computer Engineering, University of Florida** Aug. 2019– May. 2021  
**B.Eng in Computer Science, Univ. of Science and Technology of China** Sep. 2015– July 2019

## PUBLICATIONS

### [Google Scholar](#)

- [1] **J. Jia**, S. Srikant, T. Mitrovskaya, S. Chang, S. Liu, U. O'Reilly, "[Having Both: Robust and Accurate Code Models](#)", *SANER'23*
- [2] B. Hou, **J. Jia**, Y. Zhang, G. Zhang, S. Liu, S. Chang, "[TextGrad: Advancing Robustness Evaluation in NLP by Gradient-Driven Optimization](#)", *ICLR'23*
- [3] R. Francis, J. Jia, S. Prabhakar Chepuri, S. Liu, [Decentralized Stochastic Frank-Wolfe for Constrained Finite-Sum Minimization](#), *AISTATS'23*, under review
- [4] J. Jia, M. Hong, Y. Zhang, M. Akçakaya, S. Liu, [On the Robustness of deep learning-based MRI Reconstruction to image transformations](#), *NeurIPS'22 workshop*
- [5] Y. Zhang, Y. Yao, **J. Jia**, J. Yi, M. Hong, S. Chang, S. Liu, "[How to Robustify Black-Box ML Models? A Zeroth-Order Optimization Perspective](#)", International Conference on Learning Representation (*ICLR'22 - Spotlight*)
- [6] **J Jia**, C Zhang, B Yaman, S Moeller, S Liu, M Hong, M Akçakaya, "[On Instabilities of Conventional Multi-Coil MRI Reconstruction to Small Adversarial Perturbations](#)", International Society for Magnetic Resonance in Medicine (*ISMRM'21 - Oral*)

## RESEARCH EXPERIENCE

**Adversarial contrastive learning for programming language** Jul. 2021 - Present

Supervisor: [Sijia Liu](#) (MSU) Collaborator: [Shashank Srikant](#)(MIT), [Shiyu Chang](#)(UCSB), [Una-May O'Reilly](#)(MIT)

- Propose a way to co-optimize both the accuracy and robustness of code models by using adversarial codes (codes generated using semantics-preserving obfuscations to fool code models).
- Introduce robustness-promoting views in contrastive learning (CL) at the self-supervised pre-training phase.
- Utilize proper temporally-staggered schedule of adversarial code generation at fine-tuning phase to further improve the robustness and accuracy on downstream tasks.
- Conduct experiments on three downstream tasks to demonstrate effectiveness of proposed framework (e.g. 11% in robustness and 6% in accuracy on the code summarization task in Python).
- Additionally demonstrate the effectiveness of adversarial learning at pre-training phase by analyzing the characteristics of the loss landscape and interpretability of the pre-trained models.
- **Publications:** [1]

**An novel adversarial attack in Natural language processing**

Aug. 2021 - present

Supervisor: [Sijia Liu](#) (MSU)Collaborator: [Shiyu Chang](#) (UCSB)

- Propose the first-order gradient-driven white-box adversarial attack for NLP models
- Overcome the discrete nature of the textual input through an effective convex relaxation method
- Achieve state-of-the-art attack success rate on several datasets
- TextGrad-enabled adversarial training yields the most robust NLP model against a wide spectrum of NLP attacks.
- **Publications:** [\[2\]](#)

**Robustification of Black-Box ML Models by Zeroth-Order Optimization** Jan.2021-Oct.2021Supervisor: [Sijia Liu](#) (MSU) Collaborator: [Jinfeng Yi](#)(JD AI), [Mingyi Hong](#)(UMN), [Shiyu Chang](#)(UCSB)

- Formulate black-box defense problem through the lens of zeroth-order (ZO) optimization
- Propose scalable ZO optimization method to tackle defense challenge in high dimension
- Achieve state-of-the-art certified robustness on CIFAR-10 and STL-10
- Extend black-box defense from image classification to image reconstruction
- **Publications:** [\[5\]](#)

**Robustness of conventional multi-coil MRI reconstruction**

Jul. 2020 - Oct. 2020

Supervisor: [Sijia Liu](#) (MSU)Collaborator: [Mehmet Akçakaya](#)(UMN), [Mingyi Hong](#)(UMN)

- Show that conventional multi-coil reconstructions are also susceptible to large instabilities from small adversarial perturbations.
- **Publications:** [\[6\]](#)

**ACADEMIC ACTIVITIES**

---

- **Contributors to code demos** for NeurIPS'22 tutorial: Foundational Robustness of Foundation Models.
- **Reviewer:** ICASSP'22, ICML'22, ICLR'22, NeurIPS'22, CVPR
- **TPC** for KDD'22 Workshop 4th Workshop on Adversarial learning Methods for Machine learning and Data Mining
- **Student Chair** for ICML'22 Workshop AdvML:New Frontiers in Adversarial Machine Learning.

**SKILLS**

---

- **Programming Languages** Python, MATLAB, C++, Java, C
- **Libraries** Pytorch, TensorFlow, Numpy, Matplotlib, Huggingface