Zhuolin Yang | Curriculum Vitae

+86 137 3907 1100 • lucas110550@sjtu.edu.cn
lucas110550.github.io

ACM honors class, Shanghai Jiao Tong University **Shanghai**
Bachelor of Science in Engineering, Major in Computer Science *Sept 2015–June 2019*

- Member of ACM honors Class, an elite CS program for top 5% talented students.
- **Research Interests**: Adversarial machine learning, Reinforcement learning, Speech recognition, Security.

Publications

1. **Characterizing Audio Adversarial Examples Using Temporal Dependency**
   - **Zhuolin Yang**, Bo Li, Pin-Yu Chen, Dawn Song
   - Accepted by *International Conference on Learning Representations (ICLR), 2019*
2. **Data Augmentation using Conditional Generative Adversarial Networks for Robust Speech Recognition**
   - Peiyao Sheng, **Zhuolin Yang**, Hu Hu, Tian Tan, Yanmin Qian
   - Published in *International Symposium on Chinese Spoken Language Processing (ISCSLP), 2018*
3. **Mitigating Data Poisoning Attacks using the Shapley Value**
   - **Zhuolin Yang**, Ruoxi Jia, Bo Li
   - Ready to submit to *International Conference on Machine Learning (ICML), 2019*

Research Experiences

- **Security Lab** **University of Illinois Urbana-Champaign**
  *Visiting Research intern advised by **Prof. Bo Li*** *Sept 2018–Dec 2018*

  Worked on generating few-pixel adversarial example using *deep reinforcement learning*.
  - Implemented a 3-step Duel Double DQN with PER.
  - Using Shapley value as soft reward to guide each action.
  - Using attention layer to manipulate each modification action's probability during exploration action.

- **Berkeley Artificial Intelligence Research Lab** **University of California, Berkeley**
  *Visiting Research intern advised by **Prof. Dawn Song*** *July 2018–Sept 2018*

  Worked on defending poisoning attack using Shapley value.
  - Implement a Shapley value based criterion to detect and mitigate poisoning attack.
  - In easy defense situation, our performance is close to **oracle** - already known poison data index.
  - Even in severe defense situation, our method also achieve high defense successful rate and highly outperform the influence function baseline method's results.
  - This work is ready to submit to *ICML 2019*

- **Speech Lab** **Shanghai Jiao Tong University**
  *Undergraduate Researcher advised by **Prof. Kai Yu*** *Sept 2017–July 2018*

  Worked on Speech Data Augmentation using Conditional GAN.
  - Implemented Conditional Wasserstein GAN based on acoustic state.
  - Generated augmented frame-level audio feature-map with label to improve acoustic model training.
  - Decreased about 6% to 10% WER comparing to previous state-of-art work using GAN.
  - This work was published in *ISCSLP 2018*

Education

Awards

I'm an algorithm programming contest lover, with over 10 years experiences on coding beyond delicate algorithms since primary school. I participated **ACM-ICPC** (and CCPC, ICPC in China) contests many times and here're some notable awards I earned.

- **ACM-ICPC Asia Yangon Regional Contest** — **9th Place**
  University of Computer Studies, Yangon, Myanmar — *2016*
- **CCPC Hefei Regional Contest** — **Gold Medal**
  Anhui University, Hefei, China — *2016*
- **ACM-ICPC Asia Singapore Regional Contest** — **8th Place**
  National University of Singapore, Singapore — *2015*
- **ACM-ICPC Asia Shanghai Regional Contest** — **Gold Medal**
  East China University of Science and Technology, Shanghai, China — *2015*
- **CCPC Nanyang Regional Contest** — **Gold Medal**
  Nanyang Institute of Technology, Henan, China — *2015*

Scholarship

- **Eleme Scholarship** — **Shanghai Jiao Tong University**
  Top 5% students in the CS department — *2016*
- **Zhiyuan Honorary Scholarship** — **Zhiyuan College**
  Excellent students in Zhiyuan College — *2015 and 2016*
- **Academic Excellence Scholarship (2nd place)** — **Shanghai Jiao Tong University**
  Top students award in Shanghai Jiao Tong University — *2015 and 2016*

Teaching Experiences

- **ACM-ICPC Training** — **Shanghai Jiao Tong University ACM Team**
  Training co-coach — *2017–now*
- **MS105, Data Structures** — **Zhiyuan College**
  Teaching Assistant — *Spring 2017*

Notable Projects

- **Margatroid Compiler**: *A basic Compiler for simplified C language*

  Margatroid compiler is a basic compiler for M* language (a simplified C language), implementation mainly based on Java. Graph Coloring for Register Allocation and some other optimizers have been added. It contains 12000+ line code and finished in a short time. It can turn a M* language code into x86 instruction and output corresponding results with a x86 instruction simulator.

- **MIPS CPU**: *A Simple 5-stages pipelined MIPS microprocessor*

  This is a basic 5-stages pipelined MIPS microprocessor, using Harvard Structure. It's implemented by Verilog HDL, and finished in a week.

- **Implementation of Advanced Data Structures**: *Complicated data structure implementation challenge*

  I together with my two other classmates, started to implement three challenge data structures: Strict Fibonacci Heap, AAA Tree, PQ Tree without any reference code. We kept contacting with some paper's author(like Robert Tarjan) to fix our understanding and keep working. After all, we finished this really tough work and gained the highest difficulties evaluation points among all groups.