

## Zhiyuan ZHANG

+852 63107561 | zhi-shan.zhang@connect.polyu.hk | <https://zhiyuan-holly-zhang.github.io/>

### EDUCATION

#### **The Hong Kong Polytechnic University (PolyU)**

**08/2021-Present**

*BSc (Hons) Scheme in Computing*

- **Awards:** Dean's Honours List in the 2022/23 Academic Year; Best GBA Solution in Cathay Hackathon 2023

#### **Chalmers University of Technology, Sweden**

**01/2024-06/2024**

*Exchange*

- **Took 5 graduate-level courses** including Design of AI Systems, Discrete Optimization, Introduction to Artificial Intelligence, Image Analysis and Applied Machine Learning, and achieved A or above in most of them

#### **University of Cambridge, the United Kingdom**

**07/2023**

*Summer School*

- Studied mathematics for engineering, and explored British culture and its rich history

### RESEARCH & ACADEMIC PROJECTS

#### **Identity Membership Leakage on LLM**

**03/2024-Present**

*Core Member, Supervisor: Dr. WU Ruihan, University of California, San Diego*

- Trained and fine-tuned models that will be attacked (Few Shot Learning)
- Generated output using Gemma, visualized results with heatmap, and evaluated results
- A paper is pending publication in Aug. 2024

#### **Jailbreaking Towards LLM**

**05/2024-Present**

*Core Member, Supervisor: Prof. LIN Wanyu, HK PolyU*

- Came up with the idea of applying Tree of Thoughts towards attacking LLM
- Reviewed and summarized over 20 papers from top conferences, and presented to group members
- Carried out continuous fine-tuning, measurement, and improvement of processes
- A paper will be published around Jan. 2025

#### **Large Language Models for Operation Research Problems**

**06/2024-09/2024**

*Research Intern, Supervisor: Prof. GHADDAR Bissan, Western University, Canada*

- Studied the intersection of LLM and Operations Research Problems
- Wrote a survey about LLM for Operation Research Problems
- Used transformer architecture to evaluate the performance
- A paper will be published around Jan. 2025

#### **Recognition of Fresh and Rotten Fruits**

**01/2023**

*Research Assistant, Supervisor: Prof. CHOW Alan, Nvidia Deep Learning Institute*

- Developed a deep learning model that can interpret color images
- Used transformer architecture to better the performance
- Applied data augmentation to enhance a dataset and improved model generalization

#### **Solar Panel System**

**01/2022-08/2022**

*Core Member of Computing Team, Supervisor: Prof. NGAI Grace, Habitat Green in East Africa*

- Critically perused pertinent papers and handouts, and conducted lab experiments and field research
- Set up 21 solar panel systems for local villagers in 7 days with 3 teammates
- Gained insights into various aspects of East Africa, like agriculture and education

#### **Artificial Intelligence Research Camp**

**01/2021-02/2021**

*Core Member, Supervisor: Mr. ZHANG Xiao, University of Science and Technology of China*

- Completed paperwork, recognizing discrepancies, and promptly proposing solutions
- Used Arduino to program for the small lifting device
- Displayed exceptional coordination, planning, and problem-solving skills

### EXTRACURRICULAR ACTIVITIES

#### **Hong Kong, China Rowing Association**

**09/2022-Present**

*Core Member*

- Actively attended land and water training sessions to improve my rowing skills, and prepared for competitions

#### **Google Developer Student Club, PolyU**

**11/2021-Present**

*Core Member*

- Analyzed problems, offered practical solutions, attended workshops, and learned Explainable AI

#### **26<sup>th</sup> HEARTFIRE Team, The Education Service Platform**

**12/2022**

*Volunteer Teacher*

- Taught Latin dance to primary students in Taiwan, and enlightened students in and after class
- Hosted and helped design the Closing Ceremony

#### **E-formula Team of PolyU**

**10/2021-05/2022**

*Member of Computing Team and Press Officer*

- Gathered information, offered advice on activity promotion and weekly training, and reached out to sponsors

**PolyU Toastmasters Club**

**09/2021-07/2022**

*Vice President of Education*

- Completed publicity copywriting and recruited new members

## **SKILLS**

**Programming:** Python, Java, R, SQL, JavaScript, C, C++, C#

**Other Technical Skills:** Office 365, Adobe Premiere Pro, Adobe Photoshop