Jan Schuchardt

85748 Garching – Germany
j.schuchardt@tum.de • O-cixlwAAAAJ

Research interests

My research is focused on trustworthy machine learning beyond image classification. Specifically, I am interested in provably robust and privacy-preserving geometric machine learning.

Education

2021–now **Ph.D. Candidate**, *Technical University of Munich*
Advisor: Prof. Stephan Günnemann
- Publications at NeurIPS ($2\times$) and ICLR ($3\times$)
  - The first robustness certificate for group invariant models
  - The first robustness certificates for multi-output classifiers (e.g. image segmentation)
  - Specialized robustness certificates for graph neural networks
  - Sound adversarial threat models for neural combinatorial solvers

2018–2020 **M.Sc. Computer science**, *Technical University of Munich*, *GPA: 1.0 (With high distinction)*
Thesis: "Collective Robustness Certificates"

2015–2018 **B.Sc. Computer science**, *Technical University of Munich*, *GPA: 1.2 (With high distinction)*
Thesis: "Reinforcement Learning for Adaptation in Evolutionary Computation"

Work experience

2021–now **Scientific employee**, *Technical University of Munich*
- Organized ML lectures with up to 1500 students, 15 student tutors and 6 teaching assistants
- Held exercises on robustness, fairness and privacy
- Advised thesis projects resulting in publication at NeurIPS and ICLR

2016-2017 **Working student**, *PureLabs GmbH*
- Developed backend features for web stores using Python and Django

Technical skills

Languages **Python**, Java, MATLAB
Libraries **PyTorch**, numpy, scipy, scikit-learn
Tools git, LaTeX, MongoDB
OS Linux, Windows

Languages

German Native
English Full professional proficiency
French Elementary proficiency

Awards and scholarships

2017-2019 best.in.tum *Scholarship for the best students of the CS department*

Selected publications

ICLR 2023 (Spotlight) **Schuchardt, J.**, Wollschläger, T., Bojchevski, A., Günnemann, S. *Localized Randomized Smoothing for Collective Robustness Certification*.

TSRML 2022 Ayle, M., **Schuchardt, J.**, Gosch, L., Zügner, D., Günnemann, S. *Training Differentially Private Graph Neural Networks with Random Walk Sampling*.

NeurIPS 2022 **Schuchardt, J.**, Günnemann, S. *Invariance-Aware Randomized Smoothing Certificates*.

NeurIPS 2022 Scholten, Y., **Schuchardt, J.**, Geisler, S., Bojchevski, A., Günnemann, S. *Randomized Message-Interception Smoothing: Gray-Box Certificates for Graph Neural Networks*.

ICLR 2022 Geisler, S., Sommer, J., **Schuchardt, J.**, Bojchevski, A., Günnemann, S. *Generalization of Neural Combinatorial Solvers Through the Lens of Adversarial Robustness*.

ICLR 2021 **Schuchardt, J.**, Bojchevski, A., Klicpera, J., Günnemann, S. *Collective Robustness Certificates: Exploiting Interdependence in Graph Neural Networks*