

## Julian Bitterwolf

#### Education

- since 2018 **PhD Student**, *with Prof. Matthias Hein, University of Tübingen* Research topics: robust machine learning; out-of-distribution detection; empirical and provable adversarial robustness; non-identically distributed inputs.
- 2013-2014 **MSc Mathematics**, *École Polytechnique & Université Paris Sud 11*, Final grade: 15.3/20 Program: "Mathematics: Analysis, Arithmetics and Geometry". Thesis: "The Eilenberg-MacLane Theorem for Simplicial Sheaves" with Prof. Fabien Morel.
- 2012-2013 **Erasmus Year**, *École Polytechnique* 3rd year mathematics program. Final presentations on representation theory and quantum groups.
- 2011-2017 **BSc Mathematics**, *Karlsruhe Institute of Technology (KIT)*, Final grade: 1.1 Thesis: "Models for Synthetic Differential Geometry" with Prof. Frank Herrlich and Dr. Felix Wellen.
- 2010-2015 **BSc Physics**, *KIT*, Final grade: 1.3 with minor in Buisiness Administration. Thesis "Path Integration via Infinitesimal Complex Time Phases" on instantons with supervisors Prof. Jörg Schmalian and Dipl.-Phys. Pia Gagel.
- 2001-2009 Abitur, Lessing-Gymnasium Karlsruhe, Final grade: 1.4

### Professional Experience and Teaching

- 2022 ICML Workshop Organizer, "Shift happens: Crowdsourcing metrics and test datasets beyond ImageNet", see https://shift-happens-benchmark.github.io
- since 2018 **Teaching responsibilities as part of the PhD position**, organizing exercises for "Mathematics 1" and "Convex and Non-Convex Optimization", conducting student programming projects on "Auditing DNNs", supervising a master thesis on AI planning "Neural network heuristic functions: Taking confidence into account"
- 2017-2018 **Research Assistant**, *Research Center for Information Technology (FZI) Karlsruhe* Research on the influence of environmental effects on deep learning models for image recognition in autonomous driving.
- 2015, '16, '17 Lecturer: Preparatory course in physics, Karlsruhe University of Applied Sciences
  - 2017 Lecturer: Preparatory course in mathematics for economics, Karlsruhe University of Applied Sciences
  - 2011–2012 IT System Administrator, Institute of Algebra and Geometry, KIT
  - 2011–2015 Secretary and Board Member of Hector-Seminar-Alumni e.V.
  - 2010–2011 **Tutor**, accompanying the lecture "Linear Algebra and Analytic Geometry I" by Prof. Daniel Hug and Prof. Wilderich Tuschmann
  - 2009–2010 Military service, as a combat signaller in the German armed forces.

# Prizes, honours and extracurricular education 2022 Selected as "Highlighted Reviewer of ICLR 2022". since 2019 Reviewer at NeurIPS, ICML, ICLR, JMLR. 2018 School of Al at Pi School in Rome, working on a project commissioned by the Agency for Digital Italy on identifying cultural heritage items given a photo and contextual information. 2017 Participant at the EUTypes Summer School in Ohrid, MK 2012 – 2013 Holder of a Deutschlandstipendium, the German federal scholarship for highly talented students. 2002 – 2009 Participant of the Hector-Seminar, a weekly STEM seminar class. Computer skills

ProgrammingPython, C++, LeanOfficeLaTeX, LibreOfficeCal

Graphics Inkscape, GIMP, OpenCV Calculation PyTorch, TensorFlow, Numpy, MATLAB

#### Publications

- [1] D. Heller, P. Ferber, J. Bitterwolf, M. Hein, and J. Hoffmann, "Neural network heuristic functions: Taking confidence into account," accepted at SoCS 2022.
- [2] J. Bitterwolf, A. Meinke, M. Augustin, and M. Hein, "Revisiting out-of-distribution detection: A simple baseline is surprisingly effective," *Currently under review*, presented at the ICML UDL workshop 2021.
- [3] A. Meinke, J. Bitterwolf, and M. Hein, "Provably robust detection of out-of-distribution data (almost) for free," *Currently under review*, presented at the ICML UDL workshop 2021.
- [4] J. Bitterwolf, A. Meinke, and M. Hein, "Certifiably adversarially robust detection of out-of-distribution data," NeurIPS 2020.
- [5] E. Rusak, L. Schott, R. S. Zimmermann, J. Bitterwolf, O. Bringmann, M. Bethge, and W. Brendel, "A simple way to make neural networks robust against diverse image corruptions," Oral presentation at ECCV 2020.
- [6] M. Hein, M. Andriushchenko, and J. Bitterwolf, "Why relu networks yield high-confidence predictions far away from the training data and how to mitigate the problem," Oral presentation at CVPR 2019.