Nils Philipp Walter

nilspwalter.github.io | nils.walter@cispa.de | LinkedIn | nilspwalter

I am a second-year Ph.D. student specializing in **robust** and **explainable** machine learning. I am passionate about solving **real-world problems**, particularly in genomics, physics, reinforcement learning, and mechanistic interpretability. My goal is to develop novel **neuro-symbolic** methods that are not only **predictive** but also enable practitioners – me – to **gain deeper insights**.

Education

June 2023 - June 2027
CISPA Helmholtz Center for Information Security, **Ph.D. Computer Science**
Topic: *Develop novel neuro-symbolic methods that are not only predictive but also enable practitioners to gain deeper insights into the problem they are addressing.*

October 2020 - May 2023
Saarland University, **M. Sc. Computer Science** (1.3/1.0)
Thesis: *HyREAL: On Hybrid Learning and Reasoning for Explainable and Safe Navigation of Autonomous Cars in Interactive POMDPs*
Courses: Deep Reinforcement Learning, Hybrid Learning and Reasoning, Trustworthy Graph Neural Networks, Probabilistic Machine Learning, Software Engineering

October 2016 - July 2020
Saarland University, **B. Sc. Computer Science (minor Economics)** (1.7/1.0)
Thesis: *Adversarial Textures: Misleading Deep Neural Networks by Overlaying Semi-Transparent Textures*
Courses: High-Level Computer Vision, Neural Networks: Implementation and Applications, Machine Learning, Artificial Intelligence, Introduction to Computational Logic

Employment History

February 2022 - May 2023
CISPA Helmholtz Center for Information Security, *Student Researcher*, Group Vreeken
- Continuous optimization for data mining
- Knowledge discovery for high-dimensional datasets

September 2020 - December 2021
Max Planck Institute for Informatics, *Student Researcher*, Group Schiele
- Adversarial and corruption robustness of Quantized Neural Networks
- Role of BatchNorm for adversarial robustness

January 2019 - October 2019
Software AG - R&D department, *Working student*
- Detection of manufacturing defects in a production line using CNNs
- Review machine learning methods for an EU-funded project
- Administration and setup of virtual machines and LXC containers using Proxmox

Publications

[1] **Walter, N. P.**, Adilova, L., Kamp, M., Vreeken, J (2024). The Uncanny Valley: Exploring Adversarial Robustness from a Flatness Perspective. *arXiv preprint.*

[2] Xu, S., **Walter, N. P.**, Kalofolias, J., Vreeken, J. (2024). Learning Exceptional Subgroups by End-to-End Maximizing KL-divergence. In *Proceedings of the 41^{st} International Conference on Machine Learning (ICML).* (**spotlight, 3.5 % acceptance rate**)

[3] **Walter, N. P.**, Fischer, J., Vreeken, J. (2024). Finding Interpretable Class-Specific Patterns through Efficient Neural Search. In *The 38th Annual AAAI Conference on Artificial Intelligence.* AAAI.

[4] **Walter, N. P.**, Stutz, D., Schiele, B. (2022). On Fragile Features and Batch Normalization in Adversarial Training. Extended abstract in *The Art of Robustness Workshop (CVPR).*

Teaching Experience

WS 23/24	**Elements of Machine Learning**, *Teaching Assistant*
WS 21/22	**Elements of Machine Learning**, *Tutor*
SS 21	**Machine Learning**, *Tutor*
WS 19/20	**Machine Learning**, *Tutor*
WS 17/18	**Programming 1**, *Tutor*

Student Supervision

June 2024 - current	**Master Thesis**, *Jawad Al Rahwanji* - Finding subgroups with exceptional survival characteristic - Adapt *our* [2] differentiable subgroup discovery approach to account for survival analysis.
May 2024 - current	**Student Researcher**, *Benedikt Schardt* - Discovering statistically significant patterns from high-dimensional gene expression data. - Use E-values to correct for multiple hypothesis testing
February 2024 - current	**Student Researcher**, *Felix Falkenberg* - Explainable machine learning for image and graph approaches - Current focus is on analyzing the faithfulness of GradCam-like explanations

Skills

Programming	Python, C++, Java, CUDA C++, Matlab, R, Coq
Libraries	Pytorch, Numpy, Matplotlib, Pandas, Scikit-learn
Tools	Slurm, Linux, Docker, tmux, Git, Proxmox, LaTeX, Jupyter, LXC

Languages

German: Native **English:** Advanced **French:** Beginner **Italien** Beginner