Dr. Coenraad Mouton

Kiel, Germany | moutoncoenraad@gmail.com

Personal Website | LinkedIn | Google Scholar

Research Experience

Postdoctoral Research Fellow, University of Kiel – Kiel, Germany   October 2024 – Present
- Investigating the impact of non-robust features on medical imaging AI models with the goal of improving interpretability and adversarial robustness.
- Contributing to AI projects on osteoporosis-related tasks, including prediction of patient fracture risk and classification of vertebral fractures using various imaging modalities.

Research assistant, North-West University – Potchefstroom, South Africa   2019 – September 2024
- Researched margins in deep neural networks, focusing on generalization prediction and adversarial robustness.
- Contributed to several empirical studies exploring the generalization behavior of deep neural networks.
- Published several papers across multiple venues, including a top conference, a prestigious workshop, and numerous journal articles.
- Advised two M.Eng. students on research projects related to neural network robustness and generalization.
- Organized and participated in teaching activities, including an annual *Deep Learning Bootcamp*, hands-on coding and tool tutorials, and focused research sprints with postgraduate students.

Education

Ph.D. in Computer and Electronic Engineering, North-West University   2021 – August 2024
Thesis: *On margin-based generalization prediction in deep neural networks.*
Advisors: Prof. Marelie H. Davel and Dr. Marthinus W. Theunissen.

M.Eng. in Computer and Electronic Engineering, North-West University   2019 – 2020

B.Eng. in Computer and Electronic Engineering, North-West University,   2015 – 2018

Selected Publications

Input Margins Can Predict Generalization Too
Mouton, C., Theunissen, M.W., Davel, M.H.
AAAI Conference on Artificial Intelligence 2024 (February 2024)
`arXiv link`

Is Network Fragmentation a Useful Complexity Measure?
Mouton, C., Rabe, R., Haasbroek, D.G., Theunissen, M.W., Potgieter, H.L., Davel, M.H.
Sci4DL Workshop, NeurIPS 2024 (December 2024)
`arXiv link`

Does Simple Trump Complex? Comparing Strategies for Adversarial Robustness in DNNs
Brooks, W., Davel, M.H., *Mouton, C.*
Communications in Computer and Information Science, vol. 2326, Springer, Cham (November 2024)
`Springer link`

The Missing Margin: How Sample Corruption Affects Distance to the Boundary in ANNs
Mouton, C., Theunissen, M.W.*, Davel, M.H.
Communications in Computer and Information Science, vol. 1734, Springer, Cham (December 2022)
`arXiv link`

Exploring Layerwise Decision Making in DNNs
Mouton, C., Davel, M.H.
Communications in Computer and Information Science, vol. 1551, Springer, Cham (December 2021)
`arXiv link`

Awards and Grants

DAAD (German Academic Exchange Service), AInet Postdoc Fellow Award	2024
National Research Foundation, Postdoctoral Grant	2024
South African National Space Agency, Ph.D. Scholarship	2021 – 2023
MUST Deep Learning, Master's Scholarship	2019 – 2020

Student Supervision

William Brooks, M.Eng.   2023 – 2024
Project: *Margin-based regularization for deep neural networks*
Role: Advisor

Harmen Potgieter, M.Eng.   2023 – 2024
Project: *Exploring the effect of clustered hidden representations on generalization in deep neural networks*
Role: Assistant advisor

Additional Skills

Programming
Proficient in Python and accompanying machine learning libraries such as PyTorch, NumPy, and Scikit-learn.
Varying levels of experience in other languages such as MATLAB, C/C++, SQL, and PHP.

Tools
Experienced with Linux, Git, Anaconda, LaTeX, PyCharm, and other widely used tools in the software development and research technology stack.

Languages
English (native)
Afrikaans (native)