



Universiteit
Leiden
The Netherlands

Automated machine learning for neural network verification

König, H.M.T.

Citation

König, H. M. T. (2025, October 9). *Automated machine learning for neural network verification*. Retrieved from <https://hdl.handle.net/1887/4266921>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/4266921>

Note: To cite this publication please use the final published version (if applicable).

Automated Machine Learning for Neural Network Verification

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op donderdag 9 oktober 2025
klokke 13:00 uur

door

Hendrik Matthias Tilman König
geboren te Saarbrücken, Duitsland
in 1993

Promotor:

Prof.dr. H.H. Hoos

Co-promotor:

Dr. J.N. van Rijn

Promotiecomissie:

Prof.dr. M.M. Bonsangue

Prof.dr. K.J. Batenburg

Prof.dr. T.H.W. Bäck

Prof.dr. J.P. Katoen (RWTH Aachen University)

Prof.dr. M. Kwiatkowska (University of Oxford)

Copyright © 2025 Matthias König

This research was partially supported by TAILOR, a project funded by EU Horizon 2020 research and innovation program under GA No. 952215.

Backcover: Andreas Lisander Strauch

“Technical skill is mastery of complexity while creativity is mastery of simplicity.”

E.C. Zeeman

Contents

1	Introduction	1
1.1	Research Questions	3
1.2	Contributions of this thesis	4
1.3	Other Work by the Author	7
2	Preliminaries	9
2.1	Adversarial Attacks	9
2.2	Formal Neural Network Verification	10
2.2.1	Problem Definition	11
2.2.2	Incomplete Verification	12
2.2.3	Complete Verification	13
2.3	Automated Algorithm Configuration	15
2.4	Algorithm Portfolios & Selection	16
2.5	Running Time Prediction	17
3	Critically Assessing the State of the Art in Neural Network Verification	19
3.1	Common Practices in Benchmarking	
	Neural Network Verifiers	21
3.2	Verification Algorithms under Assessment	24
3.2.1	CPU-Based Methods	24
3.2.2	GPU-Based Methods	25
3.3	Setup for Empirical Evaluation	26
3.3.1	Problem Instances	26
3.3.2	Evaluation Metrics	30
3.3.3	Execution Environment and Software Used	31

Contents

3.4	Results and Discussion	32
3.4.1	CPU-Based Methods	32
3.4.2	GPU-Based Methods	37
3.4.3	Error Analysis	41
3.4.4	Analysis on Broader Set of Perturbation Radii	43
3.4.5	Joint Analysis of CPU- and GPU-Based Methods	48
3.4.6	Analysis of <i>unsat</i> Instances	52
3.4.7	Analysis of the 2022 VNN Competition Results	56
3.5	Conclusions and Future Work	59
4	Speeding Up MIP-Based Neural Network Verification via Automated Algorithm Configuration	67
4.1	Background	69
4.1.1	MIP-Based Neural Network Verification	70
4.1.2	Automated Configuration of MIP Solvers	71
4.1.3	Automatic Portfolio Construction	71
4.2	Network Verification with Parallel MIP Solver Portfolios	73
4.2.1	Configuration Procedure	74
4.2.2	MIP Solver	75
4.3	Setup of Experiments	75
4.3.1	Configuration Objective	76
4.3.2	Details of the Configuration Procedure	76
4.3.3	Data	77
4.3.4	Execution Environment and Software Used	77
4.4	Results	78
4.4.1	MIPVerify	79
4.4.2	Venus	81
4.5	Conclusions and Future Work	83
5	Dynamic Algorithm Termination for Branch-and-Bound-based Neural Network Verification	87
5.1	Method	88
5.1.1	Problem Formulation	88
5.1.2	Dynamic Algorithm Termination for BaB-based Neural Network Verification	89
5.1.3	Static Instance Features	90
5.1.4	Dynamic Instance Features	92

5.1.5	Classification Model	93
5.2	Experiments	93
5.2.1	Benchmarks	93
5.2.2	Evaluation Setup	94
5.3	Results and Discussion	96
5.3.1	Classification Metrics	96
5.3.2	Dynamic Algorithm Termination	97
5.4	Conclusions and Future Work	97
6	Adversarially Robust Model Selection via Racing	99
6.1	Adversarially Robust Model Selection	101
6.1.1	Naïve Racing Approach	101
6.1.2	F-Race	102
6.1.3	Sorting Mechanism	104
6.2	Setup of Experiments	104
6.3	Empirical Results	105
6.3.1	Local Robustness at the Decision Boundary	107
6.3.2	Evaluation of Our Proposed Selection Method	109
6.4	Conclusions and Future Work	110
7	Conclusions and Outlook	113
7.1	Answers to Research Questions	113
7.2	Directions for Future Research	115
	Bibliography	119
	Summary	131
	Samenvatting	133
	Acknowledgements	135
	Curriculum Vitae	137

