Formal Verification of Neural Networks with Linear Bounds

Lukas Koller

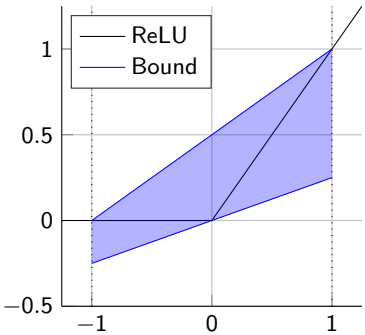
Prof. Dr.-Ing. Matthias Althoff
Cyber-Physical Systems Group
Technische Universität München

Feburary 11th, 2025

Formal Verification of Neural Networks with Linear Bounds

Neural networks are vulnerable to adversarial attacks!

→ Verify safety of neural networks by computing linear bounds for their output.



Your tasks: Review and compare different linear bounding approaches for the formal verification of neural networks, e.g., [1,2].

Interested? Contact me! Lukas Koller, lukas.koller@tum.de

[1] Wang et al., "Beta-crown: Efficient bound propagation with per-neuron split constraints for neural network robustness verification". *NeurIPS*. 2021

[2] Ferrari et al., "Complete Verification via Multi-Neuron Relaxation Guided Branch-and-Bound". *ICLR*. 2022