Formal Verification of Neural Networks

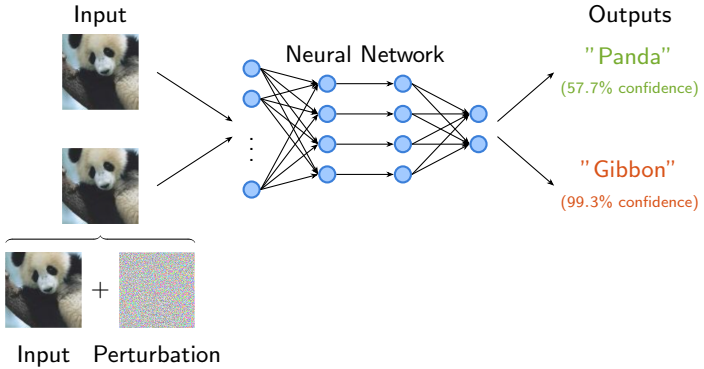
Lukas Koller

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

July 10, 2025

Neural Networks and Adversarial Attacks

Small carefully chosen input perturbation can lead to misclassifications[1].

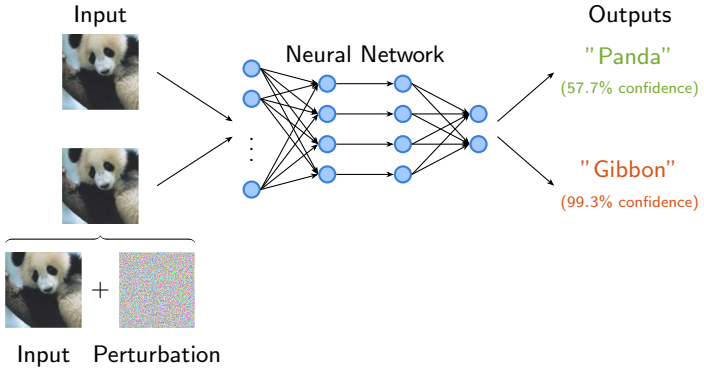


We have to verify neural networks to avoid unexpected behaviour in safety-critical enviornments!

[1] Goodfellow et al., "Explaining and Harnessing Adversarial Examples", *ICLR*, 2015

Neural Networks and Adversarial Attacks

Small carefully chosen input perturbation can lead to misclassifications[1].

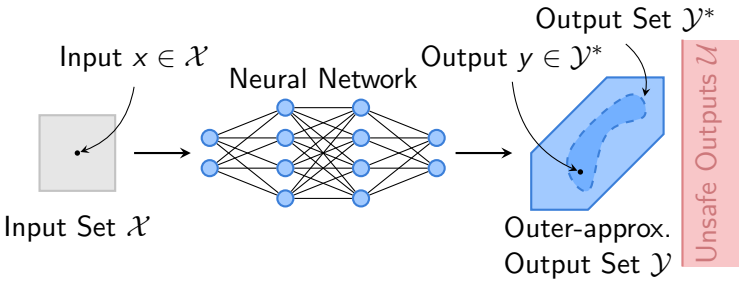


We have to verify neural networks to avoid unexpected behaviour in safety-critical enviornments!

[1] Goodfellow et al., "Explaining and Harnessing Adversarial Examples", *ICLR*, 2015

Neural Network Verification

We formally verify neural networks by enclosing the set of possible outputs.



Your tasks: You gain hands-on experience with set-based neural network verification by training and verifying neural networks[2],[3].

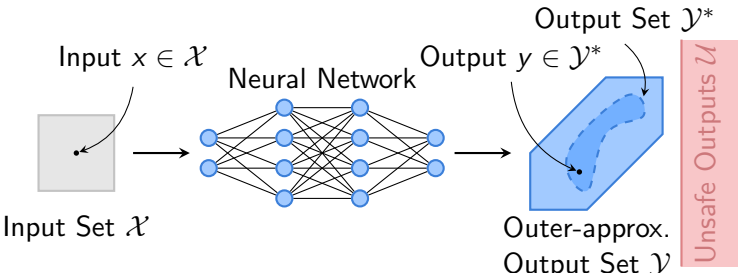
Interested? Contact me! Lukas Koller, lukas.koller@tum.de

[2] Koller et al., "Set-Based Training for Neural Network Verification", *arXiv*, 2025

[3] Kochdumper et al., "Open- and Closed-Loop Neural Network Verification Using Polynomial Zonotopes", *NASA Formal Methods*, 2023

Neural Network Verification

We formally verify neural networks by enclosing the set of possible outputs.



Your tasks: You gain hands-on experience with set-based neural network verification by training and verifying neural networks[2],[3].

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

[2] Koller et al., "Set-Based Training for Neural Network Verification", *arXiv*, 2025

[3] Kochdumper et al., "Open- and Closed-Loop Neural Network Verification Using Polynomial Zonotopes", *NASA Formal Methods*, 2023