TU Clausthal

Abschlussvortrag Masterarbeit Loich Kamdoum Deameni

„Comparison Between a Quadratic Classifier and a Piecewise Linear Classifier“

The guaranteed safety of critical systems plays a predominant role in the evolvement of DNNs, especially when such systems are prone to adversarial attacks. Multiple approaches, such as adversarial training and regularization methods, propose ef fective methods to improve the robustness of DNN to adversarial perturbations. However, most of them decrease the computational performance when the DNN model's safety is verified afterward. Therefore, co-developping novel types of Neural Networks (NNs) that can be easily verified is of growing interest to the scientific community, e.g. Polynomial Neural Network (PNN).
This thesis focuses on the comparative analysis between two classes of NNs: Piecewise Linear Neural Network and Polynomial Neural Network, exclusively with Quadratic activation function. We aim to determine the efficiency and robustness of a Quadratic Classifier (QC) compared to the most known and used type of NN (ReLU-based DNN) when exposed to adversarial perturbations. Ultimately, we were able to define the potential benefits for the safety certification of NNs when using such a classifier. We used a Projected Gradient Descend (PGD)-based attack algorithm to attack and evaluate the robustness and verification time of each type of NNs. The results show that when the QC has high accuracy (over 93%) and a near-zero loss, its robustness overcomes the Piecewise Linear Classifier (PLC).

Betreuer der Arbeit:	Prof. Dr. Rüdiger Ehlers, Prof. Dr. Steffen Herbold
Datum:	Montag, 28. März 2022, 10:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/b/sim-uc9-rvy