Verification of Binarized Neural Networks using alpha-beta-CROWN and Marabou

Rafael-Valentin Ban, Cosmin-Ștefan Negureanu, Mihai-Iosif Fârțală, Cristina-Larisa Petcu, Mădălina-Maria Radu

West University of Timișoara
Faculty of Mathematics and Informatics
Master Study Program: Software Engineering

Coordinator: Conf. Dr. Mădălina Erașcu

Wednesday 24th January, 2024

Overview

Introduction

- Motivation
  - Improving verification rates of benchmark
- Problem specification
  - Self-driving
  - Neural networks tool verifiers versus real life testing

Dataset description

Figure: Some images used in the German Traffic Signs Recognition Benchmark

Dataset description

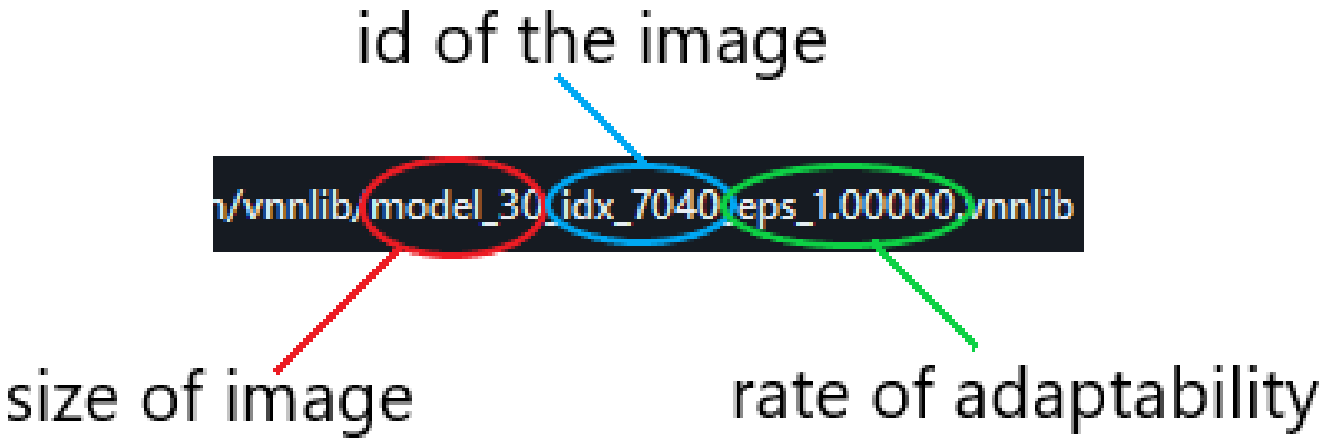

Figure: Properties file used for verification

Tools

- alpha-beta-CROWN

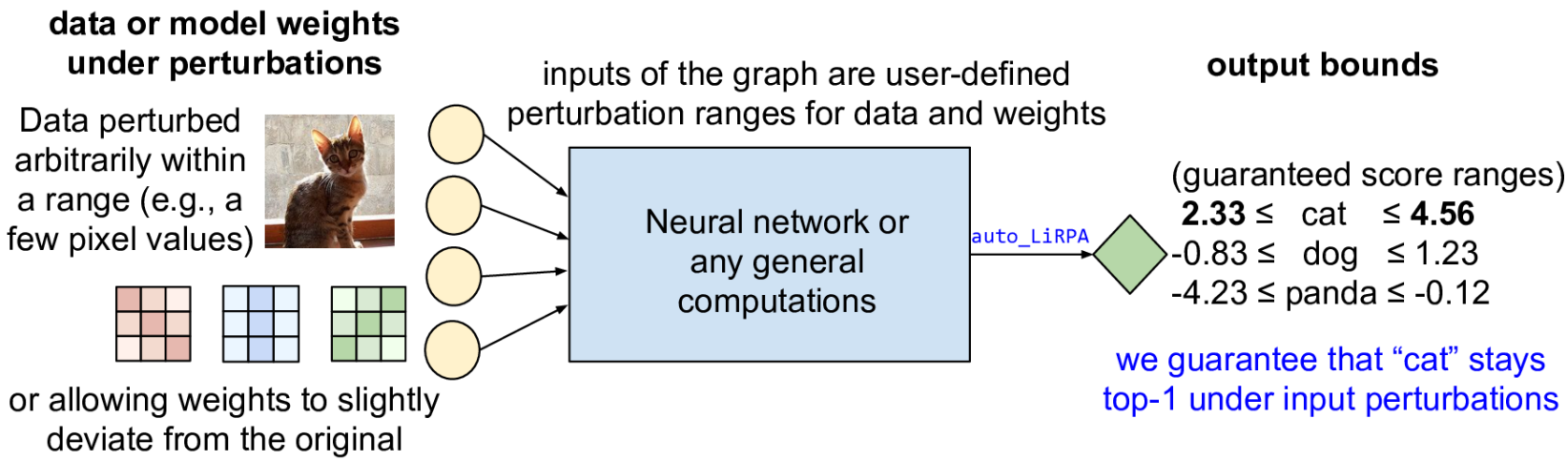

Figure: Rough explanation of efficient linear bound propagation

Tools

- Marabou
  - based on SMT technology which answers questions about the properties of a neural network
  - accepts multiple entry formats
  - performs high-level reasoning on the network that can curtail the search space and improve performance

Tools

- Nnenum
  - uses advanced abstractization for rapidly checking ReLU networks without sacrificing precisions
  - written in Python
  - utilizes GLPK for solving linear problems
  - directly accepts ONNX files and VNNLIB property files

Experimental Results

#	Tool	Verified	Falsified	Penalty
1	alpha-beta-CROWN	0	39	3
2	Marabou	-	-	-
3	Nnenum	0	0	46

Conclusion

- Posibility of verification improvement exists.
- Image verification is hard!

Demo

- alpha-beta-CROWN

  `https://www.youtube.com/watch?v=cXHRKEpAh78`

- Marabou & Nnenum

  `https://www.youtube.com/watch?v=YZIZdvPJcC8`

- Github link of the project

  `https://github.com/RafaelBan/VFProject`