Măsurarea performanţei instrumentelor specializate de verificare a reţelelor neuronale

Lect. Dr. Eraşcu Mădălina

Facultatea de Matematică și Informatică

Securitate cibernetică

Cuprins

Introducere

Această lucrare se concentrează pe performanţa instrumentelor de verificare formală a rețelelor neuronale, având ca punct de plecare competiția VNN-COMP-2023. Astfel, atenţia este orientată pe testarea celor două instrumente, α-β CROWN şi NeuralSAT.

Benchmark

In contextul acestei lucrări, s-a utilizat benchmark-ul **Traffic Sign Recognition** constituit dintr-un ansamblu de fișiere ONNX (Open Neural Network Exchange) și VNNLIB. Acesta este folosit pentru a evalua performanța instrumentelor de verificare a rețelelor neuronale.

Alpha-Beta CROWN

α , β -CROWN este un instrument de verificare a rețelelor neuronale, utilizat pentru evaluarea corectitudinii și robusteții acestora. Acesta oferă o analiză a modelelor de rețele neuronale cu scopul de a identifica posibilele vulnerabilități.

Etapele urmate pentru utilizarea tool-ului:

- instalare
- testare
- rulare

NeuralSAT

NeuralSAT este un instrument de verificare a rețelelor neuronale profunde, utilizat pentru verificarea corectitudinii și performanței rețelelor neuronale. Acesta este esențial pentru asigurarea încrederii în modelele de învățare automată utilizate într-o varietate de aplicații, inclusiv Traffic Sign Recognition.

Etapele urmate pentru utilizarea tool-ului:

- instalare
- testare
- rulare

Compararea şi interpretarea rezultatelor

idx	Alpha-Beta CROWN		VNN-COMP 2023	
	Rezultat	Timpi (s)	Rezultat	Timpi (s)
0	sat	1.8877	sat	7.6219
1	sat	1.7377	sat	7.638
2	sat	1.7808	sat	7.6334
3	sat	1.9051	sat	7.6266
4	sat	1.8577	sat	7.6384
5	unknow	6425.9012	unknow	421.8103
6	unknow	5893.2110	unknow	540.0023
...	...	...	...	...
35	timeout	2705.6367	timeout	492.7604
...	...	...	...	...
44	sat	13.1659	unsat	5.9352

Figure: α-β CROWN & VNN-COMP 2023

idx	NeuralSAT		VNN-COMP 2023	
	Rezultat	Timpi (s)	Rezultat	Timpi (s)
0	sat	0.6525	unknow	13.0525
1	sat	0.6466	unknow	12.9815
2	sat	0.6792	unknow	13.0032
3	sat	0.6176	unknow	13.0058
...	...	...	...	...
41	sat	2.3902	sat	5.8161
42	sat	2.3903	sat	5.8391
43	sat	2.3945	sat	5.8242
44	sat	2.3547	unsat	4.9611

Figure: NeuralSAT & VNN-COMP 2023

Concluzii

- Evaluarea performanței celor două tool-uri
- Interpretarea și compararea rezultatelor obținute

Demo

Figure: Demo-ul pentru cele două tool-uri

Membrii echipei

- Hasan Majd
- Chira Andreea
- Hasna Diana
- Chera Denis
- Vanciu Cătălin

Vă mulțumim pentru atenția acordată!