



UNIVERSITATEA DE VEST DIN TIMIȘOARA
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
PROGRAMUL DE STUDII DE MASTER:
Securitate cibernetică

Traffic Sign Recognition

Supervizor:

Lect. Dr. Mădălina Erașcu

Studenti:

Andreea Bîra-Negrut

Bogdan Pinghireac

Eduard Marian Neguriță

Larisa Drăgănescu

Abstract

Acest studiu explorează performanța și robustețea rețelelor neuronale în recunoașterea semnelor de circulație. În detalierea rezultatelor experimentale, raportul abordează, de asemenea, instrumentele utilizate și provocările întâmpinate în procesul lor de instalare.

Contents

1	Introducere	4
2	Dataset	4
3	Instalare Tool-uri	4
3.1	Alpha Beta Crown	4
3.1.1	Introducere	4
3.1.2	Instalare	5
3.2	Marabou	6
3.2.1	Introducere	6
3.2.2	Instalare	6
4	Rulare benchmark	8
4.1	Alpha Beta Crown	8
4.2	Marabou	9
5	Rezultate	10
6	Concluzie	12
7	Bibliografie	12

1 Introducere

Rețelele neuronale profunde au adus o transformare semnificativă în modul în care interacționăm cu tehnologia în viața de zi cu zi. Acestea au devenit un factor determinant în domenii precum mașinile autonome, smartphone-uri, jocuri, drone etc., marcând o schimbare fundamentală în modul în care sistemele complexe sunt create și utilizate. Capacitatea lor de a învăța modele complexe din seturi de date și de a face prognoze sau decizii în funcție de acestea le face o unealtă valoroasă în domeniile menționate și în multe altele.

Algoritmii Alpha-Beta-Crown și Marabou reprezintă instrumente și structuri de verificare folosite în contextul evaluării rețelelor neuronale. Acești algoritmi au scopul de a furniza analize detaliate ale modului în care rețelele neuronale se comportă și de a aborda provocările asociate testării acestora.

2 Dataset

Traffic Signs Recognition[2][3][5] este folosit pentru a automatiza recunoașterea semnelor de circulație și este deosebit de important în sistemele avansate de asistență. Aceasta reprezintă o problemă complexă în domeniul viziunii artificiale și recunoașterii modelelor.

Setul de date conține peste mii de imagini care reprezintă diferite semne de circulație. Aceste imagini reflectă variații semnificative în aspectul vizual al semnelor, din cauza factorilor precum distanța, iluminarea, condițiile meteorologice, obstrucții parțiale și unghiurile de rotație. Fiecare imagine este însoțită de mai multe seturi de caracteristici pre-calculate, ceea ce facilitează utilizarea algoritmilor de învățare automată fără a fi nevoie de cunoștințe avansate în prelucrarea imaginilor.

Setul de date cuprinde 43 de clase, a căror frecvențe nu sunt echilibrate. Participanții la benchmark au de clasificat două seturi de testare, fiecare conținând peste 12.000 de imagini.

3 Instalare Tool-uri

3.1 Alpha Beta Crown

GitHub: <https://github.com/Verified-Intelligence/alpha-beta-CROWN>

3.1.1 Introducere

Alpha Beta Crown sau α, β -Crown[6] este un tool care verifica o rețea neuronală construit pe un cadru care utilizează propagarea liniară legată și tehnici de ramificare legate.

Tool-ul este foarte eficient dacă este folosit cu un GPU deoarece are mai multe resurse decât un CPU și astfel execuția este mult mai rapidă. De asemenea se poate scala în mod eficient la rețele convoluționale de dimensiuni semnificative, inclusiv cele cu milioane de parametri.

Este compatibil cu o varietate extinsă de arhitecturi de rețele neuronale, cum ar fi CNN, ResNet și diferite funcții de activare, datorită bibliotecii versatile auto_LiRPA[7]

dezvoltate de aceeași echipă.

auto_LiRPA reprezintă o bibliotecă pentru derivarea și calcularea automată a limitelor folosind analiza perturbațiilor bazată pe relaxare liniară (LiRPA) pentru rețelele neuronale, fiind o unealtă utilă pentru verificarea formală a robusteții.

Algoritmul LiRPA folosește de asemenea un algoritm de graf pe grafuri computaționale generale definite prin intermediu PyTorch.

α, β -Crown este castigatorul în competițiile VNN-COMP (International Verification of Neural Networks Competition), din anul 2021, 2022 și 2023, obținând cel mai bun scor total și depășind semnificativ alte tool-uri de verificare a rețelelor neuronale pe o gamă extinsă de peste 2 ani.

3.1.2 Instalare

Pentru instalare avem nevoie de un sistem de operare Linux (noi am ales WLS prezent în Windows) și următoarele programe instalate, altfel se pot genera erori:

- git
- unzip
- nvidia driver
- cuda tool-kit
- anaconda sau miniconda conform documentației alpha-beta-CROWN

Primul pas este clonarea repository folosind următoarele comenzi:

```
git clone git@github.com:Verified-Intelligence/alpha-beta-CROWN.git
cd alpha-beta-CROWN
git clone git@github.com:Verified-Intelligence/auto_LiRPA.git
```

Dupa clonare trebuie creat environment-ul general folosind următoarele comenzi

```
conda env create -f complete_verifier/environment.yaml --name alpha-beta-crown
```

```
conda activate alpha-beta-crown
```

Dupa acest pas se rulează următoarele comenzi:

```
cd auto_LiRPA
python setup.py install
```

Dupa terminarea instalării am încercat un exemplu prezent în repository și anume cifar_resnet_2b.yaml.

```
cd complete_verifier
python abcrown.py --config exp_configs/tutorial_examples/cifar_resnet_2b.yaml
```

Dupa testarea unui exemplu am trecut la instalarea benchmark-ului[1] folosind următoarele comenzi:

```
git ../..
git clone git@github.com:ChristopherBrix/vnncomp2023_benchmarks.git
cd vnncomp2023_benchmarks
sh setup.sh
```

Dupa acest pas se poate trece la rularea benchmark-ului.

```

BaB round 15
batch: 1120
Average branched neurons at iteration 15: 1.0000
splitting decisions:
split level 0: [/25, 949] [/25, 949] [/25, 940] [/25, 949] [/28, 372] [/19, 52] [/25, 572] [/28, 372] [/25, 572]
pruning_in_iteration open status: True
ratio of positive domain = 786 / 2240 = 0.3508928571428571
pruning-in-iteration extra time: 0.02131342887878418
Time: prepare 1.0932 bound 1.0953 transfer 0.0091 finalize 0.4021 func 2.5999
Accumulated time: func 15.0670 prepare 4.4163 bound 8.7559 transfer 0.0586 finalize 1.7663
Current worst splitting domains lb-rhs (depth):
-0.13904 (23), -0.13604 (23), -0.13601 (23), -0.13433 (23), -0.13363 (23), -0.13287 (23), -0.13264 (23), -0.13191 (23), -0.13126 (23),
-0.12629 (23), -0.12507 (23), -0.12390 (23), -0.12290 (23), -0.12144 (23), -0.12131 (23),
length of domains: 1454
Time: pickout 0.0078 decision 1.8045 set_bounds 0.8594 solve 2.6013 add 0.0388
Accumulated time: pickout 0.0744 decision 8.5311 set_bounds 3.6271 solve 15.0734 add 0.3502
Current (lb-rhs): -0.1390395164489746
6327 domains visited
Cumulative time: 27.725351095199585

```

Figure 1:

3.2 Marabou

3.2.1 Introducere

Marabou este o unealtă bazată pe teoria satisfacției constrângerilor (SMT) care poate răspunde la întrebări legate de proprietățile unei rețele, transformând aceste întrebări în probleme de satisfacție a constrângerilor. Designul Marabou este conceput pentru a furniza o platformă robustă și eficientă pentru verificarea și analiza rețelelor neuronale profunde.

Marabou tratează fiecare neuron ca o variabilă și caută o atribuire a acestor variabile care să respecte atât constrângerile liniare, cât și cele non-liniare ale interogării. Se concentrează pe o reprezentare eficientă a acestor variabile și constrângeri.

Pentru a garanta că procesul de verificare este rapid și eficient, Marabou folosește un algoritm de căutare eficient, capabil să găsească soluții care să satisfacă toate constrângerile date.

Marabou este proiectat pentru a avea o performanță optimă în timpul procesului de verificare, concentrându-se pe minimizarea timpului de execuție și pe gestionarea eficientă a resurselor de calcul disponibile. Marabou reprezintă o resursă valoroasă pentru cei implicați în verificarea și analiza rețelelor neuronale profunde.

3.2.2 Instalare

În această secțiune vom detalia procesul de instalare al tool-ului Marabou[4]. Pentru a pregăti instalarea rulăm următoarele comenzi:

```

sudo apt install cmake
sudo apt-get update && sudo apt-get install build-essential
git clone git@github.com:NeuralNetworkVerification/Marabou.git
cd Marabou
mkdir build
cd build
cmake ..

```

În cazul în care aveți următoarea problemă:

```

(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou/build$ cmake ..
-- The C compiler identification is GNU 11.4.0
-- The CXX compiler identification is unknown
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Check for working C compiler: /usr/bin/cc - skipped
-- Detecting C compile features
-- Detecting C compile features - done
CMake Error at CMakeLists.txt:2 (project):
  No CMAKE_CXX_COMPILER could be found.

  Tell CMake where to find the compiler by setting either the environment
  variable "CXX" or the CMake cache entry CMAKE_CXX_COMPILER to the full path
  to the compiler, or to the compiler name if it is in the PATH.

-- Configuring incomplete, errors occurred!
See also "/home/vf/VF/Marabou/build/CMakeFiles/CMakeOutput.log".
See also "/home/vf/VF/Marabou/build/CMakeFiles/CMakeError.log".
(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou/build$ |

```

Figure 2: Eroare

Rulati urmatoarea comanda:

sudo apt-get update && sudo apt-get install build-essential

Dupa se executa urmatoarele comenzi pentru a da build la tool-ul Marabou[4]:

cd build

cmake --build .

Daca toate comenzile au fost executate corect trebuie sa ajungeti la pasul din poza urmatoare:

```

(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou/build$ cmake --build .
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/tools/onnx-1.12.0/onnx.proto3.pb.cc.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/deps/CVC4/context/context.cpp.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/deps/CVC4/context/context_mm.cpp.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/deps/CVC4/base/check.cpp.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/deps/CVC4/base/exception.cpp.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/deps/CVC4/base/output.cpp.o
[ 0%] Building CXX object CMakeFiles/MarabouHelper.dir/src/common/real/CommonReal.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/common/real/Errno.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/common/real/FileFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/real/ConstraintMatrixAnalyzerFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/real/CostFunctionManagerFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/real/ProjectedSteepestEdgeFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/real/RowBoundTightenerFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/real/TableauFactory.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/configuration/GlobalConfiguration.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/configuration/OptionParser.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/configuration/Options.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/AbsoluteValueConstraint.cpp.o
[ 1%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/BilinearConstraint.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/BlandsRule.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/BoundManager.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/CDSmtCore.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/ConstraintMatrixAnalyzer.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/CostFunctionManager.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/DantzigRule.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/DegradationChecker.cpp.o
[ 2%] Building CXX object CMakeFiles/MarabouHelper.dir/src/engine/DisjunctionConstraint.cpp.o

```

Figure 3: Build

4 Rulare benchmark

4.1 Alpha Beta Crown

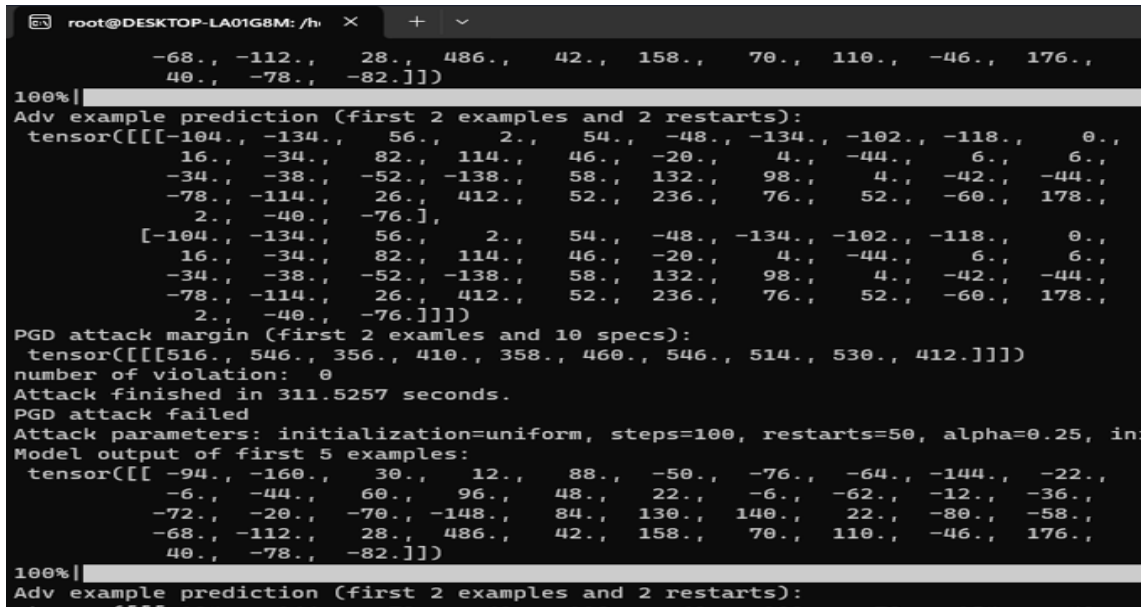
Dupa finalizarea instalarii tool-urilor avem instalat tot mediul de lucru pentru a putea rula tool-ul alpha_beta_crown.

Pentru rulare putem opta pentru rulare prin GPU sau prin CPU, noi am ales GPU pentru ca are putere de calcul mai mare. (pentru rulare prin CPU se adauga urmatorul argument **-device CPU** la comanda de executie)

Comenzile pentru rulare sunt urmatoarele:

```
cd alpha-beta-CROWN/complete_verifier
```

```
python abcrown.py -config exp configs/vnncomp23/gtrsb.yam
```



```
root@DESKTOP-LA01G8M: /h/ X + v
-68., -112., 28., 486., 42., 158., 70., 110., -46., 176.,
40., -78., -82.]]]
100%|
Adv example prediction (first 2 examples and 2 restarts):
tensor([[[[-104., -134., 56., 2., 54., -48., -134., -102., -118., 0.,
16., -34., 82., 114., 46., -20., 4., -44., 6., 6.,
-34., -38., -52., -138., 58., 132., 98., 4., -42., -44.,
-78., -114., 26., 412., 52., 236., 76., 52., -60., 178.,
2., -40., -76.],
[-104., -134., 56., 2., 54., -48., -134., -102., -118., 0.,
16., -34., 82., 114., 46., -20., 4., -44., 6., 6.,
-34., -38., -52., -138., 58., 132., 98., 4., -42., -44.,
-78., -114., 26., 412., 52., 236., 76., 52., -60., 178.,
2., -40., -76.]]]])
PGD attack margin (first 2 examples and 10 specs):
tensor([[[516., 546., 356., 410., 358., 460., 546., 514., 530., 412.]]])
number of violation: 0
Attack finished in 311.5257 seconds.
PGD attack failed
Attack parameters: initialization=uniform, steps=100, restarts=50, alpha=0.25, in
Model output of first 5 examples:
tensor([[ -94., -160., 30., 12., 88., -50., -76., -64., -144., -22.,
-6., -44., 60., 96., 48., 22., -6., -62., -12., -36.,
-72., -20., -70., -148., 84., 130., 140., 22., -80., -58.,
-68., -112., 28., 486., 42., 158., 70., 110., -46., 176.,
40., -78., -82.]]])
100%|
Adv example prediction (first 2 examples and 2 restarts):
```

Figure 4:

La finalul executiei se va genera un fisier out.txt care contine rezultatul executiei in format binar dupa cum se poate observa in figura urmatoare:

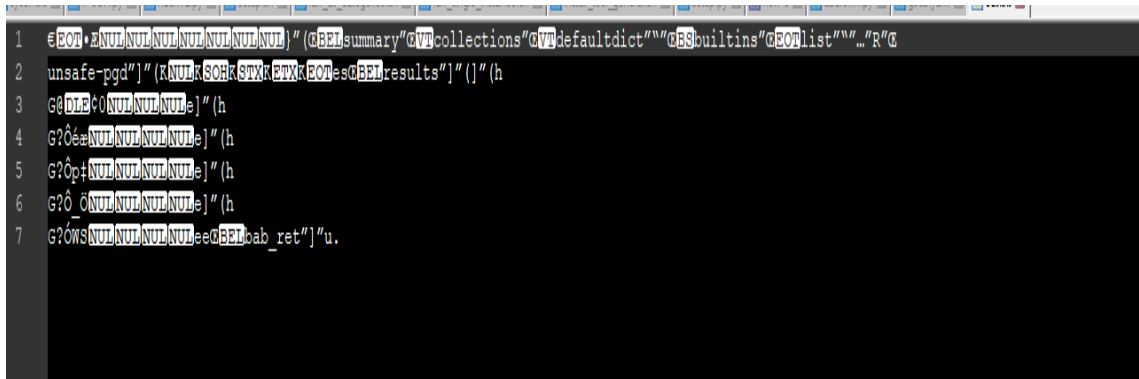


Figure 5:

4.2 Marabou

Dupa finalizarea build-ului, trebuie sa aveti urmatorul status daca build-ul a fost cu succes:

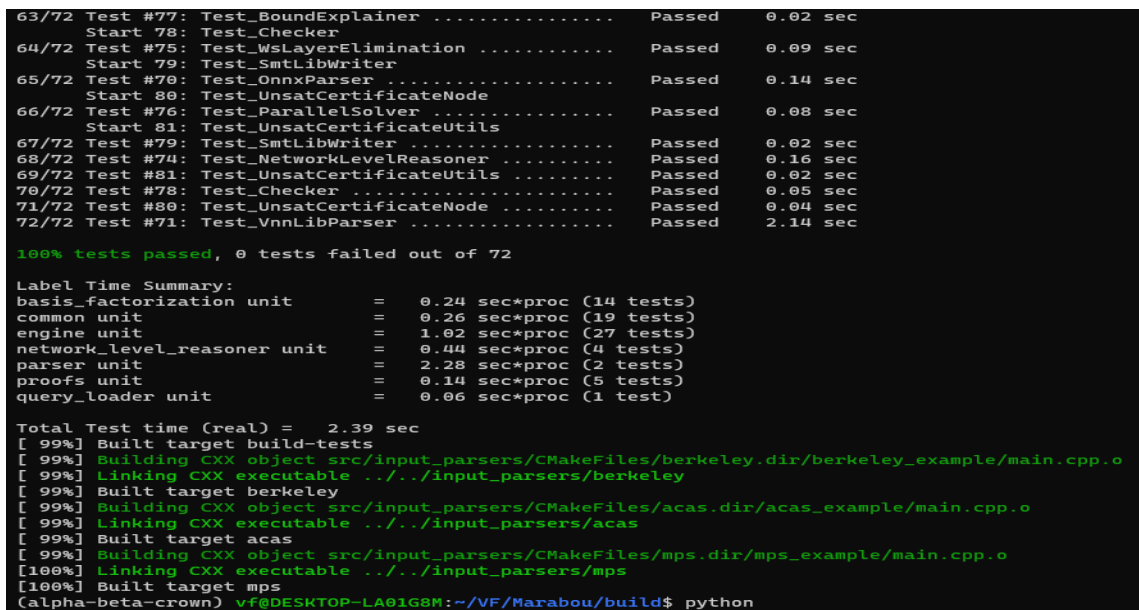


Figure 6: Final build

Apoi putem trece la rularea Marabou folosind urmatoarele comenzi:
`./build/Marabou resources/nnet/acasxu/ACASXU_experimental_v2a_2_7.nnet
resources/properties/acas_property_3.txt`

```
(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou$ ./build/Marabou resources/nnet/acasxu/ACASXU_experimental_v2a_2_7.nnet resources/properties/acas_property_3.txt
Network: resources/nnet/acasxu/ACASXU_experimental_v2a_2_7.nnet
Number of layers: 8. Input layer size: 5. Output layer size: 5. Number of ReLUs: 300
Total number of variables: 610
Property: resources/properties/acas_property_3.txt

Engine::processInputQuery: Input query (before preprocessing): 309 equations, 610 variables
Engine::processInputQuery: Input query (after preprocessing): 609 equations, 838 variables

Input bounds:
  x0: [ -0.3035, -0.2986]
  x1: [ -0.0095,  0.0095]
  x2: [  0.4934,  0.5000]
  x3: [  0.3000,  0.5000]
  x4: [  0.3000,  0.5000]

Branching heuristics set to LargestInterval
unsat
(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou$
```

Figure 7: Run Marabou

5 Rezultate

Alpha Beta Crown

Rezultatele obținute arată că din cele 46 de instanțe, 42 au fost clasificate ca sigure, iar doar instanța 45 a fost clasificată ca nesigură. Pentru instanțele 6 și 35, rezultatul a fost "run_instance_timeout", iar instanța 5 a obținut "no_result_in_file". Cele 42 de instanțe au valoarea "sat", fiind satisfiabile, astfel încât instanțele au reușit să satisfacă expresiile logice pentru ca problema să fie considerată rezolvată si pentru a găsi o soluție validă.

idx	Rezultat	Timpi(s)
0	sat	7.157972967
1	sat	7.286744442
2	sat	6.850318482
3	sat	7.472602460
4	sat	6.911085371
5	no_result_in_file	460.654262260
6	run_instance_timeout	540.033374469
7	sat	19.430611468
8	sat	7.768919104
9	sat	7.433775311
10	sat	7.918002813
11	sat	7.321949306
12	sat	7.205714470
13	sat	7.728228881
14	sat	7.777620317
15	sat	8.973640245
16	sat	7.840924381
17	sat	7.467596722
18	sat	8.919894638
19	sat	7.409615798
20	sat	7.674657312
21	sat	7.536734055
22	sat	7.530943546
23	sat	7.643930597
24	sat	7.925060305
25	sat	7.649686196
26	sat	7.522822988
27	sat	7.749032502
28	sat	7.893192003
29	sat	7.275387435
30	sat	8.904811028
31	sat	8.852287157
32	sat	8.927887925
33	sat	16.933491927
34	sat	16.378010803
35	run_instance_timeout	540.002000284
36	sat	11.136481450
37	sat	9.845497913
38	sat	9.480329464
39	sat	9.572339116
40	sat	8.855822936
41	sat	9.365495261
42	sat	8.925496347
43	sat	17.016346806
44	sat	8.997252323
45	unsat	6.135465521

Marabou

```
(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou$ ./build/Marabou resources/nnet/acasxu/ACASXu_experimental_v2a_2_7.nnet resources/properties/acas_property_3.txt
Network: resources/nnet/acasxu/ACASXu_experimental_v2a_2_7.nnet
Number of layers: 8. Input layer size: 5. Output layer size: 5. Number of ReLUs: 300
Total number of variables: 610
Property: resources/properties/acas_property_3.txt

Engine::processInputQuery: Input query (before preprocessing): 309 equations, 610 variables
Engine::processInputQuery: Input query (after preprocessing): 609 equations, 838 variables

Input bounds:
  x0: [ -0.3035, -0.2986]
  x1: [ -0.0095,  0.0095]
  x2: [  0.4934,  0.5000]
  x3: [  0.3000,  0.5000]
  x4: [  0.3000,  0.5000]

Branching heuristics set to LargestInterval
unsat
(alpha-beta-crown) vf@DESKTOP-LA01G8M:~/VF/Marabou$
```

Figure 8: Marabou

6 Concluzie

În concluzie, este esențial să continuăm să dezvoltăm și să îmbunătățim instrumentele de verificare pentru a face față noilor provocări generate de evoluția tehnologiei. Această abordare continuă este crucială pentru a ne asigura că sistemele de recunoaștere a semnelor de circulație devin tot mai precise, mai sigure și mai eficiente.

Contribuția constantă la îmbunătățirea acestor instrumente este esențială pentru a răspunde dinamicii în schimbare a mediului rutier și pentru a promova în mod semnificativ siguranța și eficiența în gestionarea traficului.

7 Bibliografie

References

- [1] Christopher Brix. *ChristopherBrix: vnncomp2023_benchmarks*. URL: https://github.com/ChristopherBrix/vnncomp2023_benchmarks.
- [2] Kaoutar Sefrioui Boujemaa, Ismail Berrada, Afaf Bouhoute, Karim Boubouh. “Traffic sign recognition using convolutional neural networks”. In: *IEEEExplore* (2017). URL: <https://ieeexplore.ieee.org/abstract/document/8238205>.
- [3] Lai Jia Shyan, T H Lim, Dk Norhafizah Pg Hj Muhammad. “Real time road traffic sign detection and recognition systems using Convolution Neural Network on a GPU platform”. In: *IEEEExplore* (2023). URL: <https://ieeexplore.ieee.org/document/10007277>.
- [4] NeuralNetworkVerification. *NeuralNetworkVerification: Marabou*. URL: <https://github.com/NeuralNetworkVerification/Marabou>. (accessed: 23.01.2024).
- [5] Twine AI. “The Best Road Sign Detection Datasets of 2022”. In: *twine* (2022). URL: <https://www.twine.net/blog/road-sign-detection-datasets/>.
- [6] Verified-Intelligence. *Verified-Intelligence: alpha-beta-CROWN*. URL: <https://github.com/Verified-Intelligence/alpha-beta-CROWN>. (accessed: 15.01.2024).

- [7] Verified-Intelligence. *Verified-Intelligence: auto_LiRPA*. URL: https://github.com/Verified-Intelligence/auto_LiRPA. (accessed: 15.01.2024).