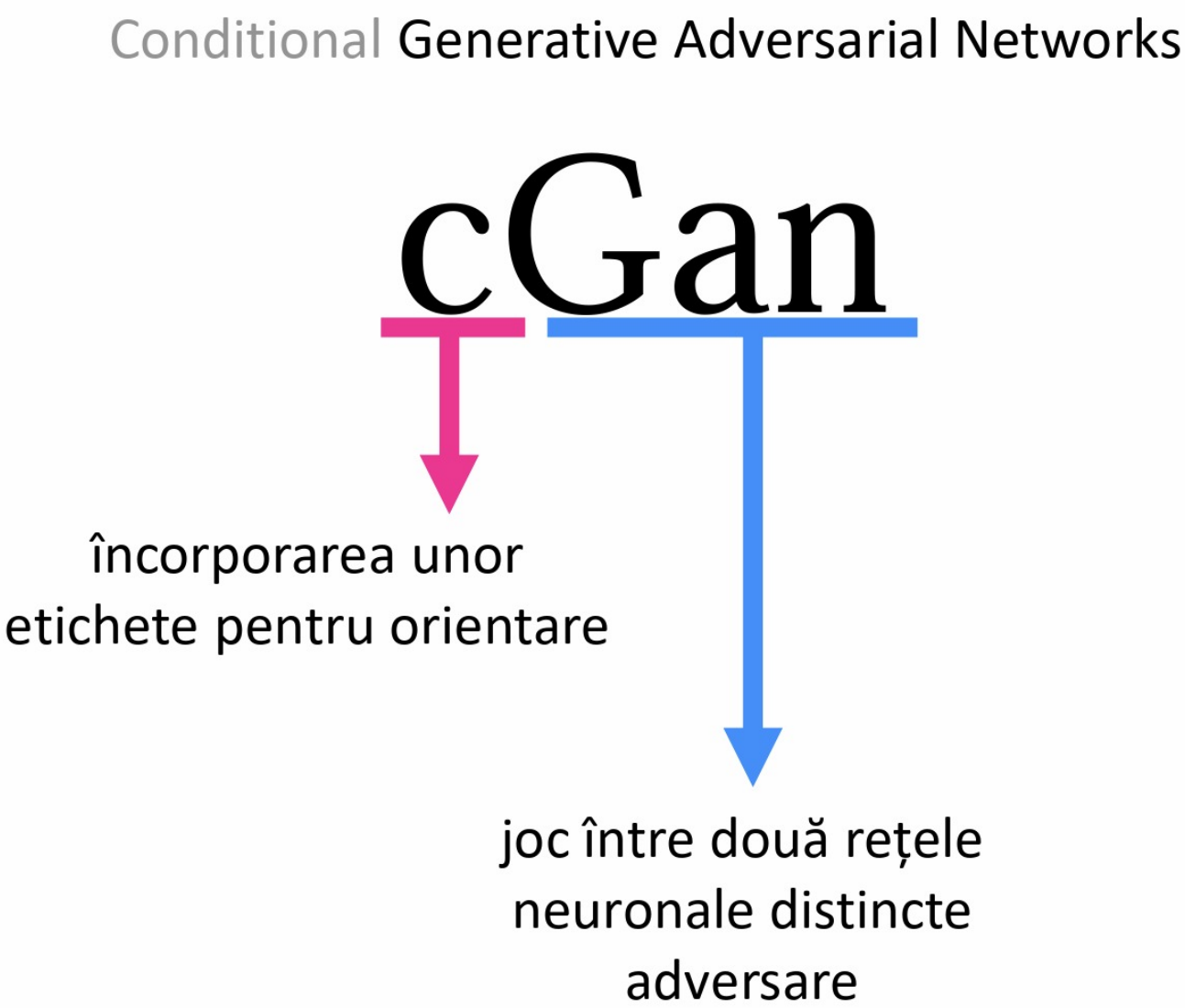
Verificarea rețelelor neuronale folosind alpha-beta-CROWN și NeuralSAT pentru benchmark-ul cGan al competiției VNN-Comp2023

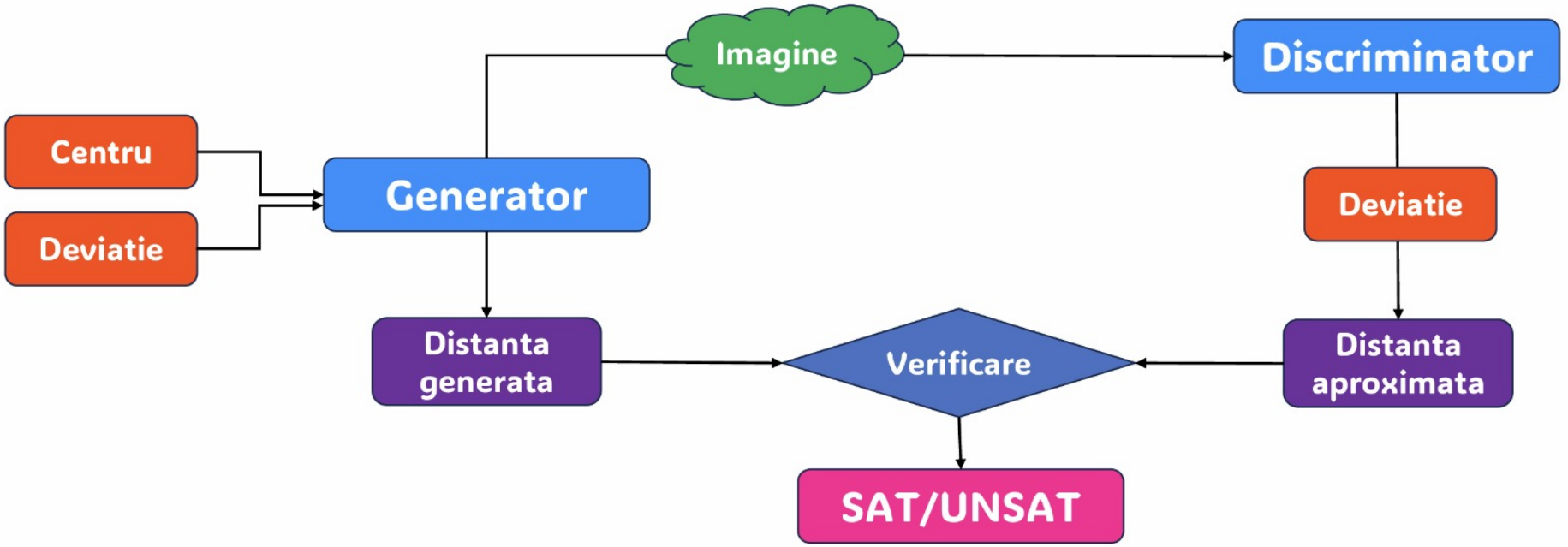
Diaconu Laura
Domșa Emanuel
Laptedulce Anastasia
Morariu Ioana-Alexandra
Romanet Rareș

Cuprins

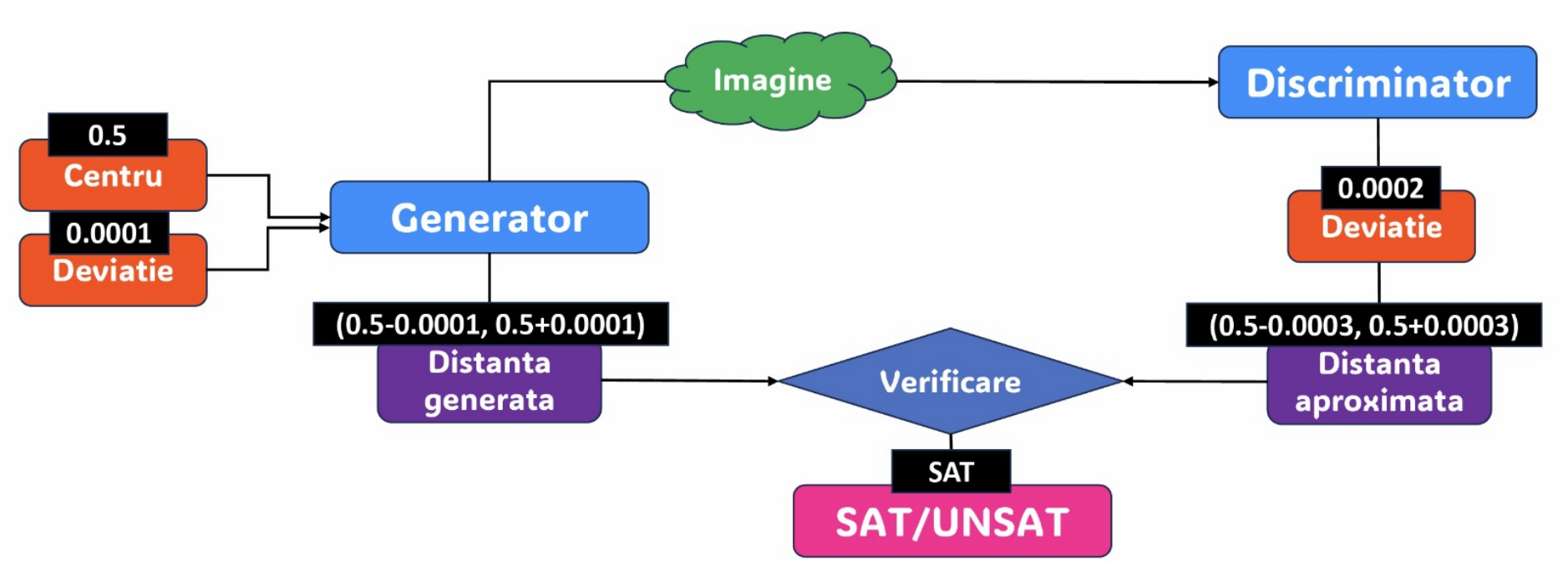
Analiza modului de functionare a retelei neuronale



Analiza modului de functionare a retelei neuronale



Analiza modului de functionare a retelei neuronale



Cuprins

Caracterizarea setului de date

- verificare corectitudine rețele neuronale
- fisiere .onnx
- fisiere .vnnlib
- denumire sugestivă

Caracterizarea setului de date

Figure: Fișierele benchmark-ului cGAN

Caracterizarea setului de date

```
(declare-const X_0 Real)
(declare-const X_1 Real)
(declare-const X_2 Real)
(declare-const X_3 Real)
(declare-const X_4 Real)

(declare-const Y_0 Real)

; Input constraints:
(assert (<= X_0 val_1_X0))
(assert (>= X_0 val_2_X0))

(assert (<= X_1 val_1_X1))
(assert (>= X_1 val_2_X1))

(assert (<= X_2 val_1_X2))
(assert (>= X_2 val_2_X2))

(assert (<= X_3 val_1_X3))
(assert (>= X_3 val_2_X3))

(assert (<= X_4 val_1_X4))
(assert (>= X_4 val_2_X4))

; Output constraints:
(assert (or
    (and (>= Y_0 val_1_Y0))
    (and (<= Y_0 val_2_Y0))
))
```

Figure: Conținut fișier VNNLIB

Cuprins

Instalare si configurare tool-uri

- Alpha-beta-CROWN
- NeuralSAT
- Pași de instalare
- Dificultăți întâlnite la instalare

```
export LD_LIBRARY_PATH=/usr/lib/wsl/lib:$LD_LIBRARY_PATH
```

```
python abcrown.py --config exp_configs/vnncomp23/cgan.yaml
```

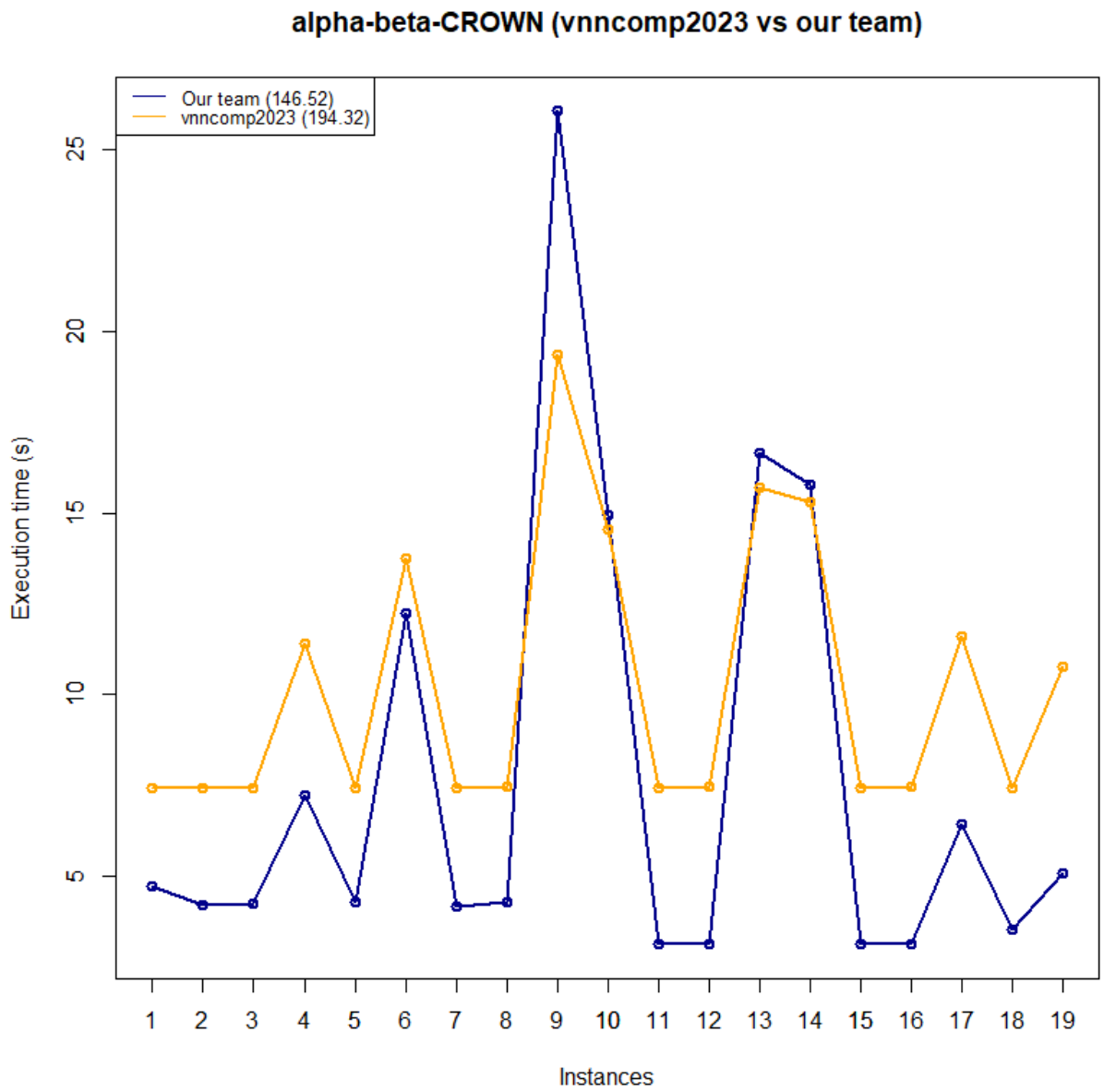
```
python3 main.py --net "cGAN_imgSz32_nCh_3_upsample.onnx" --spec
    "cGAN_imgSz32_nCh_3_upsample_prop_0_input_eps_0.010
    _output_eps_0.015.vnnlib" --result_file result19.txt
    --export_cex--timeout1200
```

Cuprins

Rezultate alpha-beta-CROWN

Benchmark	neural network (ONNX)	specification (VNNLIB)	results (vr	results (us	time to ve	time to ve
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	7.45	4.71
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	7.43	4.23
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	7.44	4.27
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	unsat	unsat	11.41	7.24
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	7.45	4.29
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	unsat	unsat	13.74	12.26
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	7.43	4.19
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	7.47	4.31
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unsat	unsat	19.36	26.06
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unsat	unsat	14.53	14.93
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	7.42	3.12
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	7.46	3.15
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unsat	unsat	15.68	16.66
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unsat	unsat	15.29	15.79
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	7.44	3.15
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	7.47	3.14
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	unsat	unsat	11.61	6.43
cgan	cGAN_imgSz32_nCh_1_	cGAN_imgSz32_nCh_1_	sat	sat	7.45	3.52
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	unsat	unsat	10.79	5.07

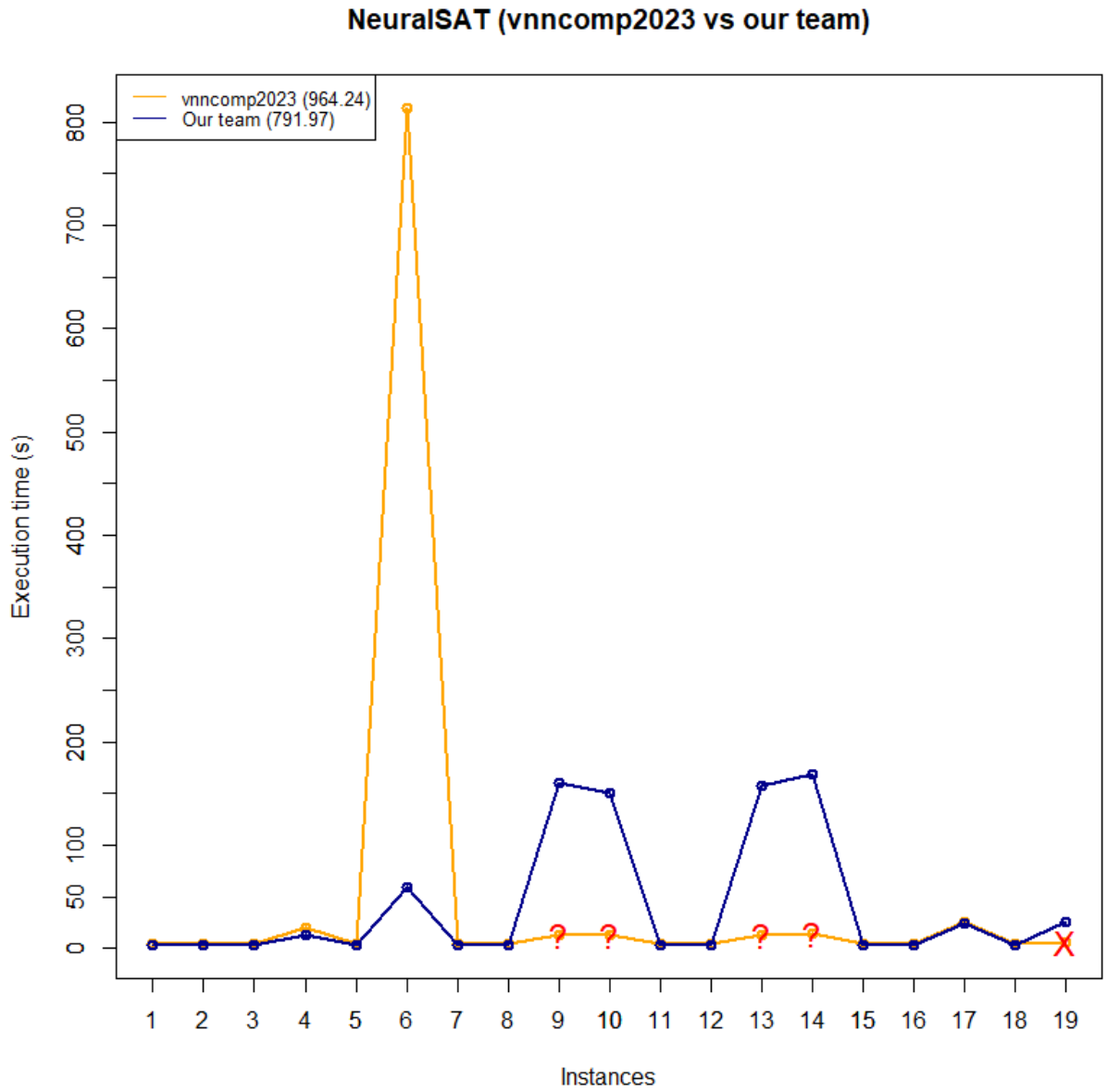
Rezultate alpha-beta-CROWN



Rezultate NeuralSAT

Benchmark	neural network (ONNX)	specification (VNNLIB)	results (vr	results (us	time to ve	time to ve
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.15	2.79
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.11	2.68
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.1	2.7
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	unsat	unsat	20.07	13.74
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.09	2.92
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	unsat	unsat	813.17	59.65
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.06	2.77
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.09	2.88
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unknown	unsat	13.63	159.81
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unknown	unsat	12.82	150.88
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	4.1	3.02
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	4.07	3.01
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unknown	unsat	13.49	157.76
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unknown	unsat	14.1	169.16
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	4.11	3.14
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	4.12	3.26
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	unsat	unsat	25.97	24.09
cgan	cGAN_imgSz32_nCh_1_	cGAN_imgSz32_nCh_1_	sat	sat	4.07	3.11
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	error	unsat	5.87	25.37

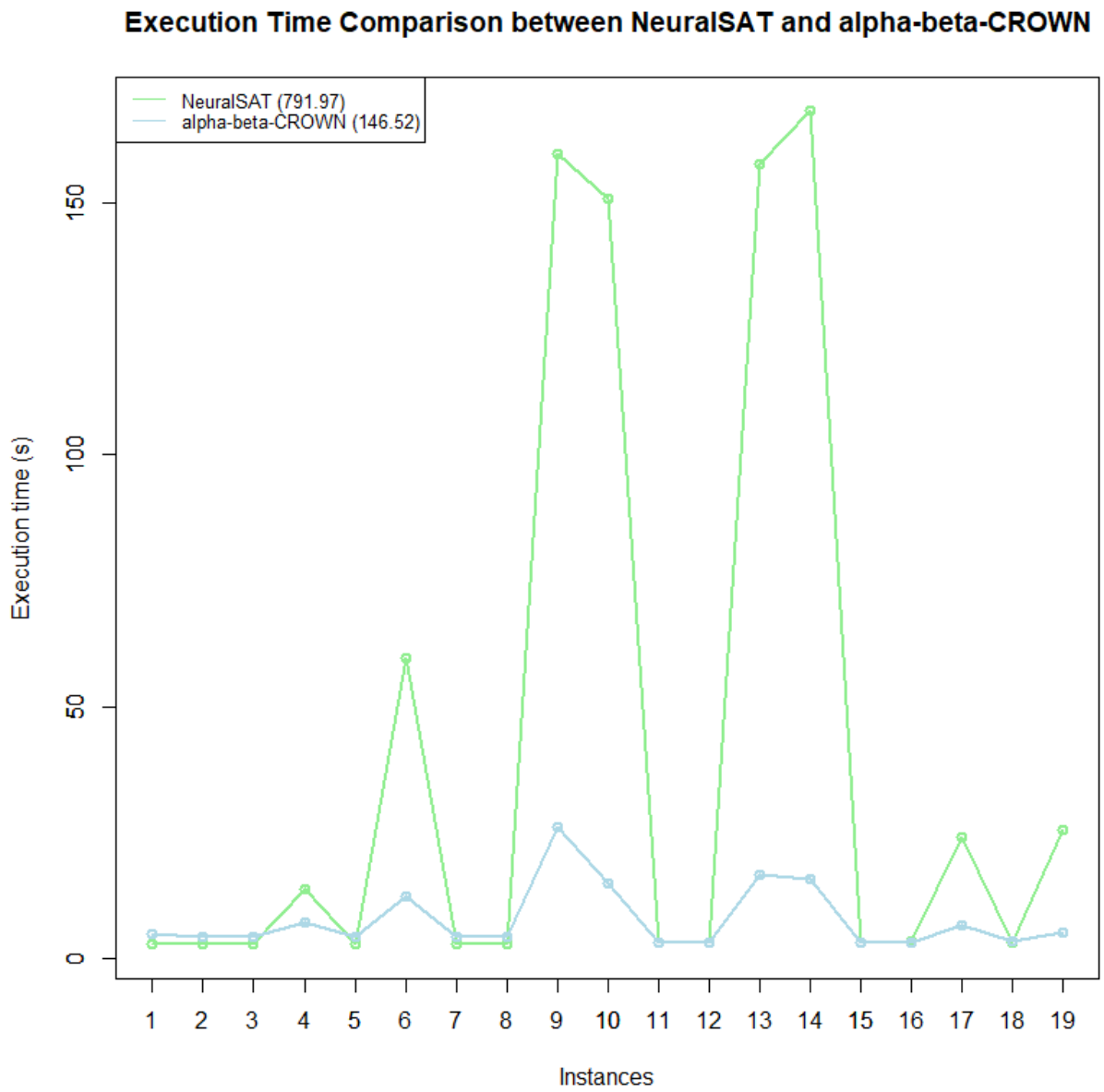
Rezultate NeuralSAT



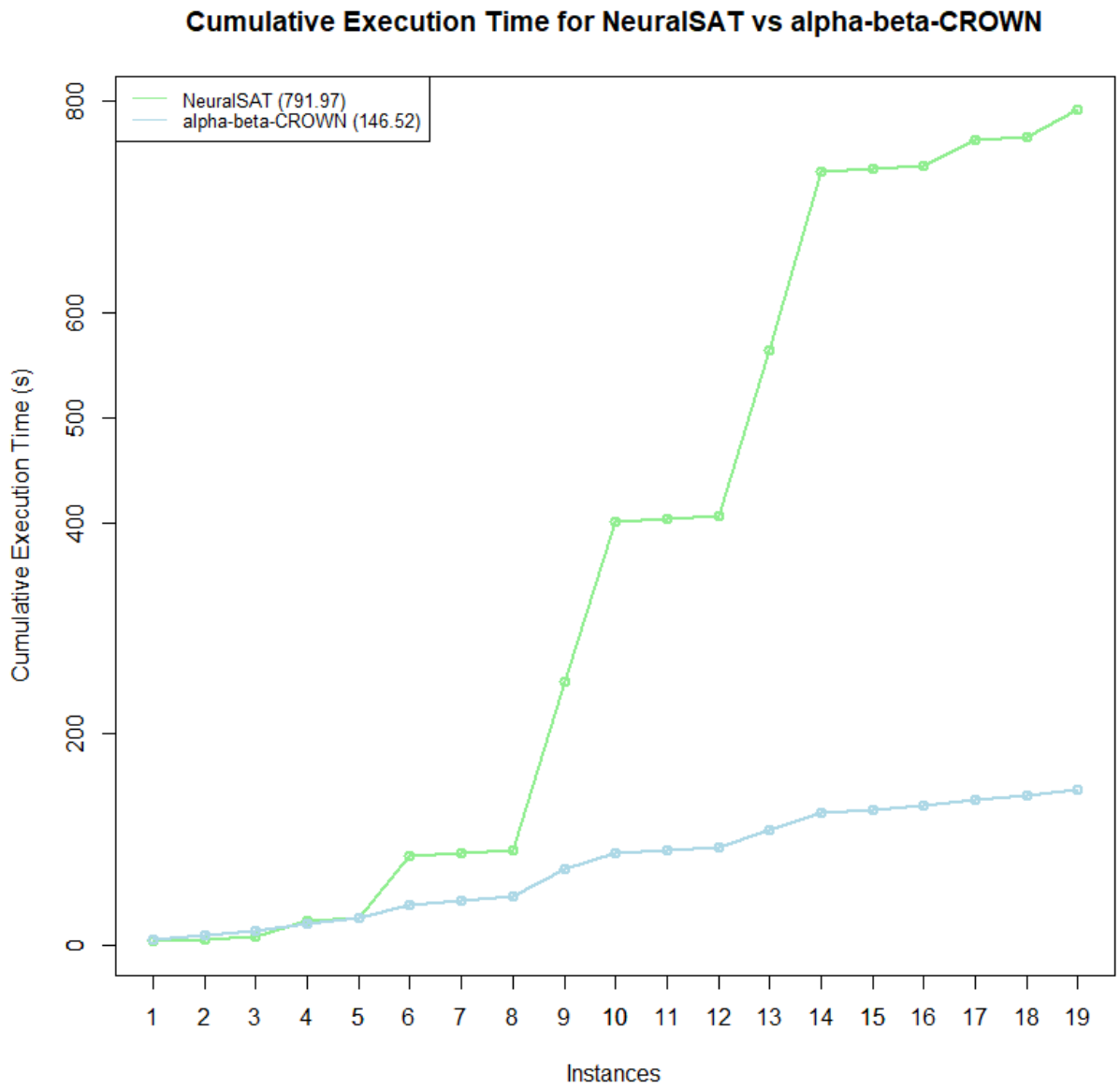
Rezultate alpha-beta-CROWN vs NeuralSAT

Benchmark	neural network (ONNX)	specification (VNNLIB)	alpha-bet	NeuralSA	alpha-bet	NeuralSA
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.71	2.79
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.23	2.68
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	sat	sat	4.27	2.7
cgan	cGAN_imgSz32_nCh_1.c	cGAN_imgSz32_nCh_1_	unsat	unsat	7.24	13.74
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.29	2.92
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	unsat	unsat	12.26	59.65
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.19	2.77
cgan	cGAN_imgSz32_nCh_3.c	cGAN_imgSz32_nCh_3_	sat	sat	4.31	2.88
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unsat	unsat	26.06	159.81
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	unsat	unsat	14.93	150.88
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	3.12	3.02
cgan	cGAN_imgSz64_nCh_1.c	cGAN_imgSz64_nCh_1_	sat	sat	3.15	3.01
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unsat	unsat	16.66	157.76
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	unsat	unsat	15.79	169.16
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	7.44	3.14
cgan	cGAN_imgSz64_nCh_3.c	cGAN_imgSz64_nCh_3_	sat	sat	7.47	3.26
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	unsat	unsat	11.61	24.09
cgan	cGAN_imgSz32_nCh_1_	cGAN_imgSz32_nCh_1_	sat	sat	7.45	3.11
cgan	cGAN_imgSz32_nCh_3_	cGAN_imgSz32_nCh_3_	unsat	unsat	10.79	25.37

Rezultate alpha-beta-CROWN vs NeuralSAT



Rezultate alpha-beta-CROWN vs NeuralSAT



Rezultate

#	Tool	Verified	Falsified	Fastest	Penalty	Score	Percent
1	α-β CROWN	8	11	0	0	190	100%
2	NeuralSAT	8	11	0	0	190	100%

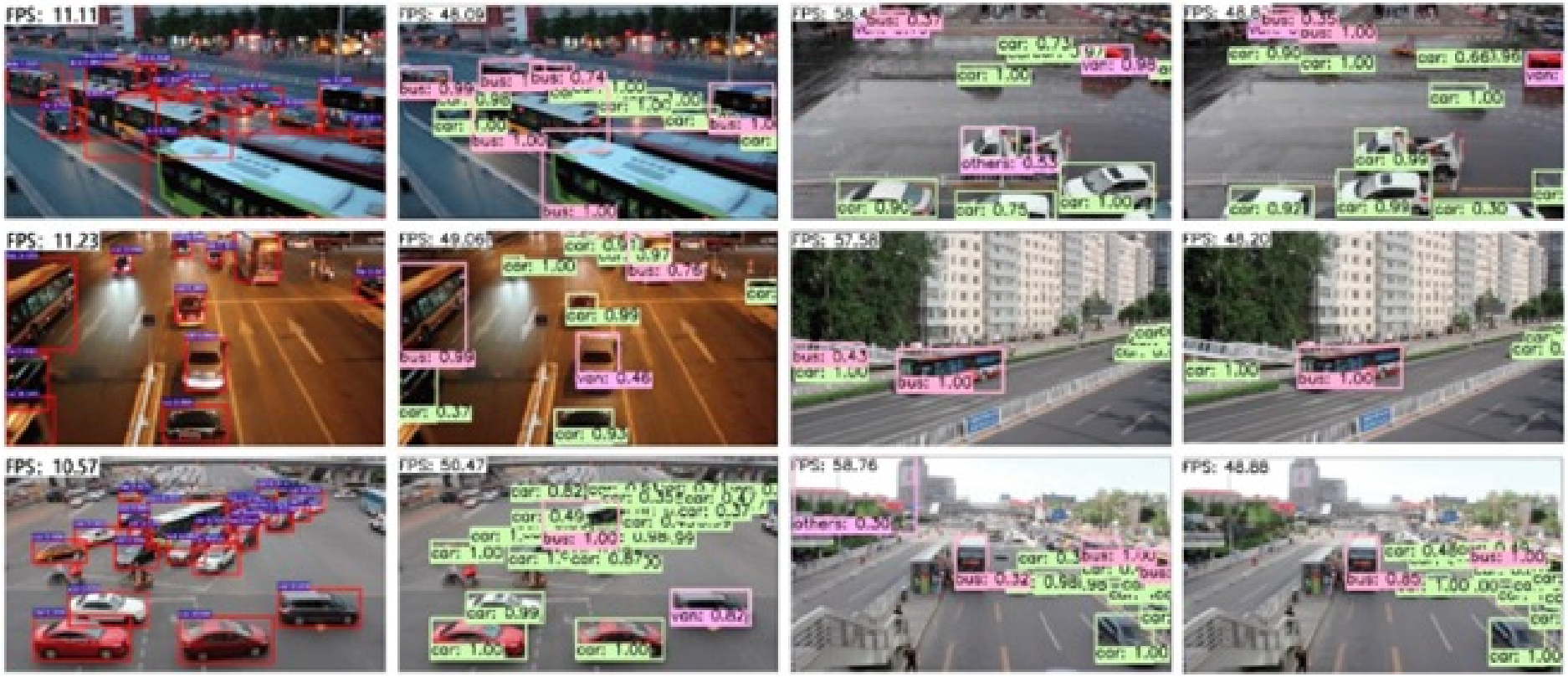
$$\rightarrow \textbf{Verified} \times \textbf{10} + \textbf{Falsified} \times \textbf{10} - \textbf{Penalty} \times \textbf{150}$$

Procentajul reprezintă scorul obținut exprimat ca procent din scorul maxim posibil, oferind o imagine de ansamblu asupra performanței, iar formula de calcul este:

$$\frac{\textbf{Score} \times \textbf{100}}{\textbf{max}(\textbf{Score})}$$

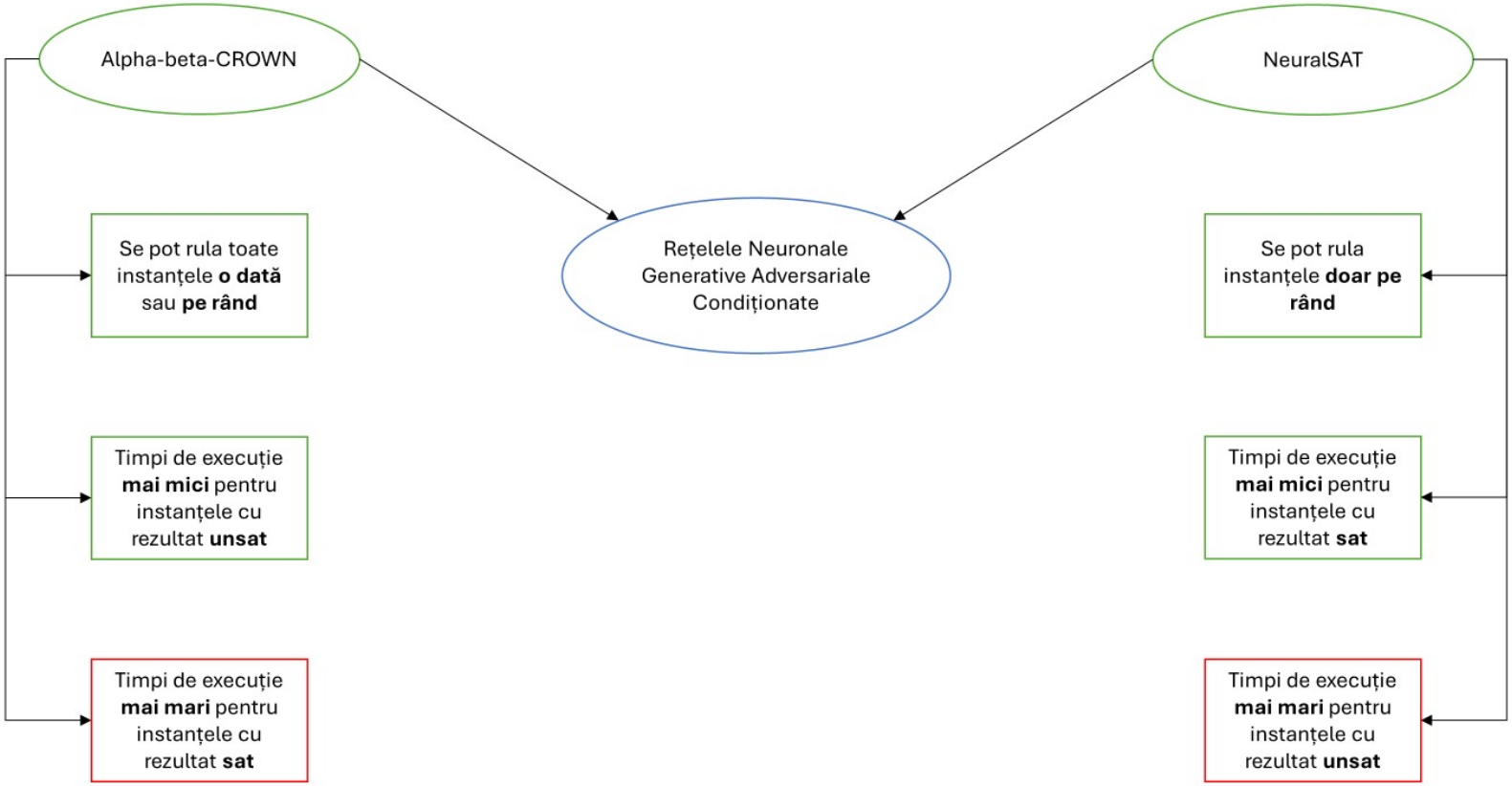
Cuprins

Rețele neuronale în simularea provocarilor reale



Cuprins

Concluzii


Alpha-beta-CROWN
NeuralSAT
Rețelele Neuronale Generative Adversariale Condiționate
Se pot rula toate instanțele **o dată** sau **pe rând**
Timpi de execuție **mai mici** pentru instanțele cu rezultat **unsat**
Timpi de execuție **mai mari** pentru instanțele cu rezultat **sat**
Se pot rula instanțele **doar pe rând**
Timpi de execuție **mai mici** pentru instanțele cu rezultat **sat**
Timpi de execuție **mai mari** pentru instanțele cu rezultat **unsat**