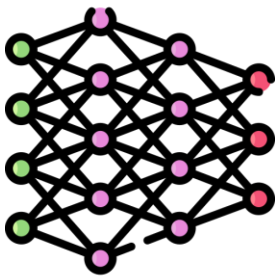
Truth Table Net: Scalable, Compact & Verifiable Neural Networks with a Dual Convolutional Small Boolean Circuit Networks Form

A. Benamira, T. Peyrin, T. Yap, T. Guérand, B. Hooi

Nanyang Technological University

Introduction

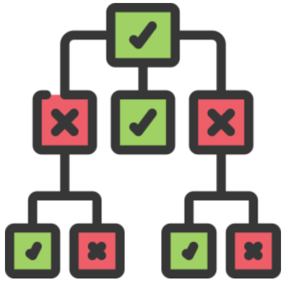
Our findings



Neural Network

A	B	C	Out
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Set of lookup tables



Boolean Circuit

- Scalable
- Performances
- Interpretable
- Verifiable

TTnet

From black box to truth tables

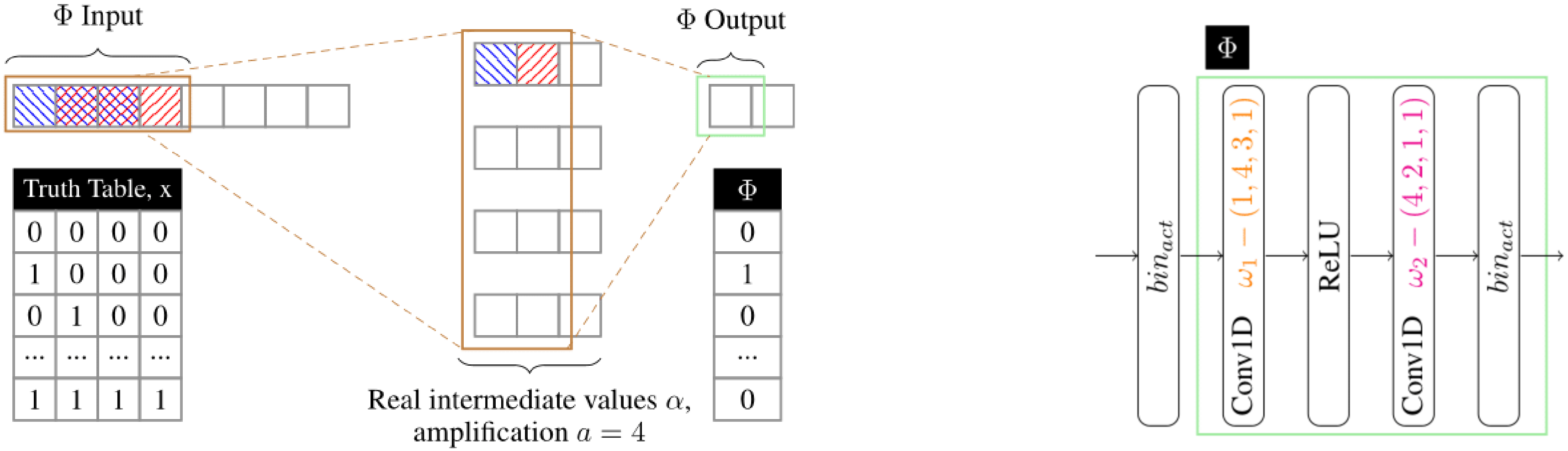


Figure from [4]

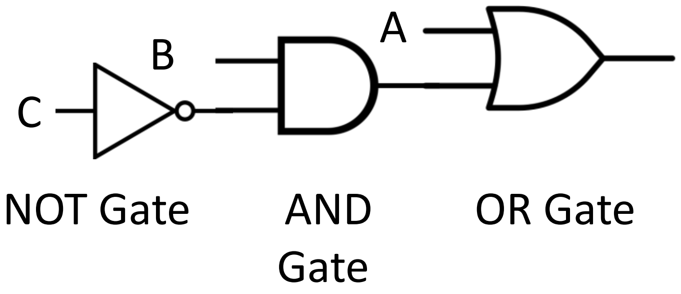
Convolution Filter ⇔ Truth Table

TTnet

From black box to truth tables

What is the most complete, objective, simple form of information?

→ Truth Tables (for discrete at least)



Out = A | (B && ~C)

Out Function Truth Table

A	B	C	Out
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

TTnet

From black box to truth tables

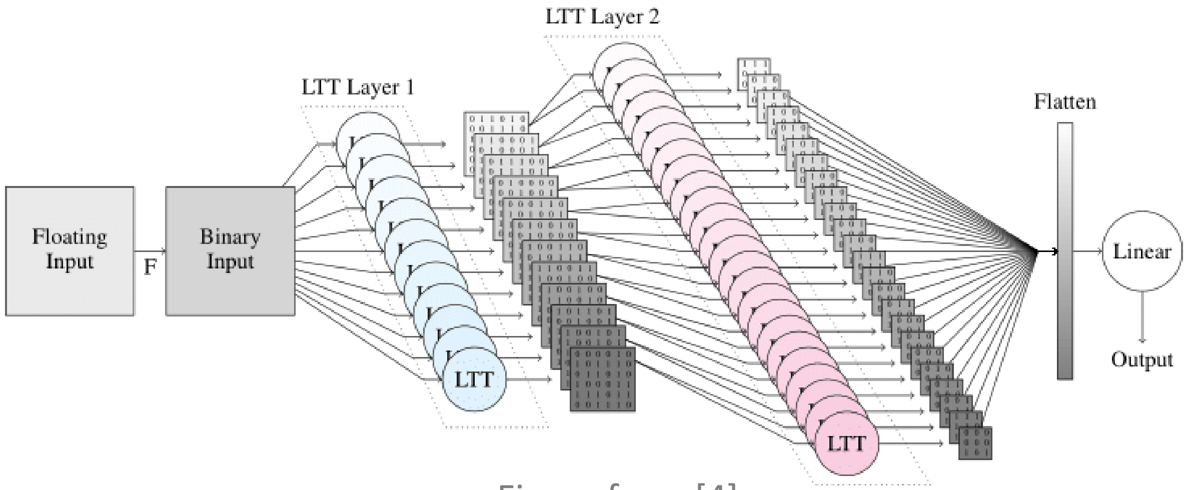


Figure from [4]

- The Neural Network is seen as an aggregate of Truth Tables
- Neural Network ⇔ Truth Tables ⇔ Boolean Expressions
- Scales to ImageNet

RESULTS

TTnet

ImageNet & Cifar-10

$\text{TTnet}_{n-|k}$: input size of *n* , last layer quantized on *k* bits

n refers to the size of the kernel of the CNN Filter: i.e. if *n* = 16, kernel size is (4,4) -> 16 values

Top 1 and Top 5 Acc. Comparison on ImageNet

Accuracy	$\text{TTnet}_{16-\|8}$	**Original BNN**	**XnorNet**
top 1	41.6 % ± 0.6	27.9 %	44.2 %
top 5	65.1 % ± 0.7	50.4 %	69.2 %

Accuracy of $\text{TTnet}_{n-|8}$ on CIFAR-10.

n	24	20	16	12	8	4
Acc.	89.1% ± 0.2	87.8% ± 0.2	86.0% ± 0.3	84.3% ± 0.2	81.2% ± 0.4	77.5% ± 0.4

State of the art accuracy on CIFAR-10, comparable accuracy to first BNNs on ImageNet

TTnet

Complexity on MNIST and CIFAR-10

MNIST		Acc.	# Param.	OPs	FLOPs
Traditional models	Linear Regression	91.60%	4K	(4M)	4K
	Neural Network	98.40%	22.6M	(45G)	45M
Boolean DNNs	Diff Logic Net (small)	97.69%	48K	48K	-
	Diff Logic Net	98.47%	384K	384K	-
	TTnet $_{6-4}$ (small)	97.44%	37K	34K	-
	TTnet $_{6-4}$ (big)	98.32%	203K	188K	-
BNNs	FINN	98.40%	-	5.28M	-
SNNs	M17	98.08%	4K	(8M)	8K
	SET-MLP	98.74%	89.8K	(180M)	180K

CIFAR-10		Acc.	# Param.	OPs	FLOPs
Boolean DNNs	Diff Logic Net (small)	51.27 %	48K	48K	-
	Diff Logic Net (medium)	57.39 %	512K	512K	-
	Diff Logic Net (large)	60.78 %	1.28M	1.28M	-
	Diff Logic Net (large x2)	61.41 %	2.56M	2.56M	-
	Diff Logic Net (large x4)	62.14 %	5.12M	5.12M	
	TTnet $_{6-4}$	50.10 %	565K	565K	-
	TTnet $_{12-4}$	70.75 %	189M	189M	-
	TTnet $_{12-\|4}$	84.63 %	1.2G	1.2G	-
BNNs	H19	91.00%	23.9 M	87.4G	-
SNNs	PBW (ResNet32)	38.64 %	-	(140M)	(140K)
	MLPrune (ResNet32)	36.09 %	-	(140M)	(140K)
	ProbMask (ResNet32)	76.87 %	-	(140M)	(140K)
	SET-MLP	74.84 %	279K	(558M)	558K

Boolean DNNs result in low complexity NN, with TTnet having the best performances

→ Competitive Ops/Performance trade-off

TTnet

Fast Verification

Application of TTnet to complete adversarial robustness verification for low and high noise bounded by l_∞. Comparison to state-of- the-art SAT methods

General DNN verification with α−β-Crown
vs
TTnet with general SAT verification method.

	General DNN + α-β-Crown [Xu *et al.*, 2020] [Wang *et al.*, 2021]		TTnet $_{9-1}$ + General SAT verification pipeline	
	Verif. time (s)	Timeout (%)	Verif. time (s)	Timeout (%)
MNIST	96	13	0.06 (× 1600)	0
CIFAR-10	175	27	0.14 (× 1250)	0

Dataset (noise)	Complete method	Accuracy Verif.	Accuracy Nat.	Verif. time (s)	Timeout
MNIST (ϵ_{test} = 0.1)	TTnet $_{9-1}$	**95.12%**	98.33%	**0.012**	0
	JR20	91.68%	97.46%	0.1115	0
	N+19 *	20.00%	96.00 %	5	0
MNIST (ϵ_{test} = 0.3)	TTnet $_{9-1}$	66.24%	97.43 %	**0.065**	0
	JR20	**77.59%**	96.36%	0.1179	0
CIFAR-10 (ϵ_{test} = 2/255)	TTnet $_{9-1}$	**32.32%**	49.23%	**0.06**	0
	JR20	30.49%	47.35%	0.1750	0
CIFAR-10 (ϵ_{test} = 8/255)	TTnet $_{9-1}$	21.08%	31.13%	**0.04**	0
	JR20	**22.55%**	35.00%	0.1781	0

* *results given on the first 1K images of the test set. Moreover, the authors only authorize a maximum of 20 pixels to switch.*

A Boolean circuit is very SAT-friendly, resulting in **ultra fast verification times**

TTnet

Limitations

TTnet has the following limitations:

1) Small size of inputs: $n < 25$ to allow Quine McClusky algorithm to find equivalent Boolean equations
2) First Layer with high bit-bandwidth is needed for large datasets (CIFAR-10, ImageNet)
3) Binarization results in a big loss of information

But we have the following advantages:

1) Very compact CNN
2) Low computational inference cost
3) Very fast verification times
4) Competitive accuracy on datasets smaller than ImageNet → fine for most real life use cases

Contact us for collaborations:
guer0001@e.ntu.edu.sg, thomas.peyrin@ntu.sg