MpBP: Verifying Robustness of Neural Networks with Multi-path Bound Propagation

Ye ZHENG, Jiaxiang LIU, and Xiaomu SHI

深圳大学
SHENZHEN UNIVERSITY

Neural Network Verification

- Verifies whether a region input results in unsafe outputs
- Difficulty: the composition of non-linear activations (e.g. ReLU)

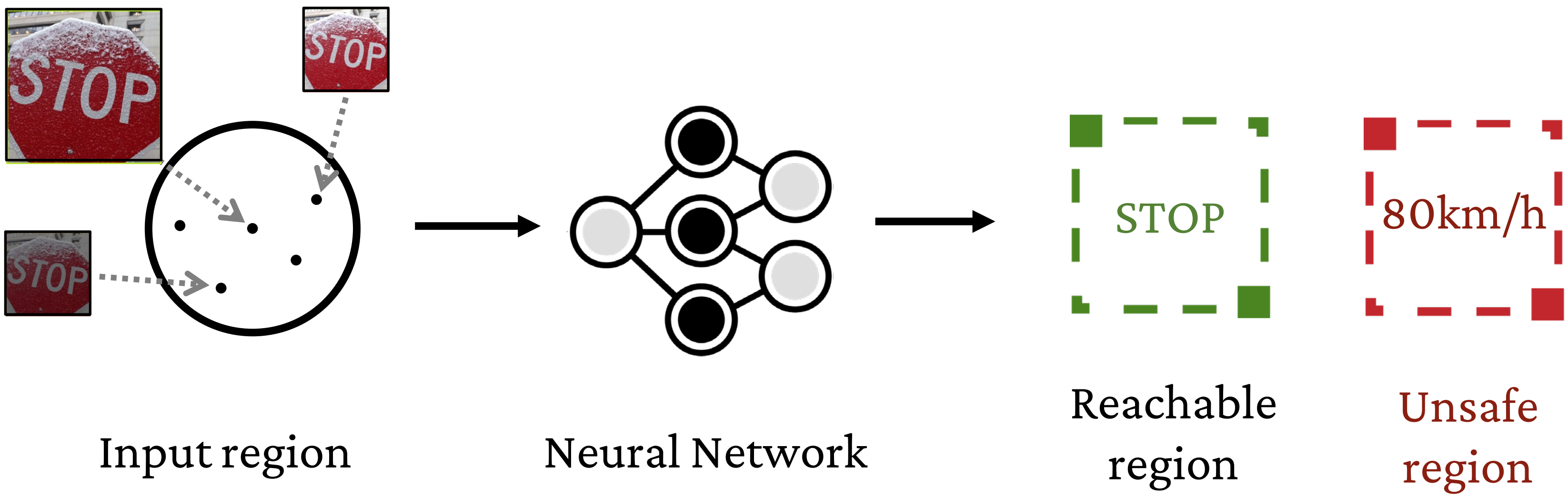
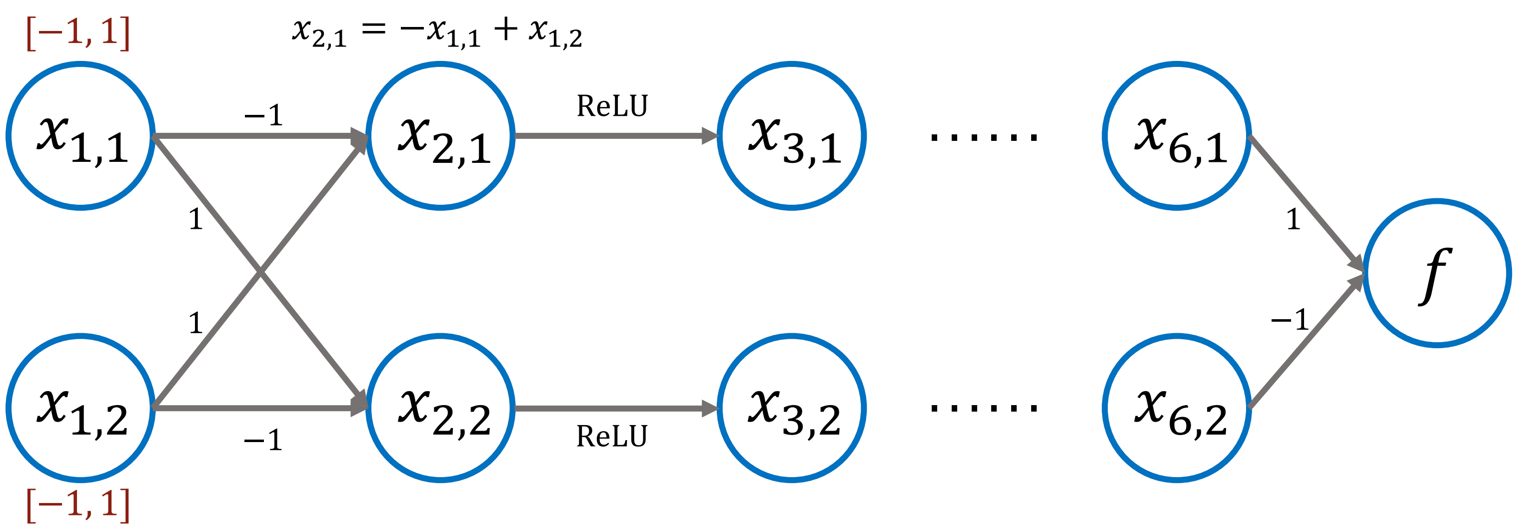


Image source: https://www.businessinsider.com/why-are-stop-signs-red

Bound Propagation

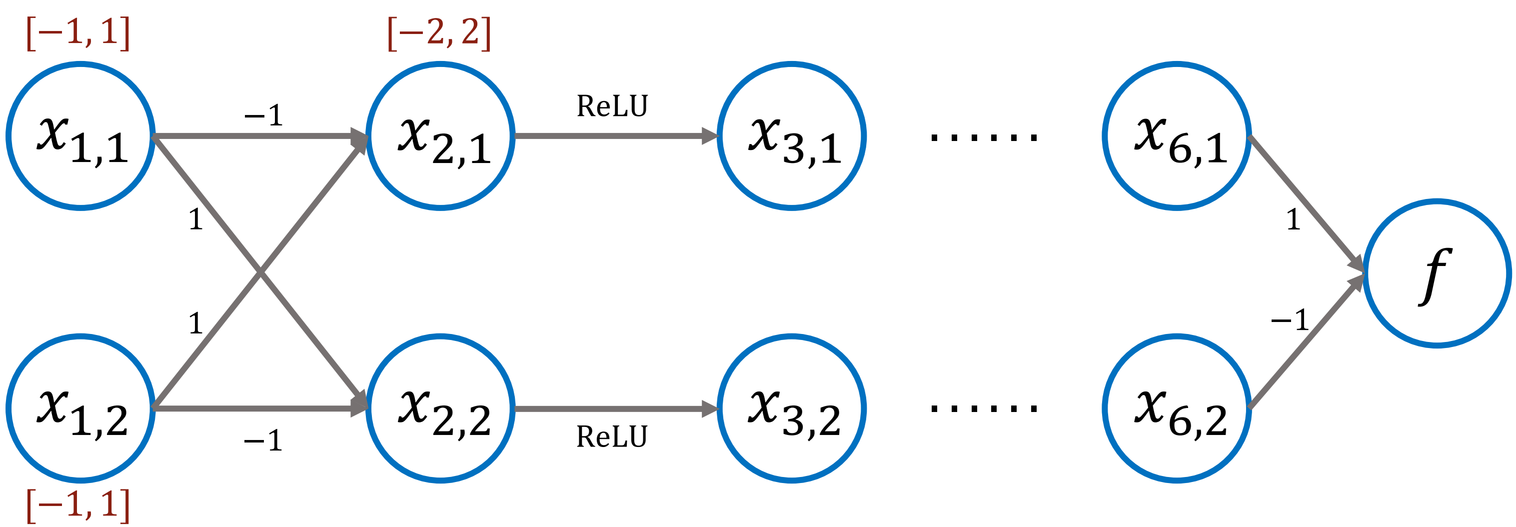
- Propagates bound functions along the neural network
- Widely-used because of its efficiency



Bound Propagation

深圳大学
SHENZHEN UNIVERSITY

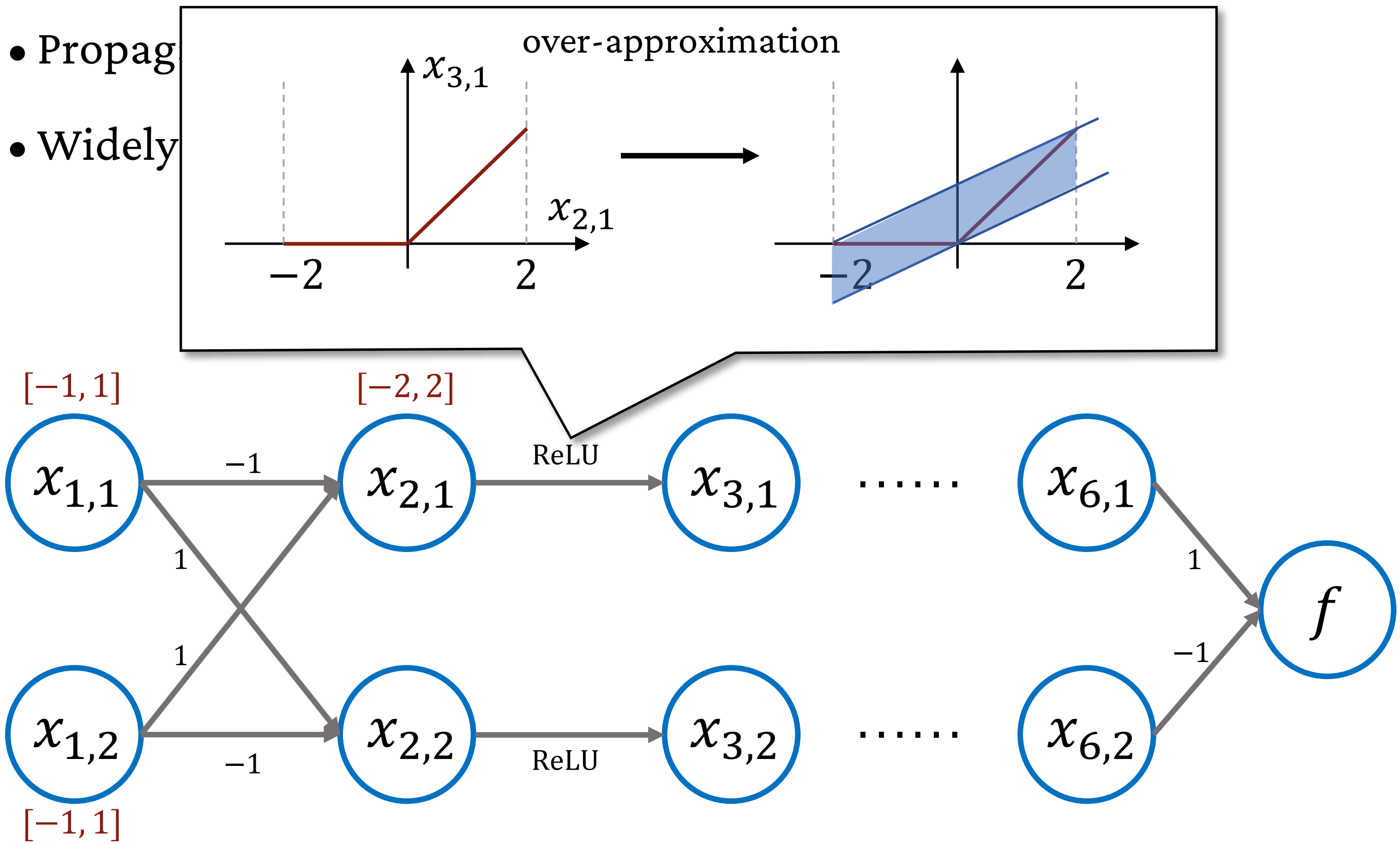
- Propagates bound functions along the neural network
- Widely-used because of its efficiency



Bound Propagation

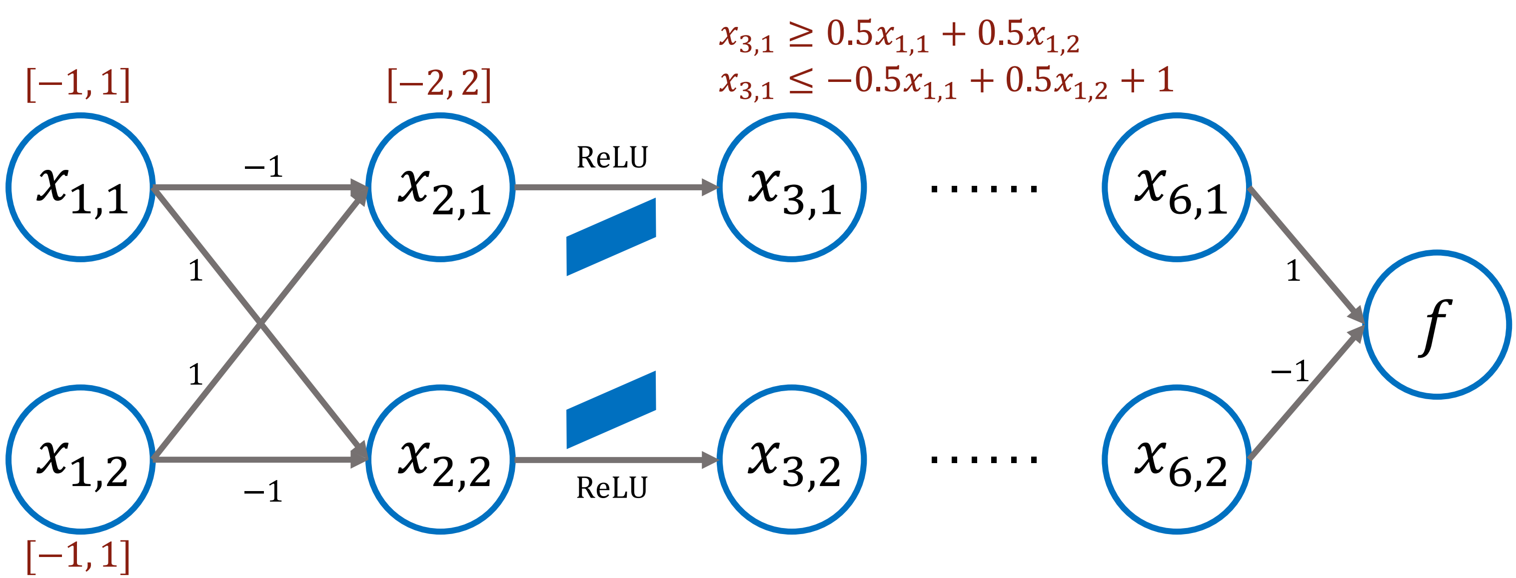
深圳大学 SHENZHEN UNIVERSITY

- Propag
- Widely



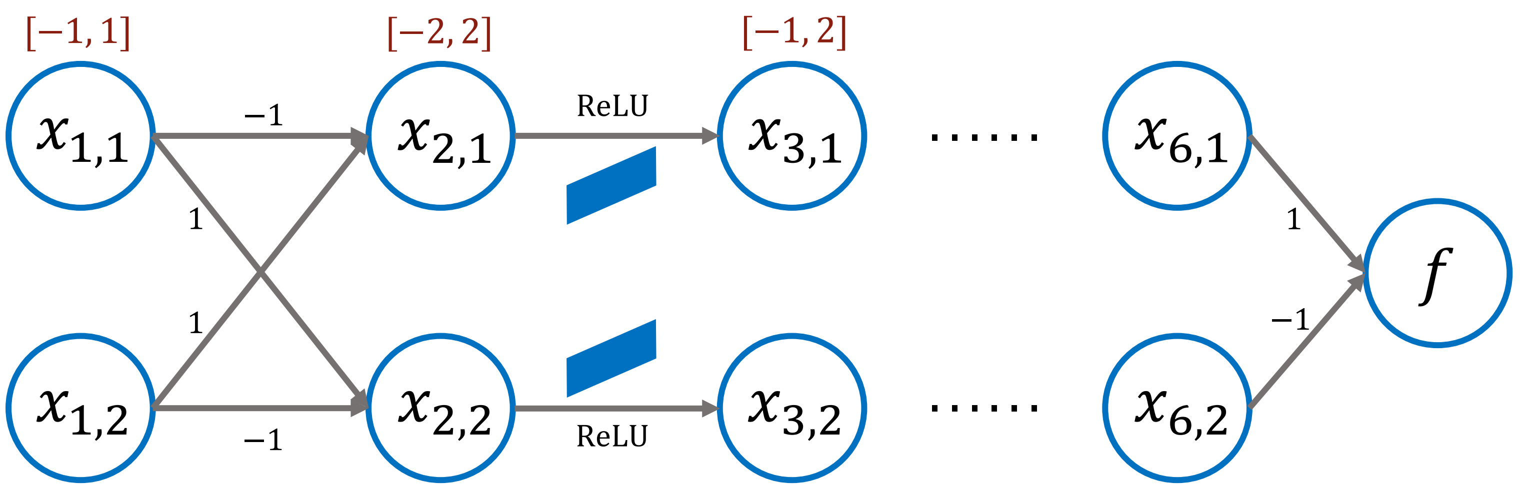
Bound Propagation

- Propagates bound functions along the neural network
- Widely-used because of its efficiency

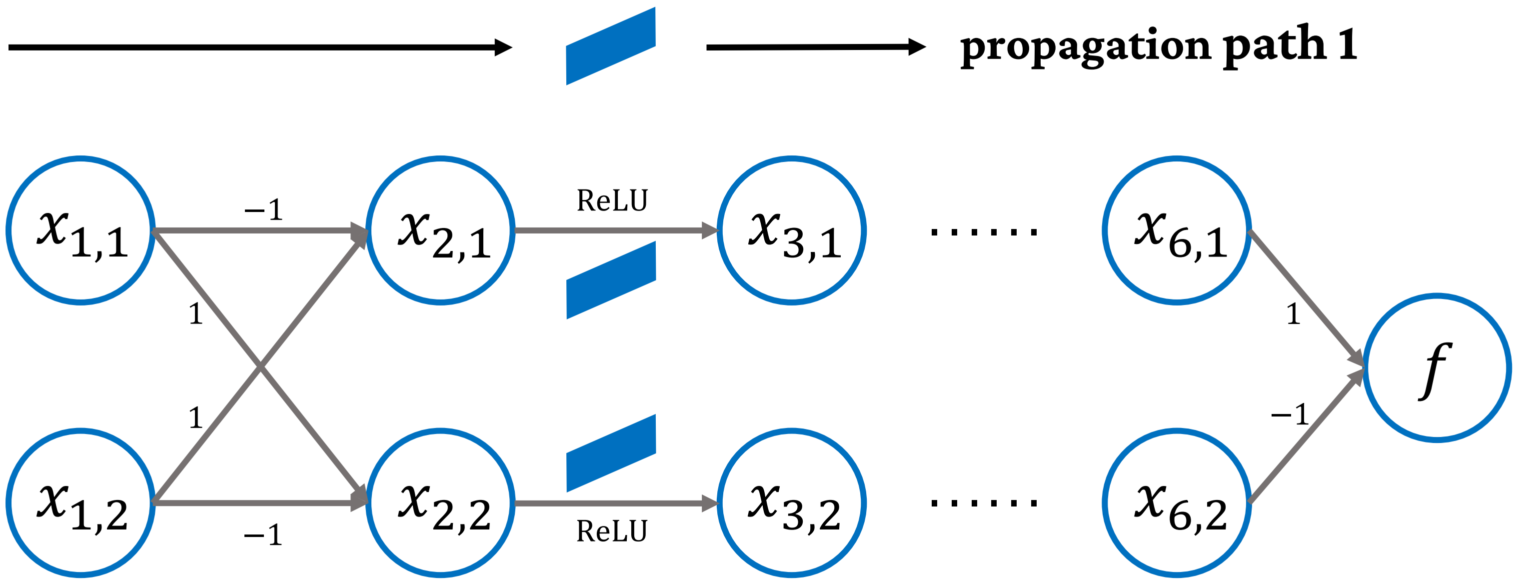


Bound Propagation

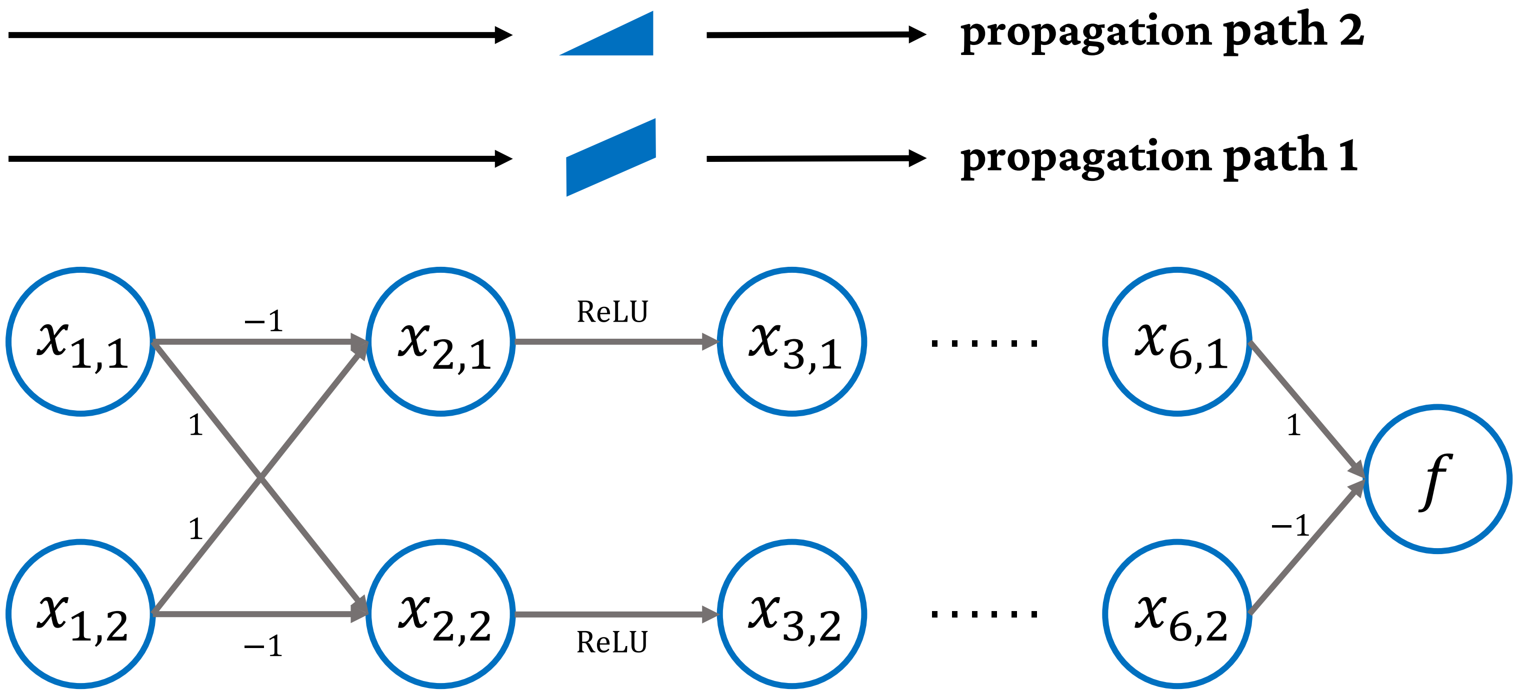
- Propagates bound functions along the neural network
- Widely-used because of its efficiency



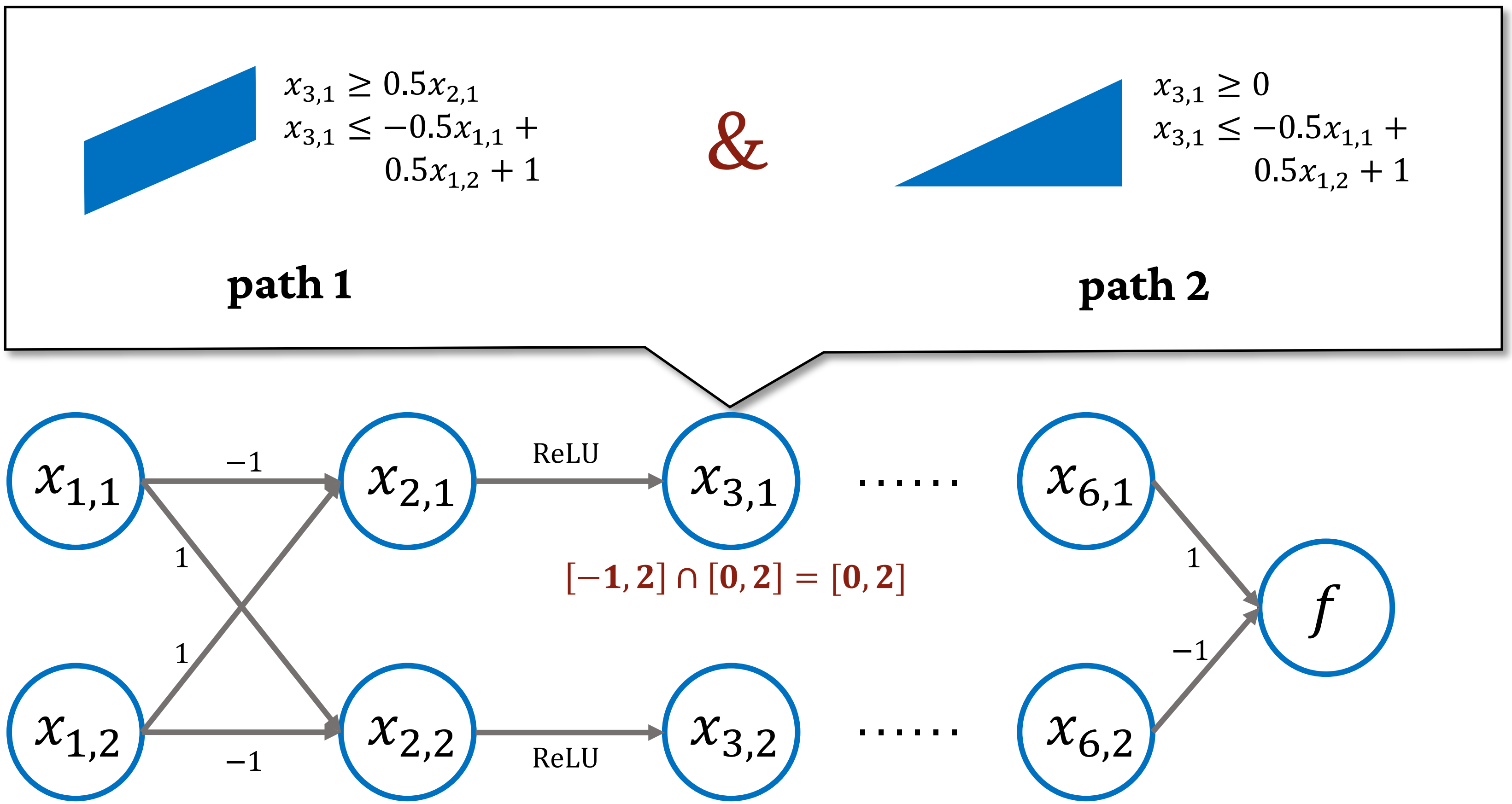
Our: Bound Propagation Path



Our: Two-path Bound Propagation



Our: Two-path Bound Propagation



This Paper

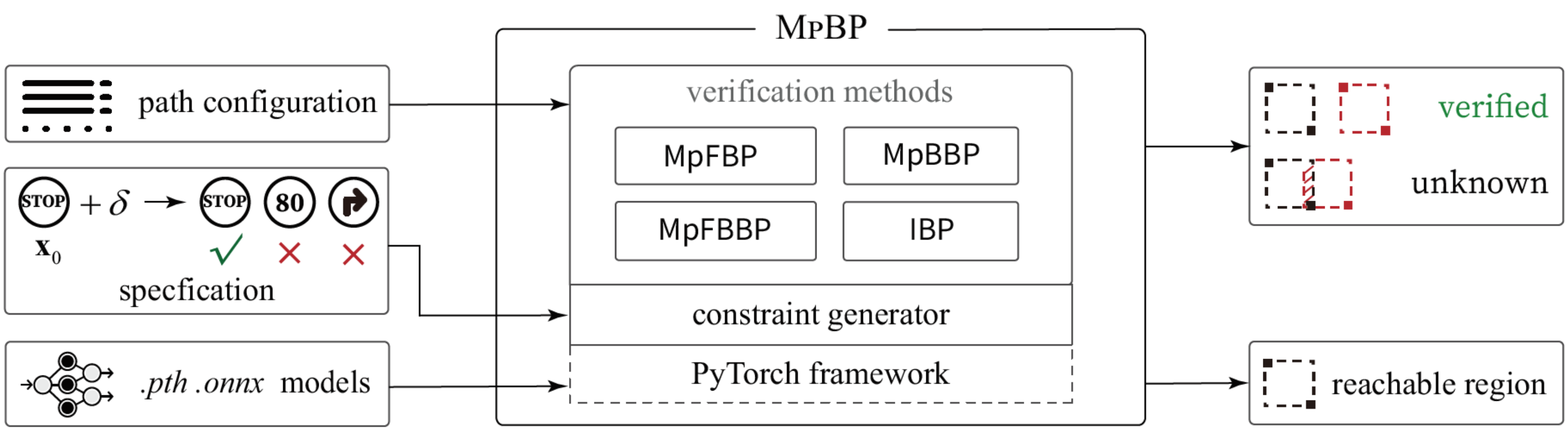
- Extends bound propagation methods to their multi-path counterparts
  - Multi-path backward bound propagation (MpBBP)*
  - Multi-path forward (MpFBP), MpFBBP, etc.
- Uses the PyTorch framework to parallelize BP along multiple paths
  - Reduces the time cost to the level of classical BP on GPUs

Multi-path Back-propagation for Neural Network Verification (in Chinese). Ye ZHENG, Xiaomu SHI, Jiaxiang LIU.

This Paper

SHENZHEN UNIVERSITY

- Extends bound propagation methods to their multi-path counterparts
  - Multi-path backward bound propagation (MpBBP)*
  - Multi-path forward (MpFBP), MpFBBP, etc.
- Uses the PyTorch framework to parallelize BP along multiple paths
  - Reduces the time cost to the level of classical BP on GPUs



Multi-path Back-propagation for Neural Network Verification (in Chinese). Ye ZHENG, Xiaomu SHI, Jiaxiang LIU.

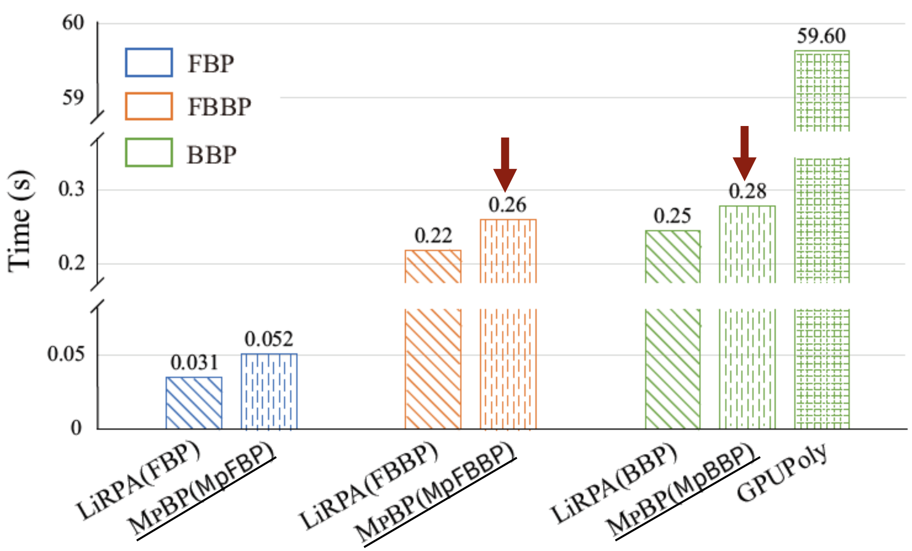
Experiments – vs. the SOTA

- Comparison w.r.t. effectiveness and efficiency

Table 1: Effectiveness Evaluation: Numbers of verified problems are shown. Larger number means more effective.

Tools		Models and Perturbation Thresholds δ			
		MNIST FFNN			
		0.0014	0.0018	0.0022	0.0026
FBP	MpBP	**73**	**62**	**51**	**40**
	LiRPA	69	59	48	33
FBBP	MpBP	**86**	**78**	**69**	**58**
	LiRPA	83	77	66	56
		CIFAR-10 CNN		Tiny ImgNet CNN	
		0.0010	0.0014	0.0010	0.0014
BBP	MpBP	**61**	**38**	**27**	**22**
	LiRPA	56	36	25	19
	GPUPoly	56	36	-	-

Figure 3: Efficiency: Comparison of Verification Time



Experiments – vs. the SOTA

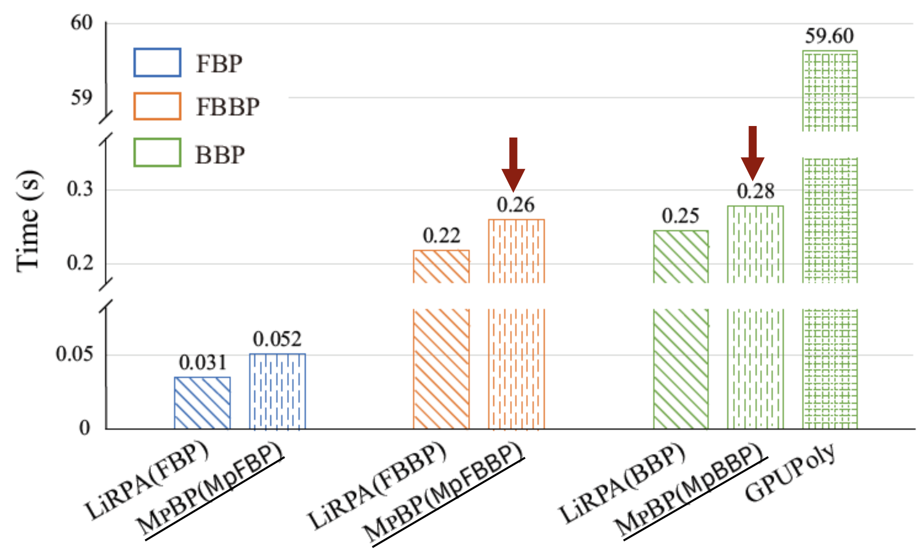
深圳大学
SHENZHEN UNIVERSITY

- Comparison w.r.t. effectiveness and efficiency

Table 1: Effectiveness Evaluation: Numbers of verified problems are shown. Larger number means more effective.

Tools		Models and Perturbation Thresholds δ			
		MNIST FFNN			
		0.0014	0.0018	0.0022	0.0026
FBP	MpBP	**73**	**62**	**51**	**40**
	LiRPA	69	59	48	33
FBBP	MpBP	**86**	**78**	**69**	**58**
	LiRPA	83	77	66	56
		CIFAR-10 CNN		Tiny ImgNet CNN	
		0.0010	0.0014	0.0010	0.0014
BBP	MpBP	**61**	**38**	**27**	**22**
	LiRPA	56	36	25	19
	GPUPoly	56	36	-	-

Figure 3: Efficiency: Comparison of Verification Time



More effective & Same efficient

MpBP: Verifying Robustness of Neural Networks with Multi-path Bound Propagation

Thank you!