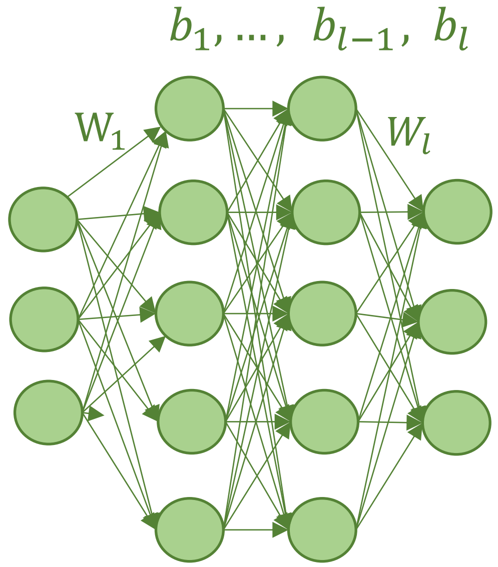
ECLipsE: Efficient Compositional Lipschitz Constant Estimation for Deep Neural Networks

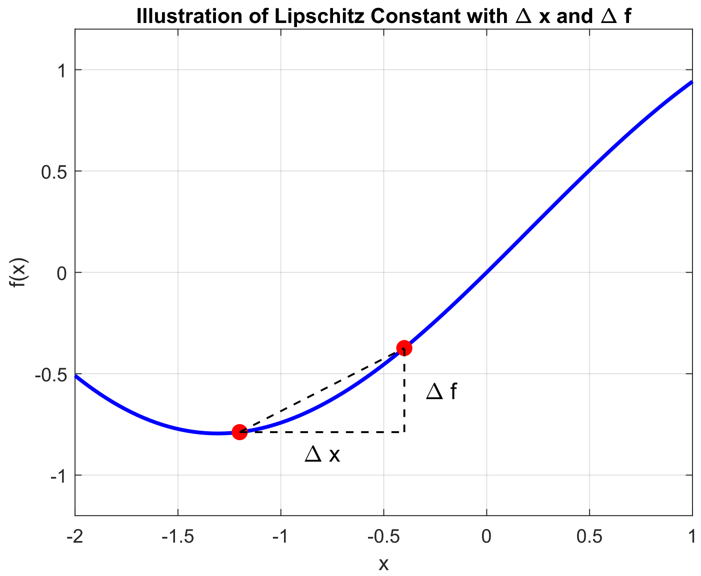
Yuezhu (Ruby) Xu *

Sivaranjani (Siva) Seetharaman

PURDUE UNIVERSITY



ECLipsE: Efficient Compositional Lipschitz Constant Estimation for Deep Neural Networks



- **Lipschitz constant** – measure of robustness
- **NP-Hard** to compute exactly
- Upper bound involves solving a **large** matrix SDP (SOTA: LipSDP methods)
- Recast as **small layer-by-layer** sub-problems

$$\boldsymbol{M_L}$$

$$\begin{bmatrix} I + pW_1^T \Lambda_1 W_1 & -mW_1^T \Lambda_1 & 0 & \cdots & 0 \\ -m\Lambda_1 W_1 & \Lambda_1 I + pW_2^T \Lambda_2 W_2 & -mW_2^T \Lambda_2 & \cdots & 0 \\ 0 & -m\Lambda_2 W_2 & \Lambda_2 I + pW_3^T \Lambda_3 W_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \Lambda_{l-2} I + pW_{l-1}^T \Lambda_{l-1} W_{l-1} & -mW_{l-1}^T \Lambda_{l-1} \\ 0 & \cdots & 0 & -m\Lambda_{l-1} W_{l-1} & \Lambda_{l-1} - FW_l^T W_l \end{bmatrix} \geq 0$$

$$||z_2^{(l)} - z_1^{(l)}||_2 \leq \sqrt{1/F}\,||z_2^{(0)} - z_1^{(0)}||_2$$

ECLipsE: Efficient Compositional Lipschitz Constant Estimation for Deep Neural Networks

- **Lipschitz constant** – measure of robustness
- **NP-Hard** to compute exactly
- Upper bound involves solving a **large** matrix SDP (SOTA: LipSDP methods)
- Recast as **small layer-by-layer** sub-problems

$$\boldsymbol{M_L \geq 0}$$

$$||z_2^{(l)} - z_1^{(l)}||_2 \leq \sqrt{1/F}||z_2^{(0)} - z_1^{(0)}||_2$$

Messenger matrix – computed layer-by-layer

$$\mathcal{M}_i = \begin{cases} I & i = 0 \\ \Lambda_i - \frac{1}{4}\Lambda_i W_i (M_{i-1})_l^{-1} W_i^T \Lambda_i & i \in \mathbb{Z}_{l-1} \end{cases}$$

1 **ECLipsE (small SDPs):** Λ_i is the solution of:

$$\max_{c_i} c_i \text{ s.t. } \begin{bmatrix} \Lambda_i - c_i W_{i+1}^T W_{i+1} & \frac{1}{2}\Lambda_i \left(W_i (\mathcal{M}_{i-1})^{-1} W_i^T\right)^{\frac{1}{2}} \\ \frac{1}{2}\left(W_i (\mathcal{M}_{i-1})^{-1} W_i^T\right)^{\frac{1}{2}} \Lambda_i & I \end{bmatrix} > 0$$

$\Lambda_i \in \mathbb{D}_+, c_i > 0$

2 **ECLipsE-Fast (closed-form solution):**

$$\Lambda_i = \frac{2}{\sigma_{\max}\left(W_i (\mathcal{M}_{i-1})^{-1} W_i^T\right)}$$

Lipschitz Estimate

$$L = \sqrt{\sigma_{\max}\left(W_l^T W_l (\mathcal{M}_{l-1})^{-1}\right)}$$

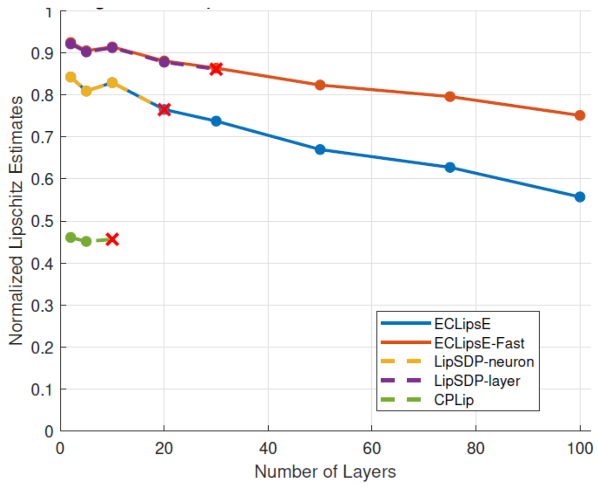
Application: Compositional Robustness Certificates for Neural Networks

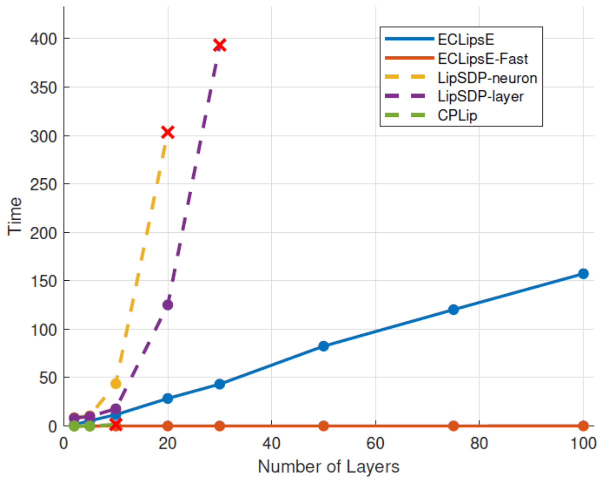
- Recast as **small layer-by-layer** sub-problems
- ECLipsE has comparable estimates with LipSDP-Neuron; ECLipsE-Fast has comparable estimates with LipSDP-Layer
- Both algorithms are much faster
- Computational time grows linearly as depth or width increases while computational time for LipSDP grows exponentially

Key Outcome:

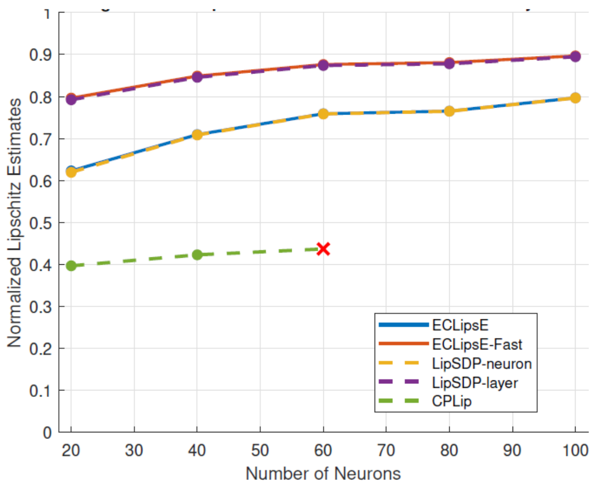
More than **10000x faster** than state of the art algorithms, with comparably tight bounds!

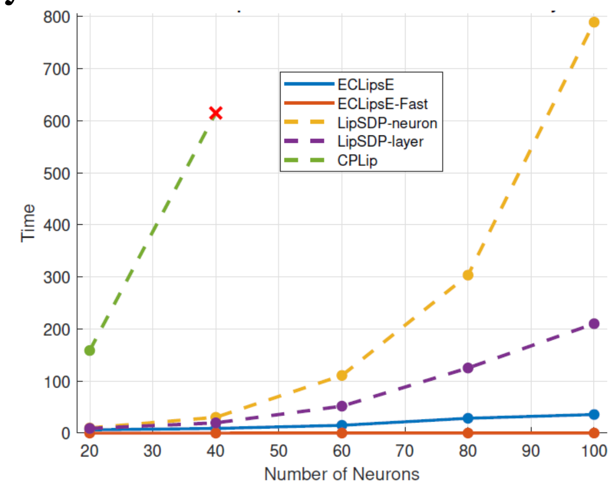
80 Neurons





20 Layers





Application: Compositional Robustness Certificates for Neural Networks

- LipSDP enhances the efficiency by splitting
- Experiment on even deeper neural networks
- ECLipsE-Fast is the most efficient method throughout all cases
- ECLipsE-Fast is more accurate compared to LipSDP-Layer no matter the splitting.
- ECLipsE has best tightness throughout all cases
- ECLipsE is faster than LipSDP-Neuron no matter the split

Key Outcome:

Our algorithms outperforms LipSDP with splitting **on both accuracy and efficiency!**

Comparison with LipSDP Splitting (100 layers)