Theoretical Analysis and Formal Guarantees of Machine Learning Algorithms

Mahalakshmi Sabanayagam

sabanaya@cit.tum.de

Supervisors: Debarghya Ghoshdastidar & Matthias Althoff

Collaborators: Julia Kempe (NYU), Kirkamol Muandet (CISPA)
Leena C Vankadara (Amazon), Anna Dawid (Flatiron) & others

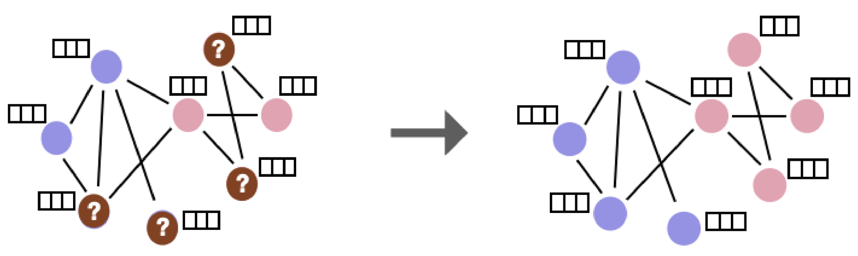
CONVEY

Analyzing Graph Neural Network Architectures through Neural Tangent Kernel

ECML PKDD 2022, arxiv:2210.09809 (under review)

Problem Setup: Node Classification

- Graph G with n nodes
- Adjacency matrix $A \in \{0,1\}^{n\times n}$
- Degree matrix $D \in \mathbb{N}^{n\times n}$
- Feature matrix $X \in \mathbb{R}^{n\times f}$
- m nodes label $Y \in \{1,\dots,K\}^m$



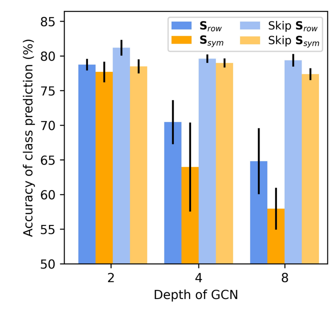
Predict labels for the unlabeled nodes

Graph Convolution Network $\phi\left(S\,\sigma\left(\cdots(S\,\sigma(SXW_1)\,W_2)\cdots\right)W_d\right)$

$S = S_{sym} = D^{-\frac{1}{2}}AD^{-\frac{1}{2}}$ or $S_{row} = D^{-1}A$, $\sigma(.) =$ Linear or ReLU, $W_i \in \mathbb{R}^{h\times h}$ are weights to learn.

Intriguing Empirical Observations

1. S_{row} performs better than S_{sym} for any depth d
2. Performance ↓ as d ↑, skip-connections fix it
3. $\sigma(.) =$ Linear performs as good as $\sigma(.) =$ ReLU



Analysis using Graph Neural Tangent Kernel and Degree Corrected Stochastic Block Model (DC-SBM)

Graph Neural Tangent Kernel as $h \to \infty$

$$\Theta = \sum_{i=1}^{d+1} \Sigma_i \odot \left(SS^T\right)^{\odot(d+1-i)} \odot \left(\bigodot_{j=i}^{d} \dot{E}_j\right)$$

where $\Sigma_1 = SXX^TS^T$, $\Sigma_i = S\Sigma_{i-1}S^T$, $\dot{E} =$ influence of $\sigma(.)$.

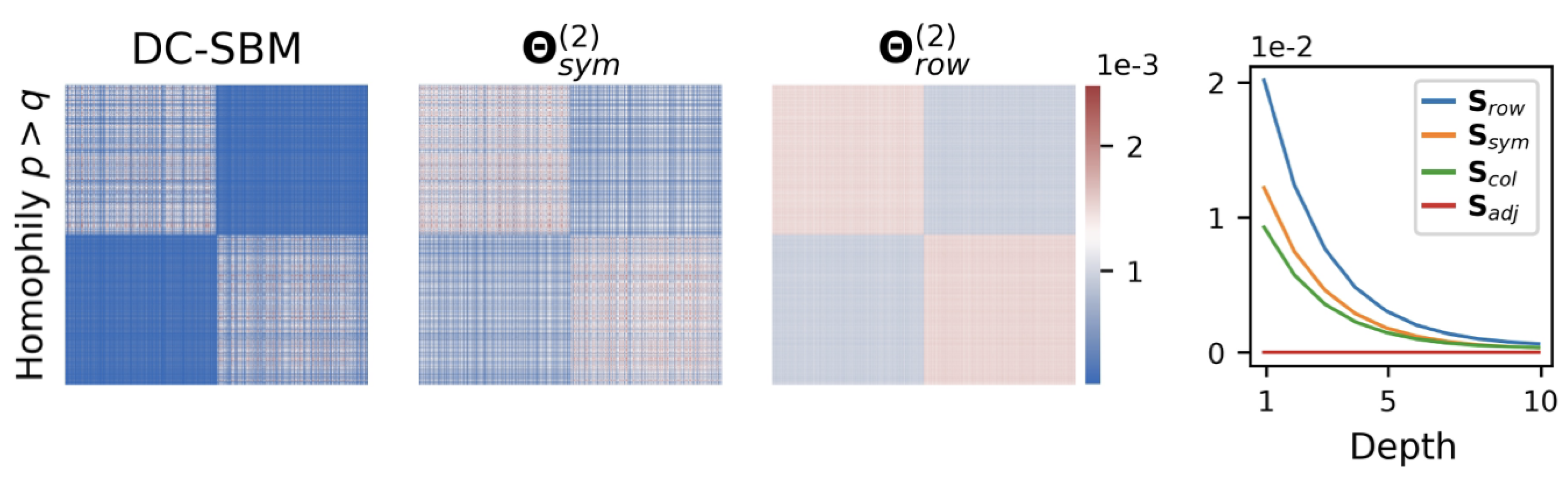
DC-SBM: Random graph model characterized by $p,q \in [0,1]$ and degree correction vector $\pi = (\pi_1,\dots,\pi_n) \in [0,1]^n$. Then for K latent classes, $\mathcal{C}_i \in \{1,\dots,K\}$, the population adjacency matrix $M = \mathbb{E}[A]$ is,

$$M_{ij} = \begin{cases} p\pi_i\pi_j & \text{if } \mathcal{C}_i = \mathcal{C}_j \\ q\pi_i\pi_j & \text{if } \mathcal{C}_i \neq \mathcal{C}_j \end{cases}$$

Visualizations of our Theoretical Results

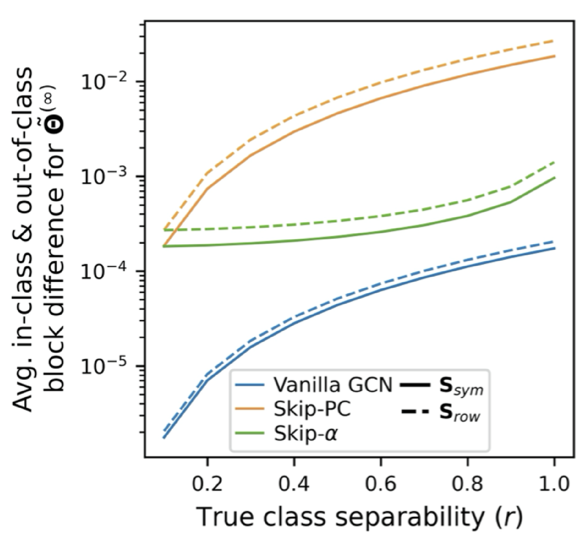
1. Class structure is preserved in S_{row}

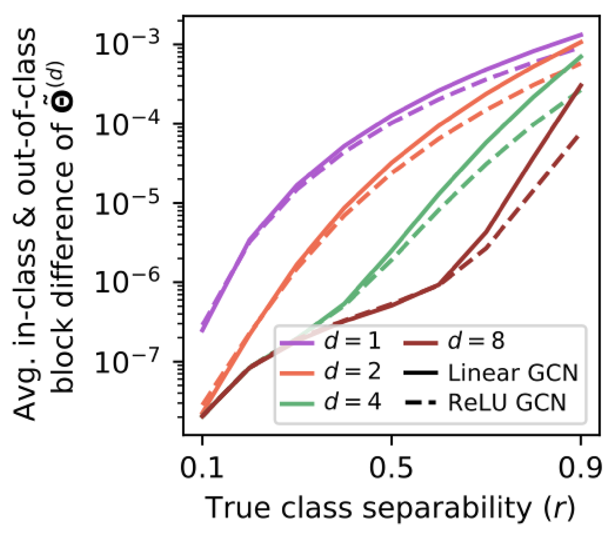
2. Performance ↓ as d ↑



3. Skip-connections retain info even at $d = \infty$

4. Linear as good as ReLU





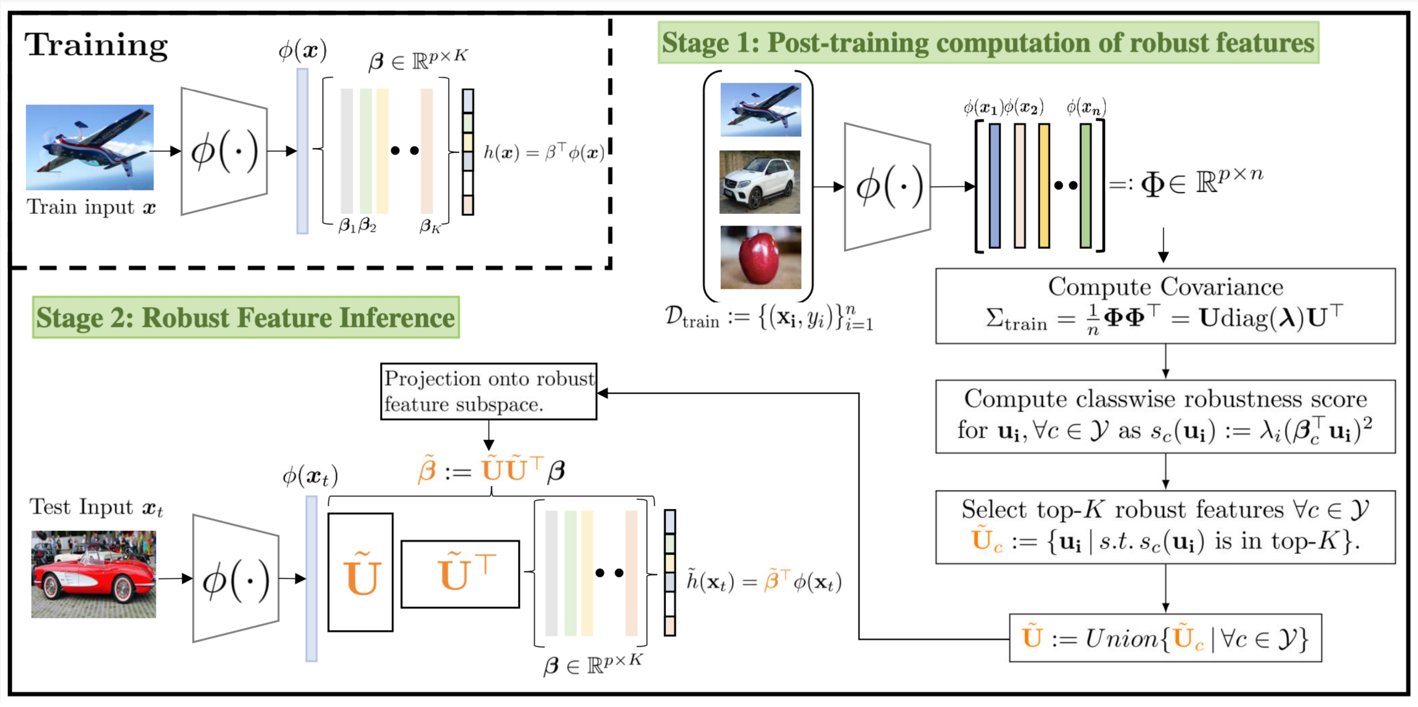
Fast Adaptive Test-Time Defense with Robust Features

Under review

Problem Statement: Improve Adaptive Test-time Defense

Given a trained neural network, how can we make it robust to adversarial attacks at *test-time*? Can we *efficiently* improve the robustness at test-time?

Idea: Project the learned features to the robust subspace



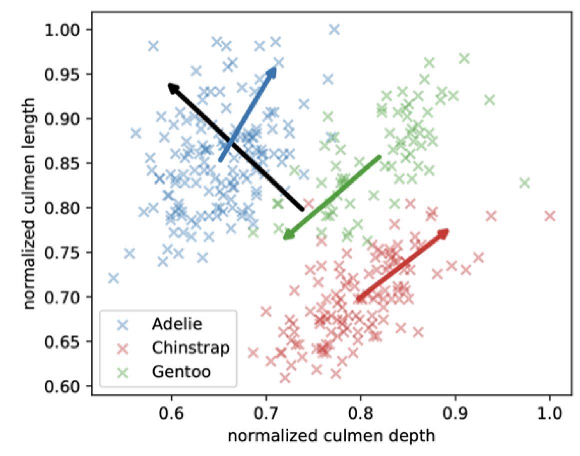
CIFAR-10 Training	Clean		$\ell_\infty(\epsilon = \frac{8}{255})$		$\ell_2(\epsilon = 0.5)$	
	Method	+RFI	Method	+RFI	Method	+RFI
PGD	**83.53**	83.22	42.20	**43.29**	54.61	**55.03**
IAT	**91.86**	91.26	44.76	**46.95**	62.53	**64.31**
C&W attack	**85.11**	84.97	40.01	**42.56**	55.02	**56.79**

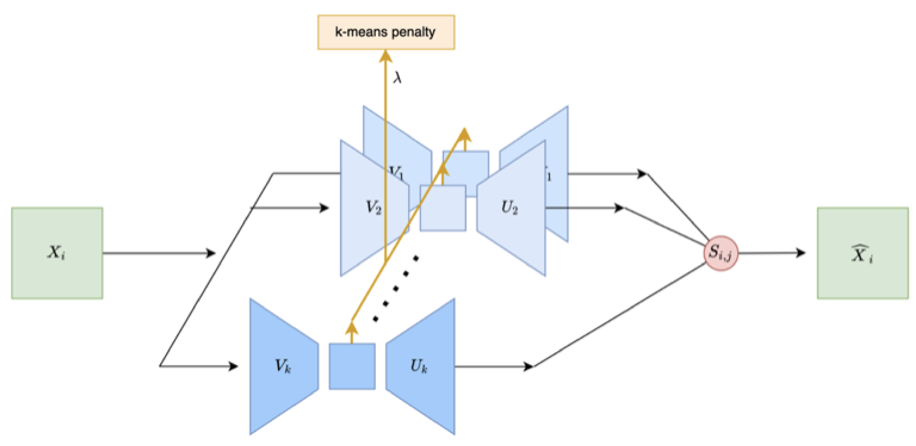
Representation Learning with Tensorized Autoencoder

AISTATS 2023

Problem Statement: Improve representation of multi-modal data

Standard AE learns one representation of the data. How to improve?





$$\min_{\{\phi_j,\psi_j\}_{j=1}^k, S} \sum_{i=1}^{n}\sum_{j=1}^{k} S_{j,i}\left[\left\|(X_i - C_j) - f_{\phi_j}\left(g_{\psi_j}(X_i - C_j)\right)\right\|^2 - \lambda\left\|g_{\psi_j}(X_i - C_j)\right\|^2\right]$$

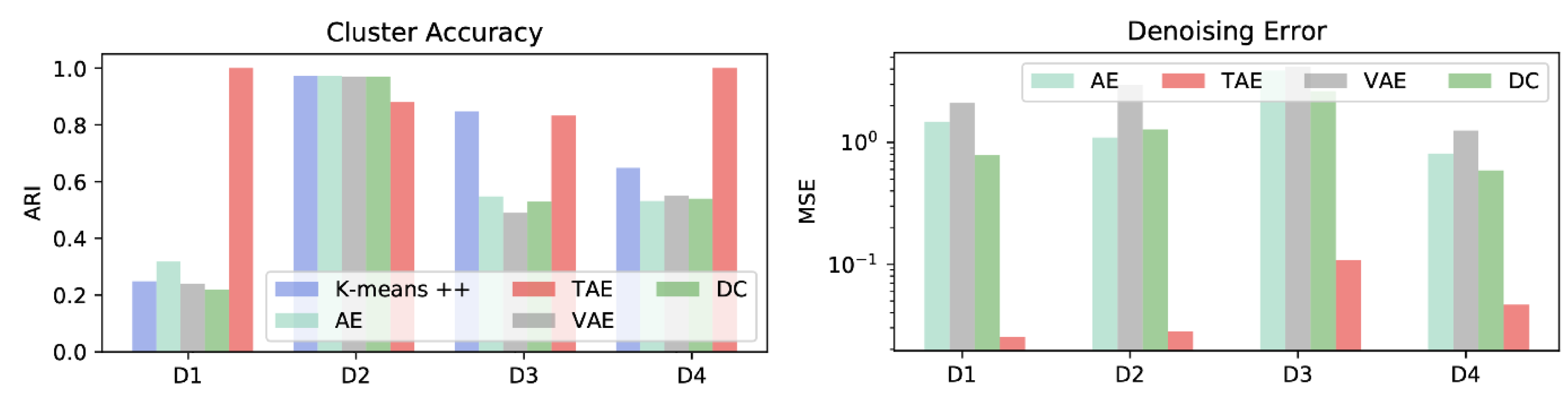
$g_j()$ and $f_j()$ are the encoder and decoder for cluster j, C_j is the center of class j, $S_{j,i}$ assigns a datapoint i to an AE j.

Theory: Optimum for Linear TAE

Class Assignment $S_{j,i} = 0$ or 1, **centers** $C_j = \frac{\sum_{i=1}^{n} S_{j,i}X_i}{\sum_{i=1}^{n} S_{j,i}}$ and **encoding** corresponds to the top h eigenvectors of $\sum_{i=1}^{n} S_{j,i}\,(X_i - C_j)\,(X_i - C_j)^T$.

Empirical Performance

TAE outperforms other methods in denoising and competitively in clustering



Publications

1. Esser, P., Mukherjee, S., *Sabanayagam, M.* and Ghoshdastidar, D. **Improved Representation Learning Through Tensorized Autoencoders.** AISTATS 2023
2. *Sabanayagam, M.*, Esser, P. and Ghoshdastidar, D. **Analyzing Graph Neural Network Architectures through the Neural Tangent Kernel.** ECML PKDD 2022
3. *Sabanayagam, M.*, Vankadara, L.C. and Ghoshdastidar, D. **Graphon based Clustering and Testing of Networks: Algorithms and Theory.** ICLR 2022
4. Singh, A., *Sabanayagam, M.*, Muandet, K. and Ghoshdastidar, D. **Fast Adaptive Test-Time Defense with Robust Features.** Under Review at NeurIPS 2023
5. *Sabanayagam, M.*, Behrens, F., Adomaityte, U. and Dawid, A. **Unveiling the Hessian's Connection to the Decision Boundary.** Under review at NeurIPS 2023
6. *Sabanayagam, M.*, Esser, P. and Ghoshdastidar, D. **Representation Power of Graph Convolutions : Neural Tangent Kernel Analysis.** Under Review at TMLR 2023