# NOT ALL LOW-PASS FILTERS ARE ROBUST IN GRAPH CONVOLUTIONAL NETWORKS

**Zepeng Zhang**

May 15, 2022

This paper [1] investigating how the eigenvalues change after a edge (or a sequence of edge) is being flipped. It can be proved that the larger eigenvalues of $\mathbf{A}$ in the robust interval changes less than smaller eigenvalues, indicating that the low-frequency components in the robust interval are more robust against one-edge perturbation. Therefore, the GCNs can be more robust against structural perturbations when their eigenvalues fall into a certain robust interval. Motivated by the theory, they present GCN-LFR (low-frequency based regularization), a general robust training paradigm for GCN-based models, that suggest training an auxiliary network jointly with the original model through parameter sharing to transfer the robustness of low-frequency component. The model is shown below.

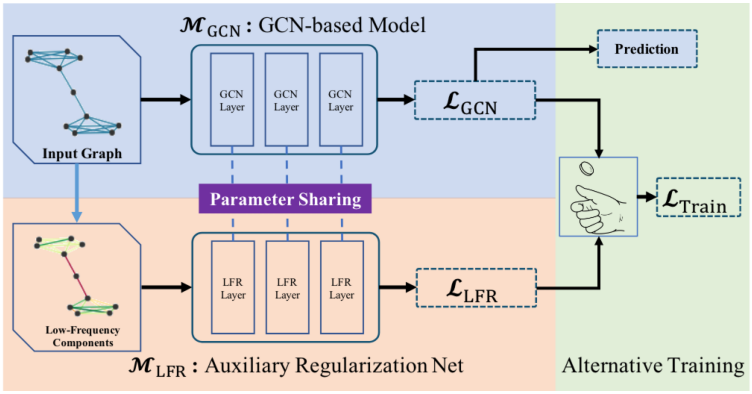


Figure 1: Overview of GCN-LFR

The update rule for the auxiliary regularization net is

$$\text{feature transformation}: \boldsymbol{H}'^{(l)} = \boldsymbol{H}^{(l)}\boldsymbol{\Theta}, \quad \text{graph convolution}: \boldsymbol{H}^{(l+1)} = \sigma\left(\boldsymbol{U}'_{\text{low}}\boldsymbol{F}\boldsymbol{U}'^{\top}_{\text{low}}\boldsymbol{H}'^{(l)}\right)$$

where $\boldsymbol{U}'_{\text{low}}$ are the top-$k$ low-frequency eigenvectors from poisoned graph and $\boldsymbol{F}$ is a learnable diagonal matrix with $k$ parameters as the graph filter. The $\mathbf{F}$ is supposed to learn the robust interval. So the auxiliary net is a learnable graph filter that only uses low-frequency components. The supervised losses for the two network are the same and the total loss is

$$\mathcal{L}_{\text{total}} = (1-\alpha)\mathcal{L}_{\text{GCN}} + \alpha\mathcal{L}_{\text{LFR}}.$$

In this way, we are able to compel the original model to learn a more reliable representation from the robust low-frequency components.

## References

[1] Heng Chang, Yu Rong, Tingyang Xu, Yatao Bian, Shiji Zhou, Xin Wang, Junzhou Huang, and Wenwu Zhu. Not all low-pass filters are robust in graph convolutional networks. *Advances in Neural Information Processing Systems*, 34, 2021. (document)