On the Stability of Spectral Graph Filters – a Probabilistic Perspective

Ning Zhang[1], Henry Kenlay[2], Mihai Cucuringu[1], Xiaowen Dong[1]

[1]University of Oxford,

[2]Exscientia

Graph Signal Processing Workshop, June 2024

Preliminary: graph signals and spectral graph filter

Graph signal: signals indexed by vertices of a graph, denoted as $\mathbf{x} \in \mathbb{R}^n$.

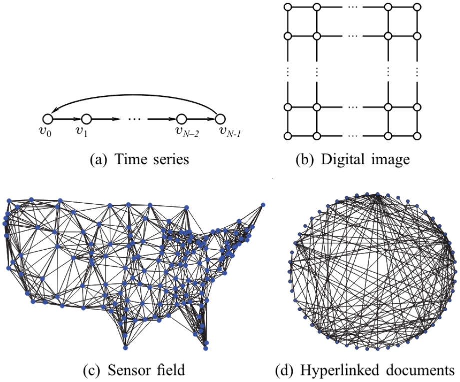


Figure: Examples of graph signals from [SM13]

Preliminary: graph signals and spectral graph filter

Graph signal: signals indexed by vertices of a graph, denoted as $\mathbf{x} \in \mathbb{R}^n$.

Spectral graph filter

A **spectral graph filter** is defined as

$$g(G) = \mathbf{U} g(\Lambda) \mathbf{U}^T,$$

where $\mathbf{U}$ and Λ come from the eigendecomposition of graph shift operator $\mathbf{S} = \mathbf{U} \boldsymbol{\Lambda} \mathbf{U}^T$, and a $g(\boldsymbol{\Lambda})$ is a function applied on each of the eigenvalues.

Preliminary: graph signals and spectral graph filter

Graph signal: signals indexed by vertices of a graph, denoted as $\mathbf{x} \in \mathbb{R}^n$.

Spectral graph filter

A **spectral graph filter** is defined as

$$g(G) = \mathbf{U} g(\Lambda) \mathbf{U}^T,$$

where $\mathbf{U}$ and Λ come from the eigendecomposition of graph shift operator $\mathbf{S} = \mathbf{U} \mathbf{\Lambda} \mathbf{U}^T$, and a $g(\mathbf{\Lambda})$ is a function applied on each of the eigenvalues.

Signal embedding: For input graph signal $\mathbf{x}$, its embedding $g(G)\mathbf{x} \in \mathbb{R}^n$.

Stability of spectral graph filters

Real-world networks may be inaccurate due to noise or adversarial attacks.

Stability of spectral graph filters

Real-world networks may be inaccurate due to noise or adversarial attacks.
Q: When a graph G is perturbed to G_p, how much does the output embedding change?

Stability of spectral graph filters

Real-world networks may be inaccurate due to noise or adversarial attacks.
Q: When a graph G is perturbed to G_p, how much does the output embedding change?

Existing definitions (worst-case view) [KTD20, KTD21, GBR20, LMBB18]

Existing works consider the worst possible graph signals and define the **embedding stability** as

$$\sup_{\mathbf{x}\neq 0} \frac{\|g(G)\mathbf{x} - g\left(G_p\right)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} = \|g\left(G\right) - g\left(G_p\right)\| = \|\mathbf{E}_g\| \tag{1}$$

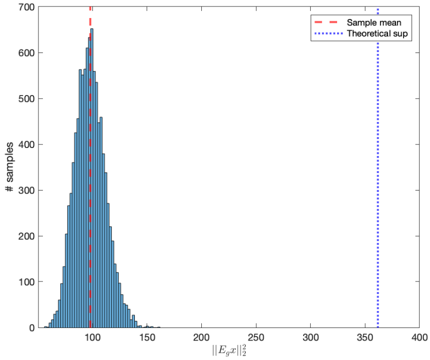
where $\|\mathbf{E}_g\|$ denotes the spectral norms of $\mathbf{E}_g$.

Missing in worst-case analysis

Experiment:

Create a graph perturbation $\mathbf{E}_g$.

Sample 10000 graph signals from unit length sphere.



A new framework from probabilistic view

Q: When a graph G is perturbed to G_p, how stable the overall output embedding is?

Our probabilistic formulation

Consider graph signal as random vector $\boldsymbol{X} = (X_1, \ldots, X_n)^T$ drawn from an arbitrary distribution $\mathcal{D}$ with mean μ and covariance matrix $\mathbf{K}$. The stability of filter g under perturbation is measured by

$$\mathbb{E}_{\boldsymbol{X}\sim\mathcal{D}}[\|\mathbf{E}_g \boldsymbol{X}\|_2^2]$$

A new probabilistic framework

Theorem 1 (simplified)

Assume the input graph signal $\boldsymbol{X} \in \mathbb{R}^n$ is sampled from a distribution $\mathcal{D}$ with covariance matrix $\mathbf{K}$ (WLOG $\mathbb{E}[\boldsymbol{X}] = 0$). Then the output embedding perturbation $\mathbf{E}_g \boldsymbol{X}$ is a random vector with

$$\mathbb{E}_{\boldsymbol{X} \sim \mathcal{D}}[\|\mathbf{E}_g \boldsymbol{X}\|_2^2] = \langle \mathbf{K}, \mathbf{E}_g^T \mathbf{E}_g \rangle. \tag{2}$$

Moreover, for any $c > 0$, we have

$$\mathbb{P}(\|\mathbf{E}_g \boldsymbol{X}\|^2 \geq (1+c)\langle \mathbf{K}, \mathbf{E}_g^T \mathbf{E}_g \rangle) \leq \frac{1}{1+c} \tag{3}$$

Average stability v.s. worst-case stability

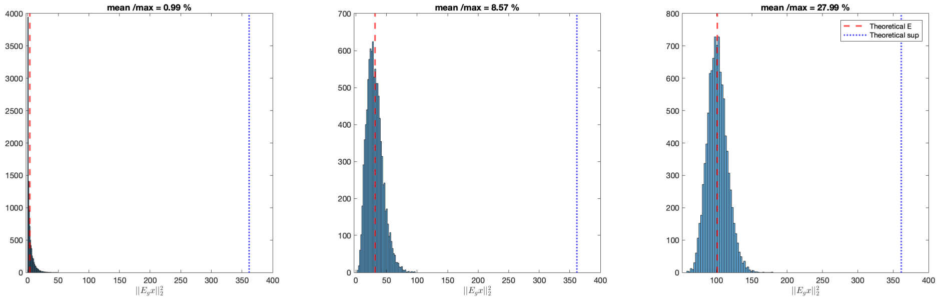
Example. $\boldsymbol{X}$ sampled uniformly at random from the unit length sphere.

$$\text{Our bound: } \frac{1}{n}\|\mathbf{E}_g\|_F^2; \quad \text{Worst-case bound: } \|\mathbf{E}_g\|^2$$

Average stability v.s. worst-case stability

Example. $\boldsymbol{X}$ sampled uniformly at random from the unit length sphere.

$$\text{Our bound: } \frac{1}{n}\|\mathbf{E}_g\|_F^2; \quad \text{Worst-case bound: } \|\mathbf{E}_g\|^2$$



(a) rank$(\mathbf{E}_g) = 1$ (b) rank$(\mathbf{E}_g) = 10$ (c) rank$(\mathbf{E}_g) = $ n

Application: attacking the graph Laplacian

Theorem 2

We consider an unweighted and undirected simple graph with graph filter $\mathbf{L}$. Under edge perturbations $\mathcal{P}$,

$$\mathbb{E}_{\boldsymbol{X}\sim\mathcal{D}}[\|\mathbf{E}_g\boldsymbol{X}\|^2] = 2\sum_{(u,v)\in\mathcal{P}}\mathcal{R}(u,v) + \sum_{(u,v),(u,v')\in\mathcal{P}}\sigma_{uv}\sigma_{uv'}(\mathcal{R}(u,v)+\mathcal{R}(u,v')-\mathcal{R}(v,v')),$$

where $\mathcal{R}(u,v)$ is defined as

$$\mathcal{R}(u,v) \triangleq \mathbb{E}[(X_u - X_v)^2] = \mathrm{Var}(X_u) + \mathrm{Var}(X_v) - 2\mathrm{Cov}(X_u, X_v).$$

Application: attacking the graph Laplacian

Setting:

Create Erdős-Rényi graph G.

Assume graph signal $\boldsymbol{X}$ is smooth, i.e., $\boldsymbol{X} \sim \mathcal{N}(\mathbf{0}, \mathbf{K})$, where $\mathbf{K} = \mathbf{L}^{\dagger}$.

Consider $g(G) = \mathbf{L}$

Goal: perturbed 20 edges to achieve large average embedding perturbation.

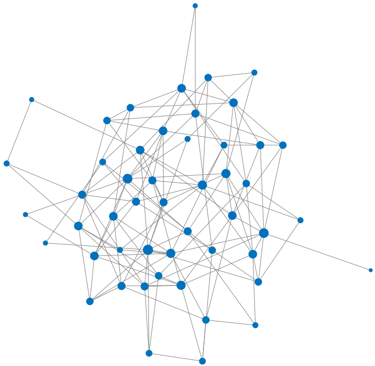
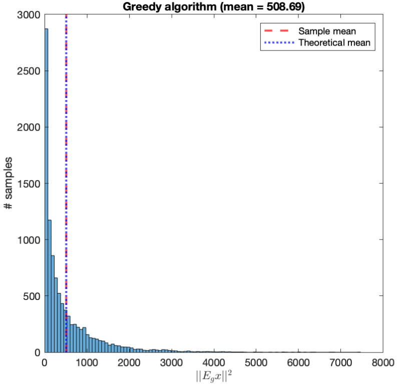
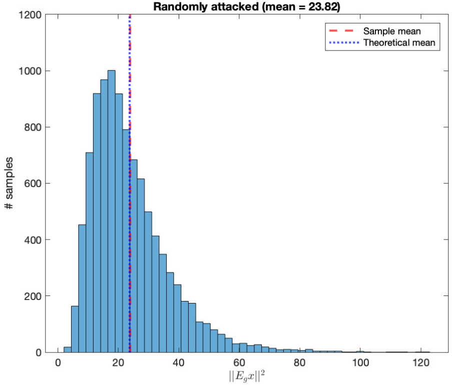


Figure: Erdős-Rényi graph $(n = 50, p = 0.1)$

Application: attacking the graph Laplacian

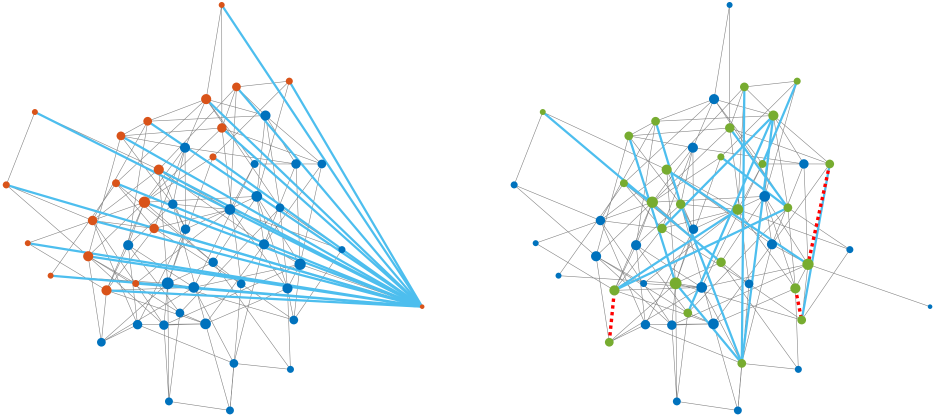


(a) Our greedy attack strategy



(b) Random attack

Application: attacking the graph Laplacian



(a) Our greedy attack strategy (b) Random attack

Conclusions

A probabilistic framework. We propose a probabilistic framework for analysing the graph filter stability. This new framework is *representative* and does *not rely on any assumptions of generative distribution*.

Interpretble analysis. We relate robustness to spectral and spatial properties of the signal covariance or graph structure.

References I

[GBR20] Fernando Gama, Joan Bruna, and Alejandro Ribeiro. Stability properties of graph neural networks. *IEEE Transactions on Signal Processing*, 68:5680–5695, 2020.

[KTD20] Henry Kenlay, Dorina Thanou, and Xiaowen Dong. On the stability of polynomial spectral graph filters. In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5350–5354. IEEE, 2020.

[KTD21] Henry Kenlay, Dorina Thanou, and Xiaowen Dong. Interpretable stability bounds for spectral graph filters. In *International conference on machine learning*, pages 5388–5397. PMLR, 2021.

References II

[LMBB18] Ron Levie, Federico Monti, Xavier Bresson, and Michael M Bronstein. Cayleynets: Graph convolutional neural networks with complex rational spectral filters. *IEEE Transactions on Signal Processing*, 67(1):97–109, 2018.

[SM13] Aliaksei Sandryhaila and José MF Moura. Discrete signal processing on graphs. *IEEE transactions on signal processing*, 61(7):1644–1656, 2013.