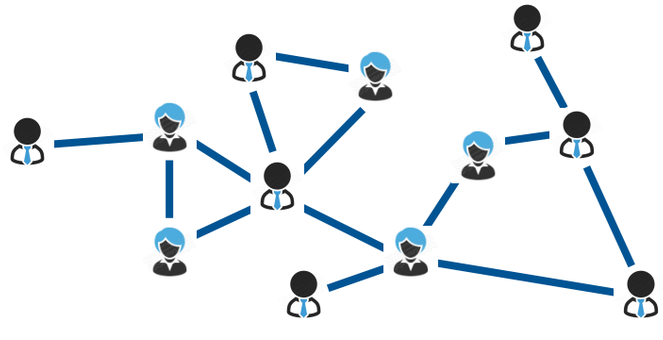
Stability of spectral graph filters and beyond

Xiaowen Dong
Department of Engineering Science
University of Oxford

CIRM, November 2022

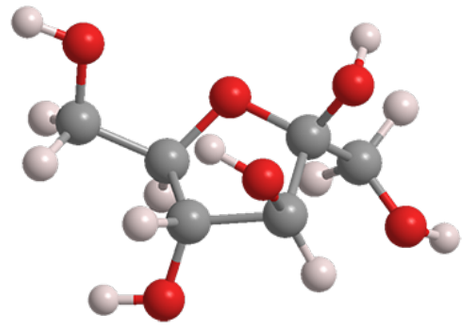
Networks are pervasive

traffic network



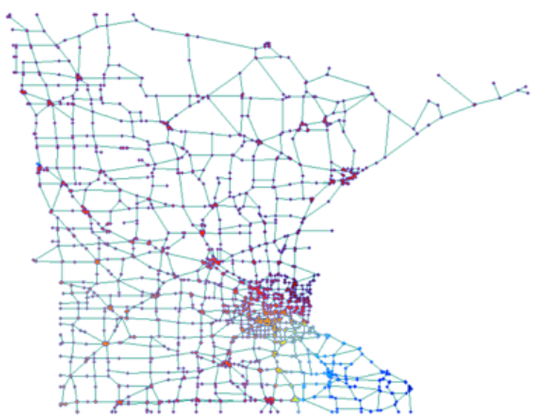
social network

brain network

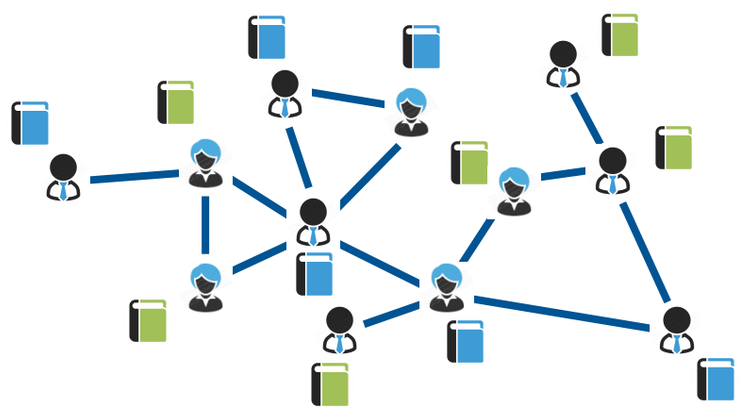


chemical network

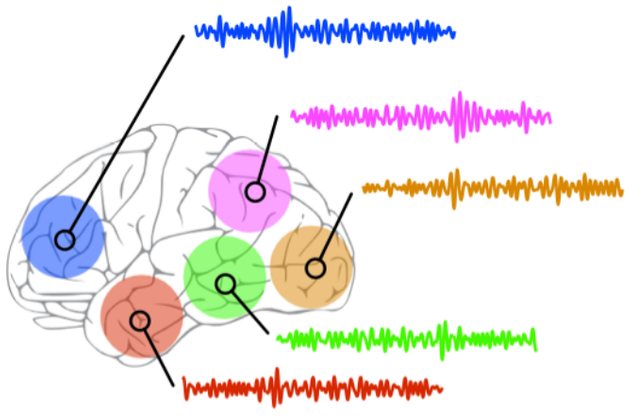
Network (graph) structured data are pervasive



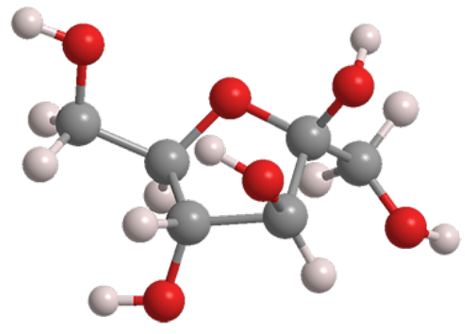
congestion in road junctions



preferences of individuals

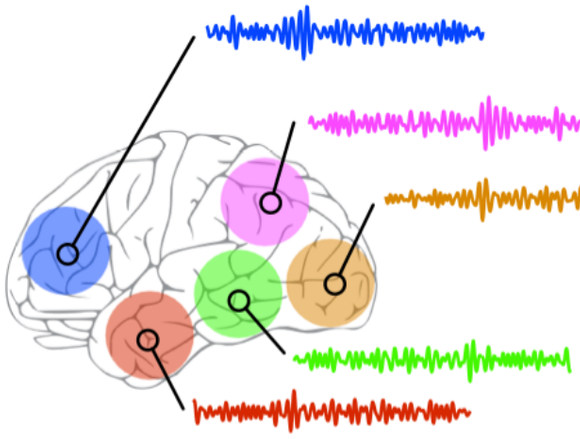


activities in brain regions



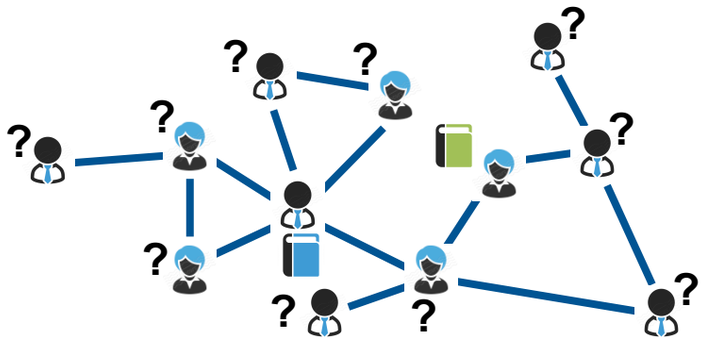
properties of atoms

Learning with graph-structured data



condition?
no condition?

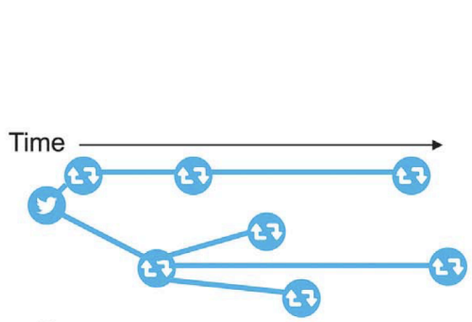
(supervised) graph-level classification

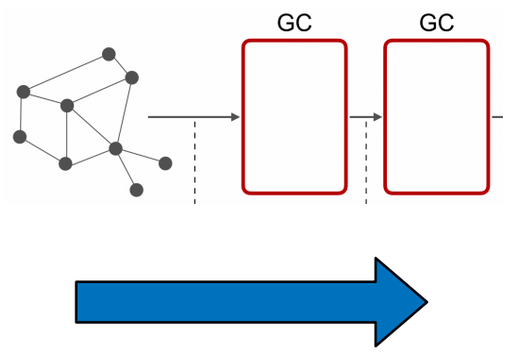


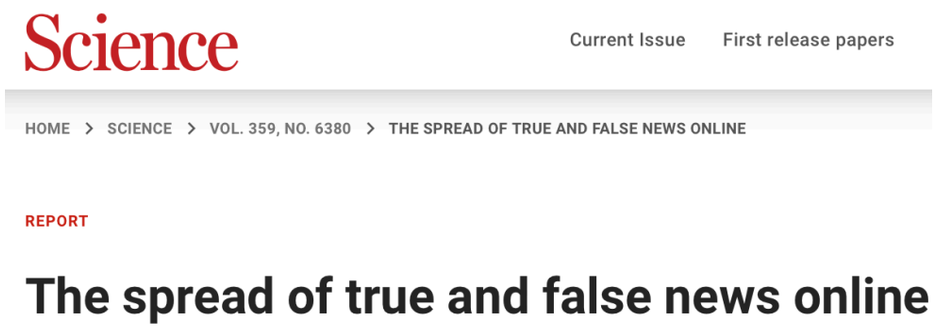
(semi-supervised) node-level classification

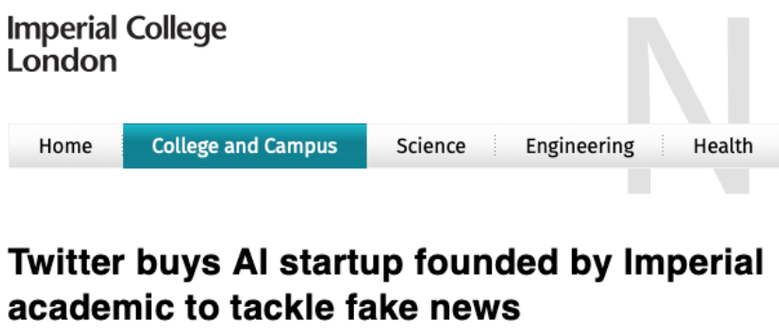
Exciting possibilities enabled by graph learning

fake news detection





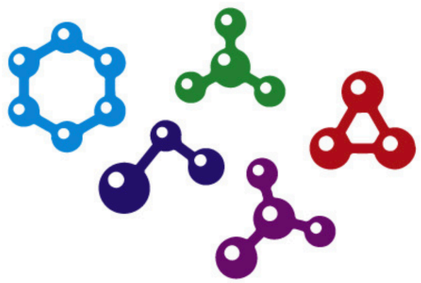


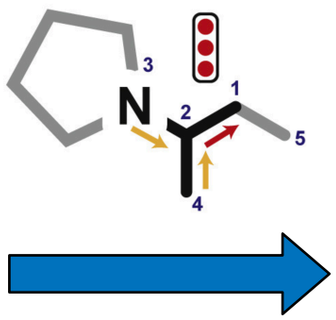


Vosoughi et al., "The spread of true and false news online," Science, 2018.
Monti et al., "Fake news detection on social media using geometric deep learning," ICLR Workshop, 2019.

Exciting possibilities enabled by graph learning

drug discovery

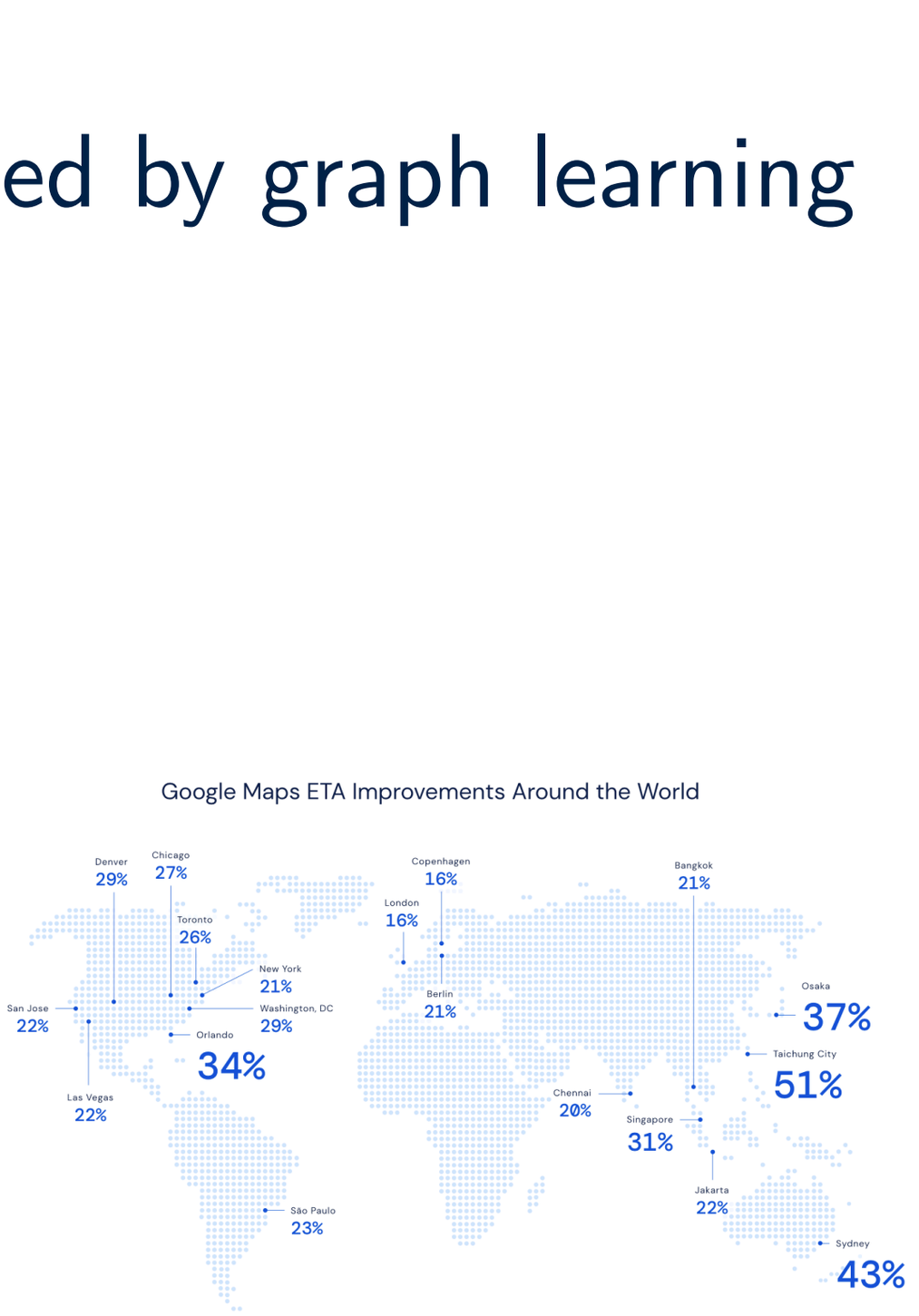




Stokes et al., "A deep learning approach to antibiotic discovery," Cell, 2020.

Exciting possibilities enabled by graph learning

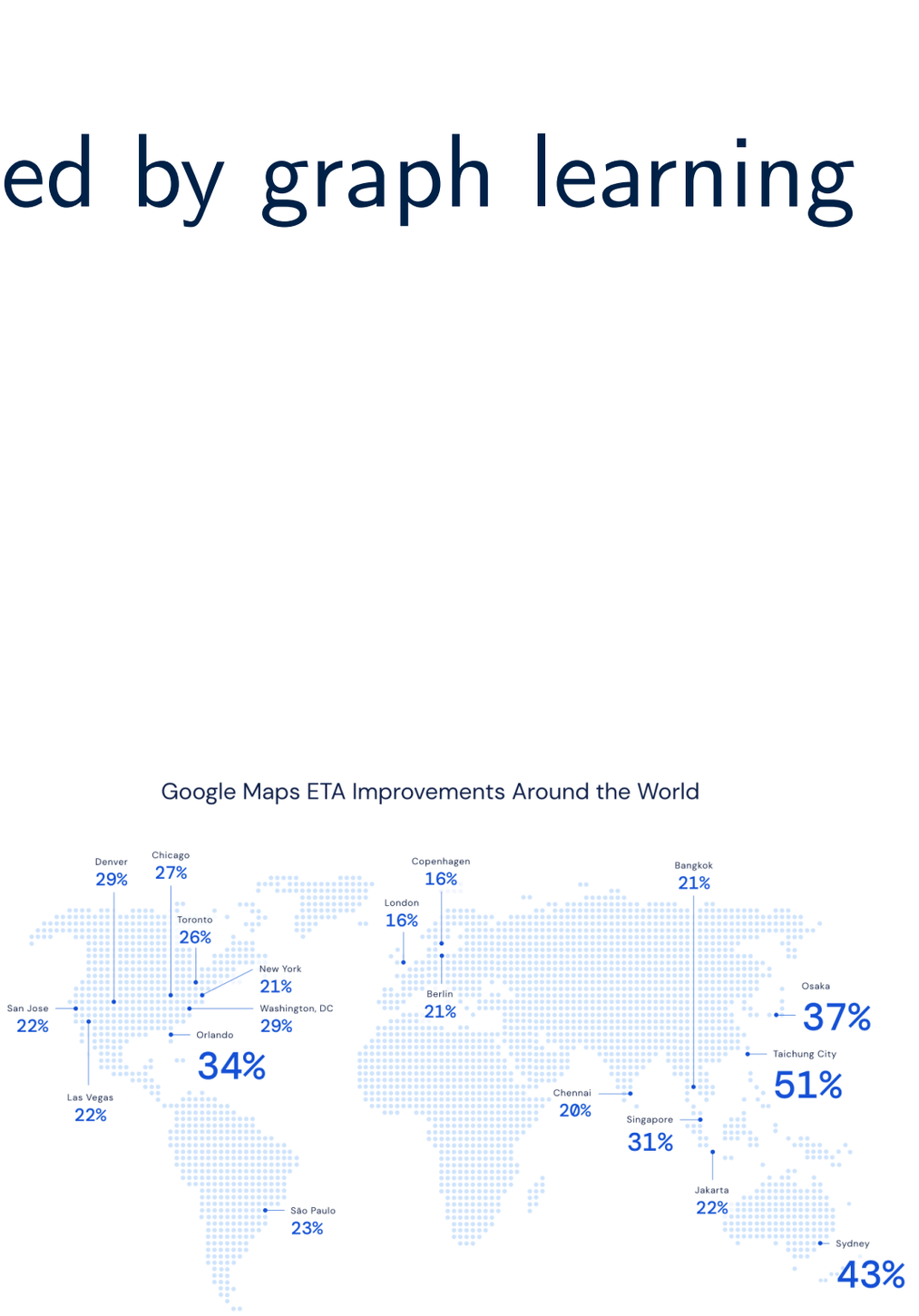
traffic prediction



Derrow-Pinion et al., "ETA Prediction with Graph Neural Networks in Google Maps," CIKM, 2021.

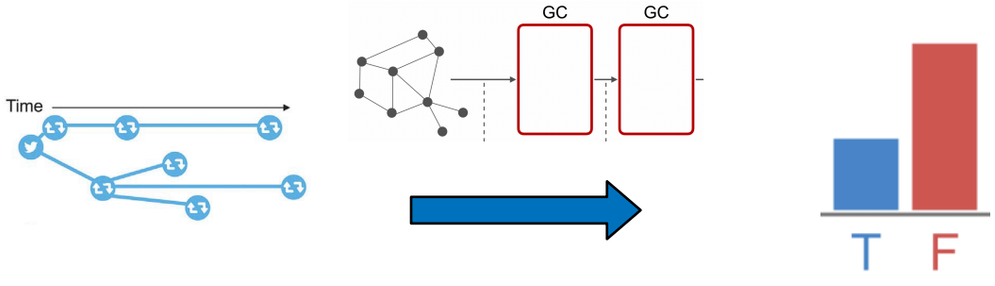
Exciting possibilities enabled by graph learning

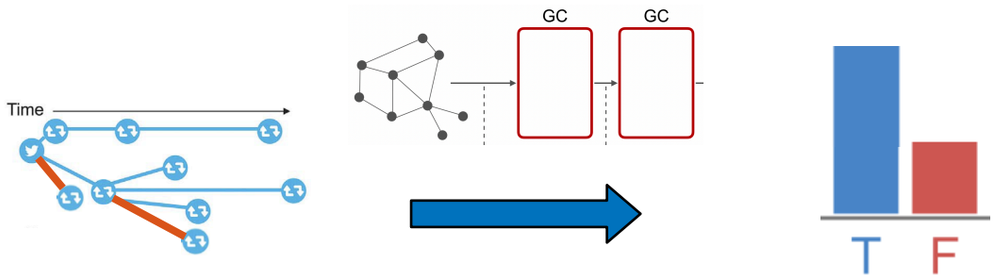
traffic prediction



Derrow-Pinion et al., "ETA Prediction with Graph Neural Networks in Google Maps," CIKM, 2021.

Limitation and open questions





One main limitation

- need accurate, deterministic, a priori known graph structure
- susceptible to structural perturbation

Two open questions

- when are graph models robust under domain perturbation?
- how is robustness related to structural change?

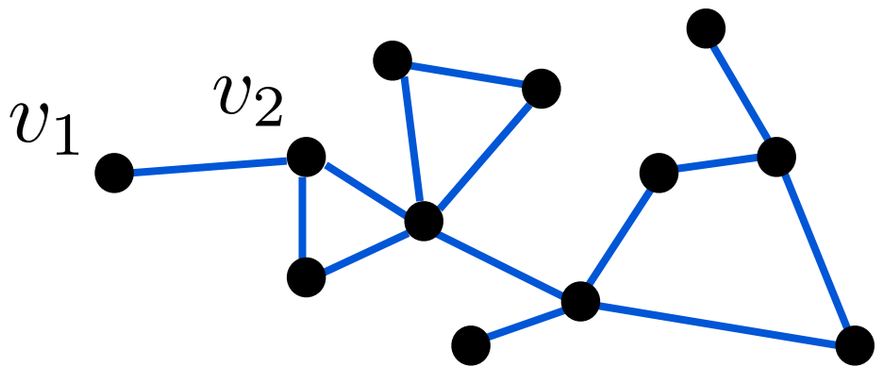
Outline

- Brief introduction to spectral graph filters
- Interpretable stability bounds for spectral graph filters
- Further results on robustness of graph machine learning models

Outline

- Brief introduction to spectral graph filters
- Interpretable stability bounds for spectral graph filters
- Further results on robustness of graph machine learning models

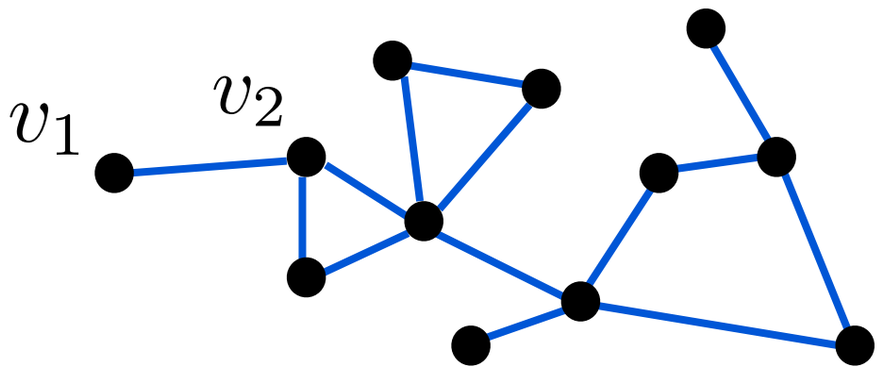
Graphs



$$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$$

- key concepts
  - vertices
  - edges (binary or weighted, undirected or directed)

Graphs



$$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$$

- key concepts
  - vertices
  - edges (binary or weighted, undirected or directed)
  - graph Laplacian (combinatorial or normalised)

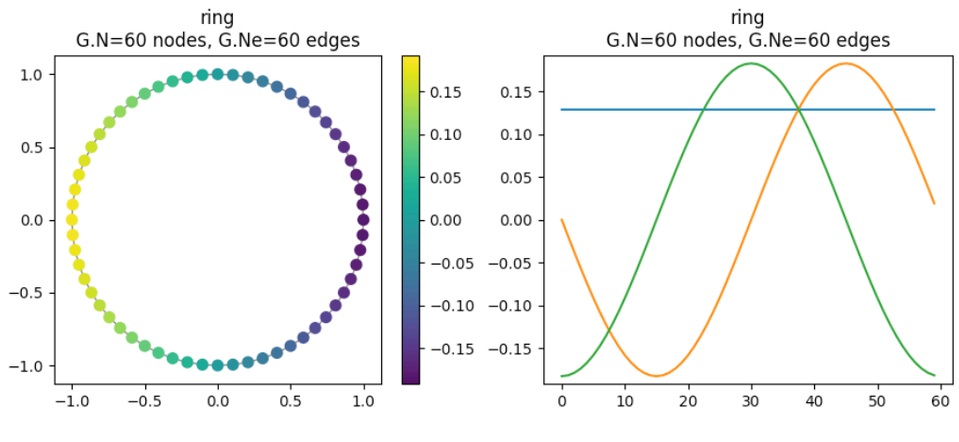
$$L = D - W$$

$$L_{\text{norm}} = D^{\frac{1}{2}}(D - W)D^{\frac{1}{2}}$$

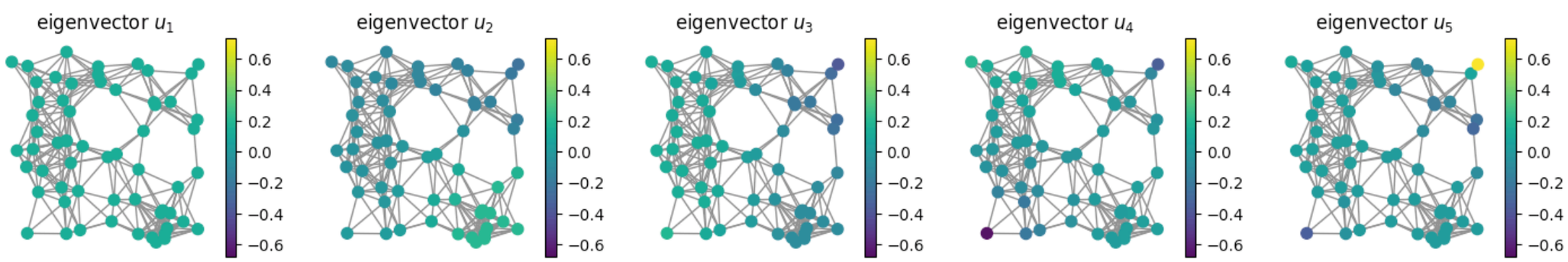
$$L = \begin{bmatrix} | & & | \\ \chi_0 & \cdots & \chi_{N\text{-}1} \\ | & & | \end{bmatrix} \begin{bmatrix} \lambda_0 & & 0 \\ & \ddots & \\ 0 & & \lambda_{N-1} \end{bmatrix} \begin{bmatrix} — & \chi_0 & — \\ & \cdots & \\ — & \chi_{N\text{-}1} & — \end{bmatrix}$$

$$\chi \qquad \Lambda \qquad \chi^T$$

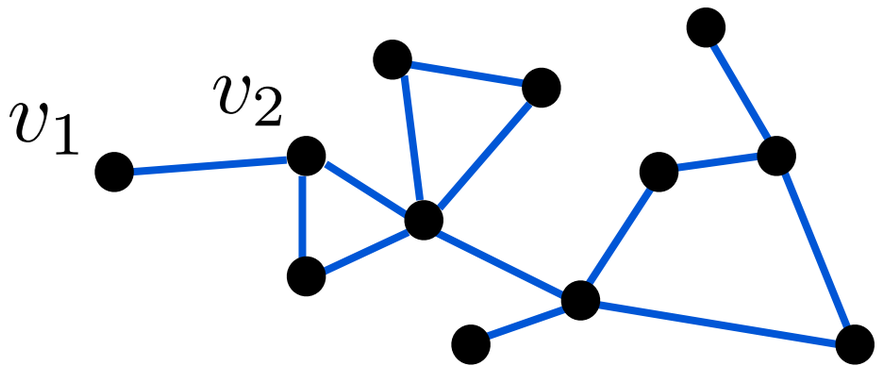
Graphs



- eigenvectors of graph Laplacian

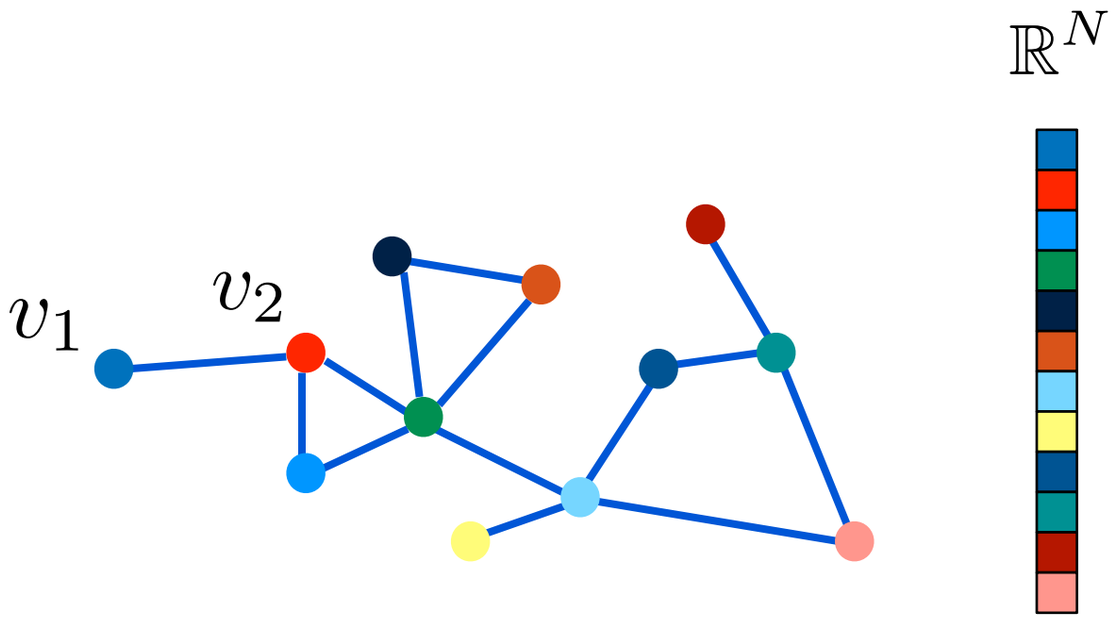


Graph signal processing



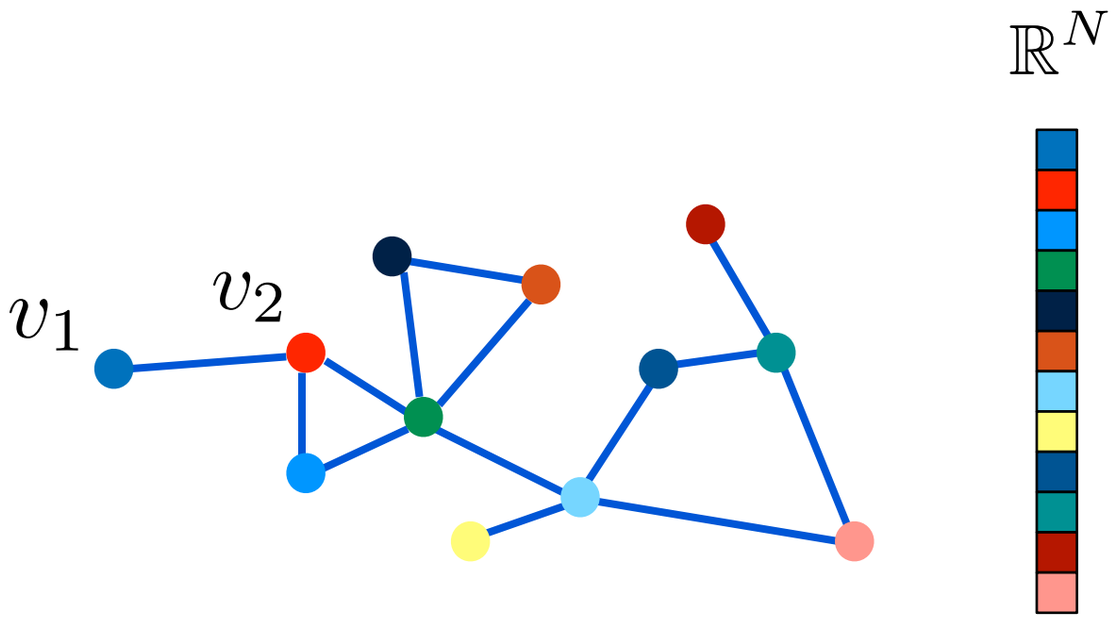
$$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$$

Graph signal processing



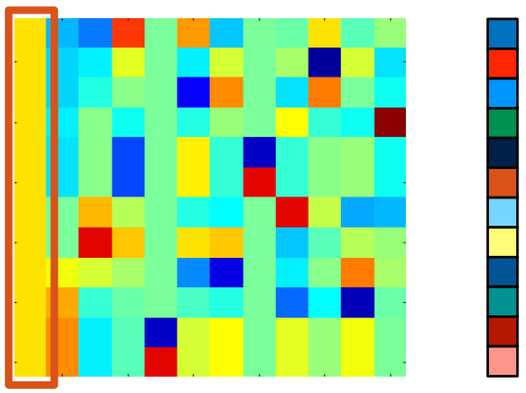
$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ $\quad$ $f : \mathcal{V} \to \mathbb{R}$

Graph signal processing



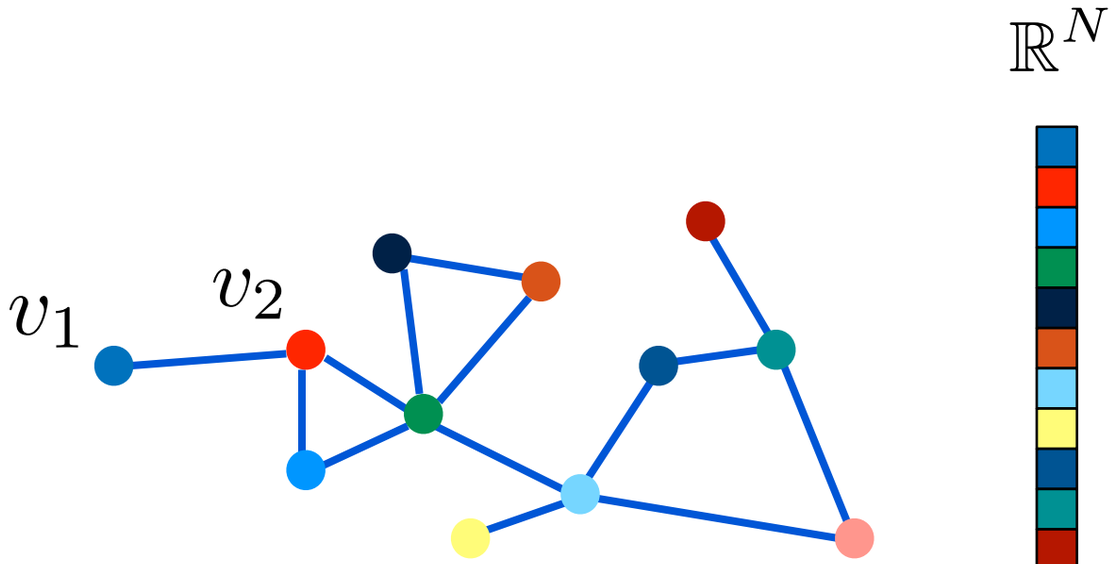
$\mathbb{R}^N$

- Fourier-like analysis



$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ $\quad f : \mathcal{V} \to \mathbb{R}$ $\quad \chi$ $\quad f$

Graph signal processing

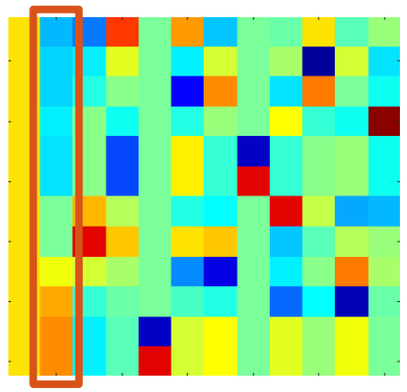


$\mathbb{R}^N$

$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$

$f : \mathcal{V} \to \mathbb{R}$

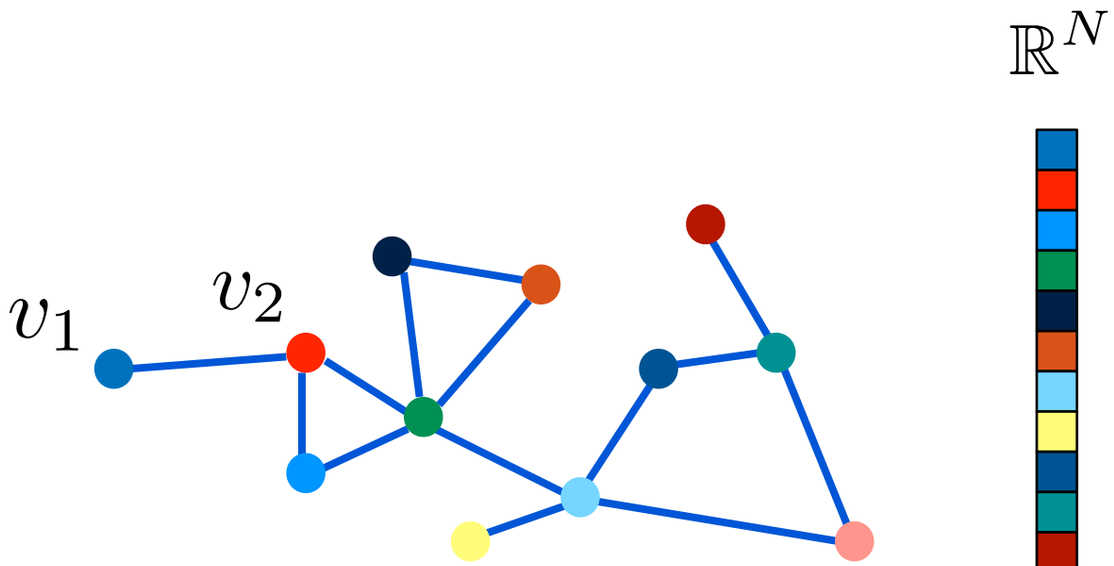
- Fourier-like analysis



χ

f

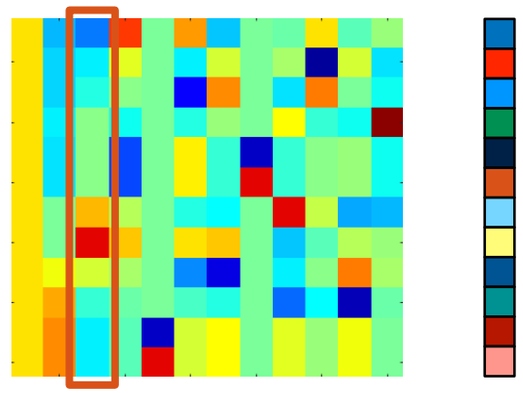
Graph signal processing



$\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$

$f : \mathcal{V} \to \mathbb{R}$

- Fourier-like analysis



χ

f

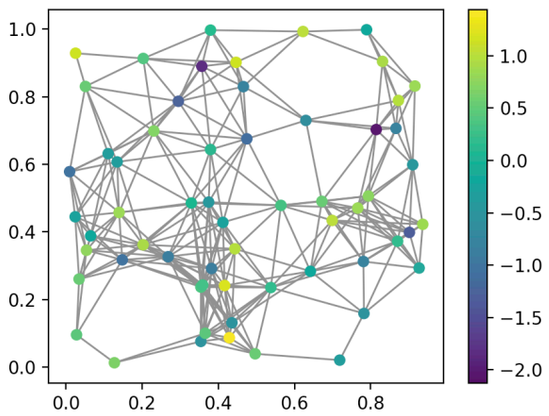
Graph spectral filtering

GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

Graph spectral filtering

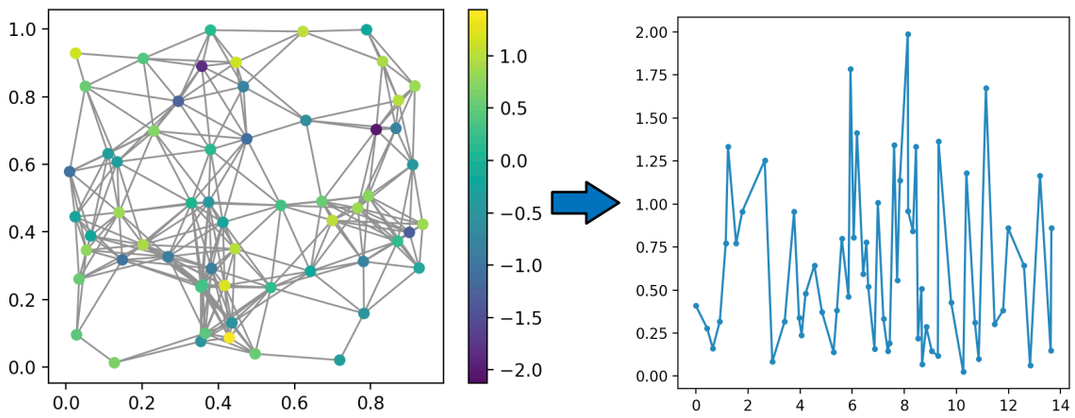
GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

f



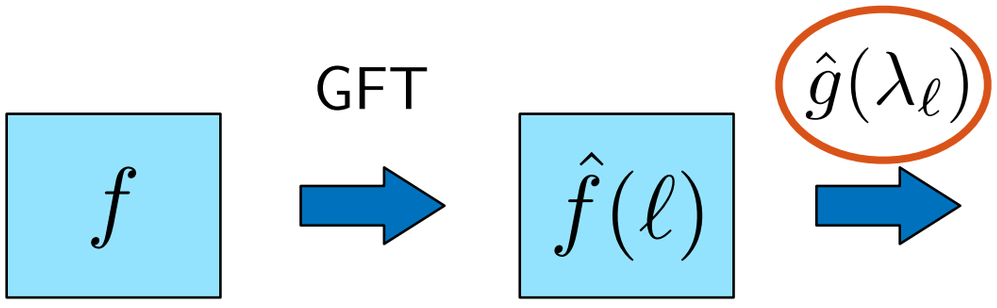
Graph spectral filtering

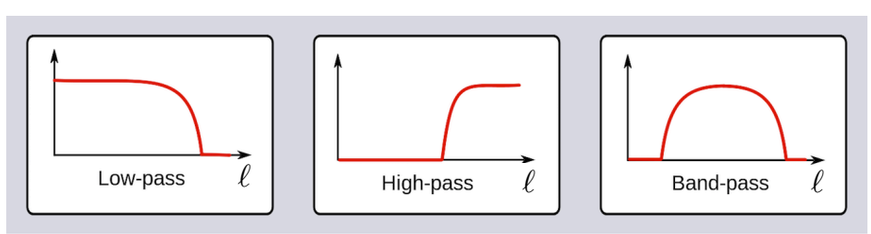
GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

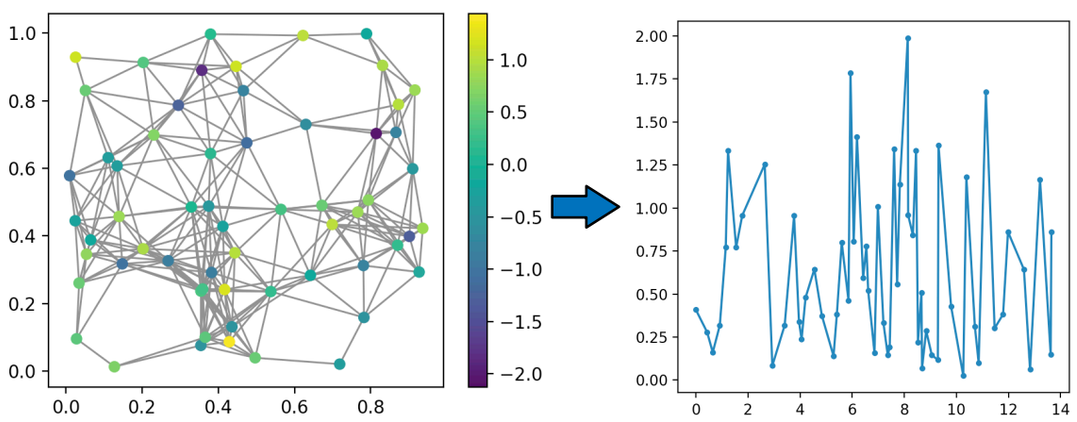


Graph spectral filtering

GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

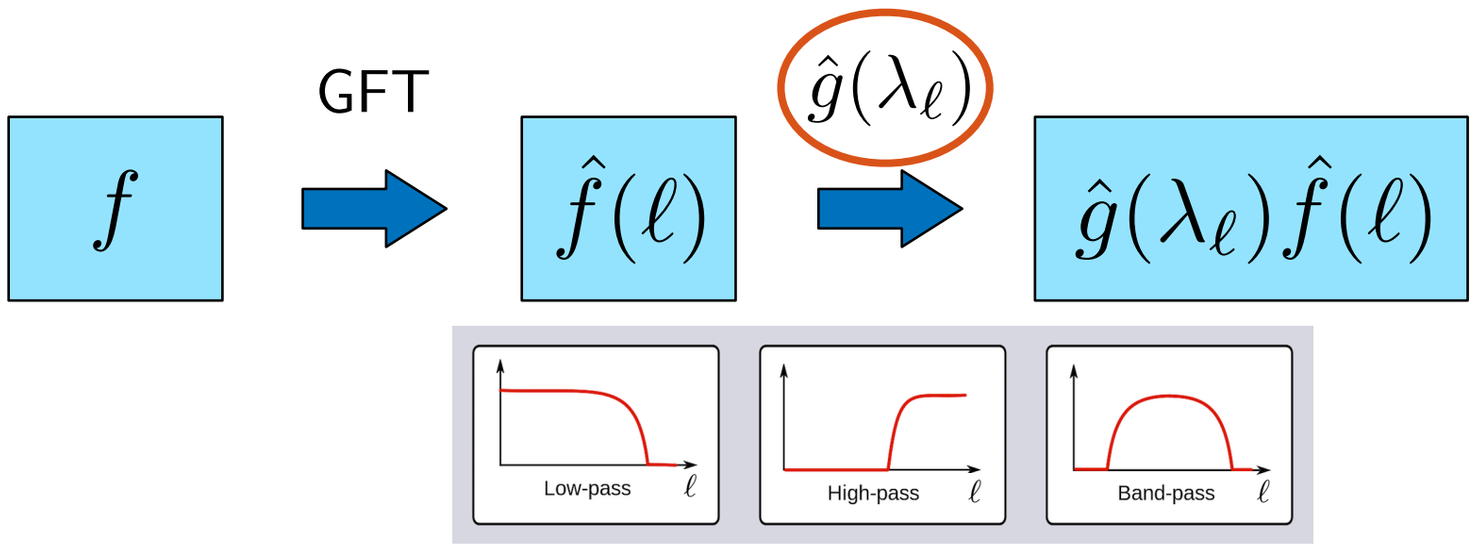


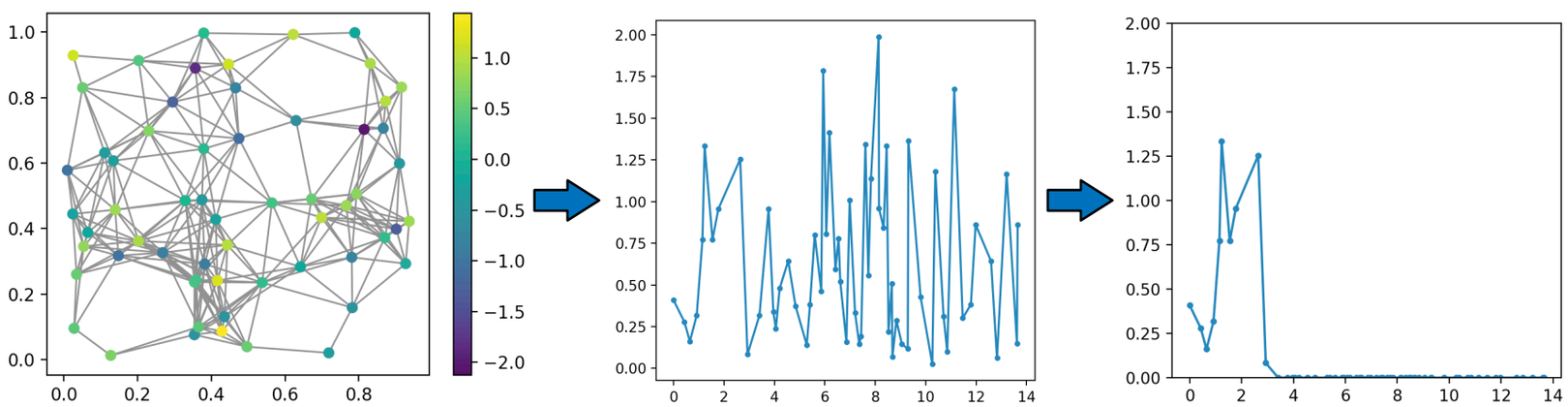




Graph spectral filtering

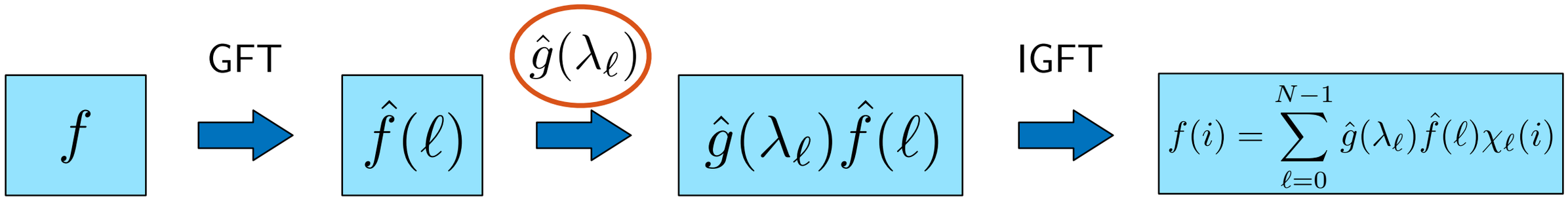
GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

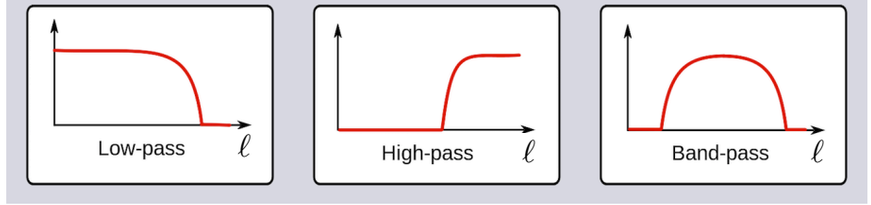


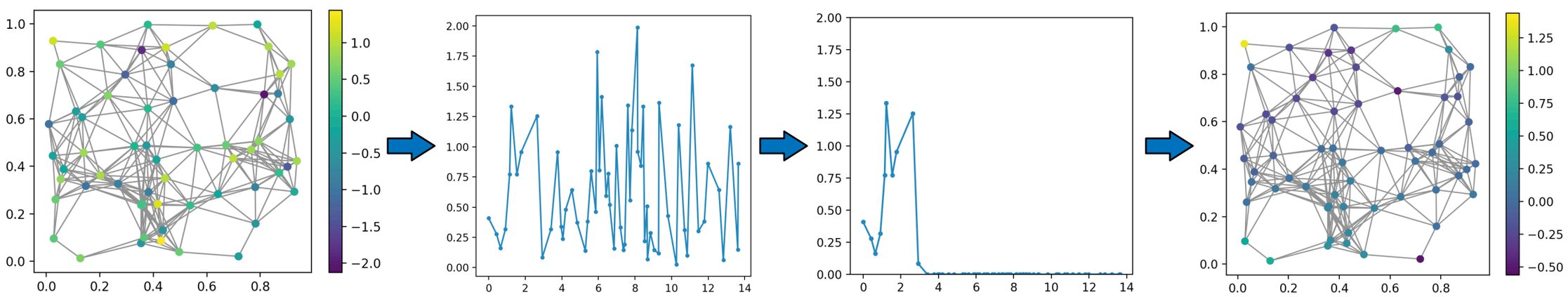


Graph spectral filtering

GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$

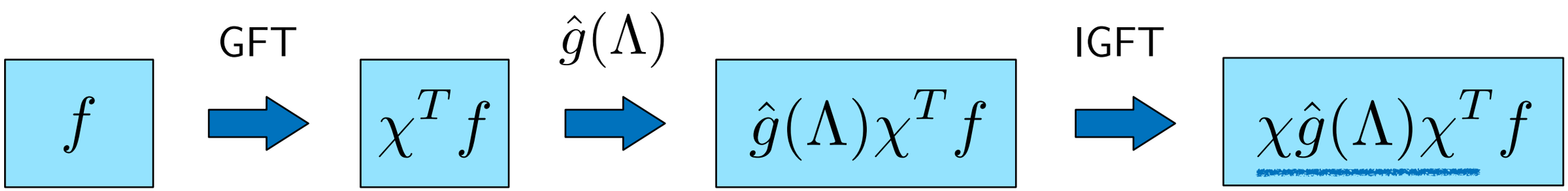






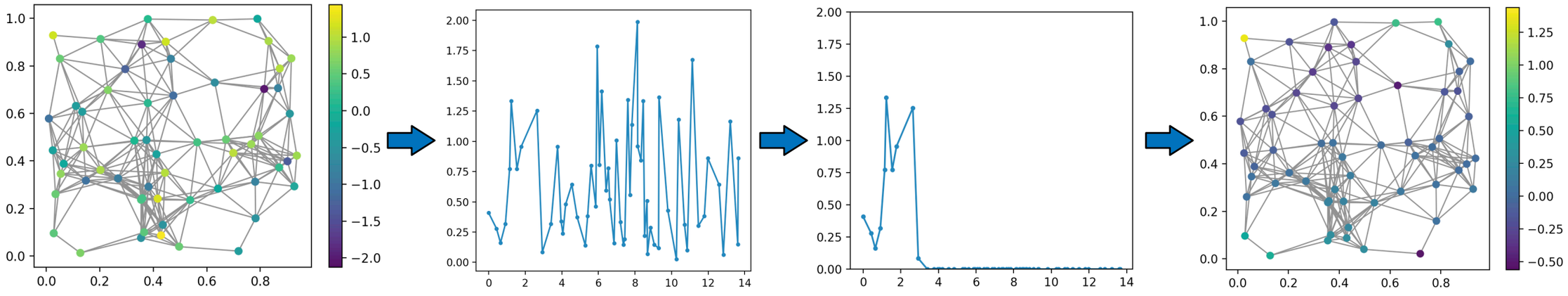
Graph spectral filtering

GFT: $\hat{f}(\ell) = \langle \chi_\ell, f \rangle = \sum_{i=1}^{N} \chi_\ell^*(i) f(i)$ IGFT: $f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\ell) \chi_\ell(i)$



spectral graph filter

$\hat{g}(L)$ **: function of L!**

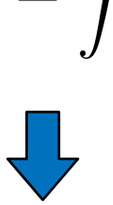


Convolution on graphs

classical convolution

time domain

$$(f * g)(t) = \int_{-\infty}^{\infty} f(t-\tau)g(\tau)d\tau$$



frequency domain

$$\widehat{(f * g)}(\omega) = \hat{f}(\omega) \cdot \hat{g}(\omega)$$

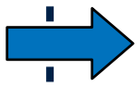
convolution on graphs

spatial (node) domain

$$f * g = \chi \hat{g}(\Lambda)\chi^T f = \hat{g}(L)f$$

graph spectral domain

$$\widehat{(f * g)}(\lambda) = \big((\chi^T f) \circ \hat{g}\big)(\lambda)$$



Convolution on graphs

classical convolution

time domain

$$(f * g)(t) = \int_{-\infty}^{\infty} f(t-\tau)g(\tau)d\tau$$

frequency domain

$$\widehat{(f * g)}(\omega) = \hat{f}(\omega) \cdot \hat{g}(\omega)$$

convolution on graphs

spatial (node) domain

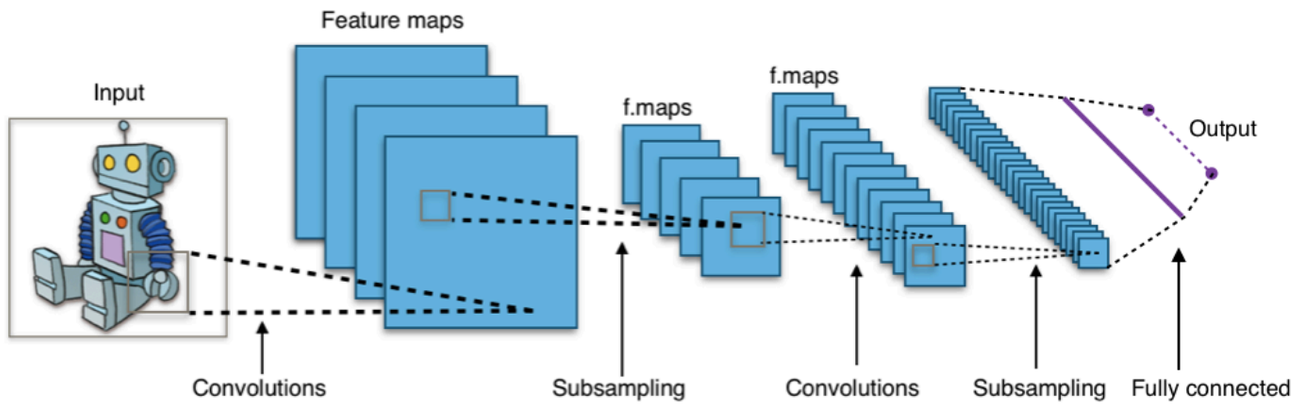
$$f * g = \chi \hat{g}(\Lambda)\chi^T f = \hat{g}(L)f$$

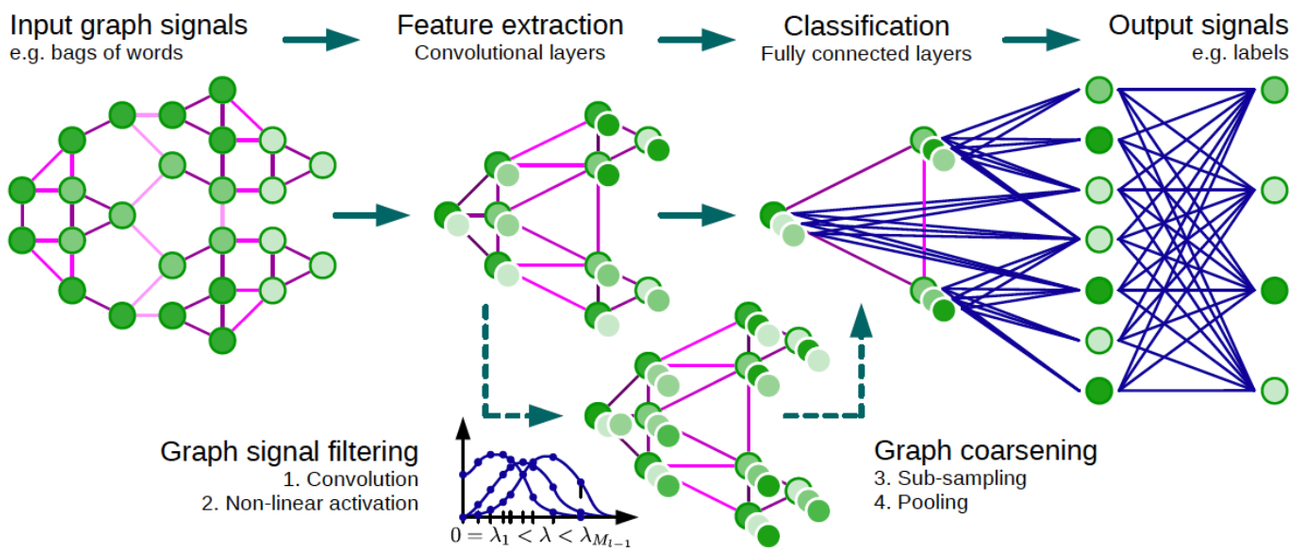
convolution = filtering

graph spectral domain

$$\widehat{(f * g)}(\lambda) = \big((\chi^T f) \circ \hat{g}\big)(\lambda)$$

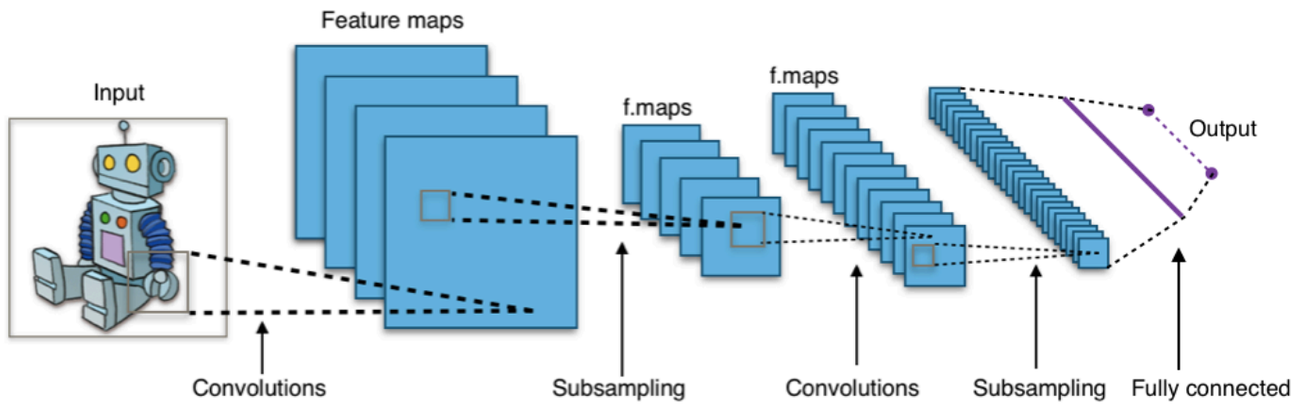
Convolutional neural networks on graphs

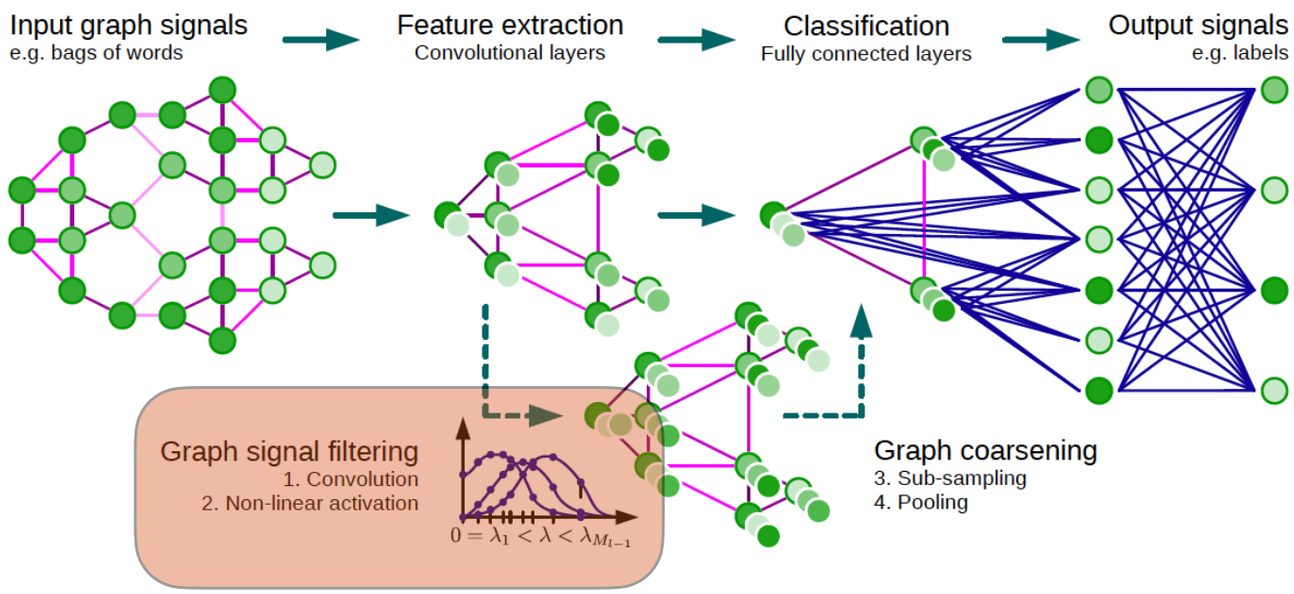




Defferrard et al., "Convolutional neural networks on graphs with fast localized spectral filtering," NIPS, 2016.

Convolutional neural networks on graphs



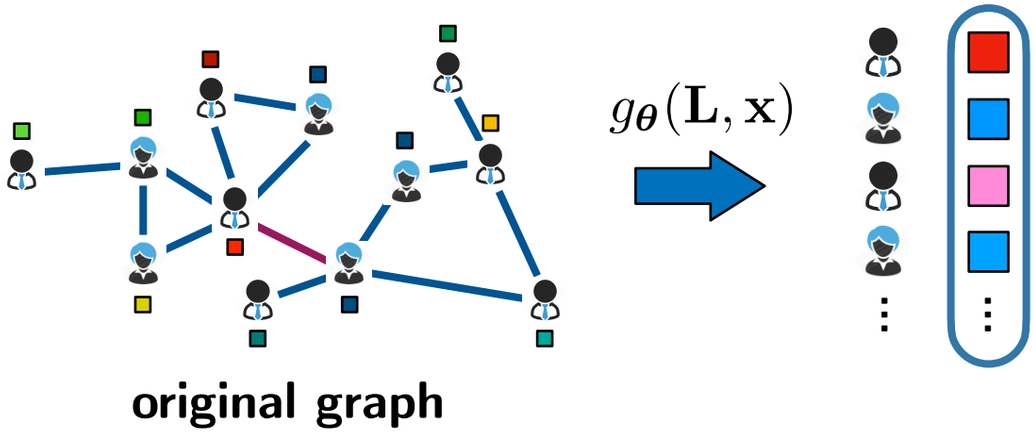


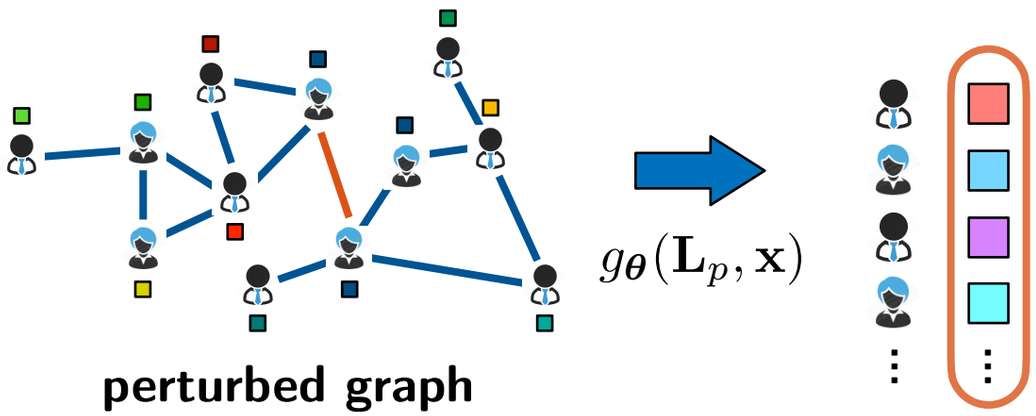
Defferrard et al., "Convolutional neural networks on graphs with fast localized spectral filtering," NIPS, 2016.

Outline

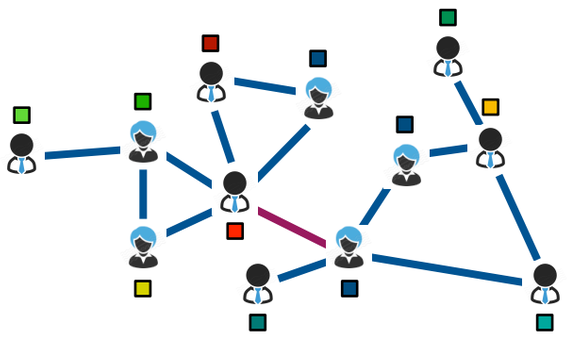
- Brief introduction to spectral graph filters
- Interpretable stability bounds for spectral graph filters
- Further results on robustness of graph machine learning models

Problem formulation



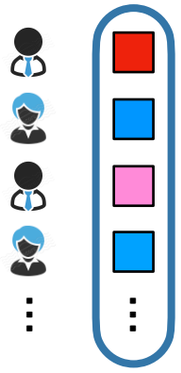


Problem formulation



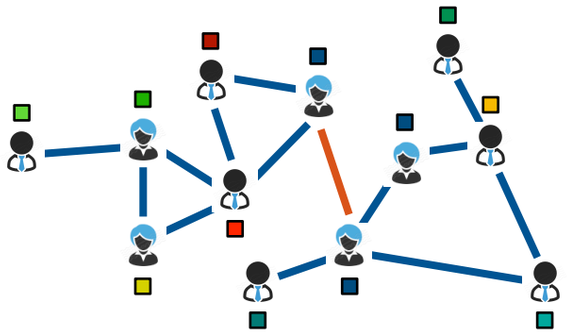
original graph

$g_{\boldsymbol{\theta}}(\mathbf{L}, \mathbf{x})$



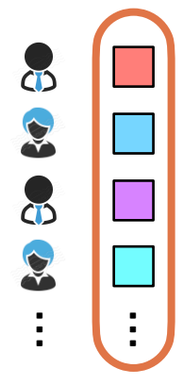
Objectives

- how filter output changes under perturbation



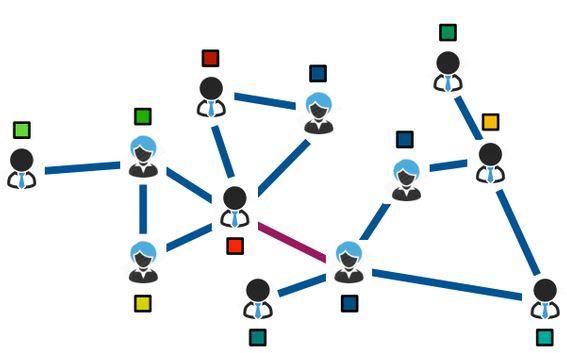
perturbed graph

$g_{\boldsymbol{\theta}}(\mathbf{L}_p, \mathbf{x})$



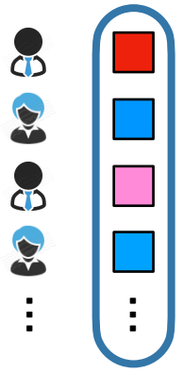
$$\frac{||g_{\boldsymbol{\theta}}(\mathbf{L}, \mathbf{x}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p, \mathbf{x})||_2}{||\mathbf{x}||_2}$$

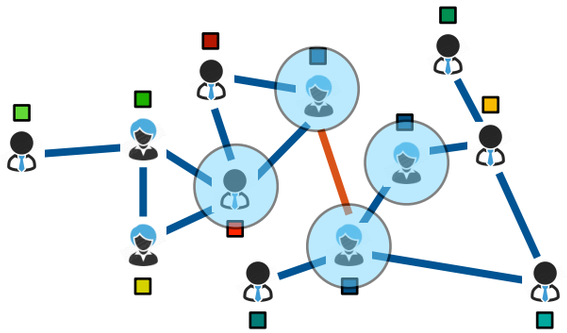
Problem formulation



original graph

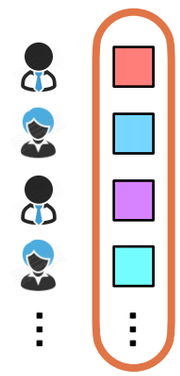
$g_{\boldsymbol{\theta}}(\mathbf{L}, \mathbf{x})$





perturbed graph

$g_{\boldsymbol{\theta}}(\mathbf{L}_p, \mathbf{x})$



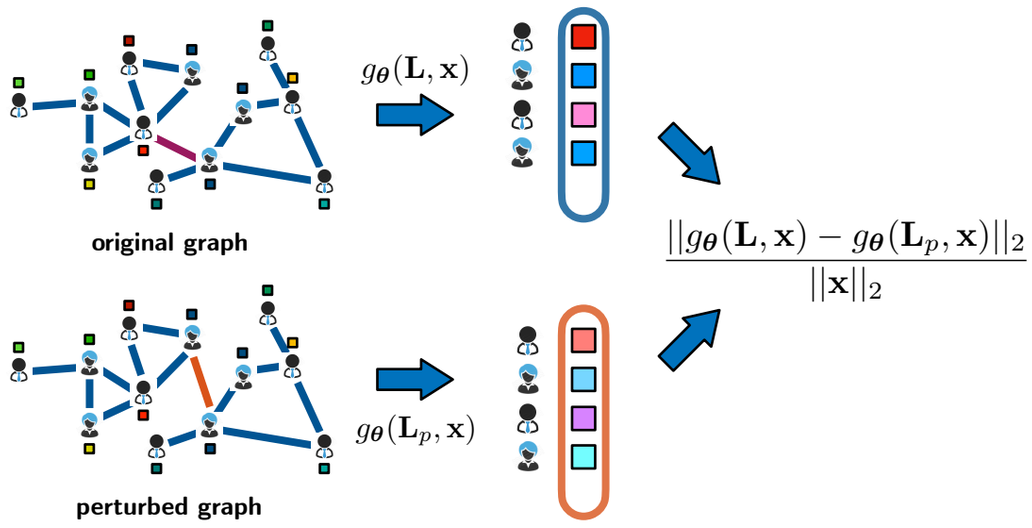
Objectives

- how filter output changes under perturbation

$$\frac{||g_{\boldsymbol{\theta}}(\mathbf{L}, \mathbf{x}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p, \mathbf{x})||_2}{||\mathbf{x}||_2}$$

- impact of structural properties of perturbation

Problem formulation



Setting

- stability via relative output distance: $\frac{||g_{\boldsymbol{\theta}}(\mathbf{L}, \mathbf{x}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p, \mathbf{x})||_2}{||\mathbf{x}||_2}$
- filter parameters $\boldsymbol{\theta}$ fixed
- filter defined via normalised Laplacian: $\mathbf{L}_{uv} = \begin{cases} 1 & \text{if } u = v \\ \frac{-1}{\sqrt{d_u d_v}} & \text{if } u \sim v \text{ and } u \neq v \\ 0 & \text{otherwise} \end{cases}$
- edge deletions/additions
- error (perturbation) matrix: $\mathbf{E} = \mathbf{L}_p - \mathbf{L}$

Main result

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u\delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u\delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u\delta_u}} \right\}$$

Levie et al., "On the transferability of spectral graph filters," SampTA, 2019.
Kenlay et al., "On the stability of polynomial spectral graph filters," IEEE ICASSP, 2020.
Kenlay et al., "Interpretable stability bounds for spectral graph filters," ICML, 2021.

Main result

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u\delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u\delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u\delta_u}} \right\}$$

step 1

by definition of filter distance: $\max_{\mathbf{x}\neq\mathbf{0}} \frac{||g_{\boldsymbol{\theta}}(\mathbf{L})\mathbf{x} - g_{\boldsymbol{\theta}}(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \stackrel{\text{def}}{=} ||g_{\boldsymbol{\theta}}(\mathbf{L}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p)||_2$

Levie et al., "On the transferability of spectral graph filters," SampTA, 2019.
Kenlay et al., "On the stability of polynomial spectral graph filters," IEEE ICASSP, 2020.
Kenlay et al., "Interpretable stability bounds for spectral graph filters," ICML, 2021.

Main result

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u\delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u\delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u\delta_u}} \right\}$$

step 1 — by definition of filter distance: $\max_{\mathbf{x}\neq\mathbf{0}} \frac{||g_{\boldsymbol{\theta}}(\mathbf{L})\mathbf{x} - g_{\boldsymbol{\theta}}(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \stackrel{\text{def}}{=} ||g_{\boldsymbol{\theta}}(\mathbf{L}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p)||_2$

step 2 — by linear stability of spectral graph filters [Levie19, Kenlay20,21]

Levie et al., "On the transferability of spectral graph filters," SampTA, 2019.
Kenlay et al., "On the stability of polynomial spectral graph filters," IEEE ICASSP, 2020.
Kenlay et al., "Interpretable stability bounds for spectral graph filters," ICML, 2021.

Main result

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

step 1 — by definition of filter distance: $\max_{\mathbf{x} \neq \mathbf{0}} \frac{||g_{\boldsymbol{\theta}}(\mathbf{L})\mathbf{x} - g_{\boldsymbol{\theta}}(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \stackrel{\text{def}}{=} ||g_{\boldsymbol{\theta}}(\mathbf{L}) - g_{\boldsymbol{\theta}}(\mathbf{L}_p)||_2$

step 2 — by linear stability of spectral graph filters [Levie19, Kenlay20,21]

step 3 — by linking norm of error matrix to structural change [Kenlay21]

Interpretation: stability of spectral graph filters in terms of **structural properties** of graph and edges added/deleted

Levie et al., "On the transferability of spectral graph filters," SampTA, 2019.
Kenlay et al., "On the stability of polynomial spectral graph filters," IEEE ICASSP, 2020.
Kenlay et al., "Interpretable stability bounds for spectral graph filters," ICML, 2021.

Linear stability of spectral graph filters

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Linear stability of spectral graph filters

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Consider low-pass filter $g(\lambda) = (1 + \alpha\lambda)^{-1}$

Proof Let $\mathbf{X} = \mathbf{I}_n + \alpha\mathbf{L}$ and $\mathbf{Y} = \mathbf{I}_n + \alpha\mathbf{L}_p$ then

$$||g(\mathbf{L}) - g(\mathbf{L}_p)||_2 = ||\mathbf{X}^{-1} - \mathbf{Y}^{-1}||_2 = ||\mathbf{X}^{-1}(\mathbf{Y} - \mathbf{X})\mathbf{Y}^{-1}||_2$$

$$\leq ||\mathbf{X}^{-1}||_2 ||\mathbf{Y}^{-1}||_2 ||\mathbf{X} - \mathbf{Y}||_2 \leq ||\mathbf{X} - \mathbf{Y}||_2 = \alpha||\mathbf{L} - \mathbf{L}_p||_2$$

Linear stability of spectral graph filters

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Consider low-pass filter $g(\lambda) = (1 + \alpha\lambda)^{-1}$

Proof Let $\mathbf{X} = \mathbf{I}_n + \alpha\mathbf{L}$ and $\mathbf{Y} = \mathbf{I}_n + \alpha\mathbf{L}_p$ then

$$||g(\mathbf{L}) - g(\mathbf{L}_p)||_2 = ||\mathbf{X}^{-1} - \mathbf{Y}^{-1}||_2 = ||\mathbf{X}^{-1}(\mathbf{Y} - \mathbf{X})\mathbf{Y}^{-1}||_2$$

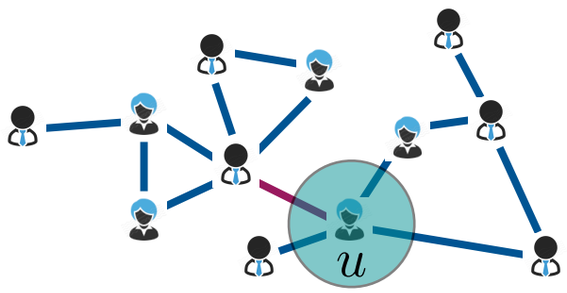
$$\leq ||\mathbf{X}^{-1}||_2 ||\mathbf{Y}^{-1}||_2 ||\mathbf{X} - \mathbf{Y}||_2 \leq ||\mathbf{X} - \mathbf{Y}||_2 = \alpha||\mathbf{L} - \mathbf{L}_p||_2$$

Table 1. Examples of linearly stable graph filters used for machine learning.

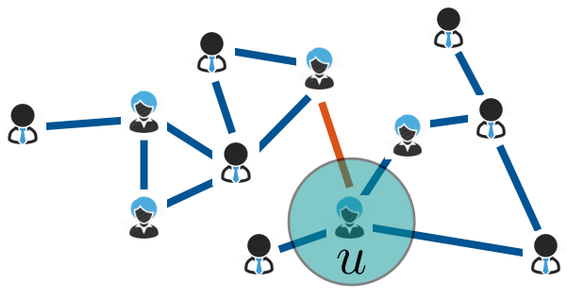
Filter	Functional form	GSO	Stability constant C	Use
Polynomial filter	$\sum_{k=0}^{K} \theta_k \lambda^k$	$\frac{2\mathbf{L}}{\lambda_{\max}} - \mathbf{I}_n$	$\sum_{k=1}^{K} k\lvert\theta_k\rvert$	Chebynet (Defferrard et al., 2016)
Low-pass filter	$(1 + \alpha\lambda)^{-1}$	$\mathbf{L}$	α	Low-pass filtering (Ramakrishna et al., 2020)
Monomial	λ^K	$\tilde{\mathbf{D}}^{-1/2}\tilde{\mathbf{A}}\tilde{\mathbf{D}}^{-1/2}$	K	Simple GCN (Wu et al., 2019)
Identity	λ	$\tilde{\mathbf{D}}^{-1/2}\tilde{\mathbf{A}}\tilde{\mathbf{D}}^{-1/2}$	1	GCN (Kipf & Welling, 2017)

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1 - \alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



original graph



perturbed graph

$\mathcal{A}_u, \mathcal{D}_u, \mathcal{R}_u$: sets of added/deleted/remained neighbours of u

Δ_u^-, Δ_u^+ : #edges deleted/added at u

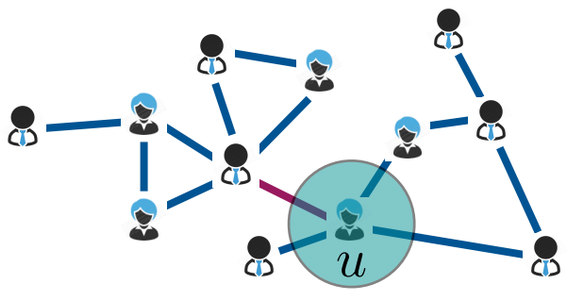
d_u, d'_u : degree of u before/after

δ_u, δ'_u : smallest degree of neighbours of u before/after

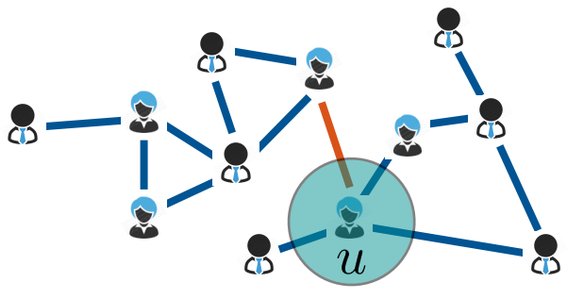
α_u : $\max_{v \in \mathcal{N}_u \cup \{u\}} |\Delta_v^+ - \Delta_v^-|/d_v$

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



original graph



perturbed graph

$\mathcal{A}_u, \mathcal{D}_u, \mathcal{R}_u$: sets of added/deleted/remained neighbours of u

Δ_u^-, Δ_u^+ : #edges deleted/added at u

d_u, d'_u : degree of u before/after

δ_u, δ'_u : smallest degree of neighbours of u before/after

α_u : $\max_{v \in \mathcal{N}_u \cup \{u\}} |\Delta_v^+ - \Delta_v^-|/d_v$

$\Delta_u^+ = 1, \Delta_u^- = 1$

$d_u = 4, d'_u = 4$

$\delta_u = 1, \delta'_u = 1$

$\alpha_u = 0.2$

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Idea 1. $||\mathbf{E}||_2^2 \leq ||\mathbf{E}||_1 ||\mathbf{E}||_\infty$ ⇒ $||\mathbf{E}||_2 \leq ||\mathbf{E}||_1 = \max_{u \in \mathcal{V}} ||\mathbf{E}_u||_1$

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Idea

1. $||\mathbf{E}||_2^2 \leq ||\mathbf{E}||_1 ||\mathbf{E}||_\infty \Rightarrow ||\mathbf{E}||_2 \leq ||\mathbf{E}||_1 = \max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1$

2. $||\mathbf{E}_u||_1 = \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} + \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} + \sum_{v\in\mathcal{R}_u} |\frac{1}{\sqrt{d_u d_v}} - \frac{1}{\sqrt{d'_u d'_v}}|$

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Idea

1. $||\mathbf{E}||_2^2 \leq ||\mathbf{E}||_1 ||\mathbf{E}||_\infty \Rightarrow ||\mathbf{E}||_2 \leq ||\mathbf{E}||_1 = \max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1$
2. $||\mathbf{E}_u||_1 = \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} + \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} + \sum_{v\in\mathcal{R}_u} |\frac{1}{\sqrt{d_u d_v}} - \frac{1}{\sqrt{d'_u d'_v}}|$
3. $\sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} \leq \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u \delta_u}} = \frac{\Delta_u^-}{\sqrt{d_u \delta_u}}$

Bounding error w.r.t. structural change

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Idea

1. $||\mathbf{E}||_2^2 \leq ||\mathbf{E}||_1 ||\mathbf{E}||_\infty \Rightarrow ||\mathbf{E}||_2 \leq ||\mathbf{E}||_1 = \max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1$
2. $||\mathbf{E}_u||_1 = \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} + \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} + \sum_{v\in\mathcal{R}_u} |\frac{1}{\sqrt{d_u d_v}} - \frac{1}{\sqrt{d'_u d'_v}}|$
3. $\sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} \leq \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u \delta_u}} = \frac{\Delta_u^-}{\sqrt{d_u \delta_u}}$
4. $\sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} \leq \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u \delta'_u}} = \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}}$

Bounding error w.r.t. structural change

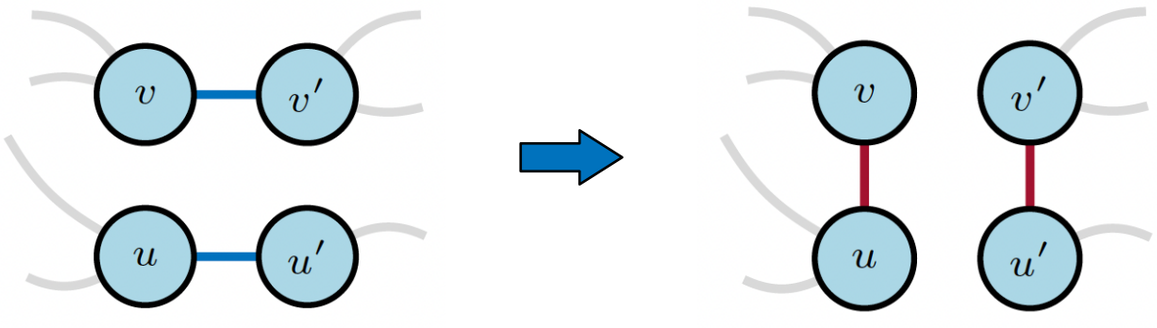
$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Idea

1. $||\mathbf{E}||_2^2 \leq ||\mathbf{E}||_1 ||\mathbf{E}||_\infty \Rightarrow ||\mathbf{E}||_2 \leq ||\mathbf{E}||_1 = \max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1$
2. $||\mathbf{E}_u||_1 = \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} + \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} + \sum_{v\in\mathcal{R}_u} |\frac{1}{\sqrt{d_u d_v}} - \frac{1}{\sqrt{d'_u d'_v}}|$
3. $\sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u d_v}} \leq \sum_{v\in\mathcal{D}_u} \frac{1}{\sqrt{d_u \delta_u}} = \frac{\Delta_u^-}{\sqrt{d_u \delta_u}}$
4. $\sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u d'_v}} \leq \sum_{v\in\mathcal{A}_u} \frac{1}{\sqrt{d'_u \delta'_u}} = \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}}$
5. $\sum_{v\in\mathcal{R}_u} |\frac{1}{\sqrt{d_u d_v}} - \frac{1}{\sqrt{d'_u d'_v}}| \leq \sum_{v\in\mathcal{R}_u} \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{1}{\sqrt{d_u d_v}} \leq \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}}$ (for $\alpha_u < 1$)

Special case: double edge rewiring

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1 - \alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



$$\Delta_u^+ = \Delta_u^- = r_u$$

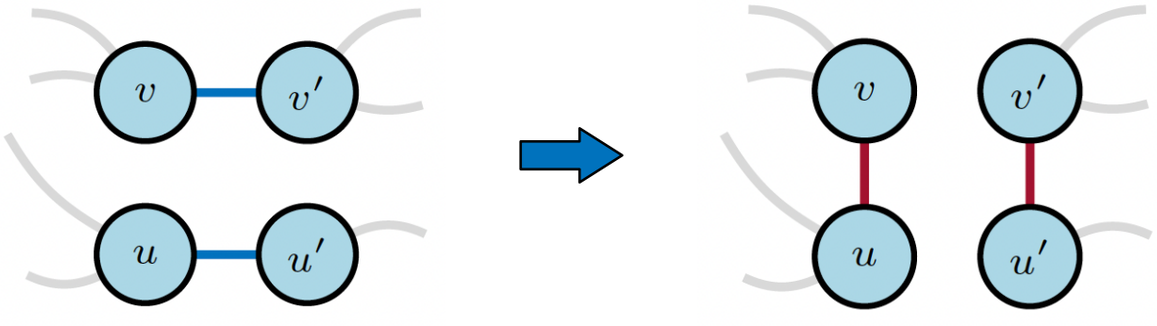
$$d_u = d'_u$$

$$\delta_u = \delta'_u$$

$$\alpha_u = 0$$

Special case: double edge rewiring

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \frac{2r_u}{\sqrt{d_u \delta_u}}$$



$$\Delta_u^+ = \Delta_u^- = r_u$$

$$d_u = d'_u$$

$$\delta_u = \delta'_u$$

$$\alpha_u = 0$$

Interpretable stability bounds

$$\frac{||g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \leq C||\mathbf{E}||_2 \leq C||\mathbf{E}||_1 = C \max_{u \in \mathcal{V}} ||\mathbf{E}_u||_1 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1 - \alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Interpretation A perturbation would cause small change in filter output if $\max_{u \in \mathcal{V}} ||\mathbf{E}_u||_1$ is small

Interpretable stability bounds

$$\frac{||g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \leq C||\mathbf{E}||_2 \leq C||\mathbf{E}||_1 = C \max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1 \leq C \max_{u\in\mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u}\right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Interpretation A perturbation would cause small change in filter output if $\max_{u\in\mathcal{V}} ||\mathbf{E}_u||_1$ is small

- small $||\mathbf{E}_u||_1$ for one node ➡ add/delete edges at high-degree nodes

Interpretable stability bounds

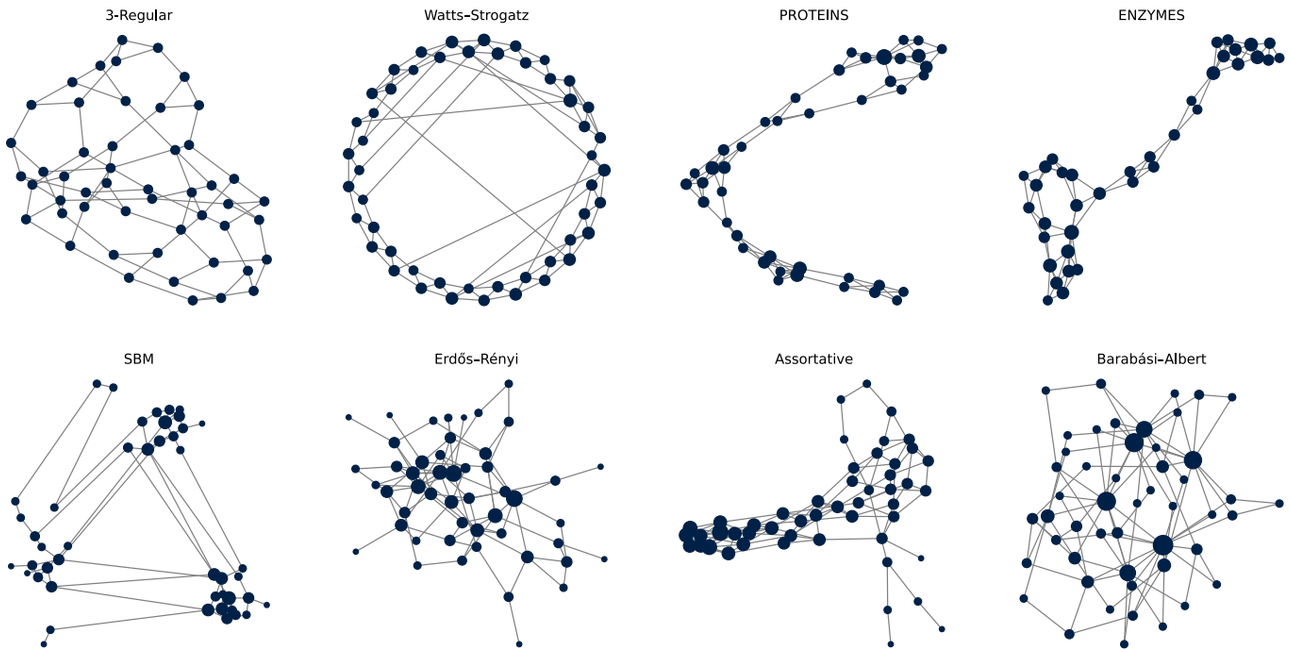
$$\frac{||g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}||_2}{||\mathbf{x}||_2} \leq C||\mathbf{E}||_2 \leq C||\mathbf{E}||_1 = C \max_{u \in \mathcal{V}} ||\mathbf{E}_u||_1 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1 - \alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

Interpretation A perturbation would cause small change in filter output if $\max_{u \in \mathcal{V}} ||\mathbf{E}_u||_1$ is small

- small $||\mathbf{E}_u||_1$ for one node ➡ add/delete edges at high-degree nodes
- small $||\mathbf{E}_u||_1$ for all nodes ➡ perturbation distributed across graph

Experimental setting

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$

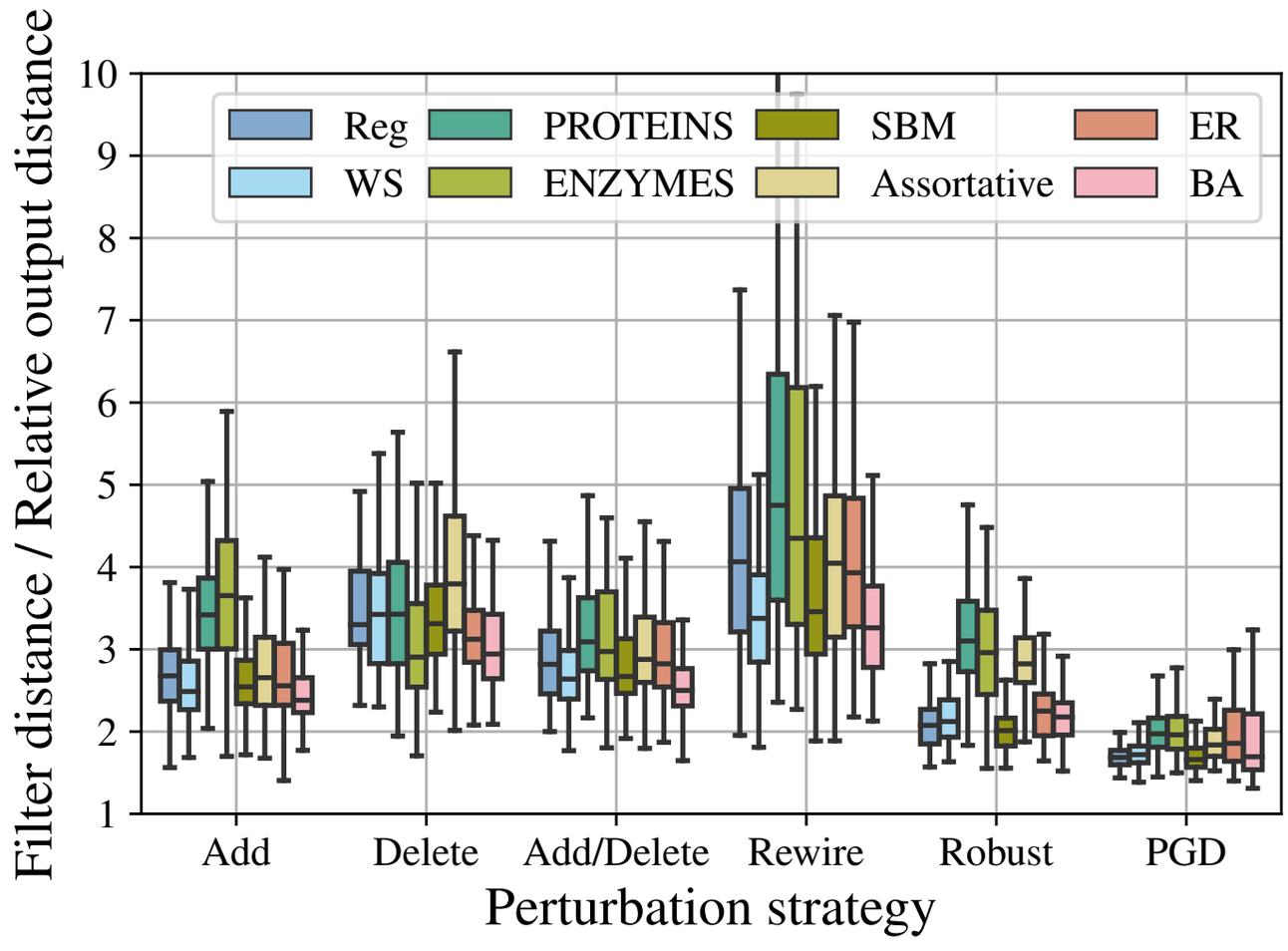


Perturbation strategies

- Add: random add
- Delete: random delete
- Add/Delete: random add/delete
- Rewire: double edge rewiring
- Robust: minimise $||\mathbf{E}||_1$
- PGD: maximise relative output distance

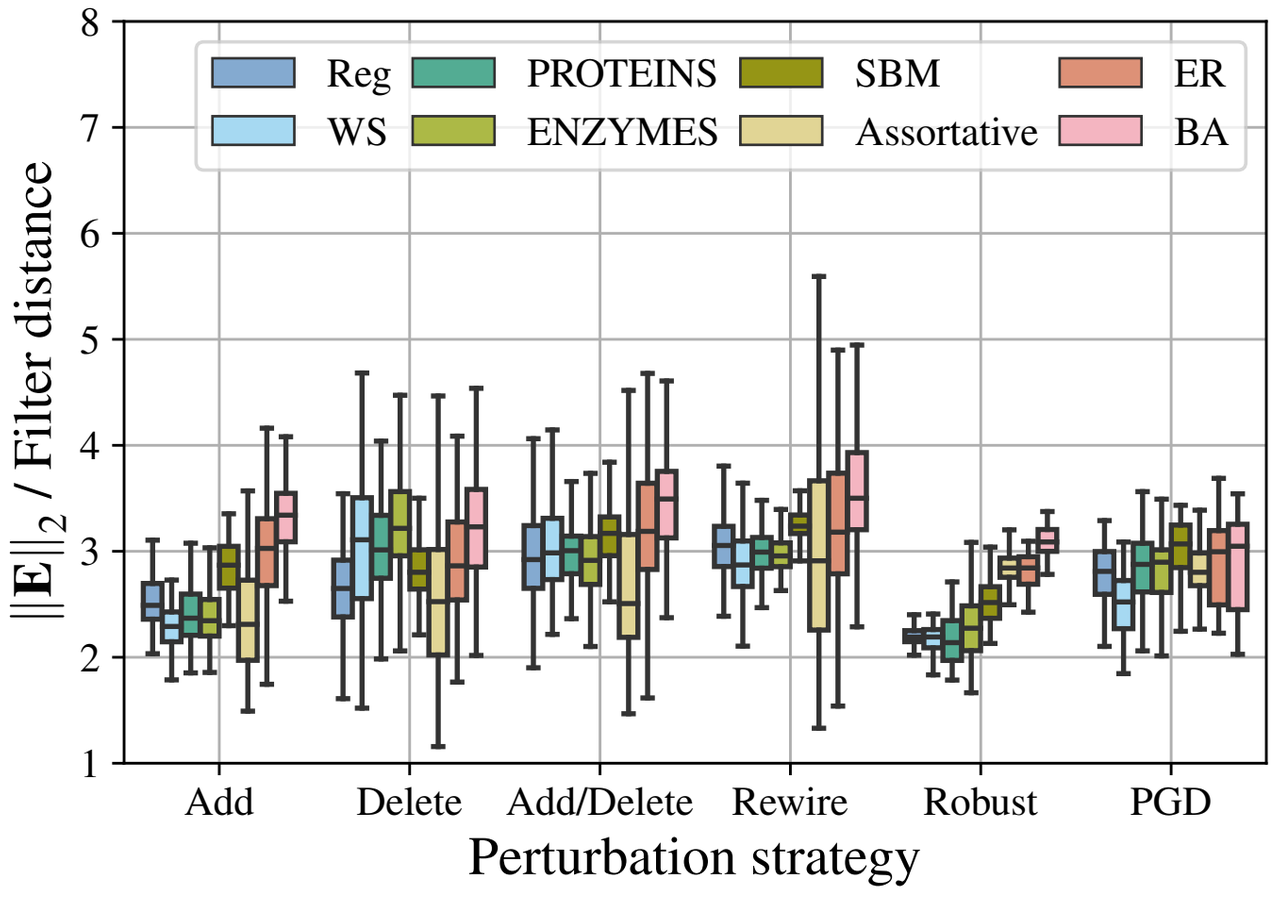
Analysis of stability bounds

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



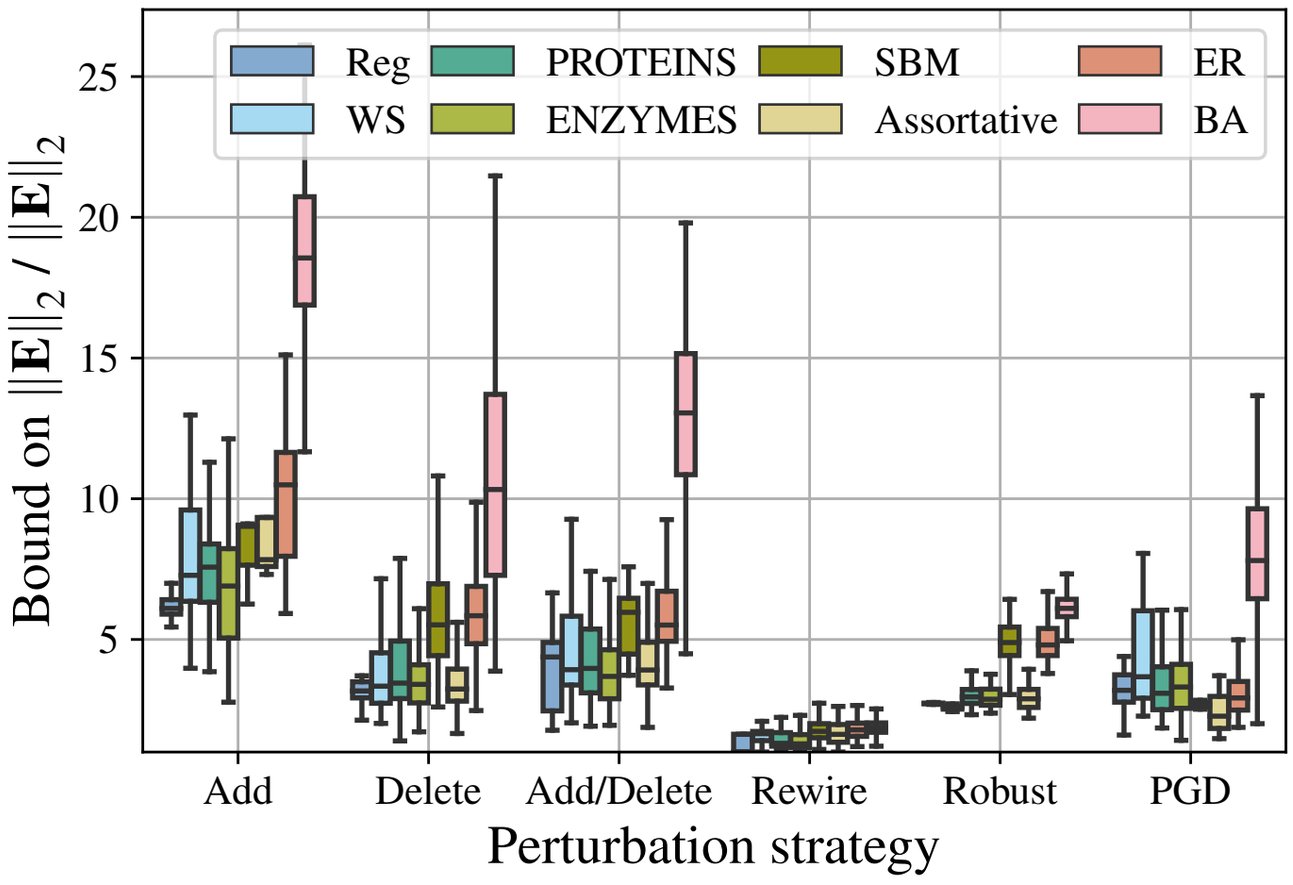
Analysis of stability bounds

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



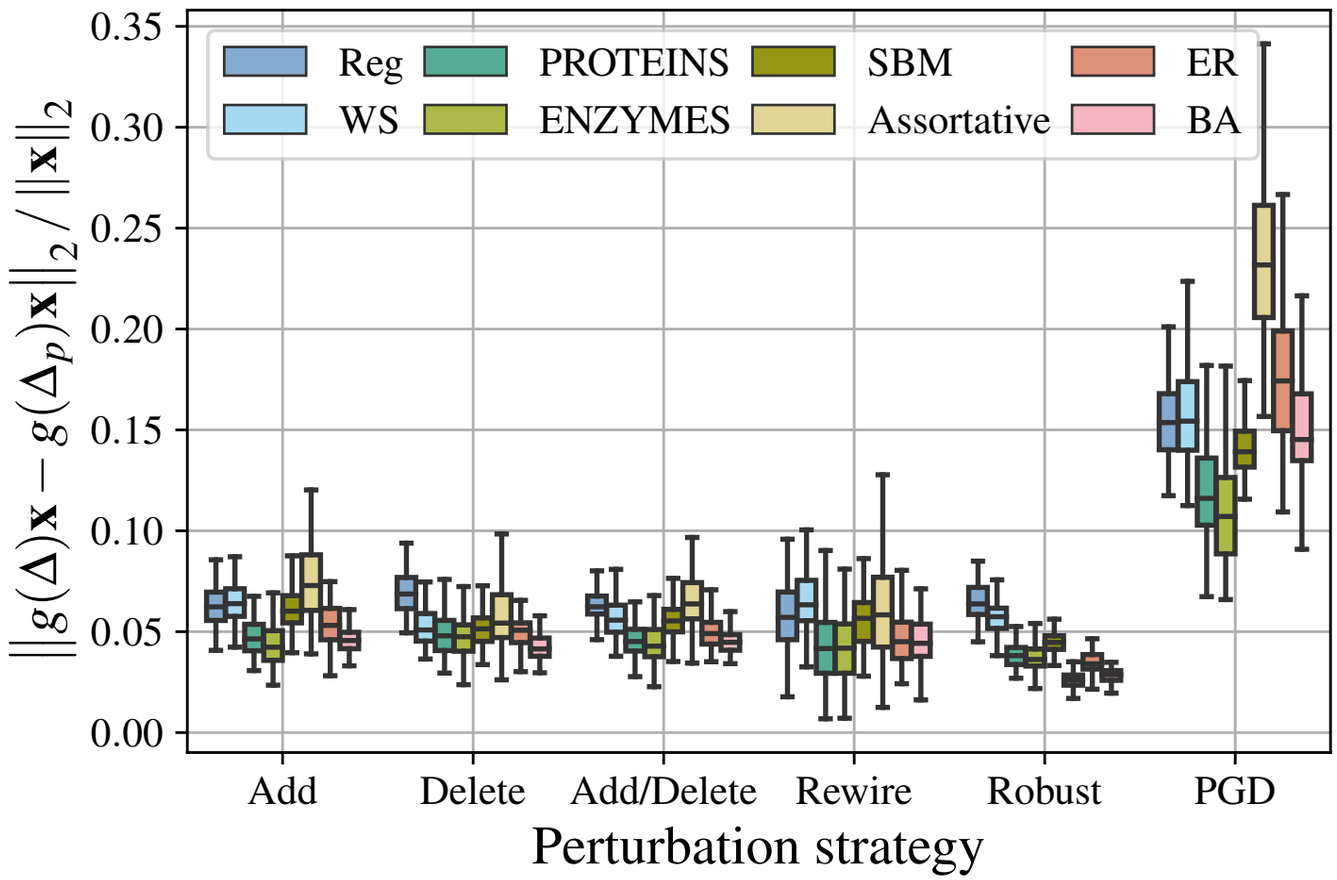
Analysis of stability bounds

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



Analysis of relative output distance

$$\frac{\|g_\theta(\mathbf{L})\mathbf{x} - g_\theta(\mathbf{L}_p)\mathbf{x}\|_2}{\|\mathbf{x}\|_2} \leq \|g_\theta(\mathbf{L}) - g_\theta(\mathbf{L}_p)\|_2 \leq C\|\mathbf{E}\|_2 \leq C \max_{u \in \mathcal{V}} \left\{ \frac{\Delta_u^-}{\sqrt{d_u \delta_u}} + \frac{\Delta_u^+}{\sqrt{d'_u \delta'_u}} + \left(\frac{\alpha_u}{1-\alpha_u} \right) \frac{d_u - \Delta_u^-}{\sqrt{d_u \delta_u}} \right\}$$



Analysis of perturbation examples

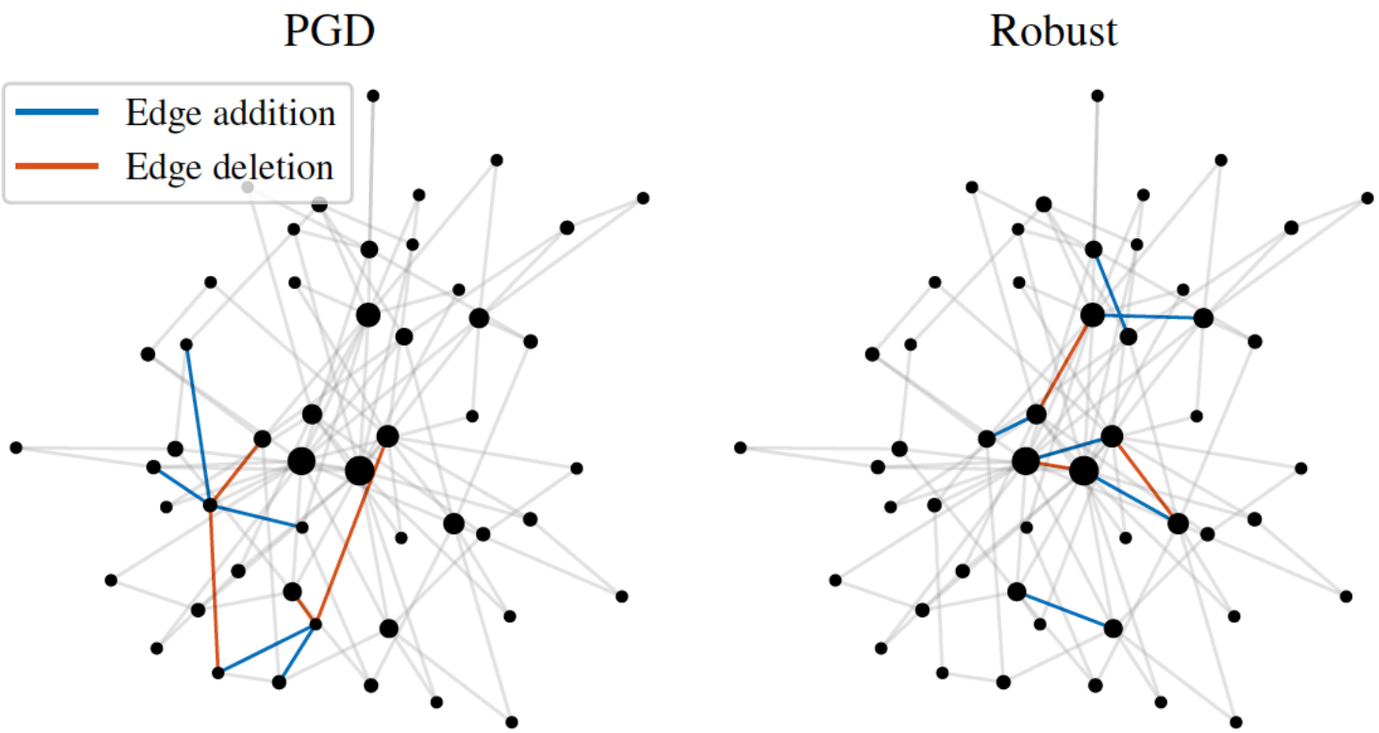


Figure 4. Perturbations of BA graphs ($n = 50$). The original and both perturbed graphs have a diameter of 5. The size of the node is proportional to the node degree.

Analysis of perturbation examples

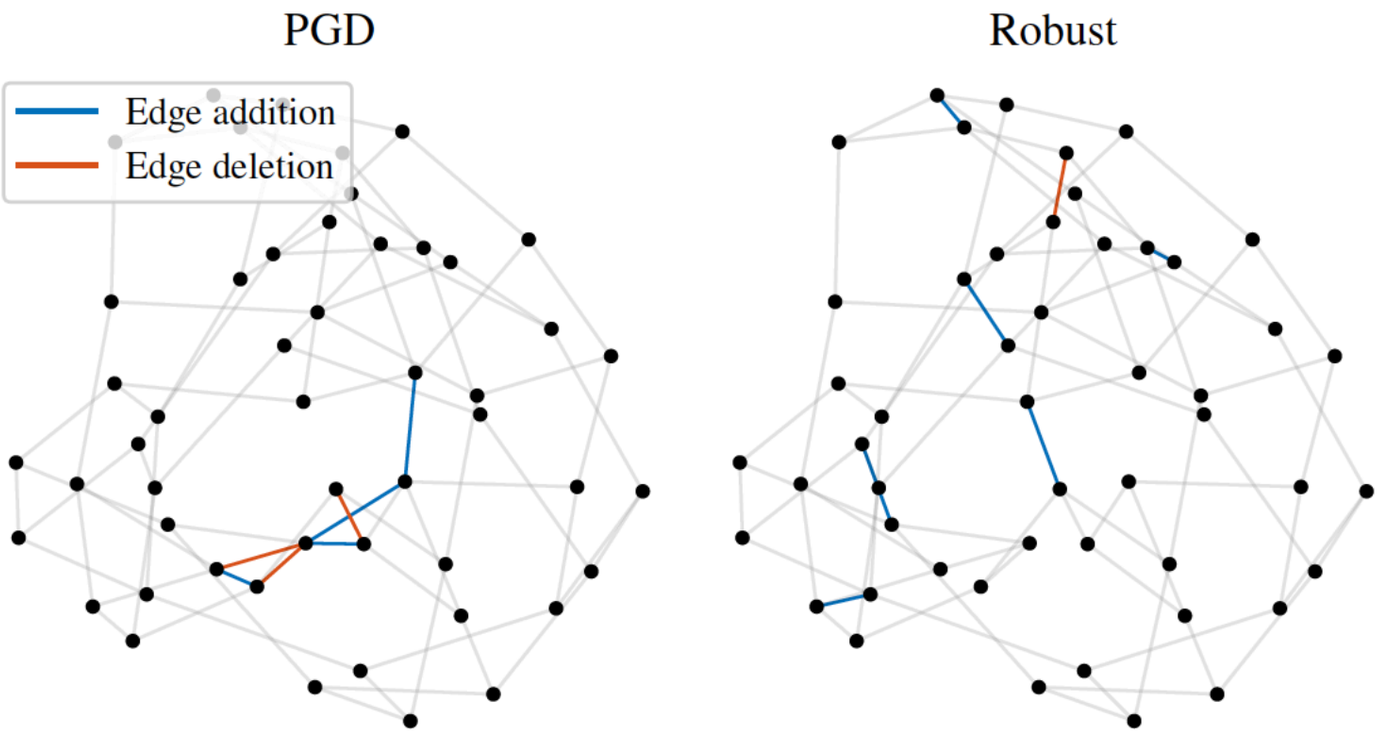


Figure 5. Perturbations of 3-regular graphs ($n = 50$).

Outline

- Brief introduction to spectral graph filters
- Interpretable stability bounds for spectral graph filters
- Further results on robustness of graph machine learning models

Stability results on GNNs

- GCN and SGCN: GNNs based on spectral graph filters
- Normalised augmented adjacency matrix + double edge rewiring

GCN

$$\mathbf{X}^{(l)} = \sigma(\boldsymbol{\Delta}\mathbf{X}^{(l-1)}\boldsymbol{\Theta}^{(l)})$$

SGCN

$$\mathbf{Y} = \operatorname{softmax}(\boldsymbol{\Delta}^K\mathbf{X}\boldsymbol{\Theta})$$

$$\underbrace{\|\mathbf{X}^{(L)} - \mathbf{X}_p^{(L)}\|_F}_{\text{GCN output change}} \leq \underbrace{\sqrt{d}}_{\text{data}}\ \underbrace{L\prod_{l=1}^{L}\|\boldsymbol{\Theta}^{(l)}\|_2}_{\text{model}}\ \underbrace{\|\mathbf{E}\|_2}_{\text{structural change}}$$

$$\underbrace{\|\boldsymbol{\Delta}^K\mathbf{X}\boldsymbol{\Theta} - \boldsymbol{\Delta}_p^K\mathbf{X}\boldsymbol{\Theta}\|_F}_{\text{SGCN output change}} \leq \underbrace{\sqrt{d}}_{\text{data}}\ \underbrace{K\boldsymbol{\Theta}}_{\text{model}}\ \underbrace{\|\mathbf{E}\|_2}_{\text{structural change}}$$

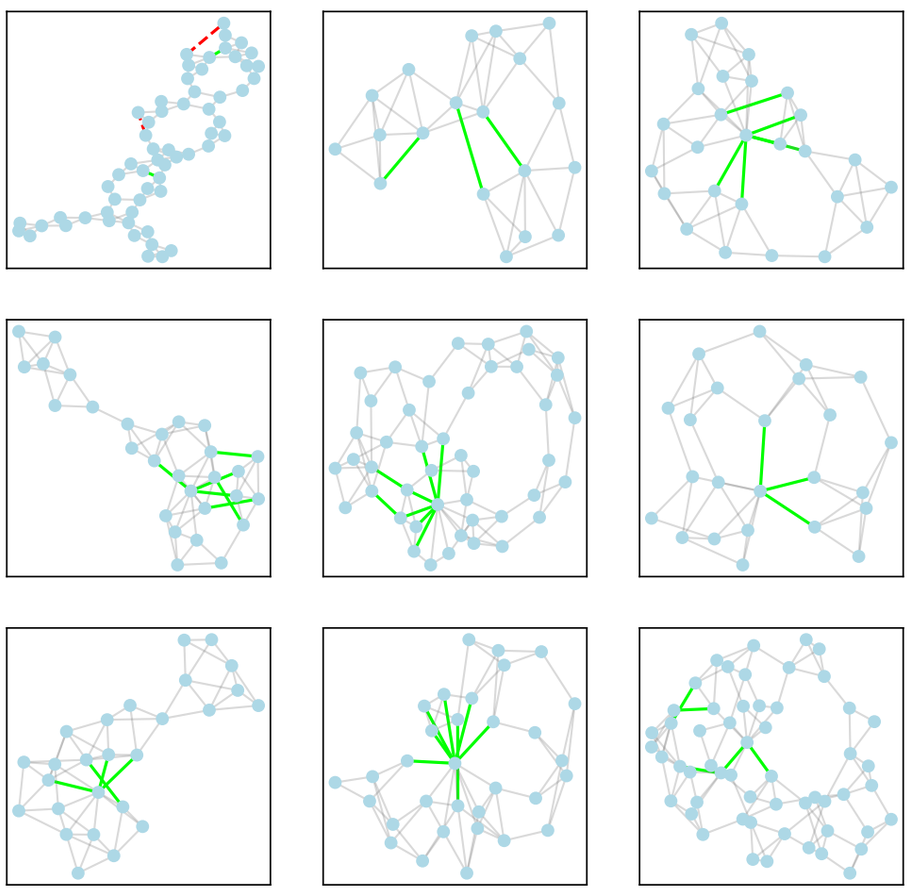
$$\underbrace{\|\mathbf{E}\|_2}_{\text{perturbation}} \leq \max_{u\in\mathcal{V}} \frac{2R_u}{\sqrt{(d_u+\gamma)(\delta_u+\gamma)}}$$

Kenlay et al., "On the stability of graph convolutional neural networks under edge rewiring," IEEE ICASSP, 2021.

Patterns of adversarial attacks on GNNs

- Topological attacks on graph classifiers
- Common structural patterns of successful attacks

PROTEINS+GCN: clustered adversarial perturbation

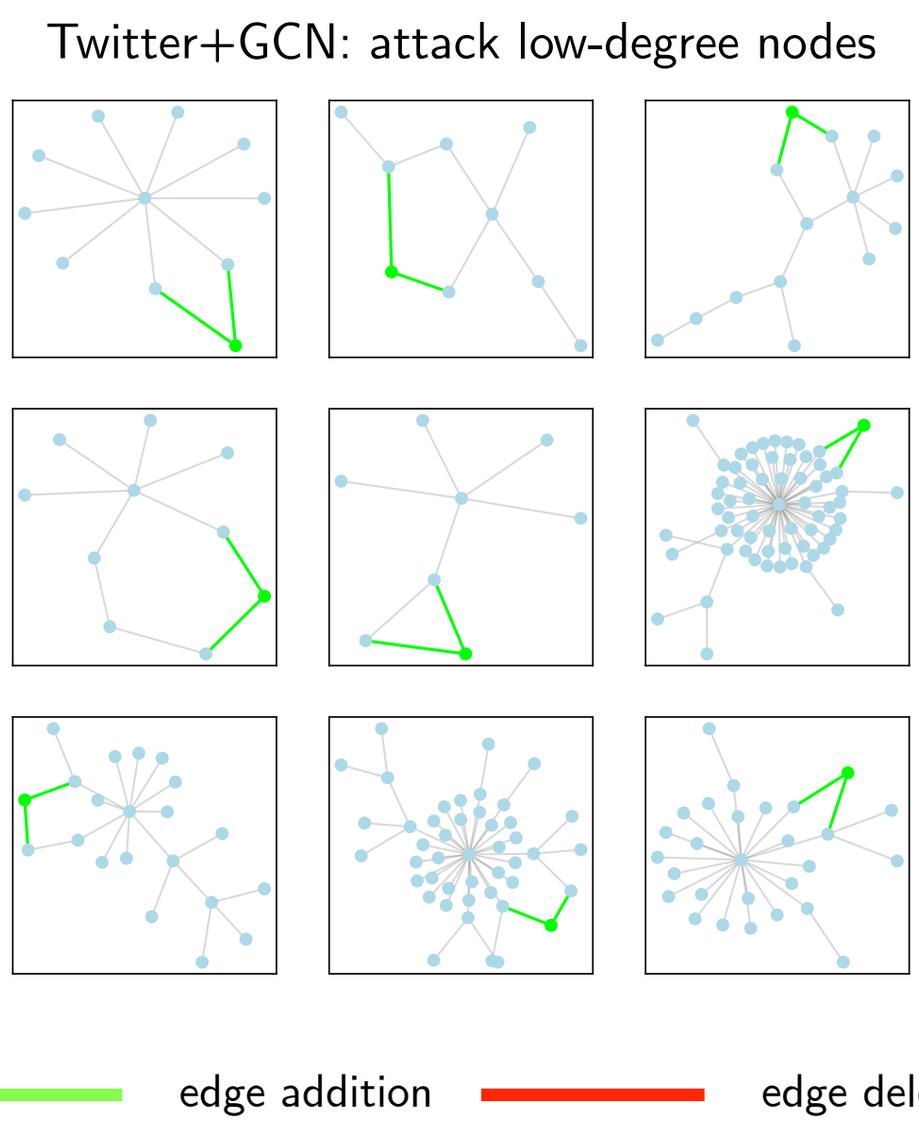


edge addition edge deletion

Wan et al., "Adversarial attacks on graph classification via Bayesian optimisation," NeurIPS, 2021.

Patterns of adversarial attacks on GNNs

- Topological attacks on graph classifiers
- Common structural patterns of successful attacks

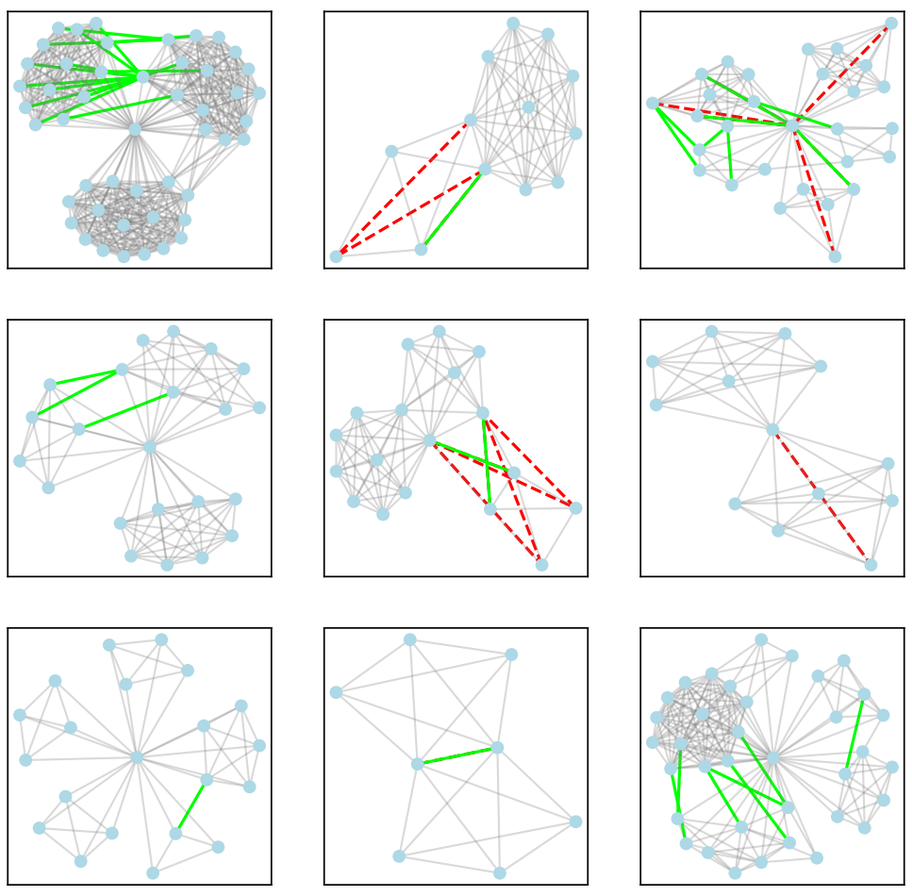


Wan et al., "Adversarial attacks on graph classification via Bayesian optimisation," NeurIPS, 2021.

Patterns of adversarial attacks on GNNs

- Topological attacks on graph classifiers
- Common structural patterns of successful attacks

IMDB-B+GCN: modify/destroy communities

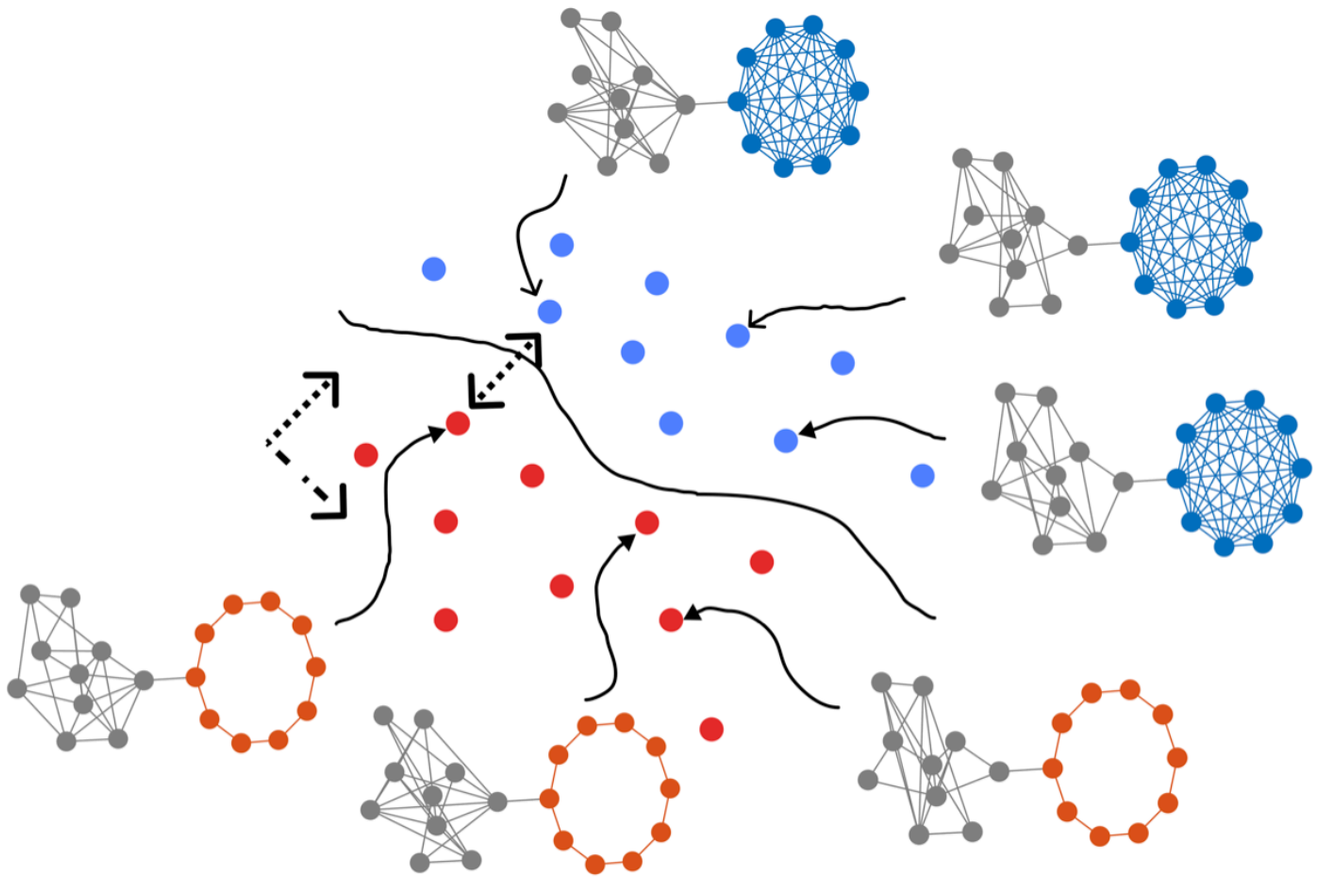


edge addition edge deletion

Wan et al., "Adversarial attacks on graph classification via Bayesian optimisation," NeurIPS, 2021.

Structure-aware robustness certificates

- Certified robustness on graph classification against topological attacks
- Quality of certificates depends on relative importance of substructure



Summary

- Stability of graph signal processing and machine learning models is an important problem
- Many open questions on robustness of graph models: data collection, model selection, training & inference
- Structural properties of the domain (and perturbation) often provide useful insight
- Interdisciplinary area connecting signal processing and machine learning with graph theory, geometry and topology