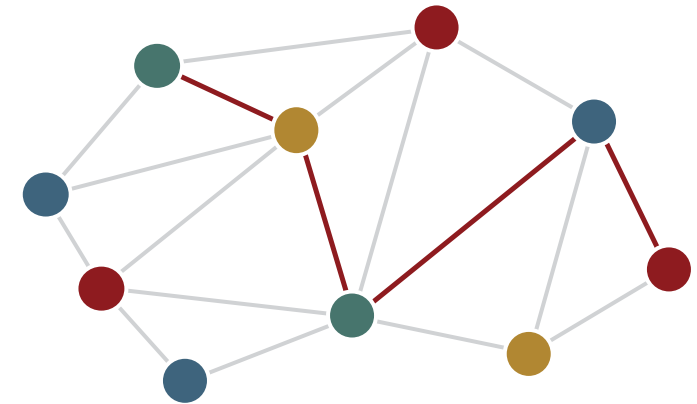


Stability of Graph Convolutional Filters and Graph Convolutional NNs



September 3

Zhiyang Wang · Electrical & Systems Engineering · WashU

Class 4 · Stability Analysis of Graph Filters and GNNs

Three questions organize the lecture

01**WHAT HAS CHANGED?**

Separate arbitrary node indexing from genuine changes in topology or edge weights -- absolute and relative perturbations

02**WHEN IS A FILTER STABLE?**

Match the perturbation model with the correct smoothness condition on $h(\lambda)$ -- Lipschitz or integral Lipschitz.

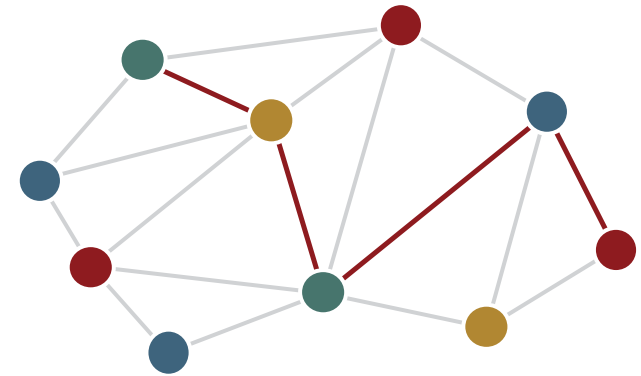
03**WHY CASCADE?**

Show that normalized nonlinear layers inherit stability while restoring discrimination.

PART I

Separate Graph Changes from Permutation Equivariance.

- 01 Equivariance is exact for any relabeling
- 02 Exact graph symmetries are rare and fragile
- 03 Align first: measure changes modulo permutation
- 04 Stability bounds the output error by ε



**Equivariance handles relabelings;
stability handles change.**

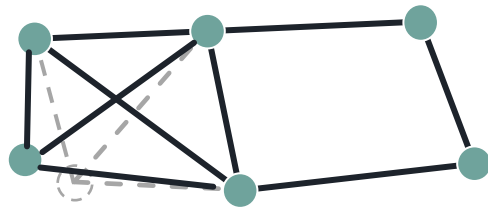
Stability matters in deployment and learning

DEPLOYMENT · THE GRAPH DRIFTS

Sensors move or fail.

Edge weights are *re-estimated*.

Controller sees graphs not present at training.

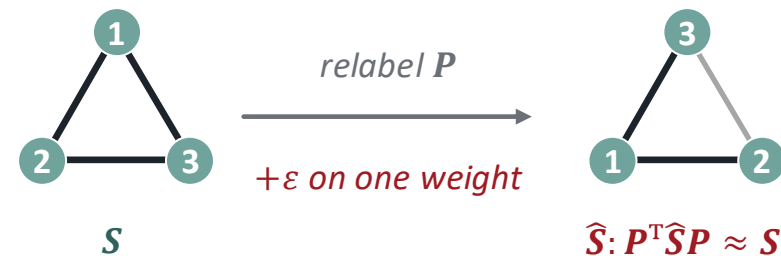


a sensor moves: $S \rightarrow \hat{S}$

LEARNING · SYMMETRIES ARE APPROXIMATE

Relabelings give exact equivariance.

Near-symmetries act like implicit data augmentation.
Similar graphs should produce similar representations.



Goal: graph distance $O(\varepsilon) \Rightarrow$ output distance $O(\varepsilon)$.

Stability is approximate equivariance under structural change.

Equivariance become quasi-equivariance

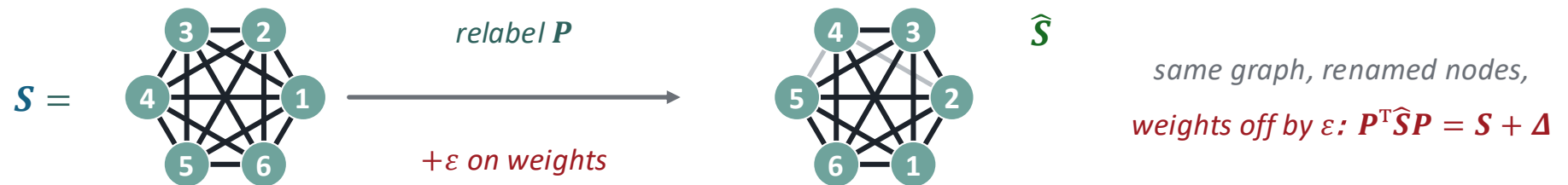
For permutation equivariance, the shift and filter commute with permutations:

$$\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} \Rightarrow h(\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P}) \mathbf{P}^T \mathbf{x} = \mathbf{P}^T h(\mathbf{S}) \mathbf{x}$$

For a quasi-equivariance, the best relabeling leaves a small residual structural change:

$$\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \Delta, \quad \|\Delta\| = \varepsilon$$

- Exact permutation equivariance gives zero output discrepancy.
- Stability makes the output discrepancy to be bounded with ε .



Equivariance is the zero-perturbation endpoint of stability.

A graph filter can be perturbed in three places

$$\mathbf{y} = h(\mathbf{S})\mathbf{x}$$

01 **INPUT** $\mathbf{x} \rightarrow \mathbf{x} + \mathbf{e}$

Easy: $h(\mathbf{S})$ is linear in $\mathbf{x}$, so the output change is controlled directly by $\|h(\mathbf{S})\|$.

02 **TAPS** $h \rightarrow h + \Delta h$

Easy: the filter is linear in its coefficients, so difference controlled by $\|\mathbf{S}\|$ and $\|\mathbf{x}\|$.

03 **SHIFT** $\mathbf{S} \rightarrow \hat{\mathbf{S}}$

Hard and essential: $\mathbf{S}$ enters through powers $\mathbf{S}^k$, so graph transfer is **nonlinear in the operator**.

Fix signal and taps, perturb only the graph

$$h(\mathbf{S})\mathbf{x} = \sum_k h_k \mathbf{S}^k \mathbf{x} \quad h(\widehat{\mathbf{S}})\mathbf{x} = \sum_k h_k \widehat{\mathbf{S}}^k \mathbf{x}$$

The same input $\mathbf{x}$ and coefficients h_k are deployed on two nearby graph shifts.

THE GRAPH DEPENDENCE LIVES IN THE POWERS

$$\begin{aligned} \Delta_h \mathbf{x} &= [h(\mathbf{S}) - h(\widehat{\mathbf{S}})]\mathbf{x} \\ &= \underbrace{[\sum_k h_k (\mathbf{S}^k - \widehat{\mathbf{S}}^k)]}_{\text{Operator norm}} \mathbf{x} \end{aligned}$$

A small shift change affects every power. Perturbations propagate by diffusions.

The stability problem is therefore an operator perturbation problem.

Compare induced filter operators after the best relabeling.

Compare graph operators modulo relabeling

Operator modulo permutation $\|\hat{\mathbf{S}} - \mathbf{S}\|_{\mathcal{P}} = \min_{\mathcal{P}} \|\hat{\mathbf{S}}\mathbf{P}^T - \mathbf{P}^T\mathbf{S}\| = \min_{\mathcal{P}} \|\mathbf{P}\hat{\mathbf{S}}\mathbf{P}^T - \mathbf{S}\|$

Apply the same measure to the induced filter operators:

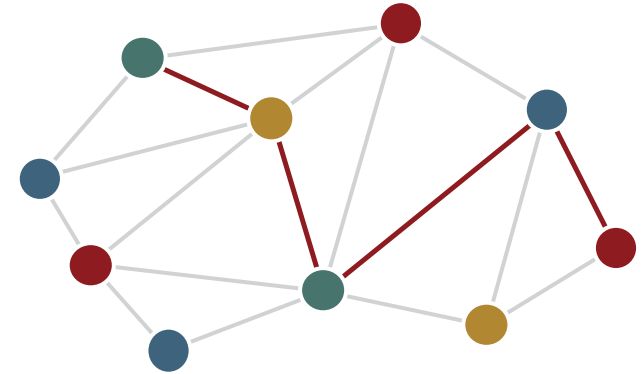
$$\|h(\hat{\mathbf{S}}) - h(\mathbf{S})\|_{\mathcal{P}} = \min_{\mathcal{P}} \|h(\hat{\mathbf{S}})\mathbf{P}^T - \mathbf{P}^T h(\mathbf{S})\|$$

- Distance zero recovers exact permutation equivariance.
- A small nonzero distance represents a quasi-symmetry after the best node correspondence.

Measure structural change within permutations.

PART II

Continuous Filters Ensure Stability under Absolute and Relative Perturbations.



- 01 Absolute model: fixed-size edge changes
- 02 Relative model: errors scale with the graph
- 03 Lipschitz filters are stable to absolute errors
- 04 Integral Lipschitz handles relative errors

Two error models,
two filter conditions,
one bound in ε .

Error and distance modulo permutation

Definition of the **error matrix** — start from the set of symmetric error matrices:

$$\mathcal{E}(\mathbf{S}, \hat{\mathbf{S}}) = \{\tilde{\mathbf{E}} : \mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \tilde{\mathbf{E}}, \quad \mathbf{P} \in \mathcal{P}\}$$

- Each permutation $\mathbf{P} \in \mathcal{P}$ gives a different error matrix $\tilde{\mathbf{E}} = \mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} - \mathbf{S}$ in the set.
- The **error matrix modulo permutation** is the one with the smallest norm: $\mathbf{E} = \arg \min_{\tilde{\mathbf{E}} \in \mathcal{E}(\mathbf{S}, \hat{\mathbf{S}})} \|\tilde{\mathbf{E}}\|$.
- $\|\mathbf{E}\| = d(\mathbf{S}, \hat{\mathbf{S}})$ measures how far $\mathbf{S}$ and $\hat{\mathbf{S}}$ are from being permutations of each other.

$$d(\mathbf{S}, \hat{\mathbf{S}}) = \|\mathbf{E}\| = \min_{\tilde{\mathbf{E}} \in \mathcal{E}(\mathbf{S}, \hat{\mathbf{S}})} \|\tilde{\mathbf{E}}\|$$

The distance modulo permutation is the norm of the best-aligned error matrix.

Δ shifts eigenvalues and rotates eigenvectors

Add and subtract the mixed term — the filter difference splits exactly into two parts:

$$\begin{aligned} h(\hat{\mathbf{S}}) - h(\mathbf{S}) &= \hat{\mathbf{V}} h(\hat{\mathbf{\Lambda}}) \hat{\mathbf{V}}^T - \hat{\mathbf{V}} h(\mathbf{\Lambda}) \hat{\mathbf{V}}^T + \hat{\mathbf{V}} h(\mathbf{\Lambda}) \hat{\mathbf{V}}^T - \mathbf{V} h(\mathbf{\Lambda}) \mathbf{V}^T \\ &= \hat{\mathbf{V}} [h(\hat{\mathbf{\Lambda}}) - h(\mathbf{\Lambda})] \hat{\mathbf{V}}^T + [\hat{\mathbf{V}} h(\mathbf{\Lambda}) \hat{\mathbf{V}}^T - \mathbf{V} h(\mathbf{\Lambda}) \mathbf{V}^T] \end{aligned}$$

- **Eigenvalue channel** — the diagonal of Δ in the eigenbasis. Weyl: every eigenvalue moves by at most ε
- **Eigenvector channel** — Davis–Kahan tells the distance between eigenvector spaces, or by defining eigenvector mismatches

Filter function controls the eigenvalue channel. Perturbation decides the eigenvector channel.

Eigenvector rotation appears in the stability bound

Why does the bound contain an alignment factor δ ?

- Eigendecompose the shift and the error: $\mathbf{S} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^H$ and $\mathbf{E} = \mathbf{U}\mathbf{M}\mathbf{U}^H$.

- Define the **eigenvector misalignment** between $\mathbf{S}$ and $\mathbf{E}$ as

$$\delta = (\|\mathbf{U} - \mathbf{V}\| + 1)^2 - 1$$

- $\mathbf{U}$ and $\mathbf{V}$ are unitary, $\|\mathbf{U}\| = \|\mathbf{V}\| = 1 \Rightarrow \delta \leq (2 + 1)^2 - 1 = 8$. – worst case bound
- If $\mathbf{S}$ and $\mathbf{E}$ share eigenvectors ($\mathbf{U} \approx \mathbf{V}$), then $\delta \approx 0$ — the perturbation mainly moves eigenvalues.

The misalignment δ can be small, depending on the error model.

Eigenvalue sensitivity is shaped by h . Eigenvector sensitivity is shaped by the graph error.

Lipschitz filters are stable to additive perturbations

- Shift matrix related with $\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \mathbf{E}$
- Error matrix $\|\mathbf{E}\| = \varepsilon$
- Lipschitz frequency response
 $|h(\lambda_2) - h(\lambda_1)| \leq C |\lambda_2 - \lambda_1|.$

$$\|h(\hat{\mathbf{S}}) - h(\mathbf{S})\|_{\mathcal{P}} \leq C(1 + \delta\sqrt{n})\varepsilon + O(\varepsilon^2)$$

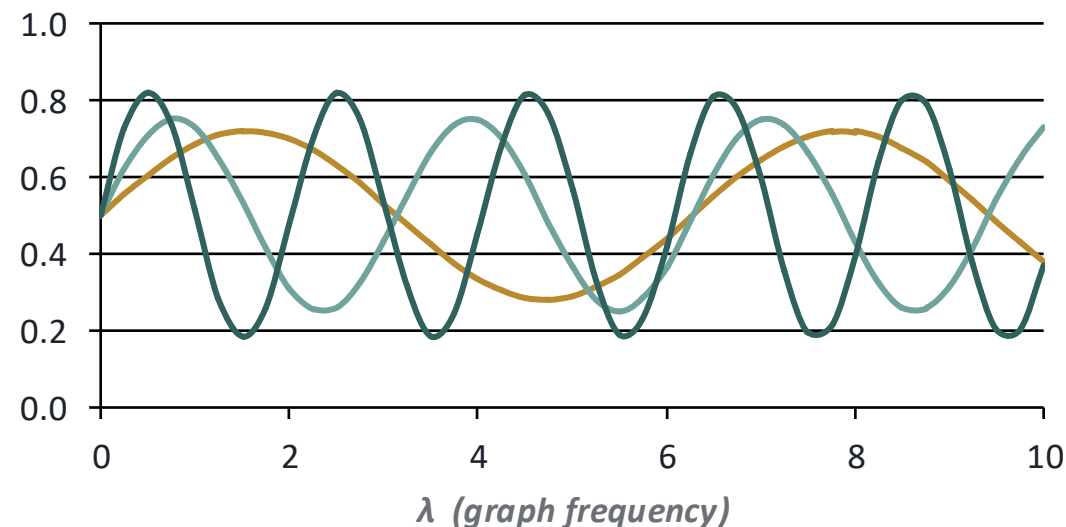
FIRST-ORDER STRUCTURE

filter error = response slope $\times$ alignment $\times$ graph error

The leading term is linear in ε . The higher-order remainder vanishes faster than ε as the perturbation shrinks.

Lipschitz responses: $|h'(\lambda)| \leq C$

— $C = 0.25$ — $C = 0.5$ — $C = 1.0$



A controllable spectral slope turns graph closeness into output closeness.

Design controls $\mathcal{C}$. Deployment controls ε, δ, n

CONTROLLED · FILTER SMOOTHNESS $\mathcal{C}$

Choose smoother $h(\lambda)$.

Regularize or constrain the taps.

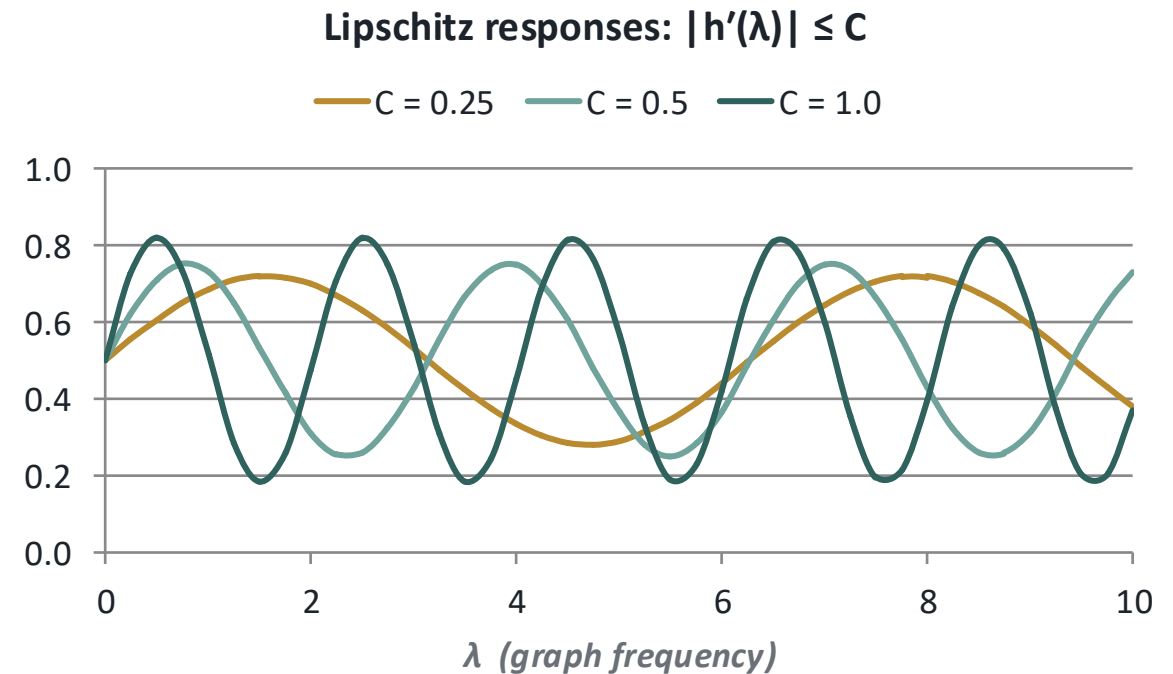
Trade sharp spectral selectivity for robustness.

UNCONTROLLED · ε, δ, n

ε measures graph drift.

δ measures eigenspace misalignment.

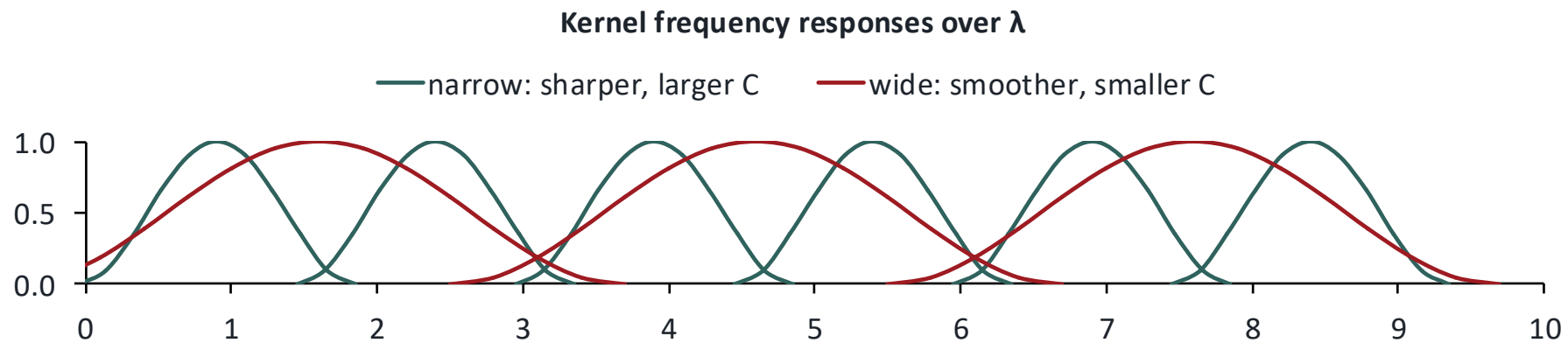
n records graph size in the universal worst-case estimate.



The theorem exposes an architectural knob and an environmental cost.

Stability trades off discriminability

- Bound is universal for all graphs with nodes n
 - Continuity of filter's frequency response
 - Properties of perturbation $\mathbf{E}$
- Discriminability and stability tradeoff – Larger C , sharper discriminability, worse stability
- The theorem factors learned-filter sensitivity from deployed-graph geometry.



Continuity says the map behaves locally. Stability quantifies how well it transfers.

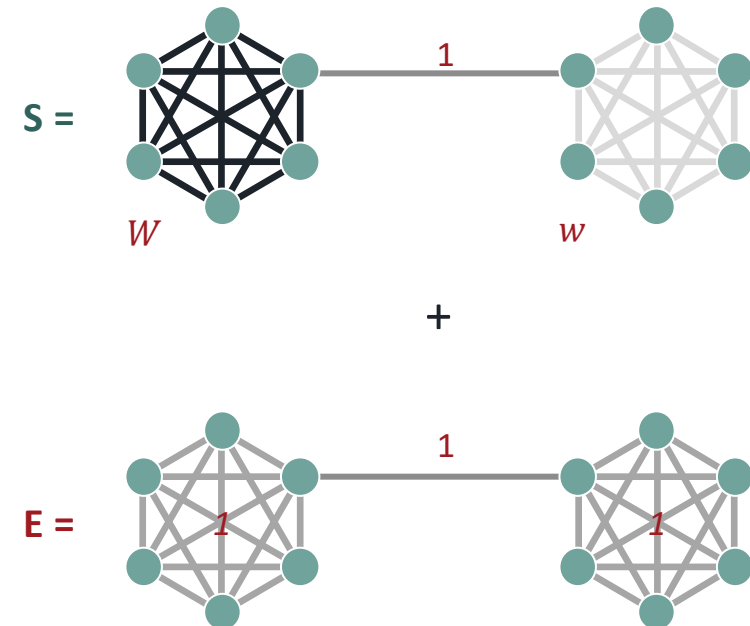
Absolute edge errors can be physically misleading

Suppose $w \ll 1 \ll W$.

$$\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \mathbf{E}$$

- Can we claim the perturbation is large or small?
- For edges with weights w — changes are larger

Many physical graphs are governed by proportional calibration, distance, or gain errors.



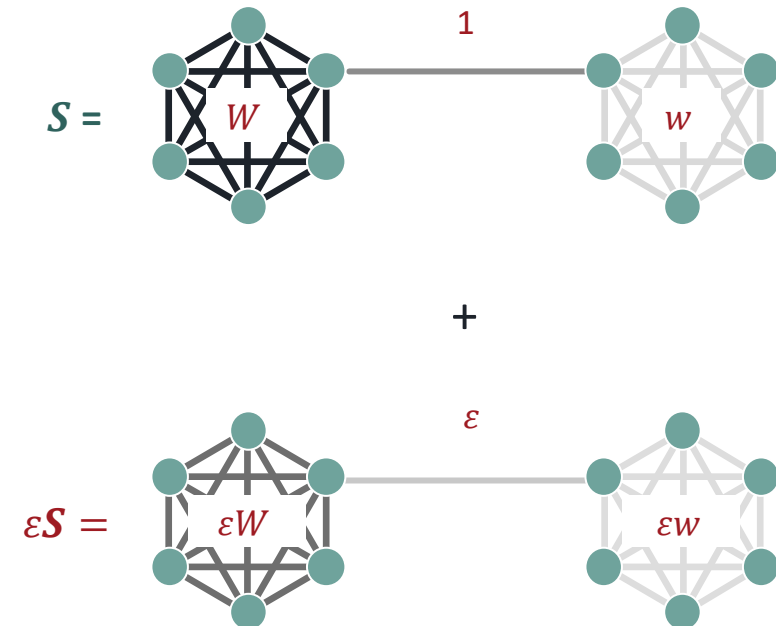
Weighted graphs often require a perturbation measured relative to local connectivity.

Relative perturbations are meaningful

Suppose $w \ll 1 \ll W$.

$$P^T \hat{S} P = S + \epsilon S$$

- Can we claim the perturbation is large or small?
- It's small with larger edge weights change more and smaller change less



Weighted graphs often require a perturbation measured relative to local connectivity.

Error and distance modulo permutation

Definition of the **error matrix** — start from the set of **symmetric** error matrices:

$$\mathcal{E}(\mathbf{S}, \hat{\mathbf{S}}) = \{\tilde{\mathbf{E}} : \mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \tilde{\mathbf{E}} \mathbf{S} + \mathbf{S} \tilde{\mathbf{E}}, \quad \mathbf{P} \in \mathcal{P}\} \quad (\mathbf{I} + \mathbf{E}) \mathbf{S} (\mathbf{I} + \mathbf{E})$$

- The **error matrix modulo permutation** is the one with the smallest norm: $\mathbf{E} = \arg \min_{\tilde{\mathbf{E}} \in \mathcal{E}(\mathbf{S}, \hat{\mathbf{S}})} \|\tilde{\mathbf{E}}\|$.
- $\|\mathbf{E}\| = d(\mathbf{S}, \hat{\mathbf{S}})$ is a **relative measure** of how far $\mathbf{S}$ and $\hat{\mathbf{S}}$ are from being permutations of each other.

$$d(\mathbf{S}, \hat{\mathbf{S}}) = \|\mathbf{E}\| = \min_{\tilde{\mathbf{E}} \in \mathcal{E}(\mathbf{S}, \hat{\mathbf{S}})} \|\tilde{\mathbf{E}}\|$$

The distance modulo permutation is the norm of the best-aligned error matrix.

Relative errors follow local connectivity

$$[\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P}]_{ij} = [\mathbf{S} + \mathbf{E}\mathbf{S} + \mathbf{S}\mathbf{E}]_{ij} = \mathbf{S}_{ij} + \sum_{m \in \mathcal{N}_j} \mathbf{E}_{im} \mathbf{S}_{mj} + \sum_{m \in \mathcal{N}_i} \mathbf{S}_{im} \mathbf{E}_{mj}$$

Edge changes are proportional to original weights and perturbations at two endpoints.

DIAGONAL ERROR OPERATORS MAKE THE SCALING EXPLICIT

$$\mathbf{E} = \text{diag}(e_1, \dots, e_n) \Rightarrow [\mathbf{E}\mathbf{S} + \mathbf{S}\mathbf{E}]_{ij} = (e_i + e_j) \mathbf{S}_{ij}$$

Parts of the graph with lower weighted degree see smaller changes

In additive perturbations weights can change the same regardless of the connectivity.

The model connects matrix perturbations to local physical calibration.

Relative errors need integral-Lipschitz smoothness

LIPSCHITZ · ABSOLUTE SCALE

Controls response change w.r.t. absolute frequency separation.
The same slope limit applies everywhere.

$$|h(\lambda) - h(\lambda')| \leq C|\lambda - \lambda'|$$

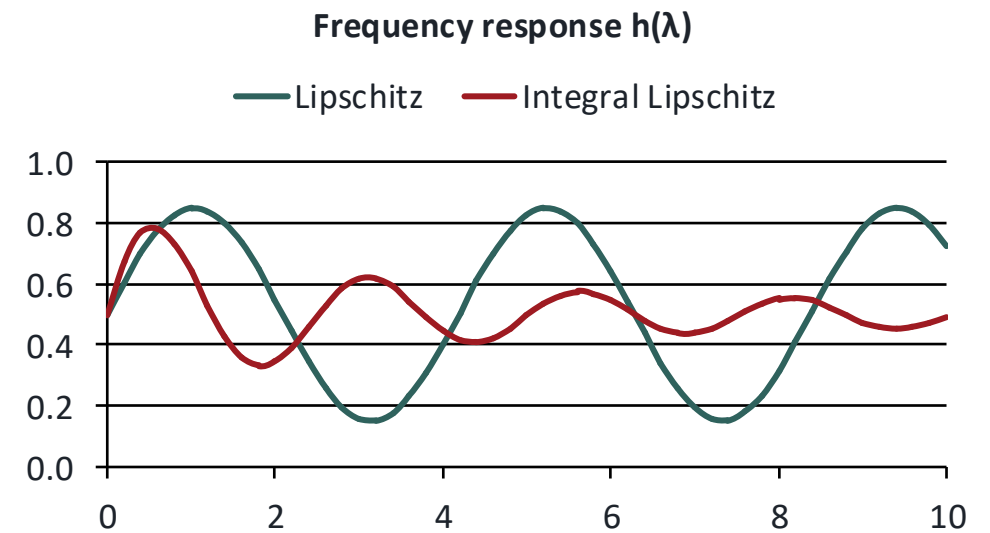
$$|h'(\lambda)| \leq C$$

INTEGRAL-LIPSCHITZ · RELATIVE SCALE

Controls response change relative to frequency changes.
The response becomes flatter at large $|\lambda|$.

$$|h(\lambda) - h(\lambda')| \leq \frac{C|\lambda - \lambda'|}{|\lambda + \lambda'|/2}$$

$$|\lambda h'(\lambda)| \leq C$$



Choose smoothness in the geometry induced by the perturbation.

Additive errors match ordinary Lipschitz. Relative errors match integral-Lipschitz.

Integral-Lipschitz filters stabilize relative errors

- Shift matrix related with $\mathbf{P}^T \hat{\mathbf{S}} \mathbf{P} = \mathbf{S} + \mathbf{E} \mathbf{S} + \mathbf{S} \mathbf{E}$
- Error matrix $\|\mathbf{E}\| \leq \varepsilon$
- Lipschitz frequency response

$$|\lambda h'(\lambda)| \leq C.$$

$$\|h(\hat{\mathbf{S}}) - h(\mathbf{S})\|_{\mathcal{P}} \leq 2C(1 + \delta\sqrt{n})\varepsilon + O(\varepsilon^2)$$

WHY THE FACTOR TWO?

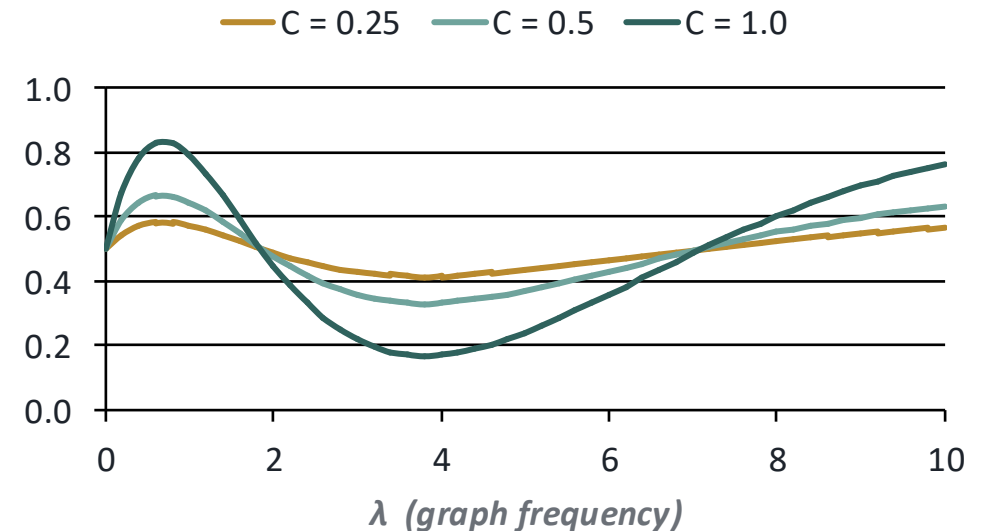
relative error = $\mathbf{E} \mathbf{S} + \mathbf{S} \mathbf{E}$

FIRST-ORDER STRUCTURE

filter error = response slope $\times$ alignment $\times$ graph error

Apart from the factor two, the first-order interpretation matches the additive theorem.

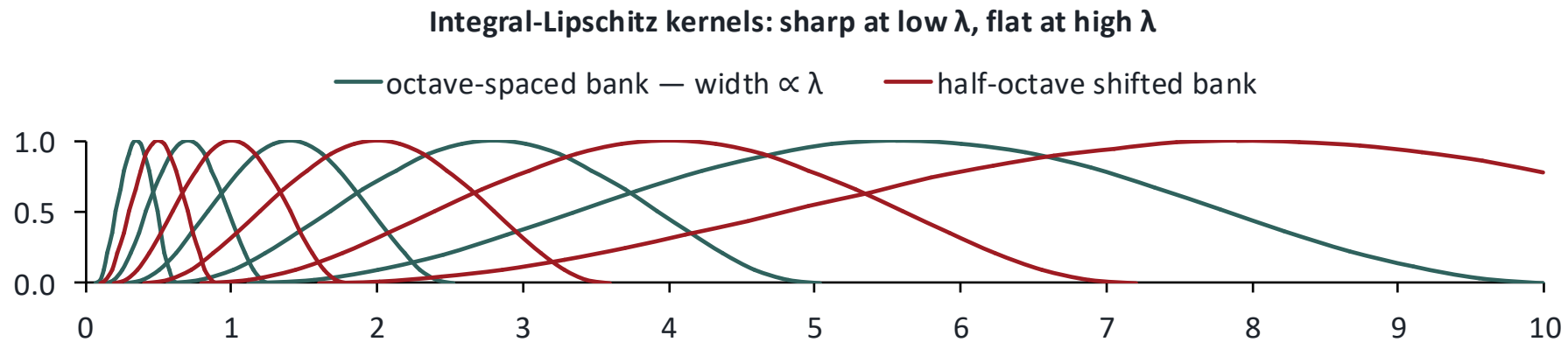
Integral-Lipschitz responses



Structure-aware errors still produce a linear first-order guarantee.

Stability tradeoff discriminability

- Bound is universal for all graphs with nodes n
 - Continuity of filter's frequency response – **integral Lipschitz filters**
 - Properties of **perturbation E**
- **Discriminability and stability tradeoff** – Larger C , better discriminability, worse stability
- The theorem factors **learned-filter sensitivity** from **deployed-graph geometry**



Continuity says the map behaves locally. Stability quantifies how well it transfers.

Linear filters trade stability for discrimination

STABILITY

Small C. Smooth spectral transitions.

Smooth response at nearby frequencies.

Reliable transfer across perturbed graphs.

Limited sensitivity to spectral detail.

DISCRIMINATION

Large C. Sharp spectral transitions.

Resolve nearby eigenvalues.

Capture task-specific high-frequency structure.

Larger perturbation sensitivity.

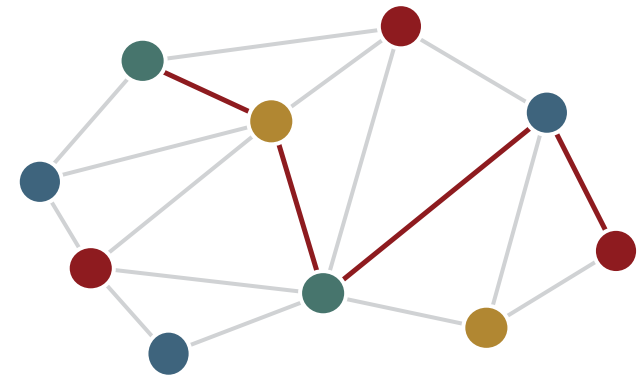
How to resolve this tradeoff?

Use nonlinear depth to recover expressivity without an unstable linear response.

PART III

Stable filters become expressive when cascaded.

- 01 Add a pointwise nonlinearity after each filter
- 02 Carry multiple feature channels at every node
- 03 Normalize filters and activations
- 04 Propagate layer-wise error through depth

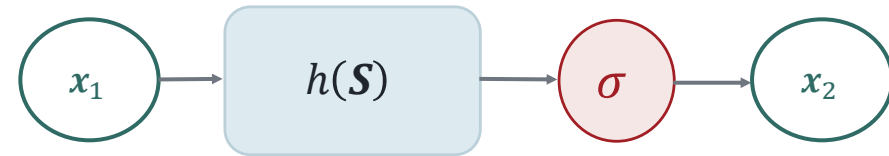


**The cascade inherits stability
and gains nonlinear
discrimination.**

A graph perceptron is a filter followed by σ

First apply a polynomial graph filter, then activate every node independently:

$$\mathbf{z} = h(\mathbf{S})\mathbf{x}_1 = \sum_k h_k \mathbf{S}^k \mathbf{x}_1 \quad \mathbf{x}_2 = \sigma(\mathbf{z})$$



- $h(\mathbf{S})$ aggregates information -- coefficients determine the spectral response and the local mixing rule.

- σ is pointwise - ReLU, tanh, or sigmoid--adds nonlinear expressivity without adding analysis complexity if it's normalized Lipschitz

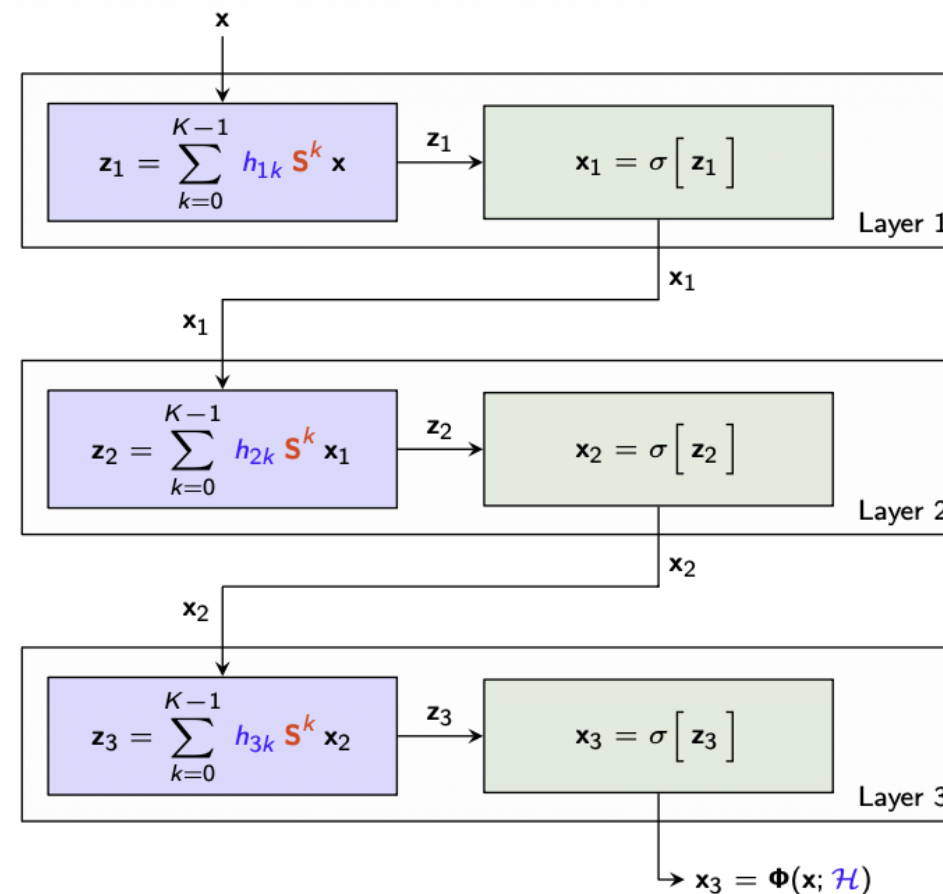
Filter locally, activate nodewise.

Filter, activate, repeat: the GNN cascade

$$\mathbf{x}_\ell = \sigma(h_\ell(\mathcal{S})\mathbf{x}_{\ell-1}), \quad \mathbf{x}_0 = \mathbf{x},$$

$$\mathbf{x}_L = \Phi(\mathcal{S}, \mathbf{x}; \mathcal{H})$$

Every stage reuses the graph geometry but **learns its own filter** and **feature representation**.



Depth expands the receptive field and composes nonlinear representations.

Normalization keeps the cascade nonexpansive

FILTER NONAMPLIFYING

$$\|h_\ell(\mathbf{S})\| \leq 1$$

A layer cannot magnify an incoming representation before the graph perturbation is considered.

ACTIVATION NORMALIZATION

$$\|\sigma(a) - \sigma(b)\| \leq \|a - b\|$$

ReLU and tanh are 1-Lipschitz
 σ is applied independently at every node.

Each layer is non-expansive except for the mismatch between $h_l(\hat{\mathbf{S}})$ and $h_l(\mathbf{S})$.

Normalization converts a local filter bound into a depth-wise recurrence.

Each layer adds graph error to inherited error

Non-expansiveness removes the activation from the upper bound.

Proof technique -- Add and subtract $h_l(\mathcal{S})\hat{\mathbf{x}}_{l-1}$

Output difference: $\Delta_\ell = \|\hat{\mathbf{x}}_\ell - \mathbf{x}_\ell\| \leq \|h_l(\hat{\mathcal{S}})\hat{\mathbf{x}}_{l-1} - h_l(\mathcal{S})\mathbf{x}_{l-1}\|$

TRIANGLE INEQUALITY SPLITS THE TWO ERROR SOURCES

$$\Delta_\ell \leq \| [h_\ell(\hat{\mathcal{S}}) - h_\ell(\mathcal{S})] \hat{\mathbf{x}}_{l-1} \| + \| h_\ell(\mathcal{S}) (\hat{\mathbf{x}}_{l-1} - \mathbf{x}_{l-1}) \| \leq c\varepsilon + \Delta_{l-1}$$

Filter stability
bound

Non-amplifying
assumption

Iterative term

Filter stability bounds the first term by $c\varepsilon + O(\varepsilon^2)$. Unit operator norm bounds the second by Δ_{l-1} .

GNNs inherit the additive and relative filter bounds

Apply the same inequality at layers $\ell - 1, \ell - 2$, and so on.

AFTER L LAYERS
$$\Delta_L \leq c\varepsilon + c\varepsilon + \dots + c\varepsilon = Lc\varepsilon$$

ADDITIVE PERTURBATIONS

$$c = C(1 + \delta\sqrt{n})$$

$$\|\Phi(\cdot; \hat{\mathbf{S}}) - \Phi(\cdot; \mathbf{S})\|_{\mathcal{P}} \leq C(1 + \delta\sqrt{n})L\varepsilon + O(\varepsilon^2)$$

RELATIVE PERTURBATIONS

$$c = 2C(1 + \delta\sqrt{n})$$

$$\|\Phi(\cdot; \hat{\mathbf{S}}) - \Phi(\cdot; \mathbf{S})\|_{\mathcal{P}} \leq 2C(1 + \delta\sqrt{n})L\varepsilon + O(\varepsilon^2)$$

Under the normalizations, errors do not multiply across layers. The worst-case first-order cost grows linearly, not exponentially, with depth.

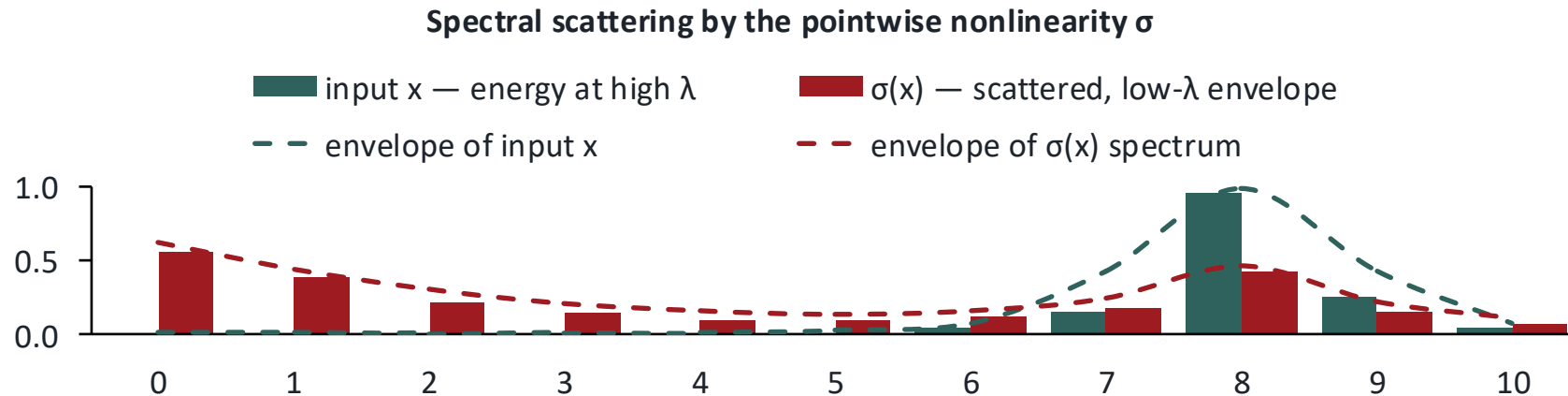
Depth accumulates stable layer errors additively.
The architecture preserves first-order robustness to graph perturbations.

Pointwise Nonlinearity restores discriminability

Nonlinearity seems affect little in vertex domain, in spectral domain it is key

- The pointwise nonlinearity scatters spectral components across the spectrum.
- The next stable filter can extract the low frequency parts robustly.

Repeating this mechanism separates signals that one smooth linear filter cannot distinguish, thus improves the discriminability while maintain stability.



Nonlinearity moves discriminative information into frequency regions where stable filters can use it.

Checkpoint: derive the guarantee

01 Before comparing two graph shifts, which optimization removes arbitrary node names?

Think: align the graphs with a permutation matrix.

minimize over $P \in \mathcal{P}$

02 Which response condition matches the relative model $S + ES + SE$?

Think: multiplicative frequency changes.

integral-Lipschitz, $|\lambda h'(\lambda)| \leq C$

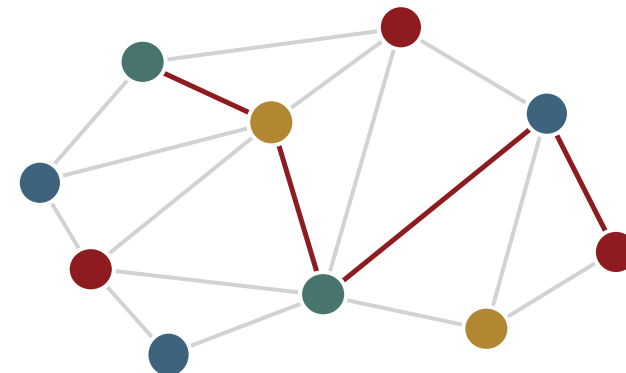
03 Why does the normalized GNN bound grow as $L\varepsilon$ instead of exponentially?

Think: nonexpansive layers and a telescoping recurrence.

each layer adds at most $c\varepsilon$ under unit norms

TAKEAWAYS

Stable layers. Expressive cascade.



- 01 Align graph shifts before measuring perturbations
- 02 Lipschitz for additive · integral-Lipschitz for relative
- 03 Normalize filters and pointwise nonlinearities
- 04 Propagate layer errors to obtain the $O(L\varepsilon)$ bound

**Nonlinear depth recovers discrimination
without sacrificing first-order stability.**